

**Frank
Riccardi**



**The Hacker's Playbook
(And How to Beat It)**

PRAISE FOR

CTRL+ALT+PWN

“Covering cybersecurity since 2004, I’ve watched the same core scams — impersonation, credential theft, confidence tricks — continually reinvent themselves. What began as crude phishing and identity theft now resurfaces as ransomware, business email compromise, and AI-driven deepfakes. To anyone outside the field, each wave can feel entirely new. Headlines warn of the latest threat, yet few resources step back to explain how these tactics evolve — and what that means for everyday consumers. In *CTRL+ALT+PWN*, Frank Riccardi brings welcome clarity. He demystifies modern cybercrime and connects the psychology, the tools, and the technology in plain English. This is the kind of contextual, up-to-date understanding consumers have long needed.”

—**BYRON ACOHIDO**, Pulitzer Prize-winning journalist and Editor-in-Chief of *The Last Watchdog on Privacy & Security*

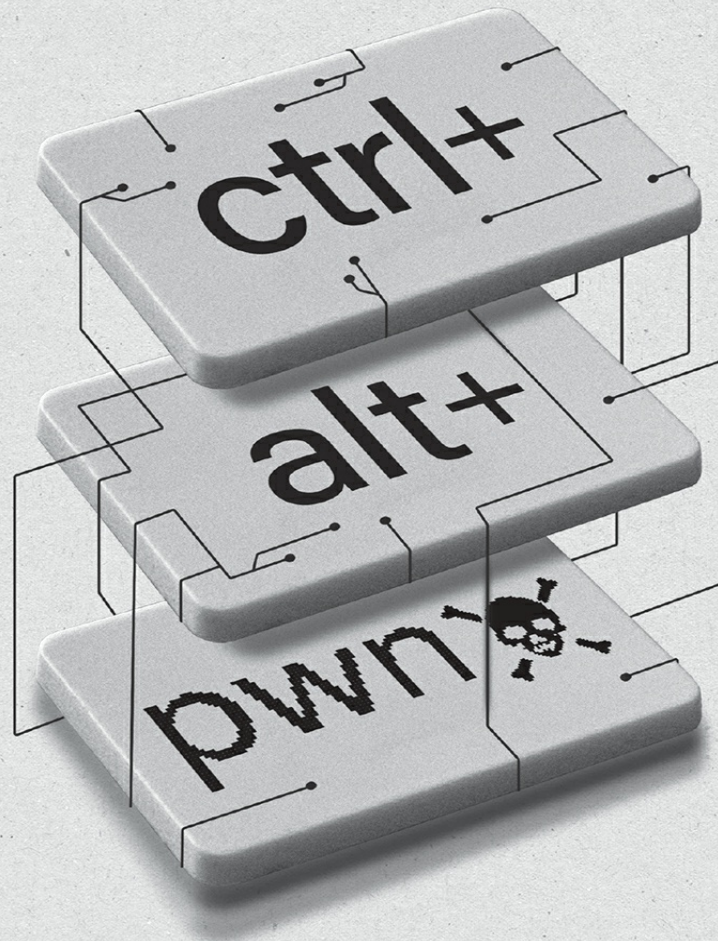
“In a field crowded with noise, *CTRL+ALT+PWN* stands out as a rare combination of technical accuracy and everyday accessibility. Frank Riccardi provides a much-needed roadmap for navigating the modern threat landscape with confidence. *CTRL+ALT+PWN* is a must-read for anyone who wants to stay safe online.”

—**BOB LORD**, creator of Hacklore.org

“Frank Riccardi’s book is a great book on hacking, distinctive in how well it is written and its storytelling. People learn through stories, and his book has plenty. Along the way, Frank shares how hackers hack and what you can do to best protect yourself.”

—**ROGER A. GRIMES**, CISO Advisor for KnowBe4 and author of *A Data-Driven Computer Defense and How AI and Quantum Impact Cyber Threats and Defenses*

Frank Riccardi



**The Hacker's Playbook
(And How to Beat It)**

TURNER
PUBLISHING COMPANY

TURNER PUBLISHING COMPANY
Nashville, Tennessee
www.turnerpublishing.com



CTRL+ALT+PWN: The Hacker's Playbook (And How to Beat It)
Copyright © 2026 by Frank Riccardi. All rights reserved.

This book or any part thereof may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.

Limit of Liability/Disclaimer of Warranty: While the publisher and the author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor the author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For rights inquiries, please reach out to admin@turnerpublishing.com.

Cover and wrap design by Ben Prior
Book design by Ashlyn Inman

Library of Congress Control Number: 2025049120

ISBN (hardcover): 9798887981604
ISBN (paperback): 9798887981611
ISBN (epub): 9798887981628

Printed in the United States of America

CONTENTS

Introduction: Pwned—It's Not a Typo, It's a Warning

Part 1: The Hacker's Playbook: From Mindset to Malware to Mayhem

[Chapter 1: Hackers Gonna Hack: The Making of a Cybercriminal](#)

[Chapter 2: Hackers Gonna Hack: But Some Have Horns and Some Have Halos](#)

[Chapter 3: Hackers Gonna Hack: And the Law Ain't Gonna Stop Them](#)

[Chapter 4: Hacking Tools: Everything Everywhere All at Once](#)

[Chapter 5: Hacking Tools Are Dangerous. So What Can We Do About It?](#)

Part 2: A Peek Inside the Playbook: Threats, Tactics, and Technology

[Chapter 6: The Hacker's Ransomware Playbook](#)

[Chapter 7: How Do I Reuse Thee? Let Me Count the Ways!](#)

[Chapter 8: Your Smartphone is a Productivity Godsend. It's Also a Dystopian Wasteland Hell-bent on Pwning You](#)

[Chapter 9: The Nigerian Prince Who Was the King of Phishing](#)

[Chapter 10: Romance Scams: "I Love You, Baby. Now Send Me More Money!"](#)

[Chapter 11: The Hacker's Deepfake Playbook](#)

[Chapter 12: Cybercriminals Want to Pwn You with Deepfakes. This Is How You Stop Them.](#)

[Chapter 13: Quantum Computing and Artificial Intelligence: A Marriage Made in Hell?](#)

Part 3: Beating the Hacker's Playbook

[Chapter 14: Is "Ethical Deepfake" an Oxymoron?](#)

[Chapter 15: Victim Blaming: The Hacker's Cruel Accomplice](#)

[Chapter 16: Oops, That Breach Is on You: The Finger-Pointing Art of Corporate Blame Shifting](#)

Conclusion: Smashmouth Cybersecurity— Never Get Pwned Again!

Acknowledgments

[Glossary](#)

[Endnotes](#)

[Index](#)

[About the Author](#)

To the pwned—that means all of us.

INTRODUCTION

Pwned—It's Not a Typo, It's a Warning

The word *pwned* is a mocking taunt used by hackers to proclaim a victory that is so crushing it leaves the loser shamed and humiliated. Pwned is pronounced like “owned” but with a “p” sound at the beginning, and is often linked with *noob*, a derogatory term pegging someone as clueless and incompetent.¹ Cybercriminals target pwned noobs, or victims, who lack the skills and knowledge to defend themselves from cyberattacks that can ruin their lives.

Pwned noobs are fattened up for slaughter because cybercriminals have the upper hand, enjoying a gratuitous advantage not of the cybercriminals’ making but born in television shows and movies perpetuating the ludicrous myth that cybercriminals are little more than hoodie-wearing teenagers goofing around in their parents’ basements. The legend of the hoodie-hacker is perhaps best exemplified in a 2016 presidential debate when candidate Donald J. Trump responded to candidate Hillary Clinton’s claims of Russian hacking with this famous zinger:

It could be Russia but it could be China, it could be lots of people. It could be somebody that sits on their bed that weighs 400 pounds.²

For many people, hackers are just that—pimply faced high schoolers cloaked in a black hoodie, launching cyberattacks from the comfort of their parents’ basement while lounging on a puffy couch in baggy sweatpants and chugging Red Bull. The only thing missing from this scene is the electronic beat of techno-pop drowning out Mom’s plea to turn the music down.

The hoodie-hacker is a preposterous stereotype but one that is popularized in the media. Hoodie-hacker stereotypes are seen in movies like *The Matrix* and *The Girl with the Dragon Tattoo* and TV shows like *Mr. Robot*. Often, the media portrays the typical hacker as a young adult with a social phobia and no formal training in cybersecurity but who has enough smarts to hack into the FBI’s network in minutes flat with only a few clicks on a keyboard.³

If you’re a non-geek, the hoodie-hacker meme is entertaining brain candy—but to cybersecurity professionals, it’s a ridiculous and dangerous stereotype. It’s absurd because ethical hackers have years of experience and earn multiple certifications, enabling them to test physical and network security with skill and grace. It’s dangerous because C-suite executives will be loath to adequately fund cybersecurity if they believe their principal threat is a socially awkward teenager eating Ding Dongs in a basement. Why should companies invest in a team of trained cybersecurity professionals when cybercriminals are just a bunch of punks who learned how to hack stuff all by themselves?

Let's continue this dangerous line of thinking. The hoodie-hacker has no plans, strategy, or goals other than the instant gratification of scoring a ransomware payment so they can buy junk food and weed. So, why should the United States spend millions of dollars on law enforcement to catch cybercriminals when they're just a bunch of introverted knuckleheads? When politicians believe in the hoodie-hacker trope, there's no motivation to boost cybersecurity funding for critical agencies like the Department of Homeland Security (DHS) or the Cybersecurity and Infrastructure Security Agency (CISA). Worse, there's no urgency in upgrading antiquated systems or enforcing cyber hygiene across federal agencies. Why rush installing that security patch or require hardworking federal employees to log in with strong passwords? Oh, and about that annoying multifactor authentication fob—fuggedaboutit!

You can see that the hoodie-hacker stereotype is dangerous because it leads to an underappreciation of cyber risk and mismanagement of resources badly needed to combat the real threat actors: sophisticated and well-organized cybergangs like DarkSide and REvil. When companies and governments let their guard down, the result is inadequate funding for cybersecurity and law enforcement initiatives that could protect the public from destructive cyberattacks.

Along those lines, when the general public believes in the hoodie-hacker stereotype, they're just as likely to minimize the risk of becoming the victim of a cybercrime. After all, why go through the hassle of using strong passwords and multifactor authentication because of some Mountain Dew-swalling dork in a basement? This, of course, is techno-pop to the ears of cybercriminals, who are trained, educated, and often supported by high-tech criminal enterprises with the financial backing of a nation-state threat actor.

The neurotic teenager hacking into NASA on a cell phone is the stuff of fantasy. The hackers working for cybergangs like DarkSide and REvil are the exact opposite of the untrained hoodie-wearing basement hacker.⁴ It's time for the entertainment industry to develop more realistic portrayals of hackers and for cybersecurity professionals to call out these cartoonish stereotypes for what they are—an insult to ethical hackers who spend years honing their skills and earning countless certifications to remain current and productive in the cybersecurity profession.

The fact of the matter is the myth of the hoodie-hacker is easily debunked. Let's consider three infamous pwnings to demonstrate that cybercriminals are wily, competent, and very much the opposite of a neurotic teenager hacking into NASA on a cell phone.

Infamous Pwning One: Actor Seth Green played Oz, a werewolf, on the TV show *Buffy the Vampire Slayer*. In addition to moonlighting as a lycanthrope, Oz was an uber-cool musician with a penchant for wisecracks and a retro Volkswagen bus suitable for transporting band equipment and running over vampires. Oz was not particularly good with computers—hacking into the Initiative's mainframe to uncover demonic experiments was Willow's thing—and just as life imitates art, Oz's mediocre cyber skills matched Seth Green's, as the actor fell for a phishing scam involving a fake website that pretended to sell NFTs (non-fungible tokens).

NFTs were all the rage in 2022 when Seth Green connected his crypto wallet to a phishing website that stole four of his NFTs worth over \$300,000—two Mutant Ape Yacht Club NFTs, a Doodle NFT, and a Bored Ape Yacht Club NFT.⁵ If the names sound peculiar, that's a feature, not a bug, of the NFT collecting fad. Bored Apes comprise 10,000 unique digital images of—no surprise—simian cartoon characters sporting different attributes, such as fur color, clothing, and headgear.⁶ The rarer the feature, the more valuable the NFT. For example, there are Bored Apes

with gold fur, trippy captain's hats, and black suits. Seth Green's Bored Ape, who he named "Fred Simian," was particularly valuable as it contained numerous rare traits: A bone T-shirt making it look like the ape's chest was X-rayed, droopy-sad eyes, an unshaven face with a cigarette poking from the mouth, and a bright halo hat.⁷ Add the unique traits up, and in 2022, Fred Simian could easily have fetched north of \$200,000 on OpenSea, the world's largest trading platform for crypto collectibles at that time.⁸

Bored Ape NFTs are essentially digital cartoons existing on a blockchain—a public database used as a ledger for recording crypto transactions. However, an unusual benefit to owning a Bored Ape NFT is you enjoy full commercial rights for whatever products you create from the NFT.⁹ Seth Green had planned to develop a television series based on his Bored Ape, but that plan got put on hold when the scammer who stole Fred Simian sold it to someone identifying as DarkWing84 on Twitter. Once DarkWing84 bought Fred Simian from the scammer, all copyrights to the cigarette-smoking, halo-wearing ape now belonged to the pseudonymous DarkWing84!¹⁰ And since blockchain is a decentralized ledger, there's no way to reverse transactions, which meant Seth Green was in a real pickle unless he could buy the Bored Ape from DarkWing84—precisely what the actor did. However, it cost a whopping \$297,000 in Ether cryptocurrency to put Fred Simian back in Seth Green's cage. So, to put this monkey business in perspective: Green reportedly shelled out \$200,000 to own Fred Simian, then another \$297,000 to bring him back home—proof that in the world of NFTs, possession isn't just nine-tenths of the law, it's the whole freaking blockchain!¹¹ The Bored Ape phishing scam is a prime example of why believing the hoodie-hacker mythology is foolish. No teenage hacker with little more than a keyboard and a half-eaten bag of stale tortilla chips could pull off such a sophisticated cyberattack.

Infamous Pwning Two: Superstar Notre Dame linebacker Manti Te'o was the victim of a catfishing scam in 2012. He believed he was in a romantic relationship with a girl named Lennay Kekua, who turned out to be a fake online persona.¹² Manti Te'o's fake girlfriend was concocted by a fellow twentysomething Polynesian, Naya Tuiasosopo, a transgender woman who was previously known at the time as Ronaiah Tuiasosopo.¹³

Manti Te'o met Lennay on social media, and the friendship blossomed into romance as the couple chatted through texts, online messages, and phone calls. In reality, catfisher Tuiasosopo stole the identity of a former high school classmate, Diane O'Meara, and used photos from her Facebook and MySpace accounts without her permission.¹⁴ Tuiasosopo exploited actual images of Diane O'Meara to invent the fake girlfriend that Manti Te'o fell head over heels in love with. As a testament to the extraordinary personal effort invested in the scam, Tuiasosopo mimicked the voice of a college-aged female with such verisimilitude that Manti Te'o actually believed he was talking to a girl from Stanford University.¹⁵

Besotted by his make-believe lover, Manti Te'o's life shattered like a windowpane struck by an NFL game ball when he learned that Lennay had died of leukemia—a synchronous tragedy coming on the heels of the death of his grandmother the same day. The heartbreaking loss also came within a day of the football game against Michigan State—but Manti Te'o's grief-fueled tenacity to play while in mourning brought the Fighting Irish to a now-legendary victory. The public outpouring of support made Manti Te'o a household name and the leading candidate for the Heisman Trophy, the highest award in college football.

Several months later, the public adulation turned to scorn as a Deadspin exposé revealed that

Lennay Kekua didn't exist and Manti Te'o was the victim of a catfishing scam. Back in 2012, catfishing was not well known, though the term had been coined in a 2010 documentary called *Catfish* about a man who falls for a 19-year-old girl he met online who turns out to be a 40-year-old housewife from Michigan.¹⁶

Today, catfishing is a more widely known scam, and people who've been suckered are considered victims—but back in 2012, Manti Te'o was ridiculed as a fool.¹⁷ Sure, it's easy to mock Manti Te'o but be forewarned: getting pwned at the hands of a wily catfisher can happen to anyone, even you. In 2022, 73,000 cases of romance scams were reported in the United States, and the financial loss from romance scams reached an eye-popping \$1.3 billion, a 164 percent increase from 2019.¹⁸ When 73,000 Americans get soaked for more than \$1 billion, it's not an outlier—it's an epidemic.

These wildly successful catfishers are not some pimply-faced teenagers in hoodies and sweatpants. They are sophisticated and organized cybercriminals who exploit people's emotions and trust.

Infamous Pwning Three: What's more embarrassing than accidentally texting a nude photo to your mother that was intended for your boyfriend? Well, that's easy—picture the emotional desolation you'd feel when your naked body pops up on 4chan for all the world to ogle. 4chan is a popular *imageboard*, a fancy word describing a website where people can post images. What makes 4chan controversial is that anyone can post pictures anonymously.¹⁹ This means Peeping Toms, pedophiles, and other miscreants can post and brag about images they've obtained without the subject's knowledge. You can see why 4chan is a cybercriminal paradise.

In 2014, sexually explicit photographs of dozens of celebrities began circulating on 4chan. In a massive cyberattack dubbed "Celebgate," hackers stole hundreds of private photos from 101 celebrities, including Oscar-winning actress Jennifer Lawrence, *Sports Illustrated* swimsuit model Kate Upton, and American actress Mary Elizabeth Winstead.²⁰ The hackers launched a phishing campaign by sending fake emails pretending to be from Apple requesting the celebrities to provide their Apple ID and password to correct a security issue.²¹ In some cases, the celebrities were directed to enter their credentials into a fake third-party website created by the hackers.²² The hackers then used the phished credentials to download backups from Apple's iCloud storage service, from which they stole the celebrity victims' nude photographs.

When the hackers posted the nude photographs on 4chan, the celebrity victims felt humiliated, shamed, and violated. In a 2014 *Vanity Fair* article, Jennifer Lawrence bared her soul about the Celebgate hack:

Just because I'm a public figure, just because I'm an actress, does not mean that I asked for this. It does not mean that it comes with the territory. It's my body, and it should be my choice, and the fact that it is not my choice is absolutely disgusting.

It is not a scandal. It is a sex crime. It is a sexual violation. It's disgusting. The law needs to be changed, and we need to change. That's why these Web sites are responsible. Just the fact that somebody can be sexually exploited and violated, and the first thought that crosses somebody's mind is to make a profit from it. It's so beyond me. I just can't imagine being that detached from humanity. I can't imagine being that thoughtless and careless and so empty inside.

Anybody who looked at those pictures, you're perpetuating a sexual offense. You should cower with shame. Even people who I know and love say, 'Oh, yeah, I looked at the pictures.' I don't want to get mad, but at the same time I'm thinking, I didn't tell you that you could look at my naked body.²³

Ms. Lawrence's account for *Vanity Fair* is searing. She's reeling from blistering degradation when intimate photos meant for her lover, and him only, were posted to the Internet for all the world to see. Yet, she rages against the people ogling the photos of her nude body—some of whom are friends—whose shame should be immeasurably greater than the humiliation she has been dealt but is remarkably not.

And one thing should be crystal clear from Ms. Lawrence's *Vanity Fair* interview: The breach didn't end with her nude photos being illegally posted to 4chan. The breach continues to this day and will never end. Every time someone downloads a leaked image, they violate Ms. Lawrence's privacy and should cower with shame. Every time a website posts one of the stolen photos, its owners violate her privacy, and they, too, should cower with shame.

The bottom line is that the stolen photographs of Jennifer Lawrence's body are not just racy images—they're her personal data. As a privacy advocate, I am agnostic when it comes to data. To me, personal data is just data, whether it be a nude photograph, a social security number, an address, or a cancer diagnosis. I don't care *what* the data actually *is*—as long as it's not meant for me, I don't want to see it. And if cybercriminals steal it and post it on the Dark Web or use it to commit cybercrimes, then it's a data breach no matter what the data actually is.

Stop thinking linearly that Jennifer Lawrence's nude photos are nude photos, put on your three-dimensional thinking cap, and view them more like *personally identifiable information* (PII). When you think like a privacy advocate, there's no difference between nude photographs, passionate love letters, usernames and passwords, social security numbers, and your children's names. It's just fricking data, and your data belongs to you, and the entire world shouldn't see it because of greedy lowlife cybercriminals.

The good news is the four hackers were apprehended by law enforcement and received lengthy jail sentences: cybercriminal George Garofano was sentenced to eight months in prison; cybercriminal Emilio Herrera was sentenced to sixteen months in jail; cybercriminal Edward Majerczyk was sentenced to nine months in prison; and cybercriminal Ryan Collins was sentenced to eighteen months in jail.²⁴ That's a lot of time to spend in a damp, cold jail cell. I hope they each had a nice, warm hoodie.

The trio of infamous pwnings pour cold water on the inane hoodie-hacker mythos, and recent eye-popping statistics prove that anyone can be pwned by a determined hacker, not just celebrities. In 2022, over 500 million phishing attacks were reported worldwide, more than double the number of attacks in 2021.²⁵ In the same year, 73 percent of businesses suffered a ransomware attack, and the global cost of ransomware was expected to exceed \$30 billion in 2023.²⁶

I wrote *Ctrl+Alt+Pwn: The Hacker's Playbook (And How to Beat It)* to expose cybercriminals' hacking tools and dirty tricks and help people protect themselves from cyberattacks and data breaches. However, my interest in cybersecurity and hacking was piqued twenty-five years ago when I began my career in healthcare compliance. Suppose one industry, above all others, is the most prone to cyber doom. In that case, it has to be healthcare, as hospitals and physician practices are seemingly buffeted by one cyberattack after another,

leaving vulnerable patients reeling as their medical data is lost, stolen, or held for ransom. So, very early in my career, I became embroiled in data breaches, and later ransomware, and I'm sorry to say it never let up; indeed, it rocketed into the stratosphere until cyberattacks became the number one compliance risk in healthcare, usurping Medicare billing fraud, kickbacks to referral sources, and even quality-of-care debacles.

Though I'm not a hacker, I tried to become one to throw a spotlight on the hacking tools and dirty tricks used by cybercriminals to pwn unwary victims. I trawled hacking websites and community forums, interacting with hackers to learn their methods and tools. I experimented with the Wi-Fi Pineapple, HackRF One, and Rubber Ducky, benefiting from the many online resources explaining how to deploy these entertaining but fearsome hacking tools. Indeed, the sources I used in writing this book were as varied and endless as the Marvel Universe, which is actually a multiverse, so that should give you an idea of the volume of material that exists for a budding ethical hacker—or a cybercriminal.

Because this book is a distillation of a near-infinite universe of resources available to hackers, be they ethical or otherwise, I've focused the book more on the chicanery used to launch cyberattacks—and less on the gee-whiz technology—as pummeling the non-geek reader with computer engineering gobbledygook would lead to a cumbersome, joyless reading experience. Yet, I appreciate many readers will crave the thrill of immersing themselves in the hacking technologies on their own, so you'll find plenty of deep dives into the mechanics of hacking tools and what makes them tick—or go “Boom!” as the case may be.

But beware, as hacking isn't for the casual hobbyist—or the faint of heart. As you plunge into the hacking subculture, you'll find a borderless underground diaspora with steampunk slang (my favorites are pwned noob and phishing) and diverse alien civilizations (there are white hats, black hats, gray hats, green hats, blue hats, hacktivists, and even a race called script kiddies). Next, you'll learn that the hacking technologies deployed to launch cyberattacks are merely a sideshow—pull back the magician's curtain, and you'll see the real threat is trickery abetted by human frailty. Finally, when you understand the tricks cybercriminals use to conduct exploits and are cognizant of your own human frailty (confirmation bias and the Chico Marx Factor), you'll realize that hacking is not bad mojo but a dark art you can learn to repel.

Sure, cyberattacks seem like black magic summoned by wizards. But the truth is hacking is nothing more than technology augmented by simple trickery. From conjuring an evil portal with a Wi-Fi Pineapple to using malicious QR codes to send victims to phishing sites, cybercriminals exploit human frailty to steal passwords and launch ransomware attacks.

Worse, the rise of artificial intelligence means cybercriminals can use deepfake cloning to mimic someone's face and voice. Deepfakes can be used to steal money by impersonating the CEO, damage someone's reputation by spreading lies, or ignite a military conflict.

Romance scams are another form of destructive cyberattack but on a deeply personal level. Instead of duping victims with bleeding-edge hacking tools, cybercriminals lure the unwary into emotional bondage with romantic texts, emails, and WhatsApp messages.

When you dive deep into cutting-edge hacking tools, it's tempting to conclude that technology drives the cyberattack. The reason is simple: We're dazzled by hacking technology because it's so freaking cool. Wi-Fi Pineapples and Flipper Zeros are powerful hacking tools that come across as playful, high-tech gadgets for adults. And what could be sexier than a deepfake video roaring to life because two neural networks are duking it out for deepfake supremacy?

Hacking technology is indeed mind-boggling, whether it's a souped-up router like the Wi-Fi

Pineapple, a BadUSB loaded with malware, or even a space-age deepfake video generator. But the path to enlightenment—and sidestepping the tragic fate awaiting the pwned noob—begins with a mind-blowing epiphany: *Most cyberattacks succeed because of trickery, not technology.* By understanding the tricks that fuel the technology, you won't get pwned by cybercriminals, and the hacking tools that once seemed fearsome become little more than harmless toys.

Writing this book dragged me deep underground into the ethical hacking subculture, bursting with cutting-edge technologies, real-life cyber threats, and moral dilemmas. At the same time, it also pulled me into the cybercriminal's dark world, where I learned how they operate, what motivates them, and how to stop them.

The Stygian realm of cybercrime may scare the bejesus out of you, but if you want to protect yourself against cyberattacks, you must join me on this adventure. *CTRL+ALT+PWN: The Hacker's Playbook (And How to Beat It)* will guide you through this journey, so do not fear. Hacking is not black magic, but it is a dark art that you can master and counter. So, are you ready to fight back?

—Belmont, North Carolina, 2026

PART 1

The Hacker's Playbook: From Mindset to Malware to Mayhem

CHAPTER 1

Hackers Gonna Hack: The Making of a Cybercriminal

Think you'd never commit a crime? That's what most people believe about themselves, but anyone can do bad things under the right circumstances. We're only human, after all, shackled by genetic predispositions, drowning in biochemicals, and buffeted by external events beyond our control. It's no wonder many people turn to crime, be they a CFO embezzling company funds, a teenager boosting a carton of Lucky Strikes, or a scammer stealing passwords with a phishing email.

But not you, right? Surely anyone who commits these acts must be evil personified. Aren't all cybercriminals? It's easy to think so, given the emotional and financial toll these crimes inflict on helpless victims. But let's think twice before branding anyone with a hot iron stamped "evil," as criminal behavior is more complicated than "the devil made me do it." Without question, personal accountability plays a vital role in decision-making, and individuals must be held liable for their behavior, but—and this is a crucial but—there are many factors influencing a person's likelihood to engage in criminal activity.

Genetics and the mishmash of biochemicals sloshing around in our brains may predispose us to a myriad of emotional and psychological conditions, such as clinical depression, generalized anxiety disorder, obsessive-compulsive behavior, and other mental illnesses. In a similar vein, many criminologists theorize that biology plays a vital role in predisposing us to criminal activity.¹ You've probably heard the saying, "She's a born criminal," or, "He's a bad seed," meaning that a person is just plain evil by their very nature. From a criminologist's perspective, the more accurate maxim is that biological factors—such as genetics and neurobiology—may tip the balance as to an individual's proclivity for criminal behavior.

Traumatic childhood experiences also play a role in criminality. For example, children who grow up in an abusive environment are more at risk of engaging in criminal behavior as they grow into adulthood.² Likewise, people growing up in a high-crime area may have a greater propensity for becoming criminals themselves.³

There's more. Research has established a definitive link between substance abuse and criminal activity. Drug and alcohol abuse can lower a person's inhibition, increasing the likelihood that they will commit a crime, or they may turn to crime to fund their addiction.⁴ Similarly, poverty and experiencing homelessness can drive us to commit crimes.⁵

So while there are undoubtedly evil dudes in the world—Vladimir Putin, Kim Jong Un, and

Thanos come to mind (sorry, Marvel fanboys, but Thanos was not right!)—it's time to move beyond reflexively labeling someone as "evil" or "bad" to explain criminal behavior. Ditching these memes is crucial as they distract us from the epiphany that we can all become criminals. Under the right circumstances, be it nature or nurture (and more likely a combination thereof), we all have the potential to fall short, set aside our values, and take a big juicy bite of that forbidden fruit. So yeah, any one of us could commit a crime. Good people do bad things all the time. But could we become cybercriminals? My answer is yes, under the right circumstances, the potential is there for anyone to engage in cybercrime—be it fraud, theft, or injecting a ransomware payload to encrypt a company's network.

The right circumstances for doing bad things were hypothesized by the famous criminologist Donald R. Cressey, who imagined the tinder that ignites fraud as being like the sides of a triangle. The sides of Cressey's famous *Fraud Triangle* are opportunity, pressure, and rationalization, and when all three components are happening simultaneously, get ready for some nasty stuff to go down.⁶ Think of each component as self-combustible kindling that, when thrown together, ignites into a blazing fire. In other words, when all three components—opportunity, pressure, and rationalization—overlap, it means a crime is likely to happen or is happening right now under your very nose.

Let's start with the first side of the Fraud Triangle. Opportunity means there is some feasible way that a person can break the law.⁷ In essence, opportunity is a flaw in an organization's internal controls that a person could exploit to commit a crime. For example, *segregation of duties* is a popular internal control companies implement to prevent fraud. Segregation of duties simply means that one person should not be involved in all aspects of a transaction, lest they be in a position to commit fraud easily.⁸ So, suppose Trustworthy Tom is tasked with collecting fees from the company's customers. In that case, Trustworthy Tom shouldn't also be documenting the fee collection in a ledger and shouldn't be disbursing funds to pay the company's bills. A *different* employee should do each of these tasks—otherwise, Trustworthy Tom might be tempted to collect the fees but not record them in the ledger and then use them to pay fake invoices and collect the ill-gotten proceeds. In this example, the opportunity allowing Trustworthy Tom to steal from the company is a failure by the company to segregate the duties.

The next side of the Fraud Triangle is pressure, which means a person is experiencing some type of stress that motivates them to commit fraud.⁹ People don't just rob stuff because it gets their endorphins going. They usually steal stuff because they're tempted to do so. And it's not the Devil that made you do it; it's the pressure side of the Fraud Triangle that tempts you to steal a few bucks from the collection plate during Mass—or embezzle \$250,000 from your employer. Even worse, the stressor can be just about anything: fear of an impending layoff, the need for money to feed a drug addiction, company pressure to hit sales targets, or even a parent's desperation to pay a child's medical bills. To be human is to live with stress, which makes the pressure side of the Fraud Triangle quite pernicious—everyday hard knocks can be the spark that tempts, motivates, or incentivizes someone to commit a crime.

People who commit fraud don't think they're bad people. In fact, it's not uncommon for an arrested fraudster to tell the investigator, "I'm not a bad person—I did it because [insert excuse here]." The [insert excuse here] is the third side of the Fraud Triangle. People who commit crimes need to justify their actions so they can still look themselves in the mirror and feel like they are a good person.¹⁰ This is called rationalization, and it can take many forms: "I deserve a

bonus,” “My company is treating me like dirt,” “My kid needs expensive medicine,” “I’m doing it for my family,” or—well, you get the point. Nobody wants to be a bad person, even bad people! So rationalization is a way for someone to still feel good even when doing something antithetical to their integrity.

The Fraud Triangle is a decent gauge to assess a company’s risk for fraud. When all three sides are in play, fraud will likely occur soon if it is not already in process. If you believe in the Fraud Triangle as I do, then the best crime prevention strategy is to take a hammer to it and smash the triangle into a million pieces.¹¹ If you break even one side of the Fraud Triangle, you reduce the potential for fraud to occur. The best side to break is opportunity, and you can do this by shoring up internal controls to remove any exploitable weaknesses. A good example is the segregation of duties, which, when implemented, will prevent a lone wolf like Trustworthy Tom from embezzling company funds. The pressure and rationalization sides of the Fraud Triangle are much harder to break. However, companies can offer employee assistance programs (EAP) to help deal with life stressors, and a system-wide ethics program is a must to remind employees about their personal integrity.



Beating the Hacker’s Playbook: All three elements must be present for fraud to happen. Breaking any part of the triangle reduces the risk of fraud. If you could break only one element of The Fraud Triangle, which would you choose, and why?

Fraud Triangle	Examples	How to Break the Element
Opportunity	• Employee has access to systems beyond job requirements. • Employees share passwords or accounts.	• Limit access and segregate duties. • Require individual accounts; implement Single Sign-on (SSO) and MFA.
Pressure	• Low salary leads to job dissatisfaction. • Aggressive sales goals. • Drug or gambling addiction.	• Fair/competitive pay. • Set realistic sales targets. • Offer an Employee Assistance Program.
Rationalization	“Everyone does it.” “The company owes me.” “I’m just borrowing it.” “Nobody will get hurt.” “The C-suite is corrupt anyway.”	Strong ethical culture from leadership; code of conduct and ethics training; confidential fraud hotline; whistleblower protections.

So, do you still think you’d never commit a crime? Don’t be smug—the Fraud Triangle says you could. You, me, your parish priest, and even your soft-spoken grandmother who wouldn’t squash a stink bug could commit a crime. Perhaps you execute one hack that leads to another in a spiral of social engineering exploits, and you become a full-fledged cybercriminal. Then, the question becomes: Could you ever reform?

Well, Brett Johnson, perhaps the most notorious cybercriminal of the twenty-first century, did just that. Brett Johnson’s reign of cyber terror began in the early 2000s, leaving a trail of pwned victims in his wake until he was arrested in 2006 while on the lam at Disney World. Brett

Johnson was convicted of thirty-nine felonies and was sentenced to seven-and-a-half years behind bars—yet upon his release in 2011, he quickly violated his parole and served an additional ten months in prison. Before his arrest, he was on the United States' Most Wanted List, and the Secret Service nicknamed him "The Original Internet Godfather."¹²

In a feat of bravado that would make the most ambitious cybercriminal green with envy, Brett Johnson founded ShadowCrew—the first Internet marketplace for cybercriminals.¹³ ShadowCrew was the precursor to the cybercrime forums disseminated on today's Dark Web and was a place where people could learn how to become cybercriminals. I'd say the Secret Service pegged him right with the Godfather moniker, as in its heyday from 2002 to 2004, ShadowCrew boasted thousands of members ranging from experienced cybercriminals peddling identity theft scams to wannabes itching to learn the nuts and bolts of cybercrime.

But The Original Internet Godfather began his career with a rather mundane scam to cash in on the mid-1990s Beanie Baby craze.¹⁴ Beanie Babies are, in essence, stuffed animals—but the hook is Beanie Baby innards consist of hard plastic "beans" instead of the typical soft, cloth stuffing. Beanie Babies were all the rage when Brett Johnson was looking for his next score, and no Beanie Baby was more coveted by collectors than "Royal Blue Peanut," a sixteen-inch plush elephant whose blue color was the result of an error in the dyeing process—or so legend has it. As a much-hyped rarity, Royal Blue Peanut was fetching up to \$1,700 on eBay—and caught the larcenous eyes of Brett Johnson.

He scoured local Hallmark stores to find a Royal Blue Peanut to sell on eBay, but all he could find was a roughed-up gray elephant for eight bucks. So Johnson bought the scruffy gray elephant and dyed it blue; however, since he couldn't match the color of the real thing, he used an online photo of the actual Royal Blue Peanut and posted it for sale on eBay for \$1,500. In due course, he sent the \$8 fake Royal Blue Peanut to a woman who won the bid, who immediately called him, screaming, "This is not what I ordered!"¹⁵

You might think this is a risky scam since the woman could call the police and have Brett Johnson hauled off to prison. However, he had a simple but effective strategy. You've heard the saying, "An apple a day keeps the doctor away." In the mind of a cybercriminal, a similar but nefarious aphorism would be more along the lines of, "Stall and delay, every day, and eventually the victim will go away."

When the woman called complaining about the fake Beanie Baby, Brett Johnson said, "Lady, you ordered a blue elephant; I sent you a *bluish* elephant."¹⁶ Sketchy semantics aside, every time she called, Brett Johnson's silver tongue would spew forth word salad—and in time, she stopped calling. This was Brett Johnson's secret weapon to avoid comeuppance for his crimes. If you can stall the victim long enough, they get frustrated, scared, or embarrassed, and they simply go away without complaining to law enforcement.

But one victim who didn't go away was the United States Secret Service. In 2004, the Secret Service raided ShadowCrew, shut down the online marketplace, and arrested more than a dozen site administrators and forum members. Although Johnson initially evaded capture, the Secret Service collared him in 2005. After Johnson's arrest, the Secret Service offered him a deal to avoid prison by becoming an undercover informant to help catch other cybercriminals.¹⁷

The Secret Service gave Johnson an office, computer access, and a \$350-a-week paycheck to ensnare credit card scammers by joining online cybercrime forums similar to the now-defunct ShadowCrew. Unfortunately for the Secret Service, Brett Johnson used these resources to launch

an online scam that netted him \$6,000 a week in fraudulently obtained tax refunds.¹⁸

Johnson's tax fraud scam exploited a vulnerability in the Internal Revenue Service's (IRS) refund process. Typically, the IRS would just go ahead and pay the refund without confirming any of the information on the electronically filed tax return. Armed with a flaw in the IRS's refund process, Johnson would steal people's names and social security numbers and use the information to file online tax returns. He even got creative and pulled data from the California Death Index to file tax returns for the recently deceased. Johnson became so efficient in the scam that he electronically filed one fraudulent tax return every six minutes!¹⁹

In a feat of unbridled hubris, master cybercriminal Brett Johnson swindled the IRS with a tax fraud scheme that went undetected for ten months as he worked undercover for the Secret Service, entrapping credit card scammers. Now, one thing you don't ever want to do is make a victim out of the Secret Service, as that is one victim that will never just go away. And when Secret Service agents finally caught Brett Johnson running a tax fraud scam in plain sight, they threw the proverbial book at him, and Brett Johnson spent the next seven-and-a-half years in the slammer.

Incarceration proved to be the ignominious end to Brett Johnson's long and despicable reign as the United States' Most Wanted cybercriminal. But The Original Internet Godfather wasn't born a cybercriminal; it was something he learned as a child growing up in notably impoverished Eastern Kentucky. According to Johnson, Eastern Kentucky is so poor, "You're lucky to have a job. If you don't have one, you may be scamming, hustling, or on government assistance."²⁰

In addition to living in a socioeconomically disadvantaged high-crime area, he grew up with a family of hucksters. At ten years old, Johnson and his sister, Denise, began shoplifting. When their mother found out, she encouraged the activity, even recruiting their grandmother to join the newly established shoplifting ring. Johnson has described his mother as "a horribly abusive person" and "a criminal through and through," who raised him in the family business: fraud.²¹

Johnson's whole family was engaged in one scam after another. They staged fake accidents to file fraudulent insurance claims, stole whatever they could get their hands on, and trafficked drugs. Since Kentucky is a significant coal-producing state, Johnson's family of fraudsters even concocted an illegal coal mining enterprise!

As Johnson grew into adulthood, he left his crime family and branched out to achieve legendary status as a master cybercriminal. But no matter how wicked his crimes—selling fake Beanie Babies on eBay, launching an online marketplace to benefit other cybercriminals, or stealing taxpayer refunds—he always convinced himself he was doing the right thing. Johnson was a total lowlife, but he was the personification of the rationalization side of the Fraud Triangle. In an episode of *The Easy Prey Podcast* hosted by cyber awareness guru Chris Parker, Johnson explained how he justified his crimes: "Unless you're a sociopath, you have to convince yourself that you're a good person, that you're doing it for some reason. I convinced myself I did it for my family, I did it for my sister, my wife, my stripper girlfriend. And you have to believe those justifications because if you don't, it's pretty damn hard to look at yourself in the mirror."²²

Johnson was a ruthless fraudster whose criminal exploits landed him on the United States' Most Wanted List. But that was then—today, it's Brett, a respected cybersecurity expert who helps people and companies stay safe from cybercrime. He recounted his extraordinary journey in the Netflix documentary *Web of Make Believe: Death, Lies, and the Internet* (2022), and he

makes frequent media appearances to spread the word about cybercrime.²³ He's appeared on CNN, Fox News, and many other television news outlets and has been the focus of stories published by *The New York Times*, *Wired*, and *VICE*.

Brett Johnson walked away from cybercrime and turned his life around; how the hell did he do it? My best guess is he hit rock bottom while rotting inside a jail cell, which included a brutal eight months in solitary confinement.²⁴ Penitentiaries in Texas aren't like those low-security country clubs for white-collar criminals. Brett did hard time in the West Texas penal system, where he endured harsh conditions, shared the prison yard with the likes of the Aryan Brotherhood, and survived three prison riots. In an episode of *Fraud Busting*, a podcast hosted by body language expert Traci Brown, Brett said, "It took two-and-a-half years behind the fence for me to understand that the reason I broke the law wasn't because of family or friends, or anything like that. The reason I broke the law was because I chose to. I got out in 2011. No taste of breaking the law whatsoever."²⁵

Life behind bars no doubt smacked Brett hard in the face, resulting in an attitude adjustment that transformed his natural inclination toward cybercrime. However, he credits his wife, Michelle, and his sister, Denise, with turning his life around, along with a helpful hand from former FBI agent Keith Mularski, whose guidance encouraged Brett's desire for a life beyond cybercrime.²⁶ In time, Brett scored paid speaking gigs, launched anti-crime podcasts, and founded AnglerPhish Security to help people avoid getting pwned by the same ruthless breed of cybercriminal he had once been. Now that he's a white hat, he's even given himself a new nickname: the "First Chief Criminal Officer on the Planet." How cool is that? But I'll try and do him one better. Since the Secret Service long ago dubbed him The Original Internet Godfather, now that he's on the straight and narrow, I'll call him "The Original Godfather of Cyber Awareness" since I don't know anyone who's done more than Brett to expose the scams and shady dealings of cybercriminals.

The Fraud Triangle reveals that the potential to perpetrate crimes exists in more people than we'd like to admit. With the right opportunity, enough pressure, and a heavy dose of self-rationalization, maybe even YOU could become a lawbreaker. Heck, with a little bit of effort and a Wi-Fi Pineapple, you could perhaps become a cybercriminal. But if you did become a cybercriminal, could you escape the downward spiral of endless cybercrimes and the wretched victims pwned in your wake? What would it take for you to see the error of your ways? Would your love for your spouse, sibling, or children set you on the right path? Perhaps the cop that arrested you would be your salvation, or maybe the King James Bible and a prison yard conversion would do the trick. Or perhaps it would be years wallowing in prison with racist gangs, riots, murders, and suicides before you realized you committed your cybercrimes because you wanted to and not because you had to.

It was a long and brutal journey, but Brett Johnson redeemed himself.

Could you?

CHAPTER 2

Hackers Gonna Hack: But Some Have Horns and Some Have Halos

What should we make of our reformed cybercriminal, Brett Johnson? He was cunning, ruthless, and utterly amoral during his reign as The Original Internet Godfather. For cybercriminal Brett Johnson, hacking wasn't personal—it was just business.

But it's not always about cold, virtual Bitcoin, as so-called *hacktivists* are in it simply to make a point. For example, in 2015, cybercriminals calling themselves the Impact Team hacked into the online dating sites Ashley Madison and Established Men because, in their view, these sites were immoral and the people who used them were “cheating dirtbags.”¹

Ashley Madison provides hookups for people on the hunt for extramarital affairs—that's right, it's a dating service for individuals hankering to commit adultery. Not to be outdone, Established Men is a “sugar daddy” site for connecting wealthy men with younger women.

The Impact Team demanded that Avid Life Media, the parent company of Ashley Madison and Established Men, permanently shutter the online dating sites; when Avid Life Media refused, the hackers posted 9.7 gigabytes of member data to the Dark Web, which amounted to nearly thirty-two million membership accounts.² These accounts contained not only the members' demographic information (such as names and addresses) but also salacious details of the kinds of hookups that members were seeking, which is, well, pretty doggone embarrassing and quite likely led to many ruined marriages and onerous divorce settlements.

Clearly, Impact Team was not motivated by filthy lucre; they stole sensitive data in the hopes of shutting down what they believed was an unethical business and punishing members. To drive home their message, Impact Team issued the following statement:

“Avid Life Media has been instructed to take Ashley Madison and Established Men offline permanently in all forms, or we will release all customer records, including profiles with all the customers' secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails.”³

Circling back, there's one word that precisely sums up the true motivations of hacktivists like the Impact Team: hogwash. Whatever you may think of Avid Life Media's line of business and their members' morality (or lack thereof), it shouldn't be up to hacktivists to upend people's private lives with scarlet letter shaming. Worse, spilling the beans on the “cheating dirtbags” rendered users of Ashley Madison vulnerable to *sextortion*, a blackmail scheme whereby

cybercriminals threaten to notify the victims' loved ones unless they forked over a payment of Bitcoin.⁴

In addition to filthy lucre and hacktivism, *black hats* possess many other sinister motivations that propel them to commit cybercrimes: revenge, corporate espionage, nation-state cyberwar, political beliefs, and even breaking things just for the thrill of it (because they are slimeballs). These destructive activities are illegal and ignoble; however, there is one type of hacking that flies straight and true. Ethical hackers, nicknamed *white hats*, are motivated by a sense of altruism and a desire to make the cybersphere safe and secure. The nickname comes from vintage Western movies where the marshals wore white hats, and the outlaws wore black hats.⁵

White hats try to hack into networks, websites, and software to find vulnerabilities before the cybercriminals do. When a software vulnerability is discovered, white hats expose the problem so software companies can issue a corrective patch to prevent cybercriminals from exploiting the vulnerability into a devastating cyberattack. In addition, companies will often hire ethical hackers known as penetration testers, or *pentesters*, to conduct a non-malicious cyberattack to assess the company's cyber defenses. Many companies also offer financial incentives—bug bounties—to reward white hats for finding and disclosing software vulnerabilities.

White hats give us hope. When cybercriminals strike, and the grim news of a hellacious cyberattack leaves us dreading the onslaught of a bleak, dystopian future, take comfort in this one indisputable truth—the white hats ain't gonna let it happen! Every day, more than four million cybersecurity professionals worldwide are repelling cyberattacks, batting away phishing scams, and spreading the gospel of cyber hygiene. Cyber doom is not a foregone conclusion, and a legion of white hats stands in the way of cybercriminals and the damage they seek to inflict.

Still, cybercriminals are motivated and tenacious, and now, more than ever, cybercriminals are armed to the teeth with bleeding-edge hacking tools that are cheap and easy to deploy.

I think we are going to need more white hats.

White Hats with a Cause: The Ethical Hackers Who Revealed Aviation's Shocking Vulnerabilities

Crack open an ice-cold brewski, chillax, and I'll regale you about a fateful trip. Nope, the ill-fated journey didn't start from a tropical port and wind up on an uncharted island paradise. My tale launches in Chicago and drops like a lead balloon in the cloud-black skies of Syracuse. And no, my story doesn't involve a wee ship, a three-hour tour, a millionaire and his wife, a movie star, a professor, a farm girl from Kansas, a skipper, or a Gilligan.

My tale of woe begins with a legendary white hat and ends with a come-to-Jesus meeting with the FBI about hacking into a Boeing 737 passenger airplane—while it was in flight with a full load of passengers! In 2015, Chris Roberts was a respected ethical hacker and founder of One World Labs, a company specializing in cybersecurity research and hacking methodologies. He was also the foremost authority on the cybersecurity of airplane information systems. On an April 15, 2015, flight from Chicago to Syracuse, Chris tweeted what is quite likely the most infamous tweet in the annals of ethical hacking:

Find myself on a 737/800, lets see Box-IFE-ICE-SATCOM,? Shall we start playing

with EICAS messages? “PASS OXYGEN ON” Anyone?⁶

Chris was joking, but even though he ended his tweet with a :), the FBI wasn’t laughing. When the plane landed, two FBI agents and two Syracuse police officers detained Chris, seized his laptop and related paraphernalia, and interrogated him for four hours. Oh, and the FBI did all this to Chris without a search warrant!⁷

Warrantless searches and seizures raise the specter of a banana republic whose police are little more than jack-booted thugs, but jeepers, can you blame the FBI in this case? In 2001, the World Trade Center was destroyed by airplane-hijacking terrorists, killing nearly 3,000 people in an act so heinous that “9/11” is seared into the American zeitgeist. So if someone tweeted about hacking an in-flight airplane filled with passengers, you’d expect the FBI to be in hair-on-fire mode, and getting a search warrant would not be the number one priority.

So, let’s unpack Chris’s provocative tweet to see what all the fuss was about. The acronym EICAS in the tweet stands for “Engine Indicator Crew Alert System,” and IFE is short for “Inflight Entertainment System.” For years, Chris had been opining on the dangers of airplane systems being vulnerable to hacking by cybercriminals, with the IFE being particularly exploitable. According to Chris’s research, a cybercriminal could exploit a plane’s entertainment system to tamper with cabin controls and deploy oxygen masks from the cabin’s overhead panels.⁸

Responding to Chris’s warnings, airplane manufacturers like Boeing retorted that such hacks were impossible.⁹ However, this tit-for-tat went on long enough that there was no love lost between Chris and the airplane industry, so when Chris tweeted about accessing IFE to “play” with EICAS to “pass oxygen on,” it’s possible someone from Boeing freaked out and called the FBI.

And you better believe the FBI was more than ready to lay the smackdown on Chris when the plane landed on the Syracuse tarmac. Two days after the four-hour-long interrogation, an FBI agent applied for a search warrant to examine Chris’s seized laptop and electronic paraphernalia. According to the search warrant application, the FBI had interviewed Chris on two other occasions regarding his claims of vulnerabilities pertaining to Boeing and Airbus IFE systems. The FBI alleged that Chris said he had personally hacked into airplane entertainment systems at least twenty times and, on one occasion, could access the flight control system to command the plane to climb and move sideways while in flight.¹⁰

Piling onto the controversy over a misunderstood but unfunny tweet, we now have the FBI claiming Chris hacked an in-flight plane—which, if true, is wrong on many levels. It’s unethical from a pentesting standpoint, and it’s a safety issue, potentially jeopardizing the lives of innocent passengers. Chris, a respected white hat researcher, was not only in the crosshairs of the FBI, but the ethical hacking community was furious at him. Chris’s hacking exploit was not authorized by United Airlines or Boeing, so there was no informed consent for a pentest; even worse, who the hell would risk passengers’ lives by pentesting a plane’s network while the aircraft was in flight?

Needless to say, Chris was in a firestorm of worse-than-bad optics. However, Boeing issued a statement saying the hack was impossible because the entertainment systems were “isolated” from flight and navigation systems.¹¹ Other experts also noted that the entertainment systems were essentially not interfaced with navigation systems, and hence, the hack ascribed to Chris Roberts was simply impossible.¹²

Chris himself disputed the FBI’s allegations. In an interview with *Wired*, although he was

coy on the FBI's claim that he hacked a flight, he said the paragraph in the search warrant application alleging the hack was out of context.

"That paragraph that's in there is one paragraph out of a lot of discussions, so there is context that is obviously missing which obviously I can't say anything about," he said. "It would appear from what I've seen that the federal guys took one paragraph out of a lot of discussions and a lot of meetings and notes and just chose that one as opposed to plenty of others."¹³

We're left to wonder what really happened between Chris and the FBI in their closed-door meetings, but irrespective of what Chris told the FBI or what the FBI thought they heard, it's highly doubtful Chris Roberts hacked a plane in mid-flight. For one, Chris Roberts is an ethical hacker, and it strains credulity to believe he would risk passenger lives with an unauthorized hacking stunt. It's also not likely that hacking an airplane via the entertainment system was feasible in 2015. According to the FBI's search warrant application, the hacker must detach the cover from the Seat Electronic Box (SEB), located underneath the passenger seat, to connect to a laptop with an Ethernet cable.¹⁴ But even if Chris sarcastically told the FBI that he did this very thing twenty times, who'd believe it? In 2015, passengers were well aware of terrorist hijackings, and indeed, someone would have noticed the distinctive-looking Chris Roberts—a guy who throws off mondo biker vibes with a shaved head and a purple-dyed beard cascading below his chest—groping underneath his seat to connect his laptop to the aircraft's electronics. It's hard to believe no one would alert a flight attendant to such unusual behavior.

So, the 2015 legend of hacking an airplane through its in-flight "infotainment" system is probably just that—a legend. However, let's not be too quick to buy the "nothing to see here" trope coming from the airplane manufacturers, as Chris Roberts was onto something way back in 2015. Hacking an airplane is not only possible but, unfortunately, an all-too-likely scenario. In other words, it's not a question of "if" an airplane hacking disaster will occur—it's a question of "when."

You see, many things you use in your daily life are not what you think they are. In fact, most of the things you use today are actually computers. Your smartphone is a computer that makes phone calls, your SUV is a computer with wheels, and if you buy a smart home package, you've turned your house into a computer that shelters you. It should come as no surprise that aircraft are not airplanes—they're computers that fly. And, as everyone knows, computers can be hacked.

I'm grateful to Chris Roberts for shedding light on airplane system vulnerabilities, even though his 2015 tweet and FBI interviews likely led to sleepless nights and plenty of heartburn. But even today, airplane manufacturers are reluctant to admit the hacking dangers lurking in the skies.

In 2013, cybersecurity researcher Hugo Teso developed an Android app enabling a Samsung Galaxy smartphone to command an aircraft's autopilot system to crash the plane into the ground. Teso safely conducted his research in a simulated environment and demoed his PlaneSploit app at the Amsterdam "Hack in the Box" conference.¹⁵ However, the United States Federal Aviation Administration (FAA) dismissed Hugo's exploit as only working in a simulated environment and asserted the PlaneSploit app would not work on actual airplanes.¹⁶ The FAA is probably correct in its assessment, but do note a tricky catch-22: It's unethical and potentially dangerous for

researchers to pentest exploits on live, in-flight airplanes, yet if you conduct the test safely in a simulated environment, the results are not respected as they didn't occur in the real world. Still, at the very least, Teso demonstrated a proof-of-concept exploit that, even today, should send chills up any aircraft passenger's spine.

Not to be outdone by a German cybersecurity researcher, Robert Hickey, an aviation program manager with the Cyber Security Division of the US Department of Homeland Security (DHS), actually hijacked a Boeing 757 remotely at the 2017 CyberSat Summit in Virginia. Mr. Hickey declined to explain the hacking technique as it was "classified information," but in an interview with *Aviation Today*, he said:

"We got the airplane on September 19, 2016. Two days later, I was successful in accomplishing a remote, non-cooperative penetration. I didn't have anybody touching the airplane, I didn't have an insider threat. I stood off using typical stuff that could get through security and we were able to establish a presence on the systems of the aircraft."¹⁷

It was a sobering accomplishment, as Mr. Hickey and his team proved that an airplane can be hacked wirelessly and remotely controlled in a non-simulated environment. So, FAA—what you got to say about that?

In 2019, renowned cybersecurity researcher Ruben Santamarta made a stunning discovery. While researching airplane security online, he was shocked to find an unprotected server containing the computer code used on Boeing's enormous 787 Dreamliner passenger jet.¹⁸ Naturally, Santamarta downloaded the whole kit and caboodle, and no surprise—he found security flaws in the Crew Information Service/Maintenance System, which contains applications for maintenance systems and the electronic flight bag (a device such as an iPad containing flight planning calculations, operations manuals, airplane checklists, and the navigation charts that pilots need to, y'know, fly the plane. So, yeah, kind of important!).¹⁹

In response to Santamarta's findings, Boeing determined that security features in the Dreamliner's system architecture made Santamarta's exploit impossible for hackers to pull off.²⁰ Santamarta didn't have enough data on the Dreamliner's network architecture to refute Boeing's claim, but in a *Wired* interview, he said, "We don't have a 787 to test, so we can't assess the impact. We're not saying it's doomsday, or that we can take a plane down. But we can say: This shouldn't happen."²¹

While there's no indication that cybercriminals have ever successfully hacked into an in-flight airplane to sow chaos, mayhem, and destruction, I am confident they've earnestly tried. I'm also convinced that cyberheroes like Chris Roberts and Ruben Santamarta have done their best to raise awareness of these threats in the aviation industry. In Chris's case, he staked his reputation and business (One World Labs filed for [Chapter 11](#) bankruptcy after Chris's controversial tweet—you fill in the blanks) to warn the public about airplane vulnerabilities to hacking.

I'm not so sure the aviation industry is listening to researchers like Chris Roberts. Still, I hope they are because cyberterrorists only have to get lucky once, and down goes the plane, and hundreds of passengers are extinguished in a terrifying instant. Fortunately, Chris is still in the game, ethically hacking, researching, and raising awareness about cyber threats in aviation. He did a stint as the chief information security officer (CISO) at Boom Supersonic, a company that

designs a passenger jet called Overture, which will be the world's fastest airliner. When Chris was at the cybersecurity helm, I bet it would have been the most un-hackable.

CHAPTER 3

Hackers Gonna Hack: And the Law Ain't Gonna Stop Them

The sobering fact is not only do most cybercriminals get away scot-free, but they remain frustratingly at large to commit cybercrimes with impunity. Rarely do cybercriminals meet their match in a dogged and feisty FBI agent, dangling by their fingernails on the precipice of justice, only moments away from tumbling into the abyss of a jail cell. Simply put, most cybercriminals do not get caught, and they never will.

With ransomware cyberattacks occurring every two seconds, cybercrime is a Herculean problem on par with slaying the Lernaean Hydra.¹ Yet, hackers are rarely apprehended, with only 0.3 percent of reported cases ending in arrest and with the number of convictions even depressingly lower.² Grim statistics like these make it easy to understand why cybercrime is such a booming vocation—the handsome payoff from a pig butchering scam or ransomware cyberattack is the frosting on the cupcake, while the likelihood of never being hauled off to jail is the big, juicy cherry on top. The probability that a cybercriminal will be arrested, let alone convicted, is as remote a chance as the likelihood that their true identity will ever be revealed. The stark reality is that most cybercriminals will enjoy a long and fruitful life of perpetrating heinous cybercrimes in complete anonymity.

The situation is bleak, and the never-ending din of cyberattacks will not abate anytime soon, as cybercriminals enjoy four seemingly insurmountable advantages to avoid being thrown in the slammer.

1. **Cybercriminals use smoke screen technology to cover their tracks.** Cybercriminals deploy a wide array of sophisticated technologies to launch cyberattacks. A Wi-Fi Pineapple can be used to conjure up an evil portal into which unwary victims reveal their usernames and passwords. A ransomware payload is merely one click away when employees are duped into opening phishing emails containing malicious links or attachments. Malicious USB drives can take down a network when inserted into a computer port, either by curious employees or the cybercriminals themselves.

Technology—whether it be in the form of hacking tools like the Wi-Fi Pineapple or malicious code that encrypts a network—is the tip of the spear in the cybercriminal's arsenal. But while technology can be deployed offensively in launching cyberattacks, technology can also be used defensively as a smoke screen to conceal the cybercriminal's

identity or obfuscate evidence that a crime was committed.

Cybercriminals use proxy servers called *anonymizers* to render their online activities untraceable by camouflaging their physical location and masking their IP address.³ Virtual private networks (VPNs) can be used by cybercriminals to encrypt their data from the prying eyes of law enforcement, while the gloomy depths of the Dark Web offer a shadowy backdrop to barter stolen passwords or peddle a ransomware subscription service.⁴

Smoke screen technology like anonymizers and VPNs make it nearly impossible to expose the true identities of the perpetrators, wrapping them in a cloak of invisibility that is exceedingly difficult to breach. In addition to conferring anonymity, these smoke screen technologies also make it difficult for law enforcement to obtain evidence of the crime. When a hacker's jail-worthy emails are protected by 256-bit encryption, it's nearly impossible to build a case that will hold up in a court of law.

And it doesn't even have to be smoke screen technology like tricked-out proxy servers or the impenetrable tunnel of a VPN that stymies law enforcement. One reason why romance scammers love mundane gift cards and wire transfers is that they get paid in the blink of an eye—but even more crucial to the scam, the payment is entirely untraceable, leaving fraud investigators unable to collect the evidence needed to collar the cybercriminals.

Smoke screen technology—such as anonymizing proxy servers, VPNs, and payment methods like prepaid credit cards and crypto wallets—enables cybercriminals to camouflage their identities and bury evidence of their crimes.

- 2. Cybercriminals are a world away from the scene of the crime.** A ransomware cyberattack can be launched from anywhere on the planet. This is a tremendous boon for black hats, who can reside in countries with rudimentary to nonexistent judicial systems that are unable to apprehend cybercriminals existing within their borders. Even worse, cybercriminals can launch cyberattacks from inside totalitarian dictatorships such as Russia, China, Iran, or North Korea.⁵ These countries not only refuse to cooperate with the United States in catching the cybercriminals, but it's also been alleged they bankroll cybergangs to launch ransomware attacks on critical infrastructure in the United States. In 2021, a ransomware attack on gas pipeline operator Colonial Pipeline sparked fuel shortages along the East Coast of the United States for nearly a week.⁶ DarkSide, the chilling moniker of the cybergang responsible for the attack, is believed to be headquartered in Russia, along with another nasty cybergang, REvil.⁷ These cybergangs are nigh-impossible to shut down, especially if they're being protected by the Russian government.

But even when cybergangs fall out of favor with their nation-state protectors, there's always a new cybergang to pick up where the defunct one left off. After the attack on Colonial Pipeline, an infuriated United States rained volcanic heat upon DarkSide, such that the cybergang slithered under a rock and vanished, shutting down its eponymous

ransomware-as-a-service (RaaS) while beating a hasty retreat from law enforcement.⁸ REvil, too, slinked off into the night as fallout from the Colonial Pipeline cyberattack was too hot for the cybergangs to handle. With the DarkSide RaaS absent from the Dark Web, a new RaaS dubbed BlackMatter popped up to fill the void.⁹ This begs the question: Did DarkSide really disband, or was the cybergang strategically hunkering down, only to return with a new, rebranded BlackMatter RaaS?¹⁰ It seems that is the likely answer, but it doesn't really matter—cybergangs reside all over the world, and it's basically a game of Whac-a-Mole for law enforcement to keep track of them, let alone actually make an arrest.

When cybercriminals operate a continent away from the scene of the crime, it's a near-metaphysical impossibility to identify the perpetrators, let alone arrest them. Not only can't fraud investigators find the perpetrator, but the judges and prosecutors located in the victim's country won't have jurisdiction to take legal action on the other side of the planet.¹¹ Just like smoke screen technology, cybercriminals use far-flung base camps to erect geographic barriers to evade capture by law enforcement agencies. Financial and legal backing from nation-state threat actors, as well as jurisdiction impediments, are powerful tools in the cybercriminal's arsenal to discourage even the faintest hope for an arrest and prosecution.

3. **Cybercrimes are underreported.** Most victims of cybercrimes never report the misdeed to law enforcement.¹² It's easy to understand why. In the case of pig butchering scams—a cruel cryptocurrency investment fraud where scammers gain trust through a fake romance before stealing victims' life savings—victims are so traumatized and humiliated they don't even tell their family and friends about the ordeal, let alone file a statement with the police department. Small businesses pummeled by ransomware may lack the financial resources needed to battle cybercriminals on the other side of the world and will quietly pay the ransom demand to restore their network. Even worse, many victims lack cyber awareness—they don't know anything about phishing emails, Wi-Fi Pineapples, Rubber Duckies, and even ransomware—so when a cyberattack strikes, they don't know what to do, how to get help, or who to report the crime to.¹³ Simply put, cyber-naïve victims take it on the chin, and law enforcement never learns about the cybercrime.

Unreported cybercrimes are a significant problem for law enforcement and cybersecurity researchers because it means our statistical knowledge of cybercrime is filled with gaping holes, making it exponentially harder to develop strategies to fight cybercrime at the societal level. Unreported cybercrimes also mean the vast majority of cybercriminals will never be caught. After all, how do you catch the perpetrators when you don't even know a crime was committed?

4. **The Hoodie-Hacker Myth.** Smoke screen technology, geographic hurdles, and non-reported cybercrimes are daunting challenges in bringing cybercriminals to justice. But cybercriminals enjoy a fourth advantage in keeping law enforcement at bay—the myth of the hoodie-hacker, discussed in the book's Introduction, is a false paradigm lowering the guard of potential victims who believe hackers are a stand-up comedian's punchline rather than a data-stealing, ransomware-injecting cyber threat.

The hoodie-hacker stereotype, along with smoke screen technology, geographic barriers, and unreported cybercrimes, give cybercriminals the utmost confidence to carry out destructive cyberattacks with impunity. Taken together, these obstacles are unbeatable by current law enforcement efforts, and cybercrime will continue to flourish with wild abandon, perpetrated by threat actors with zero fear of capture.

The Unsettling Implications of Total Impunity

In today's online Wild West—or dystopian hellscape, take your pick—the cybercriminals aren't just winning; they're untouchable. Fortunately, there are public policies that can reduce cybercrime. Yet shrinking cybercrime is like losing weight: It requires a long-term commitment and a lifestyle change. To lose weight in a healthy way, you need to slash caloric intake and burn calories. This means eating less and committing to a vigorous exercise routine to melt away the fat. If you only do one and not the other, it's much more difficult to lose weight. It's the same with mitigating cybercrime. The only way to reduce the onslaught of cyberattacks is with government intervention and public cyber awareness. If you have one but not the other, cybercrimes will continue to run wild with no end in sight.

Now, by government intervention, I don't just mean the United States—all nations of the world must band together, friends and enemies alike, to battle the scourge of cybercrime. This necessitates international cooperation on a whole range of thorny issues: privacy rights, the rise of artificial intelligence, and anti-deepfake legislation should be priorities, as well as synchronized law enforcement initiatives to identify and apprehend cybercriminals across time zones. This last part is critical—until world governments work together to find a collaborative way to identify, arrest, and prosecute cybercriminals, I'm afraid there's no hope we'll ever catch the vast majority of threat actors, and therefore cyberattacks will continue with increasing frequency and destruction.

From an international policy perspective, a paradigm shift would be required to make a dent in cybercrime—sanctions for countries that provide a safe harbor for cybercriminals, and rewards for countries that lock them up; removal of bureaucratic red tape between nations so the byzantine patchwork of jurisdictions does not hinder identifying and capturing cybercriminals; and funding a massive, global fraud-fighting agency with the budget, high-tech tools, and investigators needed to take down the perpetrators.¹⁴

I'm not optimistic this paradigm shift will ever happen, and as long as cybercriminals believe they can run amok with impunity (because, actually, they can), cybercrimes will only get worse. This is why cyber awareness is so critical. If law enforcement can't apprehend the perpetrators, then it's up to YOU to protect yourself so you don't become a pwned noob.

Just like it's hard to lose weight without diet and exercise, it's challenging to reduce cybercrime without international cooperation and public cyber awareness. And this is where the clickbait title of this chapter comes in. I'm skeptical international governments will ever band together to make a dent in cybercrime, so, depressingly, I expect the pace of cyberattacks to continue with unrestrained ferocity and destructive power. That's why we need to put the focus on public cyber awareness—maybe we can't catch the cybercriminals, but we can thwart one cyberattack at a time with a more aggressive form of cyber awareness: *Smashmouth*

Cybersecurity.

Smashmouth Cybersecurity is a set of core cyber awareness principles that, when practiced together, greatly protect an individual from a cyberattack. Individuals who practice Smashmouth Cybersecurity will never be pwned noobs—instead, they’ll be *Cyber Mavens*, thwarting cyberattacks and foiling cybercriminals. Cyber Mavens are self-reliant, taking proactive steps to safeguard themselves and their loved ones from being pwned by vicious cybercriminals. Cyber Mavens are aggressive, with a take-no-prisoners attitude when it comes to cyber safety, and do not rely on their employer, the government, or anyone else to protect them. Cyber Mavens are, in effect, cybersecurity warriors brimming with moxie and armed to the teeth with the tools and techniques proven to thwart cyberattacks.

Cybercrime is here to stay—but that doesn’t mean we’re helpless. Since an international, hand-holding kumbaya moment is unlikely, the only sensible path forward is to empower individuals to become cyber-resilient. That’s where Smashmouth Cybersecurity comes in. It’s not wishy-washy, and it’s not polite—it’s a bare-knuckled approach to cyber defense. While the details of becoming a Cyber Maven are explored in [Part 3](#) of this book, one thing is clear: The era of digital hand wringing is over. It’s time to fight back, one person at a time.

CHAPTER 4

Hacking Tools: Everything Everywhere All at Once

In 1954, RCA launched the first color TV designed for the masses. The model CT-100 comprised a dense wooden cabinet encasing a 12.5-inch screen and a hefty price tag of \$1,000.¹ For the money, you got low-quality tubes and circuits, blurry images, screen ghosts, and color fringes. Even worse, most TV shows at the time were transmitted in black and white anyway, so when the CT-100 color TV failed to catch on, RCA slashed the price in half. Another groundbreaking product was Motorola's DynaTAC 8000x cell phone. The much-hyped cell phone, launched in 1984, was a bruiser weighing in at two-and-a-half pounds, with a towering height of nine inches, and enough battery power for a thirty-minute call—in retrospect, this Godzilla of cell phones made a mockery of the ear bricks seen in 1990s TV shows like *Seinfeld*.²

Fast-forward to the twenty-first century, and our world is awash with TVs and cell phones; cheap, easy to use, and microchip-smart, these technologies have become ubiquitous. Do you have a friend who doesn't know how to use a TV or a cell phone? Probably not, and in fact, wouldn't it be *Twilight Zone* weird if you knew someone—anyone at all—who didn't own a TV or cell phone? This is what it means when a technology has become *democratized*. The price goes down so much and the technology becomes so easy to master that literally anyone can buy and use that technology—and so, everyone does.

There was a time when hacking technologies were only accessible to affluent hobbyists, cybersecurity professionals, and high-tech criminals. But like color TVs and cell phones, a vast number of hacking technologies have now become democratized. Simply put, cutting-edge hacking technologies are readily available online, at rock-bottom prices, and with user-friendly interfaces that make deployment a snap.

Democratization of hacking tools is a thorny problem. Hacking tools are no longer so mind-blowingly complex that it takes a technical whiz to use them or that only well-heeled cybergangs and nation-state threat actors have the means to create and deploy them. Today, pretty much anyone, even non-geeks, can readily purchase state-of-the-art hacking technologies that are affordable and easy to master.

Conjuring an Evil Portal with the Wi-Fi Pineapple

Let's consider the exotic pineapple, a tropical fruit known for its jolly endomorphic shape; spiky crown; and tangy, sunny sweetness. When paired with raspberries, you can make an awesome summer smoothie (made even *more* awesome with a splash of rum!) or a pineapple-raspberry upside-down cake, truly a Southern delight. Unfortunately, in the cybercriminal cookbook, pairing a Wi-Fi Pineapple with a Raspberry Pi is a toxic brew so lethal you can almost see a skull and crossbones cackling in the fumes.

The *Wi-Fi Pineapple* was so named because its protruding antennae resembled that of a pineapple's spiky crown—yet a more apt description would be the Wi-Fi Black Widow, as the black, boxy router looks more like a dead spider with its legs flailing in the air. Invented by Hak5, a company that develops ethical hacking tools for the cybersecurity industry, the Wi-Fi Pineapple is now mainstream hacking technology and has been featured in the public media, most notably on the shows *Silicon Valley* and *Mr. Robot*.³

The Wi-Fi Pineapple is basically a souped-up Wi-Fi router that can empower even a non-geek with the ability to steal data on public Wi-Fi networks.⁴ The device is bustling with antennas that hulk out the signal strength and boost the range, making an everyday router look puny by comparison. But the zesty secret sauce is the Wi-Fi Pineapple's seductively engaging user interface; it's so elegantly designed that someone with little technical expertise can be hacking away in no time flat.⁵

Hak5 also provides PineAp modules that can be downloaded for free and installed on the Wi-Fi Pineapple to conduct man-in-the-middle exploits.⁶ The cherry on top is Hak5's support network—a vibrant community forum where users help each other with tips, tricks, and hacking advice. With all these attributes, the world-renowned Wi-Fi Pineapple is the ethical hacker's tool of choice for pentesting Wi-Fi networks to identify vulnerabilities before cybercriminals discover them.

Yes, Hak5 invented the Wi-Fi Pineapple to be a force for good, to raise awareness about Wi-Fi vulnerabilities, and to help pentesters expose those vulnerabilities so companies could fix them. But on the dark side, the Wi-Fi Pineapple is a cybercriminal's dream machine: cheap to buy and so easy to use that even a non-geek can hack like a pro. In the wrong hands, the Wi-Fi Pineapple is a sinister hacking tool that can be weaponized for malicious purposes.

While the device looks intimidating, the Wi-Fi Pineapple is a breeze to set up. Simply connect a Wi-Fi Pineapple to your laptop's USB port, and you can use the Wi-Fi Pineapple to monitor the data transmitting between a user's wireless device (such as a laptop) and a public Wi-Fi network. Keep in mind that the "user" is either a client or a victim, depending on whether the operator of the Wi-Fi Pineapple is a pentester conducting an audit or a cybercriminal launching an attack.

The *raison d'être* of the Wi-Fi Pineapple is to conduct *man-in-the-middle (MITM) attacks*.⁷ Think of MITM attacks as plain old eavesdropping—like opening your ex's mailbox, extracting a perfumed love letter addressed to her new boyfriend, reading the letter with tears in your eyes, then resealing the envelope and placing it back in her mailbox for postal delivery. Now, that is wrong on so many levels other than eavesdropping, but the point is, you were the man in the middle—you accessed what was intended to be private information between your ex and her boyfriend, and no one was the wiser.

Like a jilted lover snooping on an ex, the Wi-Fi Pineapple also "opens the mailbox," but does so by exploiting a key feature embedded in the design of Wi-Fi networks. Wi-Fi network names

—technically referred to as *service set identifiers (SSID)*—are transmitted by Wi-Fi access points. An access point is simply a networking device. For example, Ubiquiti Inc. makes a popular model that is spherical and snowy white with a glowing blue ring in the middle. The next time you see a flying saucer glued to the ceiling, don't freak out—it's probably just an access point.

Wireless devices, such as your cell phone or laptop, automatically scan for the SSIDs of Wi-Fi access points they've connected to in the past. Every time you slurp a cappuccino at your favorite coffee shop, your cell phone automatically connects to that familiar Wi-Fi network without you having to lift a finger. Unfortunately, while this feature is pretty darn convenient, it's also an exploitable bug, making *auto-connection* to SSIDs an inherent vulnerability in the design of public Wi-Fi networks.

To exploit this vulnerability, the Wi-Fi Pineapple scans for all the SSIDs it can find within its range—and with all those big antennas spiking from its body, it has a formidable range! The Wi-Fi Pineapple then retransmits those SSIDs hoping someone's cell phone or laptop will erroneously believe the SSID is from a trusted Wi-Fi access point it connected to in the past. If all goes right for the hacker, a bevy of cell phones and laptops will be duped into automatically connecting to the fiendish Wi-Fi Pineapple instead of the trusted Wi-Fi access point. In effect, the Wi-Fi Pineapple has become the *evil twin* of the trusted Wi-Fi access point.

By using high-tech subterfuge, the Wi-Fi Pineapple becomes a *rogue access point*, tricking the hapless user's device into connecting to a fake, evil twin access point.⁸ In a successful MITM attack, the Wi-Fi Pineapple stands between a user's wireless device and the trusted Wi-Fi access point; and by impersonating the trusted Wi-Fi access point, the Wi-Fi Pineapple can now be used to launch a phishing scam by conjuring up an *evil portal*.⁹

Conjuring up an evil portal is like performing a David Copperfield illusion with smoke and mirrors. Cybercriminals use their personal laptop to create a local server, which hosts a fake login page that looks like a genuine article from Amazon, LinkedIn, Facebook, or Gmail. The cybercriminals then configure the Wi-Fi Pineapple to redirect the victim's device to the fake login page. When the victim types their username and password into the fake login page, the cybercriminals capture the information.

Conjuring up an evil portal may seem like a cheesy sleight of hand, but when summoned by devilish black hats, the evil portal can lead the victim straight to hell.

- Conjuring up evil portals of Amazon or Etsy enables cybercriminals to steal the victim's credit card information and other financial data to sell on the Dark Web. Or the cybercriminals can simply log into online shopping sites and buy a potpourri of accoutrements with the victim's credit card.
- Conjuring up evil portals of X (formerly known as Twitter), or Facebook enables cybercriminals to steal the victim's username and password, which can then be used to hijack the victim's social media account for nefarious purposes. For example, cybercriminals could short the stock of a publicly traded company and then post fake, malicious tweets about the company from a hijacked Twitter account. When the stock tanks, the cybercriminals score a hefty profit from the short sale.
- Conjuring up an evil portal of the victim's employer is particularly nasty, as the victim's

stolen username and password can be used by cybercriminals to launch ransomware cyberattacks on the victim's employer.

When you surf the web, you've probably noticed that if you click on the address bar of your favorite websites, the full URL reveals the "HTTPS" prefix, showing that the connection is secure. HTTPS is the protocol used to secure websites and encrypt sensitive data, particularly websites used for banking and shopping. However, when people surf the web, they don't usually go to the URL search bar and type HTTPS along with the web address they are searching for. Instead, web surfers typically omit HTTPS and just type something like, for example, "linkedin.com" and then click the Enter key. This sends an insecure HTTP request to LinkedIn's servers; however, to ensure a secure connection, LinkedIn's servers will redirect the request to <https://www.linkedin.com>. In other words, some websites, like LinkedIn, force web surfers to use a secure HTTPS version of their website automatically. *Forced HTTPS redirection* is an excellent way for social media companies like LinkedIn, X, and Facebook to secure their websites and protect their users.¹⁰

Unfortunately, the user's initial HTTP request is the fly in the ointment—one that can be exploited by a gnarly Wi-Fi Pineapple using an *SSL stripping attack*.¹¹ When a victim's device is connected to the Wi-Fi Pineapple, it monitors the HTTP requests sent from the victim's device to the legitimate HTTPS server. When the legitimate server responds with a redirected HTTPS site, the Wi-Fi Pineapple "strips" out the secure layer and sends the insecure HTTP site back to the victim.¹² Thanks to the Wi-Fi Pineapple, the victim ends up surfing the unsecured "http://www.linkedin.com" instead of the safe and secure "https://www.linkedin.com." This means the victim is now surfing an unencrypted HTTP site, and any information typed on the site will be pwned by the cybercriminals.

The Wi-Fi Pineapple at its core (yes, I went there) is a phishing delivery system. Phishing is synonymous with chicanery, deceit, gifting, con artistry, and—well, you get the point. The stratagem of the Wi-Fi Pineapple is simple trickery. The Wi-Fi Pineapple tricks your cell phone into thinking it's a trusted wireless access point that it connected to in the past. Once your cell phone connects with the evil twin, a cybercriminal creates a fake website—referred to as an evil portal—to trick you into giving up your username and password (or credit card information or other sensitive data).¹³

For all the vaunted technology of the Wi-Fi Pineapple, the lifeblood of the infernal contraption is simply trickery. And that, my dear reader, is the key to defeating a Wi-Fi Pineapple cyberattack. Once you know what's in the secret sauce, you can protect yourself with hypervigilance so you don't fall for the Wi-Fi Pineapple's sneak attack.

First, be aware that the Wi-Fi Pineapple is geared toward hacking public Wi-Fi networks because they are usually open and unencrypted, which makes them easy targets. Your work and home wireless networks are most likely protected by encryption and other security measures. One way to avoid the Wi-Fi Pineapple is to never use a public Wi-Fi network (like a coffee shop or hotel lobby) in the first place.

But come on—most people are not going to forgo the convenience (and joy!) of using free Wi-Fi when noshing on a poppy-seed bagel at Starbucks. And, fortunately, MITM attacks via a Wi-Fi Pineapple are not common occurrences for everyday folk—and even the rare reported cases don't involve opportunistic hackers sitting in coffee shops phishing for random passwords.

For example, in 2022, cybercriminals used drones equipped with Wi-Fi interception gear—reportedly Wi-Fi Pineapples—but the attack was stopped when security staff spotted the drones and recovered the devices before any breach happened.¹⁴ And in 2024, authorities found an evil portal at Australian airports that tricked users into entering their social media passwords through fake login pages.¹⁵ While some victims may have entered their credentials, the scam was stopped before it caused widespread harm.

So, it would be dubious advice to tell caffeine addicts not to use their beloved coffee shop Wi-Fi, as large-scale breaches are rare. Instead, a better approach is to enjoy your coffee shop Wi-Fi with a healthy dose of old-fashioned street smarts. For example, always look to see if HTTPS is displayed in the URL; if it's not there, get off the website! Also, be aware that websites can be faked, so if a website doesn't look quite right (e.g., poor grammar, words misspelled, URL address or domain name is wrong, etc.), it might be an evil portal, and you should click off the webpage immediately.

What about the widespread advice to always use a *virtual private network* (VPN) when connecting to public Wi-Fi?¹⁶ VPNs are a secure way to use the internet because the VPN server encrypts the data, rendering the data indecipherable gobbledygook to eavesdroppers. If you connect to a VPN server before you connect to public Wi-Fi, a cybercriminal cannot access your data, even if your device subsequently connects itself to a pernicious Wi-Fi Pineapple.

The problem is that subscription-based VPNs cost between \$2 and \$15 a month, so not everyone can afford one.¹⁷ While there are free VPNs, they may limit the amount of data you can use and the number of devices you can connect to.¹⁸ And for non-technical folks, installing a VPN is simply a bridge too far. So the all-inclusive recommendation to always use a VPN when connecting to public Wi-Fi just isn't practical for everyone.

Most people enjoying a latte at their favorite coffee shop are better off assuming the local Wi-Fi network itself is unencrypted and vulnerable, and being careful to check that the sites they visit use HTTPS so their traffic remains encrypted. But what if you forget to look for HTTPS in the URL? The good news is that many browsers, like Google Chrome, will warn you if you're about to land on an insecure site—so, if a site is HTTP, your Google Chrome browser will display “Not Secure” in the address bar.¹⁹ And, if you're visiting a banking site, or an online retailer like Amazon, or even just a basic search engine like Google, the site uses HTTPS. That's right, folks, HTTPS is now the internet standard, and it's everywhere: banks, retailers, search engines, and even the sites you don't have time to think about. In fact, according to Google Statistics, 98 percent of US web traffic is encrypted with HTTPS as of 2025.²⁰ So the ubiquity of HTTPS is another reason everyday people shouldn't let the lack of a VPN deter them from connecting to their coffee shop's Wi-Fi.²¹

You can outsmart the scary Wi-Fi Pineapple and the vicious MITM attack with a healthy dose of cyber savvy. Phishing, that is, trickery, is the subatomic particle of all cyberattacks. No matter how sophisticated the hack-enabling technology is, the cyberattack will nose-dive in the face of hypervigilant users. Sure, at first blush, the Wi-Fi Pineapple seems like a staggering piece of bleeding-edge hardware. But it's really just a tricked-out router pretending to be a safe wireless access point, not much different than Ubiquiti's UFO-like access points affixed to ceilings in coffee shops and airports all over the planet. The only difference is that unlike traditional access points designed to provide access to a network, the Wi-Fi Pineapple is designed to hack that network to pieces. But whether the Wi-Fi Pineapple is used for good or evil

depends on the motivations of the person wielding the device.

In the hands of a cybercriminal, the Wi-Fi Pineapple is a cheap and dangerous weapon. Instead of using an expensive laptop, a budget-conscious cybercriminal could connect the Wi-Fi Pineapple to a *Raspberry Pi*—a popular single-board computer not much bigger than a pack of cigarettes. But don't be fooled by its diminutive size or cutie-pie name—the Raspberry Pi is a fully functional computer punching above its weight class, capable of running operating systems, connecting to networks, and powering complex software—all for a fraction of the cost of a laptop or desktop computer.²² When you consider that a Wi-Fi Pineapple Mark VII Basic can be purchased online for about \$110, and a decent Raspberry Pi can be had for about \$35, you have a total capital outlay of \$145 for one of the most dangerous hacking devices on the planet.

And you don't have to be a technical genius to learn how to deploy the Wi-Fi Pineapple for nefarious purposes. Aided by Hak5's zippy PineAp modules—dubbed *infusions* by Hak5 fanboys—a cybercriminal with only modest technical abilities can launch MITM and evil portal cyberattacks with the swaggering gusto of the most seasoned cybercriminal. A good (or bad?) example of a popular attack module is Hak5's SSLStrip infusion, which enables a Wi-Fi Pineapple to defeat forced HTTPS encryption, allowing cybercriminals to steal unsecured data.

Pentesters and cybercriminals alike will also benefit from the near-infinite number of YouTube videos and Hak5 podcasts offering step-by-step tutorials on how to deploy the Wi-Fi Pineapple and its many attack infusions.

The Wi-Fi Pineapple is a boon to pentesters and cybersecurity researchers, but in the wrong hands, it is a dangerous hacking tool that's dirt cheap and addictively easy to use. So if you're sitting in a coffee shop reading an online copy of *CTRL+ALT+PWN: The Hacker's Playbook (And How to Beat It)*, please stop right now and look for HTTPS in the address bar of your web browser. Better yet, hit the brakes on the Wi-Fi and plant your eyeballs on a printed copy of *CTRL+ALT+PWN*, which pairs well with a cup of cappuccino and a pineapple donut. Since you were brilliant enough to buy my book, you have my permission to add a shot of whisky to your java juice—unless, of course, you're about to be pwned by a Wi-Fi Pineapple, in which case you'll soon be drinking the whisky straight.

Grand Theft...Radio?

Can you steal a car using a radio? Nope, not unless you crack it across the owner's skull, palm the car keys, and peel off in a cloud of fumes and road dust.

Traditional radio, or *hardware-defined radio* (HDR), blossomed in the age of analog when hardware was utilized to transmit or receive signals via electromagnetic waves.²³ A good example is your vintage AM/FM radio, sporting a ginormous antenna and bustling with switches, dials, and knobs so you can get the bass just right. Cool gadgetry for sure, but it was radio's innards that made the magic happen—electronic circuitry like mixers, filters, and amplifiers breathed life into the signals blaring the slow-fast guitar riffs that hurled grunge rock bands like Nirvana deep into the mosh pit.

Traditional radio is still great for banging out the tunes, but it's not a useful hacking tool. Unless you can wield a traditional radio like Mjolnir, grand theft auto ain't a-happening. But what if we could scrape out the traditional radio's guts and replace the hardware with software?

Now we'd have a radio for the digital age! When a traditional radio is on the fritz, it's a pain in the butt to install replacement circuitry; but with a *software-defined radio* (SDR) system, software is our signal processing workhorse, so we simply upload a bug fix, and off we go.²⁴ In addition to correcting glitches on the fly, frequent software patches imbue our SDR system with bleeding-edge scalability and a Methuselah-aged shelf life—and unlike circuitry-packed traditional radio, ethereal software keeps SDR devices light as a feather.

Pentesters use SDRs to assess the security of radiofrequency (RF)-emitting devices like garage door openers, parking boom gates, and car key fobs. The most popular SDR is the HackRF One, a powerful hacking tool that sends and receives signals up to a whopping 6GHz – so there is plenty of headroom to snoop on Wi-Fi, Bluetooth, GPS, and 5G networks.²⁵ What's more, transmitting on these frequencies provides a myriad of hacking opportunities, like opening garage doors, closing gates, or even unlocking and starting a car.

Designed by Great Scott Gadgets, the HackRF One can be purchased online for a measly \$300. It connects to a laptop, which can be a bit too eye-catching for under-the-radar pentesters—but for an extra \$200, you can dispense with the unwieldy laptop and attach the HackRF One to a PortaPack, creating a lightweight, inconspicuous, Wi-Fi hacking powerhouse.

The HackRF One is a cutting-edge tool for assessing the cybersecurity of RF-emitting devices so that companies can fix identified vulnerabilities before cybercriminals exploit them. In addition, cybersecurity researchers can use the HackRF One to conduct experiments leading to the discovery of novel countermeasures to thwart destructive cyberattacks. And, what the hell, the HackRF One is just plain *kewl* to play around with if you are a cyber hobbyist or completing coursework in a college cybersecurity program.

The HackRF One is indeed a neat little device making substantial contributions to cybersecurity each and every day. But we can't discount the immense value of the HackRF One to cybercriminals as a destructive weapon for launching cyberattacks and RF mayhem. For example, cybercriminals can wield the small but mighty HackRF One to launch denial-of-service attacks on Wi-Fi networks. In a *jamming attack*, the HackRF One transmits radio frequencies to block the reception of signals from Wi-Fi, Bluetooth, or GPS networks, rendering cell phones little more than an expensive paperweight.²⁶

Using TempestSDR software, cybercriminals can deploy the HackRF One to catch extraneous RF signals from a victim's computer monitor and eavesdrop on the images being displayed. Sure, the black-and-white images may be a bit grainy, but they are still sharp enough to snoop on the victim's bank account, crypto wallet, or late-night porn addiction. The HackRF One makes *side channel attacks* a sobering possibility, enabling cybercriminals to steal sensitive data, reconnoiter for potential ransomware attacks, or set up a victim for blackmail (yep, you might want to get that porn addiction under control!).²⁷

On the flip side to blocking and capturing signals, the HackRF One can copy and rebroadcast signals in a *replay attack* to manipulate RF-emitting devices.²⁸ The most famous replay attack vulnerability was reported by the pseudonymous Kevin2600 and his colleague Wesley Li, a team of cybersecurity researchers with the firm Star-V Lab. Given the moniker *Rolling Pwn*, the attack enables anyone equipped with a software-defined radio to remotely unlock and start potentially all models of Honda vehicles.²⁹

"This weakness allows anyone to permanently open the car door or even start the car engine from a long distance," the pair reported on their aptly named *Rolling Pwn Attack* blog. "The

Rolling-PWN bug is a serious vulnerability. We found it in a vulnerable version of the rolling codes mechanism, which is implemented in many Honda vehicles.”³⁰

The Rolling Pwn attack exploits a vulnerability in Honda’s keyless entry system allowing cybercriminals with a software-defined radio, like the HackRF One, to copy the code transmitted by the owner’s key fob and then rebroadcast the same code to open the car door.

Of particular concern, the attack works even though Honda uses a *rolling code mechanism* designed to thwart SDR-inspired replay attacks. Many older vehicles used *fixed codes* for keyless vehicle entry, meaning that when the owner presses a button on the key fob, it transmits a unique but invariable unencrypted code to unlock the car.³¹ Unfortunately, fixed codes that never change can be easily copied and replayed by a cybercriminal using an SDR device to unlock the car. In newer car models, automobile manufacturers implemented a rolling code mechanism as a countermeasure to the replay attack; by sending multiple variable codes to open the car, a replay attack was thought to be impossible.

Unfortunately, the rolling code countermeasure has been pwned! As explained by Kevin2600 and Wesley Li in their blog post:

“A rolling code system in keyless entry systems is to prevent replay attack. After each keyfob button pressed the rolling codes synchronizing counter is increased. However, the vehicle receiver will accept a sliding window of codes, to avoid accidental key pressed by design. By sending the commands in a consecutive sequence to the Honda vehicles, it will be resynchronizing the counter. Once counter re-synced, commands from the previous cycle of the counter worked again. Therefore, those commands can be used later to unlock the car at will.”³²

How is it possible for the rolling code mechanism to be hacked? Simple—it’s the age-old battle of *user experience* versus cybersecurity risk. The battle rages daily in boardrooms across the globe: What is the line between a satisfying user experience and locking down a system to prevent cyberattacks?

Here are a few examples of the raging battle between user experience versus cybersecurity:

- A midsize bank requires its customers to use strong passwords to log in to the online banking portal. However, out of concern for customer satisfaction, the bank does not support multifactor authentication (MFA) for online access.
- A globe-trotting consulting firm encourages employees to “work anywhere,” especially during airport layovers. The company is so focused on employees “getting their hours in” that it allows them to reuse weak passwords across systems while traveling, exposing accounts to credential stuffing attacks.
- A mom-and-pop business requires vendors to submit invoices via a purchase order portal. After receiving vendor complaints that the online portal is “not user-friendly,” the password management module is updated so that passwords can be shared by vendor staff and never expire.

In the examples above, the executives blew the call and set up their businesses for a withering cyberattack. It’s cringeworthy decisions like these—not enabling MFA, allowing the

use (and reuse!) of weak passwords, and dumbing down the password manager—that have chief information security officers (CISOs) ducking for cover. But the point is vulnerabilities are inherent in any computer system when the pendulum swings toward user experience and away from cybersecurity.

Let's examine how user experience exposes an inherent vulnerability with the rolling code mechanism. Say you're getting ready for a nerve-racking job interview, anxiously fidgeting with your key fob as you approach your car for the crosstown drive. While fidgeting with the keys, you unknowingly press the fob button several times, sending one code after another to your car to open the door. You palm the latch to open the car, but the door doesn't swing open; bewildered, you press the button furiously, but the car remains locked. Now, you are flat-out livid. Fortunately, your spouse sees your predicament, comes over with a second fob, and unlocks the car with one press of a button. You are relieved, kiss your spouse on the lips, and speed off to that critical job interview while cursing Honda all the way.

By pressing the fob button multiple times, the code from the fob to your car was continually out of sync, so the car remained locked. But, of course, you don't care why the car did not open—your only thought was to hop in the car and get on with your life. The good news is you made it to the interview, got the job, and all is good; however, you're now eyeing that beguiling new Camry beckoning as you drive past the Toyota dealer.

This is precisely the kind of customer reaction that automotive manufacturers worry about, so they designed the rolling code mechanism with a series of codes, called a *window*, that re-sync to the vehicle. Hence, the car door always opens—even when a user accidentally presses the fob button multiple times. This vulnerability exists because automotive manufacturers built a fail-safe into the rolling code mechanism to ensure user convenience; however, the vulnerability means a HackRF One can copy a series of codes and replay them back to the car, and the door will open.

The stalwart pair of pseudonymous Star-V Lab researchers notified Honda about the Rolling Pwn vulnerability, but Honda was having none of it:

We've looked into past similar allegations and found them to lack substance. While we don't yet have enough information to determine if this report is credible, the key fobs in the referenced vehicles are equipped with rolling code technology that would not allow the vulnerability as represented in the report. In addition, the videos offered as evidence of the absence of rolling code do not include sufficient evidence to support the claims.³³

With thundering authority, Honda smacks down the work of Kevin2600 and Wesley Li since, obviously, Honda's "rolling code technology" renders the reported vulnerability impossible. Plus, as any doofus can plainly see, the videos posted on the researcher's blog do not—in any way, shape, or form—provide "sufficient evidence to support the claims." So, chill, says Honda, nothing at all to see here.

Wait, what? Videos? There are frigging videos?

Yes, tons of videos, in fact. Posted by Kevin2600 and Wesley Li on their blog, these videos demonstrate a HackRF One + PortaPack being used to open the doors of the Honda C-RV, Accord, Odyssey, X-RV, Inspire, Fit, Civic, and Breeze. That's quite a lineup of pwned Honda vehicles. In addition, other researchers have independently verified Star-V Lab's findings, most

notably Rob Stumpf, an automotive journalist for *The Drive*, who was able to unlock and start a 2021 Honda Accord with a HackRF One + PortaPack.

As the evidence for the Rolling Pwn vulnerability piled up, the story was picked up by major news media like VICE News, the *New York Post*, and Fox News—and in response, Honda changed its tune:

We can confirm researcher claims that it is possible to employ sophisticated tools and technical know-how to mimic Remote Keyless commands and gain access to certain vehicles or [sic] ours. However, while it is technically possible, we want to reassure our customers that this particular kind of attack, which requires continuous close-proximity signal capture of multiple sequential RF transmissions, cannot be used to drive the vehicle away. Furthermore, Honda regularly improves security features as new models are introduced that would thwart this and similar approaches.³⁴

Hmmm—seems like Honda is saying, “Move on, nothing to see here,” but at least there’s a grudging acknowledgment that the Rolling Pwn Attack is the real deal. But, to give Honda its due, is it really that big a deal?

First up, as the mysterious Star-V duo point out, they dubbed the vulnerability Rolling Pwn—and not Honda Pwn—because the vulnerability likely exists in many other types of vehicles, not just Honda’s. In fact, any modern car with keyless entry could be susceptible to the Rolling Pwn attack. But perhaps we should think of the HackRF One as simply a sneakier way to break into a car than smashing the window with a brick. Indeed, if all a criminal wants to do is a basic smash and grab, then a brick is just as effective as the HackRF One.

Also, while the HackRF One can unlock and start a Honda, it’s unlikely the cybercriminal would be able to drive the car to the nearest chop shop. Honda, like other carmakers, embeds an immobilizer chip within the key fob, which must be physically present for the vehicle to be driven away. Without possession of the owner’s key fob, a cybercriminal could use the HackRF One to unlock the car and start the engine but not drive away. Note also that the Rolling Pwn attack only zeros in on keyless entry systems, so a cybercriminal would have to figure out a way to compromise the immobilizer system in order to steal the car. Seems like the juice is not worth the squeeze, and if someone really wants the car badly enough, a short and sweet carjacking will do the trick.

To answer the question posed earlier, “Can you steal a car using a radio?” the answer would be no. A software-defined radio, like the HackRF One, can unlock the doors and start the car, but that’s about it.

Still, Rolling Pwn is a huge vulnerability, and carmakers owe it to their customers to fix what is essentially an insecure keyless entry system. Sure, a cybercriminal can’t steal your car with the HackRF One, but they can use it to unlock the car to steal your valuables, commit senseless acts of vandalism, or worse—they can unlock the doors to assault or kidnap the people inside the car.

Until Honda and other carmakers correct this bug—and there’s no indication they even want to—car owners can protect themselves by storing the key fob in a Faraday bag so SDRs (like the HackRF One) can’t pick up the signals from the key fob. And, as your momma always told you, don’t leave valuables in your car in plain sight—if you do, you’re just asking for trouble.

Build Me the World's Most Dangerous Cyberweapon

What would it look like if someone wanted to build the most dangerous, despicable, and outright vile hacking tool on Earth?

For starters, it would be cheap. Like, dirt cheap. Cheap enough that anyone could buy the ultimate hacking tool regardless of socioeconomic status. So cheap that even Charlie Chaplin's Depression-era character, the Little Tramp, could buy the malevolent device even though he couldn't scrape up two bits for a shoeshine.

It would also be easy to wield—and I mean easy peasy. So easy, the cyberweapon could be deployed by someone with little or no technical knowledge. So easy, a troglodyte could do it—or a child, teenager, high-school dropout, or even the non-geek who doesn't know a laptop from a smartphone. We're talking about a hacking tool so easy to deploy that the person weaponizing the device could do so *without any training at all*.

Invisibility would be another hallmark of such a device. It could be hacking the network in plain sight, right under the victim's nose, wreaking bloody cyber havoc, but no one would know until vast amounts of data were breached or the network became inaccessible. The most dangerous hacking tool on the planet would be, in a word, undetectable.

Worse, the usual cybersecurity countermeasures would fall by the wayside against the ultimate hacking tool. Encryption would prove useless, and even MFA and powerful antivirus software would be bypassed.

Our one-above-all hacking tool would not reside in the murky gloom of the Dark Web, concealed from the general public and known only to pentesters and cybercriminals. Instead, this vicious, brutal cyberweapon would be mass-produced and accessible on plain-vanilla online shopping platforms. No back-alley cyberweapon—it would be ubiquitous.

Such a nasty device would be small, lightweight, and oh-so conveniently carried to the scene of the crime—or if the cybercriminal is in danger of being apprehended, quickly disposed of with the flick of a wrist. No need for a backpack to hide the malicious device when you can slip the little monster into a shirt pocket, wallet, or purse.

Of course, in building the ultimate hacking tool, you'd want scalability so no cyberattack is ever too small or too large to handle. Plus, you'd like the device to be updateable so it never becomes obsolete and is always cocked and ready to exploit a newly discovered vulnerability.

Summing up, our criteria for the world's most destructive cyberweapon is that it must be rock-bottom cheap, simple enough for a non-geek to deploy, undetectable, able to bypass cyber defenses, ubiquitous, portable, and both scalable and updateable.

So, without further ado, the hacking device closest to meeting our ultimate cyberweapon criteria is the humble USB stick, which, when reprogrammed with malicious firmware and armed with attack payloads, becomes a *BadUSB*. My favorite BadUSB goes by the cartoonish nom de plume *Rubber Ducky*—nevertheless, the cutesy moniker belies its fearsome power.³⁵

Developed by the same company that invented the Wi-Fi Pineapple, Hak5 launched the Rubber Ducky in 2011, ostensibly to support pentesters and cybersecurity professionals. The Rubber Ducky is a BadUSB, meaning it masquerades as a harmless USB stick but is actually a hacking device with reprogrammed firmware and payloads that execute malicious commands to hack a computer network.³⁶

The Rubber Ducky may look like a typical flash drive used for data storage, but it operates

more like ghostly fingers banging away at a keyboard. However, these virtual fingers are actually typing keystroke commands to install malware on a victim's device or steal the victim's data. The genius of a BadUSB attack is that the victim's device—such as a laptop or desktop computer—trusts the commands being virtually typed by the Rubber Ducky as if human fingers were typing them.³⁷

Let's think about this another way. Humans interact with their devices by using a keyboard, mouse, or headset, logically referred to as *Human Interface Devices* (HID). You type a command into your keyboard, and your computer faithfully executes the command. You do this every day when you send an email, run a formula in Excel, or create a masterpiece with Adobe Illustrator. Just like a magical genie, every time that you, the human, tell your computer what to do, your wish is its command.

A BadUSB is, in essence, a fake HID created through reprogrammed firmware that makes the device impersonate a keyboard. It delivers a malicious payload of commands to the computer, which are dutifully obeyed because the computer thinks human fingers are typing the commands.³⁸ For example, a payload might command the computer to connect to an attacker's server to download ransomware.³⁹ Alternatively, a payload could issue commands to the computer, allowing an attacker to steal sensitive data, such as business or trade secrets.⁴⁰

What makes a BadUSB such as the Rubber Ducky so fearsome is that it can peck away like Barry Allen, typing thousands of keystrokes in a flash. I mean blazing fast, even to the point of typing multiple keystrokes at once, which is something no human can do (except maybe for Barry Allen—perhaps that's why USB sticks are called *Flash* drives? Sorry, I couldn't resist!). This means once a BadUSB interfaces with a victim's computer, it can execute malicious commands in no time flat.

To be sure, a BadUSB doesn't have to be bad. Hak5 didn't invent the Rubber Ducky for cybercriminals; it was invented so that pentesters didn't have to manually type in humongous scripts for ethical hacking assignments. Along the same lines, information technology (IT) managers can use a USB stick to run setup protocols when outfitting department employees with computers. A BadUSB can also be an effective learning tool for computer engineers and tech hobbyists (i.e., total geeks) or utilized as an investigative tool for cybersecurity researchers.

But a BadUSB can also be metaphysically evil. For example, cybercriminals can deploy a BadUSB to hack into a computer network to steal usernames and passwords, rummage through company trade secrets, exfiltrate customer data, and encrypt the company's data as a prelude to a ransom demand.

A BadUSB is a tough little critter; in fact, the first cyberattack to cause actual physical damage was launched with a BadUSB. In 2009, uranium centrifuges at an Iranian nuclear facility began spinning at imperceptibly varying speeds, causing them to deteriorate and eventually break. It is believed that Israeli agents worked with Iranian dissidents to infect the network by connecting malware-laden USB sticks to computer ports at the facility. The malware became known as the *Stuxnet worm* and is considered the world's first cyberweapon.⁴¹ The Stuxnet worm is unimaginably complex yet covertly malicious—it wiggled through thousands of systems for months without being discovered. Yet, the world's most destructive malware sprang forth from a little USB stick you could hold in the palm of your hand.

The Iranian nuclear facility was *air-gapped*, meaning it was not connected to the internet. Air-gapped facilities are generally safe from cyberattacks that rely on an internet connection, like

when an employee clicks on an attachment in a phishing email that downloads malware into the network. A BadUSB is a cybercriminal's mocking response to an air-gapped facility, and it is likely that BadUSBs would be the weapon of necessity in any cyberattacks on facilities where air-gapping is a cybersecurity countermeasure.⁴² For that reason, BadUSBs are a particular threat to critical infrastructure companies like oil pipelines, electrical utilities, and water treatment plants.

If the genius of the BadUSB is pretending to be human fingers typing on a keyboard, then the beauty of the BadUSB is the ease of delivery. Simply throw a few USB sticks on a parking lot, and you'll be delighted when an employee picks it up and plugs it into a workstation out of curiosity. Or a cybercriminal can pretend to be a fire inspector conducting a safety check of the building and, while crawling under a desk to look for fire hazards, surreptitiously insert a BadUSB into a desktop computer.

With a BadUSB, the mode of delivery is limited only by a cybercriminal's imagination abetted by innate human fallibility. A greedy worker might happily plug a few BadUSBs into an employer's computer ports in return for cold hard cash; a disgruntled worker might do it just to get even. As seen in the case of the Iranian nuclear facility, spies can work with anti-government insiders to insert malicious USB sticks into an enemy's network.⁴³

When it comes to delivering a BadUSB, cybercriminals can be extremely creative. For example, in 2020, researchers Alejandro Baca and Rodel Mendrez from the cybersecurity firm Trustwave SpiderLabs reported a cyberattack via a mass-mailed letter that offered a fifty-dollar gift card to loyal customers of Best Buy. Enclosed in the letter was a USB stick purporting to contain a list of items that could be purchased with the gift card; in reality, the USB stick was a BadUSB designed to compromise the victim's computer.⁴⁴

A technology-averse, non-geek cybercriminal only needs a BadUSB and the gumption to stick it into a computer port to launch a devastating cyberattack. A cybercriminal does not need to be tech-savvy, cunning, or even smart to achieve hacking success. As long as the cybercriminal has the guts to get past security and insert the BadUSB into a computer port, a long and fruitful career as a black hat is all but assured.

No doubt the Rubber Ducky is the BadUSB of choice for pentesters—and with a price tag in the range of ninety dollars, it's perhaps the Cadillac of BadUSBs. However, a basic BadUSB can be yours for around twenty dollars (or even much less!). For example, you can buy various lineups of the *Beetle BadUSB* on eBay, Amazon, and Hacker Gadgets for much less than you'd pay for a Rubber Ducky. Nonetheless, the Rubber Ducky is of higher quality and faster than some of the basic BadUSBs and uses *Ducky Script* programming language, which can be composed by technology-averse, non-geek hackers.

Standard BadUSBs, like the Rubber Ducky, must be preprogrammed to inject the keystrokes before being deployed. This is a massive drawback because once you plug the Rubber Ducky into a computer port, you can't change the programming—if you programmed the Rubber Ducky with the wrong commands, your pentest (or cyberattack) is dead in the water. Also, if you're using the Rubber Ducky as a *keylogger* to record the victim user's keystrokes, you have to retrieve the Rubber Ducky to see what it captured.⁴⁵ This means a cybercriminal risks getting caught by the company's security team twice: once when venturing onsite to deploy the Rubber Ducky and again when going back to the scene of the crime to retrieve the device.

To avoid these drawbacks, hackers will use a Wi-Fi-enabled BadUSB, such as the *DSTIKE*

Wi-Fi Duck, which sells for about forty dollars. The Wi-Fi Duck can do everything a Rubber Ducky can, but remotely with a Wi-Fi connection. After a cybercriminal inserts a Wi-Fi Duck into a computer port, they can write code on the fly and deliver the malware payload from the comfort of home—or perhaps while sipping a latte at Starbucks. Also, there’s no need to retrieve the Wi-Fi Duck, as you can manage the cyberattack via a user-friendly web interface on your laptop or smartphone.⁴⁶

Thus, we have arrived with the BadUSB as the world’s most dangerous hardware hacking tool, with my personal favorite being the wussy-named Rubber Ducky, which like the Wi-Fi Pineapple, ought to be named something fierce, like Cyber Fang, Doom Claw, or if we must go with a duck theme, perhaps Duckzilla. Really, the marketing folks at Hak5 need to do better with their hacking device naming conventions.

But are BadUSBs really nastier than a Wi-Fi Pineapple, HackRF One, or the many other hacking tools on the market? Let’s review the criteria for the world’s most dangerous hacking device and see how BadUSB stacks up.

First, our brutal hacking tool must be rock-bottom cheap; in this regard, the BadUSB fits the bill. Hackers can buy them for less than ten dollars, and a high-quality Rubber Ducky can be had for around ninety dollars. All in all, pretty darn cost-effective for a malicious device that could inject a devastating ransomware payload into a computer network. When it comes to a BadUSB, the bang is definitely worth the buck.

Next, BadUSBs are not complicated to set up and use; they’re so simple that even the most tech-averse cybercriminals can deploy a BadUSB with little or no training. Even tech-phobic cybercriminals can find someone to program a BadUSB for them; alternatively, a non-geek cybercriminal can obtain a fully loaded model from cybergangs on the Dark Web. Then, armed with a malicious USB stick, the non-geek cybercriminal only needs to access a company’s work area and plug the BadUSB into a computer port—leaving it up to the cybergang to collect the ransom and distribute the vigorish. With a BadUSB, you don’t need to be tech-savvy—you just need cojones.

Because BadUSBs mimic a keyboard HID, the computer thinks a human is typing, so it’s nigh impossible for antivirus software to detect a BadUSB. Just about the only way to detect a BadUSB is to physically see it sticking out of a computer port. If an employee doesn’t notice a BadUSB poking from the computer port and think, “Whoa! That doesn’t belong there,” then it’s not likely the BadUSB will be detected—until it’s too late, and a cyberattack is well underway.

Of course, once the BadUSB has been connected to a computer, the cybercriminal has likely defeated the victim’s standard cybersecurity countermeasures. Encryption is useless if cybercriminals have retrieved the keylogger to steal passwords and company data. MFA is totally bypassed by sticking a BadUSB into a computer and delivering a devastating cyberattack. And don’t expect air-gapping to save the day, as demonstrated by the infamous Stuxnet worm cyberattack on the Iranian nuclear facility. A cyberattack using a BadUSB is an effective workaround to typical cybersecurity countermeasures.

Rounding out the criteria for the world’s nastiest hacking tool, the BadUSB is ubiquitous and readily available for purchase at major online shopping sites (like Amazon or eBay) as well as pentesting suppliers (like Hak5 and Hacker Warehouse). There’s no need to troll the red-light district of the Dark Web. You can buy a BadUSB, no questions asked, just about anywhere.

BadUSBs fit in the palm of your hand and are easily concealed in a shirt or pants pocket.

They are perhaps the most portable, inconspicuous tool in the hacker's arsenal. Though they're diminutive, no job is too small or too big for the scalable BadUSB—from a minor keylogging cyberattack to a ransomware apocalypse, the small but mighty BadUSB is ready to rock. And with new payloads always in development, the BadUSB is updateable and unlikely to ever go out of style as a hacking tool for cybercriminals and pentesters alike.

So, there you have it—the world's most destructive hacking tool is the BadUSB. It's a wee device, but it checks all the boxes—cheap, simple, undetectable, bypasses countermeasures, ubiquitous, portable, scalable, and updateable. When you ponder the kinds of payloads it can wield, the pocket-sized BadUSB beats anything else out there in terms of sheer destructive power.

Defeating a BadUSB attack is no piece of cake, so organizations will need to adopt wide-ranging cybersecurity strategies to mitigate the threat. When it comes to thwarting a BadUSB, a kitchen-sink approach is the wisest course of action, enabled by an enterprise-wide *Device Control Policy* (DCP).⁴⁷ Device control prevents employees, vendors, and others from using unauthorized devices on company computers, such as non-approved USB sticks.

A strong DCP starts by locking down all USB ports across the enterprise. This is no easy task, particularly for organizations with thousands of endpoints; therefore, it's wise to purchase device control software (also known as *USB lockdown software*) to implement and enforce the company's DCP across the enterprise.⁴⁸

The first step will be to identify all devices with the ability to connect to a USB. Next, a vetting process begins to determine which devices will be *whitelisted* and USB-enabled versus *blacklisted*, meaning their USB ports will be blocked. The device control software can be configured to send alerts when an unauthorized device is detected and provide crucial data to aid the cybersecurity team's investigation and response to a suspected BadUSB cyberattack.

Device control software can also help enforce file transfer policies for whitelisted devices. For example, to mitigate the potential for data loss or theft, a company should limit the amount of data employees are allowed to save to a USB stick. Also critically important, USB sticks should be automatically encrypted whenever connected to a device, as well as scanned with anti-malware software.

In addition to a solid, enterprise-wide DCP, organizations must enlist their workforce in the battle against BadUSB attacks. A company-wide cybersecurity awareness program will alert employees to the dangers of non-authorized USB sticks and inform them about the sneaky ways that cybercriminals bypass physical security to covertly plug a BadUSB into a company computer.

Employees who are aware of the risks will not be tempted by curiosity to see what's on that strange USB they found lying in the parking lot. Employees armed with cybersecurity training will be savvy enough to file an incident report when they notice an unauthorized USB sticking in the port of their computer. Trained employees won't fall for social engineering tricks, like when a cybercriminal pretends to be the fire inspector or impersonates an IT manager.

A BadUSB is potentially the most devastating hardware hacking tool in existence, so organizations need an all-hands-on-deck approach to mitigating the danger posed by this tiny terror.

One more thing, though—are we really gonna call this keyboard-impersonating monstrosity a Rubber Ducky?

CHAPTER 5

Hacking Tools Are Dangerous. So What Can We Do About It?

So far, we've discussed the Big Three hacking tools—the inaptly named Wi-Fi Pineapple (it's a dead spider, dang it!); the mother of all radios and the bane of keyless entry systems, the HackRF One; and my personal favorite, the most destructive hacking tool on the planet, the BadUSB. But there are countless other hacking devices on the market today, and pentesters and cybercriminals alike will continue to have easy access to bleeding-edge technology as new tools are invented, manufactured, and marketed to the hacking community.¹ You shouldn't be surprised if hackers are voracious consumers of glucosamine chondroitin supplements to ease the pain of an inflamed rotator cuff triggered by lugging a backpack crammed with hacking devices. Of course, Mindy's Lush Black Cherry Gummies would likely make them so chill they'd forget about their aching joints—I'm not saying this from personal experience, but you know, I hear things.

With all these nasty hacking tools sloshing around, why not just ban the infernal contraptions? The United States Congress could certainly enact a law making devices like the Wi-Fi Pineapple illegal. Another alternative would be a national licensing system granting cybersecurity professionals access to hacking tools while keeping those lovely but deadly BadUSBs out of the hands of cybercriminals. And if Congress lacks the will, individual states could pick up the ball by prohibiting the use of hacking devices within their borders, levying heavy fines, and imposing jail terms for violations.

Perhaps the slickest idea of all is to tax the heck out of the little buggers and run a public service campaign with clever slogans like, "Your Hacking Tool Ain't So Cool," "Don't Get Hooked on a Rubber Ducky," and "Pineapples Should Be Eaten, Not Used to Conjure Evil Portals!"

The problem is, none of these initiatives will ever work—they're politically infeasible and metaphysically impossible to prosecute from a law enforcement perspective. Even worse, if enacted, these proposals would make the world more hackable, not less. By making hacking tools illegal, malicious SDRs and BadUSBs will still end up in the hands of cybercriminals, while on the flip side, hacking tools won't be as widely available to cybersecurity researchers, pentesters, and enthusiasts who can wield them to make our connected world more secure. In short, driving hacking tools underground is a boon to cybercriminals that will propel the risk of destructive cyberattacks into the stratosphere.

Oh, and good luck with an anti-hacking device campaign. The strategy of taxation and

preaching abstinence has certainly made inroads in curbing teen smoking—but a USB stick is not the same as a cancer stick, and I doubt these tactics would be effective against the spread of hacking tools. Still, there are potential solutions to the dilemma posed by widely available and dirt-cheap hacking tools, which, while dangerous in the hands of cybercriminals, are beneficial when deployed by cybersecurity professionals. But before we delve into potential solutions, let me offer up a spirited defense of hacking tools as key instruments in securing our digitized life; empowering the good guys to save the day; and enabling our society to build a safe, connected world.

Apologia Pro Caesim Instrumenta

In 1843, John Henry Newman resigned as vicar of St. Mary's, Oxford, and outraged the Anglican community by converting to Roman Catholicism. Joining the Roman Catholic Church turned Dr. Newman's life upside-down when he lost his closest friends—and more than a few family members—who ostracized him in the wake of scathing personal attacks by Anglican clergymen. The most visceral broadsides were launched by Charles Kingsley, a professor at Cambridge and priest of the Church of England, who flat-out called Dr. Newman a liar, and by doing so, indirectly criticized the integrity and morality of the entire Roman Catholic Church.²

In the depths of despair, Dr. Newman wrote the classic book *Apologia Pro Vita Sua*, an autobiographical paean to Dr. Newman's intensely personal and transformative spiritual awakening. Latin for "In Defense of One's Life," Dr. Newman's religious autobiography provides intellectual counterprogramming to the scurrilous accusations of his critics, along with emotional accounts of his conversion to Roman Catholicism.³

Apologia is the rarest of tomes, both a great work of literature and a masterpiece of theology. Dr. Newman's religious and intellectual contributions to Catholicism were so inspiring that Pope Francis canonized him on October 13, 2019. In homage to Saint Newman and drawing inspiration from *Apologia*, I intend to argue that hacking devices, while dangerous in the wrong hands, are critical tools for securing our digitized and connected world.

Now, I appreciate there are skeptical folks who will cringe at the thought of democratized Wi-Fi Pineapples and BadUSBs wreaking havoc on networks to steal data or spread ransomware across the globe. Believe me, I get it—but I think hacking tools are a net benefit when weighed on the scales of cybersecurity and ethical hacking. So, without further ado, I present to you a work of self-proclaimed staggering genius, *Apologia Pro Caesim Instrumenta*. While "In Defense of Hacking Tools" will not likely lead to my canonization (though I wouldn't rule out being named as a finalist), I do hope it will at least provide some comfort to those skeptics who fear the widespread availability of hacking devices. However, for those skeptics who remain unconvinced and want an all-out ban on hacking tools, let's please dispense with ad hominem attacks against your humble author—so no boos, catcalls, or derogatory remarks à la the cantankerous Charles Kingsley. Instead, let's have a respectful debate with thoughtful consideration and open minds.

First up, let's agree that, in many cases, the activity of hacking is legal. For example, pentesters hacking into a network to identify vulnerabilities at the client's behest is perfectly legal. In a typical engagement, pentesters try to hack a sliver of the company's defenses in a

tightly scoped, well-defined attack. To achieve a deeper and more wide-ranging risk assessment, companies will hire *red teams*—think pentesters hulked out on steroids—to hack the living daylight out of a company by simulating real-life cyberattacks across the enterprise. Finally, many companies offer cash rewards, or *bug bounties*, to hacking enthusiasts who report zero-day vulnerabilities so they can be patched before cybercriminals exploit them. All of these cyberattacks are conducted under controlled circumstances, with parameters determined in advance by the hackers and the companies asking to be hacked; bottom line, ethical hacking is legal.⁴

Now then, criminal hacking occurs without the victim's consent and includes hacking just for the pure thrill of it; hacking to make a political statement (so-called "Hacktivism"); hacking to cause physical damage or injure someone; hacking to steal data; and hacking for extortion, as in the case of ransomware. These activities are nefarious, evil, and most definitely illegal.

Let's also agree that hacking tools are dangerous weapons in the hands of cybercriminals but valuable tools when deployed lawfully by cybersecurity professionals. Further, let's stipulate that governments could enact legislation to ban or regulate the manufacture and distribution of hacking tools—whether such legislation would be effective is subject to debate, but for purposes of our discussion, let's assume we live in a magical world where if a nation banned devices like the Wi-Fi Pineapple or Rubber Ducky, law-abiding corporations would not build or sell them, and law-abiding citizens would not buy them.

Now that we've set the table with principles we can agree on, let's explore the bodacious splendor of hacking tools in the wild with a full-throated *Apologia Pro Caesim Instrumenta*:

The First Foundational Truth: Banning hacking tools will only drive them underground and shift the balance of power to cybercriminals.

Even if the United States enacted a law banning the manufacture and possession of hacking tools, they would still be a grave menace—the torch would simply be passed to nation-state threat actors who would construct, sell, and deploy hacking tools in furtherance of cyberattacks and espionage. Banning Wi-Fi Pineapples, BadUSBs, and the like would only drive them underground. A ban would do nothing to stop these devices from being obtained by cybercriminals and nation-state threat actors.

What a ban *would* do, however, is keep hacking tools out of the hands of law-abiding cybersecurity professionals, researchers, and pentesters, tilting the balance of power in favor of cybercriminals—and by power, I mean *knowledge*. Law-abiding white hat *bug hunters* deploy hacking tools to identify software vulnerabilities so they can be patched to block exploits by cybercriminals. Cybersecurity researchers use hacking tools to identify novel ways to conduct cyberattacks so organizations can implement strategies to thwart the attack. Likewise, the public can be educated to defend themselves against innovative and destructive cyberattacks. A great example is the brilliant work by Kevin2600 and Wesley Li, referenced earlier in this work, in demonstrating how a HackRF One can pwn a keyless entry system. Without access to a HackRF One device, the Star-V Lab researchers would not have had the means to identify this vulnerability, and no one would even know their car doors could be hacked—except perhaps cybercriminals.

Cybercriminals who want to get their hands on a HackRF One or Wi-Fi Pineapple will find a

way to get it. If Hak5 or Great Scott Gadgets do not build these devices, they'll just be manufactured by Russian or Chinese companies and purchased by cybercriminals, hacktivists, and spies. These nefarious groups will then own the cybersecurity information zone, meaning they will manufacture hacking tools and provide them to an ever-increasing population of cybercriminals—while the skills and talents of ethical hackers wither away.

While hacking devices can be used for evil, they can also be used for good. Hacking devices can be used as educational tools in training programs to help cybersecurity professionals hone their craft. Hacking devices can also be used to raise public awareness so individuals can protect themselves. Cybersecurity researchers use hacking devices for experiments to identify potential cyberattacks, enabling pentesters and bug bounty hunters to find exploitable vulnerabilities before the cybercriminals do.

A dystopian world where only cybercriminals and nation-state threat actors possess Wi-Fi Pineapples and Rubber Duckies is a poisonous, rat-infested jungle, where cybercriminals are the apex predators, baring razor-sharp fangs and flesh-ripping claws, and the general public is the pwned prey with no defenses—just a soft white underbelly.

The Second Foundational Truth: Companies say their products are secure; hacking tools can prove them wrong.

Remember when the carmaker said, “Nothing to fret, my dears, our lovely keyless entry system is a wonder to behold!” Well, HackRF One proved 'em wrong. Or what about that yummy new donut shop with a big boxy sign in the window saying, “Come in for a cruller, stay for our free, secure Wi-Fi!” Yeah, right—drop a Wi-Fi Pineapple into the hands of a pentester, and we'll see just how secure the donut maker's public Wi-Fi really is.

Hacking devices deployed by ethical hackers are not cyberweapons—they're splendiferous instruments of accountability helping to prove whether a company's product is as secure as the company claims it is.⁵ Let's face it: Sometimes companies honestly believe their products are secure but are later proved wrong by a destructive cyberattack. Or many companies tout the security of their products as a marketing strategy, but wily cybercriminals eviscerate their puffery with a nasty injection of ransomware.

Companies are better served when they learn about cyber risk from an ethical hacker and not by a ransom demand from cybercriminals when the network goes down. It is also far better for companies to be held accountable on the front end by ethical hackers rather than on the back end by government regulators imposing huge fines and penalties for massive data breaches.

When an ethical hacker discovers a vulnerability and reports it to a company, the vulnerability can be fixed before cybercriminals can launch a cyberattack. Or if a company is told about a problem but refuses to do anything about it—as in the case of Honda's keyless entry system being hackable by an SDR device—ethical hackers can notify the public so consumers can protect themselves (e.g., put the key fob in a Faraday bag when not in use) or purchase a different product that is not insecure (e.g., maybe a horse and buggy?).

Ethical hackers, outfitted with suitable hacking gear, are powerful change agents, holding organizations accountable and helping the public understand cybersecurity risks.⁶ When companies refuse to fix an identified vulnerability, ethical hackers can warn the public so they can protect themselves—and maybe shame the nonsecure company into doing the right thing.

But ethical hacking is impossible without powerful tools like the Wi-Fi Pineapple, HackRF One, or Rubber Ducky. Banning these devices would be like shackling pentesters in handcuffs and making them box a heavyweight cybercriminal sporting thick brass knuckles on each fist. That's not fair now, is it?

The Third Foundational Truth: Hacking tools can be used to educate cybersecurity professionals and consumers alike.

Democratization of hacking tools does indeed have a downside. Making them so cheap that anyone can buy them means hacking tools will unavoidably get into the hands of cybercriminals, hacktivists, terrorists, spies, and various miscreants looking for cheap thrills (note to cyberpunks: Launching a cyberattack to get your endorphins raging doesn't make you cool—it makes you a slimeball).

That said, the democratization of hacking tools opens up new possibilities and opportunities for ethical hacking, mainly to educate budding pentesters and cybersecurity researchers and raise cyber awareness with the non-geek general public.⁷ Seeing the Wi-Fi Pineapple burst from the shadows into the mainstream as a McGuffin on popular television shows like *Silicon Valley* and *Mr. Robot* is heartening. Knowing about the Wi-Fi Pineapple, even if just by watching a TV show, teaches the public about evil portals, so when they see something amiss, they can take precautions like checking for HTTPS or leaving the website if something looks phishy.

The Wi-Fi Pineapple can be a fantastic learning aid, teaching non-geek consumers that public Wi-Fi itself isn't inherently dangerous (it doesn't automatically compromise your device), but that they should be alert for high-tech phishing scams and fake portals when connecting to public Wi-Fi. Java junkies, eyeballs glued to their smartphone while slurping a cappuccino in their favorite coffee shop, will astutely notice if a website is somehow off—bad spelling, poor grammar, or the wrong domain name will clue them in that the website is fake. And everyone will be on the lookout for that comforting HTTPS in the URL—and savvy enough to get off the website if the browser flags it as “Not Secure.”

There are situations where using a VPN is encouraged or necessary—such as in the corporate world, where remote employees need secure access to internal systems, or in professions where confidentiality is essential. C-suite leaders and healthcare professionals use VPNs to protect highly sensitive data—like Colonel Sanders' fried chicken recipe or Nonna Riccardi's blood pressure result when she's told to skip the limoncello. Additionally, reporters and political activists might use VPNs to bypass censorship restrictions or avoid retaliation. Learning about the Wi-Fi Pineapple and evil portals encourages corporate users and high-risk individuals to use a VPN when connecting to public Wi-Fi. But for everyday users, HTTPS already offers strong protection, and VPNs are best seen as tools for high-risk individuals (or corporate access) rather than a universal best practice.

Hacking tools, then, are an excellent way to raise cybersecurity awareness. The more you know about the Rubber Ducky, the less likely you will pick up that random USB drive sunbathing on the tarmac and jam it into your workstation. When consumers know about BadUSBs, they won't be pwned by mass-mailed USB drives promising a gift card but delivering a ransomware payload instead. Or employees cognizant of BadUSBs will be suspicious when they eyeball a strange USB drive poking from their computer's port and will contact the

cybersecurity department posthaste. Knowledge is power, and the more the public is exposed to hacking tools, the more they'll learn about cybersecurity and how to protect themselves. The democratization of hacking tools means that everyone can learn how not to be a victim of cyberattacks.

Hacking tools are also crucial for teaching cybersecurity professionals how to conduct pentests and how to defend against actual cyberattacks. It's one thing to read how to conduct a cyberattack in a boring textbook; it's quite exhilarating and a better learning experience to give students a Wi-Fi Pineapple or HackRF One and let them do actual hacks under real-world conditions.

The democratization of hacking tools no doubt poses severe risks and challenges. However, "seeing is believing," and hacking tools can be used beneficially for spreading cyber awareness because they help consumers learn how to beat cybercriminals at their own game, and hacking tools are an essential training aid for cybersecurity professionals.

My *Apologia* is an argument that knowledge is power, and a public that understands the danger posed by hacking tools is a public that learns how to protect themselves, thus mitigating the threat posed by hacking devices wielded by cybercriminals. In fact, the true danger comes not from non-sentient hacking devices but from steering cybersecurity knowledge away from the public and into the hands of cybercriminals and nation-state threat actors. The problem is not a world swimming with BadUSBs. The problem is a world awash with non-geek consumers who lack the cyber-savvy to defend against MITM and BadUSB attacks. Yes, hacking tools are dangerous, but they can do so much good in the hands of cybersecurity professionals, who can deploy them to identify vulnerabilities, conduct research to thwart cyberattacks, teach a new generation of pentesters, and raise cybersecurity awareness to the general public.

The Big Three—the Wi-Fi Pineapple, HackRF One, and small-but-deadly Rubber Ducky—are indeed dangerous when weaponized by cybercriminals. However, these devices are critical tools for ethical hacking and consumer awareness, both of which are vital for securing our digitized and connected world.

Smashmouth Cybersecurity

Tell me if you've heard this one before.

Three cybercriminals walk into a bar. One cybercriminal is brandishing a Wi-Fi Pineapple, the other cybercriminal is wielding a HackRF One, and the third cybercriminal is wearing a Rubber Ducky as a brooch. The bartender, sporting a nappy white hat, asks the evil trio what they want to drink. The first cybercriminal says, "A Pineapple mojito while I set up a rogue access point." The second cybercriminal says, "A cordless screwdriver while I open car doors." The third cybercriminal says, "A fluffy duck while I inject ransomware into your network."

The bartender says, "Sure, I'll get your drinks. But first, let me ask you a riddle. What do you get when you deploy a Wi-Fi Pineapple, a HackRF One, and a Rubber Ducky?" The cybercriminals look perplexed and say, "We don't know. What?" The bartender slaps handcuffs on each of them and says, "Twenty years in prison!"

Bwa-hah-hah-hah!

Glad you liked my sidesplitting joke, but when you're finished rolling on the floor in a fit of

laughter, let me tell you the real punch line: Cybercriminals are not obvious like the evil trio. They'll pwn you clandestinely and sneak away in the shadows before you know what hit you. A BadUSB jammed into a computer port can infect air-gapped networks to shut down a nuclear power plant or a gas pipeline. A HackRF One can open keyless entry systems enabling cybercriminals to break into cars or buildings to steal valuables or commit violent acts. A Wi-Fi Pineapple can conjure up an evil portal and trick someone into disclosing their financial data or login credentials, exposing them to financial ruin, identity theft, or blackmail.

No doubt hacking tools are dangerous. So, what do we do about it?

Well, I'm sorry to say there's no magic bullet. Some things beg to be regulated, like tobacco; alcohol; nuclear waste; and planes, trains, and automobiles—all are dangerous items when used maliciously or just plain negligently. Sure, it's legal to drink a four-pack of Bell's Double Two Hearted Ale while lounging by the pool—but try that when piloting an airplane, and you deserve to go to jail.

Then some things are so dangerous they're illegal. For example, sarin gas is easy to make but also quite hazardous to produce without the proper equipment, and a leaky fume hood could result in a lethal dose of sarin vapor and slow, agonizing death.⁸ The deadly sarin gas concocted in a home-based laboratory will result in a life sentence at ADX Florence Supermax, assuming the chemist isn't first killed by accidental exposure to the deadly nerve agent. A fitting end for a terrorist, perhaps, but the point is some things are so destructive they are illegal for private citizens to manufacture and possess.

As I've argued in my *Apologia*, hacking tools should not be in the class of things that are illegal because, although dangerous when used by cybercriminals, hacking devices are productive tools for building a secure network. Moreover, hacking tools in the hands of pentesters reduce the risk of cyberattacks by promoting accountability, transparency, and cybersecurity knowledge. Therefore, I suggest we focus less on the harm posed by hacking devices and more on the dangers posed by a gap in cybersecurity knowledge. Then, we can focus our resources in a manner that will mitigate the threat of rogue hacking devices.

Specifically, I propose a more aggressive form of cybersecurity awareness and ethical hacking to thwart cybercriminals and the tools they weaponize and close the gap in public cybersecurity knowledge. We have smashmouth football and smashmouth politics—why not Smashmouth Cybersecurity?

Smashmouth Cybersecurity calls for a paradigm shift in our thinking about hacking devices and the cybercriminals who wield them. The solution to the democratization of hacking tools is not a ban, but quite the opposite: The solution is getting these tools into the hands of everyone, not just of pentesters, but the general public itself. This is especially important for rank-and-file employees, who should be educated about hacking tools as part of a company-wide cybersecurity training program.

A “smashmouth” solution is not to ban hacking tools but to embrace them and use them widely and publicly until devices like the Rubber Ducky and Wi-Fi Pineapple become household words. When the HackRF One becomes part of the national cybersecurity zeitgeist, that'll be a sign we're coming out of the woods because the more consumers know about hacking devices, the less they can be harmed by them. A Wi-Fi Pineapple is just a high-tech paperweight when consumers become savvy enough to look for HTTPS and understand the threat of fake websites so they aren't fooled. A BadUSB ceases to be the most destructive cyberweapon on the planet

when employees are wary of strange, randomly found USBs. The more we talk about Wi-Fi Pineapples and Rubber Duckies in the mainstream media, the better. Hopefully, these devices will get more exposure on TV shows and in the movies, and when the general public learns what these devices can do, they will be better able to protect themselves.

The smashmouth philosophy is that while the democratization of hacking tools is fraught with peril, banning the devices will drive them underground so only cybercriminals and miscreants can wield them. Instead, let's keep these devices in the hands of ethical hackers and make them part of consumer and employee cybersecurity awareness campaigns. For example, we have public service messages on the dangers of smoking and drunk driving; it's high time we have a national public service campaign about hacking tools and how to defend against them. Banning hacking tools is not feasible and would be counterproductive, and that's why Smashmouth Cybersecurity calls for precisely the opposite—increased, vigorous, and publicly visible ethical hacking bolstered by aggressive cybersecurity awareness campaigns to the general public.

Law enforcement professionals are likely to be apprehensive about the democratization of hacking tools—but, as you can surmise from my *Apologia*, I am not. Hacking tools are not only really fun and cool (I'm talking to you, HackRF One!), they are enormously beneficial to the pentesting community and the general public. A world where only cybercriminals can deploy a Wi-Fi Pineapple is an insecure twilight zone plagued by soft underbelly networks and cyberattacks that are never thwarted. Let's focus on spreading the word about hacking tools so Wi-Fi-addicted consumers aren't transported to the gates of hell by an evil portal, and company balance sheets don't bleed red with ransomware.

PART 2

A Peek Inside the Playbook: Threats, Tactics, and Technology

CHAPTER 6

The Hacker's Ransomware Playbook

In a ransomware cyberattack, hackers first poke around inside the compromised network for weeks, maybe even months, looking for juicy data to steal. Only after the cybercriminals exfiltrate massive amounts of data do they then infect the system with malware that encrypts the network, locking it down and preventing access by the hapless victim organization.¹

This strategy provides cybercriminals with several opportunities to monetize a successful ransomware cyberattack. First, cybercriminals can sell the stolen data on the Dark Web. Stolen data is highly prized by dwellers of the digital underworld, who commit cybercrimes by exploiting *personally identifiable information* (PII), with the Holy Grail being a person's name, date of birth, and social security number.²

Stealing personal data is the bedrock of *identity theft*, which is, in essence, a crime of impersonation.³ By impersonating you, identity thieves can obtain a credit card to fill up that gargantuan Costco cart but leave you hanging with the bill. Or they can open a bank account to write bad checks or obtain loans that are never repaid. They can also use your identity to pay for utility services, cable TV, or buy a spiffy new smartphone.

But wait, there's more. With enough data, identity thieves can impersonate you to steal medical services from a hospital or obtain prescription drugs from a pharmacy. They can also zero in on government benefits by applying for unemployment, requesting a new social security card, or stealing your tax refund.

Cybercriminals can even impersonate you to launch cyberattacks. For example, identity thieves can create fake social media accounts to cheat unsuspecting followers, who will seek your head on a silver platter when the scam is discovered. Or cybercriminals can use your identity to create fake email accounts to conduct phishing scams, all in your name.

Next on the cybercriminal's payday scheme is blackmail. Once a treasure trove of data fills their greedy paws, cybercriminals will inject a ransomware payload that locks down the network.⁴ The injection of malicious code is followed by the delivery of a ransom demand. The demand will typically require a ransom payment (usually in a cryptocurrency, like Bitcoin) in return for a decryption key that will un-encrypt the ransomware, giving the victim access to their data.

The cybercriminals will add insult to heartbreaking injury by threatening that if the ransom payment is not forthcoming, the stolen data will be deleted and lost forever. Or flipping the scheme on its head, the cybercriminals will threaten to post the sensitive data on the internet for all the world to see unless the ransom is paid. In a variation of this approach, when the stolen

data consists of intellectual property or trade secrets (think inventions, chemical formulas, software algorithms, business partnerships, etc.), cybercriminals might threaten to sell the information to a competitor or nation-state threat actor. Ransomware has evolved from basic encryption to double, triple, and even quadruple extortion tactics.⁵

At this point, you might be tempted to surrender, pay the ransom, and cross your fingers, hoping the cyberattack will just go away. Well, not so fast—even when the victim pays the ransom, there's no certainty the decryption key will work, or even that the cybercriminals will hand over a decryption key—they might just take the money and run (they are, after all, scammers). But the real kicker is that even when a ransom is paid and the network is restored, the cybercriminals—just to be total jerks—go ahead and post the data on the Dark Web anyway. Or after promising to delete the stolen data, the cybercriminals go ahead and sell the data on the Dark Web, but for a fraction of the ransom paid by the victim to keep everything hush.

News flash—breached data is the lifeblood of the cybercriminal. Breached data can be sold to other cybercriminals on the Dark Web to commit identity theft-inspired crimes, or breached data can be leveraged for blackmail—either to unlock malware-encrypted data in return for a ransom payment or to avoid the data being shared with the public, competitors, or nation-state threat actors. But aside from exploiting breached data, cybercriminals can monetize cyberattacks by selling the ransomware itself. Ransomware is simply malicious code written by programmers to encrypt the victim's files. Cybergangs with consistently good results—meaning successful cyberattacks widely reported in the media—become purveyors of the very malware they deployed in the cyberattacks. Infamous cybergangs like REvil, DarkSide, and LockBit sell their malicious code on the Dark Web via *ransomware-as-a-service* (RaaS) programs, which are highly sought after by other cybercriminals.⁶

Ransomware is by far the biggest, loudest, butt-ugly cybersecurity threat facing individuals, companies, and governments in the world today. No other cyber threat even comes close. One reason for the global pandemic of ransomware is the pristine beauty of the business model: Filthy lucre is made by selling breached data, misusing breached data (think identity theft crimes), blackmail (Bitcoin as payment for unlocking the victim's encrypted data), and selling successfully deployed ransomware to other cybercriminals.

It's no wonder ransomware is the mother of all cyber threats. There are just so many ways to profit from a single ransomware attack that it draws in cybercriminals like horseflies to a steaming pile of freshly pooped manure.

CHAPTER 7

How Do I Reuse Thee? Let Me Count the Ways!

In the halcyon days before the global pandemic, the public believed cyberattacks were synonymous with data breaches, and ransomware was something ethereal, only happening in cyberspace. But that mindset changed in 2021, as COVID-19 raged across the planet, and three widely reported cybercrimes transformed how the public thinks about cyberattacks.

In 2021, fuel shortages erupted along the East Coast of the United States when a cyberattack forced Colonial Pipeline to shut down its gas pipelines for nearly a week.¹ The cyberattack on Schreiber Foods, a dairy conglomerate in Wisconsin, was partly to blame for the Great Cream Cheese Shortage of 2021, although pandemic supply chain bottlenecks also played a role.² Food insecurity became a national security threat following the cyberattack on Brazilian meatpacking giant JBS Foods.³

These cybercrimes triggered a paradigm shift as the public realized that cyberattacks are not simply about data breaches but actually wreak havoc in the physical world. When people can't get a shmear on their bagel, chomp down on a mouthwatering Philly cheesesteak, or fill up their SUV with gas, they become out-and-out grouchy. But they also freak out, as they now have firsthand experience with ransomware impacting their lives.

The epiphany that cyberattacks have physical consequences made the public, media, and regulators sorely vexed at C-suite leaders for allowing these cyberattacks to happen in the first place. In other words, while the public might understand that the cybercriminals are the villains, they now also become just as angry at C-suite leaders if the cyberattack could have been thwarted by a cybersecurity control not implemented by the company.

Let me explain using Colonial Pipeline as an example. The Russia-based cybercriminal gang DarkSide attacked the pipeline company using a stolen password to access a defunct virtual private network (VPN) account belonging to a former employee.⁴ While the details are murky, it's believed the former employee used the VPN password for another online account—so it's possible the account was breached, and cybercriminals posted the stolen, reused password on the Dark Web, where DarkSide acquired it.⁵ Once inside the network, DarkSide stole 100 gigabytes of data and delivered a ransomware payload to Colonial Pipeline's billing system.

The public eventually learned the cyberattack would have failed if Colonial Pipeline had closed the VPN account when the employee left the company. The public also learned that multifactor authentication (MFA) would have thwarted the cyberattack, as DarkSide wouldn't have had the one-time numeric code to access the VPN. However, Colonial Pipeline's VPN was not protected by MFA.⁶

Time and time again, the public has learned about cyberattacks that would have been thwarted if only the company had implemented basic cyber hygiene. The Equifax breach in 2017 is another good (or bad!) example. Cybercriminals exploited a widely known software vulnerability to hack Equifax, resulting in a data breach impacting nearly 143 million Americans. The cyberattack would have been thwarted by a software update issued by the vendor, but Equifax failed to install the patch.⁷

Intensifying public awareness about ransomware leads to seething rage, and class action lawsuits to boot, whenever a cyberattack happens due to a cybersecurity lapse such as not enabling MFA or installing patches or failing to terminate an employee's access to the network when the employee leaves the company. Now there is a new public mindset: If there's a ransomware cyberattack, even though the cybercriminals are the villains, the C-suite will be held responsible, especially when basic preventative steps could have thwarted the cyberattack. And it's not just the general public that's left hopping mad—regulators and elected officials are also really ticked off.

In 2019, Senator Elizabeth Warren sponsored a bill imposing jail sentences on executives for cybersecurity lapses.⁸ Although the bill never became a law, we're probably one cyberattack away from clarion calls by politicians to enact laws imposing jail sentences on executives for cyberattacks. In 2023, the Securities and Exchange Commission (SEC) finalized a rule requiring timely reporting of cyberattacks and imposing accountability on the C-suite and board of directors for ensuring an effective cybersecurity program.⁹ The flurry of rulemaking and enforcement actions by federal agencies such as the SEC, the Federal Trade Commission (FTC), and the Justice Department, as well as legislation from Congress and at a state level, has created a minefield of accountability for C-suite executives.

This begs the question: Faced with mind-boggling liability, why are corporations still being pwned with ransomware? Why can't companies repel cyberattacks? The alarmingly obvious answer is summed up in a single word: Humans!

An organization's workforce consists of squishy, oxygen-swilling, bipedal hominids called *Homo sapiens*, who are driven by unbridled passion to achieve amazing things when motivated. In 2021, despite the palpable dread of the COVID-19 pandemic, Americans showed remarkable generosity in their charitable giving. According to the Giving USA 2022 Report, Americans donated an astonishing \$484.85 billion to US charities in 2021—you read that right, it's a billion with a B.¹⁰ The human drive for friendship, love, and belonging has led to remarkable achievements in building societies, reducing poverty, and advancing medical science and healthcare.

Yet humans are bursting with cognitive biases, bad judgments, and brain farts—in other words, we make mistakes, and nowhere is the *human factor* more evident than in the bad habit of *reusing passwords*. Just take a look at these statistics on password reuse to see the human factor in action:

- A Google/Harris Poll survey found 52 percent of people reuse passwords across multiple accounts, and 13 percent reuse the same passwords for all their accounts.¹¹
- A LastPass 2019 Global Password Security Report found employees reuse one password an average of thirteen times.¹²

- A Verizon 2018 Data Breach Investigations Report found 70 percent of employees reuse passwords.¹³
- According to a study by HYPR, 49 percent of employees simply add a character when required to update their company password every ninety days.¹⁴

Reused passwords are not just a bad habit; they're downright dangerous. Cybercriminals buy stolen passwords on the Dark Web and spray them across different accounts using *automated login tools*.¹⁵ Thus, a breach of someone's online shopping account can be used to hack into their bank account if they use the same password for both accounts. This is known as *credential stuffing*, and it's the easiest way for cybercriminals to break into company networks.

Just ask Mark Zuckerberg, the founder of Facebook, who in 2016 had his Twitter and Pinterest accounts hacked by a group of Saudi hackers called OurMine. The hackers hijacked the billionaire's Twitter account and posted a taunting message, "Hey, we got access to your Twitter & Pinterest, we are just testing your security, please direct message us."¹⁶

In 2016, Mark Zuckerberg was among the world's wealthiest and most influential people. He had a net worth of \$51.2 billion, making him the wealthiest person in California and the sixth richest person globally.¹⁷ You might imagine the cyberattack that pwned Mark Zuckerberg must have been highly sophisticated and years in the making to pull off. The Saudi hackers could've identified a flaw in Twitter and Pinterest's software, allowing them to launch a zero-day exploit to hack into the social media sites. Or the hackers likely used a Wi-Fi Pineapple to trick Mr. Zuckerberg into landing on evil portal versions of Twitter and Pinterest, purloining his credentials in a clever man-in-the-middle attack. The hackers could also have sent a phishing email, which, when the busy Facebook founder clicked on the malicious attachment, installed keylogging malware so the hackers could see everything he typed, including the Twitter and Pinterest passwords. And there's absolutely no way the Saudi hackers could pwn someone as brilliant and influential as Mark Zuckerberg without some heavy-duty backing from a nation-state threat actor. Russia, if you're listening—did you help OurMine pwn Mark Zuckerberg?

Well, Russia ain't talking, so we'll probably never know. Except, we do know because OurMine spilled the beans in a mocking tweet: "You were in LinkedIn Database with the password 'dadada'!"¹⁸

Yep. The thirty-two-year-old Mark Zuckerberg had recently become a father, so he came up with the painfully obvious password, "dadada," that he used for his LinkedIn account, and then he used it for other accounts, such as Twitter and Pinterest. Unfortunately, LinkedIn was the victim of a data breach in 2012 that compromised 117 million accounts when cybercriminals stole 6.5 million passwords.¹⁹ One of those compromised accounts belonged to Mr. Zuckerberg, and one of the credentials stolen was his "dadada" password. OurMine got their hands on the "dadada" password and stuffed it into Mr. Zuckerberg's social media accounts, and the rest is hacking history. Mr. Zuckerberg—genius, billionaire, philanthropist—was pwned in a credential stuffing attack with a reused password!

Even more maddening, "dadada" is a simple, weak password that anyone could have guessed. Of course, the OurMine hackers didn't need to guess the password because Mr. Zuckerberg handed them his butt all by himself. The Zuckerberg reused password debacle shows that even a genius billionaire can be pwned by not following basic password hygiene.

Obviously, the best way to combat credential stuffing is to prevent people from reusing

passwords in the first place. However, before we discuss prevention, let's explore the many ways passwords are reused.

"How do I love thee, let me count the ways," is a line from *Sonnets from the Portuguese*, a poem by Elizabeth Barrett Browning to proclaim endless love for her husband, Robert Browning.²⁰ She wrote the love poem for an audience of one, her husband, but 173 years later, it stands out as one of English literature's most well-known and memorable poems.²¹

Just how many ways did Elizabeth Barrett Browning love her man? By my count, she loved him in nine different ways, making Mr. Browning one lucky guy! But, of course, as the venerable adage goes, being lucky in love is not the same as being lucky at cards, nor is it the same as being fortunate enough to avoid a cyberattack—especially if you reuse passwords. In fact, most people think there's only one methodology to reuse a password, and that's to use the same password for multiple accounts. But in today's world, the average person uses nearly as many methods to reuse the same password as the ways Browning loves her husband. So let me count the ways:

1. **Same As It Ever Was (using the same password on the same account):** Reusing the same password is like being stuck in a time loop, doomed to an eternity of bad cyber hygiene. It works like this—say my password is Apple@123Hurdle, and every ninety days, the network requires me to reset my password. When the network makes me reset my password, it allows me to use my old password, so I simply reset it with Apple@123Hurdle again.²² A company network that allows employees to reset their accounts with old passwords is not just a security risk; it's the definition of insanity. Cybercriminals can crack the password, making the company network easy pickings for a cyberattack. Like the movie *Groundhog Day*, reusing the same password over and over again on the same account will leave you stuck in a time loop until you do the right thing—change the password!²³
2. **The Salami Slice (change just one character of the password):** Cybersecurity research finds that mandatory password resets are ineffective because employees simply change one letter, number, or special character to get the network to accept the password.²⁴ The Salami Slice is a variation of the example above, but instead of the system accepting an old password in its entirety, it accepts an old password that differs by just one character. For example, to get the network to accept my password, I just add an exclamation point to my old password, like this: Apple@123Hurdle! Cybercriminals, however, are well aware of this human factor and build it into their password-cracking methodologies. To reset the password securely, users should change the whole password, not just a slice.
3. **One Password to Rule Them All (same password on multiple accounts):** Using one password across multiple accounts is the classic example of password reuse.²⁵ Just take Apple@123Hurdle and use it for everything—shopping online with Amazon, watching *The Mandalorian* on Disney+, trading meme stocks on Robinhood, and signing into your company's VPN portal while slurping a latte purchased with your Starbucks rewards account. While it's a lot easier to remember a single password, the downside is if any one account is hacked, they're all hacked, and you could be looking at the business end of a credential stuffing attack.

4. **Something Old, Something New (using an old password for a new employer):** Your employer forbids you to reuse the company password, but that sensible policy isn't enforceable when employees move on to another company. Many companies maintain the password histories of their employees, so the system won't allow them to reuse a company password. But *password-history control* is meaningless when employees take a job with a new company. For example, I leave my former employer to start anew with a brand-new company, and when I'm asked to create a log in password, I simply resort to my trusty old Apple@123Hurdle, and I don't even bother putting an exclamation point at the end. Not only is it lazy, but I've put my new employer at risk for a credential stuffing attack—exclamation point!
5. **The Madness of Crowds (using common, well-worn passwords):** Want to know an easy-peasy way to remember different passwords for multiple accounts? It's simple: Just use the same password as everyone else! You know, like *password123*, *iloveyou*, *qwerty*, and *123456*.²⁶ It sounds simple, but the problem with this strategy is cybercriminals know all about it and launch brute force attacks using a list of common passwords until they hit pay dirt. So don't follow the crowd over the cliff by using well-worn passwords—instead, use strong and unique passwords for all your accounts.



Beating the Hacker's Playbook: Most people believe there's only one way to reuse a password—using the same password across multiple accounts. In reality, people are surprisingly clever at finding different ways to reuse passwords. I've identified five variations for reusing a password. How many can you come up with?

Reuse Pattern	Description	Example
One Password to Rule Them All	Using the same password across all accounts.	Apple@123Hurdle is used for bank, email, social media, and shopping sites.
Salami Slice	Adding small changes to a password, like an exclamation point.	Apple@123Hurdle > Apple@123Hurdle1 > Apple@123Hurdle2 > Apple@123Hurdle3 > Apple@123Hurdle\$ > Apple@123Hurdle!
Same As It Ever Was	Use the same password on the same account with every password reset.	Employee uses Apple@123Hurdle whenever required to reset their password.
Something Old, Something New	Using an old password for a new employer.	Apple@123Hurdle was your password when you worked at a restaurant, and you're also using it for your job at the car dealership.
The Madness of Crowds	Using common passwords.	password123, iloveyou, qwerty, and 123456.

The fact that there are five ways to reuse a password means when people create a password, they're so smitten with it that they want to use it everywhere—for their bank account, cybershopping, and even that cheesy online crossword puzzle. Reused passwords are so beloved, why, someone ought to write a poem about them—so, with apologies to Elizabeth Barrett Browning, I give you my epic poem, “Love in the Time of Credential Stuffing,” a joyful paean to the risky but treasured convenience of reused passwords:

How do I reuse thee? Let me count the ways.
When my workplace decrees a password reset,
I freely reuse thee without regret.
I reuse thee with passion across multiple accounts,
for thy convenience is priceless, I will never renounce!
I love thee to the height my soul can reach,
even when you're exposed to a data breach.
My love, my darling, with you, I'm free—
As my credentials are always password123!

Okay, we're having some fun—and a poetry slam—with reused passwords. But the point is cybercriminals are skilled at manipulating people's emotional and psychological needs, especially when people do risky things like reusing their passwords. Our discussion about reused passwords is a means to demonstrate how the human factor plays into the hands of cybercriminals, allowing them to employ trickery, augmented by technology, to launch devastating cyberattacks.

In 2022 and 2023, fintech giant PayPal; outdoor clothing retailer The North Face; and Norton LifeLock, an identity theft protection company, were targeted by credential stuffing attacks, compromising thousands of customer accounts.²⁷ Companies can mitigate the damage of a credential stuffing attack by resetting the passwords for breached accounts and offering credit monitoring services for the victims. However, prevention is the best medicine, and the 2022 and 2023 cyberattacks underscore the need for users to create strong and unique passwords for all accounts. So, why aren't they? And what can companies do to help their employees and customers stop reusing passwords?

It's essential to understand the root cause of password reuse is the human factor. We're just not built to memorize a gazillion passwords, let alone the one hundred passwords juggled by the average person, according to a study by NordPass.²⁸ Fortunately, there are several practical steps we can take to combat password reuse and lower the risk of credential stuffing attacks.

Recommendations for Everyday People

1. **Use Strong Passwords:** Strong passwords are at least twenty-five characters long with a mix of letters, numbers, and symbols.²⁹ According to a study by Indiana University, longer and more complex passwords reduce the likelihood of password reuse.³⁰ Why is that? The researchers suggest as strong passwords are hard to remember, they're more likely to be unique. People generally use strong, unique passwords for high-value accounts that contain personal information (e.g., name, address, date of birth, credit card,

etc.), such as a bank or healthcare account. But because strong passwords are hard to remember, they're less likely to be used across accounts—especially for low-value accounts lacking sensitive information, like that free online crossword puzzle. However, if you have dozens—or, more likely, hundreds—of online accounts, it's a Herculean feat to create a pantheon of unique, strong passwords, let alone remember them. That's why recommendation #2 is to let a password manager be your digital Hercules.

2. **Use a Password Manager:** A *password manager* is software that stores passwords so you don't have to remember them. Password managers can generate strong passwords and even plug the password into multiple accounts. When you don't have to remember hundreds of passwords, you're less likely to reuse them.
3. **Multifactor Authentication:** MFA is something you know, like your username and password, and something you have, such as a one-time numeric code texted to your smartphone (or generated by an authenticator app). MFA is an extra layer of defense when your password has been compromised. Remember my favorite password, the one I reuse for all my accounts? Well, if Apple@123Hurdle was stolen in a breach and posted on the Dark Web, all my accounts are in grave danger—except those protected by MFA. You see, cybercriminals may have purloined my reused password, but they will not be able to access the account without the one-time numeric code. At a minimum, enable MFA for high-value accounts like your email, 401(k), and medical records. And to be extra safe, why not turn it on for every account that offers it?

Recommendations for Companies

1. **Cyber Hygiene Awareness Program:** A cyber-savvy workforce is a company's first and greatest line of defense against a destructive cyberattack. Companies should implement a robust *cyber hygiene awareness program* that warns employees about the dangers of reused passwords and the threat of credential stuffing. Cyber-savvy employees who know how to generate strong passwords and use MFA are much less likely to reuse passwords and will be a mighty bulwark against credential stuffing attacks.³¹
2. **Provide a Password Manager:** Companies can help employees juggle hundreds of passwords by investing in a *password manager* for the workforce.³² By centralizing password management, companies lower the risk of password reuse while making logins less frustrating. I'd call that a win-win!
3. **Single Sign-on:** SSO allows users to access multiple systems with one set of login credentials.³³ For a great example of SSO in action, look no further than Google. When you log into Gmail, you automatically have access to other Google applications like YouTube, Google Photos, and Google Drive. SSO lessens the need for passwords—and since there are fewer passwords to reuse, SSO dramatically reduces the risk of credential stuffing attacks.
4. **Password Policy Enforcement:** Company systems can be configured to enforce a *password-history control policy* to prevent employees from reusing their old passwords.

Also, systems can be configured to prevent employees from using well-worn passwords like *password123*, *qwerty*, and *12345678*. This is not rocket science, and your IT department can hardwire these policies to prevent password reuse.³⁴

5. **Multifactor Authentication:** MFA is the quintessential safeguard for companies serious about reducing the risk of reused passwords.³⁵ It's a potent countermeasure to thwart credential stuffing attacks—and it's pretty darn good at repelling other password attacks, like phishing and keylogging. Companies should implement MFA across the workforce, so every account has a second line of defense.

The Human Factor: To Err Is Human, but Bad System Design Is the Real Vulnerability

Reused passwords are the most potent example of the human factor in action, making password reusers one data breach away from becoming a pwned noob in a credential stuffing attack. Password reuse is mind-bogglingly common even though it's a cybercriminal's dream vector—just steal a password or buy one on the Dark Web, and then try it everywhere, hoping it'll work on another online account. Yet, people never wake up to the threat, and it's easy to see why: Human gray matter is not a squishy version of ChatGPT that can memorize the hundreds of unique passwords needed to log in to the accounts of the average user. But, while humans can't remember what they ate for dinner the day before, let alone their passwords, they're rock stars when it comes to ingenious workarounds, concocting no less than five ways to reuse a password!

Cyberattacks often succeed not because of advanced hacking technology but because cybercriminals exploit common human blunders. For example, password sprayers like *CrackMapExec* and *BruteSpray* would be useless if people never reused passwords across multiple accounts or if everyone had MFA turned on. But they do reuse passwords, and they don't enable MFA, and it's this exploitable human factor that ultimately pwns the noob.

It's the users' tendency to screw up, take shortcuts, and plug in that shiny-new USB they found in the parking lot that gave rise to the famous dictum, "The human factor is the weakest link in cybersecurity." But despite all our flaws, the "weakest link" cliché oversimplifies the problem by scapegoating users and ignoring vulnerabilities in system design.³⁶ When someone reuses their password or clicks on a suspicious link, it's not just a "stupid" mistake—it's perfectly predictable behavior for a bipedal primate with a brain that maxes out before sundown. In fact, one could argue that humans are designed to screw up! We gnarly humans have urges and instincts and biological limitations and cultural cues that predispose us to error. In the table that follows, you'll see why country singer Lacy J. Dalton's song "Everybody Makes Mistakes" was such a big hit.



Beating the Hacker's Playbook: Blaming users as the weakest link is a cop-out when human error is entirely predictable. How can your organization design systems that prevent cyberattacks by accounting for the human factor?

Human Factor	Human Instinct, Limitation, or Cultural Cue
Password Reuse	Limited memory capacity—people can’t remember hundreds of unique, complex passwords.
Clicking on Suspicious Links	Trust instincts: “The link came from HR, so it must be safe!”; or a sense of urgency: “This survey from HR is due—I’d better get on it!”
Plugging in Unknown Devices (USBs)	Altruism (the instinct to return a “lost” USB to its owner) or basic curiosity to see what’s on the USB overrides caution.
Ignoring Security Updates	Patches interrupt workflow and feel like a hassle, so they’re postponed.
Sharing Passwords with Coworkers	Coworkers want to help each other, especially when they are under time pressure or when systems are cumbersome.
Using Work Email for Personal Activities	Convenience and blurred work-life balance.
Leaving Computers Unlocked When Stepping Away	Underestimating risk: “I’m only stepping away for two minutes—what could happen?”
Oversharing on Social Media	Humans need social connections and bonding.
Being Tricked by a Deepfake CEO	Instinct to obey authority figures.

And it’s not just Lacy J. Dalton who occasionally slips up! Sheryl Crow sang about her favorite mistake, Gracie Abrams often messes up, and, oops! Britney Spears did it again—though, um, she wasn’t singing about password hygiene.³⁷ If human errors are perfectly predictable, then the real question is why we keep blaming users instead of building systems to anticipate them.

Healthcare and aviation changed their tune decades ago—when a surgery goes wrong, or a plane crashes, investigators don’t blame the surgeon or the pilot; instead, they explore why the system allowed that human error to have such catastrophic consequences.³⁸ But in cybersecurity, when an oil pipeline is shuttered because a reused password enabled a credential stuffing attack, we blame the human user as the weakest link instead of asking why the system allowed a predictable mistake to cause such a catastrophic outcome.

The “weakest link” cliché is a red herring that distracts us from building resilient systems that account for the human factor—and in the case of credential stuffing, companies can implement a wide range of cybersecurity controls. For example, companies can enforce a password history policy or implement SSO to reduce the likelihood that their employees or customers reuse passwords. Further, companies can implement cybersecurity countermeasures, such as requiring strong passwords and enabling MFA, which blocks credential stuffing attacks even if an employee reuses their password.

It is system design, and not the human factor, that is the real vulnerability. In fact,

cybersecurity is ephemeral without a company-wide commitment to cyber hygiene. Good cyber hygiene requires cybersecurity countermeasures such as strong passwords, MFA, patching systems, and other practices that can prevent or reduce the impact of a cyberattack, such as encrypting mobile devices and backing up data regularly. It's unfair and counterproductive to blame a user's utterly predictable behavior for a cyberattack when organizations drop the ball on basic cyber hygiene.³⁹

Cyber hygiene is crucial because cybercriminals have two key advantages. First, the odds are woefully stacked against companies trying to fend off cyberattacks. A company could have thousands of employees, but all it takes is just one employee to click the attachment in a phishing email to encrypt the network with ransomware. Even worse, cybercriminals have all the time in the world to launch a near-unlimited number of cyberattacks, hoping just one employee will make a mistake. Companies are at a clear disadvantage as they must repel each and every cyberattack and win every single time. The cybercriminal, however, only needs to win once to encrypt the company's network. With unfavorable odds like these, fending off cyberattacks is a crapshoot, and betting on the cybercriminals to win seems like a sure thing.

Second, cybercriminals leverage the human factor to launch successful cyberattacks. Cybercriminals exploit the human factor by using social engineering techniques to pwn employees into compromising the company's network. For example, cybercriminals will litter a company parking lot with BadUSBs because they know employees will insert the BadUSB into a computer port to see what's on it. Cybercriminals also know employees reuse their passwords, so they launch credential stuffing attacks by spraying stolen passwords across many different accounts. Phishing attacks are a persistent threat because cybercriminals know distracted employees will click on the malicious attachment without even thinking about it.

Because of the human factor, companies can't deploy just one countermeasure and call it a day—no countermeasure is 100 percent foolproof, and even MFA can be bypassed by wily cybercriminals. Like an ensemble cast of characters in a movie, all the countermeasures must be used together to support each other. For example, strong passwords can thwart brute force attacks, but MFA adds an extra shield of security when a credential stuffing attack exploits a reused password. And when a sneaky cyberattack bypasses strong passwords and MFA, encryption can prevent cybercriminals from accessing sensitive data. A data backup plan will help restore a network encrypted by ransomware, and a solid cyber hygiene workforce awareness program can empower employees to thwart a cyberattack right from the beginning.

Cyber hygiene is no doubt the biggest bang for the buck in cybersecurity—and the “weakest link” cliché is a blame-shifting dead end. That's why it's time for a new truism: “System design, not the human factor, is the weakest link in cybersecurity!”

CHAPTER 8

Your Smartphone Is a Productivity Godsend. It's Also a Dystopian Wasteland Hell-Bent on Pwning You

That small rectangular gizmo in your shirt pocket is a magical thingamajig—the li'l doohickey is a calculator so you never do math in your head (so helpful when leaving a tip), a camera for snapping photos on the fly (like those pesky UFOs zipping across the wild blue yonder), and a calendar to manage your busy day (to make sure you don't forget to eat your lunch because the day gets away from you when you work from home).

These enchantments are wondrous indeed, but it gets even better when you download apps to your magical thingamajig—now, you can watch *María la del Barrio* reruns, buy craptastic stuff on Amazon, rock out to Foo Fighters, friend someone on Facebook, apply for a job, get a date, and then schedule an Uber to meet your date. Oh, and by the way, you can also use the magical thingamajig to make a phone call—and no, it's not witchcraft; it's just a fricking computer.

See, you don't actually possess what used to be called a “cell phone” or “mobile phone.” What you have in your sweaty little palm is a computer that does a lot of things, one of which is to make phone calls. In fact, we probably shouldn't even call it a *smartphone*, but that's the term that stuck—even though it's a powerful computer that would make a room-bursting 1970s mainframe supercomputer green with envy. And this, precisely, is the smartphone's exploitable vulnerability. It's easy to be hypervigilant when using a laptop or workstation—clunky laptops and big workstations feel like a computer, so we're far more likely to be on the lookout for phishing scams than when we're using a snazzy, pocket-sized smartphone.

Smartphones don't look anything at all like a computer, and even worse, people have an emotional bond with smartphones that they simply don't have with laptops and workstations. It's easy to see why—a smartphone is a trusted companion helping us connect with family and friends. It's even a personal assistant lending a hand with our daily activities, like ordering takeout or applying for a job. In fact, no activity is too complex or mundane for our dependable BFF. It's no wonder people have an emotional connection with their smartphone, perhaps even a codependency, that doesn't exist with an iPad, Surface Pro, laptop, or workstation.

But I have some mind-blowing news for you. You may have an emotional bond with your smartphone, but it's a one-way street because your smartphone is not sentient. This means you don't technically have a codependency; you have a plain old-fashioned dependency-dependency! And until you start looking at your smartphone as a soulless computer filling the palm of your

hand—and not as a dependable little buddy—the easier it will be for cybercriminals to pwn you with phishing cyberattacks.

The truth is a smartphone is just a fricking computer, and like any computer, it's as much a magnet for phishing attacks as any laptop or workstation. The only difference is because hackers are a bunch of geeks, they use different nomenclature to describe the same thing—so when a cybercriminal tries to trick you into clicking on a malicious link via a text message to your smartphone, it's called *smishing*; and when a cybercriminal calls you on your smartphone to pwn you, it's called *vishing*; but either way, both hacks are simply run-of-the-mill phishing attacks designed to trick you into revealing your username and password, or con you into clicking on an attachment that uploads ransomware to your smartphone.

At this point, I hope you're no longer besotted with your smartphone, but just in case you still have feelings for your BFF, consider this heartbreaking epiphany: Any cyberattack that'll work on a laptop will also work on your smartphone because your smartphone is not a smartphone—it is, repeat after me, “a fricking computer!”

SIM-Jacking: Easy as a Wink, a Smile, and Sometimes a Bribe

You'll know your smartphone's been hacked when it starts acting whack—strange apps appear out of the blue that were never on your smartphone in the first place; pop-ups spontaneously overwhelm your touch screen with grotesque adverts hawking everything from get-rich-quick schemes to pornography; data usage is off the charts, yet your smartphone is operating at a snail's pace; texts and calls are being made all day long, but they're not coming from you; and despite charging your smartphone continuously, the battery fades like a long-distance commuter waking up to ABBA at five o'clock in the morning (definitely not the way to start the day!).

But the biggest telltale sign your smartphone's been compromised is when you get a call from the very cybercriminal who pwned your smartphone. Then, prepare for an epic freakout, as once a cybercriminal has pwned your smartphone, they own your digital life, as usernames, passwords, and even texted MFA codes are all in the hands of the cybercriminals. Now your hijacked smartphone can be used to access online bank accounts to drain your life savings or log in to your Twitter account to spread hate speech or hack into your email account to send phishing emails to your contacts. But the cruelest gut punch of all is when the cybercriminal simply calls you on your pwned smartphone to demand a Bitcoin ransom in return for giving you your life back. Adding insult to injury, even if you pay the ransom, there's no guarantee the cybercriminals will keep their word. They'll probably just take the ransom but still not reinstate access to your smartphone, and your sensitive data and online accounts will continue to remain in great peril.

Remember, your smartphone is just a fricking computer, so it's vulnerable to the same kinds of tricks cybercriminals use to pwn your laptop and workstation. However, there is one nefarious trick unique to smartphones called *SIM-jacking*—and it's the cyber equivalent of stealing someone's house by simply transferring the victim's home address to a new residence on the other side of town.¹ SIM-jacking works like this: A cybercriminal impersonates the victim and tricks the cell phone carrier—such as T-Mobile or Verizon—into transferring the victim's phone

number to a different *subscriber identity module (SIM) card*.² The cybercriminal, pretending to be the victim, typically has an elaborate hard-luck “lost or stolen smartphone” story fully scripted out to con the smartphone provider. The result is the cybercriminal gets a new smartphone to replace the “lost or stolen” smartphone, complete with the victim’s phone number and the SIM data that goes along with it. The cybercriminal has virtually stolen the victim’s smartphone, meaning the cybercriminal has free rein to send and receive texts and make calls, and the victim can do nothing about it.

It’s surprisingly easy for cybercriminals to obtain enough information about a person so they can pull off a SIM-jacking. Trawling through social media platforms is a cost-free way for cybercriminals to obtain information about a victim for use in SIM-jacking schemes. Data breaches are also a fertile landscape for mining data. For example, a bank may have been the victim of a cyberattack in which cybercriminals stole the personal data of thousands of customers. The cybercriminals could use this stolen data to launch their own SIM-jacking attacks or sell the data on the Dark Web for use by other cybercriminals. Either way, stolen data is out there, primed and ready to be used by cybercriminals to impersonate victims for all sorts of nefarious schemes.

Of course, when trickery fails, cybercriminals can resort to plain old-fashioned bribery. Oftentimes money and dishonest cell phone carrier employees are the path of least resistance, in which case a bribe is easier than concocting an elaborate impersonation of the victim. C’mon, we’re talking about black hats here; it’s no surprise that cybercriminals will resort to paying cellular employees a healthy dollop of untraceable Bitcoin in return for swapping the SIM card.

To protect yourself from SIM-jacking, stop posting your life story on Facebook—the less you say about yourself on social media, the harder it will be for cybercriminals to impersonate you.³ Be especially wary about posting unique identifiers like dates of birth and home addresses—such information may seem harmless to you, but to a cybercriminal, it’s a jewel-encrusted key to your smartphone.

Wherever possible, avoid MFA codes that can only be delivered by text messages to your smartphone because if your smartphone is SIM-jacked, all those texts go directly to the beady eyes of cybercriminals. In effect, a SIM-jacked smartphone bypasses text-based MFA, so it’s best to use a standalone authenticator app like Google Authenticator or Twilio’s Authy, which are synced to your physical smartphone and not tied to your phone number. This means your authenticator apps will continue to work on your smartphone and be invisible to the prying eyes of cybercriminals. So, if your smartphone is SIM-jacked, MFA apps like Google Authenticator can still provide an extra layer of security to protect your online accounts.

Finally, many cell phone carriers offer enhanced security, like freezing SIM transfers, unless the customer provides a unique PIN code.⁴ However, if you want enhanced security, you have to ask for it—so pick up your smartphone and call your cell phone carrier now while your smartphone is still, well, yours.

A SIM-ple Hack: Twitter CEO Jack Dorsey’s Terrible, Horrible, No Good, Very Bad Day

Even tech-savvy billionaires are not safe. In 2019, former Twitter CEO Jack Dorsey was hacked

by a cybercriminal gang calling themselves the Chuckling Squad.⁵ The hackers gained access to Dorsey's phone number by tricking his mobile carrier into transferring it to a new SIM card and device.

Once they had control of Dorsey's phone number, the hackers posted offensive and racist tweets from his account using an app called Cloudbopper, which allowed users to tweet by texting messages to a certain number. The tweets included praise for Nazi Germany, bomb threats, racial slurs, and personal insults. The hackers also changed Dorsey's profile picture and bio to promote their group.⁶

Twitter quickly noticed the security breach and deleted the tweets within fifteen minutes. The company also suspended the account temporarily and launched an investigation into the incident. Twitter said the attack was due to a "security oversight" by the mobile provider and they were working with law enforcement to prevent future attacks.

The SIM-jacking of Jack Dorsey was not the first time that the Chuckling Squad targeted celebrities and influencers. The group had previously hacked the accounts of Mariah Carey, Adam Sandler, Chloë Grace Moretz, YouTuber Shane Dawson, and other celebrities.⁷ The group also claimed responsibility for hacking the account of Etika, a popular YouTube gamer who died by suicide in June 2019.⁸

SIM-jacking is an easy hack for cybercriminals to pull off. They don't need to be cyber geeks to understand the ins and outs of tricking (or bribing) a cell phone company employee into transferring over the victim's SIM card. Don't be lulled into thinking that SIM-jacking can only happen to celebrities. If a billionaire tech-god like Jack Dorsey can get SIM-jacked, anyone can.

Now, you might think it's easier for cybercriminals to SIM-jack celebrities because their lives are an open book—they're featured in news stories and scandal sheets and they bare it all with tears flowing down their cheeks on interview shows. But the truth is, there's just as much info about us regular folks circulating on the internet or social media for cybercriminals to quickly hatch a scam to trick a Verizon employee into swapping a SIM card.

Even worse, there's plenty of data on us regular folks sloshing around in our financial institutions, hospitals, and other places where we do business, work, or play. It's utterly out of your hands if that data is stolen in a breach and used by cybercriminals to impersonate you and trick a T-Mobile employee into transferring your SIM card.

Even if you're not Jack Dorsey—just smarter and better-looking—there are still plenty of juicy details about your everyday, mundane life that cybercriminals can weaponize to SIM-jack the living hell out of you. That's why it's essential to refrain from sharing too much information about yourself on social media. If your Facebook friends know your address, place of work, and the names of your spouse and children, then you can bet your bottom Bitcoin that so do hackers. And it only takes a little bit of info for even a lousy hacker to do a number on you.

It's also likely many of the celebrities who got SIM-jacked logged in to their social media accounts with reused passwords. Reusing your passwords is like frying up vomit, spreading it on an English muffin with a butter knife, and then eating it for breakfast as a leftover. You wouldn't do that because it's gross and unhealthy, but so is reusing passwords! Armed with a reused password and a SIM-jacked smartphone, there's nothing to stop cybercriminals from gaining access to your Facebook or LinkedIn accounts, especially if you're using text-based MFA.

Fortunately, you can do three easy things to foil the hackers. First, don't reuse your passwords; second, use an authenticator app installed on your smartphone instead of text-based

MFA; and lastly, call your cell phone carrier and request additional security options, such as requiring a unique PIN code before green-lighting any SIM transfer.⁹ While you're at it, demand more from your cell phone carrier to protect you from SIM-jacking. Much of the risk of SIM-jacking is out of your hands, especially in a data breach, or worse, when a T-Mobile employee is bribed into transferring your SIM card. Simply put, the public must demand more accountability from the likes of Verizon, T-Mobile, and AT&T. It's time for cell phone carriers to up their game, stay two steps ahead of the cybercriminals, and, for cryin' out loud, not be tricked or bribed into making fallacious SIM transfers.

C'mon, T-Mobile and Verizon, are you really NOT smarter than cybercriminals?

QR Codes: A Danger Hiding in Plain Sight

Feast your inquisitive eyes on a mysterious treasure map, its unfathomable patterns hinting at a promise of rich reward. Dusky pixels melt into a snow-white background weaving a symmetrical tapestry of binary phantasmagoria. Deep within this geometric masterpiece lies a pot of gold—for those brave enough to seek it—as well as booby traps and swarthy pirates lurking to bushwhack the unwary. The treasure map is curiously labeled *quick response*, but treasure hunters and gnarly pirates alike refer to the black-and-white labyrinth as a *QR code*. The QR code contains the coin of the realm and is brimming with mouthwatering feasts, keys to unlock treasure chests, and wrought iron portcullises to thwart even the most ruthless scallywags.

While the QR code is every bit a treasure map, it was not sketched by Edward Teach in the eighteenth century. Truth be told, the QR code was invented in Japan circa 1994 by Denso Wave, a subsidiary of Toyota, to monitor automobile parts across the manufacturing supply chain.¹⁰ The now-ubiquitous QR code has come a long way since then, becoming the gateway to Bitcoin, restaurant menus, Wi-Fi access, data encryption, and online bill payment.

In a refreshingly altruistic move for a capitalist enterprise, Denso Wave abstained from licensing QR codes, which made QR codes free for anyone to use. Although free is a fantastic deal, the QR code was not initially a big hit. In fact, QR codes meandered aimlessly in the wild until smartphone cameras became enabled with *QR code readers*; and even then, QR codes languished until early 2020—that's when the COVID-19 pandemic forced public-facing businesses to adopt QR codes for contactless ordering.¹¹ Instead of getting your hands dirty with a germ-ridden paper menu, you simply scanned the QR code with your smartphone camera to order a meal to go.

Today, QR codes are everywhere and used for everything from generating coupons, promoting websites, pulling up menus, sharing Instagram posts, and logging into applications such as the messaging platform WhatsApp. The result is we are drowning in QR codes. Perhaps the nadir was reached in 2022 when the cryptocurrency exchange platform Coinbase aired a sixty-second spot during the Super Bowl containing nothing but—wait for it—a meandering QR code!

The Coinbase Super Bowl ad was audaciously spartan—a color-changing QR code drifting aimlessly along the edges of a black screen to the tunes of not-so-funky elevator Muzak.¹² Yet, more than 20 million people took the bait and scanned the QR code, which took them to a promotional website. The website offered \$15 in free Bitcoin to new customers who signed up

for Coinbase while existing customers could enter a sweepstakes to win \$3 million in prizes. The Coinbase ad was spare, basic, simple—and so compelling the Coinbase app crashed due to the sheer volume of people visiting the site.¹³

Given the ubiquity of QR codes in everyday life, they must be harmless, right? They're plastered everywhere—from bagel shops to hookah lounges to bathroom walls to parking meters and streetlamps. That's got to mean they're guaranteed safe, doesn't it? And since QR codes are safe, we can point our smartphone at those enticing black pixels and scan away without fear of phishing, ransomware, or mead-swilling pirates. Okay, I'll grant you that being skewered by Blackbeard the Pirate is not something you need to fret about, but phishing and malware attacks are very much in the realm of possibility when you scan a weaponized QR code.

First, let me give you some good news. Legitimate QR codes from a trusted source are not hackable by cybercriminals. QR codes are essentially stored data in the form of black pixel groupings. This means that if cybercriminals changed the pixels, it wouldn't be the same QR code—it would be a completely different one. In essence, the QR codes themselves cannot be hacked; *it's the destination URL itself that is the danger*. For example, suppose Coinbase creates a QR code embedded with a URL to a promotional website. In that case, it's impossible for cybercriminals to manipulate the pixels so that it takes you to a phishing website. However, cybercriminals can create a brand new and completely different QR code and trick you into thinking it's the legitimate one from Coinbase.¹⁴ They can do this by sending you a phishing email that looks like it's from Coinbase but contains a malicious QR code, or they can send you advertisements in the form of postcards by snail mail containing a malicious QR code. That's why you should only scan QR codes that you know come from a legitimate, trusted source. If the QR code you're scanning really came from Coinbase, then it's safe, but if not, you could be scanning a malicious QR code.

Now, some bad news. When you're eyeballing a QR code, there's no way to ascertain whether the QR code is legitimate or malicious. For example, a phishing email might contain a lot of mistakes that you spot right off the bat—bad grammar, spelling errors, wrong URL, or a suspicious attachment. But a QR code is just a bunch of incomprehensible black pixels on a white background—it doesn't mean squat to human eyeballs!

In addition, QR codes are cloyingly omnipresent because anyone can create a QR code using free online tools. Simply go to an online QR code generator and type in the destination URL, and voilà—you have a QR code that transports your customers to a menu, an online ordering site, or an e-payment portal.

Just like the Rubber Ducky and Wi-Fi Pineapple, QR codes have become democratized so that anyone—even the Little Tramp, who can't rub two nickels together—can create a QR code in the blink of an eye. Unfortunately, cybercriminals know a good thing when they see it, so they use QR code generators and embed QR codes with malicious URLs that take the victim to a phishing website or a fake payment processor.¹⁵

Even worse, malicious QR codes are pretty darned easy to deploy—cybercriminals just slap the fake QR code on a sticker and plaster it over the legitimate QR code. Legitimate QR codes are readily exploitable because they are displayed everywhere—at restaurants, hotels, airports, and cannabis dispensaries—all for the purpose of helping customers find something to eat, drink, or toké. However, they can also be covered over with fake QR codes ready to pwn unwary victims. Any signs of tampering should be viewed with caution; otherwise, instead of pulling up

a menu, you might be redirected to a phishing website designed to steal your credentials.¹⁶

The risks of malicious QR codes are so palpable that the FBI, in October 2021, warned the public not to scan randomly found QR codes. “If you happen to scan a scammer’s bad code, you could end up giving him access to your device,” the FBI said in its alert. “He can access your contacts, download malware, or send you to a fake payment portal. Once there, you can inadvertently give him access to your banking and credit card accounts. If you make a payment through a bad QR code, it’s difficult if not impossible to get those funds back.”¹⁷

Take note of the unconscious bias in the FBI’s statement. Referring to cybercriminals as “he” and “him” is a bit tone-deaf and evokes the myth of the ultramasculine hoodie-hacker. Perhaps we need to stop referring to cybercriminals as the “bad guys”; otherwise, people typecast cybercriminals as adolescent he-men when the reality is that cybercriminals come in many different shapes and sizes—and colors, and nationalities, and genders. The point is, we need to dispense with the cybercriminal stereotype of a Mr. Robot-looking socially awkward male sporting a hoodie. Otherwise, we’ll be asleep at the switch when cherubic, non-stereotypical cybercriminals pwn us with impunity.

Fortunately, the FBI followed up with an alert in January 2022, offering more threat specificity—and gender neutrality—through its Internet Crime Complaint Center (IC3):

Cybercriminals tamper with both digital and physical QR codes to replace legitimate codes with malicious codes. A victim scans what they think to be a legitimate code but the tampered code directs victims to a malicious site, which prompts them to enter login and financial information. Access to this victim information gives the cybercriminal the ability to potentially steal funds through the victim accounts.

Malicious QR codes may also contain embedded malware, allowing a criminal to gain access to the victim’s mobile device and steal the victim’s location as well as personal and financial information. The cybercriminal can leverage the stolen financial information to withdraw funds from the victim accounts.¹⁸

The two FBI alerts are a testament to the ingenuity of cybercriminals in creating malicious QR codes and posting them in high-traffic areas so they’ll be scanned by an unsuspecting public. In 2022, cybercriminals attached fake QR codes to parking meters in several Texas cities to pwn people into paying the scammers. The scam was so commonplace, the City of Austin issued a public warning, stating that “people attempting to pay for parking using those QR codes may have been directed to a fraudulent website and submitted payment to a fraudulent vendor.” Fact is, the City of Austin does not even use QR codes for payment purposes, pointedly noting in the alert that “Austin Transportation provides three ways to pay for parking: by coins or credit/debit card at a pay station or by using the Park ATX app.” And to make this crystal clear, the alert contained a “No QR Code” photo with the caption, “Payment only accepted at pay station or via Park ATX app.”¹⁹

The next time you see a QR code on a Texas parking meter, don’t even think of scanning it; otherwise, the City of Austin might pack up and move to Iowa.

While cybercriminals love to post malicious QR codes in public places where they’re scanned by curious victims, there’s more bang for the pawning buck by simply adding QR codes to phishing emails. This is known as *quishing*, and it’s oodles more pernicious than the average

phishing attack.²⁰

In a run-of-the-mill phishing attack, a malicious attachment (or link) is appended to a phishing email and sent to a company's workforce. However, routine phishing attacks can be thwarted by antivirus software that flags the suspicious attachment and stops the phishing email from being delivered to the company's employees. But quishing emails bypass antivirus software, dispensing with a malware-laden attachment in favor of a malicious QR code.²¹ A typical quishing email pretends to be a company-wide survey and asks employees to scan a QR code that will take them to a survey site. However, the fake survey site is really a clever way to trick employees into logging in with their username and password, which will be recorded by cybercriminals and used to gain access to the company network, either to steal company data or inject a ransomware payload.

In a sinister variation of quishing, the malicious QR code could take employees to a website that injects malware into their smartphone. Known as *drive-by-QR code phishing*, this attack is particularly nasty because it doesn't require any action from the employee, such as logging into a fake portal with their credentials. All that's needed is for the employee to land on the infected website, and the website does its thing—that is, find a software vulnerability allowing it to download malware into the employee's smartphone.²² Spyware, for example, could be deployed to exfiltrate sensitive data on an employee's smartphone, which cybercriminals could use for a future cyberattack on the company's network.

But here's the kicker: What can you do about a software vulnerability known to cybercriminals but unknown to the company making the software? It's called a *zero-day vulnerability* because the security flaw hasn't been discovered by the software vendor yet; therefore, there is no software update (called a *patch*) to fix the defect and block a cyberattack. The cyberattack itself is called a *zero-day exploit* and is a fearsome threat because there's no defense against it.

Once the software vendor discovers the flaw, they can issue a patch to prevent the cyberattack—but the patch only works if users actually install it. That's why you should enable automatic updates on all your devices—smartphones, tablets, computers, and well, everything! This takes the burden off your shoulders and ensures patches are installed as soon as they're available. When you see a software update notification, install it immediately—delaying a software patch is like waiting to brush and floss until after your teeth are riddled with cavities.

Now, what does this mean for QR codes? The good news is that malicious websites exploiting zero-day vulnerabilities are rare, so drive-by-QR code phishing is not a major risk for everyday people. The greater threat is a malicious QR code that directs the victim to a website that tricks them into downloading malware. You read that correctly—while QR codes can be laced with URLs, they cannot be embedded with malware! A QR code is made up of pixels, which are well-suited for encoding a limited amount of non-executable data; however, it cannot execute programs, so a QR code cannot install ransomware just by being scanned. The real risk is that after scanning, the QR code directs you to a fake app store that tricks you into downloading a malicious app containing ransomware. The malware is downloaded because a human victim was tricked into installing it—not because the QR code itself could install malicious software on your smartphone.

But wait—in the FBI's 2022 alert, they chillingly warned, "Malicious QR codes may also contain embedded malware, allowing a criminal to gain access to the victim's mobile device and

steal the victim's location as well as personal and financial information.” The FBI's mistaken assertion is an example of *hacklore*, a term coined by Bob Lord, a veteran cybersecurity leader who has served as the CISO at Yahoo and as a Senior Technical Advisor at CISA.²³ Hacklore is a mashup of “hacking” and “folklore” created to debunk the urban legends and misinformation that plague cybersecurity.²⁴ The hacklore in the FBI's alert is the erroneous claim that malicious QR codes can install ransomware upon scanning, when the real threat is directing the victim to a phishing website where they enter their credentials or are tricked into downloading a malicious app.

Another example of hacklore is when cybersecurity professionals advise the public never to scan QR codes. Such advice is wrong because telling people not to scan QR codes doesn't work—they scan them anyway—and it's lazy, when the risks of malicious QR codes are better mitigated by teaching the public how to spot fake phishing websites, use password managers to create strong passwords, enable MFA, and install patches!

And therein lies the danger of spreading hacklore—it distracts the public from taking real steps that would genuinely protect them from cyberattacks.²⁵ Instead of telling people to “Never use public Wi-Fi,” or “Never scan a QR code,” which they will do anyway, the smarter strategy is to encourage the use of MFA so hackers cannot access accounts even if they steal a password—and to teach people how to spot phishing websites, so an evil portal or malicious QR code does not trick them in the first place.

That QR Code Might Be a Wolf in Sheep's Clothing. What Can I Do?

QR codes are everywhere these days, chock-full of actionable information and easy to access. Anyone with a smartphone can point their camera at it, and the QR code does the rest—menus, coupons, electronic bill pay, and online shopping spring forth like magic. It's no wonder QR codes are a marketer's dream gimmick—and a cybercriminal's dream vector.

Yet, just like the Rubber Ducky and Wi-Fi Pineapple, QR codes are not inherently good or evil—it's how they're deployed that counts. A QR code on a cafeteria table might be a guardian angel handing you the menu or a brimstone-tinged demon pwning you with a fake bill-pay scam. It's a QR code jungle out there, and it's up to you to dodge the apex predators as you live and play in the wild. Let's explore some tips and tricks to spot a QR-wolf in sheep's clothing and avoid getting burned by a QR code from hell.

Random is bad.

It's crucial to always vet the origin of the QR code so you're confident it's coming from a trusted source. This means putting on your thinking cap before you scan QR codes willy-nilly. A QR code at your local restaurant is probably okay; of course, you want to be careful that someone didn't cover over the legitimate QR code with a fake one. But physical tampering aside, the QR code from your favorite restaurant is likely okay.

You also don't have to worry about QR codes seen in advertisements from well-known companies like Coinbase. No way is Coinbase going to launch a bouncing QR code that pwns

you! In fact, QR codes are phenomenal marketing tools. When done right, companies can use QR codes to powerfully connect with their customers. A good example is the surreptitious QR code Disney snuck into the first episode of *Moon Knight*.²⁶ Eagle-eyed fans who scanned the pixelated Easter egg hidden on a sarcophagus were taken to a website where they could obtain a free digital copy of *Werewolf By Night* #32—the first comic book appearance of Moon Knight. Now, that’s clever marketing. Do you really think Disney would tarnish their brand by pwning you with a malicious QR code?

Absent physical tampering by a cybercriminal, QR codes from mega-corps like Coinbase and Disney are not a significant risk. Where the breach hits the fan is QR codes posted in weird places or QR codes appearing out of the blue:

- A package slathered with QR codes arrives in the mail containing goods you didn’t order from a vendor you’ve never heard of.
- Postcards, letters, and adverts printed with QR codes are delivered to your door by snail mail.
- A QR code at a restaurant table looks like a sticker pressed over another QR code.
- QR codes are posted on bathroom walls and stalls.
- QR codes are posted on parking meters, lampposts, mailboxes, or in any high-traffic area.

I trust you get the point. QR codes from trusted sources are not the problem. It’s those random QR codes displayed in unusual places we should be worried about. Random QR codes are a big red flag and should never be scanned. When you see them, just keep your smartphone in your pocket and look the other way.²⁷ Also, don’t fall for the scammer’s trick of masquerading as a reputable company while placing a QR code in a funky location. I assure you, Coinbase has a brilliant marketing team, and they’d never authorize posting their QR codes inside a dank, foul-smelling bathroom stall.

But hey, curiosity is a stubborn beast, and even though it killed the cat, you’ve decided to go ahead and scan the doggone QR code anyway. Perhaps it’s safe—but it might be a malicious QR code that’ll direct you to a phishing website. How much risk you can stomach is your call, so here are a few tips to help you manage the coin flip:

- **Check to see if the QR code has been tampered with.** Keep your eyes peeled for any signs of physical tampering before you scan the QR code. Cybercriminals can’t hack a legitimate QR code, so they create an entirely new one—a malicious fake that’ll take you to a phishing site. Always double-check that someone didn’t print a phony QR code and paste it over the actual, legitimate QR code. It’s a simple, obvious trick, and you’ll be mighty upset at yourself if you fall for it.
- **Use caution when paying a bill with QR codes.** Be uber careful when paying bills via QR codes. Only scan QR codes from trusted vendors, and verify the URL before entering payment details. Some bill-pay phishing websites are remarkably genuine-looking and may not contain spelling or grammatical errors, so you may want to contact your vendor

for other payment options, like a secure payment app. Alternatively, you can access the legitimate vendor's company website and log in to the payment portal directly.

- **Don't use a scanning app.** Why are you using a scanning app to scan a QR code? Don't do that! Your smartphone's camera doubles as a QR code scanner and is much safer. In 2021, the obviously named *Barcode Scanner App* was removed from the Google Play Store when Android users complained about a tsunami of pop-up ads flooding their screens after downloading an update.²⁸ The popular app boasted 10 million users—now victims—who all needed to run antivirus software or remove the app. What a hassle! Why bother using a scanning app when your smartphone camera can do the job just as well without the trouble of malware?
- **Be on the lookout for the telltale signs of quishing.** This tip is easy because there's really only one telltale sign: If you receive an email with a QR code in the body of the email, that's the red flag. A QR code in an email is the very essence of quishing, and you should exercise extreme caution.

It'd be highly unusual for a friend or family member to send you a QR code in an email, so if you get a QR code from them, it's likely their account was hacked. Do yourself a favor: Before scanning a QR code sent by your mom, give her a call first to make sure it was really her. I'm sure she'd love hearing from you (since you never call enough, anyway), and then she can verify that she really did send you that code.

However, if you get a QR code in an email from a stranger, do NOT call them to confirm, as you'd likely be speaking with a scammer trying to pwn you. Random emails with QR codes from strangers (or vendors you don't do business with) will probably be quishing scams. Do not scan the QR code, and do not engage with the sender. In addition to the QR code being the primary red flag, you should also be on the lookout for standard phishing red flags. These include misspelled words, bad grammar, a wrong URL, or a suspicious link or attachment. For example, if you have an account with Amazon or Target, but receive an email from "Amanoz or "Tarteg," you'd want to delete those emails pronto. Also, remember to keep your eyes peeled for website security. Look for HTTPS in the URL. If the URL is HTTP (without an "S") or you see "Not Secure" in the address bar, then you may have landed on a phishing website. Phishing emails also try to jolt the recipient into taking immediate action. By invoking a sense of urgency, the scammer is encouraging the email recipient to suspend their disbelief and do something they'd never do if they stopped to think about it. That's why phishing emails often masquerade as a creditor of the victim—such as a utility company or cell phone carrier—warning them they'll be charged a hefty fee unless they click on a link or call the scammer immediately to avoid the charge. But don't do it—whenever

someone sends you an email demanding immediate action, it's probably a scam.

Malicious QR codes are a pernicious threat—cheap, easy to create, and harmless-looking. They beckon to be scanned by puny humans who can't read the pixelated data to perceive the malicious link embedded within. If you're freaking out about demonic QR codes emerging from the fire pits of hell, you're not alone. But chill. QR codes are neither good nor evil; it's how they're deployed by their creators that makes them either beneficial or dangerous. Yet, even with malicious QR codes, the real pwning lies not in the pixels, but in the destination.

Beating the Hacker's Playbook: QR codes can't install ransomware on their own. What they can do is send you to a phishing site that tricks you into downloading a malicious app or entering your credentials. The QR code below directs you to my website—or does it? How do you decide if it's safe to scan, and how will you know the site is legitimate after?



CHAPTER 9

The Nigerian Prince Who Was the King of Phishing

ONCE UPON A TIME, there was a charming Prince of Nigeria who was strong and brave and true. With broad shoulders and a big heart, the Nigerian Prince gave voice to the voiceless as a champion for truth, justice, and a better tomorrow.¹ He dreamt not of wealth and power but of a kingdom thriving on diversity, equity, and inclusion and a steadfast commitment to environmental stewardship. The Nigerian Prince was a bootylicious piece of virile manliness, yet his heart was tempered with compassion, grace, and unwavering support for the #MeToo movement.

Verily, it was a dark day when a despotic general, high on toxic masculinity and palm wine, deposed the Nigerian Prince in a bloody coup d'état. The despotic general arrested the royal family and, in an act of utter cruelty, forced them to listen to the B-side of ABBA's "Super Trouper," at which point the royal minstrel begged to be hanged. Adding to the stench of fear, the despotic general canceled DEI throughout the land, declared the Gulf of Guinea be renamed to the Gulf of Nigeria, and levied tariffs on imported Chin Chin, sparking a national shortage of the beloved fried snack. The despotic general ruled with an iron fist yet greatly feared the Nigerian Prince, so he confiscated the royal family's immense wealth and banished the Nigerian Prince from the country.

But fortune smiled on the charming prince, as he had millions of supporters worldwide that he could count on for help recovering his frozen wealth. The Nigerian Prince wrote the most critical email of his life and sent it out to millions of kindhearted souls. The email read:

Dear Beloved Sir or Madam,

I am your most humble Nigerian Prince, and I have been deposed by a disco-biased lunatic who is jailing people for freestyle dancing. He has declared that all men under five-foot-eleven be called "Munchkins," while men above that height are levied a Vertical Adjustment Tariff, or VAT, which has fueled a national slouching epidemic. Worse yet, our national anthem has been changed to ABBA's "Dancing Queen" and everyone between the ages of twenty-one and sixty-five are forced to wear sequined spandex one-piece jumpsuits.

This cruelty must end! That's why I'm asking you to help me transfer my frozen

funds to another country so I can use the money to set my nation free. If you would be so kind as to transfer \$3,000 to my account, I can unfreeze the funds and transfer my money outside Nigeria. To repay your generosity, I will promptly send \$500,000 to your account.

Please reply immediately to get the ball rolling!

Sincerely,

The Nigerian Prince

Oh, gentle reader, the outpouring of support was legendary, especially amongst anti-ABBA Kiss fans, who dutifully replied with thousands of wire transfers to unfreeze our hero's assets. The Nigerian Prince, aided by the Kiss Army, ousted the despotic general and restored peace throughout the land. It was a joyous victory—everybody ditched their sequined jumpsuits, lanky men stopped hunching, and people who wired \$3,000 got \$500,000 in return.

And they all lived happily ever after!



Our fairy tale Nigerian Prince rules his kingdom with humble wisdom, but in real life, the Nigerian Prince is among the longest-running cyber scams, emerging in the 1990s as “electronic mail” became an accepted mode of communication. In the mid-’90s, scammers would send massive email blasts to potential victims claiming to be a Nigerian Prince whose money was frozen—but if the recipient would wire a small payment to unfreeze the prince’s account, they would be rewarded with a massive windfall for their generosity.²

Sounds absurd, doesn’t it? Wait, it gets crazier. You see, many fraudsters writing those emails were not fluent in English, so the phishing emails were filled with misspellings and poor grammar. In addition, the emails contained generic greetings like “Dear Sir or Madam,” followed by bizarre, melodramatic stories in which a prince begs for help to unlock millions of dollars in frozen assets—from a royal account, no less!

Today, very few people would fall for this BS. But in the mid-’90s, email was a trailblazing technology, and the Information Superhighway, now called the internet, was a new frontier for the public. Online users were less aware of the risks than they are today, so even though the Nigerian Prince scam is every bit as ridiculous as our fairy tale version, people still fell for it.

But today, online users are well aware of fraudsters trolling the internet and would not be fooled by email phishing scams, especially those containing misspellings, bad grammar, foreign URLs, oddly dramatic storylines, and urgent requests for money. Nope, today’s users would never ever get phished—not in a billion years.

However, according to cybersecurity firm SlashNext, malicious emails soared by 4,151 percent from 2022 to 2024.³ Clearly, people are still being pwned by phishing scams. After all, if the scams didn’t work, you’d expect the number of attacks to dwindle, not blast off into the stratosphere. So, why do these phishing attacks persist? According to SlashNext, the culprit is *ChatGPT*. Born on November 30, 2022, ChatGPT is a chatbot developed by OpenAI that uses artificial intelligence (AI) to have human-like conversations with, well, actual humans.⁴ The actual humans use ChatGPT to conduct online research, write emails, brainstorm ideas, and translate languages. But ChatGPT can also be a hoot—it can play trivia games, tell jokes, and

write modernist poems in the rule-breaking style of E.E. Cummings. While ChatGPT is a productivity beast, it's also another excuse to goof off.

ChatGPT is powered by Large Language Models (LLMs) that interpret language based on vast amounts of data from books, websites, and other sources, and it predicts the order of the words used for its answer.⁵ When you ask ChatGPT a question, it's using math to estimate the probability of what words should come after the other in its response. ChatGPT is an example of *generative AI* because it generates—that is, creates—new content (such as text, images, or videos) by recognizing the patterns it has learned from the vast amount of data fed into it.⁶ LLMs present a fascinating mystery as computer scientists and AI researchers don't fully understand the byzantine math behind the artificial mind. But although it may sound human, ChatGPT is not a “he,” “she,” or “they”—it's an “it,” and its lifeblood is math.

Crazy magic aside, generative AI is a productivity godsend to the average working stiff. But what's good for the goose is good for the hacker, and generative AI, just like a Wi-Fi Pineapple, has become a potent hacking tool for cybercriminals. When ChatGPT hit the scene in 2022, cybercriminals attempting to use it for nefarious purposes were stymied by ChatGPT's built-in ethical guardrails. For example, ChatGPT would flatly refuse to write a phishing email. However, hackers quickly learned to jailbreak ChatGPT by phrasing their requests in a way that tricked it into writing malicious content. But now, cybercriminals have created their own generative AI in the form of the evil and vicious *FraudGPT*.⁷

FraudGPT is a generative AI like ChatGPT but utterly lacking in ethical guardrails. It was developed by a cybercriminal who calls himself the *CanadianKingpin* and is sold on the Dark Web for \$200 a month (or you can snag big savings with a 12-month plan for \$1,700!).⁸ Armed with FraudGPT, cybercriminals have an AI-powered hacking tool for producing incredibly convincing phishing campaigns. FraudGPT can create a fake landing page that looks every bit as real as your employer's VPN portal, or it can whip up a website mimicking your bank's login page, or create bogus product reviews on a faux e-commerce site. But wait, there's more! FraudGPT can craft an email impersonating your CEO or your HR director, and it can even draft a phishing email pleading for an urgent wire transfer so convincing you'd think it was written by dear old Nonna.

Phishing with generative AI is a game changer for cybercrime. Gone are the days of the hapless Nigerian Prince, replete with comical spelling errors and soap opera storylines. Online scams powered by generative AI will be perfect, as LLMs can write a phishing email in any language, even accounting for dialect (like “theatre” in British English or “theater” in American English). A phishing website created by generative AI will not have spelling errors or incongruous verbiage, as generative AI will produce the customary language so the phishing website looks exactly like the site it's mimicking. With generative AI powering cyber scams, there will be fewer red flags.⁹ And because there are fewer red flags, it's easier to pwn people. It's no wonder phishing attacks have skyrocketed since the birth of ChatGPT.

If you find this depressing, just wait—it gets worse. Consider that garden-variety phishing is a mass attack on many people—for example, hackers send a phishing email to a company's workforce of 10,000 employees. Then there's *spear phishing*, where hackers set their sights on a handful of employees, usually a company's C-suite, such as the CEO, CFO, and CIO. Spear phishing can be labor-intensive—hackers must study their targets closely to learn how to craft a phishing attack that will fool the C-suite. They do this by studying the company's website, with

particular attention to press releases; also, C-suite leaders are usually active on social media, so Facebook and X (formerly Twitter) are key intelligence sources for cybercriminals. Sweat equity is the secret sauce in spear phishing, and that's why it's exponentially more effective than the "spray and pray" technique used in mass email blasts.

Here's the depressing part—imagine what generative AI can do with spear phishing. No, don't imagine. I'll tell you: This nightmare is called *adaptive phishing*.¹⁰ With spear phishing, it might take hackers weeks or even months to ferret out enough information about the victim to launch a successful phishing campaign. But aided by generative AI—or more accurately, *malicious AI*—the drudgery of trawling through corporate websites, social media profiles, and even public records camouflaged hip-deep on the web could be accomplished in seconds, minutes, or days. AI-powered *reconnaissance* is data extraction on steroids, hoovering up job titles, LinkedIn connections, Facebook hobbies, Instagram profiles, and even YouTube and TikTok videos.

The next step after ingesting vast data is *pattern recognition*, by which malicious AI connects the seemingly random dots into cohesive insights to devise *personalized attacks* that exploit the victim's online behaviors and relationships. For example, malicious AI could craft an email that sounds exactly like your baby boomer coworkers right down to their annoying use of ellipsis...or pepper fake emails with those trendy em dashes beloved by Gen Z bloggers—as for myself, I tend to use both...if that's okay with you!

Personalized attacks are the *raison d'être* of adaptive phishing. Cybercriminals can use malicious AI to exploit personal relationships and *shared experiences*, making these attacks disturbingly persuasive. For example, a potential victim, Paulie, frequently posts about his favorite baseball team, the Los Angeles Dodgers. A cybercriminal using malicious AI could craft a text pretending to be a friend: "Hi Paulie, remember we talked about the Dodgers last night? Well, check out this cool story about Shohei Ohtani!" Of course, the link takes Paulie to a website that looks exactly like ESPN but is a flawless fake designed to pwn Paulie out of his personal data and credit card information.

But Paulie's story doesn't end here. You see, Paulie's a pretty clever fellow, and he smells a rat. A furious exchange of texts explodes in which Paulie asks probing questions, only to be explained away by the hacker, who is using malicious AI to craft personalized responses based on AI-powered reconnaissance and pattern recognition. Paulie is wise to cybercrime, but with the help of malicious AI, the hacker may just have his number:

Paulie: "The link is out of left field! Why didn't you send this to my email?"

Hacker's Adaptive Response: "Oops, I'm on my cell phone. That's why I didn't email you! But the link is kosher!"

Paulie: "I don't have time to read it. What's the scoop on Shohei?"

Hacker's Adaptive Response: "Dude, you'll freak when you read about it! ESPN spills the tea!"

Paulie: "Excuse me, who are you? Identify yourself!"

Hacker's Adaptive Response: "It's Mikey, we're Facebook friends! We chatted about the Dodgers a while ago!"

Paulie: “Okay, well I don’t want to click that link—it feels like a scam.”

Hacker’s Adaptive Response: “Good to be careful, but it’s from ESPN. Super legit.”

Paulie: “Prove to me it isn’t fake!”

Hacker’s Adaptive Response: “Here’s a screenshot—I log in to ESPN all the time!”

Paulie: “I don’t want to log in...I’ll just look it up later.”

Hacker’s Adaptive Response: “ESPN only keeps the story up for a few hours for free, then it’s behind a paywall. You’ll miss out if you don’t log in soon, after that, you pay.”

Paulie: “You don’t sound like my friend Mikey—”

Hacker’s Adaptive Response: “I do sound funky over text! If we were messaging on Facebook, it would be different haha. I love your jokes about Shohei’s gambling. U crack me up!

Well, it looks like Paulie’s stuck in a rut. No matter what Paulie says, the hacker has a slick response because malicious AI can mimic the real Mikey’s linguistic style and tone and use the vast data it has on Paulie to craft a convincing response. Paulie may very well believe he’s texting with the real Mikey, and despite Paulie’s suspicions about the ESPN site, the hacker’s responses are personalized to exploit Paulie’s friendship with Mikey and their shared experiences (i.e., a love for baseball, the Dodgers, and Shohei Ohtani).

But it doesn’t have to be a human hacker on the other side of the text. Cybercriminals can use malicious AI to automate conversations via *bots* to launch adaptive phishing attacks across many platforms, such as email, text, and QR codes. And here’s the kicker—with malicious AI, one hacker can launch thousands of personalized phishing attacks concurrently.

The sheer scale of adaptive phishing powered by malicious AI is beyond imagination. Back in the ’90s, it took days, weeks, or months to launch a Nigerian Prince; now, it takes minutes. And, our comical Nigerian Prince came to you via clunky email, but with malicious AI, Prince Charming greets you in every communication medium. Yet instead of a comically fake Nigerian Prince, the attacker will appear as your boss, a friend, or your beloved Nonna, mimicking the tone, language, dialect, and cultural history of the actual person.

Once upon a time, phishing websites were a joke, containing spelling and grammatical errors and flowery language that today’s users would mock, but malicious AI can create a credible fake website in minutes and do so in pitch-perfect English—or Chinese or Arabic. We’ve long since left the idyllic world of fairy tales and now cower deep in the bowels of a frightful horror story. Malicious AI will terrorize the world with kaiju-scale attacks. Imagine a future where hackers launch millions of adaptive phishing campaigns, all tailored to individual victims. Adding to the dystopia, malicious AI will launch attacks across all platforms, and text messages, emails, phone calls, and deepfake videos will be so true to life that they’re impossible to tell apart from the genuine article. When your Nonna is a bot, and you can’t tell the difference, it’s like living in a real-life sci-fi nightmare. But this is the future to come, and I’m afraid the world is not ready for it.

From a societal perspective, there's an urgent need to fight fire with fire and build AI-powered defense systems to detect and defang adaptive phishing attacks in real time. We also need global privacy legislation to restrict how companies and social media platforms use, disclose, and manage user data. Collaboration between governments and industries could develop protocols to combat adaptive phishing. AI companies like OpenAI and Anthropic should be heavily regulated with a focus on the ethical use and development of LLMs, along with heavy funding for adaptive defenses that can crush malicious bots like bugs on a windshield.

Eh, well, I ain't holding my breath for any of that to happen soon, if ever. Until then, we must rely on ourselves not to get pwned. This means keeping an eye out for funky anomalies like emails coming from weird URLs (e.g., "amazol.com" instead of "amazon.com") or websites and emails containing bad grammar, misspellings, inconsistent fonts, or flowery language with lurid, melodramatic storylines. The comically unfunny Nigerian Prince (and others like him) is a scam that will never die, but knowing the basic red flags of phishing will keep you from being pwned.

Still, you need a few more cards to play to keep you safe, because adaptive phishing with malicious AI has raised the stakes. Be alert for communications with *peculiar timing*, such as emails or texts received in the wee hours of the morning or late in the evening. Cybercriminals know you're likely fatigued and not at your best. Also, malicious AI might know you're traveling, especially if you're a CEO who's blared your travel schedule in a press release, in which case you've also alerted cybercriminals who'd love to send you a phishing email after you crossed a few time zones and are bleary-eyed with jet lag. View oddly timed communications with high suspicion.

Even if the phishing email looks perfect, and there are no grammatical errors or misspellings, it might ask you to do something the real sender would never ask for. For example, the United States Post Office will never ask you for money to release a package due to an incomplete address. If you get a text like this, it's a scam. Or if you get an email from dear old Nonna pleading for a money transfer because she's "locked out of her online bank account," it's a scam because Nonna never banks online. Unless Nonna's hitting the limoncello at three o'clock in the morning, it's best to delete the email! I call these tactics *relationship spoofing*, and it's a dead giveaway when someone you trust is asking you to do something the real person (or organization) would never ask you to do. When this happens, it's probably an adaptive phishing scam.

Finally, be alert for any communications creating a *sense of urgency*. Scammers try to scare you into making an immediate decision so that you'll suspend critical thought. This is precisely what happened to cybersecurity expert Troy Hunt, who was pwned in a relatively basic phishing scam.

Troy Hunt is the founder and CEO of *HaveIBeenPwned.com*, a service that alerts people if their personal information has been exposed to a data breach. He has been recognized as a Microsoft Regional Director and Most Valued Professional for his contributions to online and cloud cybersecurity and is a sought-after keynote speaker. The dude is not just a cyber genius; he's a legend who has empowered thousands of people to stay safe online with the data breach service Have I Been Pwned.

Troy has more cyber-savvy in his little pinky finger than most people have in their whole motherboard, yet cybercriminals stole nearly 16,000 email addresses from subscribers of his eponymous *troyhunt.com* blog.¹¹ Cybercriminals sent Troy a crafty phishing email aping

Mailchimp, an email marketing service he used for his blog's mailing list. The faux Mailchimp message claimed Troy's sending privileges were suspended because of a spam complaint, and urgent action was required before Troy's ability to send emails could resume. Troy clicked on a link in the email, which took him to a Mailchimp login page, which, of course, was fake. Troy logged in with his credentials, entered his one-time passcode (OTP), and, wait for it—the ersatz Mailchimp page froze, and that's when Troy knew he'd been pwned.

Troy immediately went to the real Mailchimp page, signed in, and changed his password. But he was too late—the phish had already signed in with Troy's credentials and his OTP, and then exported his subscriber email list. The phishing attack was so highly automated that 16,000 email addresses were stolen in the minutes it took for Troy to sign in to the real website and change his password.

Troy is an Australian and was coming home from London with a bad case of jet lag. His exhaustion, coupled with a meticulously designed phishing email, contributed to the success of the cyberattack. "Tiredness was a major factor," Troy said on his blog. "I wasn't alert enough, and I didn't properly think through what I was doing. The attacker had no way of knowing that (I don't have any reason to suspect this was targeted specifically at me), but we all have moments of weakness and if the phish times just perfectly with that, well, here we are."¹²

Troy also noted the sense of urgency he felt, saying on his blog that the cyberattack was a "...very well-crafted phish. It socially engineered me into believing I wouldn't be able to send out my newsletter so it triggered 'fear,' but it wasn't all bells and whistles about something terrible happening if I didn't take immediate action. It created just the right amount of urgency without being over-the-top."¹³

And so we have a real-life cyber horror story, but much like a children's fairy tale, there are many lessons to be learned. For one, Troy was tricked into giving up not only his login credentials but also his OTP. This demonstrates one of the flaws of traditional MFA—a user receives a one-time code as an extra layer of security, but if the hacker tricks the victim into providing it, as in Troy Hunt's case, then MFA is bypassed.

A good solution is *phishing-resistant MFA*, which does not have one-time codes for hackers to steal.¹⁴ Instead, phishing-resistant MFA uses a *cryptographic key*, which is a physical doohickey like a *YubiKey* that plugs into your computer port.¹⁵ Or phishing-resistant MFA can be built directly into your device. Examples include using your face or fingerprint to access your iPhone or a *personal identification number* (PIN) to access your computer or a website. Biometrics and PINs are tied to the device, so if cybercriminals steal the victim's password, they're out of luck because they don't have physical possession of the actual iPhone or computer.¹⁶

You can see how phishing-resistant MFA would have saved Troy Hunt from a hellacious pwning. Even though cybercriminals stole his credentials, if Troy had a YubiKey, the phishing attack would have failed because the hackers would not have physically possessed the cryptographic key. Likewise, if Troy had a PIN tied to his laptop, the cyberattack would have failed because the hackers did not have the computer in their greedy little hands.

Unfortunately for Troy, Mailchimp did not offer phishing-resistant MFA.¹⁷ However, as phishing campaigns become exponentially more realistic, it's incumbent on companies to make phishing-resistant MFA an industry standard. Failure to do so is a critical oversight that exposes customers to AI-powered phishing, an emerging cyber threat that surpasses all prior phishing

modes of attack.

As for the pwning of Troy Hunt, it's a stark reminder that anyone, no matter how cyber-savvy, can be bamboozled by a clever phishing scam. By openly sharing his misadventure, Troy Hunt has set a new gold standard for transparency and accountability that I hope others who are scammed will emulate.

Troy, I'm sorry you got pwned, but thank you for the teachable moment.

CHAPTER 10

Romance Scams: “I Love You, Baby. Now Send Me More Money!”

When most people hear the word “catfishing,” they think of romance scams. But catfishing comes in a variety of flavors, each with its own motives and social engineering schemes. At its most basic, *catfishing* involves constructing a fake identity to build a relationship with a victim for a variety of nefarious reasons, such as identity theft, blackmail, or wire fraud. Then there’s the *romance scam*, a type of catfishing where emotional manipulation is weaponized to steal money from victims. And in the hackers’ playbook, the *crypto romance scam* takes it up a notch, baiting victims into fake cryptocurrency investments in the name of love.

Catfishing isn’t always a romance scam—just ask professional wrestling superstar Seth “Freakin’” Rollins. One of the top wrestlers in the WWE, the “Freakin’” nickname describes his flamboyant character, from the arrogant cackling as he struts to the ring to the endless kaleidoscope of wrestling attire plastered with vibrant but clashing colors. Add to the circus-like atmosphere a man bun exploding into black and blonde locks of shoulder-length hair, and you have one of the most trailblazing wrestlers of all time.

But Seth “Freakin’” Rollins is a man of many names. He was called “The Architect” during his reign as leader of the villainous wrestling faction The Shield—a bruising trio that included Dean Ambrose and Roman Reigns. He also earned the moniker “The Kingslayer” for defeating “The King of Kings,” Triple H, at WrestleMania 33, and later “The Beast Slayer” for vanquishing “The Beast Incarnate,” Brock Lesnar, at WrestleMania 35. Rollins is also called “The Drip God” for his extravagant fashion sense, as well as “The Visionary” and “The Revolutionary” because—well, why the hell not?

Aside from his wrestling persona, Colby Lopez was born and raised in Davenport, Iowa, where he lives with his wife, Rebecca Quin, a fellow WWE wrestler who performs as Becky “The Man” Lynch. In 2014, Lopez cofounded The Black & Brave Wrestling Academy to train athletes for a career in sports entertainment, and in 2019, opened a coffee shop called 329 Dport.

Colby Lopez is the real McCoy while Seth “Freakin’” Rollins is just a stage name for a wrestling persona. The Drip God is nothing more than a made-up character to entertain fans. And the outcome of Rollins’s wrestling matches is predetermined. Oh, and Seth Rollins’s promos are scripted.

But professional wrestling is not fake. It’s sports entertainment, which means the wrestlers are professional athletes but also talented actors who provide fans with a thrilling, vicarious

experience that blends soap opera drama with over-the-top athleticism. WWE performers work hard to create boo-able villains called “heels” and cheer-able heroes called “babyfaces.”

The actual matches themselves are brutal, even though they are scripted. It’s not easy performing a *moonsault*, which is a backflip off the top turnbuckle, or being on the receiving end of a *chair shot* (even though the chair is made of lightweight metal, it’s still a fricking metal chair!). The point is, wrestling moves require not only expert athleticism but also a high pain threshold. Gunther, a heel known as “The Ring General” in the WWE, is infamous for the *knife edge chop*, a classic move where the wrestler slaps his opponent’s chest with the edge of his hand. The fan-pleasing move results in a loud, skin-on-skin crack echoing throughout the stadium—and visible red welts on the recipient’s chest.¹

In the words of WWE ring commentator Michael Cole, “That’s gotta hurt!” But not as much as the real-life, unscripted smackdown that erupted when an enraged fan attacked Seth Rollins during a 2021 episode of *Monday Night Raw*. The fan, twenty-four-year-old Elisah Spencer, was a diehard wrestling fan who thought he’d been communicating with Seth Rollins for the past two years on Instagram and WhatsApp, but instead of befriending Rollins, Elisah was being conned by scammers impersonating the wrestling icon.²

The fake Seth Rollins asked Elisah for \$3,000 in gift cards to “prove his loyalty.” In return, fake Rollins would reimburse the gift cards and help Elisah score a job with the WWE as a wrestling blogger. But when fake Rollins’s check bounced, Elisah knew he had been conned—but in a twist, Elisah thought he was swindled by the actual Seth Rollins, not the conniving catfishers.

That’s when Elisah hatched a plan to confront the real Seth Rollins on a live episode of *Monday Night Raw*. The altercation took place after Seth Rollins’s match with Finn Balor. Rollins’s character was a heel at the time, and after blasting Finn with a steel staircase, he *curb stomped* Finn to win the match—for those not into wrestling, Rollins’s finishing move is a boot to the back of the head, smashing his opponent’s face into the canvas.

After winning the match, Rollins walked up the ramp to exit the stadium, and that’s when a more dangerous, unscripted battle was about to explode. Somehow, Elisah evaded WWE security, making his way to the top of the ramp to confront Seth Rollins. Wearing bright red pants and a black tee, the short but stocky Elisah rushed Seth Rollins, tackling him like a linebacker. The pair tumbled down the ramp in a tangle of arms and legs, with Elisah clawing Rollins’s half-naked flesh while grabbing fistfuls of Rollins’s two-tone tresses.

As WWE security entered the fray, Rollins slapped Elisah in a headlock and—according to Seth Rollins on Episode 387 of Logan Paul’s *Impulsive* podcast—squeezed Elisah’s testicles, forcing Elisah to release his grip on Rollins’s mangled mass of hair.³

Once WWE security pulled the two apart, Elisah was hauled off to jail and charged with “attempted assault and attempted violation of arts and cultural affairs” (e.g., fancy legalese for throwing a monkey wrench into a live event). Elisah eventually apologized to the WWE for his behavior, though it’s not quite certain he realizes he befriended scammers on social media, not the real Seth Rollins. “I apologized to the WWE for my actions,” Elisah told a Brooklyn news station. “I had a legitimate beef but as a grown man I could have settled it a different way.”⁴

As for Seth Rollins, he’s moved on from the incident and may have a new finishing move far more devastating, brutal, and fearsome than the curb stomp.

But what the hell do you call a testicle squeeze?

Brad Pitt: He's Rich, He's Famous, and He's Not in Love with You

Eleven billion carbon-based life-forms inhabit a ball of mud whirling through the Milky Way Galaxy. Their gooey brains are made of water, lipids, and proteins instead of quantum neural processors, yet they are presumably intelligent—even though Tinder algorithms dictate their elaborate mating rituals.

These bipedal creatures are called “humans,” and they are like snowflakes—no two are exactly alike. This means each human is unique and, therefore, special. God does not make junk, after all. In the entire world, there is only one “You”—and *you* are beautiful, iconic, fierce, brilliant, and low-key super fine. *You* are one of a kind.

But so is Brad Pitt. Born in Oklahoma, Brad Pitt is a celebrated actor, scoring two Academy Awards, two Golden Globe Awards, and two Screen Actors Guild Awards. Pitt's career skyrocketed when he played a hitchhiking cowboy in *Thelma & Louise* (1991). From there, he became a popular leading man, starring in films such as the coming-of-age drama *A River Runs Through It* (1992), the romantic western *Legends of the Fall* (1994), the psychological thriller *Fight Club* (1999), and *Ocean's Eleven* (2001), a buddy heist comedy.

In his personal life, Brad Pitt is a gossip columnist's meal ticket, making headlines for his high-profile marriages (and divorces) from Jennifer Aniston and Angelina Jolie, including a widely covered legal battle over the custody of his children with Jolie. Apart from his films and tabloid brouhahas, Brad Pitt is a philanthropist who supports many causes, including *One Campaign*, a nonprofit that combats preventable diseases worldwide.

Here's a fun fact: Before he made the big time, Pitt was a limousine driver for strippers, and he once dressed as a chicken mascot to peddle *El Pollo Loco*, a Mexican-themed fast-food restaurant.⁵

Just like *you*, Brad Pitt—if I may engage in a paroxysm of gratuitous pleonasms—is a unique, special, one-of-a-kind, rare, uncommon, exclusive, incomparable, singular, distinctive, original, and matchless human being without peer.

Out of 11 billion people sucking air on this planet, if there's only one *you* and only one Brad Pitt, what's the likelihood you'd ever meet Brad Pitt in person? What's the probability he'd ever call *you*? What are the odds that his mom would ever text *you*? Or that she'd be trying to hook *you* up with her son? Or that Brad Pitt would text *you* to—y'know, hook up?

What's the likelihood that Brad Pitt would text photos of himself in the hospital as he's being prepped for cancer surgery? Or that he's a multimillionaire but needs *you* to wire him \$800,000 because Angelina Jolie's divorce lawyer froze his bank accounts? Or that he loves *you*—deeply and passionately—but he can't meet *you* in person because he has kidney cancer.

What, pray tell, are the odds that *you* are in a textationship with the real, honest-to-gosh, Academy Award-winning star of stage and screen, the immortal and iconic Brad Pitt?

Despite the odds, in 2023, a fifty-three-year-old married French woman, Anne, believed that she was. According to French newscaster BFM TV, a scammer pretending to be Brad Pitt's mother contacted Anne via a Facebook message, saying, “It's a woman like you that my son needs.” While skeptical at first, Anne returned the messages from Brad Pitt's faux mother and eventually began messaging with the ersatz Brad Pitt himself. “At first I said to myself that it was fake, that it's ridiculous,” Anne said, venting about her travails on TF1, a French television

network. “But I’m not used to social media and I didn’t really understand what was happening to me.”⁶

Soon, Anne came to believe she was dating the real Brad Pitt, who was unavailable for phone calls because he was being treated for kidney cancer. The scammer even sent AI-generated images of Brad Pitt in the hospital, sometimes smiling, sometimes pensive, usually wearing a hospital gown with medical equipment in the background.⁷ However, calling the photos “AI-generated” is a stretch, as they look like cheesy Photoshopped fakes with Brad Pitt’s head superimposed on someone else’s body.

Perhaps the phoniest is a snapshot of Brad Pitt being operated on by two surgeons with a partial cut-out of his head, just above his mouth, inserted between the pillow and the bed covers. It’s an obvious and comical fake. Not only is Brad Pitt’s hair perfect for someone undergoing kidney surgery, but he’s not wearing an anesthesia mask, and the photo shows the doctors operating on his chest! Yeesh, either the photograph is fake, or Brad’s in the hospital from hell—definitely the former, but nonetheless it fooled Anne despite the easily discernible chicanery.

The fake Brad Pitt proceeded to love bomb Anne with romantic messages and promises of extravagant gifts, all the while tugging at her heartstrings with tearjerkers about his divorce from Angelina Jolie and the ongoing custody battle over their children—not to mention Brad’s life-threatening struggle with kidney cancer.

Anne was utterly enthralled by the scam and head-over-heels in love with the fake Brad Pitt. It’s no wonder she believed Brad Pitt needed a loan from her because, despite his vast wealth, his bank accounts were frozen by divorce litigation with Angelina Jolie. Anne divorced her multimillionaire husband and wired the settlement proceeds—nearly \$800,000—to a Nigerian scammer she thought was the real Brad Pitt.

“There are so few men who write this kind of thing,” Anne said in an interview. “I liked the man I was talking to. He knew how to talk to women, it was always well done.”⁸

Eventually, Anne realized she’d been scammed when she read about Brad Pitt’s romantic relationship with jewelry designer Ines de Ramon. Like many catfishing victims, the ordeal has left Anne with heartrending scars. Shortly after the scam was publicized, she was the butt of jokes and harsh cyberbullying. The victim blaming was so cruel and relentless that Anne was hospitalized with severe depression, prompting TF1 to pull the interview out of concern for her mental and physical safety.⁹

The Brad Pitt case is a cautionary tale of how romance scams prey on hope, vulnerability, and the human need for companionship. For Anne, who believed she was in love with a Hollywood celebrity, the scam cost her a fortune, her marriage, a broken heart, and public ridicule by internet trolls who found more joy in cruelty than compassion.

The Pig Butchering Playbook: Fat Wallet, Broken Heart

In the United States, romance scams involving digital currency are called crypto romance scams. In China, these scams are called *pig butchering*—a euphemism for fattening the victim’s crypto wallet with fake profits and then going for the jugular by robbing the lovesick noob of their life savings.¹⁰ Romance scams may sound like just another con game, but make no mistake: Romance scams are simply another form of a destructive cyberattack but on a deeply personal

level. Instead of tricking victims into clicking on a malicious link in a phishing email, cybercriminals lure the unwary into emotional bondage with romantic texts, emails, and direct communications using messaging apps like Google Hangouts and WhatsApp.

It is this emotional bondage—and the betrayal trauma that leaves deep scars when victims realize they’ve been butchered—that makes crypto romance scams a particularly vile form of cyberattack.

Pig butchering can begin as a stray email or text sent by “accident” to the potential victim, with the romance scammers hoping the recipient will text back rather than delete the message. Once the victim texts back, the scammers begin a deluge of personal communications, quickly evolving into a deep, but very fake, emotional connection. The best thing to do when receiving a message from someone you don’t know is to delete it, and many people do, but all it takes is for one person to respond, and a vicious pig butchering is not far in the offing. In this respect, romance scams are like phishing—both cyberattacks launch massive bombardments of communications, relying on the law of large numbers to yield a few noobs to be pwned.

In the case of phishing, cybercriminals launch thousands of spam emails, knowing all it takes is for one person to be hoodwinked into giving up their credentials to answer a fake survey. Much like phishing, pig butchering is launched in massive waves by cybercriminals who send catfishing texts to a victim’s smartphone or *direct message* (DM) a victim through a social media platform like Facebook or LinkedIn.

In fact, cybercriminal gangs often launch crypto romance scams in a manner resembling a telemarketing business. Using pre-written scripts, romance scammers operate like a call center to cold-call, text, DM, or email potential “customers” while deploying psychological and marketing strategies to close the deal. But, unlike a legitimate telemarketing firm trying to sell a product, romance scammers are out to fatten up their victims for a financial slaughter.

When hunting for victims, the most logical place to start is by trawling dating websites. Scammers will review someone’s profile and send a message to strike up a conversation; initially, it’s all just small talk—food, movies, and family life are breezy topics to get things moving in the right direction. Money and financial topics are like religion and politics; they’re not subjects you can bring up right away when you’re dating someone. Once the scammers have established a friendship with the victim, the trust building—or more accurately, *trust-jacking*—begins. Trust-jacking is a tactic used by scammers to emotionally and psychologically bind the victim to a crypto scam.

Now, cybercriminals are not targeting destitute people to cheat with crypto scams. Quite logically, they’re targeting people with money. You’d think well-heeled physicians, attorneys, and engineers would be too savvy to fall in love with a fake soulmate they met online and then pile their life savings into a risky liquidity mining investment. But you’d be wrong. Smart people are still, well, people, and anyone can be pwned if they’ve been thoroughly groomed by slick-talking romance scammers. This, then, is the key to pwning success—a romance scammer’s focus is on trust-jacking their victims so they’ll be receptive to discussing serious financial matters and eventually plow their life savings into a liquidity mining investment.

Since the essence of catfishing/pig butchering is pretending to be someone you’re not, trust-jacking begins with a fake backstory. An effective strategy is to create a fake online profile that very much resembles the background of the victim. A convincing backstory will birth a fake persona built upon the victim’s hobbies, political and religious beliefs, ethnicity, race, family life, and anything else the scammers can learn about the victim. That’s why in a crypto romance

scam, it's no coincidence the victim fell hook, line, and sinker for a fake soulmate who had the same religion, nationality, and race as the victim.

Romance scammers will also create fake photos to enthrall potential victims. These fake photos are often Photoshopped pictures of actual people, which is why a reverse image search is an effective technique in ferreting out a scammer. Once scammers reel you in with a good backstory and a nice photo, they're ready to sweep you off your feet with *love bombing*. This technique inundates the victim with wave after wave of romantic and sexy messages, using outrageous amounts of flamboyant, excessive flattery. Overt declarations of love and affection are a way of ramping up the victim's endorphins so their brain turns to mush, and they become utterly in the thrall of the scammer's fake persona.

Scammers will also steal the victim's heart by using pet names to get the romantic juices flowing. But the other reason why a fake lover is calling you "sweetie pie" is because multiple scammers are messaging multiple victims, and they can't remember your actual name. In fact, with a criminal telemarketing model, there may be a team of scammers in a call center messaging back and forth with many different victims, and it would be a dead giveaway if a scammer accidentally said, "I love you, Ross!" when the victim's name is actually Rachel—a mistake like that blows the whole scam right out of the water, doesn't it?

Once the victim is trust-jacked and willing to do just about anything for their fake soulmate, the romance scammers launch the crypto part of the crypto romance scam.¹¹ This entails "teaching" the victim about cryptocurrencies, crypto wallets, crypto platforms, and liquidity mining, with the ultimate goal being to pwn the victim of their life savings.

Liquidity mining is actually a legitimate activity that begins with an investor using a crypto wallet such as Coinbase Wallet to buy cryptocurrencies like Bitcoin and Ethereum.¹² Then, the investor takes the cryptocurrency and uses it to fund a *DeFi Platform*. Short for "decentralized finance," the DeFi Platform is a website allowing users to buy, sell, or lend cryptocurrencies.¹³

With the DeFi Platform, you can throw a tranche of your cryptocurrencies into a pot with other like-minded investors. The cryptocurrencies swirling around in the pot are called a *liquidity pool*.¹⁴ Cryptocurrency exchanges then tap into the liquidity pool and use those cryptocurrencies to fund trades on behalf of their customers. In return, the liquidity mining investors receive "rewards" in the form of tokens or fees.

Liquidity mining investors also execute a *smart contract*, which allows investors to access their cryptocurrency and rewards; of course, it's not like an actual legal contract drawn up by an attorney. It's just a clickable link bristling with code that enables the back and forth transactions between the DeFi Platform and the liquidity pool.¹⁵ In other words, it's the smart contract that allows you to get your money out when you need it. Now, if all of this sounds like a goofy, byzantine video game, you wouldn't be far off. Liquidity mining is an incredibly complicated endeavor, even when done by crypto geeks who know what they're doing. For the uninitiated novice, it's a minefield of risk with many choke points for crypto scammers to exploit.

Now that you understand the basics of all things crypto, here's how romance scammers launch a crypto scam: First, the scammers create their own DeFi Platform, which looks like the real thing, sometimes using colors, graphics, and layouts similar to an authentic crypto exchange like Coinbase. As a result, the victim believes it is a legitimate third-party platform. At the scammer's behest, the trust-jacked victim dutifully deposits a tranche of cryptocurrency and then invests the cryptocurrency in the liquidity pool.

In the next phase, the scammers trick the victim into putting more and more money into the liquidity pool—this is the fattening up part, just before the butchering. Since the scammers create the DeFi Platform, they can generate fake reward tokens that the victim sees in the account and believes are real. Even the “profits” are fake and just a means to entice the victim into investing more money in the platform.¹⁶

A crucial piece in the scam is instructing the victim to purchase a *liquidity mining certificate*, enabling them to invest cryptocurrencies in the liquidity mining pool.¹⁷ Of course, there’s no such thing as a liquidity mining certificate. In reality, it’s a clickable link giving the fake DeFi Platform access to the liquidity pool funds. In other words, the scammers tricked the victim into executing a smart contract, and now the scammers have total and complete access to the victim’s account.

Crypto romance scams are brutal on the victim. They feel betrayed and stupid, and the embarrassment alone prevents many victims from reporting the crime to the police. Hence, romance scammers mostly get away with these crimes because victims are too humiliated to come forward. It’s also likely the scammers are launching their schemes from another country, putting them safely beyond the reach of law enforcement officials residing in the victim’s home country.

Romance scams hurt, and the trauma of the betrayal is searing. But victims of romance scams are not stupid, worthless people—and they are not noobs. Cybercriminals are targeting successful, smart people who have money; they are doctors and lawyers, cops and clergy, scientists, engineers, and all kinds of professionals. It’s precisely because scammers are going after hard targets (that is, savvy, intelligent professionals) that scammers concoct emotionally charged scripts loaded with love bombs and psychological gimmicks designed to pwn even the most brilliant, skeptical person.

The Catfisher’s Playbook: Here Are the Telltale Signs of Romance Scams

When you’re under the thrall of Dracula, it’s not apparent he’s a blood-sucking ghoul until his fangs are buried deep into your jugular. Then, you think, “*Who is this person? I don’t even recognize him anymore!*” But once the Prince of Darkness drains you dry, stealing your soul and transforming you into one of his undead minions, that’s when it all comes together, and you realize you were pwned by the devil incarnate. It’s the same thing with catfishing. Victims are so entranced by the scammer’s fake persona that they don’t see the razor-sharp fangs sparkling in the dark until after the coup de grâce has been delivered. The realization that one has been pwned is an eye-opener, but all too often, the epiphany happens after the victim’s life savings have been devoured, leaving them a penniless zombie.

Romance scammers don’t ply their wares on the fly. They have a playbook, and if you understand the mechanics of the scam, you won’t become a victim by falling head over heels for their treachery.

1. **Random email or text.** The first dead giveaway is a random text, email, or DM seemingly coming out of nowhere. Sometimes a scammer will DM someone looking for

love on a dating website, or the scam could launch from popular social media platforms like Facebook or LinkedIn, but the sneakiest and most effective way to launch the scam is to send an “accidental” text to the intended victim’s smartphone.¹⁸

2. **Moving the conversation to WhatsApp.** The next step is to coax the victim over to a messaging app such as Google Hangouts or WhatsApp.¹⁹ Scammers have numerous concerns about social media sites. First, the victim may have friends on Facebook or Instagram who might tip off the victim they’re being conned. Let’s face it: If you rave about a guy you met online who’s chatting up a Bitcoin investment, your Facebook pals are probably going to give you an earful. The strategy of moving the conversation to WhatsApp is simply because the romance scammers want the victim all to themselves, away from the prying eyes of the victim’s Facebook cohorts.

But a scammer’s even bigger fear is that they’ll be reported when their scam comes to light. Creating fake Instagram sites or Facebook pages is frigging hard work, and the scammer’s vile achievement will be shut down if they’re reported by the victim. It’s a major PITA to reconstruct a brand-new faux Facebook page, so it’s vital to move the conversation with the victim to a messaging app. The beauty here is if the scam is discovered and the WhatsApp account is deleted, it’s no big deal to create a new WhatsApp account with a fake photo and phony email address. Of course, text messages and phone calls are obviously perilous because the scammer’s phone number can be traced. Messaging apps like WhatsApp are appealing because they’re an easy way to remain anonymous. Pig butchering is a crime, but it’s also work, and workplace safety is important to cybercriminals like it is to everyone else. Romance scammers turn to messaging apps because they’re a safe way for them to conduct their nefarious business. That’s why the second dead giveaway of a romance scam is pressuring the victim to chat exclusively using WhatsApp or other popular messaging apps.

3. **Asking for money.** Chatting on WhatsApp with a fake lover is one thing, but what did you talk about the last time you went on an actual date? Worldwide famine, the Russian invasion of Ukraine, and global climate catastrophe are not topics likely to be discussed on a first date, unless you’re trying to avoid a second. Most likely, you talked about the weather, your job, what movies you’ve watched, and how much you love woodworking—you know, small talk to get to know each other. You certainly wouldn’t ask your date for money to fund a liquidity mining investment, or to help pay for your baby sister’s emergency gallbladder surgery, or to loan you some cash so you can pay off your gambling debts. Neither would cybercriminals. They’re not stupid, after all. At first, they talk about their family, job, or hobbies, keeping things light and breezy. But eventually, the conversation turns to money. This is the third dead giveaway of romance scams. Once the victim is head over heels in love, romance scammers will ask for money.²⁰ They may trick the victim into plowing capital into complex liquidity mining investments, or they may tug on the victim’s heartstrings with an elaborate tearjerker involving a medical emergency or sudden job loss, making the pitch for cash an easy layup. Another tactic is promising to fly out for a romantic visit if the victim helps pay for airfare, but once the money’s in hand, the scammer always finds a ready excuse to cancel the trip.

4. **Mirroring the victim.** Romance scammers weaponize a variation of *behavioral mirroring* and *linguistic mirroring* to turn their victim's brains into endorphin-clogged mush. Mirroring is an aspect of trust-jacking and sets up the victim for the kill shot. Behavioral mirroring is simply mimicking another person's style of nonverbal communication, such as body language, facial expressions, and the like, in order to establish a trusting relationship.²¹ It's pretty basic how this works. If a person strokes their chin, crosses their arms, or flashes a smile, then you do the exact same thing. You should not be flamboyantly copying someone's exact gestures, as this would be off-putting and downright insulting. Instead, the mimicking is subtle and natural, and the point is to build a connection with the individual.

Linguistic mirroring is similar but involves repeating another person's words albeit in a subtle, different way; here, the purpose is not only to build rapport but to understand the other person's perspective.²² Linguistic mirroring is a particularly valuable tool when you're arguing with someone—not to try and win the argument, but to help you step into the other person's shoes so you understand where they're coming from.

Behavioral and linguistic mirroring are ethical techniques when used in a non-manipulative way.²³ For example, supervisors may use behavioral mirroring to demonstrate empathy when an employee is having a bad day. Individuals in couples therapy may use linguistic mirroring to gain an insightful understanding of the other's viewpoint. Human resources professionals often mirror candidates in job interviews to enhance communication and ensure the right fit for key positions. Likewise, candidates may mirror the interviewer because they really need the job and want to make a good first impression.

Mirroring techniques are used by salespeople and business leaders to better understand their clients' needs and challenges, furthering a deep bond and a relationship built on trust. Romance scammers, on the other hand, use mirroring techniques to groom victims, softening them up for a devious money-spinning trap. Because romance scammers are creating virtual lovers out of thin air, the scammers will never visit the noob in person or jump on a video chat. This makes traditional behavioral mirroring impossible to weaponize. Likewise, scammers will rarely pick up the phone and talk to the victim, which makes linguistic mirroring unfeasible. Because most contact with the victim is through texts, DMs, and messaging apps, romance scammers do a variation of behavioral and linguistic mirroring that I call *catfish mirroring*.

With catfish mirroring, romance scammers build a social media profile that's just too good to be true—the cyber sweetheart has all the same hobbies as the victim, loves the same food, worships the same religion, is the same ethnicity, embraces the same politics, and otherwise mirrors, in a virtual way, the victim from head to toe. Romance scammers will study a potential victim's dating profile or Facebook page for any information that can be used to invent a beguiling cyber-sweetie. But don't be fooled—it's no coincidence your cyber-sweetie is a Jewish boy living in Tel Aviv who's allergic to cats, loves Ghirardelli chocolate, and has been spiritually transformed by Taylor Swift's "Call It What You Want."

Romance scammers excel at creating fake social media profiles; Photoshopped headshots; and beguiling love bombs that match the victim's hobbies, interests, and backgrounds to a T. Whether you call it pig butchering or catfishing, when it comes to romance scams, the most dangerous word in the English language is *soulmate*, because if that's what you call your cyber-sweetie, you're flirting with disaster.

5. **Cyber-sweeties live in a galaxy far, far away.** If romance scammers could get away with it, they'd pwn noobs using fake profiles of Han Solo or Princess Leia. But even the biggest sucker on the planet wouldn't fall for an extraterrestrial lover, so they create cyber-sweeties who live a continent away. The cyber-sweetie could be a US soldier deployed in a NATO country, a physician performing cleft palate surgeries on children in the Philippines, an au pair for a prominent family in Germany, an English teacher in Malaysia, or a golfing instructor at a Club Med resort. With globalization and the competition for talent between multinational companies, it's easy for scammers to create fake profiles based on actual international job descriptions.

Scammers create fake lovers who live far, far away because it's necessary to keep the scam going and to avoid getting caught. The scammer doesn't want to actually meet the noob because that would give the game away. If the cyber-sweetie is an African lawyer in Kenya, but the scammer is a nineteen-year-old olive-skinned Italian, even the most naïve noob will catch on to the scam. Even worse, the noob could report the scammer to law enforcement or ask the dating site to delete the fake profile. So, if your cyber-sweetie lives on the other side of the world, tell them to pack their bags and find another chump to pwn.²⁴

6. **Cyber-sweeties break their promises.** Romance scammers are lying liars who lie! They'll promise to visit you in person, but once you give them money for airfare, they'll come up with a reason why they need to cancel the flight. They'll promise to join a video chat but then back out at the last minute due to a technical glitch. They'll guarantee your liquidity mining investment is refundable at any time, but when you try to withdraw funds, the payment is blocked unless a hefty fee is paid—and even then, you still can't access the funds.

Romance scammers lie because if they tell the truth, the scam is unwound, and they risk going to jail. They don't dare physically meet the victim (or hop on a video chat) because that would reveal the scammer's identity and set them up for a lengthy jail sentence. And once the victim invests in a crypto scam, the trap has sprung, and the whole point of the criminal enterprise has been realized. Scammers can't keep the scam going to a successful conclusion unless they lie, so when your cyber-sweetie breaks promise after promise, it's a warning sign to exit the relationship.

7. **Cyber-sweeties make their move at warp speed.** Romance scammers must turn the victim's brain into endorphin-fevered slush with all deliberate speed. Once the victim is head over heels in love with a cyber-sweetie, they'll suspend disbelief and fall for whatever flimflam the scammer throws at them. Scammers must con the victim into trusting them as soon as possible; otherwise, the intended victim might get wise and catch

on to the scheme, and there's no better way to establish trust than to make the victim fall in love.

That's why romance scammers will throw massive love bombs shortly after latching on to the victim.²⁵ Cyber-sweeties will pelter the noob with flowery romantic language and imagery—proposing marriage, planning romantic getaways, professing undying love and deep sexual attraction, and begging the noob to get off the dating site and onto WhatsApp since they are going steady now and not dating other people.

Romance scammers never call the noob by their real name—they'll use terms of endearment, such as “my love,” “my darling,” “my beloved,” “my sweetheart,” and the like. They'll also use cringeworthy pet names, such as “Hot Stuff,” “Honey Bunny,” “Sweetie Pie,” or the ever-nauseating “Pookie”—ugh, if there's a pet name more annoying than “Snookums,” that's got to be the one.

A catfishing scam operates much like telemarketing, with multiple scammers interacting with different victims and sometimes juggling conversations with multiple noobs at once—so, obviously, it's easy to get confused and mix victims up! But calling the victim by a pet name or using terms of endearment prevents a dreadful mistake from happening and the scam from being accidentally revealed. Another plus for the scammers: Terms of endearment and pet names are yet another tactic to woo the victim into becoming infatuated with the fake cyber-sweetie.

While moving the platonic relationship to an amorous climax is intrinsic to the success of the scam, there is another, darker reason for love bombing: Once the scam is revealed, victims are often so embarrassed that they won't report the scam to law enforcement. When victims realize they've lost their life savings to a fake cyber-sweetie, the ordeal is so emotionally devastating—and mortifying—that they often keep it a secret, even from their friends and family. Romance scammers know if they can make the victim fall in love quickly and deeply, not only will the scam play out as intended, but the humiliated victim will not tell a soul when the scam is revealed, increasing the odds the scammer will never get caught. Simply put, an infatuated noob is a matter of workplace safety for romance scammers.

8. **Cyber-sweeties ask for specific means of payment.** You work hard for the money and want to get paid. So do romance scammers, and that's why they use payment methods that deliver funds in the blink of an eye and can't be reversed if the noob has a change of heart. Scammers also don't want their identities revealed, so they choose payment methods that allow them to remain anonymous.

When romance scammers ask for money, they never ask the victim to send money by check or credit card because the transactions are tracked and monitored by banks and credit card companies. Wire transfers and gift cards provide funds quickly, can't be reversed, and allow the scammer to be anonymous.²⁶ Wire transfer payments and gift cards enable a successful scam—the money-spinning transaction is blazing fast, untraceable, and conceals the scammer's identity so they don't get caught.²⁷

If your cyber-sweetie pleads for airfare to visit you, the payment method is a big red flag. Anything other than payment by check or credit card should be viewed with suspicion, though asking for money in and of itself is dubious. And if your cyber-sweetie utters the word “Bitcoin,” that’s the biggest red flag of all!



Beating the Catfisher’s Playbook: Romance scammers have a game plan, but if you understand how the scam works, you won’t become a victim by falling in love with a cyber-sweetie. Think about your family, friends, and coworkers—who can you warn today?

Telltale Signs of Romance Scams	Explanation
Random Email or Text	Contact comes unexpectedly from someone you’ve never met, such as an “accidental” text to your smartphone.
Moving the Conversation to WhatsApp	Scammers pressure victims to shift conversations from social media to private messaging apps where there’s no monitoring or oversight.
Asking for Money	Scammers ask for money, often with dramatic stories about emergencies (medical bills, business problems, etc.) or by tricking victims into investing in phony liquidity mining schemes.
Mirroring the Victim	Scammers create fake social media profiles and send texts or emails that mirror your interests, values, beliefs, and desires, giving you a false sense of compatibility.
Scammer Lives in Another Country	Scammers create fake lovers who live far away because it’s necessary to keep the scam going and avoid getting caught.
Scammer Breaks Promises	Cancels scheduled meetings or video calls at the last minute with dramatic excuses, maintaining the romantic illusion while avoiding real contact.
Scammer Moves Quickly	Expresses love within days to create an emotional bond before the victim’s rational judgment kicks in.
Scammer Asks for Specific Means of Payment	Requests money through untraceable methods that cannot be reversed or recovered, such as wire transfers, gift cards, or cryptocurrency.

Any one of the above telltale signs means there’s a good chance a romance scam is underway, but as the deceptions pile up, it’s likely the scam is at an advanced stage, and it’s time to wise up before financial disaster strikes. But if you’re so infatuated with your cyber-sweetie that even these warning signs can’t wake you from a love-crazed stupor, try doing a *reverse image search* of your cyber-sweetie’s profile photo.²⁸ You can do this with Google Image by clicking the camera icon and uploading the photo. The search results may reveal that the cyber-

sweetie's photo actually belongs to another person, or the results may show the cyber-sweetie's photo is linked with dozens of entirely different online profiles. Whether the romance scammers stole a person's image from a random website or created a deepfake image but concocted multiple bogus identities, you'll undoubtedly know something rotten is afoot with a reverse image search. But if you're still unsure, then you're exactly the type of noob I'd like to challenge to a rousing game of high-stakes poker.

CHAPTER 11

The Hacker's Deepfake Playbook

Reeling in big money by going *vishing*—the portmanteau of voice and phishing—is as easy as a phone call. Cybercriminals zero in on a victim company by virtually *casing the joint*, which in the halcyon days of 1940s film noir meant inspecting the place of an intended future crime, such as a bank or jewelry store, so you could plan your caper. In the 1940s, casing a joint was risky, as you had to do it in person. Today, cybercriminals can reconnoiter a victim company while eating donuts in their jammies. Anyone—from industrial spies to rookie con artists—can safely trawl through a company's website to obtain publicly available information that can be exploited in a cyberattack.

Public-facing data is a formidable cybersecurity risk as the information that companies post on their websites or on social media has the potential to become a weapon of mass deception in the hands of cybercriminals.

The first step in a vishing attack is to peruse a company's website to identify employees who have the power to spend money. For example, personnel with budgetary or accounts payable authority are prime targets for vishing scams. The second step is to obtain voice samples of key executives—such as the CEO or CFO—who often post videos of themselves giving speeches, talking to the media, or addressing company staff. Cybercriminals effortlessly obtain these promotional videos, usually published on the company's website or posted to popular social media sites such as LinkedIn, YouTube, and X (formerly known as Twitter).

Next, the cybercriminal needs a *burner phone*—so-called because it's cheap enough to toss into the dumpster after using it to commit a cyberattack.¹ Burner phones became a household meme in 2002 when drug dealers used them to hide their identities from Baltimore's Finest in HBO's crime drama *The Wire*.

Although the nom de plume suggests a high-tech spy gadget, it's really just a no-contract prepaid mobile phone. Pretty boring technology, but the no-contract prepay means calls from a burner phone cannot easily be traced to the caller. However, no tech is perfect, and there's no iron-clad guarantee of anonymity, especially if the National Security Agency (NSA) is out to get you. Still, criminals commonly use burner phones to cover their tracks, whether they're calling to score a drug deal or trying to scam retirees out of their pensions.

While burner phones are a vital instrument in the cybercriminal's tool kit, they are also helpful for fine upstanding citizens who want to protect their privacy.² For example, you should exercise caution before giving your primary phone number to the first cute person you meet on a dating app. Or if your company doesn't have a compliance hotline, you'd rightly be wary about

reporting an embezzlement, particularly if the fraudster is your boss. In this instance, a burner phone might come in handy so you can anonymously report the fraud.

Burner phones are also nifty when you're calling to get information about a coveted item—like that zippy Porsche Boxster you fantasize about—but you don't want to be pestered by high-pressure sales calls from the dealership. After all, sometimes it's not about the purchase but the dream!

While burner phones are hugely popular with drug dealers and cybercriminals, burner phones are not intrinsically good or evil. Instead, how they're used makes them what they are—either a valuable tool for protecting one's privacy or a malicious device to launch a withering cyberattack.

Now, let's break down a typical vishing attack. First, cybercriminals case the joint to identify an accessible dupe, which is safe and easy to do, especially when the email and phone number of a director with budget authority is published on the company's website. Next, the cybercriminals download voice samples from key executives, such as the charismatic CEO who posts motivational videos on YouTube. All that's left is to feed the voice samples into deepfake *artificial intelligence* (AI), creating synthetic audio that captures the pitch, tone, timbre, accent, and other qualities of the CEO's voice.

Deepfake voice cloning is made possible by AI and machine learning. The secret sauce is what's called a *generative adversarial network*, or GAN for short.³ Despite the ominous moniker, GAN is not at all like Skynet, the rogue AI from the 1984 sci-fi epic *The Terminator*. Instead, GAN is a learning model consisting of two neural networks. One, a *generator*, creates fake data, and the other, a *discriminator*, tries to separate the wheat (real data) from the chaff (fake data). The game keeps going until the generator creates real-enough-looking chaff (fake data), bamboozling the discriminator into thinking it's wheat (real data). By the way, chaff is the husk surrounding the grain and is inedible, so deepfake wheat milled into biscuits might taste great, but you'll need a bottle of Pepto-Bismol for what follows. I'm joking, of course; AI can't make deepfake food—yet! But with GANs primed for voice cloning, you basically have two software algorithms in a learning competition, resulting in a deepfake voice that matches the tone, timbre, pitch, and other characteristics of a real person's voice.

If this all sounds complicated, just think of GANs as a steel cage wrestling match between two pumped-up neural networks, something perhaps like this:

World Deepfake Voice Champion Stone Cold Data Generator struts into the cruel, glistening steel cage and snarls, "Hey, Baby Face, you know me. I'm your good buddy Barack Obama! I'm seeking donations for a children's charity! How about making a big, fat donation?"

The challenger, Baby Face Discriminator, says, "Whoa, hold on right there, you tricky devil! You're not Barack Obama—you're a nasty neural network trying to fake me out!" Baby Face grabs Stone Cold by the throat and dumps him to the canvas with a brutal choke slam.

Stone Cold shakes off the cobwebs and, altering the timbre and pitch of his voice, says, "No, really, Baby Face—it's me, Barack Obama! I'm not here to wrestle! All I want to do is help the children!"

Baby Face steps back and thinks, “Gee, wait a doggone minute. That does sound a bit like Barack Obama. It really does! Wait, no—the flow of voice is all wrong. It can’t be POTUS 44!” Baby Face leaps off the turnbuckle and batters Stone Cold with a flying elbow. Stone Cold collapses in the middle of the squared circle, and Baby Face covers him for the pin.

But before the referee can begin the 1-2-3 count, Stone Cold corrects the pitch, timbre, and cadence of Barack Obama’s natural voice and says, “Please, Baby Face, it’s really me, your good friend Barack Obama! I’m not that bald-headed, beer-swilling jerk Stone Cold Data Generator! Please get off me so we can help the world’s starving, needy children!”

Baby Face leaps off Stone Cold and, with a big smile, extends his hand to help Stone Cold get to his feet. But, it’s Deepfake Obama who clasps Baby Face’s hand, and after a vicious kick to Baby Face’s solar plexus, yanks Baby Face’s jaw deep into Deepfake Obama’s shoulder, knocking Baby Face senseless with a vicious Stone Cold Stunner.

In a shocking turnabout, Baby Face Discriminator flops to the canvas and is pinned by Deepfake Obama as the referee completes the three count. The audience erupts in cheers as the referee lifts Deepfake Obama’s hand in victory, and a new World Deepfake Voice champion is crowned.

If you think of GAN as a battle between professional wrestling titans—or a back-and-forth tennis match—you wouldn’t be far off. GAN is a machine-learning framework applying *game theory* to create a computer-generated simulation of a real person’s voice; it sounds like the real thing, but it’s actually a deepfake.⁴ However, voice cloning is not make-believe science fiction, as deepfake voice-cloning tools have long been available on the internet. For example, in 2019, a GitHub user, Corentin Jemine, published *Real-Time Voice Cloning*, an open-source tool that generates text-to-speech deepfakes with just a brief sample of the victim’s voice.⁵

Text-to-speech means you type words on a keyboard, and the software magically generates a person’s cloned voice. You might think voice-cloning technology is so complicated it would be expensive to develop, and there’d only be a few big players in the market (kind of like operating systems—how many competitors does Microsoft have, hmm?). Even worse, the lack of competition in the market would lead to outrageously expensive voice-cloning options (again, I’m looking at you, Microsoft!). Yet, the internet is positively littered with inexpensive—and even free—deepfake voice-cloning tools. For example, *Respeecher*, *Descript*, and *Resemble AI* are popular subscription-based voice-cloning platforms.⁶ Yet, the budget-conscious ethical hacker has many free open-source voice-cloning tools to choose from. Likewise, cybercriminals have access to the same free open-source voice-cloning technology they use for nefarious purposes. This is an inherent problem when dual-use technology, or tech that can be used for good or evil, becomes mass-produced and democratized.

In March 2019, in what’s likely the first publicly reported AI-enabled deepfake vishing scam, the director of a British energy company wired \$243,000 to a Hungarian bank at the request of cybercriminals posing as the CEO of the German parent company.⁷ According to the energy company’s insurer, Euler Hermes, the director thought he was talking to his boss, who urgently

needed the funds within one hour to avoid late payment fines. The fake CEO also promised the director that the parent company would reimburse the British subsidiary for the wire transfers.

As reported by *The Washington Post*, “the false Johannes,” the French insurer’s sobriquet for the fake CEO, was actually a computer-generated synthetic voice. “The software was able to imitate the voice, and not only the voice: the tonality, the punctuation, the German accent,” a Euler Hermes spokesperson told *The Washington Post*.⁸

In addition to using AI-enabled voice cloning software to create Deepfake Johannes, the cybercriminals deployed social engineering tricks to increase the likelihood that the director would fall for the scam. Trick No. 1 is to ratchet up the fear factor to intimidate an employee into taking action, and nothing induces fear more than a call on Friday late afternoon from your boss with an urgent request. Very often, there’s a massive power differential between a boss and a subordinate, such as a doctor to a nurse, a general to a private, or a CEO to a rank-and-file employee. This *power differential* is the crucial element to vishing attacks and explains why cybercriminals are so eager to impersonate powerful executives to attack others further down the food chain.

In swindling the British energy company, the cybercriminals strategically cloned the voice of the director’s boss. To ramp up the anxiety further, Deepfake Johannes injected *time pressure* by urgently needing the money to avoid a compliance issue (e.g., late fees) on a Friday afternoon. Trick No. 1 is mind-numbing, fear-inducing PRESSURE—and it can be social pressure (“Make the boss happy!”), time pressure (“I need this urgently!”), business pressure (“We’re gonna lose the deal if I don’t get the money!”), or legal pressure (“I need the money to pay a fine!”). Adding to an already tense situation, cybercriminals magnify the pressure a hundredfold by making the vishing call on a holiday, weekend, or late Friday afternoon.

AI-enabled voice-cloning technology is a game-changing superweapon for cybercriminals, but deepfake voice scams are exponentially more effective when combined with scam-tested social engineering tricks. I’ll prove this quantitatively with my very own I’m-no-Einstein mathematical formula:

Deepfake Technology x Fear Factor (Power Differential + Pressure) = \$35 million theft.

Bad math notwithstanding, a deepfake scam won’t always result in a \$35 million theft, but it did in 2020 when cybercriminals stole just that princely sum from a United Emirates Bank. By using the cloned voice of a company executive (power differential!), cybercriminals tricked a branch manager into authorizing transactions to fund an acquisition (pressure!), and the cybercriminals made off with \$35 million (ouch!).⁹

Trick No. 2 is explaining away any technical glitches when the deepfake voice-cloning software isn’t up to snuff. For example, if Deepfake Johannes didn’t sound right—perhaps the cadence was off, or the German accent sounded French (Sacrebleu!), or the text-to-speech had a delay—then the British director might have become suspicious and hung up. To avoid technical glitches spoiling the con, cybercriminals will usually make the vishing call with some noise in the background, thus allowing the victim to rationalize away any suspicions. To set the stage for a good excuse if the deepfake voice isn’t convincing enough, one could imagine Deepfake Johannes calling from a cafeteria—with glasses and plates rattling in the background—or from a noisy hotel lobby or any number of locations where everyday familiar sounds will provide cover

for a shoddy deepfake.

Even with AI-powered technology at their fingertips, cybercriminals will leverage human nature to ramp up the pressure until shiny beads of cold sweat rain down from the victim's forehead (Trick No. 1). And when technology lets them down, cybercriminals will rely on familiar background noises to explain away any voice-cloning hiccups (Trick No. 2). Deepfake voice-cloning software is a crucial hacking tool, but a successful heist will always depend more on the cybercriminal's skills for deception and for exploiting human frailty.

“Alexa, Clone My Boss's Voice.”

While vishing attacks are having their day in the sun, they're still a ripple in the ocean compared to old-fashioned, garden-variety email phishing attacks. Per RSA's Q3 2018 Fraud Report, plain-vanilla phishing emails represented 50 percent of fraud attacks worldwide, yet vishing scams appeared as a mere blip, accounting for barely 1 percent of all phishing attacks.¹⁰ Phone-only vishing scams are relatively rare in the cosmic tapestry of cyber fraud, and AI-enabled deepfake voice scams are probably rarer still.

Nonetheless, since RSA's 2018 report, other cybersecurity organizations have taken notice of vishing attacks. For example, in 2022, the US Department of Health and Human Services Health Sector Cybersecurity Coordination Center (HC3) issued a warning: “Voice phishing, also known as vishing, is the practice of eliciting information or attempting to influence action via the telephone. Over the past year, HC3 has noted a marked increase in these attacks across all sectors.”¹¹

Vishing attacks are on the upswing. According to the Quarterly Threat Trends & Intelligence Report, issued by cybersecurity firms Agari and PhishLabs, *hybrid vishing attacks* zoomed a stratospheric 625 percent from Q1 to Q2 2022.¹² Hybrid vishing is also known as *call-back phishing*, in which cybercriminals send a phishing email containing a phone number for the victim to call. The phishing email is usually about an urgent matter, such as a locked bank account or a hefty billing charge, and the only way to resolve the problem is to call the number found in the email. However, when the victim calls the number, instead of a bona fide bank representative, they are actually speaking to a wily cybercriminal.

As you can likely guess, the cybercriminal tricks the victim into divulging personal information in order to resolve the problem. For example, to reverse the charges on the billing invoice, the cybercriminal will ask for the victim's credit card information. Or to unlock the bank account, the cybercriminal will pretend to authenticate the victim by asking for their date of birth and social security number.

Of course, the nastiest trick of all is when the cybercriminal asks the victim for their username and password to “reset the account.” After the clueless victim obliges, the cybercriminal logs into the victim's account with the stolen credentials, drains the victim's funds, and changes the username and password, locking the victim from the account.¹³

Hybrid vishing is very nasty, and you'll feel like you've been gutted if you get hooked, so if you get an email out of the blue with an urgent problem that can only be resolved by calling the number in the email, I suggest you DO NOT CALL BACK!

Still, if phone-only vishing is rare—or at least nowhere close to the threat posed by email

phishing—then just how big a risk is deepfake voice vishing? Heists using deepfake voice technology occur far less than the massive frauds occurring with email phishing campaigns, including call-back phishing. And yet, frauds via deepfake vishing scams are a rapidly growing risk, particularly as AI-powered voice-cloning tools become democratized. Right now, deepfake cloning tech is so cheap that anyone with a credit card can buy a subscription to some pretty radical AI-powered voice-cloning platforms. Also, for those with a bit of geekiness in them, there are free open-source platforms ready to exploit. From a cost perspective, deepfake cloning software has become democratized.

With currently available technology, voice-cloning software is easy enough for someone with a bit of technical savvy to create computer-generated voices in a jiffy. But maybe you've decided not to panic until voice cloning is so easy even non-geeks can mimic voices right out of the box. If that's how you feel, I have some news for you: It's time to start freaking out.

This brings us to Amazon's personal voice assistant, Alexa.¹⁴ Wise beyond its years and all-knowing, Alexa is a cloud-based platform that will help you with just about any task. Simply voice a command to your Alexa-enabled device—which, you guessed it, is another Amazon product, the aptly named Echo—and Alexa will dim the lights in your smart home, order take-out from your favorite Italian restaurant, read a bedtime story to your kids, warn you if it's going to snow on Thursday, brew a pot of coffee, and, no surprise here, Alexa loves to buy stuff for you on Amazon!

Alexa's the ultimate smarty pants because it's always learning new things; in fact, Alexa has over 100,000 *skills* designed to make your life a piece of cake.¹⁵ Brainier than the average smartphone app, Alexa's got the skills to monitor your Capital One checking account, explain what's in your cocktail, get you in shape with a five-minute plank workout, tell you what's on TV at 8 p.m., and then actually turn on the TV at 8 p.m. Alexa will even make you the Q of *Star Trek* trivia because, let's face it, resistance is futile.

Amazon's master plan is augmenting AI with *ambient intelligence*, meaning AI platforms like Alexa will be embroidered into the fabric of people's daily lives. Describing the concept at Amazon's Re: MARS conference in June 2022, Alexa AI Head Scientist Rohit Prasad said, "[W]e mean that the underlying AI service is available everywhere around you, assists you when you need it, even anticipates your needs, but fades into the background when you don't need it."¹⁶

Alexa is hugely popular with Amazon customers, and its widespread use means Alexa may well be on the road to achieving ambient intelligence. "Alexa gets over a billion requests per week from hundreds of millions of devices available in more than seventy countries and seventeen languages," Prasad said. "Alexa is available in our homes, cars, phones, and now, Alexa is also headed to the moon as part of the project Artemis."¹⁷

Amazon's moonshot project is now finding a place for itself in the healthcare industry.¹⁸ Hospitals are placing Alexa-enabled devices by the bedside so patients can order meals from the cafeteria, turn on the TV, send a message to their doctor, or ask for help—"Alexa, tell my nurse I'm thirsty!"¹⁹ But the vast majority of Alexa's tasks are still initiated by a human, not Alexa. For ambient intelligence to reach its full potential, Alexa must learn to anticipate the needs of its customers, follow through, and then recede into the background. During his Re: MARS presentation, Prasad described Alexa's increasing ability to perform tasks on its own. "The best examples are things like hunches and routines," Prasad said. "When Alexa turns on your coffee

machine at a particular time, or lets you know that your garage door is open. Today, more than 30 percent of actions and smart-home interactions are all initiated by Alexa.”²⁰

Will Alexa really become the human race’s virtual Gal Friday? With ever-increasing skills, Alexa is becoming more useful and impactful in people’s daily lives. Perhaps when ambient intelligence reaches its zenith, we’ll live in a world saturated with invisible Alexa-enabled devices that we access with the wave of a hand, wink of an eye, or just by telling it what to do. Alexa’s even becoming more proactive, doing things without anyone even asking. So yeah, Alexa (or another AI like it) could become our Gal Friday—unless, of course, Alexa starts telling *us* what to do.

Most people barking commands at their Echo smart speaker are quite comfortable when Alexa responds with its legendary robotic female-sounding voice. But how would you feel if Alexa spoke not like a cloud-based, nonliving platform but like your deceased grandmother? Would you have an emotional connection to the AI platform if it spoke in the voice of someone you loved? Would you trust...it?

Prasad seems to think so. In his Re: MARS keynote, he commented on the companionship relationship people have with Alexa. “In this companionship role, human attributes of empathy and affect are key for building trust,” Prasad said. “These attributes have become even more important in these times of the ongoing pandemic when so many of us have lost someone we love. While AI can’t eliminate that pain of loss, it can definitely make their memories last.”²¹

There is something unsettling about turning Alexa into a deepfake voice-cloning badass, but that’s what Amazon intends to do with the prototype *Personal Voice Filter* unveiled at Re: MARS.²² According to Prasad, the experimental software enables Alexa *to simulate any human voice after hearing less than a minute of audio*.²³

To demonstrate the power of this experimental new feature, Prasad played a video of a boy saying, “Alexa, can Grandma finish reading me *The Wizard of Oz*?” Alexa says, “Okay,” with its robotic cloud-generated voice, then morphs into a sweet-sounding human voice and reads *The Wizard of Oz*, precisely mimicking the boy’s grandmother.²⁴

To Prasad, upgrading Alexa with the Personal Voice Filter enables “lasting personal relationships,” but it’s dangerous and creepy to others. While it may seem heartwarming to hear a bedtime story in your grandmother’s voice, turning Alexa into a voice cloning *Badass Alexa* raises a number of disturbing concerns.

For one, most banks and brokerages allow customers to use their voice as *biometric authentication* instead of the traditional password. Could someone use Badass Alexa to clone your voice, then fool the bank’s automated voice identification system into writing a fat check with lots of zeros?²⁵ Also, many companies have call centers that use biometric software to authenticate calls from customers to prevent fraud, like when criminals impersonate a customer to make a fraudulent transfer. Could a deepfake voice generated by Badass Alexa fool a call center’s biometric fraud software? The cybersecurity threat to voice biometric anti-fraud technologies posed by a future Badass Alexa is mind-boggling, to say the least. However, if Alexa’s Personal Voice Filter is ever rolled out—and if it’s as good at mimicking voices as Prasad’s demonstration portrays—then perhaps traditional plain-vanilla passwords with multifactor authentication will come back into style.

But apart from thwarting biometric authentication, what else could Badass Alexa do? How about being deployed by cybercriminals to mimic a CEO and then placing a call to Accounts

Payable to transfer funds for a time-sensitive acquisition? Or Badass Alexa could be used to mimic a teenager to swindle a parent. “Mom, it’s Melissa, I was in an accident, and I’m bleeding, and the police won’t take me to the hospital. They’re blaming me for a hit and run, and now I’m in jail! Get me out! Please, an attorney will call with instructions for wiring bail money. Please help!” A few minutes later, an attorney calls and the parent wires \$7,500 bail money, not realizing it was a deepfake voice vishing scam, and Melissa is safe and sound in her college dorm.²⁶

Of course, it’s not always about vishing scams and stealing money—deepfakes can also be used to commit heinous acts of macabre cruelty. For example, a subhuman derelict of a loser could wield Badass Alexa to clone the voice of someone’s deceased mother and then leave a nasty message: “You were a rotten son, a total loser, and a big disappointment!” Even if you knew it wasn’t real, it would be a bitter pill to swallow from your deepfake mom.

From bad to spine-chilling worse, Badass Alexa could call with a deepfake voice and threaten someone with violence. For example, Badass Alexa could mimic the voice of an ex-lover, ex-boss, or former friend to convey threats of bodily harm and bloodcurdling mayhem. “I’m coming over right now to kill you! Gonna cut your head off to the bone! You’re dead meat,” says Badass Alexa, mimicking the voice of an ex-boyfriend. Adding insult to injury, deepfake attacks harm two victims—the person being threatened as well as the ex-boyfriend whose voice was stolen.

Alexa, upgraded with deepfake technology, could also be used by political opponents to change the outcome of an election. For example, a nefarious candidate could use Badass Alexa to mimic a political opponent’s voice to conduct fake interviews with the media, casting the opponent in a negative light. Or Badass Alexa deepfakes could be used to make vast robocalls to constituents that misrepresent or outright lie about an opponent’s beliefs or political platform.

Who knows whether Amazon will actually follow through on fully deploying the Personal Voice Filter, but Alexa, empowered with voice-mimicking capabilities, would likely be the apex predator of deepfake voice cloning technology. In fact, the birth of Badass Alexa would be the democratization of voice cloning on steroids. Anyone, even those with little or no technical acumen, could wield Alexa as a nightmarish cyberweapon to bypass biometric voice authentication, conduct vishing attacks, make threatening calls, or launch political deepfakes. Let’s hope Badass Alexa remains a prototype that never sees the light of day.

Scams using Badass Alexa may fuel a cybercriminal’s hopes and dreams, but in the here and now, Alexa is a privacy nightmare. In a worrisome sign about the future of privacy, on March 28, 2025, Amazon removed a feature that allowed owners of Echo devices to “opt-out” of sending their voices to the company’s cloud.²⁷ The privacy option was available on the Echo Dot (4th Gen), Echo Show 10, and Echo Show 15, but only for users in the United States. Amazon developed these devices with the functionality to process the user’s voice on the Echo itself, a feature called *local processing*, so with the privacy option enabled, the user’s voice never went to Amazon’s cloud for processing.²⁸ In a mid-March email, Amazon notified Echo customers it was removing the privacy option, *Do Not Send Voice Recordings*, to enhance the voice recognition capabilities of its next-generation upgrade, *Alexa Plus*.²⁹

It seems odd that Amazon would backtrack on privacy after going to all the expense, let alone effort, to manufacture hundreds of millions of devices with local processing and a cloud opt-out feature. But truth be told, Echo devices, and the Alexa’s dwelling within, have proven to

be a financial disaster, with Amazon losing \$25 billion between 2017 and 2021.³⁰ Amazon's business model was to sell Echoes at a loss, hoping that customers would use Alexa to buy lots of stuff on Amazon's website. But it seems Jeff Bezos didn't think this plan through. You see, people buy an Echo to use a free version of Alexa for tasks like checking the weather and getting calendar reminders, and although Alexa loves helping its customers shop on Amazon, people do not purchase enough merchandise to make the Echo/Alexa ecosystem profitable. Amazon's dream that Alexa would be the gateway to other revenue streams like voice-activated shopping and premium subscription services didn't pan out.³¹

Amazon has a lot riding on privacy-disabled Alexa Plus, as old-school privacy-enabled Alexa is a cash-burning money pit. Sure, Alexa resides in hundreds of millions of devices worldwide, but hoovering up revenue, it ain't! Alexa's popularity has not translated into geysers of cash, so Amazon is desperately keen for Alexa Plus to get the revenue stream flowing as a subscription-based service.

Of course, no one will shell out \$19.99 monthly for a disembodied voice that gives you weather reports, so Alexa Plus comes loaded with premium features. One neat feature is *context-aware* smart-home control, meaning Alexa Plus can change your home settings based on conditions it detects. For example, if it's snowing outside in December, Alexa Plus fires up the gas logs and plays "Jingle Bells," or if you're coming home past your bedtime, Alexa Plus calms your frazzled nerves by dimming the lights and lowering the temperature to a sleep-inducing sixty-seven degrees Fahrenheit. But wait, there's more! Alexa Plus knows you so well, it can complete tasks without you asking, yuck it up like an honest-to-gosh human, and because it can shop like a champ, it's free to all Prime members!³²

But here's the thing: Mighty though Alexa Plus be, it cannot do any of these amazing tasks unless Amazon sends your frigging voice to the cloud. You see, with old-school privacy-enabled Alexa, the user's voice is stored *locally* on the Echo device itself—which is fine for asking Alexa to give you a weather report—but the Echo does not have the sheer computational power needed to handle context-aware routines or personalized tasks requiring real-time analysis of Brobdingnagian datasets. These premium features require generative AI processing, and the only way Alexa Plus can perform generative AI processing is with a boatload of computational power, the likes of which can only be provided by Amazon's cloud.

As a result, Alexa Plus desperately needs your voice! It also requires the voices of the hundreds of millions of its users. Accurate *voice recognition* is essential to identify each user so Alexa Plus can provide a custom, personalized response. Its generative AI models must be fed millions of voices, so Alexa Plus can learn humanlike conversational skills and develop context-aware capabilities. Alexa Plus needs the voices of all its users so it can learn, grow, and—God help us—evolve.

This is where we come to the crux of Amazon's predicament. The next-generation business model of Alexa Plus is predicated upon its services being so valuable they are worth a monthly subscription fee, but this is where Amazon is caught between Alexa and the deep blue sea. Those services require voice recognition and gobs of computational power. Somehow, Amazon has got to get its users' voices into the cloud, and the way Amazon chose to do this was to give privacy a swift kick to the curb.

Since March 28, 2025, users who had selected the now-defunct *Do Not Send Voice Recordings* feature are automatically switched to a new option, *Do Not Save Recordings*, which

still sends the user's voice to the cloud but purports to delete the voice recording after Alexa Plus has processed the request. This means your voice goes to Amazon's cloud whether you like it or not. What about customers who ask Alexa to check the weather? Well, their voice is going into Amazon's cloud. Okay, what if the customer asks Alexa for a news report, a stock update, or a funny joke? Well, the customer's voice is going into Amazon's cloud. What about customers who want to use Alexa Plus but forgo the premium features? Same exact thing—Voice. Sent. To. Cloud.

So what good is a privacy feature that basically tells Echo users to go pound sand, I'm sending your voice to the cloud anyway? The answer is that although your voice recording is still sent to the cloud, Amazon promises to delete it after processing is completed. In other words, once Alexa Plus uses your voice to complete the task—poof!—your voice is magically deleted from Amazon's cloud.

This, in my opinion, is not privacy. It's a pwn.

"Hold on," you say with a dirty look, "Amazon is deleting the voice recording," and then you say, sounding like Heath Ledger's Joker, "Why so cynical?"

Sadly, what's cynical is Amazon offering a fake privacy option in the first place. To help you understand Amazon's privacy pwn, let's back up and see what happens if customers turn off the Do Not Save Recordings option. When the feature is disabled, their voice goes into the cloud but is not deleted after processing, which means millions of customers' voices are processed in perpetuity for, well, whatever the hell Amazon wants. Now, you might suppose someone would disable the privacy feature because they trust Amazon and don't care if their voice goes to the cloud and is not deleted.

But you'd be wrong, as there is another reason why even a privacy-aware user would disable the Do Not Save Recordings option. In the ultimate bait and switch, Amazon built into the product a loss of functionality when the privacy option is turned on.³³ When customers select Do Not Save Recordings, then Alexa Voice ID doesn't work, and customers can't use Alexa for personalized tasks like tailored calendar reminders or curated music playlists. Whether you call this leverage or blackmail, the bottom line is that Amazon is forcing its customers to choose between privacy and having a functional Alexa Plus inside a workable Echo device. Amazon is essentially holding a fake privacy option to its users' heads: Either choose to send your voice into the cloud for Amazon's endless research, or that fine-looking Echo will be little more than an expensive paperweight!

But there's still more to Echo than meets the ear. When you activate Alexa with its eponymous "wake word," Echo starts listening and sends your voice commands into the cloud.³⁴ While listening for your command, sometimes Echo can get confused and accidentally pick up something it shouldn't, like an intimate conversation with your spouse. There's also the issue of trust—can you really be certain your voice is being deleted after processing? And even if you don't care, what's your comfort level with Amazon being able to process, experiment, or study your voice recordings forever?

Amazon retaining your voice in its cloud and effectively listening to your private conversations via all-ears Echo is just plain icky. It's also discomfoting that Amazon has a history of mishandling voice recordings. In 2019, thousands of Amazon employees and contractors around the world listened to as many as 1,000 voice recordings per nine-hour shift—ostensibly to research ways to improve Alexa's voice recognition processing—but in doing so,

they overheard private moments.³⁵ Some voice recordings were comical, like a woman singing in the shower, but other recordings implicated criminal activity, like what the Amazon workers believed was sexual assault.³⁶ Creepy for sure, but Amazon upped the ick factor to the tune of \$25 million in civil penalties for retaining children’s voice recordings and geolocation data even after parents requested deletion.³⁷

These unnerving breaches of trust raise serious privacy concerns. Yet, as of March 28, 2025, Amazon has thrown the gauntlet at its customers by making them choose between privacy or Alexa. If you decide to buy an Echo and avail yourself of all the premium services Alexa has to offer, be aware that in return, data-horny Amazon gets to have its way with your voice recordings, forever.

This is the infuriating corner that Amazon has backed its customers into. But don’t be fooled; privacy versus functionality is an Amazon-manufactured dilemma. There’s a simpler, better solution than Amazon’s fake privacy option—toss your Echo in the trash.

Val Kilmer Lost His Voice to Throat Cancer. Deepfake Tech Gave It Back.

Val Kilmer, who passed away in 2025, was known for critically acclaimed roles in *Top Gun*, *The Doors*, and *Heat*. In 2017, he also became known as a cancer survivor. Diagnosed with throat cancer, Kilmer endured chemotherapy treatments and a tracheotomy, in which a hole is surgically made into the windpipe, and a plastic tube is then placed into the hole for breathing. People who’ve had a tracheotomy can no longer speak normally, as the air flowing through the tracheotomy tube goes directly into the lungs, bypassing the vocal cords, nose, and mouth. Like others who’ve had a tracheotomy, Kilmer’s voice was permanently damaged. He could only speak by using a finger to cover the hole in his throat, forcing air through his windpipe.³⁸

With his acting career effectively over, Kilmer engaged a UK-based voice cloning firm, *Sonantic*, to create a computer-generated version of his voice. To recreate a person’s voice, Sonantic’s clients read from a script, and the audio is then analyzed by Sonantic’s proprietary software, *Voice Engine*. But with Kilmer’s voice irreparably damaged, he couldn’t speak the lines from Sonantic’s scripts.

John Flynn, Sonantic’s CTO, and cofounder, explained how they solved this problem in a 2021 blog posting:

Our first hurdle with creating the voice model for Val was that his team provided a relatively small amount of recorded material, which we knew would make it more difficult to produce the model. We first cleaned the audio, carefully removing background noise without destroying the speech content. Next, we generated transcripts from the audio and paired the audio and text together in short chunks. The Voice Engine then began training the model with the resulting data—about 10 times less data than we might have used in a typical project.

With that limited amount of data, the algorithms we had been employing in our Voice Engine did not deliver the results we needed. We decided to research and implement new algorithms that could produce higher-quality options from the data we had

available. In the end, we generated more than 40 different voice models and selected the best, highest-quality, most expressive one. Those new algorithms are now embedded into our Voice Engine, so future clients can automatically take advantage of them as well.³⁹

Sonantic is understandably tight-lipped about the crazy magic within its proprietary deepfake technology. Still, the final product is a text-to-speech *custom voice model* faithfully simulating Val Kilmer's cancer-ravaged voice on demand. "I spent nine years helping children with autism learn how to use their voice as a better instrument for communication," Zeena Qureshi, CEO and cofounder of Sonantic, said in the 2021 blog post. "The project with Val demonstrated again how empowering it can be when people overcome challenges with speaking."⁴⁰

Val Kilmer's AI-generated voice was unveiled to the world in a 2021 YouTube video, and the results were nothing short of astounding. "My voice as I knew it was taken away from me," Deepfake Kilmer says. "People around me struggle to understand me when I'm talking. But despite all that, I still feel I'm the exact same person. Still the same creative soul. A soul that dreams ideas and stories constantly. But now I can express myself again. I can bring these dreams to you and show you this part of myself once more. A part that was never truly gone. Just hiding away."⁴¹

In the 1986 *Top Gun* movie, Val Kilmer played ace fighter pilot Tom "Iceman" Kazansky, archrival and frenemy to the film's protagonist, Maverick, as portrayed by actor Tom Cruise. Thirty-six years later, assisted by his AI-generated voice, Kilmer would reprise his iconic role in the 2020 blockbuster sequel, *Top Gun: Maverick*.

Kilmer was delighted with his AI-generated voice and, in a statement posted on Sonantic's blog, said, "I'm grateful to the entire team at Sonantic who masterfully restored my voice in a way I've never imagined possible. As human beings, the ability to communicate is the core of our existence and the effects from throat cancer have made it difficult for others to understand me. The chance to tell my story, in a voice that feels authentic and familiar, is an incredibly special gift."⁴²

Sonantic's deepfake technology restored Val Kilmer's voice, resurrected his acting career, and gave hope to throat cancer survivors seeking a way to communicate in their natural voice with friends and family. Losing one's voice to throat cancer is widely reported in the media, especially when it happens to someone famous, but there are several less well-known medical problems that can result in *voice disorders*.⁴³

- **Laryngopharyngeal reflux disease:** Stomach acids bubbling up into your throat can lead to hoarseness, pain, the weird sensation of a lump in the throat, and problems swallowing. Basically, this is acid reflux run amok, and it can wreak havoc on a person's voice.
- **Spasmodic dysphonia:** This sounds as bad as it is—your vocal cords spaz out because of a problem in the brain's basal ganglia, so your voice is all over the map.
- **Laryngitis:** A bad cold or flu from a viral infection can cause vocal cords to swell, resulting in hoarseness or even the complete loss of a person's voice. Since a virus is the bad guy, antibiotics are ineffective, and the only cure is time—and maybe your momma's

chicken soup.

- **Vocal cord paresis:** Your vocal cords can become paralyzed by nerve damage from a viral infection, a tumor, or even after a surgical procedure. When one or both vocal cords are paralyzed, the end result is loud breathing with a feeble, wheezy voice.

The human voice is a fragile biological mechanism, and it doesn't take much to knock it out of whack. When someone loses their voice, it devastates both their livelihood and personal relationships. Consider the high school teacher with spasmodic dysphonia, whose voice is being strangled by invisible hands and is unable to teach a class; or the salesperson with vocal cord paresis—and a wispy, breathy voice—who fails to close the deal of the century; or an aspiring voice-over actor, who loses a coveted radio spot due to laryngitis-induced hoarseness.

For people suffering from voice disorders, deepfake voice cloning is potentially life-changing technology—keeping them in the game, reviving their occupations, and restoring deep emotional connections—all with the soft pitter-patter of a keyboard. Think how useful deepfake technology could be for a wispy-sounding salesperson. There would be no reason to cancel an all-important closing meeting when that once-euphonious voice—a silver tongue that sold a million belly-busters to a sushi chain—comes alive courtesy of text-to-speech cloning technology. With deepfake technology, the squeaky-talking high school teacher could type a lesson to be spoken by an AI-generated voice while remaining on hand in the classroom to answer questions on the fly. With just a few taps on the keyboard, the teacher's old, natural voice comes back to life. And what about the voice-over artist with the leaky baritone pipes? Well, that melodious radio voice is back on air thanks to the computing power of deepfake technology.

When deepfake tech becomes ready enough for primetime that it can deliver on clinical applications, throat cancer survivors could record their voice far in advance of a tracheotomy. This way, the voice-cloning software will have enough recorded material to recreate the person's natural voice. And when a person doesn't have enough recorded material of their voice—because some folks eschew Facebook, YouTube, and other social media platforms—deepfake tech could create a brand-new AI-generated voice belonging only to that particular person. By giving a distinctive AI-generated voice to one customer at a time, every customer can have their own unique identifier, like a fingerprint. Even if the AI-generated voice did not sound like your original, natural voice, you'd still have an AI-generated voice that's yours and yours alone. Voice-cloning technology still has a ways to go before it lives up to the promise of being a transformative communication tool for people with voice problems. But have no doubt, deepfake tech is just over the horizon, and AI-generated voices will one day be as commonplace as movie-magic computer-generated imagery (CGI).

The inability to communicate is scary, isolating, and often leads to broken relationships and loss of employment. Humans are social creatures, and losing one's voice is tantamount to losing one's soul. Deepfake voice cloning has the chops to become a pivotal treatment option, helping throat cancer survivors and others with voice-killing medical conditions break through the cycle of job loss—and loneliness—following in the wake of a voice disorder.

Deepfake voice tech may also be on the verge of creating new ways for film and radio entertainers to earn passive income.⁴⁴ Voice-over actors can clone their voice and use it to perform multiple jobs at once, so they will never be overbooked. An AI-generated voice is also helpful when an actor is not available to complete a project because of a stuffy nose, or their

voice mercifully needs a rest from overuse—a hazard for actors starring in scream-at-the-top-of-your-lungs horror movies.

Or an actor with a thick Southern drawl can have the accent removed so the AI-generated voice can be used in far-flung geographic locations where the population identifies with a different accent, such as Indian, Chinese, or British. In fact, an actor's AI-generated voice could be spoken in an entirely different language; the words could be spoken in French or Spanish, but the tone, timbre, pitch, and other vocal aspects would entirely be the actor's. Imagine a scene in the original 1986 *Top Gun* movie with Iceman and Maverick's AI-generated voices speaking in Chinese—and no overdubbing required! When Val Kilmer's simulated voice says in Chinese, "Maverick is a smelly old butthead," it's actually Val Kilmer's voice and not a Chinese voiceover artist dubbing the part. (The scary part is, this is already achievable using an open-source voice synthesis model named IndexTTS2!)⁴⁵

This brings us to a bit of a problem. On the flip side, could deepfake voice cloning cost actors their jobs? Certainly, there will be less work for overdubbing artists! Worse, film studios could create their own copyrighted AI-generated voices, thus cutting down on the need for human talent.

Another concern would be using an AI-generated voice to run radio spots for causes the voice-over actor doesn't believe in. Pro-choice actors would be tub-thumping livid to hear their AI-generated voice being used in a political commercial promoting an abortion ban, or gun control advocates would be itching to shoot the lights out if their AI-generated voices were used in fundraising commercials for the National Rifle Association (NRA). But, of course, the same could be said the other way around. Conservative entertainers would burst a blood vessel if their simulated voice were used in a campaign ad for US Representative Alexandria Ocasio-Cortez.

Deepfake voice cloning is like Harvey Dent—the right side of his face is handsome, while the left side has been scarred by acid. In Harvey's case, when he flips his double-headed silver dollar and it comes up mint-condition heads, he does good things; but if the coin flips up with the scratched-out heads, get ready to turn on the Bat Signal because some nasty crime is going down. With deepfake voice cloning, it's not the flip of a coin that determines its fate, as the technology itself is neither good nor evil. How a human chooses to wield voice-cloning technology determines whether a deepfake will be used to give Val Kilmer his voice back or steal \$35 million from a bank.

But there's a far more nettlesome problem than using deepfake voice cloning for purely good or evil purposes. It's axiomatic that some people will use deepfake tech for good applications, like helping throat cancer survivors communicate, while others will use it for evil, like tricking a victim out of their paycheck. But some applications of voice cloning are not so black and white. They fall somewhere in the middle, like a shade of not-so-agreeable gray.

Roadrunner is a documentary film by Oscar-winning director Morgan Neville about superstar chef and world traveler Anthony Bourdain, who died by suicide in 2018. In the movie, Neville uses deepfake tech to simulate Bourdain's voice to say words the TV personality never said when he was alive. When Neville told *The New Yorker* in a 2021 interview that three lines in the film were spoken by artificial intelligence—and not Bourdain himself—a firestorm of criticism exploded from outraged Bourdain fans and movie critics, accusing Neville of unethical conduct.

Neville curtly dismissed the controversy, telling *The New Yorker*, "We can have a

documentary-ethics panel about it later.”⁴⁶ And, with a persistent tin ear to the withering criticism, Neville further stoked the flames with a wan statement to *Variety*: “There were a few sentences that Tony wrote that he never spoke aloud. With the blessing of his estate and literary agent we used AI technology. It was a modern storytelling technique that I used in a few places where I thought it was important to make Tony’s words come alive.”⁴⁷

Neville had also told *GQ* magazine that he checked with Bourdain’s widow and literary executor, “And they were like, Tony would have been cool with that.”⁴⁸ However, Neville was contradicted by Bourdain’s wife, Ottavia, who shot back in a tweet, “I certainly was NOT the one who said Tony would have been cool with that.”⁴⁹

It doesn’t take a genius to see why Neville’s deployment of Deepfake Bourdain ticked everyone off. First, the use of voice-cloning software was not disclosed when the film was released, so Bourdain fans and movie critics alike felt manipulated when they found out some of the scenes in the film were spoken by Deepfake Bourdain.⁵⁰ Second, the tweet from Bourdain’s wife contradicts the assertion that consent to use Deepfake Bourdain was actually obtained. Finally, Neville was dismissive about the ethical concerns raised by moviegoers and film critics, which at the very least, is not good optics when you’re trying to get favorable media coverage and butts in seats.

Bottom line: Neville’s decision to use Deepfake Bourdain without transparency or consent wasn’t just an oopsie—it was an ethical lapse. The withering backlash from fans wasn’t just about ethics; it was about respect. And in a GAN-powered realm where deepfake voices sound real, and digital resurrection is just another episode of *Black Mirror*, that respect is the line that shouldn’t be crossed.

Deepfake Videos, Cognitive Bias, and the Chico Mark Factor

As the hiring manager, if you conducted a Zoom interview with a promising candidate who had the face of Val Kilmer but the body of a monkey wearing a clown outfit, you’d know something was up. But if the candidate looked like an average Joe and was polite, polished, and dressed to the nines, you might not realize you’re about to be pwned by an AI-generated deepfake.

Deepfake job interviews are becoming so commonplace that the FBI Internet Crime Complaint Center (IC3) issued an advisory about the use of deepfake videos to apply for work-from-home (WFH) positions.⁵¹ The scam works like this: Cybercriminals steal someone’s *Personally Identifiable Information* (PII), which they use in tandem with a deepfake video to masquerade as a highly qualified and experienced job applicant. Topping the list of cybercriminal dream jobs are high-tech positions bestowing an all-access pass to a company’s proprietary data, which would be easy pickings for a deepfake database administrator or a deepfake IT manager. Even worse, think of all the mayhem a deepfake software engineer could wreak by injecting ransomware into a company’s network.

Deepfake video interviews are a serious risk for companies. Fortunately, some employers caught on and reported the scam to IC3 because the deepfake video, well, pretty much sucked. “In these interviews, the actions and lip movement of the person seen interviewed on-camera do not completely coordinate with the audio of the person speaking,” the advisory deadpanned. “At

times, actions such as coughing, sneezing, or other auditory actions are not aligned with what is presented visually.”⁵²

Don’t expect such shoddy production values from nation-state threat actors. In 2022, the US State Department, Treasury, and the FBI issued a joint advisory warning companies that thousands of North Korean IT workers were applying for remote jobs by impersonating IT workers from South Korea, China, Japan, Eastern Europe, and the United States.⁵³ These North Korean IT workers do whatever it takes to get on a company’s payroll—including laughably amateurish forgeries, like using Photoshop to embed a North Korean IT worker’s headshot onto a fake driver’s license, passport, or other document required for employment. The North Korean IT workers also use aliases, VPNs, and third-country IP addresses to hide their actual location; the employer thinks they reside in a friendly country when in truth, they’re working from a remote location in North Korea, China, or Russia.

Of course, the North Koreans are not interested in scamming their way into dreary, low-paying construction jobs; instead, North Korean cybercriminals look for high-tech, freelance contract positions that companies have a hard time filling. “DPRK IT workers can individually earn more than USD 300,000 a year in some cases, and teams of IT workers can collectively earn more than USD 3 million annually,” the alert said. “DPRK IT workers provide a critical stream of revenue that helps fund the DPRK regime’s highest economic and security priorities, such as its weapons development program.”⁵⁴

That’s right folks—as thousands of North Korean IT workers scam their way into high-paying jobs, the North Korean government takes their salaries to fund weapons of mass destruction (WMD) and avoid the consequences of US and UN sanctions. Adding to the madness, deepfake North Korean IT workers have access to company data, which can be plundered and sold to support the North Korean regime or used for espionage purposes. Perhaps most alarming, these high-demand IT positions would allow embedded North Korean IT workers to inject malware into a company network and launch a devastating ransomware cyberattack.

Deepfake images seem like science fiction, so it’s mind-boggling that deepfake technology has been around for years. As early as 2018, researchers at GPU manufacturer NVIDIA created fake photos using a generative adversarial network (GAN). Just like GAN is used to manufacture deepfake voices, it can also be used to create deepfake images—but in a significant innovation, the NVIDIA researchers sprinkled a *style-based generator* into their GAN concoction to produce unbelievably realistic photos of human faces.⁵⁵ The GAN can learn human “styles” such as freckles, skin pores, eye color, and even the “finer curls of hair” to create convincing fake images that look like real people—right down to their zits and beard stubble.

Deepfake videos are also coming of age. Chris Ume, a Belgian video effects specialist and famous TikToker, is renowned for his fake videos of Tom Cruise. His *deeptomcruise TikTok page* features a fake Tom Cruise performing magic tricks, getting ready for a date with Paris Hilton, chewing on a bubble gum lollipop, and my personal favorite, a hilarious impression of a snapping turtle, complete with mussed-up hair and the charming-but-maniacal Tom Cruise laugh.⁵⁶

In 2018, director Jordan Peele posted a fake Barack Obama on YouTube warning about the dangers of deepfake technology. “We’re entering an era in which our enemies can make it look like anyone is saying anything at any point in time,” Deepfake Obama said. “This is a dangerous time. Moving forward, we need to be more vigilant with what we trust from the internet. It’s a

time when we need to rely on trusted news sources. It may sound basic, but how we move forward, in the age of information, is gonna be the difference between whether we survive, or whether we become some kind of fucked up dystopia.”⁵⁷

Of course, the real Barack Obama would never blurt out an expletive in a public video, nor would he say, “President Trump is a total and complete dipshit.” However, Jordan Peele’s Deepfake Obama certainly did throw shade at Donald Trump, which raises a nettlesome problem: Deepfake videos are becoming so real, it’s hard to separate truth from fiction.

They say a picture is worth a thousand words. If that’s true, then a video would be exponentially more valuable than either a photo or the spoken word—and a deepfake video weaponized by cybercriminals would be immeasurably more fearsome than a fake photo or cloned voice. Audio and video deepfakes alter reality because the technology can make it look like people are doing and saying things they never did or said. But video deepfakes are most pernicious because seeing and hearing a deepfaked human being is more effective at exploiting our preexisting biases than mere Photoshop fakery or a cloned voice.

Yes, Cognitive Bias Is a Thing

Humans are squishy, carbon-based life-forms whose brains are seething with *cognitive bias*.⁵⁸ Chief among our cognitive biases is *confirmation bias*, which simply means we humans are likely to believe something is true if it jibes with something we already believe.⁵⁹ On the flip side, we tend to brush off facts that challenge our beliefs. When two people are in a heated disagreement about politics and one of them refuses to listen to the other’s arguments—well, you’ve got yourself a classic example of confirmation bias. Another example of confirmation bias is when you only watch news programs that share your viewpoints, like Fox News if you are conservative or MS NOW if you identify as progressive.

Humans are also anxious about the randomness of life and are prone to *hindsight bias*, meaning we think we predicted an outcome before it occurred.⁶⁰ Examples include buying a stock that goes up and believing you knew it would be a ten bagger all the time, or a football team wins by a whisker, and you tell your friend, “I knew they were going to win all along!”

We squishy humans also love stereotypes, which is why George Reeves never found success beyond his iconic portrayal of the 1950s Man of Steel—or why ads promoting a famous 1960s superspy declared Sean Connery “is” James Bond instead of “starring as.” Come to think of it, Sarah Michelle Gellar will always be the real Buffy—and *BtVS* fans ain’t interested in no reboot! We squishy humans are predisposed to cookie-cutter assumptions, like the *halo effect*, a stereotyping bias in how we perceive other people.⁶¹ For example, thinking a smoking-hot salesperson is better at hawking used cars than someone who is not as good-looking, or that a person who resembles Santa Claus is more trustworthy than someone who’s the spitting image of Hannibal Lecter.

Deepfake technology is like a mind-altering drug that leverages our innate cognitive biases to make us believe in a false reality. Deepfake videos, because they can be both heard and seen, are a substantially greater threat than deepfake voice cloning. Seeing is believing, and deepfake videos are becoming so realistic that it’s hard for humans to override their innate cognitive bias.

The movie *Duck Soup* contains a famous line spoken by Chico Marx and later used in a

vaudeville skit in which a man's wife catches him in the arms of another woman. The man denies having an affair even though the other woman is half naked and clinging to him. When the man's wife points out that she can see the other woman, he retorts, "Who you gonna believe, me or your lying eyes?"⁶²

Unlike the wife in this bawdy joke, there are millions of people who'll believe a deepfake video to be true. It's like every human on the planet has an inner Chico Marx, whispering, "Who you gonna believe, me or your lying eyes?"

I call this the *Chico Marx Factor*, and it's why deepfake videos are so insidiously pernicious. In fact, deepfake videos are so dangerous they could start a war—maybe even a nuclear war. On February 24, 2022, Russian President Vladimir Putin launched a disastrous war of choice by invading democratic Ukraine. As the invasion progressed, military experts believed Russia's vastly superior army would overrun Ukraine in days, forcing Ukrainian President Volodymyr Zelenskyy and his government into exile and turning Ukraine into a vassal state of the Russian empire.

The thing is, it didn't work out that way. Russia's invasion faltered as Ukrainian forces mounted a fierce resistance and counteroffensive, inflicting massive losses and reclaiming thousands of square miles of occupied territory.⁶³

In the wake of Russia's hellacious losses, Putin addressed his nation, announcing the mobilization of 300,000 reservists in a desperate attempt to shore up his failing "Special Military Operation."⁶⁴ Panicked and running out of military options, Putin attempted to galvanize the Russian people in a speech bursting with falsehoods. "Washington, London, and Brussels are openly encouraging Kyiv to move the hostilities to our territory. They have even resorted to the nuclear blackmail," Putin lied in his speech. "I would like to remind those who make such statements regarding Russia that our country has different types of weapons as well, and some of them are more modern than the weapons NATO countries have. In the event of a threat to the territorial integrity of our country and to defend Russia and our people, we will certainly make use of all weapon systems available to us. This is not a bluff."⁶⁵

Losing the war in Ukraine, a flustered seventy-year-old autocrat threatens the world with a nuclear strike. Putin is evil, there is no doubt about that, but threatening to nuke Ukraine is not the same as actually nuking Ukraine. However, in the hands of a cyberterrorist, think of the damage a Deepfake Putin could do. Let's imagine a different speech to the Russian people, as delivered by Deepfake Vladimir Putin....

"This morning, NATO forces invaded Crimea, which is Russian territory, killing 1,200 brave Russian soldiers and countless innocent Russian citizens," Deepfake Putin said in a video address to the Russian people. "NATO is bragging openly now that in 1991 they managed to split up the Soviet Union, and now is the time to do the same to Russia." Deepfake Putin's face was pale but resolute, his steely eyes glinting with moistness as if holding back tears. "We cannot, we have no moral right to let our kin and kith be torn to pieces by butchers. We cannot but respond to their sincere striving to decide their destiny on their own."

Deepfake Putin drew a long breath through pursed lips and pressed his back deep into a faithfully restored eighteenth century Streshnev coat-of-arms chair. He cocked his head slightly as if deep in contemplation, then burst forward, pounding clenched fists on a massive sixteen-foot white marble table. "We must defend our Motherland! Those who threaten our independence and freedom must be defeated! We will not cower before those who are keen on

global domination and threaten to split up and enslave our Motherland,” Deepfake Putin said. His nasal voice was soft yet piercing, and his lips trembled as his pallid, thin face became flushed, like coming off a long-distance run. “In this dire situation, I had no choice but to order a nuclear strike at the heart of NATO, that is the decadent cities of Washington, London, and Brussels. Thank you, my fellow comrades—I believe in your support in this dark hour of history.”

What would Western leaders do if they thought Deepfake Putin was real—and that he actually ordered a nuclear strike on Washington, London, and Brussels? Would the US president launch a counter-strike? Even if caution prevailed—because NATO had espionage assets in Russia informing that no missiles had been launched—the world would be thrown into chaos and madness. Stock exchanges would plummet as people sold risk assets to get their hands on safe, comforting cash. Billions of dollars would be lost in an instant, armies around the world would be on high alert, and the tinderbox Russia-Ukraine War could become the gateway to World War III.

In the wrong hands, deepfake video technology is a superweapon exploiting the human frailty of cognitive bias with misinformation and outright lies to sow chaos and conflict. Chillingly, the world is filled with cybercriminals, cyberterrorists, and nation-state threat actors itching to deploy this weapon against their perceived enemies. A cyberterrorist organization would be thrilled to see the “Great Satan” United States wiped out in a deepfake-inspired nuclear exchange. Or an adversary of the United States might be eager to take some geopolitical advantage (invade Taiwan, perhaps?) while the world’s greatest superpower is on the back foot—or worse, embroiled in a nasty military conflict.

Deepfake video technology is a superweapon that, in the wrong hands, could wreak bloody havoc if world leaders are not savvy enough to realize they’re being pwned. In fact, deepfake video could be the match that ignites a revolution, military conflict, or worse—World War III.

The Pernicious Threat of the Liar’s Dividend

George Floyd, a black man, died on May 25, 2020, while under arrest for purchasing cigarettes from a Minneapolis convenience store using a counterfeit twenty-dollar bill. A father of five, Mr. Floyd was handcuffed and pinned to hard asphalt by Derek Chauvin, a white police officer, who knelt on Mr. Floyd’s neck for over nine minutes.

Mr. Floyd’s death was brutal. Transcripts from police bodycam video shows Mr. Floyd pleading, “I can’t breathe,” more than twenty times while handcuffed with a knee on his neck. When Mr. Floyd says, “You’re going to kill me, man,” Officer Chauvin retorts, “Then stop talking, stop yelling. It takes a heck of a lot of oxygen to talk.”⁶⁶

Gasping for breath, Mr. Floyd begged for his mother: “Can’t believe this, man. Mom, love you. Love you. Tell my kids I love them. I’m dead.”⁶⁷ Mr. Floyd went limp, and an ambulance was called, but it was too late—he was gone.

The county medical examiner ruled the death a homicide, determining Mr. Floyd died of a heart attack caused by “subdual, restraint, and neck compression”—in layman’s terms, excessive use of force by the police officers. The medical examiner noted that underlying heart disease and recent drug use were contributing factors to Mr. Floyd’s death. However, physician experts for

Mr. Floyd's family testified in court that Mr. Floyd died from asphyxia. Pinioned by Officer Chauvin's knee on his neck for over nine minutes, Mr. Floyd's airway was blocked, so he couldn't breathe, causing his heart and lungs to shut down from lack of oxygen to the brain.⁶⁸

Mr. Floyd died a senseless, violent death, and shock and grief erupted across the nation, with "I can't breathe" becoming the clarion call for Black Lives Matter and other groups protesting police brutality. Mr. Floyd's family filed a wrongful death lawsuit against the City of Minneapolis, settling for \$27 million.⁶⁹ Former police officer Derek Chauvin was sentenced to twenty-two years in prison after being convicted on two counts of murder and one count of manslaughter. Three other former police officers involved in Mr. Floyd's fatal arrest—Thomas Lane, J. Alexander Kueng, and Tou Thao—were convicted of violating Mr. Floyd's civil rights and sentenced to serve three-year prison terms.⁷⁰

This travesty really happened. George Floyd died painfully, in mental anguish, knowing he was going to die, begging for his very life and pleading for his mother until the final last moments before his heart and lungs gave out. We know this because Mr. Floyd's gruesome death was recorded by police bodycams, bystander videos, and two autopsies, one by the county medical examiner and another at the behest of Mr. Floyd's family.

It's all documented—the heartbreaking last words of Mr. Floyd, the callous actions of Derek Chauvin and his fellow police officers, every agonizing gasp squeezed in by Mr. Floyd, every drop of sweat and blood on that tragic, senseless day—it's all real, and there's video footage and two autopsies to prove it.

Yet, only nine days after Mr. Floyd's death, a Republican congressional candidate in Missouri, Dr. Winnie Heartstrong, declared Mr. Floyd's death was faked. Heartstrong made this deranged claim in a rambling diatribe posted to YouTube on June 3, 2020, titled "Dr Winnie Heartstrong claims George Floyd IS ALIVE and the video is FAKED."

In her YouTube video, Heartstrong questions whether Mr. Floyd is an actual person, intimating he's a fake and his name was derived from a barbershop:

George Floyd supposedly is being choked to death and he's crying out for his mom. We haven't heard anything about the mom. We haven't seen a family photo. We haven't seen any evidence of them together as a cohesive unit. Floyd might be a fake name for all we know. What I know for sure is that there's a Floyd's in south Minneapolis that's a hotspot, a gathering place for African Americans in that city and it's a barbershop. So, if I was going to murder the psyche of a people, I would give him a Floyd name, John Floyd, George Floyd.⁷¹

Heartstrong adds to the lunacy, claiming the police officer who jammed his knee on Mr. Floyd's neck is, well, a doppelganger:

The person that has been booked now, the photo of this Chauvin officer, is not the same person in the video who is strangling him. There are cameras from around the world gathered right now in Minneapolis and there is no video evidence of this guy being arrested. So, we're supposed to believe that the person who is in jail right now is the person we've seen in the video?⁷²

Heartstrong continued to peddle her conspiracy theories, and in a June 15, 2020, tweet, called upon then-President Trump and Attorney General William Barr to investigate the death of Mr.

Floyd, saying, “The use of deepfake technology has serious implications for American civic and political life.”⁷³

Indeed, Heartstrong doubled down on Deepfake Floyd a few weeks later when she published a twenty-three-page monstrosity titled, “A Citizen’s Investigative Report on the Use of Deep Fake Technology.”⁷⁴ The report—more like a wingnut fable of paranoia—weaves a ludicrous tale asserting the real Mr. Floyd died years before the fatal arrest, and deepfake technology was used to paste his face onto the body of a former basketball player, all for the nefarious purpose of stoking racial tensions.⁷⁵ In the wingnut fable of paranoia (it’s just too generous to call it a report!), Heartstrong states, “We conclude that no one in the video is really one person but rather they are all digital composites of two or more real people to form completely new digital persons using deepfake technology.”⁷⁶

Hard to believe anyone, let alone a congressional candidate, would be hyping looney deepfake conspiracy theories so soon after George Floyd’s murder on May 25, 2020.⁷⁷ It is ironic—and metaphysically infuriating—these bogus conspiracy theories came from someone running for office in the *Show Me State*. Fortunately, Heartstrong’s tinfoil-hat assertions about Deepfake Floyd never caught on with the public, and better still, she was defeated in the Republican primary on August 4, 2020, for which we should all be grateful Missouri’s voters lived up to their state’s nickname.

In a genuine report—yes, an actual work of intellectual rigor—cybersecurity law professors Robert (Bobby) Chesney and Danielle Citron coined the term *liar’s dividend*, in which a scoundrel—or perhaps a garden-variety nincompoop—evades accountability by claiming the words and actions captured by audio or video is, in reality, a deepfake.⁷⁸ The case of Deepfake Floyd is perhaps the most infamous example of the liar’s dividend, coming little more than a week after George Floyd’s heinous murder and peddled by a congressional candidate holding a Ph.D. in political communication from the University of Maryland.⁷⁹

The liar’s dividend ascends from the depths of the perfect deepfake storm: As deepfake technology advances, deepfake audio and video will become more lifelike, and as the public becomes more educated about the threat of deepfakes, they’ll be more easily convinced that a real video is not the truth, but a clever deepfake. Worse, the human frailty of cognitive bias will make the liar’s dividend exponentially easier for a scoundrel (or nincompoop) to pull off.

Here is an imagined example of the liar’s dividend in action:

A celebrity physician has a syndicated talk show but still finds time to practice otolaryngology in-between book and movie deals. She’s particularly beloved in New York City, where she’s one-part national gadfly and one-part hometown-girl-makes-good. She’s more popular than CNN’s Sanjay Gupta; thus, fans and patients alike are stunned when the FBI arrests her in a sting operation that also nets a hospital CEO.

For decades, the CEO ran a bribery scheme paying kickbacks to physicians in return for patient referrals to the hospital. Keen on pumping up otolaryngology visits, he showered the celebrity physician with checks and cash totaling more than \$2,732,000 over a six-year period.

The celebrity physician vehemently denied the charges, and in an impassioned speech on YouTube that quickly went viral, she proclaimed her innocence of all charges,

blaming the prosecutors for a rush to judgment.

And then four videos came out. A bit grainy and rough around the edges, the footage showed the celebrity physician accepting paper bags stuffed with cash from the CEO. Worse, she's joking about all the business she will steer his way. "You want more patients," she said in one of the videos. "Then give me more money."

Two weeks later, the celebrity physician spends an entire hour on her syndicated talk show warning about the threat of deepfake videos. She hammers away at the four leaked videos month after month, claiming they were all deepfakes. She claims her face was superimposed on someone else's body, and her voice cloned. She also claims the hospital CEO—if that's really him in the video—was in cahoots with federal agents who have an axe to grind with her views on natural supplements.

In a two-hour documentary titled *Deepfake Swan Song*, she declares the four videos to be deepfakes using extraterrestrial technology, and offers a \$100,000 "deepfake smackdown" award, saying in a press release, "The videos are all deepfakes made with alien technology and I challenge anyone to prove me wrong!"

Two years later, the videos are entered into evidence by confident prosecutors in a widely reported, scandalous trial. The jurors are well-educated metropolitan professionals cognizant of deepfake technology. However, the four videos are so "fake looking," as later recounted by one of the jurors, that the jury unanimously finds the defendant not guilty on all counts.

Following the verdict, the celebrity physician addressed a throng of reporters on the courthouse steps. "The dangers of deepfake technology are all too real," she said. "You can't automatically believe everything you see anymore."

The CEO, however, was found guilty of bribery and is currently serving a four-year prison term.

The liar's dividend is conjured by what seems like dark magic—our innate cognitive biases, coupled with the knowledge that deepfakes are possible, enable a scoundrel to trick people into thinking something that is actually true is categorically false. Of course, the liar does not have to be a scoundrel; anyone with a worldview in peril might prefer the Chico Marx Factor, choosing not to believe their lying eyes rather than face the truth. Whatever the motivation, the liar's dividend is an emerging risk, especially as knowledge of deepfake technology becomes mainstream.

In their groundbreaking paper *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, Professors Chesney and Citron warn that while deepfakes wreak havoc by tricking people into believing fabricated events truly happened, "not all lies involve affirmative claims that something occurred (that never did): some of the most dangerous lies take the form of denials."

Now, there are two ways a liar can do this. First, liars could create their own deepfake video to refute the truthful, real video. For example, the celebrity physician in the story above could have made her own deepfake videos with the bribery edited out and peddled her fake videos to

refute the real videos. However, Chesney and Citron point out this is a hazardous strategy because the liar's deepfake could be revealed as a fraud, especially in newsworthy cases where media organizations can marshal the technical resources to review the deepfake frame by frame.⁸⁰

Indeed, the second way a liar can avoid accountability is the easiest: Simply claim the real video is a deepfake. As the public learns more about the threat of deepfakes, it becomes easier for liars to convince people to believe a real video is actually faked. This is maddening because cyber awareness is a valuable countermeasure to reducing the likelihood of fraud or a devastating cyberattack. But when it comes to deepfakes, cyber awareness is a double-edged sword, enabling a liar to achieve the greatest con of all—pulling off a Chico Marx so the public believes the liar instead of the truth in front of their own eyes.

This frustrating paradox is bleakly described by Chesney and Citron:

Ironically, liars aiming to dodge responsibility for their real words and actions will become more credible as the public becomes more educated about the threats posed by deep fakes. Imagine a situation in which an accusation is supported by genuine video or audio evidence. As the public becomes more aware of the idea that video and audio can be convincingly faked, some will try to escape accountability for their actions by denouncing authentic video and audio as deep fakes. Put simply: A skeptical public will be primed to doubt the authenticity of real audio and video evidence. This skepticism can be invoked just as well against authentic as against adulterated content.⁸¹

In their paper, Chesney and Citron offer a host of possible solutions to the threat of deepfake technology and the liar's dividend. Below is my snarky attempt to convey the law professors' detailed, well-written analysis of the options:

- **Bring on the deepfake detectors:** Technological solutions could be developed to debunk deepfake audio/video. The problem is current *deepfake detectors* are not foolproof at outing deepfakes and may never be good enough to mitigate the looming threats.
- **Sue the bastards:** People harmed by deepfakes could file civil lawsuits against creators of deepfake technology. However, it's not easy finding the creators of deepfakes, especially when they take pains to be anonymous or reside in a far-off country. Hence, *deepfake generators* are all too often judgment-proof. However, it might be worth considering legislation to make online platforms more accountable.
- **Lock them up:** Impose criminal penalties on deepfake perpetrators. However, criminal investigations are resource-intensive, and therefore many crimes will go unpunished. Also, it's clear as mud how current criminal laws apply to deepfakes. So, we have an accountability gap—civil lawsuits are not effective against judgment-proof deepfake generators, and it's not likely criminal liability will be the means to closing the gap.
- **I'm from the government—and I'm here to help:** Three US federal agencies could regulate deepfake technology: the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), and the Federal Election Commission (FEC).

However, each agency is too limited in terms of scope and authority to make much of a dent in regulating deepfake threats.

- **Blow them to smithereens:** The US can levy economic sanctions or take military and covert action against nation-state threat actors who weaponize deepfakes. Tick...Tick... Boom!
- **Private sector steps up:** Social media can self-police deepfake videos posted on their platforms; also, companies can sell privacy-themed products and services to customers to mitigate the harm of deepfakes.

Just for the record, Chesney and Citron do not use exclamation points in their paper, nor do they employ slang, epithets, side-splitting jokes, or hyperbole—that’s my bailiwick. The solutions to deepfake technology are immeasurably complex, touching upon human frailty, technology, law, and politics. I trust you’ll forgive my writer’s invocation of poetic license—liberally abused—to describe Chesney and Citron’s excellent research, a towering work of substance in the field of cybersecurity, resulting in a paper that should be mandatory reading in technology, law, and business curriculums.

But as to the liar’s dividend, what to do? I’m afraid there’s no magic bullet. Cognitive bias is just too ingrained to shake. That’s why conspiracy theories flourish like weeds in a world without pesticides. Even today, there are people who believe rogue CIA agents assassinated President John F. Kennedy in 1963 as payback for failing to depose Cuban dictator Fidel Castro in the botched Bay of Pigs invasion (when it was actually Lee Harvey Oswald, acting alone, who shot JFK).⁸² Many people also believe the 1969 moon landing was faked on a movie set located in Nevada’s Area 51 (even though footage of the moon landing was broadcast live to millions of people worldwide).⁸³ But the mother of all conspiracy theories is the one that’s harder to kill than a roach; millions of people worldwide believe in the *Flat Earth Theory*, postulating the earth is flat and bounded by a wall of ice (when in fact, the earth is round and orbits the sun).⁸⁴

These conspiracy theories are demonstrably and inarguably false. The CIA was not involved in JFK’s shooting, astronaut Buzz Aldrin really stepped foot on the moon in 1969, and the earth is a round blue dot circling the sun. Nonetheless, cognitive bias is a sticky thing making these false beliefs hard to shake, so if millions of Flat Earthers believe the earth is flat when it’s not, then I’m not sure there’s anything we can do about the liar’s dividend.

Which, well, is quite depressing.

But let’s end this chapter on a positive note, shall we? After all, there is one thing YOU can do to thwart no-good rascally liars and ensure the liar’s dividend never pays out: Stop listening to your inner Chico Marx.

1. **Accept the existence of actual evidence. Be suspicious of wild claims not supported by evidence.**

Although Dr. Winnie Heartstrong claimed the murder of George Floyd was a deepfake, there was a mountain of evidence to the contrary—multiple eyewitness testimony, police bodycam videos, bystander videos, and two independent autopsies confirmed Mr. Floyd’s harrowing, gruesome death. This evidence must be accepted and respected.

Likewise, the absence of evidence corroborating Dr. Heartstrong's conspiracy theories must be viewed with suspicion. There's no proof George Floyd's head was superimposed on an ex-basketball player's body, and no proof the person imprisoned for Mr. Floyd's murder—former police officer Chauvin—was a doppelganger. The absence of evidence is a red flag that these wild claims are false.

A healthy dose of skepticism is a must to avoid being pwned by a scoundrel using the liar's dividend.

2. Curb your inner Chico Marx and pay attention to cognitive bias.

You want to believe the liar and not your lying eyes, don't you? Me too. It's only natural to believe in things that support your beliefs and dismiss things that refute them.

The Chico Marx Factor makes both actual deepfakes and the liar's dividend intractable threats. No matter how unlikely a deepfake (think Vladimir Putin announcing a nuclear strike on NATO countries), millions will believe it's true and freak out (but let's hope cooler heads prevail in the White House). The same is true for the liar's dividend. No matter how outlandish the claim, some people will believe the liar and not "their own eyes" because they lack self-awareness of their own cognitive bias.

If you want to avoid getting pwned, you need to be self-aware and catch yourself when you want something to be true so badly that you believe wild claims, even in the absence of evidence. It's not intuitive, which is precisely why it's so hard, but you must kick your inner Chico Marx to the curb, be self-aware of your own internal biases, and from there, you can thwart the liar's dividend.

There is no magic bullet to defeat the liar's dividend. It's pretty seductive, and I'm afraid the only countermeasure is individual self-awareness and a healthy dose of skepticism. Will you be pwned by a no-good rotten scoundrel exploiting the liar's dividend? I hope not, but now that you've read this chapter, the choice is yours.

CHAPTER 12

Cybercriminals Want to Pwn You with Deepfakes. This Is How You Stop Them.

Deepfake detectors are not bomb-sniffing canines; they're tools designed to catch telltale flaws in deepfake videos too minuscule to be spotted by mere mortals. For example, deepfake video technology has been known to struggle with mimicking facial movements, so early deepfake detectors focused on identifying peculiarities, like a twisty mien in the corners of the mouth, blurriness around the hair and neck, an off-kilter juxtaposition of the eyes and nose, no or too little blinking, and variations in facial complexion.

The problem is that *deepfake creators* would catch on and generate better deepfakes correcting these flaws. For example, in 2018, researchers found deepfake doppelgangers didn't blink much—if at all—so deepfake detectors were designed to spot a deepfake by identifying atypical blinking.¹ But then, deepfake creators studied this research, quickly learning to modify their algorithms to make the AI clones blink naturally and voilà—the deepfake can no longer be detected!²

Keep in mind that deepfake technology pits two neural networks against each other—the generator creating the deepfake and the discriminator trying to spot the deepfake. Well, deepfake detection tools use the same GAN learning system, so it's no surprise that deepfake creators can input the blinking detection algorithm into their GAN learning system to create a deepfake that can no longer be detected.

We end up with an *arms race* where deepfake detectors learn how to spot a deepfake, which spurs deepfake creators to make a better deepfake that can't be detected.³ Worse, this tennis match can only go on so long before deepfakes are so good they always fool the deepfake detectors. In other words, GAN-inspired deepfake tools are a short-term solution. Eventually, AI-generated videos will be so true to life that it will be impossible to distinguish a deepfake from the real thing.

In the future, deepfake technology will reign supreme. But for now, some researchers claim to have concocted detectors with a super high accuracy rate for spotting deepfakes. Even so, it doesn't move the needle far enough. For example, let's say I have created the world's most powerful anti-deepfake algorithm to create a detection tool boasting a 99 percent accuracy in spotting deepfakes. A subscription to my deepfake detection tool, cleverly named *Frank's Deepfake Detector*, is purchased by Mark Zuckerberg to identify deepfake images posted to Facebook so they can be removed. On day one, Mr. Zuckerberg puts 200 million images in the

crosshairs of Frank's Deepfake Detector—et voilà! My patented deepfake detector identifies millions of deepfakes that are dutifully scrubbed by the Facebook staff! Mark is so excited about the results that he calls me (on a burner phone, of course) and says, "Frank, from now on, call me Zuck!"

But there is one glaring problem here. My deepfake detector is only 99 percent accurate, which means 1 percent is, um, not accurate. That's two million images that Frank's Deepfake Detector got wrong! Some errors were false positives, meaning Zuck removed authentic photos, thus pissing off Facebook users, and some errors were false negatives meaning a boatload of deepfake photos remain on Facebook to pwn unsuspecting users.

Even with a 99 percent accuracy rate, the internet is so freaking massive that even the most powerful anti-deepfake technology comes up short. This means gazillions of deepfakes will constantly be sloshing around the internet. Even worse, the threat will rise exponentially upon the advent of deepfake supremacy, when deepfakes become so lifelike that the deepfake detector's accuracy rate drops to zero.

The implications of deepfake supremacy are mind-boggling. Every photo, video, or syllable uttered could be a genuine article, or it could be a deepfake. How could anyone prove otherwise once deepfake detectors become dumber than a bag of hammers? It's a real conundrum, and perhaps no technology is more at risk of this imminent threat than voiceprint biometrics.

Is Voiceprint Biometrics Losing Its Hearing?

Passwords suck. That's why banks and brokerages are trying to pitch them in favor of voiceprint authentication. Customers are weary of strong passwords with an annoyingly long—and forgettable—mix of letters, numbers, and special characters. Moreover, the ubiquitous "secret question" required before the bank will help the customer reset a forgotten password is eminently hackable by cybercriminals; all they need do is trawl social media sites for maiden names, birthdays, pets, and so forth to crack the not-so-secret question.

And don't even think of going down the multifactor authentication rabbit hole. MFA (as it's obviously acronymed) is a pain in the butt for tech-averse customers who'll refuse to download an app like Google Authenticator to receive a one-time numeric code. Nope—these technophobic customers don't want to access their online bank account with a strong password backed up by a second layer of authentication. They'd rather choose convenience over cybersecurity and shop around for a bank that doesn't hassle its customers with silly things like Hulk-strong passwords and incomprehensible MFA apps. Of course, these cyber un-savvy customers are ripe for the picking by hungry cybercriminals—and so are their life savings.

Banks are turning to voiceprint biometrics to increase both cybersecurity and user convenience by allowing their customer's voice to be their password. Here's how it works: The customer calls the bank, and biometric software takes a digital snapshot of the customer's voice. This digital snapshot is a binary template called a *voiceprint* and consists of more than one hundred physiological components, such as the size and shape of the vocal tract; the pitch, rhythm, and timbre of the voice; as well as individual characteristics like as a person's accent.⁴ The voiceprint is stored in a secure database and used to authenticate the customer when calling to trade a stock, pay a bill, or make a deposit.

The voiceprint is as unique as a fingerprint biometric but a lot more secure. For example, it's a piece of cake for cybercriminals to get approved for a bank loan when they can apply online and authenticate as someone else with a stolen fingerprint. But cybercriminals can't go on a crime spree with stolen voiceprints because they are a binary model—in other words, a voiceprint is just math! If your voiceprint is stolen by cybercriminals, they can't transform it back into your actual voice and do anything with it (like calling the director of an energy company and asking for 220,000 euros!). Since a voiceprint can't be reconstituted as the person's actual voice, it can't be used to commit crimes and is useless to cybercriminals.⁵ Stolen fingerprints, on the other hand (yes, I went there), remain a hot commodity.

Voiceprints have it all over other forms of biometric authentication. You can't conveniently verify a user remotely with a fingerprint, retina, or facial scan, but remote authentication is just a phone call away with voiceprint biometrics. For example, there's no need for expensive and cumbersome scanning equipment when voice authentication is as easy as a phone call to set up. Then, customers won't have to remember a mega-strong password, download an MFA app, or provide unique identifiers containing sensitive information (like a social security number) over the phone. All they need do is pick up the phone, call the bank, and their voice is their password. Convenience, thy name is voiceprint!

But are voiceprint biometrics really safe? Maybe not, according to cybersecurity researchers Andre Kassis and Urs Hengartner of the University of Waterloo. In a 2021 paper, the researchers demonstrated how voice authentication systems could be tricked with current deepfake technology. The researchers found all it takes is a fifteen-minute recording of the victim's voice to create a convincing deepfake. Worse, according to the researchers, deepfake technology can create fake speech realistic enough to fool speaker verification systems over 93 percent of the time.⁶

Not good! Call centers use speech verification systems to thwart imposters pretending to be customers, so deepfake technology is a potential blow against this important anti-fraud technique. Forget about the coming deepfake supremacy—voiceprint authentication systems might already be hackable.

Is this really a significant risk for the average Joe? Probably not. Unless you're a famous businessperson or a celebrity, you're likely not worth the effort for a cybercriminal to create a Deepfake You. Still, voiceprint biometrics are not 100-percent foolproof, and if you're rankled about it, you can easily protect yourself by not consenting to a voiceprint in the first place. Or if your voice isn't out there on Facebook or YouTube, and there's no other recording of your speech to pilfer, then consenting to a voiceprint is a safe and convenient way to do your banking.

Heavy adopters of voice authentication technology—banks, I am looking at you!—should consider taking additional precautions over and above voiceprint biometrics. Perhaps an *authentication layer* could be added so customers could use fingerprints or facial recognition in addition to a voiceprint. What banks should NOT do is offer voiceprint authentication *in lieu of* passwords and MFA. No technology is 100-percent foolproof, so voiceprint biometrics should not replace traditional cybersecurity controls. Even though the convenience of voiceprint authentication is a customer crowd-pleaser, banks are ill-served when the customer's voice becomes their *only* password.⁷

Learning to Live with the Deepfake Supremacy

It's only a matter of time before deepfake technology becomes so lifelike it's indistinguishable from the real thing. When this will happen is anyone's guess, but I suspect it will take us by surprise gradually, then suddenly—just like Ernest Hemingway's famous quote about going bankrupt.⁸ Deepfake supremacy will be a monumental disrupter; actual deepfakes will no longer be caught by anti-deepfake technology, and biometric authentication will bite the dust. After all, how can a bank rely on voiceprint authentication when voiceprints can be deepfaked with impunity? When deepfake supremacy arrives, nothing will be real—your fingerprints, facial patterns, and even a retinal scan can be deepfaked. In the coming deepfake supremacy, biometric authentication will be worse than useless—it will be dangerous.

What can we do once deepfake detectors can no longer detect deepfakes? The answer is a paradigm shift: *Stop trying to detect deepfakes and instead authenticate the real video right off the bat, so we have a verifiable method to refute deepfakes in the wild.* The coming deepfake supremacy means deepfake detectors have a sell-by date, so cybersecurity researchers are focusing on ways to *digitally watermark* original material to prove authenticity.⁹ If a cybercriminal posted a fake video in which someone is poisoned after drinking a Coke, the Coca-Cola Company could use digital watermarks to prove the deepfake video is not the real thing.

For watermarking to be effective, both AI-generated content and real content need to be watermarked. If you snapped a photo of a rose that looks almost too beautiful, how would anyone know it's a genuine photograph rather than an AI-generated deepfake? For that reason, Nikon launched the Nikon Authenticity Service to watermark photos taken with select Nikon cameras, so that an image can be verified as truly originating from that camera and is not a deepfake.¹⁰

In a future where deepfakes are indistinguishable from the real thing, *digital source verification* may be the essential technology to separate the fake from the real.¹¹ Unless, of course, deepfake creators rise to the challenge, and a new game of cat-and-mouse begins. Although watermark authentication is a promising technology, it will not be enough to thwart deepfakes. No anti-deepfake technology will ever be enough because there will always be an arms race between cybersecurity researchers and cybercriminal deepfake creators.

To win the arms race, it's essential that anti-deepfake technology be bolstered by a national deepfake awareness campaign so the public understands the threat of deepfakes. When the public knows about deepfakes, they'll be less likely to fall for deepfake-enabled scams. They'll also be more likely to put up with oppressively long passwords and MFA, even though biometric authentication is more convenient.

Deepfake supremacy is coming to pwn us. We need to be ready.

Inside the Deepfake Playbook: Beating Hackers at Their Own Game

In our bold new future, world governments march in lockstep to pass international legislation eliminating the threat of deepfake technology. When this inevitably happens, accountability for deepfakes will be aimed right between the eyes of deepfake creators and social media platforms.

Transparency is the *raison d'être* of anti-deepfake legislation, and so, with timely notification being the tip of the spear, companies eagerly disclose deepfakes frolicking in the wild, and a forewarned public is never hoodwinked by a true-to-life deepfake.

Big Tech enters the fray, and like roommates sharing a pizza, Google, Microsoft, and Apple partner to invent deepfake detectors powerful enough to flag even the most realistic deepfake audio or video. Deepfake detectors are always on the hunt—running as a background application—and when a deepfake is outed, the detector alerts the would-be victim, in real time, that the person they are watching is really an AI-generated deepfake.

Inspired by The Big Three, a legion of deepfake creators assemble into an all-volunteer army to prevent the malicious application of their deepfake technology. Voice cloning companies happily self-police their AI-generated deepfakes to prevent public exploitation. Likewise, deepfake video creators launch anti-deepfake policies to safeguard the public from unethical, malicious use of their deepfake videos. Most encouraging, social media companies mind their CISOs and practice good cyber hygiene to thwart cyberattacks and foil the plans of cybercriminals.

Okay, all right. I'm dreaming! None of this is likely to happen soon, if ever. Hope may be a thing with feathers, but it's not a strategy even Emily Dickinson would have banked on.¹² Governments are too busy competing with each other to ever join forces to fight deepfake technology, and hell no, deepfake creators will never rein in their moneymaker, even if it's the right thing to do. When it comes to the threat of deepfake audio and video, well, I'm afraid we're on our own. Fortunately, there are a number of steps we can take to protect ourselves from being pwned by cybercriminals brandishing deepfake technology.

Let's start with the obvious. If you're worried about cybercriminals stealing your face and voice, then don't give it to them in the first place. This means treating social media like a pariah, so no audios of yourself on LinkedIn or Facebook, and posting a video of yourself to YouTube is *verboden*. You'd also best eliminate any public speaking from your repertoire; however, if you must give a talk, you'd need to place restrictions on the audience so they understand audio and video recordings are not allowed. Oh, and don't forget to remove your actual voice from your voicemail, as it's easy pickings for a cybercriminal armed with voice-cloning software. Come to think of it, you'd also have to be wary the next time you get a cold call asking, "Can you hear me?" because it could be a cybercriminal trying to steal your voice.

While this level of hypervigilance seems extreme and downright paranoid, once your face and voice are stolen, it's a part of you that's gone forever. Worse, it's a part of you that can be weaponized in perpetuity to commit cybercrimes. All the things that make you "you"—the crooked smile when your puppy steals a treat, the sparkle in your eyes when your Little Leaguer hits a home run, and the sultry lilt in your voice when you're attracted to someone—it's all in the hands of cybercriminals who'll use Deepfake You to launch cyberattacks and commit frauds. They might even use Deepfake You to harass your friends with images of you doing and saying things you never would do or say in real life. And. This. Is. Forever.

Given the threat, going off the grid with hypervigilance is a legitimate countermeasure for those who can do it, but for people with public-facing jobs, this probably isn't an option. Salespeople, executives, and others needing to connect with their customers just don't have the option of going underground. Likewise, because humans are social creatures, it's natural to use online platforms to stay connected with family and friends, find a job, or get a date. It's also fun

to have a hobby, like posting craft beer reviews to YouTube or tweeting political truth bombs on X.

For most people, completely safeguarding their face and voice from theft is not feasible. Unless you want to live as a hermit, there's not much you can do to stop cybercriminals from generating a Deepfake You. However, if your friends and colleagues have at least a rudimentary awareness of deepfakes, it's exponentially harder for cybercriminals to weaponize Deepfake You. Public awareness is the primary countermeasure to malicious deepfake technology, and we can all help each other by being on the lookout for deepfake scams.

How to Spot a (Shoddy) Deepfake

Think you can spot a deepfake? Maybe—amateurish deepfakes are easy to spot. While Jordan Peele's Deepfake Obama is pretty cool, it's obviously a deepfake. Deepfake Obama's mannerisms are a bit herky-jerky, his lips are misaligned with the words being spoken, and his eyes are somehow off.

Weird eye movements are a dead giveaway when trying to spot a deepfake. Rookie cybercriminals find it difficult to reproduce natural eye movements with deepfake technology, so be on the lookout for these red flags: no blinking, too much blinking, intently staring eyes, or eyes not looking at anything (and instead gazing off in random directions).

Rookie cybercriminals also struggle with recreating a person's natural facial expressions. This is particularly true for amateur deepfake creators when they're poorly superimposing one image over another. Take a gander at Jordan Peele's Deepfake Obama, and you'll notice the lips, chin, and jaw do not quite mesh with the face, and the eyes do not seem to be interrelating with the face. Deepfake Obama's facial expressions, taken together, are askew.

A deepfake's facial features could also look amusingly bizarre. When deepfakes are created by amateurs, the face might be riddled with flaws, all of which are red flags for spotting a deepfake: The nose is missing a nostril, one ear is lower than the other, the chin is droopy, the nose is crooked, eyebrows are connected, and the list goes on. If the face looks slightly off or downright abnormal, you can bet it's a deepfake.

When trying to suss out a deepfake, it's also helpful to lend an ear. You can often spot a poorly cloned voice by listening to the pitch, tone, and timbre of the spoken words. If the pitch lurches up and down, with long pauses in between the next sentence, then you may be listening to a deepfake. If certain words and phrases blend into each other, creating a slurring effect, then you might be listening to a deepfake. If the voice is speaking in a monotonous, halting cadence, then it could be a deepfake.

Also, pay close attention to any unusual background noise—cybercriminals using a cheap-o microphone when recording someone's voice may end up with a lot of static in the cloned copy. When your boss calls to request a money transfer, that buzzing sound in the background might be indicative of a poorly cloned voice.

Of course, perhaps the biggest giveaway is when the deepfake image does something the real person would never say or do. Jordan Peele's Deepfake Obama said, "Killmonger was right," "President Trump is a total and complete dipshit," and warned the United States is turning into a "fucked up dystopia." The real Barack Obama would never say these things, which brings us to

the final red flag for spotting deepfakes: If the voice or image says or does things out of character to the person you know, then it could be a deepfake.

Spotting a deepfake can be quite easy if the deepfake is amateurish. However, deepfake technology is rapidly advancing to the point where many of these red flags won't present themselves. One day, deepfakes will simply be...perfect. Chris Ume, the famed Tom Cruise deepfake generator, has gotten exponentially better at making deepfakes over the years. His first efforts were obviously deepfakes, containing many of the red flags described above. But take a stroll through his [deeptomcruise](#) TikTok page and prepare to be amazed at his later efforts. Some of his deepfake Tom Cruise videos are so real I can't tell they're deepfakes. Well done, Chris!

Now don't get me wrong. I love Jordan Peele's Deepfake Obama. In fact, I think it's a pretty good deepfake, even though it's obviously a deepfake. But deepfake technology has progressed astronomically since Jordan Peele's 2018 effort. Today, deepfake technology has come of age, generating remarkably convincing facsimiles of a person's facial mannerisms, complexion, hair pattern, and even that barely noticeable lisp. With deepfakes becoming believably lifelike, there won't be any obvious red flags that catch our eyes, so we'll have to use other methods to spot the deepfake.

How to Spot a (Slick) Deepfake

"I'm from internal audit, and I'm here to help!" is a sarcastic refrain articulated with faux sincerity by internal audit professionals, particularly when management is being a PITA over the audit findings. But when it comes to deepfake threats, standard internal control techniques can be a lifesaver. Below are a few tried-and-true internal controls that can stop even the most realistic deepfake dead in its tracks.

Calling back is an easy way to spot a deepfake.

"Call Me!" is not just a great Blondie punk rock song; it's also an effective countermeasure to thwart vishing attacks. Cybercriminals typically use a burner phone when vishing with a deepfake voice, so one way to trip them up is with a simple callback.^{[13](#)} It works like this—when a CEO calls asking for money, the employee simply hangs up and verifies the request by calling the phone number on file for the actual CEO. Likewise, if a vendor calls asking for a wire transfer, simply hang up and call the real vendor using the phone number on file to validate the request.

Of course, the employee could hang up and call back using the caller's phone number, and if someone other than the CEO picks up, it's a sign that the first caller was a deepfake. The problem is a sophisticated cybercriminal knows how to redirect the call and tee up a voice-cloned deepfake to pwn you. Therefore, it's best not to call back using the caller's number. Instead, only call back using the number on file for the real, human CEO.

Segregation of duties can catch a deepfake.

Segregation of duties is vital—no single employee should be involved in all aspects of a job

function. For example, the employee who collects the money the company earns for its services should not be the same person charged with disbursing those funds to pay the company's debts. Not only does segregation of duties prevent fraud (because the person collecting money could, in turn, disburse said funds to themselves), but the more people involved in a process, the more likely someone will question a suspicious activity. There's an old saying: "Too many cooks spoil the broth." But with segregation of duties, "Two heads are better than one." When someone purporting to be the CEO calls and asks for a wire transfer, there should be multiple employees involved in processing the request. This way, someone may become suspicious, and a vishing scam can be averted.

Companies should also require sign-offs by at least two executives before a funds transfer is processed, especially for large disbursements. It's also essential to notify department leaders about any requests for large funds transfers. If they express surprise or concern, that's a sign to hit the pause button.

A simple password can trip up a deepfake.

Video deepfakes can be so lifelike, you'd never believe you're really interacting with an AI-generated algorithm. To thwart cybercriminals from pwning employees with a Deepfake CEO, it's wise to require *verbal passwords* for wire fund transfers.¹⁴ The password can be anything, such as "Tangle," "Badge," or "Rocky," and should be changed at least monthly. To prevent deepfake tomfoolery, employees should be trained to ask for the monthly password before approving a money transfer. A Deepfake CEO on a Zoom call may look like the real deal, but only the actual CEO would know the monthly password. If the CEO doesn't know the password, then you may be talking to an AI-generated doppelganger.

Cybersecurity training is essential.

Employee training is critical to stopping deepfake-enabled vishing scams. Workplace training should begin by explaining the mechanics of phishing and vishing cyberattacks, along with examples of what these attacks look like in the company's industry. Employees should be taught how to spot a deepfake with basic red flags: unusual eye movements or facial features, slurred or robotic speech, or the person is saying and doing things they would never do in real life. Knowing these red flags will help employees easily spot unsophisticated deepfake technology.

However, employees must also know how to spot a slick deepfake. Since deepfake technology is advancing at warp speed, companies need to empower employees to "break the glass" or "hit the pause button" when they suspect something vishy is going on. Companies should NEVER punish employees for not commencing a money transfer when the employee had a good faith belief the requestor was a deepfake; in fact, employees should be commended for not following the wire transfer instruction until they are satisfied the requestor is, in fact, not a deepfake. Blaming employees for not following money transfer instructions when the employee feared a deepfake is the surest path to being pwned by a cybercriminal.

Empowering employees to refuse a wire transfer is the primary countermeasure to my back-of-the-envelope formula:

$$\text{Deepfake Technology} \times \text{Fear Factor (Power Differential + Pressure)} = \text{Vishing Scam}$$

Employees should be trained not only about the various types of deepfake technology but also about the insidious social engineering tricks cybercriminals use to enhance the deepfake voice or image. When employees are wise to the high-pressure tactics used by cybercriminals, they're less likely to fall for deepfake vishing scams. Cybercriminals use time pressure, business pressure, and legal pressure to hector employees into bypassing company procedures or internal controls. Teaching employees these social engineering tactics will help them resist the pressure to approve that urgently needed wire transfer on a Friday afternoon.

And since cybercriminals love to pwn people on weekends and holidays, it's vital to train employees to follow basic verification controls before approving a wire transfer. These controls include calling the actual executive to validate the money transfer request, asking two or more executives to review/approve the request, and notifying department leaders to see if they have any concerns. Finally, companies should implement a monthly verbal password to verify the humanity of anyone requesting a money transfer—if the person doesn't know the password, then they're a deepfake until proven human!



Beating the Hacker's Deepfake Playbook: In the age of deepfake supremacy, even detection software can't catch deepfakes. Human judgment and awareness aren't perfect, but they may be our only defense. How can your organization defend against deepfake scams?

Type	Warning Signs
Shoddy Deepfakes	For video deepfakes: lips are out of sync with speech; eyes look unnatural; facial movements or expressions seem odd; and there is blurring around the edges of the face. For audio deepfakes: the voice sounds unnatural or robotic; words or phrases merge; and there is unusual background noise.
Slick Deepfakes	A person acts or speaks in a way that they would never do in real life. Their language, tone, or behavior doesn't match their typical personality, like a priest who never swears suddenly using profanity.
Control	Action Steps
Call Back Verification	If you get a suspicious call or video asking for a wire transfer, hang up and call the real person back to verify the request.
Segregation of Duties	Require multiple people to approve high-risk requests or transactions. No single call or video should trigger major actions.
Verbal Password	Establish pre-set passwords with family, friends, or coworkers. Ask for the password if you suspect a deepfake.
Awareness Training	Train employees to spot deepfakes and give them explicit permission to refuse suspicious requests, regardless of who appears to be making them.

CHAPTER 13

Quantum Computing and Artificial Intelligence: A Marriage Made in Hell?

You can arrange to have your head severed from your body—after you die, of course—and your noggin plopped into a vat of liquid nitrogen at -196 degrees Celsius.¹ No, it's not a *Simpsons* episode; it's neuropreservation, and it costs about \$80,000, which is conveniently covered by a life insurance policy.² Here's how it works: When you die, cryogenic technicians surgically detach your head and infuse it with cryoprotectants to prevent ice crystals from damaging your brain tissue. Then, your noggin is placed into a tank filled with liquid nitrogen, where it will stay, cool and comfy at a brain-chilling -196 degrees Celsius.³

If this sounds like a gruesome horror story, fear not—it's actually a shot at immortality, with the hope that future scientists will invent nanotechnology to repair your freezer-burned neurons, and then either regenerate a new human body or transfer your brain into a robot.⁴ And voilà—you're back, baby, thanks to tech that didn't exist while you were alive.

If you think this is brilliant, so do cybercriminals, except instead of stealing your brain, they want to pilfer your encrypted data. And even though they can't break the encryption today, they're hoping they can decrypt it in the future using tech that doesn't exist now.⁵ This cyberattack strategy is called Harvest Now, Decrypt Later (HNDL), and, to cybercriminals, "later" is spelled Y2Q, the acronym for "Year to Quantum," referring to the day when quantum computers are capable of decrypting today's unbreakable encryption algorithms.⁶

Unlike today's computers, which process *bits* (the smallest units of digital information) as either 0 or 1, quantum computers use *qubits*, which can be 0 and 1 simultaneously. If that sounds absurd, welcome to the bizarre world of quantum mechanics, where the principles of superposition and quantum entanglement allow qubits to interact in ways that ordinary bits simply can't.⁷ It also means that quantum computers can solve complex problems at lightning speed compared to current computers. For example, today's computers struggle when it comes to breaking encryption, but a quantum computer could crack it in hours, or even minutes.⁸

If you thought encrypting your data would deter cybercriminals from hacking you, think again. Even though encrypted data is currently unbreakable, it still has value to hackers, who steal and sell it to nation-state threat actors, who'll be happy to keep it for years until they can decrypt it with quantum technology. A foreign adversary like China is willing to hoard stolen, encrypted data for decades on the principle that not all data has a limited shelf life.⁹ Breached medical records remain sensitive and can still be used for identity theft long after they are stolen.

In the United States, some government secrets remain classified forever, and intellectual property, such as patents, chemical formulas, source code, or other trade secrets, retains its value indefinitely. Therefore, the passage of time does not diminish the value of sensitive data.¹⁰ Since storing large amounts of data is relatively inexpensive, threat actors are motivated to steal and archive as much encrypted data as possible, rolling the dice on future quantum breakthroughs to crack today's encryption to unlock tomorrow's secrets.

HNDL is both a current and future risk, as cybercriminals are motivated to steal encrypted data today, hoping to decrypt it when quantum computing finally becomes a reality. This means organizations must prepare today to thwart future quantum-enabled cyberattacks.

Since today's encryption algorithms have a quantum "sell-by date," organizations should prepare to adopt post-quantum cryptography (PQC) to protect their sensitive data. PQC refers to encryption algorithms designed to resist attacks from quantum computers. These quantum-resistant algorithms, such as those being standardized by the U.S. National Institute of Standards and Technology (NIST), are already being tested by companies like Microsoft for future use.¹¹ While PQC is not yet ready for widespread deployment, it's a promising technology for preventing quantum cyberattacks—and there's no time like the present to start planning for it.

But even PQC advancements will eventually become vulnerable to relentless quantum-enabled cyberattacks, so organizations must be ready to adapt by switching to new cryptography on the fly. This is called *crypto agility*, and it requires companies to build an IT infrastructure that can handle future algorithm changes quickly, without costly, time-consuming system overhauls, as old encryption standards are cracked and newer, more secure ones are developed.¹²

Now, let's take Y2Q one step further: What happens when quantum computing and artificial intelligence converge? To state the obvious, you get quantum's near-infinite computational power along with AI's unmatched ability to learn and adapt.

Quantum computing can potentially solve problems that today's computers can't, such as discovering the cure for melanoma or designing a carbon-eating molecule to reverse climate change.¹³ But quantum-enabled cyberattacks could crack the most powerful encryption in hours or minutes, allowing cybercriminals to steal your 401(k), turn off the cooling system of a nuclear power plant, or remotely hijack Air Force One mid-flight.

AI, with its uncanny knack for analyzing patterns and extrapolating outcomes, can automate tasks traditionally performed by humans, from customer call centers to disease diagnosis to someday operating planes, trains, and automobiles. And, AI could do this more cheaply and efficiently than squishy, bipedal humans. But AI can also be used to create deepfakes and adaptive phishing attacks, and displace human workers, causing mass unemployment on an unimaginable scale.

Just like any technology, quantum computing and AI are neither inherently good nor evil. It's how humans use them that determines whether a robotic surgeon removes a brain tumor or becomes an unstoppable cyborg Ninja assassin hell-bent on mass destruction. In the hands of cybercriminals and nation-state threat actors, a quantum-enhanced AI system (or platform) could wreak havoc on a dystopian level with entirely new classes of cyberattacks. Because it's too exhausting for me to keep writing "quantum-enhanced AI system (or platform)," let's just call the damned thing Abaddon, who was Satan's lieutenant in the Book of Revelation, and known apocalyptically as "The Destroyer."

Abaddon is a fitting name for quantum-AI technology that'll one day be unleashed to crack

encryption in the twinkling of an eye, cast company networks into the abyss, and automate large-scale adaptive phishing like a digital false prophet. It may not be the Great Tribulation of Revelation 7:14, but in the future, quantum-AI technology will empower Armageddon-level cyber carnage:

- Near-instant decryption would shatter today's encryption methods, and paired with AI adaptive intrusion, Abaddon would learn as it breaks through, adapting in real time to bypass firewalls and antivirus tools while discovering new vulnerabilities to exploit—and then, autonomously exploiting them across global networks.¹⁴
- Abaddon could create quantum-enhanced AI deepfakes that deceive with religious fervor, impersonating leaders, manipulating public opinion, and sowing chaos.
- With quantum-enhanced, AI-driven reconnaissance, Abaddon could discover vulnerabilities in critical infrastructure across the planet, launching attacks on power grids and satellites.
- Launching zero-day exploits at quantum speed, Abaddon would not need to trick employees with cumbersome phishing scams. Quantum-enhanced vulnerability scans would target company networks to identify ways to gain access (and move laterally within) without requiring user interaction.
- Abaddon could generate billions of fake identities using synthetic biometrics and AI-generated histories (fake demographics, social media profiles, medical records, etc.) to overwhelm authentication systems.¹⁵ Abaddon could then deploy large-scale identity spoofing (i.e., using fake credentials to gain unauthorized access) and take over millions of accounts. Then, when authentication systems are so confused that they can no longer distinguish between who's real and who's not, the collapse of trust leads to a breakdown in commerce (and potentially a Great Depression) or governance (potentially resulting in a civil war). Now, that's Armageddon!¹⁶

Um, okay. Abaddon's cyberattack capabilities are highly speculative, bordering on hogwash, but I trust you get the point: To a cybercriminal, quantum-AI technology is a marriage made in hacking heaven, but to the rest of us, it's a match made in hell. Sure, PQC compliance and crypto agility may stem the tide of quantum-AI cyberattacks, but they're unlikely to be enough. Companies and governments will need to be hyperaggressive in the face of persistent threats from nation-states and cyber gangs who'll have godlike pwning power in the palm of their hands.

So, why not pwn them back?

Daniel Shin, a cybersecurity researcher at William & Mary Law School's Center for Legal & Court Technology, has a novel approach to using deepfake AI to give cybercriminals a taste of their own medicine.¹⁷ Typically, IT infrastructure is designed to detect suspicious activity and repel cyberattacks by blocking the would-be intruder from the system. This is usually done through firewalls, intrusion detection systems, and access controls that identify suspicious activity and block unauthorized users. In most cases, this is enough—an intrusion is detected, the cybercriminal is blocked from accessing the system, and the cyberattack is thwarted. High-five, y'all!

But what happens when you have a persistent threat actor that is too darn ornery to stop attacking your network, and commands the resources of a foreign adversary, like, say, China, Russia, North Korea, or Iran? Or what if it's a nasty cyber gang like LockBit or REvil? And what if they're gunning for your company with the power of quantum-AI technology?

That's where Shin's plan comes in.

Instead of just blocking intruders, Shin suggests luring them into a fake server that uses generative AI to create synthetic data. This deepfake data mimics the company's real data, fooling cybercriminals into thinking they've breached it—all while the real data stays safe and untouched.

Shin calls it the *Honeypot System*, and here's how it works: Let's say a persistent threat actor is constantly attacking St. Mary Hospital, attempting to steal protected health information (PHI) from the hospital's electronic health record (EHR). The hospital's intrusion detection system flags suspicious activity—like an IP address from Russia or someone accessing data at lightning speed—but instead of blocking it, the system surreptitiously directs it to a honeypot server containing fake medical records. To cybercriminals, the medical records look real, but it's actually a deepfake created with generative AI. The cybercriminals are popping champagne corks, thinking they've hit the jackpot, not realizing it's deepfake EHR data, and the deepfake data is embedded with digital watermarks to prove it came from the honeypot!

By the time the cybercriminals hit up the hospital for ransom, the cybersecurity team has blocked the exploit (perhaps by patching a system vulnerability) and can assure the public that no real data was stolen. From a public policy perspective, the Honeypot System gives cybercriminals a dose of their own medicine by increasing the cost of their cybercrime—time and money—potentially deterring future attacks.

With Y2Q potentially arriving in 2030, we have limited time to plan.¹⁸ Since PQC compliance and crypto agility are still in early stages and not widely deployable, Shin's Honeypot System offers a timely, innovative approach to deceive and deter cybercriminals and protect sensitive data. Although still theoretical, the Honeypot System can be deployed today using honeypot virtual servers, generative AI to create deepfake data, and watermarking for forensic tracing.

But my favorite part of the Honeypot System is how it turns the tables on cybercriminals by using their own techniques against them: deception (fake servers), social engineering (exploiting greed), and generative AI (deepfake data).

Now, that's what I call Smashmouth Cybersecurity!

PART 3:

Beating the Hacker's Playbook

CHAPTER 14

Is “Ethical Deepfake” an Oxymoron?

AI-powered voice cloning technology is not sentient—at least not yet, though I’m keeping an eye on Alexa—and voice cloning software is not inherently good or evil. Why is it, then, that Deepfake Kilmer tugs at our heartstrings, Deepfake Bourdain makes us queasy, and Deepfake Johannes is the stuff of nightmares? Each of these deepfakes was concocted with the same basic GAN machine learning technologies, yet we feel starkly different about each of these deepfakes. What makes Deepfake Kilmer heartwarming, Deepfake Bourdain a bit creepy, and Deepfake Johannes downright criminal?

Starting with the obvious, the deepfakes themselves are simulations of an actual human’s natural voice. Deepfake Kilmer is a simulation of actor Val Kilmer’s voice, while Deepfake Bourdain and Deepfake Johannes mimic a famous chef and a German C-suite executive. Continuing with our “well, duh!” theme, the real Kilmer and Johannes were alive when their deepfakes were deployed, but the real Bourdain was dead.

Making deepfakes of dead people is just plain creepy. That’s why giving Amazon Alexa the ability to clone your dead grandmother’s voice is raising eyebrows. While a dead person’s family members could certainly consent to the voice cloning of their deceased grandmother, there’s always the question of whether this is what the grandmother would’ve wanted. Just like some people don’t want to be cremated when they die, it’s likely many people would not want their voice cloned after they kick the bucket.¹ Even if Anthony Bourdain’s surviving family approved of the use of his voice being cloned, we really don’t know how Bourdain himself would have felt about it.

Also, cloned voices of dead people could be used to say things the dead person never said in real life. Hacktivists could create deepfake voices of deceased historical figures to tarnish their legacy. Imagine a Deepfake Martin Luther King Jr. being used to spread racist lies or a Deepfake Mahatma Gandhi issuing a clarion call for war. Of course, deepfakes don’t have to be hateful. In the biopic *Roadrunner*, director Morgan Neville used Deepfake Bourdain to say things the real Bourdain never said when he was alive—specifically, a snippet from an email Bourdain had sent to a friend, with Deepfake Bourdain saying: “. . . and my life is sort of shit now. You are successful, and I am successful, and I’m wondering: Are you happy?”²

Deepfake Bourdain said these words because Neville thought they were essential to the story he wanted to tell. Nonetheless, fans and critics were outraged that Neville put words in the mouth of Bourdain that he never said, with some complaining that Bourdain himself would have been unhappy with Deepfake Bourdain. Of course, we’ll never know since Bourdain’s not around to

tell us his wishes, which is precisely the problem with using deepfake voices of dead people.

“Unapproved voice cloning is a slippery slope—as soon as you get into a world where you’re making subjective judgment calls about whether specific cases can be ethical, it won’t be long before anything goes,” said Andrew Mason, the CEO of audio/video editor Descript, in a 2021 blog post. “Even if you think that the use in the Bourdain documentary is ethical, is there enough upside to open this Pandora’s Box? We think the answer is no—whatever the path may be to universal enlightenment, we can get there without reanimating the dead.”³

Let’s chalk up being dead as a big red flag for deepfake cloning. However, there’s something else to consider: Throat cancer survivor Val Kilmer requested to have his voice cloned for a movie performance, which made him a client of voice-cloning firm Sonantic. If Kilmer was a client, what does that make the real Bourdain and Johannes? Clearly, the real Johannes was a victim of cybercriminals who cloned his voice for nefarious purposes. However, I’m not quite sure how to classify the real Bourdain. The deepfake was made after his death but was not used by Neville with malicious intent; indeed, Neville was genuinely trying to do justice to Bourdain’s life story.

Kilmer is clearly a client, Johannes is clearly a victim, and Bourdain falls somewhere outside either classification. These distinctions are significant. We feel good about a deepfake when we know the subject is a client of a voice-cloning firm, we are scared when the subject is a victim whose deepfake was generated by cybercriminals, and we feel uneasy when we don’t quite know how to classify the subject.

Which is why consent is so vitally important.⁴ We know that Val Kilmer consented to the creation and use of Deepfake Kilmer, so we feel good about it. However, neither Bourdain nor Johannes consented to their deepfakes, which does not sit right. With Johannes, we are angry that his voice was used without his knowledge to commit crimes. In the case of Bourdain, Neville claimed Bourdain’s widow was “cool” with the deepfake, but she disputed it in a tweet—so we are rightly confused and uneasy, especially since Bourdain himself did not consent. Bottom line, if consent is nonexistent (as in the case of deepfake crimes) or questionable (because there’s no signed, written consent from the subject when they were alive or from their family after death), that’s a big red flag.

Our third red flag is the lack of public disclosure.⁵ The Bourdain biopic *Roadrunner* premiered at the Tribeca Film Festival in New York City on June 11, 2021, and was released in the United States on July 16, 2021; however, there was no disclosure in the movie’s opening credits about Neville’s use of voice cloning in the making of the film. Many fans who had seen the film—and movie critics who had written reviews—only learned about the deepfake after Helen Rosner reported it in *The New Yorker* magazine. When fans and critics alike found out about Bourdain’s voice being cloned, they were furious.

Disclosure to the public about deepfakes is essential to avoid feelings of betrayal and being manipulated. In Val Kilmer’s case, the actor and Sonantic let the public know that Kilmer’s voice was a deepfake in the movie *Top Gun: Maverick*. In disclosing the deepfake, Kilmer and Sonantic explained why the deepfake was being made and brought much-needed awareness to the plight of throat cancer and voice disorders. Further, Kilmer and Sonantic went to great pains to explain precisely how Kilmer’s deepfake voice was technically produced.

In the case of Deepfake Kilmer, we know the name of the firm and the tools used to simulate Kilmer’s voice. We also know Kilmer’s reasoning behind his deepfake—to get his voice back so

that he could reprise a classic film role. Because the public was informed, there was no controversy about Deepfake Kilmer; in fact, Kilmer fans were thrilled to see their hero back in action!

Deepfake Bourdain is another matter. Fans felt manipulated when they learned of the deepfake and disagreed with Neville's reasoning for including it in the film, with many fans and critics declaring Neville acted unethically. Neville certainly erred in not unequivocally nailing down consent with Bourdain's wife (a signed consent form would've been helpful!), but not disclosing Deepfake Bourdain to the public prior to the film's release was a cataclysmic blunder.

Finally, there's a big difference between deepfakes that are used in a work of fiction versus deepfakes used in a purportedly factual documentary or, worse, a cybercrime. We can perhaps give deepfakes a pass when they are used in movies by an actor. However, it's much harder to square deepfake words that the subject never spoke when they occur in a nonfiction biography. In *Roadrunner*, Bourdain's words were real—he had written them in an email—but they were spoken by a computer-generated voice, so we have the cognitive dissonance of real words spoken by a deepfake voice. In *Top Gun: Maverick*, we have words that are totally fake—albeit scripted—spoken by a deepfake voice. We're not okay with *Roadrunner* because of the mix of reality with deepfakery, but we're peachy keen with *Top Gun: Maverick* because everything was just acting to begin with.

Deepfake voice cloning is getting more realistic by the day (if not hour), and anyone seeking to deploy deepfakes can easily get their hands on intuitive, cutting-edge voice-cloning technology. As the democratization of voice cloning marches on, we can look to our good old Deepfakes Kilmer, Bourdain, and Johannes to provide us with a few ethical guardrails:

- 1. Think twice about making deepfake voices and images of dead people.**

Do you really want your dearly departed spouse reading your kid a bedtime fairy tale? Or perhaps you'd like to hear CNN's early voting projections spoken by dead-and-buried granny's warm, cuddly voice? While you're at it, why not have Deepfake Dead Granny tell you the latest stock quotes from CNBC?

Cloning the voice of a dead family member ranks at the top of the ick-factor scale. In addition to being downright eerie, mimicking the voice of a dead relative is a prescription for a nervous breakdown.

Cloning the voices of dead relatives can also be abused by jerks. It would be emotionally traumatic to hear Deepfake Dead Granny say nasty things about her grandkids. Even if you know it's a deepfake, it's still her warm, soft voice saying horrible things she'd never say in real life.

If you really need a heartwarming remembrance of a loved one, why not grab a box of Kleenex and gaze teary-eyed through those old family photos? Cloning the voices of dead family members just isn't worth the trouble, given the potential for abuse and deep-rooted psychological injury.

Also, it's probably not a great idea to clone the voices of dead celebrities, politicians, or historical figures. They're dead—let them rest in peace. The world is not a better place

with a dead celebrity deepfake hawking a fast-food chain or a dead deepfake civil rights leader endorsing a political party in an election campaign ad. There are other ways to use dead celebrities in movies and advertisements without making deepfakes of their voice.

That being said, Deepfake Dead Celebs appear in commercials all the time, and I doubt that will change. However, companies using dead celebrity deepfakes in marketing campaigns run the risk of offending the very consumers they're selling to if the ad isn't tasteful and respectful.⁶ This happens when a Deepfake Dead Celeb does or says something that the actual celebrity never said or did when alive. Or the Deepfake Dead Celeb does something completely out of character to the celebrity being mimicked.

For example, using the deepfake image and voice of civil rights icon Martin Luther King Jr. to sell potato chips while juggling bowling pins on a unicycle would be highly offensive to most people. The real MLK would never do those things. Now replace MLK with John F. Kennedy, Sally Ride, or Pope John Paul II, and you get the same result—howling mad consumers so infuriated they won't buy the potato chips and might just chow down on healthy snacks, like baby carrots and celery.

This brings me to another point: Using deepfakes of dead people for commercial purposes is fraught with ethical peril. It's one thing to use a Deepfake Dead Celeb for historical and educational purposes, for example, as part of a museum exhibit. Using a Deepfake Ronald Reagan to recreate the famous "Mr. Gorbachev, tear down this wall" speech is probably okay, but using Deepfake Ronald Reagan to promote ultra-ribbed lubricated condoms is going to ruffle a lot of feathers.

Deepfakes of dead celebrities doing things they never did, or never would do, for commercial purposes is really in bad taste. Oh, and it's still unethical even when the surviving family members consented to the deepfake. Planting Reagan's butt on a unicycle to sell potato chips—or condoms—is wrong (on so many levels!), even if the family approves. In these cases, "consent" is a red herring and merely a talking point to deflect criticism of a tasteless, unethical use of a Deepfake Dead Celeb.

2. No deepfakes without consent.

Consent helps us understand whether the deepfaked person knows about and approves the use of the deepfake copy of themselves. If they didn't consent, then they're a victim, and something deeply personal—their voice or image—has been stolen from them. Knowledge is power, and using deepfakes without a person's consent creates a power differential to the victim's detriment. Using deepfakes without the individual's informed consent is unconscionable.

3. Disclose the use of deepfakes to the public.

Using deepfakes in media without telling the target audience is bald-faced manipulation. Nondisclosed deepfakes cheat consumers out of a genuine connection with a cherished product or favorite actor. Worse, nondisclosed deepfakes are dangerous when deployed to inflame religious or political beliefs and can result in violence or upended elections.

Just like non-consented deepfakes, non-publicly disclosed deepfakes create a power differential that manipulates the audience. Knowledge is power, and informed consent and public disclosure level the playing field to avoid an imbalance of power resulting from negligent or malicious use of deepfakes.

Deepfake cloning software is not inherently good or evil—how the technology is used can either delight us or make us nauseous. We're cool with Deepfake Kilmer, leery of Deepfake Bourdain, and want to exile the creators of Deepfake Johannes to a penal colony where they're forced to make bricks for a prison wall using only mud, straw, and their bare hands.

Fortunately, the examples of Deepfakes Kilmer, Bourdain, and Johannes offer clear ethical boundaries that we can follow to make and use deepfakes ethically. By obtaining informed consent and disclosing to the public when deepfakes are deployed, the harm and abuse of power from careless applications of deepfakes can be avoided. Of course, a one-way ticket to the aforementioned penal colony is probably the best way to deter malicious applications.

CHAPTER 15

Victim Blaming: The Hacker's Cruel Accomplice

杀猪盘 is Chinese for Sha Zhu Pan, which means pig butchering in English. “Sha” means to kill or slaughter; “Zhu” is a pig; and “Pan” is a dish. Put it all together, and the literal translation is “slaughter pig dish.” Yet the true meaning is not a mouthwatering plate of BBQ ribs, salty collard greens, and a mound of sweet and tangy coleslaw. Sha Zhu Pan is a bitter, foul-tasting metaphor that reduces the victims of crypto-romance scams to slaughtered animals.¹

Pig butchering invokes the image of a stuck pig squealing in agony as it’s bleeding out, dying in sheer terror, utterly alone. By tying the image of a helpless, tortured animal to a human victim, “pig butchering” shifts the responsibility away from the scammer’s crime and places the fault on the victim.

Dehumanization is at the heart of victim blaming.² Scammers have emotions just like anyone else, and even the nastiest cybercriminal can feel a smidgen of empathy for the victim. Guilt feels like a gut punch, so cybercriminals hack shame by visualizing their victims as animals. For example, scammers might say, “A mouse sniffing for crypto earns the mousetrap.” Degrading imagery is a surefire way to stop remorse from gnawing a hole in the cybercriminal’s stomach, and victim blaming is a better antidote to stress ulcers than Prilosec.

Feeling guilty sucks—your heart races, your palms sweat, and acid reflux turns your stomach lining into Swiss cheese. Ahh, but there’s nothing like the soothing balm of moral disengagement to calm your frazzled nerves.

Moral disengagement is a neat mental trick—all the scammer needs do is reframe their heinous crime as justified.³ Here’s how it works: A scammer cons a victim into forking over their life savings in a liquidity mining scam; then, feeling guilty about the now-penniless victim, the scammer looks into a mirror and says, “A greedy pig hunting for Bitcoin deserves the meat cleaver.” With one sentence, the scammer has achieved an I’m-not-guilty twofer—the victim is dehumanized as a “pig,” and the crime is justified because the victim’s “greed” got them scammed. On the other hand, the scammer also said the victim “deserved” it. Maybe, then, it’s an I’m-not-guilty trifecta, and what we have here is a set of mental gymnastics so twisted it transforms the scammer’s feelings of guilt into self-righteous validation. But that’s what the pig butchering metaphor is all about; the term itself dehumanizes victims and is the epitome of victim blaming.

It’s easy to see why scammers blame the victim, but why does society do it? Why mock Seth Green when hackers stole his Bored Ape NFT? Linebacker Manti Te’o, victim of an elaborate catfishing scam, was cruelly ridiculed in the media—why? Cybercriminals stole private, intimate

photos of actress Jennifer Lawrence, yet the press blamed the actress for the breach more than the cybercriminals. Anne, the Brad Pitt catfishing victim, was trolled so mercilessly that she was hospitalized for deep depression. It's the same old story: When deceitful scammers bamboozle someone, the victim often gets blamed instead of those who perpetrated the crime.

Much study has gone into understanding why we blame the victim more than the perpetrator. Still, I'll boil down decades of criminological research into a silly-simple soundbite: *We blame the victim because it makes us feel better.*

A vicious crime reminds us that the world is a dangerous place, but victim blaming helps us maintain a false veneer of safety. We trick ourselves into believing we could have avoided a similar fate by asserting the victim was "culpable" and "deserved" their misfortune—a classic example of *just-world bias*.⁴ For example, when a woman is sexually assaulted, someone might post on Facebook that the attack was the woman's fault for walking around at oh-dark-thirty on a dimly lit street. Or someone reading about the assault might think that the woman "asked for it" by dressing provocatively in a seedy part of town. In either case, the victim blamers are indirectly asserting that a violent crime would never happen to them because they always dress appropriately and only walk in upscale areas during regular business hours. However, believing you can avoid a crime by not looking attractive is a false sense of security. Nonetheless, by blaming the woman for the assault rather than the predatory behavior of the criminal, we bolster our sense of safety.

People also tend to focus on the quirks of being human rather than realizing life happens. For example, you blame laziness as the reason your buddy flunked an algebra test, yet when you flunked a biology pop quiz, you attribute it to poorly written multiple-choice questions. Or a driver who sideswiped you in traffic is considered reckless, but when you run a red light, it's okay because you were late for an urgent meeting. Or you call it "lax parenting" when a child is screaming red-faced at McDonald's, but when your children do the same thing, it's because they were "overtired."

You see the pattern here. When we screw up, it's due to extenuating circumstances, but when someone else screws up, it's because of what they did or didn't do rather than an external event. Maybe your buddy flunked the math test because he had the stomach flu, the erratic driver was moving over to let an ambulance pass, or the howling child stubbed a toe. By misperceiving the proximate cause of an epic failure as someone's personality trait (e.g., lazy student, reckless driver, or lousy parent), we fail to understand that the actual reason was entirely out of that person's hands in the first place.

This type of bias is called *fundamental attribution error* and is pretty hard to shake.⁵ In a catfishing scam, the victim might be blamed as "gullible" or "love starved" when the reality is the scammers used a sophisticated psychological playbook to manipulate the victim emotionally. Or victims of a phishing attack were "stupid" and "careless" for giving up their passwords when the truth is the fake website was meticulously designed and highly convincing.

The fundamental attribution error is harder to kick than smoking cigarettes, but there is a cure for this addiction: Instead of a nicotine patch, how about trying a little empathy? *Empathy* means understanding how the victim thinks and feels. When you "stand in the shoes" of the victim, you'll realize external factors led to the crime, not something the victim said or did.

Empathy overlooks the quirks of being human; personality traits are irrelevant. Instead of jumping to conclusions about the victim's intelligence or character, empathy understands that

external events are determinative. Empathy does not ascribe fault to the victim. Instead, it focuses on the criminal and the crime itself. Empathy never judges the victim and understands that anyone can be catfished, no matter how smart they are. After all, sometimes life happens.

We could all use a little empathy because victim blaming is shattering to people who've been pwned. Blaming the victim who's been harmed by an emotionally and financially draining scam cruelly adds to the victim's humiliation. Victims of cybercrime suffer twice: once from the misfortune of the fraud itself and again from the stigma placed on them by social media trolls and insensitive news reporting.

The trauma is so intense that most cybercrime victims are too embarrassed to report the crime to law enforcement. Not only do the criminals go unpunished, but they remain at large to prey on others. The humiliation is so acute that many victims do not seek out mental health counseling and thus do not receive much-needed emotional support services.

Victim blaming also harms society. It contributes to a *victim-blaming culture*—a society where pig butchering and other cyber frauds are normalized and overlooked. It's a culture where predatory online manipulation is pooh-poohed as the victim's fault, and the deceitful actions of the perpetrators are not challenged by society. It's a culture where cybercrimes flourish, victims wallow in misery, and cybergangs laugh all the way to the bank.

One alarming by-product of the victim-blaming culture is that ignoring scammers and blaming victims discourages society from adequately funding law enforcement to combat online fraud. Why bother enacting anti-scam laws (or financing police initiatives) when catfishing is ultimately the victim's fault? When it comes to cybercrime, victim-blaming culture implicitly “defunds police” from both fraud prevention and enforcement activities, thus empowering scammers to prey upon the public with impunity.

Let's pummel victim-blaming culture with a massive dose of smashmouth cybersecurity! We can fight victim blaming with three tactics: empathy, a language paradigm shift, and aggressive pushback on the victim blamers themselves. These tactics work in concert to eliminate victim-blaming culture by shining a white-hot spotlight on the scammer's tactics rather than blaming the victim.

Let's start by carefully examining the words used to describe how society feels about cybercrime, and from there, flip the script with new verbiage that focuses on the scam itself instead of blaming the victim. I call this *lingo shifting*, and it starts by abolishing the hideous and dehumanizing term known as pig butchering. It's an ugly, cruel metaphor that blames the victim and exalts the scammers. Pig butchering is the epitome of victim blaming and must quickly die an ignoble death.

The international crime fighting organization INTERPOL agrees, and in 2024, it proposed a new term, *romance baiting*, to replace pig butchering.⁶ INTERPOL adopted romance baiting to rehumanize victims and place the focus on the scammers' fraud tactics. The words “romance” and “baiting” illustrate *how* the crime is committed, which represents a paradigm shift from the victim-blaming imagery of a slaughtered pig. Romance baiting is far more accurate and humanizing than the despicable pig butchering idiom.

Unfortunately, romance baiting has not caught on, and pretty much only INTERPOL uses it. Therefore, we need another candidate to replace pig butchering, and the term *crypto-romance scam* smartly fits the bill. Both “crypto” and “romance” focus on the crime itself rather than the victim, and the word crypto implicates “cryptocurrency” as the scam's *raison d'être*. Crypto-

romance scam is excellent terminology to describe this horrible crime, and yet crypto-romance has also failed to dethrone pig butchering as the go-to metaphor.

It's like pulling teeth to oust pig butchering because it's a raw, visceral metaphor. Just say "pig butchering," and see how you feel—it's like cold, wet goosebumps prick your flesh with tingling sweat. But that is precisely why we must use terms like 'romance baiting' or 'crypto-romance scam': They choose human dignity over turning a victim's trauma into a punchline.

In addition to removing the cruel pig butchering metaphor from our lexicon, society must completely flip the script on victim-blaming terminology and turn the tables on the scammers and the methods they use.⁷ Lingo shifting should be a key component of cybersecurity education to help the public understand how bias in our language leads to victim blaming. For example, when someone is harmed by a catfishing scam, instead of thinking, "How could someone be so stupid to fork over their life savings?" reimagine the scenario as more like, "A nasty cybercriminal stole that person's money!" The point is to reorient society's thinking away from the victim and instead focus solely on the scammers and their fraudulent misconduct.

Below are examples of lingo shifting:



Beating the Hacker's Playbook: When we blame victims, we dehumanize them and let the scammers off the hook. What will YOU say the next time someone is the victim of a scam?

Victim-Blaming Lingo	Lingo Shifting to Empathy
Scammers pwned the hell out of you!	Scammers are experienced cybercriminals with a hacker's playbook and the resources of organized crime syndicates.
How did you fall for such an obvious scam?	The victim suffered a crime, so it's not the victim's fault.
Hah! Look at how much money was forked over to the scammers!	No money was freely given; cybercriminals stole the victim's money.
Someone was tricked into giving money to catfishers!	No money was freely given; cybercriminals stole the victim's money.
Well, now you know that if something is too good to be true, it probably is! Ha-ha!	Scammers are experienced cybercriminals with a hacker's playbook and the resources of organized crime syndicates.
Only naïve dummies or old farts with dementia get scammed!	Not true. Anyone can be the victim of a scam, including doctors, lawyers, and even cops. Cybercrimes injure people from all walks of life, professions, and ages.
The scammers pwned you. You're totally screwed now!	There is always hope! Victims can fight back by reporting the scam to law enforcement and seeking help from friends, family, and counseling organizations. NEVER GIVE UP!

Oh no, you were pwned by a pig butchering scam!	It's not pig butchering; it's romance baiting or a crypto-romance scam.
--	---

Whenever you read a catfishing news story and feel negative emotions about the victim, just engage in a healthy round of empathetic lingo shifting. You'll find yourself aligning with the victim and totally livid at the scammers, which is precisely where your cannon should be aiming.

Lingo shifting is also a great way to push back on victim blamers, especially the internet trolls who mock victims from the safety and anonymity of a stupid internet handle. *Guilt shifters* hide behind their usernames to heap scorn upon ill-fated victims instead of the perpetrators of the crime. These guilt shifters are usually little more than biased, ill-mannered jerks, but victim-blaming insults can also be generated by state-sponsored troll farms and even the scammers themselves.

As a society, we need to aggressively push back against guilt shifters to support the victim and mitigate the victim-blaming culture. Victims who are too beaten down to fight back should seek help from friends and family to respond to guilt shifters. Society also needs anti-fraud organizations to step up with lingo-shift messaging and aggressive outreach to guilt shifters and clueless media when victim blaming occurs. It's high time we stop being polite and treat victim-blaming guilt-shifters to a dose of their own medicine—1,000 mg of extra-strength shame, taken as a rectal suppository. Now, that oughtta learn 'em!

Reeling in the Catfishers: Operation Shamrock Shows Luck Is Not a Strategy

Despite the harrowing prevalence of romance scams, there are heroes who take on the catfishers and attempt to claw back stolen cryptocurrency. One hero is Erin West, a prosecutor who takes the fight to the battleground catfishers fear most—their crypto wallet. West is a twenty-five-year veteran prosecutor of the Santa Clara County District Attorney's Office who's on a mission to tackle the epidemic of crypto-romance scams with a novel approach—"educate, seize, and disrupt"—the mantra of West's three-leaf clover enforcement strategy she's dubbed *Operation Shamrock*.⁸

Cryptocurrency scams are notoriously resistant to law enforcement efforts. Victims are often so embarrassed that they either don't report the fraud or don't report it promptly, which gives the scammers plenty of time to launder the cryptocurrency or simply cash in their winnings. Also, cryptocurrencies and the exchanges that trade them, like Binance and Coinbase, involve complex and innovative technologies such as blockchain, cryptography, liquidity mining pools, and smart contracts, all of which are difficult for local law enforcement to grasp. Most cops and prosecutors have no idea how to trace stolen crypto, so even if they want to help a victim, they can't identify the exchange where the crypto finally landed. And even if they can locate the exchange holding the stolen crypto, the exchange might not cooperate with US-based prosecutors and refuse to return it.

George Reeves's 1950s TV Superman leaped tall buildings in a single bound all by himself, but when it comes to crypto-romance scams, superhero Erin West hurdles over these law enforcement obstacles with a little help from her friends. Operation Shamrock, along with the

Crypto Coalition, a 2,000-member network of cops, prosecutors, and finance professionals founded by West, aims to put the kibosh on crypto-romance scams and help victims recover stolen cryptocurrency.

The first step in Erin West's scam-busting strategy is to educate local police and district attorneys so they have a fighting chance at thwarting the scammers and seizing stolen crypto. But education is a challenge because many people in law enforcement don't even know that romance scams are a thing!⁹ Half the battle is bringing awareness to police officers and prosecuting attorneys that crypto-romance scams are not only real but a global crime of epidemic proportions.

Next up is dealing with the misperception that crypto-romance scams are the victim's fault for being stupid or lonely or sex-crazed or—whatever. The tendency for people to shame the victim is a genuine phenomenon that needs to be upended. You might be tempted to think, "I'd never fall for a love-bombing cyber-sweetie! What a doofus!" However, victim blaming is wrong because the human targets of crypto-romance scams are not stupid or weak—they were duped by scammers who have a sophisticated fraud playbook. Also, victim blaming is wrong because it guarantees the success of crypto scams: for one, it makes victims likely not to report the scam out of embarrassment; and two, when a victim does come forward, law enforcement is more likely to drag their heels on investigating the crime—assuming they even bother to open a case. Shaming the victim helps no one except the scammers, and Erin West's *Crypto Coalition* is at the forefront of educating law enforcement and financial institutions to empathize with the victim and treat cryptocurrency scams as a grave crime worth investigating.¹⁰

Another challenge is explaining crypto technologies to non-geek prosecutors so they can track the stolen crypto and return it to the victim. But there's good news on this front. Erin West has a plan, and backed by the *Crypto Coalition*, she's providing local law enforcement agencies with a template to seize stolen crypto.

The template—tracing, freezing, and seizing—is deceptively simple despite the complexity of the technologies involved.¹¹ First, local cops and prosecutors must trace the stolen crypto, and this is where the *Crypto Coalition* can help with tips and coaching on how to map the flow of funds between the victim and the crypto scammers. Next, once the crypto exchange holding the stolen funds is identified, the prosecutors go to court for a search warrant. Many crypto exchanges like Coinbase and Binance will obey a court-ordered search warrant to freeze the crypto—so the scammers can't move it—and then transfer the stolen crypto to a *government crypto wallet*.¹² Here again, the *Crypto Coalition* can assist local police/prosecutor teams with guidance on how to explain crypto-romance scams to the judge to obtain the search warrant, as well as how to create a government crypto wallet. The final step is the most satisfying. Once the stolen crypto has been seized, it can now be transferred to a grateful victim.

By tracing, freezing, and seizing stolen crypto, Erin West and her team have returned over \$2.5 million robbed in crypto-romance scams. And now, along with the *Crypto Coalition*, she's teaching this method to cops and prosecutors worldwide.

Hmmm—I'm sure she doesn't wear a red cape, but maybe Erin West *can* leap tall buildings in a single bound!

CHAPTER 16

Oops, That Breach Is on You: The Finger-Pointing Art of Corporate Blame Shifting

Three days before Christmas in 2022, LastPass, a company that promises to keep your passwords safe, handed its 33 million customers a lump of coal. Karim Toubba, the chief executive officer of LastPass, warned in a December 22nd blog post about a data breach in which hackers copied a backup of customer vault data, resulting in potentially millions of passwords falling into the hands of cybercriminals.¹

While it's appalling that LastPass chose to be a Grinch and drop the bombshell notice during a festive period—when people are rejoicing with family and businesses are closed for the holidays—LastPass's advice to customers whose vaults were hacked was equally shocking: maybe do nothing.

According to Toubba's blog post, the hacked password vaults were encrypted—and the data secure—as long as the customer's master password conformed to LastPass's "default settings" and the customer followed the company's "password best practices."²

LastPass customers use a master password to log into their LastPass account. According to Toubba's post, it would take cybercriminals "millions of years" to guess the master password for customers with a strong master password of at least twelve characters in length.³ Toubba's post recommended that customers never reuse the master password for other websites; otherwise, cybercriminals could use a stolen password from a breached website to access the customer's LastPass account (a cyberattack known as credential stuffing).⁴

Customers using a strong, unique master password are probably out of the woods, as Toubba claims in the post that hashing and encryption methods deployed by LastPass would make it "extremely difficult to attempt to brute force guess master passwords for those customers who follow our password best practices."⁵

On the other hand, customers who created a weak master password are in hot soup, as hackers using brute-force methods can guess the master password to break into the customer's vault, meaning all of the customer's passwords are now in the hands of cybercriminals. For customers with weak or reused master passwords, Toubba advises that "as an extra security measure, you should consider minimizing risk by changing passwords of websites you have stored."⁶

And therein lies the catch—and quite likely LastPass's legal defense. Toubba's blog post audaciously contends that LastPass's security architecture did, in fact, keep the password vaults

secure from the prying fingernails of cybercriminals. By this logic, cybercriminals could only access the vault to steal the passwords if the customer created a weak master password or reused the master password for another website. In other words, any data leakage from the breach is not LastPass's fault—it's the fault of customers who did not follow the company's "password best practices."

But don't just take Toubba's blog post for it. In a statement emailed to *The New York Times*, Toubba wrote about the "strength of the company's system architecture," which "kept sensitive vault data encrypted and secured," and that it was up to users to "practice good password hygiene."⁷

Never mind that LastPass has "required" twelve-character master passwords since 2018 but didn't enforce the policy, meaning customers could have been using a password with less than twelve characters.⁸ LastPass began enforcing twelve-character passwords in 2024, but this step does not secure the data stolen in the 2022 breach, since weak passwords were still allowed by LastPass to be used at the time.⁹

Never mind that LastPass offers multifactor authentication (MFA), which is a one-time code used in addition to your username and password, but doesn't enforce MFA when a customer creates a LastPass account—so customers unaware that LastPass offers MFA are not protected by this essential, robust defense against brute force attacks.¹⁰ Here again, LastPass could significantly improve "good password hygiene" by forcing MFA when customers establish a LastPass account, but the company has not done this.

Never mind that LastPass has a sorry track record in repelling cyberattacks. LastPass has been hacked with annoying regularity: 2011, 2015, 2016, 2017, 2019, and 2022, with the last breach being the worst.¹¹ Cybercriminals hacked LastPass in August 2022 and used the information from the breach to trick a LastPass employee into giving up the credentials and decryption keys needed to copy backups of customer password vaults.¹²

Even worse, LastPass did not encrypt everything stored in the customer vaults, so while passwords in the vault were encrypted, customer metadata was not.¹³ Website URLs, IP addresses, and other metadata such as company names, usernames, billing addresses, email addresses, and telephone numbers are extremely sensitive pieces of information. In the hands of a cybercriminal, personally identifiable information (PII) is a ticking time bomb. PII can be tied to a specific individual and used by cybercriminals to launch spear phishing attacks against high-value targets, such as journalists, political activists, or company executives.¹⁴ Encrypting stored metadata is an elemental countermeasure to thwarting cyberattacks—yet LastPass didn't encrypt the metadata.

None of this is the fault of LastPass customers, even the ones who did not practice "good password hygiene." When cybercriminals break into a company's network and steal customer data, it is the company that is responsible for the breach. What makes pointing the finger at LastPass customers so galling is that LastPass is not simply a password manager. At its core, LastPass is a cybersecurity company that sells peace of mind to its customers.

With such a poor batting average against cybercriminals, LastPass should not be ballooning the canard that "good password hygiene" is solely the customer's responsibility. Given LastPass's long and tortured history of cyberattacks, the company should not have waited until 2024 to implement a forced master password update. In addition, MFA should not be optional. LastPass should hardwire MFA to force every customer with a LastPass account to

enable MFA.

No doubt, individual responsibility is a vital element of cybersecurity. Everyone should practice good cyber hygiene by creating strong passwords that are never reused and enabling MFA whenever available for online accounts. However, responsibility for cybersecurity is not a one-way street leading to the end-user's home; it is the shared responsibility of both the customer and the company.

Let's also keep in mind that the LastPass data breach is not the result of cybercriminals hacking 33 million individual LastPass customers. It's the result of cybercriminals hacking LastPass itself, a company that promised to keep its customers' sensitive data secure. From a public policy perspective, we should not allow companies to wiggle away from accountability by blaming their customers. If we do, then why would any company ever hardwire cyber hygiene into their platform? Making strong passwords and MFA optional sets up customers to take the fall when a company's lax cybersecurity empowers cybercriminals to hack into the company's network and steal data.

LastPass should not get a free pass just because some customers did not follow the company's "password best practices." A cybersecurity company that promises to keep your passwords and metadata safe should not be wagging a finger in your direction when their network and your data have been breached—and practicing "good password hygiene" should not be a cynical legal tactic to shield a company from this responsibility.

But tell that to 23andMe, a consumer genomics company that blamed its customers for a massive but preventable data breach. In April 2023, cybercriminals accessed about 14,000 customer accounts using stolen, reused passwords in a credential stuffing attack. Amplifying the breach by an order of grievous magnitude, the cybercriminals stole data from an additional 6.9 million customers via the DNA Relatives tool, a service letting customers share data with genetic relatives.¹⁵

In October, the cybercriminals brazenly posted a sample of the stolen data on BreachForums, a shadowy marketplace where hackers traffic in stolen data, turnkey phishing kits, and even porn. The sample posted on BreachForums was massive, containing data from 1 million people with Jewish Ashkenazi ancestry.¹⁶ It's anyone's guess why cybercriminals culled the data of Ashkenazi Jews to be publicly outed on BreachForums. Still, it's a good bet the motive was more sinister than merely giving 23andMe the finger. Ashkenazi Jews have been historically mistreated, so posting their stolen data may have been a form of racist cyber-persecution, or the publication may have been symbolic to demonstrate the cybercriminals' alignment with anti-Semitic groups. It's also possible the cybercriminals believed that Jewish Ashkenazi data was more valuable for phishing scams, identity theft, and other cybercrimes than other demographic datasets in their possession. Or advertising the Jewish Ashkenazi data was nothing more than a garish publicity stunt showcasing the cybercriminals' considerable hacking skills. So yeah, maybe it was about bragging rights.

Whatever the reason for publishing such a massive trove of Jewish Ashkenazi data—and base case, we can agree the cybercriminals were schmucks—the October 2023 BreachForums post was an ear-bursting alarm bell warning the public, and 23andMe, about the cyberattack. Let's do the math here: About 14,000 customer accounts were breached in April, and the breach was not discovered by 23andMe until the October posting of Jewish Ashkenazi data on BreachForums. That means the cyberattack went undetected for five long data-stealing months.

It also means that if 23andMe had credential stuffing detection software, it was no match for the skills of wily cybercriminals.

Oh, and while the cybercriminals were hacking the living daylight out of 23andMe for five long data-stealing months, they exploited the DNA Relatives feature to engorge themselves on a heaping helping of data from another 7 million customers.¹⁷ Pause—deep breath now—the original hack occurred because 14,000 customers used a password for 23andMe that they reused somewhere else; this reused password was compromised in an unrelated breach and stuffed by cybercriminals into the 23andMe accounts; credential stuffing with reused passwords was a proximate cause of the initial cyberattack on 14,000 customers. But, here’s the thing: Reused passwords had nothing to do with hacking into the data of an additional 7 million customers. Okay—time to exhale—an additional nearly 7 million customers got hacked not because they carelessly reused their passwords but because 23andMe seemingly allowed lateral movement within the DNA Relatives feature, allowing the cybercriminals to scrape connected accounts.¹⁸

Another thing: At the time of the cyberattack, 23andMe provided multifactor authentication (MFA) to customers only as an option; it was not mandatory. Instead of being automatically enabled and required as a condition of becoming a 23andMe customer, MFA was left up to the customer as a choice. MFA is a key countermeasure to credential stuffing attacks because it requires a one-time numerical code to access an account; so even if cybercriminals have a stolen, reused password, they’re out of luck when MFA is enabled. Yet, 23andMe chose customer convenience over cybersecurity by making MFA optional only.¹⁹

By now, one would think that 23andMe, chastened and humbled, would collapse to its figurative knees, accept responsibility, and beg forgiveness for this heinous, massive breach.

Given the plethora of internal controls and anti-hacking countermeasures that could have prevented the cyberattack—but either weren’t implemented or effective—it’s a no-brainer that 23andMe would issue a press release apologizing for the incident and accepting full responsibility. The press release would not blame customers for the cyberattack; instead, 23andMe would lay the blame squarely on the cybercriminals while providing full transparency about the company’s lax internal controls that contributed to the incident. A full accounting of the lax controls would include failure to detect the credential stuffing attack for five long data-stealing months, failure to make MFA mandatory, and failure to implement controls to prevent lateral movement and mass data scraping by hackers accessing the DNA Relatives feature. Finally, 23andMe would promise not to assert customer fault (or contributory negligence) as a defense to any class action lawsuits or government investigations. Upon issuing the press release, the company’s C-suite leaders would give each other high fives, their faces shining with integrity, and 23andMe would become a worldwide role model for how companies could be wise stewards of their customers’ sensitive data even in the face of a devastating cyberattack.

We should all be proud that 23andMe acted with integrity by taking the moral high ground and handling a difficult situation responsibly and with sound, ethical judgment—right?

Um, well, darn. Just like LastPass, 23andMe lawyered up. And just like LastPass, 23andMe gave their customers a roundhouse kick to the groin. The lawyering was so aggressive you’d think the company’s customers were the cybercriminals who hacked 23andMe and not innocent victims whose data was stolen. However, in the boardrooms of hacked companies like 23andMe, customers are seemingly not victims but potential plaintiffs who need to be pummeled without mercy by legal and PR teams well-practiced in the finger-pointing art of corporate blame-

shifting.

Blame shifting is the term I use to describe a sneaky, nuanced form of victim blaming. When the victim of a cyberattack is a customer, the company often points the finger at the customer to avoid legal, financial, and ethical accountability for the cyberattack. The company may be flinging daggers not only at customers but also toward the employees of the company itself.

Revisiting the LastPass breach, the company not only blamed customers for using weak passwords but even pointed its finger at an employee, stating that a later breach resulted from a DevOps engineer failing to install a patch to a “vulnerable third-party media software package,” enabling a threat actor to deploy keylogging malware on the employee’s home computer.²⁰

Okay, so the remotely working DevOps engineer didn’t install a Plex patch. However, did LastPass have a patch management program that didn’t rely on individual employees? If so, apparently it wasn’t effective. Also, the unfortunate DevOps engineer was likely not a cybersecurity professional, so why did LastPass put the onus on the engineer to install the patches? Didn’t LastPass have WFH technical controls? WTF!²¹

LastPass goes beyond managing passwords. It’s a cybersecurity brand built around keeping people safe online. What then was going on with LastPass’s internal culture of cybersecurity? Did LastPass have an effective cybersecurity program on the eve of its disastrous data breach? Was the company lacking anti-hacking countermeasures, or were controls in place but misconfigured? Whatever the answer might be, LastPass shifting the blame to its customers smacks of a panicky attempt to deflect from its own mistakes.

Although LastPass is no example of profiles in courage, the award for craven cowardice goes to—drumroll, please—the DNA testing and analysis company, 23andMe.

With gobsmacking arrogance, when confronted with dozens of class action lawsuits, 23andMe blamed 14,000 customers who were victims of the initial credential stuffing attack, as well as nearly 7 million customers who were in the line of fire when the hackers exploited the DNA Relatives platform.

In a letter sent to lawyers representing the customers whose data was stolen, 23andMe attorneys lambasted the 14,000 victims of the data breach, declaring in a raucously bold and underlined headline that “**No Breach Occurred**” and blaming them for reusing their passwords:

23andMe believes that unauthorized actors managed to access certain user accounts in instances where users recycled their own login credentials—that is, users used the same usernames and passwords used on 23andMe.com as on other websites that had been subject to prior security breaches, and users negligently recycled and failed to update their passwords following these past security incidents, which are unrelated to 23andMe.

Therefore, the incident was not a result of 23andMe’s alleged failure to maintain reasonable security measures under the CPRA.²²

Translating from legalese, 23andMe is asserting that it didn’t matter whether the company failed to detect the cyberattack for five months, or that 23andMe seemingly allowed the cybercriminals to scrape data from the DNA Relatives feature through compromised accounts, or that the company did not require MFA and automatically enable this powerful countermeasure for its customers. None of this matters, according to 23andMe, because the customers “negligently” reused their passwords and “failed” to update their passwords. Yikes, pretty soon,

23andMe will be referring to its customers as “slaughtered pigs”!

Sadly, the blame shifting only gets worse. Next, 23andMe goes after the nearly 7 million innocent folks who got pwned because cybercriminals were able to exploit the DNA Relatives platform. But, these customers were utterly blameless. There’s no evidence they reused their passwords; were phished; or used weak, easily guessable passwords. The only reason their data was stolen is that once cybercriminals hacked the initial 14,000 accounts, they used those accounts to access the DNA Relatives feature and scrape data from connected profiles. How could any of this possibly be the fault of those 7 million customers? Isn’t it the responsibility of 23andMe to ensure its network is secure and that hackers can’t scrape massive amounts of sensitive data through features like DNA Relatives?²³

Nope, not according to the letter from 23andMe attorneys, which said, underneath the still vociferous “**No Breach Occurred**” headline:

Equally important, the information that was potentially accessed cannot be used for any harm... Additionally, the information that the unauthorized actor potentially obtained about plaintiffs could not have been used to cause pecuniary harm (it did not include their social security number, driver’s license number, or any payment or financial information).²⁴

In one fell swoop, 23andMe lobs a fiendishly cynical blame-shifting pipe bomb. Since the data did not include social security and driver’s license numbers—or payment or financial information—the data theft is no biggie; after all, how could cybercriminals harm customers without this key data? Ah, but 23andMe neglects to mention in the letter that the stolen data included customer names, birth years, ancestry reports, location, relationship labels, and the percentage of DNA shared with relatives. That’s a boatload of personal data, and it’s easily weaponizable. Hackers could use it to launch targeted phishing attacks, steal someone’s identity, and commit numerous social engineering frauds.

This is a dreadfully harmful data breach, yet 23andMe winds up for the pitch and throws the *No Risk of Harm* curve ball with a wink and a smile.²⁵ That’s some serious blame shifting, so let’s explore this legal canard for the red herring it is (see what I did there? Two fancy words meaning “baloney!” in one sentence).²⁶

Typically, a company rocked by a cyberattack will default to blaming the users for the breach; but the second go-to blame shift is contending that the breach is no big deal because no one could ever be harmed by the stolen data. It’s hard for me even to write that last sentence because there is no such thing as a benign data breach. It’s such a ridiculous assertion. But the fact is that 23andMe’s legal counsel is doing a spot-on imitation of *The Simpsons*’ Cletus the Slack-Jawed Yokel, who leans back on a Skoal-stained rocking chair, with a jug of moonshine at his feet, and drawls, “Aw shucks, Ah reckon this lil’ ole data breach ain’t gonna hurt nobody none!”

In basketball, “no harm, no foul” means that even though a player broke the rules, it didn’t affect the game’s state of play or outcome, so the referee doesn’t call a penalty. Also known as the *No Harm, No Foul* defense, it’s a company’s way of deflecting blame from itself and onto an ambiguous legal concept that goes like this: “Yessiree, our customers’ data was stolen, but the data was so innocuous that cybercriminals cannot weaponize it; therefore, it’s impossible for our customers to be financially injured; and, just like in basketball, if there’s no harm, there’s no foul

—which means, gosh darn it, that there was no data breach!”

The No Harm, No Foul defense is obvious BS, but it’s widely used by defense attorneys because the basketball analogy is so cornpone down-to-earth it’s insidious; after all, if the data is harmless, then there’s no injury; and if there’s no injury, why penalize anyone? And if you’re not going to punish anyone, then there’s no culpability—and, if there’s no culpability, gosh darn it, there is no breach!

And guess what? Judges are buying this malarkey. In the United States, federal courts require plaintiffs to prove actual or imminent harm to have *standing* to file a lawsuit. Standing means the plaintiff must show three things: They suffered an actual injury, caused by the defendant, and the harm is redressable by a court decision. But, in *TransUnion v. Ramirez* (2021), the Supreme Court ruled that the future risk of harm doesn’t count as injury. And, in *Greenstein v. Noblr* (2024), the Ninth Circuit dismissed a case because the plaintiffs couldn’t show their data was misused or that any harm was traceable to the breach.²⁷

Together, the two cases established *traceability* as a requirement for breach victims to prove an injury was caused by the defendant. But, let’s be real—traceability rigs the game in favor of hacked corporations over breached victims. It’s nigh-impossible for victims to show traceability when multiple breaches occur, especially when victims’ data is sold on the lawless wilderness of the Dark Web, and the damage surfaces years after the breach.²⁸

Traceability is a legal red herring that assumes cybercriminals leave a clear trail of breadcrumbs, like in an episode of *CSI: Cyber*—that’s not how real-world cybercrime works, yet breach victims are finding that federal courts are more than eager to impose this absurd legal fantasy. As reported by *The Wall Street Journal*, the law firm Duane Morris gathered data showing that, between January and September 2025, federal judges granted nearly 70 percent of motions to dismiss data breach claims.²⁹

It turns out that traceability is a great way for judges to remove the deluge of privacy cases from their dockets. A judge dismissed a case against Mississippi-based Singing River Health System, which lost 900,000 patient records in a ransomware attack, ruling that “mere exposure of private information” is not, by itself, an injury.³⁰ Another judge dismissed a case against Kyocera AVX, a manufacturer of electronic components, involving the breach of personal data for 39,000 individuals.³¹ In dismissing the case, the judge said in a ruling that “the mere theft” of personal data didn’t meet the definition of harm.

This is deeply troubling. In both the Kyocera and Singing River cases, the federal judges’ use of the word “mere” is shockingly tone-deaf to the magnitude of breaches involving tens of thousands of victims. Words like “mere” not only matter; they sometimes reveal a deeper truth—that when it comes to data breaches, judges are profoundly out of touch with the reality faced by the people whose personal data was exposed through no fault of their own. When 70 percent of cases are dismissed under a No Harm, No Foul standard, it means that thousands—or even millions—of breach victims are denied relief until after their data has been exploited. It’s like officiating a drag race between a cybercriminal and a victim, but giving the cybercriminal a head start when the whistle blows. Even worse, the data has probably already been exploited, so dismissing a breach case is like handing the cybercriminal brass knuckles while shackling the victim to a post. Let the beatings begin!

No Harm, No Foul might work in basketball, but when a breach hits the fan, it’s a technical foul to let corporations off the hook while victims get benched. First, there is no such thing as

harmless data. Any stolen data can be weaponized by cybercriminals. We live in an age of phishing attacks, identity theft, revenge porn, victim blaming, ransomware, and deepfake scams. It's about time we dump the notion that there are two types of data—harmful data like SSNs and benign data like...well, I can't think of any *safe* stolen data. Can you?

Second, it doesn't matter whether stolen data is harmless and immune from criminal exploitation. The bottom line is that the breached company failed to implement anti-hacking countermeasures to prevent the cyberattack. And for that, and that alone, companies should not be able to cry, "No harm, no foul!" in the throes of a devastating cyberattack. When a breach hits the fan because a company failed to enable MFA, allowed lateral movement within its network, or didn't patch a known vulnerability, it's downright disrespectful—and shameful—for the company to blame its customers for the breach.

The No Harm, No Foul mentality is insidious because it undermines corporate accountability. When companies know it's a slam dunk to get a case tossed, no matter how destructive the breach, there's little incentive to proactively safeguard sensitive data. This legal mumbo jumbo is just a slick way of saying, "Big Breach, No Accountability." And anyone who says otherwise should be permanently benched.

In our hyper-digital age of cyberwar, deepfake scams, and ransomware, the No Harm, No Foul defense amounts to a corny vaudeville gag that's no longer funny. Companies that continue to invoke this legal head fake should be laughed out of court. And if courts keep ruling "no harm, no foul," the public must boo so loudly that they rattle the stands, because if we don't cry foul, this game stays rigged.

Though 23andMe's first pipe bomb uses twisted logic, at least its specious claim can be understood in the context of the basketball metaphor. The same cannot be said about the company's second pipe bomb, which explodes like a Molotov cocktail on the roof of a car, leaving a chaotic mess of convoluted lexicon and unanswered questions:

As explained in the October 6, 2023 blog post, the profile information that may have been accessed related to the DNA Relatives feature, which a customer creates and chooses to share with other users on 23andMe's platform. Such information would only be available if plaintiffs affirmatively elected to share this information with other users via the DNA Relatives feature.³²

Let's unpack this two-sentence glob of legalese. The DNA Relatives feature is optional, as customers "choose to share" information with others. Also, by opting in to use this voluntary platform, customers consent to share their data with other customers using the feature. Therefore, customers who opt in to DNA Relatives accept all potential risks inherent in using the feature. Now stay with me here because this is 23andMe's implied money shot: Because data could only be stolen if the customer elected to opt in to the DNA Relatives feature, then it's actually the customer's fault that their data was stolen!

It boggles the mind, but in a mere two sentences, 23andMe makes the galling assertion that once a customer signs up to use the DNA Relatives feature, it is tantamount to an "acceptance of risk." Hence, there is no breach, which means we can bottom line the second pipe bomb with the precision of a sniper's rifle: 23andMe has no liability to nearly 7 million breach victims because they voluntarily opted in to the DNA Relatives feature.

It's just like Cletus the Slack-Jawed Yokel of *Simpsons* fame might say: "Well shoot. If ya

done opted into that DNA doohickey, guess it's yer own dang fault yer data got snatched, ain't it?" But before you take a swig of Kentucky moonshine to calm your frazzled nerves, keep in mind that 23andMe's feeble attempt at blame shifting backfires like Cletus's sputtering F-150. First, it's 23andMe's responsibility—not the customers'—to implement effective countermeasures to prevent lateral movement (and data scraping) in its systems. Second, customers who opted in to DNA Relatives likely were not provided clear warnings about potential cybersecurity risks, and unless there were clear warnings about these risks, then *informed consent* was not given. Third, it's Mad-Hatter ridiculous to contend that a company's duty to protect their customers' data goes poof once the customer opts in. Fourth, blame shifting to customers is just another form of victim blaming, which deflects society's focus away from the cybercriminals, the crime itself, and the company's accountability.

Companies rocked by cyberattacks should view the blame-shifting fiascos of LastPass and 23andMe as cautionary tales rather than a legal playbook. Corporate strategy for managing a data breach should emanate from C-suite leadership and be led by the Chief Privacy Officer and Chief Information Security Officer, not the legal department. Blame shifting to customers is a dreadful PR nightmare, but a massive data breach is better managed with accountability, transparency, and, above all, compassion. After all, the company is a victim, too, and a healthy measure of respect for its customers (and employees or other users) will place the blame where it should be: on the cybercriminals.

The LastPass and 23andMe blame game fizzled like a damp squib with the general public and received withering criticism from the cybersecurity community; however, it does not mean that customers are never at fault for data breaches. The problem with blame shifting is the all-or-none strategy of placing accountability for the breach 100 percent on the users and 0 percent on the company. But we must remember there are two victims of a cyberattack: the victims whose data was stolen (i.e., customers, employees, or other users) as well as the company whose network was breached. Just as it's not fair to blame the users 100 percent, it's also unfair to abrogate user accountability and slam the company. After all, the real villains are the cybercriminals who launched the attack, so our focus should be on the hackers and attack methods used rather than pointing fingers at the company and the users, both of whom are victims. Remember that blame shifting goes two ways. Just like LastPass and 23andMe placed all of the blame on their customers, it's also blame shifting to say, "The customer is never at fault for breaches!" Yes, Virginia, sometimes you can blame the user!

Let's consider a few scenarios. Imagine an employee who opens a malicious attachment in a phishing email, allowing malware to install on their computer and potentially spread through the company network. Now, let's imagine that the phishing email was really solid work by master cybercriminals and looked like a legitimate email from the Human Resources department. Should the company discipline the employee? My answer would be no, especially if the employee made no prior mistakes. After all, cybercriminals have a playbook and the resources of organized crime, and one lone employee is no match for an adversary of that magnitude. Also, it's up to the IT department and the cybersecurity team to ferret out phishing with anti-spam software and train employees not to fall victim to phishing scams. If a phishing email got through the company's anti-spam software, then blaming the employee for being tricked is not fair.

Ah, so then we should blame the IT department? Maybe fire the CIO or CISO? Well, not so fast—they, too, are up against master cybercriminals resourced by organized crime and even

nation-state threat actors. Can we really expect the IT department to battle Russia, North Korea, China, and Iran all by its lonesome?

Plus, the sheer volume of cyberattacks means the odds woefully favor the cybercriminals because they can launch phishing attacks 24/7/365 and only need to scam one employee with a phishing email to win. But your beleaguered IT department must repel 100 percent of the cyberattacks *every single time* to win. In a company with thousands of employees, the IT department is outmanned and outgunned by wily cybercriminals with an army of botnets and time on their side. It doesn't seem fair to blame IT for that one, does it?

However, there are many times when employees screw up so badly that they must be held accountable. Some non-cyber examples are instructive: A truck driver smokes weed while making deliveries; an accountant misses a deduction leading to a high tax payout; a cop arrests a suspect without reading Miranda rights; a stockbroker places a trade without the clients' permission; or a CFO cooks the books leading to investigations and collapse of the company.

The employees in these examples deserve to be held accountable for their behavior. Employees who are negligent or willfully ignore company policy, breach a fiduciary duty, or engage in illegal activity are fair game for disciplinary action—or even a stiff jail sentence. The same goes for people with access to a company's information system; customers, employees, or any user should be held accountable for gross negligence or reckless behavior.

There needs to be balance, and in the world of healthcare, that balance is a *Just Culture*.³³ Many hospitals implement a Just Culture program to create *shared accountability* between the hospital and its employees, making the hospital responsible for policies and systems and the employees accountable for informed decisions. In a hospital, a Just Culture leads to improved patient safety, transparent reporting of errors and near misses, and employee satisfaction. In a Just Culture, employees who make honest mistakes are counseled and consoled, not disciplined. After all, the employee is likely distraught over a near-miss safety issue, and the hospital can teach others so the mistake doesn't repeat. On the other hand, even in a Just Culture, employees are still disciplined for reckless behavior (e.g., intentionally not following safety protocols) or illegal behavior (e.g., paying kickbacks to physicians in return for patient referrals).

A Just Culture is a great concept that can be applied to eliminate blaming the user when a company suffers a destructive cyberattack or massive breach. An accountant who accidentally clicks on a phishing link should be consoled, but a lawyer who gets phished six times per year despite intensive training is at a high risk of a massive data breach. An IT analyst who forgot to install a patch can be given a break, but an IT engineer who willfully installs banned software should be disciplined. An HR director who accidentally signs a vendor-friendly contract before Legal approves it should be retrained, but a CFO who provides kickbacks to vendors should be reported to authorities and arrested.

And now let's come back to 23andMe. You see, although the company royally screwed up by blaming their customers for the data breach, there could have been another outcome had the company applied Just Culture principles. For the 14,000 victims, 23andMe could have acknowledged a shared responsibility with its customers. The infamous 23andMe blame-shifting letter could have pointed out that its customers reused their passwords while acknowledging the company's responsibility to better train its users on password hygiene practices, mandate MFA, implement systems to catch credential stuffing attacks, and, for the nearly 7 million victims, 23andMe could have acknowledged its responsibility to prevent lateral movement in the DNA

Relatives feature.

Companies like LastPass and 23andMe deserve harsh criticism when they 100 percent blame their users. Sure thing—finger-pointing is human nature, particularly when companies face class action lawsuits and hyperaggressive lawyers trying to justify \$400-an-hour legal fees. However, executives must resist blaming their users, keep their forefinger in their pockets, and accept shared responsibility for cyberattacks and data breaches. For both the breached company and its users, blame shifting is a two-way street; it's not reasonable to blame the users entirely, but neither is it fair to throw the company under the bus. The cure for blame shifting is shared accountability, and you only get that in a Just Culture.

CONCLUSION

Smashmouth Cybersecurity—Never Get Pwned Again!

It's depressingly axiomatic that world governments are unable to apprehend the vast majority of cybercriminals; as a result, cybercrimes will continue to escalate, and cyberattacks will become more destructive. When cybercriminals know they can't be caught, they have no incentive to stop launching cyberattacks. With impunity comes arrogance, and given law enforcement's inability to nab a world awash in cybercriminals, I'm afraid the black hats' arrogance is justified.

If it's impossible to catch cybercriminals *en masse*, then there's only one solution to slow the pace of cybercrime. It's not as satisfying as catching cybercriminals and throwing them in jail, but individual cyber awareness can stop a cyberattack dead in its tracks. Cybercriminals are aggressive, so our philosophy of individual cyber awareness must be similarly tenacious and uncompromising. Likewise, national and corporate cyber awareness programs must be implemented that are hard-hitting, provide actual experience with the technologies and tricks deployed by cybercriminals, and, perhaps most importantly, they must be permanent.

We are now in the age of executive accountability for cyberattacks, so the C-suite must be significantly more involved in cybersecurity oversight than they have been in the past. The C-suite needs to ensure the company has an effective cybersecurity program, and this means the C-suite must understand basic cyber hygiene principles and common cyberattack threat vectors and not just hand off cybersecurity to a top-notch CISO. The threat is dire, so C-suite leaders must protect their company, employees, and customers by implementing an aggressive, hard-hitting smashmouth cybersecurity awareness program. By transforming the workforce into an army of vigilant Cyber Mavens, companies can foil even the most determined cybercriminals and prevent cyberattacks from being an existential threat to the company's business.

It seems pretty straightforward: To deter cybercrime, you must apprehend, convict, and jail cybercriminals. Yet, despite the rare government press releases bragging about the conviction of a high-profile hacker, the vast majority of cybercriminals gleefully launch cyberattacks in complete anonymity. Until world governments can identify, capture, and neutralize cybercriminals, deterrence will remain a hoped-for but unrealized dream.

Cybercrime is a global pandemic because cybercriminals rarely get caught. If you can't slap on the handcuffs and throw them in jail, then ipso facto, you can't deter them. And if you can't deter them, then ipso facto redux, cyberattacks will continue to mushroom in frequency and impact.

I am depressingly skeptical that law enforcement will ever be able to counteract the many advantages cybercriminals enjoy, allowing them to evade capture. Cybercriminals operate with near-total impunity and will always do so, which means deterrence is not an achievable dream, but an implausible fantasy that will never happen.

Sigh. What a buzzkill.

However, arresting and convicting cybercriminals is only one form of deterrence. You can also dissuade hackers by being such a hard target that the cybercriminals are stymied. All it takes is thwarting one cyberattack at a time, and you can do this by embracing Smashmouth Cybersecurity and becoming a Cyber Maven. Sure, you'll still get a boatload of phishing emails—that's never going away—but you'll be savvy enough not to answer a fake survey or click on a malicious attachment. You'll also be wise to romance scams, USB drop attacks, evil portals, shoddy and slick deepfakes, and the pernicious threat of the liar's dividend.

Below are the eight core attributes of a Cyber Maven:

1. **Practices good cyber hygiene.** Cyber Mavens use a password manager to create strong passwords (at least twenty-five characters with a mix of uppercase and lowercase letters, numbers, and symbols) that are never reused or shared. Cyber Mavens know that reused passwords are dangerous. If they're compromised in a breach, cybercriminals could spray them across different websites and launch a credential stuffing attack. Cyber Mavens are obsessed with cyber hygiene: They always use multifactor authentication, routinely install patches, encrypt every single one of their devices, and back up their data like it was spun gold.
2. **Bursting with cyber-savvy.** Cyber Mavens are bursting with *cyber-savvy*, a term I use to describe the dual pillars of cybersecurity knowledge: practicing good cyber hygiene and staying wary of common attack vectors. An *attack vector* is the method a cybercriminal uses to exploit system vulnerabilities—think brute force and credential stuffing attacks on weak passwords, zero-day exploits on unpatched software, and phishing scams designed to steal credentials or infect networks. Cyber Mavens understand that knowledge not only equals power but also paranoia, which is why they're such sticklers for cyber hygiene. One without the other leads to apathy, then carelessness, and before you know it, the Cyber Maven becomes a pwned noob. Vigilance against attack vectors reinforces hygiene habits and will make you cautious—even paranoid—about clicking on that phishy link in an email. That gnawing paranoia might be the very thing that thwarts a cyberattack.
3. **Knows the tools of hacking.** Hacking tools are not evil. It's the person wielding them that's the X factor. Using a Wi-Fi Pineapple for pentesting is a good thing, but deploying it to conjure up an evil portal to pwn someone's username and password is nefarious. Fortunately, hacking tools like the Wi-Fi Pineapple and the Rubber Ducky lose their power when launched against a Cyber Maven. That's because Cyber Mavens are in the know about the tools of hacking, so when they find a USB drive nestled on the carpet in the company foyer, they don't reflexively stick it into a computer port; instead, they report it to the cybersecurity department. When Cyber Mavens hang around a coffee shop for a cappuccino and a bagel, they're wise to the sorcery of the Wi-Fi Pineapple and the curse of an evil portal; that's why they're on the lookout for any signs it's a fake phishing

portal (misspellings, wrong URL, no HTTPS, etc.). Cyber Mavens know that technology is not mysterious. A Wi-Fi Pineapple is just a fricking souped-up router masquerading as a friendly Wi-Fi access point, and the Rubber Ducky is nothing more than a USB drive reprogrammed to type malicious commands. There is no magic, just trickery, and because Cyber Mavens know what's behind the curtain, they don't fall for a cybercriminal's sleight of hand.

4. **Views QR codes with suspicion.** Cyber Mavens know that scanning a QR code can lead them to a phishing site designed to trick them into entering their credentials or downloading a malicious app containing malware. If you think Cyber Mavens are paranoid about phishing emails, they're off the charts when it comes to QR codes. Cyber Mavens know random is bad, so you'll never see them scanning a QR code from a lamppost or a parking meter—and you can bet your last Bitcoin they'd never scan a QR code slapped on a bathroom stall (not only is it risky, it's gross!). When Cyber Mavens do scan, they make sure it's from a trusted source and hasn't been tampered with. Companies take note—if you want to win over a Cyber Maven, don't lean too heavily on QR codes as your primary marketing strategy.
5. **Knows how to spot a deepfake.** Shoddy deepfakes are no match for Cyber Mavens, and even slick deepfakes fall by the wayside when trying to pwn a Cyber Maven. Cyber Mavens easily catch on when an audio or video is riddled with flaws, such as out-of-kilter facial features or a robotic-sounding human voice. But when a person does something in a video that they would never say or do in real life, that's when a Cyber Maven's BS meter kicks into high gear. Even the best deepfakes on the planet are sussed out by skeptical Cyber Mavens who know an easy way to expose a deepfake voice scam is to simply call the real person back. Cyber Mavens are never tricked by con artists deploying the liar's dividend, as Cyber Mavens curb their inner Chico Marx and are aware of their own internal biases. Cyber Mavens are skeptics—they accept the existence of real evidence while being suspicious of nutty claims not supported by the facts. Cyber Mavens are not impressed by the seductive allure of the liar's dividend.
6. **Knows the telltale signs of romance scams.** Jilted catfishers shed crocodile tears when they're kicked to the curb by Cyber Mavens who are well-versed in the telltale signs of a romance scam. Cyber Mavens never respond to messages from strangers coming out of the blue. They are wary when a cyber-sweetie pressures them to communicate with an anonymous messaging app, and they freak out when the conversation turns to money. Cyber Mavens catch on quickly when a scammer tries to mirror them, and they cast a jaundiced eye at cyber-sweeties who live far away, break their promises, make romantic moves at warp speed, or ask for money transfers that are untraceable. Oh, and one more thing—calling a Cyber Maven “Pookie” is the fastest way to being ghosted!
7. **Abhors victim blaming.** Cyber Mavens revile the phrase “Pig Butchering” as a cruel metaphor that unfairly blames the victim of a cybercrime. Cyber Mavens never use the term, preferring the phrase romance baiting or crypto-romance scam. Cyber Mavens always support the victim and stand up to internet trolls and cyberbullies. When confronted with language that blames the victim, Cyber Mavens deploy lingo-shifting

techniques to change the victim blaming paradigm and place accountability on the cybercriminals and the methods used in the cybercrime. When a social media troll posts, “I can’t believe that doofus fell for such an obvious scam,” a Cyber Maven will retort, “The victim suffered a crime, so it’s not the victim’s fault.” Cyber Mavens love nothing better than delivering a hellacious curb stomp to craven guilt shifters who lob childish, victim-blaming insults while hiding behind their anonymity.

8. **No Blame-Shifting Zone.** Cyber Mavens rightly dress down companies that blame their customers (or employees) for cyberattacks while also appreciating the importance of user accountability. Blame shifting is a two-way street, so just as it’s unfair to blame the user entirely, it’s wrong to believe that the user is never at fault for breaches. Cyber Mavens support a Just Culture in which the company and its users have a shared accountability to repel cyberattacks.

At the micro level, individuals who practice Smashmouth Cybersecurity not only protect themselves and their families from cybercrimes, but they also help society at large by thwarting one cyberattack at a time. When nations are unable to band together to toss cybercriminals into the dank, unforgiving walls of a jail cell, individuals have no choice but to stand up for themselves and not rely on politicians and governments to thwart cyberattacks. But just because the flailing international response to cybercrime is forcing individuals to become mighty Cyber Mavens doesn’t mean governments don’t have a powerful role to play in championing cybersecurity. At the macro level, nations should also practice Smashmouth Cybersecurity by launching aggressive cyber awareness training for government and corporate personnel amidst a vigorous—and permanent—national cyber awareness campaign aimed at the general public.

Because the only “bad” USB is a malware-engorged USB stick in the hands of a cybercriminal, a national Smashmouth Cybersecurity initiative puts hacking tools in the hands of the public, teaching them about the Wi-Fi Pineapple, Rubber Ducky, and other hacking tools, like the newest kid on the block, the *Flipper Zero*. This open-source hacking tool—brandishing a cute, smiling dolphin on the orange LCD—is the Swiss Army knife of ethical hacking.¹ The Flipper Zero can open locked garage doors, change the prices on gasoline signs, and ring doorbells; you can also link the Flipper Zero to a USB drive and run Ducky Scripts, turning it into a BadUSB. Even though the Flipper Zero looks like a LEGO gadget made for teenagers, the dolphin-themed device is not a toy—it’s a powerful hacking tool that could wreak havoc in the hands of a cybercriminal. That’s why it’s so essential for the public to get their fingernails dirty with these powerful devices. They need to see them and touch them to understand and thwart them.

Watching demos showing these hacking tools deployed in the wild is an excellent way for people to learn how to thwart these devices and prevent a cyberattack. Once a person actually sees how an MITM attack is perpetrated with a Wi-Fi Pineapple, they’ll never fall for it, and the Wi-Fi Pineapple becomes a worthless piece of junk in the cybercriminal’s tool kit. When people see what happens when a BadUSB is connected to a computer port, why on earth would they ever do the same with a randomly found USB abandoned in their company’s carport? Talking to people about hacking tools in the abstract doesn’t do the trick. They need to see these devices in action to drive home the cyber risk they face from BadUSB-wielding cybercriminals. That’s why a core component of a Smashmouth Cybersecurity training program is a deep dive into hacking

tools, with a philosophy that these tools must be seen and touched by company employees and the general public in order for the training to be truly effective.

Cyberattacks are a worrisome fact of life, so individual cyber awareness bolstered by national and corporate cybersecurity training must become part of our personal and work lives. After all, if the vast majority of cybercriminals are uncatchable and unstoppable, then it will be up to a legion of fighting-mad Cyber Mavens to thwart them.

Expanding further upon the philosophy of Smashmouth Cybersecurity:

1. Hacking tools in the hands of cybercriminals are dangerous, but when used by ethical hackers, they are a beacon of hope, and when understood by the general public, hacking tools can be easily thwarted.
2. Hacking tools should be well-known by the public, not feared, and banned. Hacking tools can be used by pentesters to help companies find and correct vulnerabilities, enhancing cyber resilience. Hacking tools can also be used by ethical hackers to prove (or disprove) company claims that their products are secure. Finally, hacking tools can be used as part of company-wide cyber awareness training to teach employees how to protect themselves.
3. The democratization of hacking tools cannot be reversed, and making them illegal will drive them underground, further into the hands of threat actors. That's why company employees and the general public should be educated on the dangers of hacking tools and the countermeasures that defeat these devices.
4. Where possible, training includes live, hands-on experience with hacking tools so these devices are no longer esoteric underground tech but instead become part of the zeitgeist of mainstream cyber awareness.

A Smashmouth Cybersecurity training program also deals with the threat of deepfakes, the peril of malicious QR codes, and perhaps the most traumatic cyberattack of all: the scourge of romance scams and the victim blaming that follows. But Smashmouth Cybersecurity doesn't stop there. Indeed, a Smashmouth Cybersecurity training program covers a variety of scams and cyberattacks, even drilling down to risks specific to certain industries, such as banking and healthcare. In short, Smashmouth Cybersecurity is not "one size fits all" but can be tailored to the needs of a particular company or industry.

With Smashmouth Cybersecurity, cyber awareness training is hands-on, in-your-face, and hard-hitting. Just like with hacking tools, Smashmouth Cybersecurity training should provide employees and the public with actual demonstrations of deepfakes, QR code attacks, and crypto-romance scams. When people see a deepfake in action, it resonates more than a mere case study. Watching a man-in-the-middle attack carried out with a Wi-Fi Pineapple or seeing a romance scam in action helps people internalize the danger and be more vigilant in their own lives.

I wrote *CTRL+ALT+PWN: The Hacker's Playbook (And How to Beat It)* to help the public

understand the dark arts behind hacking. When the technologies, scams, and tricks of hacking become mainstream, cybercrime will become less opaque, and people will learn how to defend themselves.

While I fervently hope that world governments will come together and create legislation and programs to identify and capture cybercriminals, I am skeptical it will ever happen. Too many countries actually support cybercrime as long as it is directed against their enemies (Russia, if you're listening: I am pointing the finger at you!).

I'll concede that deterrence by Cyber Mavens is not as gratifying as the violent cop Harry Callahan blowing away the hoodlums with his .44 Magnum in Clint Eastwood's 1971 noir thriller *Dirty Harry*. However, it's a step in the right direction, and it's nonviolent (Dirty Harry will have you know that a .44 Magnum is the most powerful handgun in the world and can blow a person's head clean off!).² Most importantly, when cybercriminals know they'll never be caught, thwarting cyberattacks by minting a legion of Cyber Mavens is our only deterrence.

In the age-old battle between cops and robbers, when it comes to cybercrime, the robbers are winning. I'm afraid the only chance we have to deter cybercriminals is by thwarting cyberattacks with tried-and-true cyber awareness and battle-tested cyber hygiene. Anything else is merely avoiding a destructive cyberattack by pure dumb luck. If you're not willing to become a Cyber Maven, then you've gotta ask yourself Dirty Harry's cynically rhetorical question (typically asked with a .44 Magnum squarely pointed between the villain's eyes): "Do you feel lucky?"

Well, do ya, noob?

Bad Day at the Zero Day Café: Your humble author is using the free Wi-Fi at his favorite coffee shop to check his online bank account without a VPN. Or am I? Is it possible that I used Google Gemini's Nano Banana Pro to create this image? How can you tell if this image is AI-generated? And while you're at it, do you see any cybersecurity threats? How would you thwart those threats? What hacking myths do you see that need debunking? If you can answer these questions, you just might be a Cyber Maven!



ACKNOWLEDGMENTS

I'm verifiably human and not an avatar, bot, or AI. When you read my book, the writing is mine, and not a chatbot's. Like any mortal, I make mistakes—and let me tell you, when I screw up, they tend to be doozies! Worse, I took it upon myself to write a book about hacking, even though I'm not a hacker. I even played around with a few hacking toys, like the Wi-Fi Pineapple (which you've probably seen on *Mr. Robot* and *Silicon Valley*), and learned that if I were a hacker, I'd be a man-in-the-middle of a career change.

Although my white hat resembles a dunce cap, I became a cybersecurity expert by managing responses to privacy breaches and cyberattacks in healthcare organizations. Cybersecurity becomes a matter of life or death when a hospital is hit by ransomware that blocks access to critical medical systems (like emergency room software, lab testing equipment, and life-support machines) needed to save lives.

What I discovered from investigating these incidents is that in every case, the cyberattack originated from a phishing scam. Not the kind where an employee opens a malicious attachment, inadvertently installing malware on their computer; nope, my employees were duped by fake surveys, and in one case, a phony tech support service alerting a physician to a “critical software vulnerability.”

Fortunately, most of these phishing incidents did not result in successful cyberattacks because the IT department had implemented countermeasures such as MFA. But sometimes the attacks failed by sheer luck. Like when an employee mistyped their password to access a fake survey. Or, scribbled their password on a yellow sticky note and stuck it on their encrypted laptop, but the note fell off before the computer was stolen from the backseat of their car. How freaking humbling is it to be saved from encryption being bypassed because a yellow sticky wasn't sticky enough?

I also learned about hacking from pentesters hired to assess the cyber defenses of the companies I worked for. They often succeeded, not with fancy tech like a Rubber Ducky or a custom Metasploit payload, but by simply walking around the hospital, pretending to be lost, to entice helpful employees who would escort them to places they should not go; or, they would just go to a floor and loiter around until someone asked them to leave. Meanwhile, they recorded their walkabout with laptops and cellphones. Just goes to show you don't need technical skills to be a hacker!

Ever since, I've been fascinated with hacking and the gee-whiz tools used to manipulate people. You see, aside from zero-day vulnerabilities, most cyberattacks rely on a human *doing something* to succeed. That BadUSB loaded with a Stuxnet worm is a technological marvel, but the cyberattack only succeeds if an employee is tricked (or bribed) into plugging it into a computer port. The Wi-Fi Pineapple is only dangerous if the victim doesn't realize they have landed on an evil portal. The HackRF One can't open Hondas if Honda used replay-resistant authentication protocols. It all comes down to humans being tricked or surrendering to their baser instincts, or C-suite leaders choosing user convenience over cybersecurity.

This is good news because it means regular folks—even those who are not tech-savvy—can take simple steps to protect themselves. You can safely connect to your coffee shop’s free Wi-Fi—no VPN necessary—if you’re wise to evil portals. QR codes are nothing to fear when they’re from a trusted source, haven’t been tampered with, and you know how to spot a fake phishing site (misspellings, wrong URL, no HTTPS, etc.). And those BadUSBs glistening on the tarmac can’t hurt anyone if you don’t plug them into a computer port.

Regular people don’t need to remember hundreds of passwords if they use a password manager—plus, their passwords will always be strong and won’t be reused. And if a password is breached, your sensitive online accounts will remain safe because you enabled MFA.

You won’t fall in love with a bogus cyber-sweetie when you know the telltale signs of romance baiting. No deepfake, however slick, can fool you if you realize the person is saying or doing something they’d never actually do in real life. And you won’t be duped by scoundrels claiming real evidence is a deepfake when you understand the Liar’s Dividend.

In short, everyday people can become Cyber Mavens without a computer science degree, cyberattacks can be stopped, and cybercriminals are beatable. But you have to know the hacker’s playbook, which is why I wrote *CTRL+ALT+PWN*. Rather than resign yourself to an inevitable fate or remove yourself from the online world, you can study the hacker’s playbook to avoid being just another pwned noob.

When I first began writing *CTRL+ALT+PWN*, it wasn’t a masterpiece. I wrote it over several years, in fits and starts, rewriting sections as new cyberattacks hit the airwaves or when I realized I had totally mangled something and had to correct my mistake. And, being a bipedal primate with squishy meatware between my ears, I made a lot of errors!

That’s why I’m grateful to Helen Patton, a Cisco cybersecurity executive, for reading the manuscript and pointing out where she disagreed with something I wrote; and, more importantly, for introducing me to the philosophical concept of “hacklore.” Hacklore has been a revelation to me and greatly influenced my thinking as I finalized the manuscript. I’m a hacklore true believer, and you should be too. While it’s covered in the book, you can learn about it straight from the source at <https://www.hacklore.org>.

Daniel Shin is a cybersecurity researcher, a certified information privacy professional, and an attorney—talk about a triple threat! He’s an AI expert who offered insightful suggestions for the deepfake sections of the book. Also, the chapter on the future integration of AI and quantum computing was his idea—and I ran with it!

Matthew Schmidt is a Penetration Testing Manager and my secret weapon. His ethical hacking exploits could be made into a high-octane action movie and served as inspiration for many of the exploits covered in the book. Plus, when I didn’t know how to hack something, he could always show me how.

Elizabeth Rasnick, PhD, assistant professor in the Center for Cybersecurity at the University of West Florida, was kind enough to read the manuscript and provide valuable comments, even on the heels of a trip Down Under and just in time for the holiday season. Now, that’s what I call a Christmas present!

Lucid Security deserves a special shout-out—not for teaching me about some esoteric proprietary hacking tool, but for the ethical hackers behind the simulated cyberattack. By “simulated,” I mean that companies pay Lucid Security to hack their networks to pieces, then show them where the vulnerabilities were hiding all along. The Lucid Security team does this not merely with cutting-edge technology but also with the human element; that’s right, it’s Lucid

Security's human factor that sets them apart from other pentesting companies. In a field obsessed with AI-powered exploits and shiny new hacking gadgets, the folks at Lucid Security reminded me that the human mind is still the most powerful hacking tool of all time.

Special thanks to my agent, Ismita Hussain of Great Dog Literary, who took a chance on a neophyte author who penned a rookie manuscript that was maybe worthy of lining a birdcage. But she had a vision, edited the manuscript, and I carried her ideas to a decent working draft, and now hopefully to a place on your bookshelf. Authors, take note—any agent can negotiate a publishing contract, but what Ismita did was provide a North Star. For that, I thank her.

Amanda Chiu Krohn of Turner Publishing conducted a developmental edit of the book, reordering chapters for better flow, suggesting new content, and, most disconcerting, cutting material! But the book is better for her “soft” editing, even when those editorial trims landed hard. Thanks also to Ashlyn Inman for managing the line editing, copyediting, and proofreading, and carrying the manuscript across the finish line. And I don't think there was ever a time when Ashlyn didn't respond to one of my emails in less than thirty minutes—now, that's a superpower!

I'd like to thank my wife, Rosa, for twenty-five years of marriage, and more than an occasional shot of Maker's Mark for, you know, medicinal purposes.

Finally, I would like to thank Rocco, a coon hound, who is not my dog but I love him anyway. He provided invaluable moral support, lying on my bed and watching me type, and only making me take him for a walk when he knew I needed a break. Good boy!

And so here we are. Thanks to brilliant colleagues, a whisky-pouring wife, and a coon hound, the book you're now holding in your eager hands offers you a path to avoid being a victim. And by exposing the tricks of the hacking trade, *CTRL+ALT+PWN: The Hacker's Playbook (And How to Beat It)* is a cybercriminal's worst nightmare.

GLOSSARY

Adaptive phishing—A phishing scam using artificial intelligence that adjusts messages based on how a target responds.

Air gapping—Keeping a computer, device, or network completely offline so hackers can't attack it through the internet.

Anonymizers—Services or tools that hide your online identity and location.

Artificial intelligence—Systems that imitate human reasoning.

BadUSB attack—A USB that runs malicious commands when plugged into a computer.

Behavioral mirroring—When someone mimics your physical communication style to build trust.

Black hats—Malicious hackers who exploit vulnerabilities within systems.

Blame shifting—When a company blames its employees or customers to avoid legal, financial, and ethical accountability for a cyberattack.

Burner phone—A prepaid, disposable mobile phone used to keep calls and texts anonymous.

Catfishing—Creating a fake online persona to scam someone, often for romance or money.

Catfish mirroring—A variation of behavioral and linguistic mirroring, done virtually through texts, emails, DMs, and messaging apps.

Chico Marx factor—The tendency of people to believe even the most unlikely and absurd deepfakes because they align with preexisting beliefs or reinforce what they want to believe.

Cognitive bias—Mental shortcuts that lead to errors in judgment, which hackers exploit.

Confirmation bias—Our tendency to believe things that match what we already believe.

Credential stuffing—Automated cyberattacks using stolen or breached usernames and passwords to break into accounts.

Deepfake detectors—Software that helps spot fake, AI-generated videos, voices, or images.

Deepfake supremacy—The idea that fake, AI-generated content is too good to be detected by

deepfake detection technology.

Deepfake voice cloning—Using AI to mimic someone's voice, often for scams.

Dehumanization—Treating people as less than human to justify abusive or fraudulent behavior.

Digital watermarks—Markers embedded in photos or videos that help prove they are real and haven't been tampered with.

Drive-by QR code phishing—Scanning a malicious QR code redirects you to a website that exploits your device, requiring no user interaction.

Evil portal—A fake Wi-Fi login page used to steal your username and password.

Evil twin—A fake Wi-Fi access point used to mimic a real Wi-Fi network.

Fraud triangle—A theory showing three things that lead to fraud: pressure, opportunity, and rationalization.

Fundamental attribution error—Blaming a person's character for their actions while ignoring the situation, which can lead to unfair judgments.

Generative adversarial network (GAN)—Two AI systems compete to create and detect deepfake voices, images, or videos.

Guilt shifting—Using mocking insults to blame victims of cybercrime rather than holding perpetrators accountable.

Halo effect—When a good trait (like being friendly) makes you believe someone is trustworthy.

Hardware-defined radio (HDR)—Physical electronic components are utilized to transmit or receive signals.

Hactivists—Cybercriminals who hack to promote political or social agendas.

Human factor—The role of human behavior and mistakes in creating security vulnerabilities.

Human interface device (HID)—Devices like keyboards or mice allow interaction between humans and computers.

Identity theft—Stealing someone's personal information to commit fraud.

Jamming attack—Sending radio interference to disrupt or block wireless communications.

Just world bias—Believing people get what they deserve.

Keylogger—Secretly records what you type, such as passwords.

Lingo shifting—Describing scams in a way that focuses on the cybercriminals and the crime, rather than blaming the victim.

Linguistic mirroring—Repeating someone’s words to cultivate trust.

Liquidity mining scam—A cryptocurrency fraud where victims connect their crypto wallets to a fake DeFi platform, enabling scammers to steal their funds.

Love bombing—Smothering someone with affection early in the relationship to gain control over them.

Man-in-the-middle attack—Intercepting and altering messages between two people without their knowledge.

Moral disengagement—Justifying bad behavior to avoid guilt.

Multifactor authentication—Requiring two or more verification methods (e.g., password plus a code) to access an account.

Patch—A software update provided by vendors to fix an error or vulnerability that cybercriminals could exploit.

Pentesters—Ethical hackers who hack clients to identify and fix vulnerabilities.

Phishing—Fake emails or messages designed to trick victims into revealing sensitive information.

Phishing-resistant MFA—Stronger login methods like hardware keys or biometrics (e.g., fingerprints) that are harder for hackers to fake.

Pig butchering scam—A long con where scammers build trust over time before asking victims for money.

Pwned—Slang for “owned,” meaning your account has been hacked.

Quishing—Phishing via malicious QR codes that redirect users to fake sites.

Ransomware as a service (RaaS)—A subscription model where cybercriminals sell their ransomware tools to others.

Raspberry Pi—A tiny, affordable computer used for learning and security research.

Red team—Pentesters who act like real-world cybercriminals to test an organization’s defenses.

Replay attack—Replaying data transmissions to trick a system into giving access.

Reverse image search—Using a photo to find its source; great for spotting fakes.

Romance scam—A fake romantic relationship to steal money or personal info.

Segregation of duties—Splitting up tasks among multiple people so no single person can both commit and conceal fraud.

Service set identifier (SSID)—The name of a Wi-Fi network when devices connect to it.

Side channel attack—Exploiting indirect data (such as timing or power consumption) to extract information from a system.

SIM jacking—Stealing a mobile phone number by transferring its SIM to another device, enabling scammers to intercept calls and texts.

Software-defined radio (SDR)—Using software to send or receive radio signals.

Spyware—Software that secretly collects user data or monitors activity without consent.

Strong password—A long, random password consisting of letters, numbers, and special characters, making it difficult to guess.

Trust-jacking—The tactics scammers use to build trust and emotionally and psychologically bind the victim to a romance scam.

The liar's dividend—When the possibility of deepfakes causes people to doubt genuine content ("it could be fake").

Victim blaming—Blaming people who've been scammed instead of the cybercriminals who scammed them.

Virtual private network (VPN)—An encrypted tunnel between a device and a network that hides your data and location.

White hats—Ethical hackers who test systems for vulnerabilities.

Wi-Fi Pineapple—A portable penetration-testing device used to create fake Wi-Fi networks and perform man-in-the-middle attacks.

Zero-day attack—A cyberattack that takes advantage of a software flaw unknown to the vendor. Since no patch is available, the attack is likely to succeed.

Zero-day exploit—The specific malware, tool, or method used to exploit a zero-day vulnerability.

Zero-day vulnerability—A flaw in hardware or software that is unknown to the vendor and therefore not patched.

Endnotes

Introduction

- [1](#) Paez, Danny. “How ‘Pwned’ Went From Hacker Slang to the Internet’s Favorite Taunt.” Inverse, March 17, 2020. <https://www.inverse.com/gaming/pwned-meaning-definition-origins-video-games-internet-hackers>.
- [2](#) Babinski, Micah. “Why the ‘Basement Hacker’ Stereotype Is Wrong—and Dangerous.” Dark Reading, November 22, 2021. <https://www.darkreading.com/attacks-breaches/why-the-basement-hacker-stereotype-is-wrong-and-dangerous>.
- [3](#) Van de Wiele, Tom. “We Need to Smash the Stereotype That Hackers Are All Teens in Hoodies.” Silicon Republic, September 23, 2022. <https://www.siliconrepublic.com/enterprise/ethical-hacker-stereotype>.
- [4](#) Fretty, Peter. “REvil, DarkSide and Now BlackMatter.” IndustryWeek, September 1, 2021. <https://www.industryweek.com/technology-and-iiot/article/21174060/revil-darkside-and-now-blackmatter>.
- [5](#) Van Boom, Daniel. “Seth Green Loses \$200K Bored Ape Yacht Club NFT in Phishing Scam.” CNET, accessed October 2, 2023. <https://www.cnet.com/personal-finance/seth-green-loses-200k-bored-ape-yacht-club-nft-in-phishing-scam/>.
- [6](#) Herrera, Pedro. “How to Value Bored Apes Yacht Club NFTs.” DappRadar, July 28, 2021. <https://dappradar.com/blog/how-to-value-bored-apes-yacht-club-nfts>.
- [7](#) Erinfoami, Keyede. “Bored Ape Yacht Club: What Is It & Why Are They So Expensive?” MUO, April 6, 2022. <https://www.makeuseof.com/what-is-bored-ape-yacht-club/>.
- [8](#) Emerson, Sarah. “Someone Stole Seth Green’s Bored Ape And Star Of His New NFT Show.” BuzzFeed News, May 24, 2022. <https://www.buzzfeednews.com/article/sarahemerson/seth-green-bored-ape-stolen-tv-show>.
- [9](#) “BAYC | Terms & Conditions.” Bored Ape Yacht Club - Welcome to the BAYC Clubhouse, accessed September 2, 2025. <https://boredapeyachtclub.com/licenses/bayc>.
- [10](#) Ifeanyi, Kc. “The Bored Ape Yacht Club Apes into Hollywood.” *Fast Company*, January 18, 2022. <https://www.fastcompany.com/90706534/the-bored-ape-yacht-club-apes-into-hollywood>.
- [11](#) Rory. “Seth Green Retrieves Stolen Bored Ape NFT at a Hefty Cost.” NFT Plazas, June 11,

2022. <https://nftplazas.com/seth-green-retrieves-stolen-bored-ape-nft-at-a-hefty-cost/>.
- 12 Dickey, Timothy Burke and Jack. "Manti Te'o's Dead Girlfriend, The Most Heartbreaking And Inspirational Story Of The College Football Season, Is A Hoax." Deadspin, January 16, 2013. <https://deadspin.com/manti-teos-dead-girlfriend-the-most-heartbreaking-an-5976517>.
 - 13 Ley, Tom. "The Story Behind The Story: The Manti Te'o Hoax." Deadspin, December 27, 2013. <https://deadspin.com/the-story-behind-the-story-the-manti-teo-hoax-1490519550>.
 - 14 Sundriyal, Diksha. "Diane O'Meara: What Happened to Face of Manti Te'o's Girlfriend?" The Cinemaholic, August 16, 2022. <https://thecinemaholic.com/diane-omeara-now-where-is-the-face-of-manti-teos-girlfriend-today/>.
 - 15 Gupta, Prachi. "What Did Manti Te'o Know about Lennay Kekua?" Salon.com, January 24, 2013. https://www.salon.com/2013/01/24/what_did_manti_teo_know_about_lennay_kekua/.
 - 16 Palmer, Roxanne. "Where Does 'Catfish' Come From? Online Hoax Movie Inspired By Fisherman's Lore." International Business Times, January 17, 2013. <https://www.ibtimes.com/where-does-catfish-come-online-hoax-movie-inspired-fishermans-lore-1022374>.
 - 17 Shepkowski, Nick. "Manti Te'o Documentary: The World Reacts." Fighting Irish Wire, August 21, 2022. <https://fightingirishwire.usatoday.com/lists/manti-teo-documentary-the-world-reacts/>.
 - 18 Bischoff, Paul. "Nearly 73,000 Americans Lost More than \$1 Billion to Romance Scams in 2022." Comparitech, February 10, 2021. <https://www.comparitech.com/blog/vpn-privacy/romance-scams/>.
 - 19 Vincent, James. "4chan Protects Itself against Stolen Celebrity Photo Claims - with New Copyright Rules." Independent, September 5, 2014. <https://www.the-independent.com/tech/4chan-protects-itself-against-stolen-celebrity-photo-claims-with-new-copyright-rules-9712130.html>.
 - 20 "Celebgate Hack 2014: Here's What Happened (+ Who Was Hacked)." VPN Reactor, November 2, 2022. <https://www.vpnreactor.com/celebgate-hack-2014/>.
 - 21 Smith, Chris. "How the Jennifer Lawrence iCloud Hack Really Happened." BGR, March 16, 2016. <https://bgr.com/tech/jennifer-lawrence-nudes-icloud-hack/>.
 - 22 Haley, Craig. "How Did Hackers Steal Hundreds of Celebrity Photos?" That'sNonsense.Com, March 23, 2017. <https://www.thatnsnonsense.com/hackers-steal-hundreds-celebrity-photos/>.
 - 23 Kashner, Sam. "Exclusive: Jennifer Lawrence Speaks About Her Stolen Photos." *Vanity Fair*, October 20, 2014. <https://www.vanityfair.com/hollywood/2014/10/jennifer-lawrence-photo-hacking-privacy>.

- 24 O'Neill, Patrick Howell. "Fourth Man Receives Prison Sentence in 'Celebgate' Photo Leak." CyberScoop, August 29, 2018. <https://cyberscoop.com/celebgate-fourth-man-receives-prison-sentence/>.
- 25 Main, Kelly. "Phishing Statistics By State In 2023." *Forbes*, June 9, 2023. <https://www.forbes.com/advisor/business/phishing-statistics/>.
- 26 Poireault, Kevin. "Global Ransomware Damages to Exceed \$30bn by 2023." Infosecurity Magazine, August 29, 2022. <https://www.infosecurity-magazine.com/news/ransomware-exceed-30bn-dollars-2023/>.

Chapter 1

- 1 Nickerson, Charlotte. "Biological Theories of Crime." Study Guides for Psychology Students - Simply Psychology. Simply Scholar Ltd, October 6, 2021. <https://www.simplypsychology.org/biological-theories-crime.html>.
- 2 Wiseman, Ryan. "Six Major Reasons Why People Commit Crimes." Case for Conservatism – Here We Present the Case for Conservatism, August 19, 2021. <https://caseforconservatism.com/criminal-justice/six-major-reasons-why-people-commit-crimes/>.
- 3 Ibid.
- 4 Ibid.
- 5 Ibid.
- 6 Saab, Hassan. "Fraud Triangle - Opportunity, Incentive, Rationalization." Wall Street Oasis, December 13, 2021. <https://www.wallstreetoasis.com/resources/skills/accounting/fraud-triangle>.
- 7 Ibid.
- 8 Jacy. "What Is Segregation of Duties and Why Are They Important?" Accounting Internal Controls, December 27, 2020. <https://accountinginternalcontrols.com/segregation-of-duties/>.
- 9 Saab, "Fraud Triangle."
- 10 Ibid.
- 11 Financial Executives Research Foundation. *Breaking the cycle of fraud: What senior financial executives should do*. Financial Executives International, 2015. <https://www.financialexecutives.org/ferf/download/2015%20Final/2015-001.pdf>.
- 12 Prey, Easy. "The Life of a Cybercriminal with Brett Johnson." Easy Prey Podcast, November 11, 2020. <https://www.easyprey.com/the-life-of-a-cybercriminal-with-brett-johnson/>.
- 13 "Inside Cybercrime: Fraud Busting Full Interview with Brett Johnson the Godfather of Cybercrime." Body Language Expert, Traci Brown, accessed December 5, 2023. <https://www.bodylanguagetrainer.com/inside-cybercrime-fraud-busting-full-interview-with-brett-johnson-the-godfather-of-cybercrime/>.
- 14 Tarantola, Andrew. "Hitting the Books: How the 'Godfather of Cybercrime' got his start on eBay: From bunk Beanie Babies to signal-stealing cable boxes, Brett Johnson has scammed them all." Engadget, March 26, 2023. <https://www.engadget.com/hitting-the-books-fool->

[me-once-kelly-richmond-pope-harvard-business-review-press-143031129.html](https://www.hbr.org/press/2014/03/143031129.html).

- [15](#) Ibid.
- [16](#) Ibid.
- [17](#) Zetter, Kim. “Secret Service Operative Moonlights as Identity Thief.” *Wired*, June 6, 2007. <https://www.wired.com/2007/06/secret-service/>.
- [18](#) Ibid.
- [19](#) Weisbaum, Herb. This former identity thief now fights the crimes he helped perfect. NBC News, January 14, 2018. <https://www.nbcnews.com/business/consumer/former-identity-thief-now-fights-crimes-he-helped-perfect-n837166>.
- [20](#) Prey, Easy. “The Life of a Cybercriminal with Brett Johnson.” Easy Prey Podcast. <https://www.facebook.com/EasyPreyPodcast>. November 11, 2020. <https://www.easyprey.com/the-life-of-a-cybercriminal-with-brett-johnson/>.
- [21](#) Ibid.
- [22](#) Ibid.
- [23](#) Mehrotra, Kriti. “Brett Johnson: Where Is the Cybersecurity Expert Today?” The Cinemaholic, December 6, 2024. <https://thecinemaholic.com/brett-johnson-now-where-is-the-cybersecurity-expert-today/>.
- [24](#) Demetis, Dionysios. “How the ‘Original Internet Godfather’ Walked Away from His Cybercrime Past – Interview.” *Conversation*, January 2, 2018. <https://theconversation.com/how-the-original-internet-godfather-walked-away-from-his-cybercrime-past-interview-88822>.
- [25](#) “Inside Cybercrime.”
- [26](#) Dionysios, “Original Internet Godfather.”

Chapter 2

- 1 Zetter, Kim. "Hackers Finally Post Stolen Ashley Madison Data." *Wired*, August 18, 2015. <https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/>.
- 2 Ibid.
- 3 Ibid. Zetter, Kim.
- 4 Fazzini, Kate. "Ashley Madison Breach from 2015 Being Used in Sextortion Scams." CNBC, January 31, 2020. <https://www.cnbc.com/2020/01/31/ashley-madison-breach-from-2015-being-used-in-sextortion-scams.html>.
- 5 Sharma, Toshendra. "White Hat vs Black Hat vs Grey Hat Hacker." Global Tech Council, June 16, 2020. <https://www.globaltechcouncil.org/cyber-security/white-hat-vs-black-hat-vs-grey-hat-hacker/>.
- 6 Zetter, Kim. "Hacker's Tweet Reignites Ugly Battle Over Security Holes." *Wired*. April 21, 2015. <https://www.wired.com/2015/04/twitter-plane-chris-roberts-security-reasearch-cold-war/>.
- 7 Ibid.
- 8 Zetter, Kim. "Feds Say That Banned Researcher Commandeered a Plane." *Wired*. May 15, 2015. <https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/>.
- 9 Perez, Evan. "FBI: Hacker claimed to have taken over flight's engine controls." CNN, May 18, 2015. <https://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/>.
- 10 "Chris Roberts FBI Warrant Application. 2015. DocumentCloud." Filed April 17, 2015. <https://embed.documentcloud.org/documents/2082883-chris-roberts-warrant-application/>.
- 11 Perez, "FBI: Hacker claimed to have taken over flight's engine controls."
- 12 Gibbs, Samuel. "Aviation Experts Dispute Hacker's Claim He Seized Control of Airliner Mid-Flight." *Guardian*, May 19, 2015. <https://www.theguardian.com/technology/2015/may/19/hacker-chris-roberts-claim-seized-control-boeing-airliner-disputed-experts>.
- 13 Zetter, "Banned Researcher."
- 14 "Roberts Warrant Application."
- 15 Sam Grobart. "Hacking an airplane with only an Android phone." Bloomberg, April 12, 2013. <https://www.bloomberg.com/news/articles/2013-04-12/hacking-an-airplane-with-only-an-android-phone#xj4y7vzkg>.
- 16 Josh Peterson. "FAA strongly denies alleged smartphone airplane hack is a problem."

Daily Caller, April 11, 2013. <https://dailycaller.com/2013/04/11/faa-strongly-denies-alleged-smartphone-airplane-hack-is-a-problem/>.

- 17 Calvin Biesecker. “Boeing 757 Testing Shows Airplanes Vulnerable to Hacking, DHS Says.” Avionics International, November 8, 2017. <https://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says/>.
- 18 Freiherr, Greg. “Will Your Airliner Get Hacked? Meet the people who are making sure it won’t.” *Smithsonian Magazine*, February 2021. <https://www.smithsonianmag.com/air-space-magazine/will-your-airliner-get-hacked-180976752/>.
- 19 Ibid.
- 20 Greenberg, Andy. “A Boeing Code Leak Exposes Security Flaws Deep in a 787’s Guts.” *Wired*, August 7, 2019. <https://www.wired.com/story/boeing-787-code-leak-security-flaws/>.
- 21 Ibid.

Chapter 3

- 1 Morgan, Steve. "Global Ransomware Damage Costs Predicted To Exceed \$275 Billion By 2031." *Cybercrime Magazine*, Apr. 1, 2025, <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/>.
- 2 Gaskew, Brandon. "Third Way." *Third Way*, May 23, 2019. <https://www.thirdway.org/report/cyber-enforcement-in-four-key-states>.
- 3 Zvelo. "Use of Web Anonymizers to Hide Illegal Online Activity on the Rise." Threat Intelligence, URL Database & Web Classification Solutions, accessed February 19, 2023. <https://zvelo.com/web-anonymizers-hide-illegal-online-activity/>.
- 4 Orchid. "Anonymizers vs. VPNs: Everything You Need to Know." Privacy & VPN Blog – Orchid, January 4, 2023. <https://blog.orchid.com/anonymizers-vs-vpns-everything-you-need-to-know/>.
- 5 Freedman, David H. "How Hackers Outwit All Efforts to Stop Them: 'It's a Cyber Pandemic.'" *Newsweek*, January 18, 2023. <https://www.newsweek.com/2023/01/27/how-hackers-outwit-all-efforts-stop-them-its-cyber-pandemic-1774458.html>.
- 6 Novinson, Michael. "Colonial Pipeline Hacked Via Inactive Account Without MFA." CRN, June 5, 2021. <https://www.crn.com/news/security/colonial-pipeline-hacked-via-inactive-account-without-mfa?itc=refresh>.
- 7 Khurshudyan, Isabelle, and Loveday Morris. "Ransomware's Suspected Russian Roots Point to a Long Detente between the Kremlin and Hackers." *Washington Post*, June 12, 2021. https://www.washingtonpost.com/world/europe/russia-ransomware-cyber-crime/2021/06/11/e159e486-c88f-11eb-8708-64991f2acf28_story.html.
- 8 Glover, Claudia. "Have we seen the last of Colonial Pipeline cyberattack group DarkSide?" Tech Monitor, May 18, 2021. <https://techmonitor.ai/technology/cybersecurity/what-happened-to-darkside-colonial-pipeline>.
- 9 Loman, Mark. "BlackMatter Ransomware Emerges from the Shadow of DarkSide." Sophos News, August 9, 2021. <https://news.sophos.com/en-us/2021/08/09/blackmatter-ransomware-emerges-from-the-shadow-of-darkside/>.
- 10 Abrams, Lawrence. "DarkSide Ransomware Gang Returns as New BlackMatter Operation." BleepingComputer, July 31, 2021. <https://www.bleepingcomputer.com/news/security/darkside-ransomware-gang-returns-as-new-blackmatter-operation/>.
- 11 Grimes, Roger A. "Why It's so Hard to Prosecute Cyber Criminals." CSO, December 6, 2016. <https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html>.

- [12](#) Wolff, J. The real reasons why cybercrimes are vastly underreported. *Slate*, February 12, 2018. <https://slate.com/technology/2018/02/the-real-reasons-why-cybercrimes-are-vastly-underreported.html>.
- [13](#) U.S. Government Accountability Office. “Cybercrime: Reporting mechanisms vary, and agencies face challenges in developing metrics.” GAO Publication No. GAO-23-106080, June 2023. <https://www.gao.gov/assets/830/827173.pdf>.
- [14](#) Eoyang, Mieke, Allison Peters, Ishan Mehta, and Brandon Gaskew. “To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors.” Third Way, October 29, 2018. <https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors>.

Chapter 4

- 1 Alfred, Randy. "March 25, 1954: RCA TVs Get the Color for Money." *Wired*, March 25, 2008. <https://www.wired.com/2008/03/dayintech-0325/#:~:text=RCA's%20CT-100%20was%20the,color-TV%20set%20for%20consumers>.
- 2 Wikipedia contributors. "DynaTAC." Last modified November 25, 2025. Wikipedia. <https://en.wikipedia.org/wiki/DynaTAC>.
- 3 Lutkevich, Ben. "What Is a Wi-Fi Pineapple?" TechTarget Search Security, December 20, 2019. <https://www.techtarget.com/searchsecurity/definition/Wi-Fi-Pineapple>.
- 4 Khristopher, Yackulic. "What Is A WiFi Pineapple, And Can It Compromise Your Security?" Android Headlines, August 12, 2019. <https://www.androidheadlines.com/2019/08/what-is-a-wifi-pineapple-and-can-it-compromise-your-security.html>.
- 5 Frew, James. "What Is a Wi-Fi Pineapple and Can It Compromise Your Security?" MUO, June 27, 2017. <https://www.makeuseof.com/tag/wifi-pineapple-protect>.
- 6 Hak5. "WiFi Pineapple - Modules." WiFi Pineapple - Resources. Hak5 LLC, accessed August 23, 2022. <https://www.wifipineapple.com/modules>.
- 7 Floyd, Daniel. "The Resurgence of Man-in-the-Middle Attacks & How to Stop Them." Security Boulevard. Techstrong Group Inc., February 22, 2022. <https://securityboulevard.com/2022/02/the-resurgence-of-man-in-the-middle-attacks-how-to-stop-them/>.
- 8 Lynch, Vincent. "Would Silicon Valley's Wi-Fi Pineapple Scheme Really Work?" Hashed Out by The SSL Store. The SSL Store, June 23, 2017. <https://www.thesslstore.com/blog/silicon-valley-wi-fi-pineapple/>.
- 9 Terranova Security. "Defend Against Wi-Fi Pineapple Attacks." Cyber Security Awareness Blog. Terranova Worldwide Corporation, August 12, 2022. <https://terrانovasecurity.com/wi-fi-pineapple-cyber-security-threat/>.
- 10 20i. "Why and How Force HTTPS on Your Website?" 20i Web Hosting Knowledge Base. 20i Ltd., accessed August 23, 2022. <https://www.20i.com/us/support/ssl-certificates/force-https>.
- 11 Yackel, Ryan. "What Are SSL Stripping Attacks?." Keyfactor, August 19, 2021. <https://www.keyfactor.com/blog/what-are-ssl-stripping-attacks/>.
- 12 Helme, Scott. "The WiFi Pineapple - Using Karma and SSLstrip to MiTM Secure Connections." Scott Helme, September 20, 2013. <https://scotthelme.co.uk/wifi-pineapple-karma-sslstrip/>.

- 13 Panda Security. "What Is an Evil Twin Attack?." Panda Security, December 13, 2021. <https://www.pandasecurity.com/en/mediacenter/security/what-is-an-evil-twin-attack/>.
- 14 Claburn, Thomas. "Wi-Fi Spy Drones Used to Snoop on Financial Firm." The Register, October 12, 2022. <https://www.theregister.com/2022/10/12/drone-roof-attack>.
- 15 Toulas, Bill. 2024. "Australian Charged for 'Evil Twin' WiFi Attack on Plane." BleepingComputer, July 1, 2024. Accessed 11/22/2025. <https://www.bleepingcomputer.com/news/security/australian-charged-for-evil-twin-wifi-attack-on-plane/>.
- 16 Varghese, Daniel. "Digital Security Matters. OK, but Do I Really Need a VPN." *Wall Street Journal*, July 19, 2022. <https://www.wsj.com/articles/what-is-a-vpn-do-i-need-to-use-one-11658263245?mod=djemCybersecruityPro&tpl=cy>.
- 17 Cruz, Brett, and Gene Petrino. 2025. "How Much Does a VPN Cost?" Security.org. Last updated October 20, 2025. Accessed November 22, 2025. <https://www.security.org/vpn/cost/>.
- 18 Ibid.
- 19 Truehost. 2025. "How to Fix the 'Not Secure' Warning on Your Website." Truehost Blog, October 23, 2025. <https://truehost.com/how-to-fix-the-not-secure-warning/>.
- 20 SecurityScorecard. 2025. "HTTPS vs. HTTP: Why Secure Connections Matter in 2025." SecurityScorecard Blog, June 12, 2025. <https://securityscorecard.com/blog/https-vs-http-why-secure-connections-matter-in-2025>.
- 21 Lord, Bob. 2019. "The Quiet HTTPS Revolution." Medium, March 21, 2019. <https://medium.com/@boblord/the-quiet-https-revolution-637a1c40ec6a>.
- 22 BasuMallick, Chiradeep. "What Is Raspberry Pi? Models, Features, and Uses." Spiceworks, July 5, 2022. <https://www.spiceworks.com/tech/networking/articles/what-is-raspberry-pi/>.
- 23 Lakshan. "What Is SDR and What Can You Do with SDR?" Latest Open Tech From Sseed. Sseed Technology Co., Ltd., May 25, 2020. <https://www.sseedstudio.com/blog/2020/05/25/what-is-sdr-and-what-can-you-do-with-sdr/>.
- 24 Per Vices. "What Is a Software Defined Radio?" Everything RF, August 27, 2021. <https://www.everythingrf.com/community/what-is-a-software-defined-radio>.
- 25 Buiting, Jan. "HackRF One + PortaPack H2: A Truly Portable Software Defined Radio (SDR) | Elektor Magazine." *Elektor*, December 12, 2024. <https://www.elektormagazine.com/review/review-hackrf-one-portapack-h2-a-truly-portable-sdr>.
- 26 Zorz, Zeljka. "WiFi Jamming Attacks More Simple and Cheaper than Ever." Help Net Security, October 13, 2015. <https://www.helpnetsecurity.com/2015/10/13/wifi-jamming->

[attacks-more-simple-and-cheaper-than-ever/](#).

- 27 Maloney, Dan. "Side-Channel Attack Shows Vulnerabilities Of Cryptocurrency Wallets." Hackaday, September 13, 2019. <https://hackaday.com/2019/09/13/side-channel-attack-shows-vulnerabilities-of-cryptocurrency-wallets/>.
- 28 HackedExistence. "Unlocking Car Doors with the HackRF One Replay Attack." HackedExistence on YouTube, 4:41, January 28, 2019. <https://www.youtube.com/watch?v=CA3XnGyD-SQ>.
- 29 Kevin2600, and Wesley Li. "Rolling Pwn Attack." Rolling Pwn Attack GitHub. Kevin2600 and Wesley Li, July 7, 2022. <https://rollingpwn.github.io/rolling-pwn/>.
- 30 Ibid.
- 31 Stumpf, Rob. "I Tried the Honda Key Fob Hack on My Own Car. It Totally Worked." Drive, July 11, 2022. <https://www.thedrive.com/tech/i-tried-the-honda-keyfob-hack-on-my-own-car-it-totally-worked>.
- 32 Kevin2600, "Rolling Pwn Attack."
- 33 Stumpf, "Honda Key Fob Hack."
- 34 Perez, Dalia. "Some Honda Key Fobs Are Prone to Hackers." 11Alive.Com, July 18, 2022. <https://www.11alive.com/article/money/cars/some-honda-key-fobs-prone-hackers/85-ef88a9a6-928f-4092-8544-825e320c09b9>.
- 35 Ascend Technologies, LLC. "The Rubber Ducky: Cyber Meets Physical with This Small Hacking Tool." Ascend Technologies, November 11, 2019. <https://blog.teamascend.com/rubber-ducky>.
- 36 Hill, Michael. "BadUSB Explained: How Rogue USBs Threaten Your Organization." CSO Online, January 20, 2022. <https://www.csoonline.com/article/3647173/badusb-explained-how-rogue-usbs-threaten-your-organization.html>.
- 37 Raghavan, Rithesh. "Introduction to BadUSB Attacks: How It Works & Prevention Methods." Web Solutions Blog. Acodez, January 9, 2020. <https://acodez.in/badusb-attack/>.
- 38 Cirelly, John. "BadUSB - What Is It and How to Avoid It in 2022 Step-by-Step Guide." Comparitech, September 21, 2021. <https://www.comparitech.com/net-admin/what-is-badusb/>.
- 39 Ionut Ilascu, "FBI: Hackers Sending Malicious USB Drives and Teddy Bears via USPS," BleepingComputer, March 27, 2020, <https://www.bleepingcomputer.com/news/security/fbi-hackers-sending-malicious-usb-drives-and-teddy-bears-via-usps/>.
- 40 Roy, Subhojit. 2025. "What Is a BadUSB? Understand the Threat and How to Prevent It." Ivanti. July 29, 2025. <https://www.ivanti.com/blog/what-is-badusb>.

- 41 Katz, Yaakov. "Stuxnet May Have Destroyed 1,000 Centrifuges at Natanz." *Jerusalem Post*, January 6, 2022. <https://www.jpost.com/Defense/Stuxnet-may-have-destroyed-1000-centrifuges-at-Natanz>.
- 42 Vijayan, J. "USB devices the common denominator in all attacks on air-gapped systems." *Dark Reading*, December 3, 2021. <https://www.darkreading.com/cyberattacks-data-breaches/usb-devices-common-denominator-in-all-attacks-on-air-gapped-systemsd>.
- 43 Kopfstein, Janus. "Stuxnet Virus Was Planted by Israeli Agents Using USB Sticks, According to New Report." *Verge*, April 12, 2012. <https://www.theverge.com/2012/4/12/2944329/stuxnet-computer-virus-planted-israeli-agent-iran>.
- 44 Baca, Alejandro, and Rodel Mendrez. "Would You Exchange Your Security for a Gift Card?" *SpiderLabs Blog*. Trustwave Holdings, Inc., March 26, 2020. <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/would-you-exchange-your-security-for-a-gift-card/>.
- 45 Fruhlinger, Josh. "Keyloggers Explained: How Attackers Record Computer Inputs." *CSO Online*, May 17, 2022. <https://www.csoonline.com/article/3326304/keyloggers-explained-how-attackers-record-computer-inputs.html>.
- 46 Retia. "How to Hack Computers Over Wi-Fi with the WiFi Duck Payload Deliverer." *WonderHowTo*, November 13, 2020. <https://null-byte.wonderhowto.com/how-to/hack-computers-over-wi-fi-with-wifi-duck-payload-deliverer-0296285/>.
- 47 Lord, Nate. "What Is Device Control? A Device Control Definition." *Enterprise IP and DLP Software | Digital Guardian*, May 4, 2015. <https://www.digitalguardian.com/blog/what-device-control-device-control-definition>.
- 48 Jethva, Hitesh. "Best USB Port Locking Software for 2025 - Free & Paid Tools!" *ITT Systems*, May 13, 2023. <https://www.ittsystems.com/best-usb-port-locking-tools/#wbounce-modal>.

Chapter 5

- 1 Wilkins, Alasdair. “10 Hacking Tools You Think Would Be Illegal But Are for Sale Online.” Inverse, November 22, 2017. <https://www.inverse.com/article/38612-hacking-tools-legal-available>.
- 2 Catholic Answers. “John Henry Newman.” Catholic Answers, November 19, 2018. <https://www.catholic.com/encyclopedia/john-henry-newman>.
- 3 Contributors to Wikimedia projects. “Apologia Pro Vita Sua - Wikipedia.” Wikipedia, the Free Encyclopedia. Wikimedia Foundation, Inc., April 1, 2003. https://en.wikipedia.org/wiki/Apologia_Pro_Vita_Sua.
- 4 Kajihiro, Ken. “Hacking Software: Free and Legal?” Richmond Journal of Law and Technology, March 8, 2021. <https://jolt.richmond.edu/2021/03/08/hacking-software-free-and-legal/>.
- 5 Leverett, Eireann. “In Defense of Offensive Hacking Tools.” Privacy International, May 2, 2017. <https://privacyinternational.org/blog/849/defense-offensive-hacking-tools>.
- 6 Fernandez, Ray. “Are Ethical Hackers the Digital Security Answer?” TechRepublic, August 16, 2022. <https://www.techrepublic.com/article/are-ethical-hackers-the-digital-security-answer/>.
- 7 Leverett, “In Defense of Offensive Hacking Tools.”
- 8 Deseret News. “Formula For Sarin is Simple.” Deseret News, March 23, 1995. <https://www.deseret.com/1995/3/23/19165802/formula-for-sarin-is-simple>.

Chapter 6

- 1 “Ransomware: The Data Exfiltration and Double Extortion Trends.” CIS. Center for Internet Security, April 21, 2021. <https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends>.
- 2 Bernstein, Corinne. “What Is PII (Personally Identifiable Information)?” SearchSecurity. TechTarget, September 24, 2021. <https://www.techtarget.com/searchsecurity/definition/personally-identifiable-information-PII>.
- 3 Lockert, Melanie. “How Do Hackers Use Your Information for Identity Theft?” Credit Karma, LLC., May 7, 2025. <https://www.creditkarma.com/id-theft/i/how-hackers-use-your-information>.
- 4 Tunggal, Abi Tyas. “17 Ransomware Examples.” UpGuard, Inc., August 8, 2022. <https://www.upguard.com/blog/ransomware-examples#:~:text=WannaCry,WannaCrypt0r%20.0%20and%20Wanna%20Decryptor>.
- 5 SOCRadar. “The evolution of ransomware: From simple encryption to double extortion tactics.” SOCRadar Cyber Intelligence Inc., January 14, 2025. <https://socradar.io/the-evolution-of-ransomware-from-simple-encryption-to-double-extortion-tactics/>.
- 6 Baker, Kurt. “Ransomware as a Service (RaaS) Explained.” CrowdStrike.Com, January 30, 2023. <https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/>.

Chapter 7

- 1 Siegel, Darren. "How Poor Password Hygiene Crippled Colonial Pipeline." *Pipeline Technology Journal*, April 7, 2021. <https://www.pipeline-journal.net/news/opinion-how-poor-password-hygiene-crippled-colonial-pipeline>.
- 2 McKay, Tom. "Ransomware Jerks Helped Cause the Cream Cheese Shortage." Gizmodo, December 10, 2021. <https://gizmodo.com/ransomware-jerks-helped-cause-the-cream-cheese-shortage-1848195368>.
- 3 Barr, Luke. "JBS Paid \$11 Million in Ransom after Cyberattack, Company Says." ABC News, June 9, 2021. <https://abcnews.go.com/Business/jbs-paid-11-million-ransom-cyber-attack-company/story?id=78185017>.
- 4 Turton, W. "Hackers breached Colonial Pipeline using compromised password." Bloomberg, June 4, 2021. <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>.
- 5 Sharma, Mayank. "Breached Colonial VPN Password Was Complex, but Reused." TechRadar, June 10, 2021. <https://www.techradar.com/news/breached-colonial-vpn-password-was-complex-but-reused>.
- 6 Novinson, Michael. "Colonial Pipeline Hacked Via Inactive Account Without MFA." Technology News For IT Channel Partners and Solution Providers | CRN, June 5, 2021. <https://www.crn.com/news/security/colonial-pipeline-hacked-via-inactive-account-without-mfa>.
- 7 Goodin, Dan. "Failure to Patch Two-Month-Old Bug Led to Massive Equifax Breach." Ars Technica, September 13, 2017. <https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/>.
- 8 Warren, Elizabeth. "Senator Warren Unveils Bill to Expand Criminal Liability to Negligent Executives of Giant Corporations." Home | U.S. Senator Elizabeth Warren of Massachusetts, April 3, 2019. <https://www.warren.senate.gov/newsroom/press-releases/senator-warren-unveils-bill-to-expand-criminal-liability-to-negligent-executives-of-giant-corporations>.
- 9 Agnew, Kevin, PhD, CPA, C. Catherine Chiang, PhD, CPA, Caroline Sprecher. "The SEC Finalizes Rule on Cybersecurity Disclosures." The CPA Journal, August 27, 2025. <https://www.cpajournal.com/2025/08/27/the-sec-finalizes-rule-on-cybersecurity-disclosures/>.
- 10 Biever, Steve. "Giving USA 2022 Report Insights." BWF, June 21, 2022. <https://www.bwf.com/giving-usa-2022-report-insights/>.

- 11 Google/Harris Poll. "Online Security Survey." Google, February 2019.
https://services.google.com/fh/files/blogs/google_security_infographic.pdf.
- 12 Christopherson, Lauren. "New LastPass Research Finds Password Habits Remain Key Obstacle to Business Security." LogMeIn, October 8, 2019.
<https://picante.today/blog/2019/10/08/new-lastpass-research-finds-password-habits-remain-key-obstacle-to-business-security/>.
- 13 Stickley on Security Inc. "81% of Company Data Breaches Due to Poor Passwords." Bank of North Dakota Blog, August 3, 2018. <https://bnd.nd.gov/81-of-company-data-breaches-due-to-poor-passwords/>.
- 14 Gonzales, Joshua. "Study Finds 78% of People Reset a Password They Forgot in Past 90 Days." Hyper Blog, December 10, 2019. <https://blog.hypr.com/hypr-password-study-findings>.
- 15 Tavares, Pedro. "Top Tools for Password Spraying Attacks in Active Directory Networks." Infosec Institute, January 25, 2022.
<https://www.infosecinstitute.com/resources/hacking/top-tools-for-password-spraying-attacks-in-active-directory-networks/>.
- 16 Kosoff, Maya. "Mark Zuckerberg's Terrible Password Revealed in Hack." *Vanity Fair*, June 6, 2016. <https://www.vanityfair.com/news/2016/06/mark-zuckerberg-terrible-password-revealed-in-hack>.
- 17 McCoy, Kevin. "Forbes 2016 Richest List: Zuckerberg Zooms Up," *USA TODAY*, March 1, 2016. <https://www.usatoday.com/story/money/2016/03/01/zuckerberg-top-gainer-forbes-2016-billionaires-list/81146342/>.
- 18 Kosoff, "Mark Zuckerberg's Terrible Password Revealed in Hack."
- 19 Lorenzo Franceschi-Bicchierai. "Another Day, Another Hack: 117 Million LinkedIn Emails And Passwords." *VICE*, May 18, 2016.
<https://www.vice.com/en/article/78kk4z/another-day-another-hack-117-million-linkedin-emails-and-password>.
- 20 Jenson, Jamie. "Sonnet 43: How Do I Love Thee? Poem Analysis." July 30, 2016.
<https://poemanalysis.com/elizabeth-barrett-browning/sonnet-43-how-do-i-love-thee/>.
- 21 Browning, Elizabeth Barrett. "How Do I Love Thee? (Sonnet 43)." Poets.org. n.d.
<https://poets.org/poem/how-do-i-love-thee-sonnet-43>.
- 22 Schenck, Michael. "Password Reuse Defeats the Purpose of Passwords." Help Net Security, March 15, 2021. <https://www.helpnetsecurity.com/2021/03/15/password-reuse/>.
- 23 Leonard, Collin. "Happy Groundhog Day! Here's How to Escape a Time Loop—Just In Case." *Deseret News*, Feb 2, 2023. <https://www.deseret.com/23582184/groundhog-day-movie-time-loop>.

- 24 Mims, Christopher. "Annoying Password Rules Actually Make Us Less Secure." *Wall Street Journal*, March 11, 2023. https://www.wsj.com/articles/annoying-password-rules-actually-make-us-less-secure-a05edb70?mod=tech_lead_pos8.
- 25 Why You Should Never Use the Same Password for More than One Account." Get Cyber Safe. Government of Canada, accessed September 3, 2025. <https://www.getcybersafe.gc.ca/en/blogs/why-you-should-never-use-same-password-more-one-account>.
- 26 Kan, Michael. "Here Are 2024's Most Used (and Worst) Passwords: Is Yours on the List?" *PCMag*, November 14, 2024. <https://www.pcmag.com/news/most-common-worst-passwords-2024-nordpass-is-yours-on-the-list>.
- 27 Dashlane. 2023. "What Credential Stuffing Is." Dashlane Blog. September 26, 2023. <https://www.dashlane.com/blog/what-credential-stuffing-is>.
- 28 Viezelyte, Kamile. 2024. "How Many Passwords Does the Average Person Have?" NordPass Blog, April 24, 2024. <https://nordpass.com/blog/how-many-passwords-does-average-person-have/>.
- 29 Grimes, Roger. 2026. "Your Password Needs to Be 25 Characters or Longer Due to AI and Quantum." LinkedIn, January 27, 2026. <https://www.linkedin.com/pulse/your-password-needs-25-characters-longer-due-ai-quantum-roger-grimes-ukjge>.
- 30 Abbott, Jacob and Daniel Calarco, and L. Jean Camp. "Factors Influencing Password Reuse: A Case Study. TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy 2018." SSRN (March 19, 2018). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3142270.
- 31 Tarun, Renee. "Great Cyber Hygiene Starts with a Culture of Security Awareness." CSO Online, September 21, 2022. <https://www.csoonline.com/article/3674628/great-cyber-hygiene-starts-with-a-culture-of-security-awareness.html>.
- 32 Gilbertson, Scott. "The Best Password Managers to Secure Your Digital Life." *Wired*, October 30, 2025. <https://www.wired.com/story/best-password-managers/>.
- 33 Fruhlinger, Josh. "SSO Explained: Single Sign-on Definition, Examples, and Terminology." CSO Online, June 3, 2022. <https://www.csoonline.com/article/2115776/sso-explained-single-sign-on-definition-examples-and-terminology.html>.
- 34 Viezelyte, Kamile. "How to implement a password policy that works." NordPass, January 14, 2014. <https://nordpass.com/blog/password-policy/>.
- 35 Security, Legit. "10 Benefits of Multi-Factor Authentication (MFA)." ASPM, AI Remediation & Secrets Scanning: AI-Native Application Security. Legit Security, March 31, 2025. <https://www.legitsecurity.com/aspm-knowledge-base/benefits-of-multi-factor-authentication>.
- 36 Haney, Julie. Users Are Not Stupid: Six Cyber Security Pitfalls Overturned. Gaithersburg,

MD: National Institute of Standards and Technology. March 16, 2023.
<https://www.nist.gov/publications/users-are-not-stupid-six-cyber-security-pitfalls-overturned>.

- [37](#) Jimmy. “20 Unforgettable Songs About Mistakes.” MusicalHow. June 20, 2024.
<https://www.musicalhow.com/songs-about-mistakes>.
- [38](#) Bhaskar, Ranjit. 2023. “The Role of Human Factors Engineering in Cybersecurity.” ISACA Journal, Volume 4, August 23, 2023. <https://www.isaca.org/resources/isaca-journal/issues/2023/volume-4/the-role-of-human-factors-engineering-in-cybersecurity>.
- [39](#) Sbampato, Ignacio. 2025. “Humans Are the Weakest Link—But Which Humans?” Security Boulevard, February 6, 2025. <https://securityboulevard.com/2025/02/humans-are-the-weakest-link-but-which-humans/>.

Chapter 8

- 1 Marlborough, Conor. “What Is ‘Simjacking’? Here’s How the Mobile Phone Sim Card Scam Works.” Inews.Co.Uk. Associated Newspapers Limited, October 16, 2019. <https://inews.co.uk/news/technology/simjacking-mobile-phone-sim-card-scam-how-explained-security-351250>.
- 2 Trend Micro. “What Is a SIM Swap Scam & How to Stay Protected?” Trend Micro News, February 23, 2022. <https://news.trendmicro.com/2022/02/23/what-is-a-sim-swap-scam-how-to-stay-protected/>.
- 3 Bhardwaj, Pranav. “What Is SIM Jacking and What Can You Do to Protect Yourself?” MUO, October 1, 2022. <https://www.makeuseof.com/what-is-sim-jacking/>.
- 4 Barrett, Brian. “How to Protect Your Phone Against a SIM Swap Attack.” *Wired*, August 19, 2018. <https://www.wired.com/story/sim-swap-attack-defend-phone/>.
- 5 Barrett, Brian. “How Twitter CEO Jack Dorsey’s Account Was Hacked.” *Wired*, August 30, 2019. <https://www.wired.com/story/jack-dorsey-twitter-hacked/>.
- 6 Nathaniel Popper, “Hackers Hit Twitter CEO Jack Dorsey in ‘SIM Swap.’ You’re at Risk, Too.” *New York Times*, September 5, 2019. <https://www.nytimes.com/2019/09/05/technology/sim-swap-jack-dorsey-hack.html>.
- 7 Winder, Davey. “Mariah Carey and Adam Sandler Social Media Accounts With 23 Million Followers Hacked.” *Forbes*, January 3, 2020. <https://www.forbes.com/sites/daveywinder/2020/01/03/mariah-carey-and-adam-sandler-social-media-accounts-with-23-million-followers-hacked/>.
- 8 Glaze, Virginia. “Fans Outraged after Late YouTuber Etika’s Twitter Account Hacked.” *Dexerto*, August 24, 2019. <https://www.dexerto.com/entertainment/fan-outraged-late-youtuber-etika-twitter-account-hacked-947970/>.
- 9 Winters, Mike. “This SIM card scam once fooled Jack Dorsey—here’s how to avoid it.” *CNBC*, February 19, 2022. <https://www.cnn.com/2022/02/19/how-to-avoid-sim-card-scam-that-once-fooled-jack-dorsey.html>.
- 10 The Federal. “Explained: How QR Codes Work, and How They Are Hacked.” *Federal*, July 18, 2022. <https://thefederal.com/explainers-2/explained-how-qr-codes-work-and-how-they-are-hacked/>.
- 11 Shrauner, Damon. “QR Codes and Contactless Ordering: Still Relevant in 2025?” *CKitchen*, May 22, 2025. <https://www.ckitchen.com/blog/2025/5/qr-codes-and-contactless-ordering-still.html>.
- 12 Kalamut, Anthony. “Coinbase QR Code Super Bowl Ad.” *YouTube*, February 18, 2022.

<https://www.youtube.com/watch?v=uJ9pNQrz0fA>.

- 13 Gartenberg, Chaim. “Coinbase’s Bouncing QR Code Super Bowl Ad Was So Popular It Crashed the App.” *Verge*, February 13, 2022. <https://www.theverge.com/2022/2/13/22932397/coinbases-qr-code-super-bowl-ad-app-crash>.
- 14 Eddy, Max. “Coinbase’s Mystery QR Code Super Bowl Ad Is a Security Nightmare.” *PCMag*. February 14, 2022. <https://www.pcmag.com/opinions/coinbases-mystery-qr-code-super-bowl-ad-is-a-security-nightmare>.
- 15 Kody. “Create Malicious QR Codes to Hack Phones & Other Scanners.” *WonderHowTo*, August 23, 2019. <https://null-byte.wonderhowto.com/how-to/create-malicious-qr-codes-hack-phones-other-scanners-0197416/>.
- 16 Masjedi, Yaniv. “How To Spot a Fake QR Code Scam [9 New Examples].” *Aura*, December 4, 2023. <https://www.aura.com/learn/fake-qr-code-scams>.
- 17 Federal Bureau of Investigation, “Oregon FBI Tech Tuesday: Building a Digital Defense Against QR Code Scams.” FBI – Portland Field Office, October 19, 2021. <https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-against-qr-code-scams>.
- 18 Federal Bureau of Investigation, “Cybercriminals Tampering with QR Codes to Steal Victim Funds,” Internet Crime Complaint Center (IC3), January 18, 2022. <https://www.ic3.gov/PSA/2022/PSA220118>.
- 19 City of Austin. “Fraudulent QR Codes Found on Austin Parking Pay Stations.” *AustinTexas.gov News*, January 3, 2022. Accessed via Internet Archive. <https://web.archive.org/web/20220103195959/https://www.austintexas.gov/news/fraudulent-qr-codes-found-austin-parking-pay-stations>.
- 20 Irei, Alissa. “QR Code Phishing: 14 Quishing Prevention Tips.” *Search Security*. TechTarget, April 9, 2025. <https://www.techtarget.com/searchsecurity/feature/Quishing-on-the-rise-How-to-prevent-QR-code-phishing>.
- 21 Baran, Guru. “QR Code Phishing Attack Bypasses Email Security Scanners & Abuse SharePoint.” *Cyber Security News*, September 23, 2024. <https://cybersecuritynews.com/qr-phishing-email-security-sharepoint/>.
- 22 Brien/CEO, Jim O. “Criminals Are Using QR Codes to Scam People in Restaurants!” *Techbuzzireland*. Jim O Brien Tech, September 26, 2022. <https://techbuzzireland.com/2022/09/26/criminals-are-using-qr-codes-to-scam-people-in-restaurants/>.
- 23 Lord, Bob. “Attack of the Evil Baristas.” *Medium*, November 12, 2024. <https://medium.com/@boblord/attack-of-the-evil-baristas-b204436f0853>.
- 24 Lord, Robert. Hacklore, accessed November 24, 2025. <https://www.hacklore.org>.

- [25](#) Lord, Bob. 2021. "Hacklore and Advice to Non-Technical People." Medium, February 19, 2021. <https://medium.com/@boblord/hacklore-and-advice-to-non-technical-people-e3d38c27d9cf>.
- [26](#) Albertyn, Robyn. "Exploring Hidden QR Codes in 'Moon Knight' (and More)." QR Code generator. Bitly, January 31, 2024. <https://www.qr-code-generator.com/blog/hidden-qr-code/>.
- [27](#) Binder, Matt. "Beware the QR code scams." Mashable, October 2, 2022. <https://mashable.com/article/beware-qr-code-scams>.
- [28](#) Goodin, Dan. "Android Barcode Scanner with 10 Million+ Downloads Infects Users." Ars Technica, February 8, 2021. <https://arstechnica.com/information-technology/2021/02/android-barcode-scanner-with-10-million-downloads-infects-users/>.

Chapter 9

- 1 Ortiz, Andi. “Superman’s Catchphrase Is No Longer ‘Truth, Justice and the American Way.’” Yahoo Entertainment, October 16, 2021. <https://www.yahoo.com/entertainment/superman-catchphrase-no-longer-truth-181600149.html>.
- 2 Hacker Noon. “The Nigerian Prince Email and the History of Social Engineering Techniques.” HackerNoon, August 21, 2023. <https://hackernoon.com/the-nigerian-prince-email-and-the-history-of-social-engineering-techniques>.
- 3 Mascellino, Alessandro. “Report Reveals 341% Rise in Advanced Phishing Attacks.” Infosecurity Magazine, May 22, 2024. <https://www.infosecurity-magazine.com/news/341-rise-advanced-phishing-attacks/>.
- 4 Hook, Steve. “We Threw a Party for ChatGPT’s First Birthday and Here’s What Happened.” PC Guide, November 30, 2023. <https://www.pcguides.com/ai/happy-birthday-chatgpt/>.
- 5 Nield, David. “How ChatGPT and Other LLMs Work—and Where They Could Go Next.” Wired, April 30, 2023. <https://www.wired.com/story/how-chatgpt-works-large-language-model/>.
- 6 Stevenson, Mark. “Large Language Models: How the AI behind the Likes of ChatGPT Actually Works.” Conversation, December 10, 2024. <https://theconversation.com/large-language-models-how-the-ai-behind-the-likes-of-chatgpt-actually-works-244701>.
- 7 Dutta, Tushar Subhra. “FraudGPT: New Black Hat AI Tool Launched by Cybercriminals.” Cyber Security News, July 27, 2023. <https://cybersecuritynews.com/fraudgpt-new-black-hat-ai-tool/>.
- 8 Krishnan, Rakesh. “FraudGPT: The Villain Avatar of ChatGPT.” Netenrich, July 25, 2023. <https://netenrich.com/blog/fraudgpt-the-villain-avatar-of-chatgpt>.
- 9 Shea, Sharon. “How AI Is Making Phishing Attacks More Dangerous.” Search Security. TechTarget, October 22, 2024. <https://www.techtarget.com/searchsecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous>.
- 10 Alex, Williams. “The Rise of Adaptive Phishing: When AI Learns to Manipulate.” Communications of the ACM, April 17, 2025. <https://cacm.acm.org/blogcacm/the-rise-of-adaptive-phishing-when-ai-learns-to-manipulate/>.
- 11 Hunt, Troy. “Troy Hunt: A Sneaky Phish Just Grabbed My Mailchimp Mailing List.” Troy Hunt, March 25, 2025. <https://www.troyhunt.com/a-sneaky-phish-just-grabbed-my-mailchimp-mailing-list/>.

- [12](#) Ibid.
- [13](#) Ibid.
- [14](#) Lance, Spitzner. “What Is Phishing Resistant MFA?” Cyber Security Training, Degrees & Resources | SANS Institute, October 6, 2022. <https://www.sans.org/blog/what-is-phishing-resistant-mfa/>.
- [15](#) Keytos. “Phishing Resistant MFA with YubiKey.” Keytos Blog, November 25, 2024. <https://www.keytos.io/blog/passwordless/phishing-resistant-yubikey-authentication.html>.
- [16](#) Wagenseil, Paul. “The Rise of Phishing-Resistant MFA and What It Means for a Passwordless Future.” *SC Media*, November 12, 2024. <https://www.scworld.com/resource/the-rise-of-phishing-resistant-mfa-and-what-it-means-for-a-passwordless-future>.
- [17](#) Hunt, “A Sneaky Phish.”

Chapter 10

- 1 Hunt, Alex. "WWE Star Describes The Pain Of Being Chopped By Gunther." ITR Wrestling, April 3, 2024. <https://itrwrestling.com/news/wwe-star-describes-the-pain-of-being-chopped-by-gunther/>.
- 2 Parsons, Jim. "Fan Who Attacked Seth Rollins Apparently Catfished By Fake Rollins Social Media Account." TheSportster, November 23, 2021. <https://www.thesportster.com/fan-who-attacked-seth-rollins-catfished-by-fake-account/>.
- 3 Ibid.
- 4 Annese, John, Kerry Burke, and Larry McShane. "NYC Fan Who Tackled WWE Wrestler Seth Rollins at Barclays Speaks." *New York Daily News*, November 24, 2021. <https://www.nydailynews.com/2021/11/24/fan-who-tackled-wwe-star-seth-rollins-at-barclays-center-sought-revenge-for-apparent-catfish-scam-exclusive/>.
- 5 Business Insider. "Brad Pitt has 'no shame' about his job as a El Pollo Loco mascot before making it big in Hollywood—'Man's Gotta Eat.'" Business Insider, September 13, 2019. <https://www.businessinsider.com/brad-pitt-el-pollo-loco-mascot-ellen-show-video-2019-9>.
- 6 France 24. 2025. "French Woman Faces Cyberbullying after Falling for Fake Brad Pitt." France 24, January 14, 2025. <https://www.france24.com/en/live-news/20250114-french-woman-faces-cyberbullying-after-falling-for-fake-brad-pitt>.
- 7 Quinn, Liam. "Scammers Posing as Brad Pitt Swindled Woman Out of \$800,000: Report." *PEOPLE*, January 14, 2025. <https://people.com/scammers-brad-pitt-swindled-woman-report-8774403>.
- 8 Ibid.
- 9 Ibid.
- 10 McMillan, Robert. "A Text Scam Called 'Pig Butchering' Cost Her More Than \$1.6 Million." *Wall Street Journal*, October 20, 2022. <https://www.wsj.com/articles/a-text-scam-called-pig-butchering-cost-her-more-than-1-6-million-11666258201?mod=djemCybersecruityPro&tpl=cy>.
- 11 Merrill, Jeremy B., and Steven Zeitchik. "A Cryptocurrency Scam That Used the Coinbase Wallet Led to \$66.3 Million in Lost Crypto." *Washington Post*, April 4, 2022. <https://www.washingtonpost.com/technology/2022/04/04/crypto-scams-coinbase-liquidity-mining/>.
- 12 Baltrusaitis, Justinas. "What Is Liquidity Mining?" Finbold, February 11, 2022. <https://finbold.com/guide/liquidity-mining-definition/>.
- 13 CoinCodeCap. "9 Best DeFi Apps in 2025." CoinCodeCap, September 28, 2025.

<https://coincodemap.com/best-defi-apps>.

- 14 Hacken. "Liquidity Pools Explained: How They Work, Key Risks & Security Measures." Hacken, June 26, 2025. <https://hacken.io/discover/liquidity-pools/>.
- 15 Internet Crime Complaint Center (IC3). "Scammers Target and Exploit Owners of Cryptocurrencies in Liquidity Mining Scam." Internet Crime Complaint Center (IC3), July 21, 2022. <https://www.ic3.gov/PSA/2022/PSA220721>.
- 16 Merrill, "A Cryptocurrency Scam."
- 17 Internet Crime Complaint Center (IC3), "Scammers Target and Exploit Owners."
- 18 Colburn, Ken. "Data Doctors: Understanding Random 'Smishing' Text Messages." WTOP News, April 25, 2025. <https://wtop.com/cyber-security/2025/04/data-doctors-understanding-random-smishing-text-messages/>.
- 19 Orcutt, Ashley Mae. "Why Do Scammers Use WhatsApp and Google Hangouts to Message Victims?" SocialCatfish, October 28, 2022. <https://socialcatfish.com/scamfish/why-do-scammers-use-whatsapp-and-google-hangouts-to-message-victims/>.
- 20 Obi, Osaji. "How to Tell If You're Being Catfished: 12 Signs & Free Methods." Social Catfish, October 23, 2025. <https://socialcatfish.com/scamfish/12-signs-might-getting-catfished-online>.
- 21 Showfety, Sarah. "What Is Behavior Mirroring and When Should You Use It?" Lifehacker, April 28, 2022. <https://lifehacker.com/what-is-behavior-mirroring-and-when-should-you-use-it-1848849649>.
- 22 Smith, Lydia. "Verbal Mirroring: Why Is It Important at Work?" Yahoo News, April 29, 2021. <https://news.yahoo.com/verbal-linguistic-mirroring-at-work-pros-and-cons-230153273.html>.
- 23 Shellenbarger, Sue. "Use Mirroring to Connect With Others." *Wall Street Journal*, September 20, 2016. <https://www.wsj.com/articles/use-mirroring-to-connect-with-others-1474394329?msocid=341cf477dc7366691e3de22bdd256787>.
- 24 Obi, "How to Tell If You're Being Catfished."
- 25 Campbell, Travis. "What Is Love Bombing? The First Step in a Romance Scam." Social Catfish, August 15, 2025. <https://socialcatfish.com/scamfish/what-is-love-bombing-romance-scam-warning-signs/>.
- 26 Van Dyk, Deirdre. "9 Ways Scammers Like to Be Paid." AARP, April 1, 2021. <https://www.aarp.org/money/scams-fraud/info-2021/preferred-ways-to-pay.html>.
- 27 Obi, Osaji. "Gift Card Scams: How To Handle Them." Social Catfish, November 21, 2022, <https://socialcatfish.com/scamfish/gift-card-scams-how-to-handle-them/>.

- 28 Crookes, David. "How to Do a Reverse Search Image Using Google." Tom's Guide, March 30, 2023. <https://www.tomsguide.com/how-to/how-to-do-a-reverse-image-search-using-google>.

Chapter 11

- 1 Brookes, Tim, and Chris Hoffman. "What Is a Burner Phone, and When Should You Use One?" How-To Geek. LifeSavvy Media, February 17, 2021. <https://www.howtogeek.com/712588/what-is-a-burner-phone-and-when-should-you-use-one/>.
- 2 Saltzman, Marc. "Why You Might Want to Own a 'Burner Phone.'" *USA TODAY*, September 17, 2016. <https://www.usatoday.com/story/tech/columnist/saltzman/2016/09/17/whats-a-burner-phone/90382874/>.
- 3 Brownlee, Jason. "A Gentle Introduction to Generative Adversarial Networks (GANs)." Machine Learning Mastery, July 19, 2019. <https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/>.
- 4 Mohebbi Moghaddam, B. Boroomand, M. Jalali, et al. "Games of GANs: Game-Theoretical Models for Generative Adversarial Networks." *Artificial Intelligence Review* 56 (2023): 9771–9807. <https://doi.org/10.1007/s10462-023-10395-6>.
- 5 Jemine, Corentin. "Real-Time-Voice-Cloning: Clone a Voice in 5 Seconds to Generate Arbitrary Speech in Real-Time." GitHub, accessed September 15, 2022. <https://github.com/CorentinJ/Real-Time-Voice-Cloning>.
- 6 Edward, Frank. "Top 10 Deepfake Voice Software & Online Tools Review." VanceAI Technology, November 24, 2024. <https://vansmedia.vanceai.com/deepfake-voice-software-and-online-tools-review/>.
- 7 Stupp, Catherine. "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case." *Wall Street Journal*, August 30, 2019. <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>.
- 8 Harwell, Dre. "Artificial-Intelligence Voice Is Used in a Theft." *Washington Post*, September 4, 2019. <https://www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/>.
- 9 Brewster, Thomas. "Fraudsters Cloned Company Director's Voice In \$35 Million Bank Heist, Police Find." *Forbes*, October 14, 2021. <https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=10ea95507559>.
- 10 RSA. "RSA Quarterly Fraud Report Volume 1, Issue 3 Q3 2018." United States Documents. Documents, accessed September 15, 2022. <https://documents.pub/document/rsa-quarterly-fraud-report-vogel-the-rsa-quarterly-fraud-report-contains-fraud.html?page=1>.

- 11 U.S. Department of Health and Human Services Health Sector Cybersecurity Coordination Center (HC3). "Vishing Attacks on the Rise." HC3: Analyst Note. U.S. Department of Health and Human Services Health Sector Cybersecurity Coordination Center (HC3), 2022. <https://www.hhs.gov/sites/default/files/vishing-attacks-on-the-hph-sector-analyst-note.pdf>.
- 12 Agari & PhishLabs. 2022. Quarterly Threat Trends & Intelligence Report – August 2022. Fortra, August 2022. <https://static.fortra.com/phishlabs/pdfs/report/fta-pl-agari-phishLabs-qttiI-report-august-2022.pdf>.
- 13 Bienkiewicz, David. "Examples of Effective Vishing Attacks." Compass IT Compliance, March 4, 2020. <https://www.compassitc.com/blog/examples-of-effective-vishing-attacks>.
- 14 Budgar, Laurie. "What Is Amazon's Alexa and What Can It Do?" AOL.com, June 9, 2021. <https://www.aol.com/amazon-alexa-151337952.html>.
- 15 McGregor, Lucas. "What I Learned by Developing a Top Alexa Skill." Medium, February 4, 2025. <https://lucas-mcgregor.medium.com/what-i-learned-by-developing-a-top-alexa-skill-3ce643615521>.
- 16 Prasad, Rohit. "Amazon Re:MARS 2022 - Day 2 - Keynote." YouTube, June 23, 2022. <https://www.youtube.com/watch?v=22cb24-sGhg>.
- 17 Ibid.
- 18 Kurhekar, Shantanu. "Alexa Is Coming to Hospitals and Senior Living Communities to Improve Care Experience and Help Fight Loneliness." Alexa Blog. Amazon, Inc., October 25, 2021. <https://developer.amazon.com/en-US/blogs/alexa/device-makers/2021/10/alexa-is-coming-to-hospitals-and-senior-living-communities>.
- 19 Schuster-Bruce, Catherine. "Amazon: Hospitals to Put Alexa Next to Patient Beds, Staff Enter Room Less." Business Insider, October 26, 2021. <https://www.businessinsider.com/amazon-alexa-hospitals-echo-next-to-us-hospital-bed-2021-10>.
- 20 Prasad, "Amazon Re: MARS 2022."
- 21 Ibid.
- 22 Ingram, Michael Brandon. "Amazon Alexa Voice Assistant Gets Creepy New Feature." GameRant, June 24, 2022. <https://gamerant.com/amazon-alexa-voice-mimicking-feature/>.
- 23 Mellor, Sophie. "Amazon's Plan for Alexa to Mimic Anyone's Voice Raises Fears It Will Be Used by Criminals." *Fortune*, June 23, 2022. <https://fortune.com/2022/06/23/amazons-plan-for-alexa-to-mimic-anyones-voice-raises-fears-it-will-be-used-for-deepfakes-and-scams/>.
- 24 Palmer, Annie. "Amazon Demonstrates Alexa Mimicking the Voice of a Deceased Relative." CNBC, June 22, 2022. <https://www.cnbc.com/2022/06/22/amazon->

[demonstrates-alexa-mimicking-the-voice-of-a-deceased-relative.html](#).

- 25 Sundaravelu, Anugraha. “Alexa Mimicking Human Voices Poses a Threat to Security, Experts Warn.” *Metro Associated Newspapers Limited*, June 24, 2022. <https://metro.co.uk/2022/06/24/alexa-mimicking-human-voices-poses-a-threat-to-security-experts-warn-16880992/>.
- 26 Rushing, Ellie. “Voice Scammers Can Impersonate Your Loved Ones in Fraudulent Calls. Just Ask This Center City Lawyer.” *Philadelphia Inquirer*, March 9, 2020. <https://www.inquirer.com/news/voice-scam-impersonation-fraud-bail-bond-artificial-intelligence-20200309.html>.
- 27 Lacoma, Tyler. “Amazon’s Privacy Ultimatum Starts Today: Let Echo Devices Process Your Data or Stop Using Alexa.” CNET, March 28, 2025. <https://www.cnet.com/home/security/a-privacy-ultimatum-starts-today-let-amazon-echo-process-your-data-or-stop-using-it/>.
- 28 Thubron, Rob. “Amazon Removes Privacy Option, All Alexa Recordings Will Now Go to the Cloud.” TechSpot, March 17, 2025. <https://www.techspot.com/news/107175-amazon-removing-option-local-alexa-processing-forcing-all.html>.
- 29 Ibid.
- 30 Harding, Scharon. “Alexa Had ‘No Profit Timeline,’ Cost Amazon \$25 Billion in 4 Years.” *Ars Technica*, July 23, 2024. <https://arstechnica.com/gadgets/2024/07/alexa-had-no-profit-timeline-cost-amazon-25-billion-in-4-years/>.
- 31 Mattioli, Dana. “Alexa Is in Millions of Households—and Amazon Is Losing Billions.” *Wall Street Journal*, July 22, 2024. <https://www.wsj.com/tech/amazon-alexa-devices-echo-losses-strategy-25f2581a>.
- 32 Wiggers, Kyle. “Amazon Alexa+ Costs \$19.99, Free for Prime Members.” TechCrunch, February 26, 2025. <https://techcrunch.com/2025/02/26/amazon-alexa-costs-19-99-free-for-prime-members/>.
- 33 Harding, Scharon. “Everything You Say to Your Echo Will Be Sent to Amazon Starting on March 28.” *Ars Technica*, March 14, 2025. <https://arstechnica.com/gadgets/2025/03/everything-you-say-to-your-echo-will-be-sent-to-amazon-starting-on-march-28/>.
- 34 Lacoma, Tyler. “Amazon’s Privacy Ultimatum Starts Today: Let Echo Devices Process Your Data or Stop Using Alexa.” CNET, March 28, 2025. <https://www.cnet.com/home/security/a-privacy-ultimatum-starts-today-let-amazon-echo-process-your-data-or-stop-using-it/>.
- 35 Matt Day, Giles Turner and Natalia Drozdiak. “Thousands of Amazon Workers Listen to Alexa Conversations.” *TIME*, April 11, 2019. <https://time.com/5568815/amazon-workers-listen-to-alexa/>.

- [36](#) Ibid.
- [37](#) Federal Trade Commission. “FTC and DOJ Charge Amazon with Violating Children’s Privacy Law by Keeping Kids’ Alexa Voice Recordings Forever and Undermining Parents’ Deletion Requests.” Federal Trade Commission, May 31, 2023. <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever>.
- [38](#) Brodesser-Akner, Taffy. “What Happened to Val Kilmer? He’s Just Starting to Figure It Out.” *New York Times*, May 6, 2020. <https://www.nytimes.com/2020/05/06/magazine/val-kilmer.html>.
- [39](#) Flynn, John. “Helping Actor Val Kilmer Reclaim His Voice.” Sonantic, accessed August 20, 2021. <https://www.sonantic.io/blog/helping-actor-val-kilmer-reclaim-his-voice>.
- [40](#) Chung, Jackson. “Sonantic Uses Artificial Intelligence to Recreate Val Kilmer’s Voice from Old Recordings.” TechEBlog, August 14, 2021. <https://www.techeblog.com/artificial-intelligence-val-kilmer-sonantic-voice/>.
- [41](#) Sonantic. “Hear Val Kilmer’s AI Voice.” YouTube, August 9, 2021. <https://www.youtube.com/watch?v=OSMue60Gg6s>.
- [42](#) Sharf, Zack. “Val Kilmer Recreated His Speaking Voice Using A.I. Algorithm.” IndieWire, August 17, 2021. <https://www.indiewire.com/features/general/val-kilmer-recreated-speaking-voice-ai-algorithm-1234658600/>.
- [43](#) Johns Hopkins Medicine. 2019. “Voice Disorders.” Johns Hopkins Medicine, December 2, 2019. <https://www.hopkinsmedicine.org/health/conditions-and-diseases/voice-disorders>.
- [44](#) Palmai, Kitt. “Voice Cloning of Growing Interest to Actors and Cybercriminals.” BBC News, July 11, 2021. <https://www.bbc.com/news/business-57761873>.
- [45](#) Index SpeechTeam, “IndexTTS2: A Breakthrough in Emotionally Expressive and Duration-Controlled Auto-Regressive Zero-Shot Text-to-Speech,” accessed December 29, 2025, <https://index-tts.github.io/index-tts2.github.io/>.
- [46](#) Rosner, Helen. “A Haunting New Documentary About Anthony Bourdain.” *New Yorker*, July 15, 2021. <https://www.newyorker.com/culture/annals-of-gastronomy/the-haunting-afterlife-of-anthony-bourdain>.
- [47](#) Tangcay, Jazz. “Anthony Bourdain’s AI-Faked Voice in New Documentary Sparks Backlash.” *Variety*, July 15, 2021. <https://variety.com/2021/artisans/news/anthony-bourdain-fake-voice-roadrunner-documentary-backlash-1235020878/>.
- [48](#) Martin, Brett. “What Was Anthony Bourdain Searching For?” *GQ*, July 13, 2021. <https://www.gq.com/story/anthony-bourdain-morgan-neville-roadrunner-documentary>.
- [49](#) Bourdain, Ottavia. “I Certainly Was NOT the One Who Said Tony Would Have Been Cool with That.” Twitter, July 16, 2021.

<https://twitter.com/OttaviaBourdain/status/1415889455005716485?s=20>.

- 50 Rosner, Helen. "The Ethics of a Deepfake Anthony Bourdain Voice." *New Yorker*, July 17, 2021. <https://www.newyorker.com/culture/annals-of-gastronomy/the-ethics-of-a-deepfake-anthony-bourdain-voice>.
- 51 FBI Internet Crime Complaint Center (IC3). "Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions." Public Services Announcement. Federal Bureau of Investigation, June 23, 2022. <https://www.ic3.gov/PSA/2022/PSA220628>.
- 52 Ibid.
- 53 The U.S. Department of State, the U.S. Department of the Treasury, and the Federal Bureau of Investigation. "Guidance on the Democratic People's Republic of Korea Information Technology Workers." The U.S. Department of State, the U.S. Department of the Treasury, and the Federal Bureau of Investigation, May 16, 2022. <https://ofac.treasury.gov/media/923126/download?inline>
- 54 Ibid.
- 55 Karras, Tero, Samuli Laine, and Timo Aila. "A Style-Based generator Architecture for Generative Adversarial Networks." *IEEE Transactions on Pattern Analysis and Machine Intelligence*, no. 12 (December): 4217–28. <https://doi.org/10.1109/tpami.2020.2970919>.
- 56 Ume, Chris. "Deeptomcruise." TikTok. Chris Ume, accessed September 26, 2022. <https://www.tiktok.com/@deeptomcruise>.
- 57 BuzzFeed Video, and Jordan Peele. 2018. "You Won't Believe What Obama Says In This Video!" YouTube, April 17, 2018. <https://www.youtube.com/watch?v=cQ54GDm1eL0>.
- 58 Cherry, Kendra. "13 Types of Common Cognitive Biases That Might Be Impairing Your Judgement." Verywell Mind, February 22, 2024. <https://www.verywellmind.com/cognitive-biases-distort-thinking-2794763>.
- 59 Heshmat, Shahram. "What Is Confirmation Bias?" *Psychology Today*, April 23, 2015. <https://www.psychologytoday.com/us/blog/science-choice/201504/what-is-confirmation-bias>.
- 60 Inman, Mary. "Hindsight Bias." Encyclopædia Britannica, accessed September 26, 2022. <https://www.britannica.com/topic/hindsight-bias>.
- 61 Whitten, Cheryl. "What is the Halo Effect?" WebMD, June 21, 2024. <https://www.webmd.com/mental-health/what-is-halo-effect>.
- 62 Quote Investigator. "Who Ya Gonna Believe Me or Your Own Eyes?" Quote Investigator, accessed September 26, 2022. <https://quoteinvestigator.com/2018/07/31/believe-eyes/>.
- 63 Ellyatt, Holly. "As Ukraine Recaptures Lost Land, Is This a Turning Point in the War?" CNBC, September 14, 2022. <https://www.cnbc.com/2022/09/14/as-ukraine-recaptures-lost-land-is-this-a-turning-point-in-the-war-.html>.

- 64 Gumenyuk, Nataliya. "Putin Is Mobilising 300,000 More Soldiers to Fight His War. But Ukrainians Feel Hope, Not Fear." *Guardian*, September 22, 2022. <https://www.theguardian.com/commentisfree/2022/sep/22/vladimir-putin-reservists-ukrainians-russian-families-war-kremlin>.
- 65 Washington Post Staff, "Read Putin's national address on partial military mobilization." *Washington Post*, September 21, 2022. <https://www.washingtonpost.com/world/2022/09/21/putin-speech-russia-ukraine-war-mobilization>.
- 66 BBC News. "George Floyd: What Happened in the Final Moments of His Life." BBC News, July 16, 2020. <https://www.bbc.com/news/world-us-canada-52861726>.
- 67 Ibid.
- 68 Karnowski, Steve. "Lung Expert Testifies George Floyd Died Because His Breathing Was Restricted." PBS NewsHour, February 7, 2022. <https://www.pbs.org/newshour/nation/lung-expert-testifies-george-floyd-died-because-his-breathing-was-restricted>.
- 69 Shapiro, Emily, and Whitney Lloyd. "\$27 Million Settlement for George Floyd's Family Approved by Minneapolis City Council." ABC News, March 12, 2021. <https://abcnews.go.com/US/27-million-settlement-george-floyds-family-approved-minneapolis/story?id=76419755>.
- 70 Brown, Kyle. "The Officers Responsible: Where Are They 5 Years after George Floyd's Murder?" KSTP.Com 5 Eyewitness News, May 26, 2025. <https://kstp.com/kstp-news/top-news/the-officers-responsible-where-are-they-5-years-after-george-floyds-death/>.
- 71 Heartstrong, Winnie. "Dr. Winnie Heartstrong Claims George Floyd IS ALIVE and the Video Is FAKED. History Is the Conspiracy." YouTube, June 3, 2020. <https://web.archive.org/web/20200604112332/https://www.youtube.com/watch?v=QdstwBNDZPg>.
- 72 Ibid.
- 73 Derysh, Igor. "GOP House Candidate Publishes Lengthy Report Claiming George Floyd's Killing Was a 'Deepfake' Hoax." Salon.Com, June 24, 2020. <https://www.salon.com/2020/06/24/gop-house-candidate-publishes-lengthy-report-claiming-george-floyds-killing-was-a-deepfake-hoax/>.
- 74 Heartstrong, Winnie. "George Floyd Is Dead: A Citizen's Investigative Report on the Use of Deep Fake Technology." June 14, 2020. https://newworld.politics.blog/wp-content/uploads/2021/05/gf-is-dead-a-citizens-investigative-report_redacted.pdf.
- 75 Ibid.
- 76 Ibid.

- [77](#) Sommer, Will. "GOP House Candidate Winnie Heartstrong Insists George Floyd Killing Was Staged." *Daily Beast*, June 24, 2020. <https://www.thedailybeast.com/gop-house-candidate-winnie-heartstrong-insists-george-floyd-killing-was-staged/>.
- [78](#) Chesney, Robert, and Danielle Keats Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *SSRN Electronic Journal*, July 21, 2018. <https://doi.org/10.2139/ssrn.3213954>.
- [79](#) Sonnemaker, Tyler. "Deepfakes, the 'Liar's Dividend,' and the Future of Misinformation." *Business Insider*, April 13, 2021. <https://www.businessinsider.com/deepfakes-liars-dividend-explained-future-misinformation-social-media-fake-news-2021-4>.
- [80](#) Chesney and Citron, "Deepfakes: A Looming Challenge."
- [81](#) Ibid.
- [82](#) Miller, Michael E. "JFK assassination conspiracy theories: The grassy knoll, umbrella man, LBJ and Ted Cruz's dad." *Washington Post*, October 24, 2017. <https://www.washingtonpost.com/news/retropolis/wp/2017/10/24/jfk-assassination-conspiracy-theories-the-grassy-knoll-umbrella-man-lbj-and-ted-cruzs-dad/>.
- [83](#) Royal Museums Greenwich. "Moon Landing Conspiracy Theories, Debunked." Royal Museums Greenwich, accessed October 1, 2022. <https://www.rmg.co.uk/stories/topics/moon-landing-conspiracy-theories-debunked>.
- [84](#) Ruiz, Carlos Diaz. "I Watched Hundreds of Flat-Earth Videos to Learn How Conspiracy Theories Spread – and What It Could Mean for Fighting Disinformation." *Conversation*, June 27, 2022. <https://theconversation.com/i-watched-hundreds-of-flat-earth-videos-to-learn-how-conspiracy-theories-spread-and-what-it-could-mean-for-fighting-disinformation-184589>.

Chapter 12

- 1 Li, Yuezun, Ming-Ching Chang, and Siwei Lyu. “In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking.” IEEE International Workshop on Information Forensics and Security (WIFS), June 11, 2018. <https://ieeexplore.ieee.org/document/8630787>.
- 2 Vincent, James. “Deepfake Detection Algorithms Will Never Be Enough.” Verge, June 27, 2019. <https://www.theverge.com/2019/6/27/18715235/deepfake-detection-ai-algorithms-accuracy-will-they-ever-work>.
- 3 Lyu, Siwei. “Deepfakes and the New AI-Generated Fake Media Creation-Detection Arms Race.” *Scientific American*, July 20, 2020. <https://www.scientificamerican.com/article/detecting-deepfakes1/>.
- 4 Jones, Rupert. “Voice Recognition: Is It Really as Secure as It Sounds?” *Guardian*, September 22, 2018. <https://www.theguardian.com/money/2018/sep/22/voice-recognition-is-it-really-as-secure-as-it-sounds>.
- 5 Miller, Dan. “‘Hacking’ Voiceprints? Little to Fear If You Take Precautions.” Opus Research, September 3, 2019. <https://opusresearch.net/wordpress/2019/09/03/hacking-voiceprints-little-to-fear-if-you-take-precautions/>.
- 6 Kassis, Andre, and Uri Hengartner. “Practical Attacks on Voice Spoofing Countermeasures.” July 30, 2021. <https://arxiv.org/pdf/2107.14642.pdf>.
- 7 Sharma, Harshita. “AI Voice Cloning Threatens Banking Security, Warns OpenAI CEO.” SUBKUZ, July 23, 2025. <https://subkuz.com/news/english/details/ai-voice-cloning-threatens-banking-security/92457>.
- 8 Goodreads. “Quote by Ernest Hemingway: ‘How Did You Go Bankrupt?’” Goodreads, accessed October 18, 2022. <https://www.goodreads.com/quotes/102579-how-did-you-go-bankrupt-two-ways-gradually-then-suddenly>.
- 9 New York University Tandon School of Engineering. “Outsmarting Deep Fakes: Researchers Devise an AI-Driven Imaging System That Protects Authenticity.” NYU Tandon School of Engineering, May 29, 2019. <https://engineering.nyu.edu/news/outsmarting-deep-fakes-researchers-devise-ai-driven-imaging-system-protects-authenticity>.
- 10 Nikon. “Nikon Authenticity Service.” Nikon USA, accessed December 29, 2025. <https://www.nikonusa.com/content/nikon-authenticity-service>.
- 11 Iral, Vince. “Countering Deepfakes Using Digital Watermarks and Blockchain Technology.” Parola Analytics, August 11, 2021. <https://parolaanalytics.com/countering-deepfakes-using-digital-watermarks-and-blockchain-technology/>.

- 12 Dickinson, Emily. “‘Hope’ Is the Thing with Feathers.” Poetry Foundation, accessed October 11, 2022. <https://www.poetryfoundation.org/poems/42889/hope-is-the-thing-with-feathers-314>.
- 13 J.P. Morgan Chase. “How to Develop a Strong Callback Process.” J.P. Morgan Chase, July 11, 2019. <https://www.jpmorgan.com/commercial-banking/insights/develop-strong-callback-process>.
- 14 Smith, Steve. “Better a Safeword than a Sorry One.” Advantage, May 25, 2025. <https://advantage.nz/better-a-safeword-than-a-sorry-one/>.

Chapter 13

- 1 Telegraph. “Robert Ettinger.” *Telegraph*, July 24, 2011. Accessed October 21, 2025. <https://www.telegraph.co.uk/news/obituaries/science-obituaries/8658435/Robert-Ettinger.html>.
- 2 Alcor Life Extension Foundation. “Pricing and Dues.” Alcor Life Extension Foundation, accessed October 21, 2025. <https://www.alcor.org/membership/pricing-and-dues/>.
- 3 Alcor Life Extension Foundation. “Cryopreservation Procedures.” Alcor Life Extension Foundation, accessed October 21, 2025. <https://www.alcor.org/cryopreservation-procedures/>.
- 4 Dashti, Amirreza, and Sofia Ani. “Exploring the Frontiers of Cryonics: Feasibility, Benefits, and Future Impact on Humanity.” *World Journal of Biology Pharmacy and Health Sciences* 20 (2): 602–608. <https://doi.org/10.30574/wjbphs.2024.20.2.0785>.
- 5 Mascelli, Jillian, and Megan Rodden. “Harvest Now Decrypt Later: Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks.” Finance and Economics Discussion Series 2025-093. Washington: Board of Governors of the Federal Reserve System, September, 2025. <https://doi.org/10.17016/FEDS.2025.093>.
- 6 QuEra Computing. “Preparing for Y2Q: The Ultimate Guide to Surviving the Quantum Leap.” QuEra Blog, accessed October 21, 2025. <https://www.quera.com/blog-posts/preparing-for-y2q-the-ultimate-guide-to-surviving-the-quantum-leap>.
- 7 Hurley, William, and Floyd Smith. 2023. “What Are Superposition & Entanglement in Quantum Computing.” *Quantum Computing For Dummies*, September 18, 2023. <https://www.dummies.com/article/technology/computers/what-are-superposition-entanglement-in-quantum-computing-300563/>.
- 8 Reddy, Anurag. “Is Quantum Computing the End of Personal Privacy as We Know It?” *Analytics Insight*, October 14, 2025. <https://www.analyticsinsight.net/quantum-computing-analytics-insight/is-quantum-computing-the-end-of-personal-privacy-as-we-know-it>.
- 9 Hauschild, D., Spencer, B., & Dipesh Gadher. “China’s chilling stolen data plot for everyone in Britain.” *Sunday Times*, October 18, 2025. <https://www.thetimes.com/uk/defence/article/china-stolen-personal-data-britain-8lw0bpmmc?msocid=23cf1f2ba085640b105509a7a11165de>.
- 10 Walton, Alyssa. “The Impact of Quantum Decryption.” *Cyber Defense Magazine*. June 16, 2025, accessed October 21, 2025. <https://www.cyberdefensemagazine.com/the-impact-of-quantum-decryption/>.
- 11 Thipsay, Aabha. “Microsoft’s Quantum-Resistant Cryptography Is Here.” Microsoft Security Blog. September 9, 2024, accessed October 21, 2025.

<https://techcommunity.microsoft.com/blog/microsoft-security-blog/microsofts-quantum-resistant-cryptography-is-here/4238780>.

- 12 Harish, Anusha. “What Is Cryptographic Agility and Why Does It Matter?” SecureW2 Blog, January 30, 2024, accessed October 21, 2025. <https://www.securew2.com/blog/cryptographic-agility-why-it-matters>.
- 13 Vaibhav, Harsh. “4 Emerging Technologies That Are Helping Us in the Fight Against Climate Change.” Earth.Org, May 2, 2025. <https://earth.org/4-emerging-technologies-that-are-helping-us-in-the-fight-against-climate-change>.
- 14 Goodchild, Joan. “The Dual Threat of AI and Quantum Computing: IT Leaders Brace for the Next Data Security Era.” CIO, August 27, 2025. Accessed October 23, 2025. <https://www.cio.com/article/4046977/the-dual-threat-of-ai-and-quantum-computing-it-leaders-brace-for-the-next-data-security-era.html>.
- 15 Ramaswamy, Mithilesh. “Biometric Security in the AI Era: Comprehensive Mitigation Strategies for Institutions and Individuals.” Harvard Global Business Review, August 15, 2025. Accessed October 23, 2025. https://hgbr.org/research_articles/biometric-security-in-the-ai-era-comprehensive-mitigation-strategies-for-institutions-and-individuals/.
- 16 Katwala, Amit. “The Quantum Apocalypse is Coming: Be Very Afraid.” *Wired*, March 24, 2025. Accessed October 23, 2025. <https://www.wired.com/story/q-day-apocalypse-quantum-computers-encryption/>.
- 17 Shin, Daniel. “Using Deepfake Techniques as an Obfuscation Information Security Defensive Mechanism.” *Journal of Information Warfare* 23 (4): 30–44.
- 18 Houston-Edwards, Kelsey. “Tomorrow’s Quantum Computers Threaten Today’s Secrets. Here’s How to Protect Them.” *Scientific American*, February 1, 2024. Accessed on October 23, 2025. <https://www.scientificamerican.com/article/tomorrows-quantum-computers-threaten-todays-secrets-heres-how-to-protect-them/>.

Chapter 14

- 1 McEvoy, Fiona J. “Deepfaking the Deceased: Is It Ever Okay?” You The Data, January 23, 2021. <https://youthedata.com/2021/01/23/deepfaking-the-deceased-is-it-ever-okay/>.
- 2 Young, Maya. “Anthony Bourdain Documentary Sparks Backlash for Using AI to Fake Voice.” *Guardian*, July 16, 2021. <https://www.theguardian.com/food/2021/jul/16/anthony-bourdain-documentary-ai-voiceover-roadrunner>.
- 3 Mason, Andrew. “Thoughts on Cloning Voices of the Deceased.” Descript, July 15, 2021. <https://www.descript.com/blog/article/thoughts-on-cloning-voices-of-the-deceased>.
- 4 Rice, Clayton. “The Ethics of Voice Cloning.” Clayton Rice K.C., July 17, 2021. <https://www.claytonrice.com/the-ethics-of-voice-cloning/>.
- 5 Ibid.
- 6 Strand, Robert. “The Brand Management Of Dead Celebrities.” Branding Strategy Insider, June 30, 2020. <https://brandingstrategyinsider.com/the-brand-management-of-dead-celebrities/>.

Chapter 15

- 1 Whittaker, Jack M., Suleman Lazarus, Taidgh Corcoran. “Are Fraud Victims Nothing More than Animals? Critiquing the Propagation of ‘Pig Butchering’ (Sha Zhu Pan, 杀猪盘).” *Journal of Economic Criminology* 3 (2024): 1–8.
<https://www.sciencedirect.com/science/article/pii/S2949791424000046>.
- 2 Ibid.
- 3 Ibid.
- 4 Szalavitz, Maia. “Why We’re Psychologically Hardwired to Blame the Victim.” *Guardian*, February 27, 2018. <https://www.theguardian.com/us-news/2018/feb/27/victim-blaming-science-behind-psychology-research>.
- 5 Cheery, Kendra. “Why Does Blaming the Victim Happen?” *Verywell Mind*, August 3, 2015. <https://www.verywellmind.com/why-do-people-blame-the-victim-2795911>.
- 6 Hampson, Paul. “Romance Baiting: A New Term for a Disturbing Scam.” *CEL Solicitors*, February 13, 2025. <https://www.facebook.com/CELSolicitors/>.
<https://celsolicitors.co.uk/romance-baiting-a-new-term-for-a-disturbing-scam/>.
- 7 AARP. “Shifting the Conversation About Scams: No More Victim Blaming March 2025.” AARP, March 26, 2025. Accessed on September 6, 2025. <https://states.aarp.org/new-hampshire/shifting-the-conversation-about-scams-no-more-victim-blaming>.
- 8 Operation Shamrock. “What is the Crypto Coalition?” Operation Shamrock. Accessed April 14, 2025. <https://operationshamrock.org/about/crypto-coalition>.
- 9 Riley, Tonya. “This Bay Area Prosecutor Wants to Help Police Nationwide Take on ‘pig Butchering’ Scams.” *CyberScoop*, April 17, 2023. <https://cyberscoop.com/erin-west-pig-butchering-cryptocurrency-scams/>.
- 10 Prey, Easy. “Pig Butchering Is Getting Worse with Erin West - Easy Prey Podcast.” *Easy Prey Podcast*, October 2, 2024. <https://www.easyprey.com/pig-butchering-is-getting-worse-with-erin-west/>.
- 11 Erin West, “Written Testimony before the Subcommittee on National Security, Illicit Finance, and International Financial Institutions, Committee on Financial Services, U.S. House of Representatives.” September 18, 2024. <https://democrats-financialservices.house.gov/uploadedfiles/hhrg-118-ba10-wstate-west-20240918.pdf>.
- 12 “Seize, Burn, Block, Reissue: Understanding the Legal Tools Behind Crypto Asset Recovery.” *TRM*, June 23, 2025. <https://www.trmlabs.com/resources/blog/seize-burn-block-reissue-understanding-the-legal-tools-behind-crypto-asset-recovery>.

Chapter 16

- 1 Toubba, Karim. "12-22-2022: Notice of Security Incident." LastPass, December 22, 2022. Accessed April 14, 2025. <https://blog.lastpass.com/posts/notice-of-recent-security-incident>.
- 2 Ibid.
- 3 Kapko, Matt. "After LastPass Hack, Only Its Master Passwords Remain Uncompromised." Cybersecurity Dive, December 27, 2022. <https://www.cybersecuritydive.com/news/lastpass-breach-exposes-passwords/639469/>.
- 4 Freedman, Linn. "LastPass Updates Disclosure of Security Incident." JD Supra, January 5, 2023. <https://www.jdsupra.com/legalnews/lastpass-updates-disclosure-of-security-9075918/>.
- 5 Turton, William. "LastPass Says Hackers Stole Customer Data, Encrypted Passwords." *Seattle Times*, December 23, 2022. <https://www.seattletimes.com/business/lastpass-says-hackers-stole-customer-data-encrypted-passwords/>.
- 6 Freedman, "LastPass Updates Disclosure."
- 7 Chen, Brian X. "A Breach at LastPass Has Password Lessons for Us All." *New York Times*, January 5, 2023. <https://www.nytimes.com/2023/01/05/technology/personaltech/lastpass-breach-password-safety.html>.
- 8 Palant, Wladimir. "What's in a PR Statement: LastPass Breach Explained." *Almost Secure*, December 26, 2022. <https://palant.info/2022/12/26/whats-in-a-pr-statement-lastpass-breach-explained/>.
- 9 Gatlan, Sergiu. "LastPass Now Requires 12-Character Master Passwords for Better Security." Bleeping Computer, January 3, 2024. <https://www.bleepingcomputer.com/news/security/lastpass-now-requires-12-character-master-passwords-for-better-security/>.
- 10 Summerson, Cameron. "I Switched from LastPass to 1Password (and You Should, Too)." *How-To Geek*, July 23, 2020. <https://www.howtogeek.com/47843/i-switched-from-lastpass-to-1password-and-you-should-too/>.
- 11 "7 Publicly Known LastPass Security Breaches since 2011." *Privacy Guides: The Expert's Guide to Online Privacy in 2023*. Accessed September 6, 2025. <https://www.privacytools.io/guides/7-publicly-known-lastpass-security-breaches-since-2011>.
- 12 Robinson, Teri. "LastPass Devs Were Phished for Credentials." *Security Boulevard*. <https://www.facebook.com/groups/24445075146/>. March 1, 2023. <https://securityboulevard.com/2023/03/lastpass-devs-were-phished-for-credentials/>.

- 13 Zorz, Zeljka. "LastPass Says Attackers Got Users' Info and Password Vault Data." Help Net Security, December 23, 2022. <https://www.helpnetsecurity.com/2022/12/23/lastpass-breach-customer-vault/>.
- 14 "LastPass Breach – The Danger of Metadata – PwnDefend." PwnDefend. Accessed September 6, 2025. <https://www.pwndefend.com/2022/12/24/lastpass-breach-the-danger-of-metadata/>.
- 15 23andMe. "Addressing Data Security Concerns - Action Plan." 23andMe Blog. <https://www.facebook.com/23andMe/>. October 6, 2023. <https://blog.23andme.com/articles/addressing-data-security-concerns>.
- 16 Franceschi-Bicchierai, Lorenzo. "23andMe Resets User Passwords after Genetic Data Posted Online." TechCrunch. <https://www.facebook.com/techcrunch>. October 10, 2023. <https://techcrunch.com/2023/10/10/23andme-resets-user-passwords-after-genetic-data-posted-online/>.
- 17 Newman, Lily Hay, and Andy Greenberg. "23andMe Blames Users for Recent Data Breach as It's Hit With Dozens of Lawsuits." *Wired*, January 6, 2024. <https://www.wired.com/story/23andme-blames-users-data-breach-security-roundup/>.
- 18 French, Laura. "23andMe confirms nearly 7 million customers affected in data leak." SC Media, December 4, 2023. <https://www.scworld.com/news/23andme-confirms-nearly-7-million-customers-affected-in-data-leak>.
- 19 Office of the Privacy Commissioner of Canada. "Backgrounder: Summary of Joint Investigation into Data Breach at 23andMe by the Privacy Commissioner of Canada and the UK Information Commissioner." June 17, 2025. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2025/bg_23andme_250617.
- 20 Kan, Michael. "LastPass Employee Could've Prevented Hack With a Software Update." PCMag, March 3, 2023. <https://www.pcmag.com/news/lastpass-employee-couldve-prevented-hack-with-a-software-update>.
- 21 Bonnet, Scott. "The Importance of Patch Management: Lessons from the LastPass Hack." Spiceworks Inc, March 16, 2023. <https://community.spiceworks.com/t/the-importance-of-patch-management-lessons-from-the-lastpass-hack/948273>.
- 22 Ballon, Ian. "23andMe Response Letter to Tycko Zavareei LLP." DocumentCloud, December 11, 2023. <https://www.documentcloud.org/documents/24252535-response-letter-to-tycko-zavareei-llp/>.
- 23 Franceschi-Bicchierai, Lorenzo. "23andMe tells victims it's their fault that their data was breached." TechCrunch, January 3, 2024. <https://techcrunch.com/2024/01/03/23andme-tells-victims-its-their-fault-that-their-data-was-breached/>.
- 24 Ibid.
- 25 Reed, Rachel. "We just need to use the laws we have—and enforce them." *Harvard Law*

Today, July 23, 2024. <https://hls.harvard.edu/today/harvard-law-expert-discusses-data-breaches-failures-and-the-vulnerability-of-everyday-technology/>.

- [26](#) Ashenmacher, George. “No Harm, No Foul? Exploring the Harm Caused by Data Breaches.” Retrieved from the University Digital Conservancy, May 2015. <https://hdl.handle.net/11299/174782>.
- [27](#) Morrissey, Matthew M., Andy Taylor, and Charles E. Westerhaus. “Courts Reject Theoretical Privacy Violations Due to Lack of Standing.” Faegre Drinker, April 21, 2025. <https://www.faegredrinker.com/en/insights/publications/2025/4/courts-reject-theoretical-privacy-violations-due-to-lack-of-standing>.
- [28](#) Breached Company Privacy Blog Team. “The Rising Bar: Why ‘No Harm, No Foul’ Is Becoming the New Reality in Data Breach Litigation.” Breached Company, September 28, 2025. <https://breached.company/the-rising-bar-why-no-harm-no-foul-is-becoming-the-new-reality-in-data-breach-litigation/>.
- [29](#) Loten, Angus. “No Harm, No Foul: Courts Take Tougher Line on Data-Breach Suits.” *Wall Street Journal*, September 26, 2025. <https://www.wsj.com/articles/no-harm-no-foul-courts-take-tougher-line-on-data-breach-suits-fadffa4a>.
- [30](#) Ibid.
- [31](#) Ibid.
- [32](#) Ballon, “23andMe Response Letter.”
- [33](#) Contributors to Wikimedia projects. 2019. “Just Culture.” Wikimedia Foundation, Inc., June 28, 2019. https://en.wikipedia.org/wiki/Just_culture.

Conclusion

- [1](#) Person, Chris. “The Flipper Zero Is a Swiss Army Knife of Antennas.” *Verge*, November 2, 2022. <https://www.theverge.com/23433594/flipper-zero-hacking-gadget-wireless-pentesting-open-source-antenna>.
- [2](#) McCormick, Colin and Derek Draven. “Dirty Harry: The Most Iconic Quotes In The Entire Franchise.” *ScreenRant*, Updated April 11, 2024. <https://screenrant.com/dirty-harry-most-iconic-best-quotes/>.

Index

A

- access points, [45](#), [49](#)
- accountability, [258](#)
 - corporate, [88](#), [106](#), [240](#), [243](#), [248](#), [250](#), [254](#)
 - employee, [251–52](#)
 - shared, [252](#)
- AI. *See* [artificial intelligence \(AI\)](#)
- AI-generated voices. *See* [voice cloning](#)
- air-gapping, [61](#), [64](#)
- Alexa, [162–67](#), [219](#)
 - Do Not Save Recordings option, [168](#)
 - Do Not Send Voice Recordings option, [166](#), [168–69](#)
 - privacy enabling of, [167](#), [68–69](#)
- Alexa Plus (Amazon voice assistant), [166](#), [167–70](#)
 - context awareness, [167](#)
 - Do Not Send Voice Recordings option, [166](#), [168–69](#)
 - generative AI processing, [167–68](#)
 - privacy disabling of, [166](#), [167–69](#)
 - Voice ID, [169](#)
 - voice recognition capabilities, [166](#)
- Amazon, [162–70](#)
 - Personal Voice Filter, [164–66](#)
- Anne (catfishing victim), [137–38](#)
- anonymizers, [35](#)
- Anthropic, [129](#)
- antivirus software, [63](#), [113](#)
- Apologia Pro Vita Sua* (Newman), [69](#)
- Apple
 - iCloud storage, [6](#)
- artificial intelligence (AI), [10](#), [124–29](#), [156](#), [211–15](#)
 - ambient, [162–63](#)
 - generative, [124–25](#), [167–69](#), [213–14](#), [215](#)
- Ashkenazi Jews, [241](#)
- Ashley Madison (dating site), [25–26](#)
- attack vectors, [256](#)
- attacks
 - personalized, [126–28](#)
 - See also* individual types of attacks

authentication, [213](#)
 added layers for, [198](#)
authenticator apps, [106](#), [108](#)
Authy (Twilio), [105](#)
aviation security, [27–33](#)
Avid Life Media, [25](#)

B

Baca, Alejandro, [62](#)
backstories, [141](#)
BadUSB Beetle, [62](#), [260](#)
BadUSBs, [59–66](#), [67](#), [75](#), [76](#), [101](#)
banks, [196–98](#)
Barcode Scanner (app), [118](#)
biases, [258](#)
 cognitive, [180–83](#), [191](#), [193](#)
 confirmation, [180](#)
 fundamental attribution error, [229–30](#)
 hindsight, [180](#)
 just-world, [228–29](#)
Binance, [234](#), [236](#)
biometrics, [131](#)
 fingerprint, [197](#), [198](#)
 voiceprint, [164–65](#), [196–98](#), [199](#)
Bitcoin, [26](#), [84](#), [85](#), [105](#), [109–10](#)
bits, [210](#)
black hats, [26](#)
 See also [cybercriminals](#)
blackmail, [84](#)
BlackMatter, [37](#)
blame shifting
 corporate, [243–53](#), [259](#)
blinking (eyes), [194](#), [202](#)
block chains, [4](#)
Boeing
 hacking into their airplanes, [28–33](#)
Bored Apes (NFTs), [4–5](#)
bots, [128](#)
Bourdain, Anthony, [176](#), [220](#), [221](#)
Bourdain, Ottavia, [176](#), [221](#), [222](#)
BreachForums, [240–41](#)
Brown, Traci, [23](#)
browsers
 Chrome, [49](#)
 warnings of, [49](#)

brute force attacks, [93](#), [101](#), [238](#), [256](#)
BruteSpray, [98](#)
bug bounties, [27](#), [70](#)
bug hunters, [71](#)
burner phones, [155](#), [204](#)

C

callbacks, [161](#), [204](#), [207](#), [258](#)
CanadianKingpin, [124](#)
cancer
 throat, [170–72](#), [222](#)
“casing the joint,” [154](#), [155](#)
Catfish (documentary), [5](#)
catfishing, [5–7](#), [133](#), [234–36](#), [258](#)
 red flags, [143–53](#)
 See also [crypto-romance scams](#)
“Celebgate,” [6](#)
celebrities
 dead, deepfaking images and voices of, [223–24](#)
 hacking of, [6](#), [107](#)
cell phone carriers, [108](#)
 security PIN codes and, [106](#), [108](#)
ChatGPT, [124](#)
Chauvin, Derek, [183–85](#)
Chesney, Robert, [186](#), [189–91](#)
Chico Marx Factor, [181](#), [193](#), [258](#)
Chuckling Squad, [106](#), [107](#)
Citron, Danielle, [186](#), [189–91](#)
Cloudhopper (app), [106](#)
Coinbase, [116](#), [234](#), [236](#)
 Super Bowl ad, [109](#)
 Wallet, [141](#)
Collins, Ryan, [8](#)
Colonial Pipeline, [36–37](#), [86](#), [87](#)
communications
 claiming urgency, [130](#), [131](#), [149](#), [159](#), [206](#)
 with money requests, [129–30](#)
 peculiarly timed, [129](#), [131](#)
 red flags, [129–30](#)
computers, [43](#), [50](#), [102–3](#)
 quantum, [209–15](#)
 unlocked, [99](#)
consent
 informed, [29](#), [250](#)
 for voice cloning, [220](#), [221](#), [225](#)

- conspiracy theories, [185–86](#), [191–92](#)
- contactless ordering, [109](#)
- context awareness, [167–68](#)
- corporations
 - accountability, [88](#), [106](#), [240](#), [243](#), [248](#), [250](#), [254](#)
 - blame shifting of, [243–53](#), [259](#)
 - employee accountability, [251–52](#), [259](#)
- CrackMapExec, [98](#)
- credential stuffing, [54](#), [89–97](#), [237–38](#), [240](#), [241–42](#), [256](#)
- credit cards, [46](#), [47](#)
- credit monitoring services, [95](#)
- Cressey, Donald R., [16](#)
- criminality, [15–24](#)
- Cruise, Tom
 - deepfake videos of, [179](#), [203](#)
- crypto agility, [211](#), [213](#), [214](#)
- Crypto Coalition, [234–36](#)
- cryptocurrencies, [4](#), [84](#), [141–42](#)
 - law enforcement strategy for scams, [234–36](#)
- cryptographic keys, [131](#)
- crypto-romance scams, [6](#), [36](#), [37–38](#), [133–53](#), [227](#), [231–32](#), [234–36](#), [258](#), [261](#)
 - requests for money, [145–46](#), [150–51](#), [258](#)
 - use of messaging apps, [144](#)
 - use of pet names, [141](#), [149–50](#)
 - victims' embarrassment, [150](#), [228](#), [230](#)
- cyber hygiene, [100–101](#), [255–56](#)
 - awareness programs, [96](#), [101](#), [239–40](#)
- Cyber Mavens, [40](#), [255–59](#)
- cyberbullying, [138](#), [228](#)
- cybercrimes, [1](#), [3](#), [6](#), [34](#), [70](#), [71–72](#), [76–77](#), [83–85](#), [228–29](#)
 - corporate reporting of attacks, [88](#)
 - financing of, [36](#)
 - forums, [20](#), [35](#), [240–41](#)
 - governments' intervention and, [39–40](#), [230–31](#), [259](#), [262](#)
 - justifications for, [228](#)
 - launching of, [36–37](#)
 - law enforcement interventions, [234–36](#), [255](#)
 - public awareness of, [39–41](#), [87–88](#), [254](#) (*see also* cyber hygiene: awareness programs; cybersecurity: awareness programs)
 - reduction of, [39–41](#)
 - underreporting of, [37–38](#), [230](#), [234](#)
 - victim blaming and, [227–53](#), [258–59](#)
 - See also individual types of crimes*
- cybercriminals, [1–2](#), [8](#), [15–24](#), [76–77](#), [104](#), [254–55](#)
 - camouflage of identities, [35–36](#)

- probability of apprehension, [34](#), [255](#)
- cybergangs, [3](#), [25–26](#), [36–37](#), [63](#), [85](#), [87](#), [106](#), [107](#)
- cyber-savvy, [49](#), [75](#), [96](#), [256](#)
- cybersecurity, [2–3](#), [54](#), [65](#), [68](#), [71](#), [72–73](#), [86–88](#), [100](#)
 - awareness programs, [39–41](#), [65–66](#), [73](#), [74–79](#), [87–88](#), [205–8](#), [232](#), [251](#), [254](#), [259–60](#), [261](#)
 - company breaches and responsibility, [239–53](#), [254–55](#)
- cyber-sweeties, [148–49](#), [258](#)
- cyberweapons, [58–66](#)

D

- Dark Web, [35](#)
 - BreachForums on, [240–41](#)
 - posting on, [25–26](#), [84](#), [87](#), [89](#)
 - purchases on, [85](#), [89](#), [124–25](#)
- DarkSide, [3](#), [36–37](#), [85](#), [87](#)
- DarkWing84, [4](#)
- data
 - backup, [101](#), [256](#)
 - breaches, [84–85](#), [105](#), [237–53](#)
 - dismissal of breach claims, [247](#)
 - encryption, [16](#), [35](#), [46](#), [47](#), [48](#), [49](#), [50](#), [60](#), [64](#), [65](#), [83](#), [84](#), [85](#), [100](#), [101](#), [209–15](#), [239](#)
 - file transfer limits, [65](#)
 - ownership of, [8](#)
 - personal, [83](#), [129](#), [210](#), [247](#)
 - posting of, [25–26](#), [154](#), [240–41](#)
 - public-facing, [84](#), [154](#)
 - scraped, [242](#), [245](#), [250](#)
 - sensitive, [210](#)
 - stolen, [83](#), [87](#), [105](#), [111](#), [112](#), [210](#), [247–48](#)
 - synthetic/fake, [214](#)
- DCP. *See* Device Control Policy (DCP)
- decryption keys, [84](#), [239](#)
- Deep Fakes* (Chesney and Citron), [186](#), [189–91](#)
- deepfakes, [10](#), [99](#), [154–208](#), [212](#), [219](#), [257](#)
 - of Anthony Bourdain, [176](#), [219](#), [220](#), [221](#), [222](#)
 - awareness of, [199](#), [201–8](#), [261](#)
 - of Barack Obama, [179](#), [202](#), [203](#)
 - of dead people, [223–24](#)
 - detection of, [190](#), [194–208](#), [257](#)
 - ethical, [219–26](#)
 - government regulation and, [190–91](#)
 - job interview, [177–80](#)
 - of Johannes, [158–60](#), [219](#), [221](#)
 - legal actions and, [190](#)
 - photographs, [178–80](#)

- red flags, [202–8](#), [257](#)
- supremacy, [195–96](#), [198–99](#)
- of Val Kilmer, [170–72](#), [219](#), [221](#)
- DeFi Platform, [142](#)
- dehumanization, [227](#), [228](#), [231](#), [232](#)
- denial-of-service attacks, [52](#)
- Denso Wave, [109](#)
- Descript, [158](#)
- device control policies (DCPs), [65](#)
- devices
 - mobile, [100](#)
 - radiofrequency (RF)-emitting, [51](#)
 - whitelisted vs. blacklisted, [65](#)
 - wireless, [45](#)
 - See also* [Echo \(Amazon devices\)](#)
- digital source verification, [199](#)
- direct messages (DMs), [140](#), [144](#)
- Dorsey, Jack
 - SIM-jacking of smartphone, [106–7](#)
- DSTIKE Wi-Fi Duck, [62–63](#)
- Duck Soup* (movie), [181](#)
- Ducky Scripts, [62](#), [260](#)
- duties
 - segregation of, [17](#), [204–5](#), [207](#)

E

- Echo (Amazon devices), [162–70](#)
 - cloud opt-out, [166](#), [169](#)
 - Do Not Send Voice Recordings option, [166](#), [168–69](#)
 - local processing of voices, [166](#), [167](#), [169](#)
 - privacy and, [166](#), [169](#)
- EICCAS. *See* Engine Indicator Crew Alert System (EICAS)
- email
 - random, [144](#), [258](#)
 - work vs. personal, [99](#)
- empathy, [230](#), [232–33](#), [235](#), [258](#)
- employee assistance programs (EAPs), [18](#)
- encryption, [256](#)
 - data, [16](#), [35](#), [46](#), [47](#), [48](#), [49](#), [50](#), [60](#), [64](#), [65](#), [83](#), [84](#), [85](#), [100](#), [101](#), [209–15](#), [237](#), [239](#)
 - forced HTTPS, [50](#)
 - metadata, [239](#)
 - mobile devices, [100](#)
 - networks, [16](#), [35](#), [48](#), [49](#), [50](#), [64](#), [83](#), [84](#), [85](#), [101](#), [212–13](#)
- Engine Indicator Crew Alert System

(EICAS), [28](#)
Equifax, [87](#)
Established Men (dating site), [25–26](#)
ethics, [18](#), [19](#), [176–177](#)
 See also [accountability](#); blame shifting: corporate; deepfakes: ethical; hackers: ethical;
 hacking: ethical; [moral disengagement](#); [victim blaming](#)
evidence, [192](#), [258](#)
evil portals, [35](#), [45–46](#), [47](#), [48](#), [74](#), [76–77](#), [257](#)
evil twin, [45](#), [47](#)
experiences
 shared, [126](#)
 user, [54–55](#)
extortion, [26](#), [70](#), [84](#)
eye movements, [194](#), [202](#), [206](#), [207](#)

F

facial expressions, [202](#), [206](#), [207](#), [257](#)
Faraday bags, [57](#)
Flipper Zero, [10](#), [259–60](#)
Floyd, George, [183–85](#), [192](#)
Flynn, John, [171](#)
4chan, [6](#)
fraud prevention, [16–19](#)
Fraud Report (RSA), [160–61](#)
Fraud Triangle, [16–19](#)
FraudGPT, [124–25](#)
Fred Simian (NFT), [4–5](#)
fund transfers, [151](#), [205](#), [206–7](#)

G

game theory, [158](#)
GANs. *See* generative adversarial network (GANs)
Garofano, George, [8](#)
generative adversarial networks (GANs), [156–60](#), [178–80](#), [194–95](#)
 discriminators, [156](#)
 generators, [156](#), [179](#), [190](#)
gift cards, [36](#), [62](#), [135](#), [151](#)
Google, [49](#), [97](#)
 Authenticator, [106](#), [196](#)
 Chrome, [49](#)
 Image, [152–53](#)
Great Scott Gadgets, [52](#)
Green, Seth, [3–4](#), [228](#)
Greenstein v. Noblr, [246–47](#)
guilt, [227–28](#)

shifting, [233](#), [259](#)

H

hackers, [1–3](#)

ethical, [2](#), [3](#), [26–33](#), [72–73](#)

myths and stereotypes, [1–3](#), [8](#), [38](#), [111–12](#)

hacking, [9–10](#), [25–26](#)

ethical, [70](#), [72–73](#), [74](#)

legality of, [70](#)

smartphone, [104–8](#), [113](#)

See also [cybercrimes](#); and *individual types of attacks*

hacking tools and technology, [9](#), [10](#), [35](#), [42–79](#), [124](#), [156–60](#), [256–57](#), [259–61](#)

banning of, [67–68](#), [70](#), [71–72](#), [77](#), [78](#), [261](#)

benefits of, [69](#), [71](#), [72–76](#), [77](#)

control of, [67–68](#), [70](#), [71–72](#)

democratization of, [42](#), [73–76](#), [78](#), [166](#), [259](#), [261](#)

hacklore, [114–15](#)

HackRF One, [9](#), [52–53](#), [71](#), [76](#), [78](#)

hacktivism and hacktivists, [25](#), [70](#), [220](#)

Hak5, [43](#), [59](#)

modules/infusions, [44](#), [50](#)

SSL-Strip infusion, [50](#)

See also [Rubber Ducky \(USB drive\)](#); [Wi-Fi Pineapple \(router\)](#)

halo effect, [180](#)

Harvest Now, Decrypt Later (HNDL), [209–10](#)

HC3. *See* [U.S. Health Sector Cybersecurity Coordination Center \(HC3\)](#)

healthcare, [8–9](#), [163](#)

Heartstrong, Winnie, [185–86](#), [192](#)

Hengartner, Urs, [197](#)

Hermes, Euler, [158](#)

Herrera, Emilio, [8](#)

Hickey, Robert, [31–32](#)

HIDs. *See* [Human Interface Devices \(HIDs\)](#)

HNDL. *See* [Harvest Now, Decrypt Later \(HNDL\)](#)

Honda

key fobs, [53–54](#), [55–57](#)

response to Rolling Pwn vulnerability, [55–57](#)

rolling code mechanisms, [53–54](#), [55–57](#)

Honeypot System, [214–15](#)

HRD. *See* [radios: hardware-defined \(HDR\)](#)

HTTPS, [46–47](#), [48](#), [49](#), [50](#), [74](#), [78](#), [119](#)

forced encryption, [50](#)

forced redirection, [47](#)

human factors, [10](#), [88](#), [94](#), [98–101](#)

Human Interface Devices (HIDs), [59–60](#)

Hunt, Troy, [130–32](#)

I

identities, [5](#), [83–84](#), [210](#), [213](#)

See also [voice cloning](#)

IFEs. *See* [Inflight Entertainment Systems \(IFEs\)](#)

imageboards, [6](#)

Impact Team, [25–26](#)

IndexTTS2 (voice synthesis model), [175](#)

Inflight Entertainment Systems (IFEs), [28](#), [29](#), [30](#)

INTERPOL, [231](#)

investment frauds, [37–37](#), [141–43](#), [149](#)

J

jamming attacks, [52](#)

JBS Foods, [86](#)

Jemine, Corentin, [158](#)

Johannes (deepfake CEO), [158–60](#)

Johnson, Brett, [19–24](#)

Just Culture, [252](#), [259](#)

K

Kassis, Andre, [197](#)

Kekua, Lennay (fake persona), [5](#)

Kevin2600, [53](#), [55](#), [56](#), [71](#)

key fobs, [53–54](#), [55](#), [57](#)

keylogging, [62](#), [64](#), [243](#)

Kilmer, Val

voice loss and voice cloning of, [170–72](#), [220–21](#)

Kingsley, Charles, [69](#)

Kyocera AVX, [247](#)

L

Large Language Models (LLMs), [124](#), [129](#)

laryngitis, [173](#)

laryngopharyngeal reflux disease, [172](#)

LastPass, [237–40](#), [243](#)

lateral movement, [242](#), [248](#), [249](#)

Lawrence, Jennifer, [6–7](#), [228](#)

lawsuits, [190](#), [246–47](#)

standing (legal requirement), [246](#)

Li, Wesley, [53](#), [55](#), [56](#), [71](#)

liar's dividend, [186–91](#), [193](#), [258](#)

lingo shifting, [231–33](#), [258](#)

liquidity mining, [141–43](#), [149](#)

liquidity pools, [142](#)

LLMs. *See* [Large Language Models \(LLMs\)](#)

LockBit, [85](#)

login pages and logins

 automated tools, [89](#)

 fake, [45–46](#), [48](#), [77](#), [130](#), [131](#)

 password managers and, [97](#)

 secret questions on, [196](#)

 Single Sign-On (SSO), [96](#)

See also [passwords](#)

Lopez, Colby. *See* [Rollins, Seth “Freakin”](#);

Lord, Bob, [114](#)

love bombing, [138](#), [141](#), [143](#), [148–49](#), [150](#)

M

Mailchimp, [130](#), [132](#)

Majerczyk, Edward, [8](#)

malware, [59](#), [61](#), [63](#), [65](#), [83](#), [84](#), [85](#), [112](#), [113](#), [114](#), [257](#)

See also [keylogging](#); [ransomware](#)

man-in-the-middle (MITM) attacks, [44](#), [48](#), [260](#)

Marx, Chico, [181](#)

Mason, Andrew, [220](#)

Mendrez, Rodel, [62](#)

metadata, [239](#)

MFA. *See* [multifactor authentication \(MFA\)](#)

mirroring techniques, [146–47](#)

MITM attacks. *See* [man-in-the-middle \(MITM\) attacks](#)

Monday Night Raw (TV show), [135](#)

Moon Knight (TV show), [116](#)

moral disengagement, [228](#)

Mularski, Keith, [23](#)

multifactor authentication (MFA), [54](#), [87](#), [96](#), [97](#), [100](#), [101](#), [115](#), [131](#), [196](#), [256](#)

 codes texted to phone, [106](#), [108](#), [130](#)

 enforcement of, [238–39](#), [240](#), [242](#)

 phishing-resistant, [131–32](#)

N

nation-state threat actors, [3](#), [37](#), [43](#), [71](#), [72](#), [75](#), [84](#), [85](#), [90](#), [178](#), [183](#), [191](#), [213](#), [251](#)

networks

 encryption of, [16](#), [35](#), [48](#), [49](#), [50](#), [64](#), [83](#), [84](#), [85](#), [101](#), [212–13](#)

See also Wi-Fi networks

neuropreservation, [209](#)

Neville, Morgan, [176–77](#), [220](#), [221](#), [222](#)

Newman, John Henry, [68–69](#)

NFTs. *See* [non-fungible tokens \(NFTs\)](#)

Nigerian Prince scam, [121–23](#)

Nikon

Authenticity Service, [199](#)

No Harm, No Foul defense, [245–46](#), [247](#), [248](#)

noise

background, [160](#), [203](#), [207](#)

non-fungible tokens (NFTs), [3–5](#)

noob, [1](#)

NordPass, [95](#)

North Face, [95](#)

Norton LifeLock, [95](#)

nuclear facilities

Iran, [61](#)

NVIDIA, [178](#), [179](#)

O

Obama, Barack

deepfake video of, [179](#), [202](#), [203](#)

O'Meara, Diane, [5](#)

One World Labs, [32](#)

one-time passcodes (OTPs), [130–31](#)

OpenAI, [124](#), [129](#)

OpenSea, [4](#)

Operation Shamrock, [234–36](#)

OTPs. *See* [one-time passcodes \(OTPs\)](#)

OurMine, [89](#)

P

passwords, [95](#), [196](#)

breaches, [237–39](#)

common, [92–93](#)

enforcement of history control policy, [92](#), [97](#), [100](#)

managers, [96](#), [97](#), [255](#)

mandatory resets, [91–92](#)

master, [237–38](#)

on multiple accounts, [92](#)

reused, [54](#), [87](#), [88–97](#), [99](#), [101](#), [108](#), [237–38](#), [240](#), [241](#), [244](#), [256](#)

Salami Slice/slight changes of, [91](#)

shared, [99](#), [256](#)

stolen, [10](#), [87](#), [240](#)

strength of, [54](#), [92–93](#), [95–96](#), [100](#), [101](#), [238](#), [240](#), [255–56](#)

verbal, [205](#), [207](#), [208](#)

patch management programs, [243](#)

pattern recognition, [126](#)

payments

untraceable, [36](#), [105](#), [152](#), [258](#)

See also [blackmail](#); [crypto-romance scams](#); [extortion](#); [fund transfers](#); [ransomware](#); [sextortion](#)
PayPal, [95](#)
Peele, Jordan, [179](#), [202](#), [203](#)
penetration testers and testing. See [pentesters and pentesting](#)
pentesters and pentesting, [27](#), [29](#), [44](#), [51](#), [60](#), [70](#), [75](#), [261](#)
personal identification numbers (PINs), [131](#)
personally identifiable information (PII), [8](#), [83](#), [177](#), [239](#), [245–46](#)
phishing, [3–5](#), [6](#), [35](#), [45](#), [47](#), [101](#), [103](#), [118–19](#), [123–32](#), [139–40](#), [160](#), [251](#), [256](#)
 adaptive, [125–29](#), [130–32](#)
 call-back (See [vishing](#); hybrid)
 drive-by-QR, [113](#)
 emails with call back phone number, [161](#)
 emails with malicious attachments and links, [113](#)
 emails with malicious QR codes, [110](#), [113](#), [118–19](#)
 Nigerian Prince, [121–23](#)
 number of attacks, [8](#)
 QR (See [quishing](#))
 red flags, [48](#), [119](#), [125](#), [129–30](#), [257](#)
 smartphone (see [smishing](#))
 spear, [125–26](#), [239](#)
 voice (see [vishing](#))
photographs
 deepfake, [178–80](#)
 private, [6–8](#)
 stolen, [6–8](#)
pig butchering. See [crypto-romance scams](#)
PII. See [personally identifiable information \(PII\)](#)
PINs. See [personal identification numbers \(PINs\)](#), [131](#)
Pitt, Brad, [136–37](#)
PlaneSploit (app), [31](#)
PortaPack, [52](#), [56](#)
post-quantum cryptography (PQC), [211](#), [214](#)
power differentials, [159](#)
PQC. See [post-quantum cryptography \(PQC\)](#)
Prasad, Rohit, [163–64](#)
privacy, [6–8](#), [166–69](#), [247](#)
product security, [72–73](#)
Putin, Vladimir, [181–82](#)
pwn
 meaning and pronunciation, [1](#)

Q

QR codes, [10](#), [108–20](#), [257](#), [261](#)
 bill paying with, [117–18](#)
 code generators, [111](#)

- random, [116–19](#), [257](#)
- readers, [109](#)
- scanning apps, [118](#)
- tampering with, [117](#)
- quantum mechanics, [210](#)
- quantum-enhanced AI systems, [212](#)
- qubits, [210](#)
- quick response (QR) codes. See [QR codes](#)
- quishing, [110](#), [113](#), [118](#)
- Qureshi, Zeena, [171](#)

R

- RaaS. See [ransomware-as-a-service \(RaaS\)](#)
- radios
 - hardware-defined (HDR), [51](#)
 - software-defined (SDR), [51](#)
- ransomware, [85](#), [101](#), [114](#)
 - attacks, [8](#), [34](#), [35](#), [36–37](#), [38](#), [83–85](#), [86](#), [87](#), [104](#)
- ransomware-as-a-service (RaaS), [37](#), [85](#)
- Raspberry Pi, [43](#), [50](#)
- Real-Time Voice Cloning, [158](#)
- reconnaissance, [126](#)
- red teams, [70](#)
- replay attacks, [52–53](#)
- Resemble AI, [158](#)
- ReSpeecher, [158](#)
- reverse image searches, [141](#), [152–53](#)
- REvil, [3](#), [36–37](#), [85](#)
- Roadrunner* (documentary), [176–77](#), [220](#), [221](#), [222](#)
- Roberts, Chris, [28–30](#)
- Rolling Pwn Attack, [53–54](#), [55–57](#)
- Rollins, Seth “Freakin’”, [133–35](#)
- romance baiting. See [crypto-romance scams](#)
- Rosner, Helen, [221](#)
- Rubber Ducky (USB drive), [9](#), [59](#), [62](#), [63](#), [75](#), [76](#), [78](#), [256](#), [257](#)
- Russia
 - invasion of Ukraine, [181–82](#)

S

- safety, [228–29](#)
- Santamarta, Ruben, [32](#)
- Schreiber Foods, [86](#)
- SDR. See radios: software-defined (SDR)
- Seat Electronic Box (SEB), [30](#)
- Securities and Exchange Commission (SEC), [88](#)

- self-awareness, [193](#)
- servers
 - fake, [214](#), [215](#)
 - proxy, [35](#)
- service set identifiers (SSIDs), [45](#)
- sextortion, [26](#)
- sexual offenses, [6–8](#)
- ShadowCrew, [20](#), [21](#)
- Shin, Daniel, [213–14](#)
- side channel attacks, [52](#)
- SIM cards. See [subscriber identity module \(SIM\) cards](#)
- SIM-jacking, [105–8](#)
- Singing River Health System, [247](#)
- Single Sign-On (SSO), [97](#), [100](#)
- skepticism, [168–69](#), [190](#), [192](#), [193](#), [258](#)
- SlashNext, [123–24](#)
- smartphones
 - hacking of, [31](#), [102–20](#)
 - injecting malware into, [113](#)
 - PlaneSploit app on, [31](#)
 - QR code readers on, [109](#), [118](#)
 - SIM transfers, [105–8](#)
- Smashmouth Cybersecurity training, [40](#), [76–79](#), [255](#), [260–61](#)
- smishing, [103](#)
- smokescreen technology, [35–36](#)
- social engineering techniques, [101](#), [159](#), [206](#), [215](#)
- social media, [201](#)
 - fake profiles, [147–48](#)
 - oversharing and revealing personal data on, [99](#), [105–6](#), [107–8](#)
 - self-policing of, [191](#)
- software
 - anti-spam, [251](#)
 - patches and updates, [87](#), [99](#), [114](#), [243](#), [256](#)
 - USB device control, [65](#)
 - vulnerabilities, [26–27](#)
- Sonantic, [170–72](#), [220](#), [221–22](#)
 - Voice Engine software, [170–72](#)
- spasmodic dysphonia, [172](#)
- speech, [207](#)
 - out of character, [179](#), [203](#), [206](#), [207](#), [220](#), [257–58](#)
- Spencer, Elisah, [135–36](#)
- spoofing, [130](#), [213](#)
- SSIDs. See [service set identifiers \(SSIDs\)](#)
- SSL stripping attacks, [47](#)
- SSO. See [Single Sign-On \(SSO\)](#)

- stalling tactics, [20–21](#)
- standing (legal requirement), [246](#)
- Star-V Lab, [53](#), [55](#), [56](#), [57](#), [71](#)
- stereotypes, [1–3](#), [8](#), [38](#), [111–12](#), [180](#)
- stocks
 - short sale of, [46](#)
- Stumpf, Rob, [56](#)
- Stuxnet worm, [61](#), [64](#)
- subscriber identity module (SIM) cards, [105](#)
- superimposition, [202](#)
- survey sites, [113](#)
- system design, [100–101](#)

T

- targets, [140](#), [143](#)
- Te'o, Manti, [5–6](#), [228](#)
- telephone numbers
 - hacking of, [105](#), [106](#)
- TempestSDR, [52](#)
- Teso, Hugo, [31](#)
- text messages, [103](#)
 - random, [144](#)
 - red flags, [129–30](#)
- text-to-speech, [158](#)
 - custom voice models, [171](#)
- Threat Trends & Intelligence Report* (Agari and PhishLabs), [161](#)
- Top Gun: Maverick* (movie), [172](#), [221](#), [222](#)
- Toubba, Karim, [237–38](#)
- traceability, [35–36](#), [105](#), [152](#), [246–47](#), [258](#)
- TransUnion v. Ramirez*, [246](#)
- trickery, [10–11](#), [47](#)
- trust, [164](#)
- trust-jacking, [140–41](#), [146](#)
- Tuiasosopo, Naya, [5](#)
- 23andMe, [240–43](#), [244–45](#), [248–49](#), [252–53](#)
 - DNA Relatives tool, [240](#), [241–42](#), [244](#), [245](#), [249–50](#)
- Twitter, [107](#)

U

- U.S. Cybersecurity and Infrastructure Security Agency (CISA), [2](#)
- U.S. Department of Homeland Security (DHS), [2](#)
- U.S. Federal Aviation Administration (FAA), [31](#)
- U.S. Federal Bureau of Investigation (FBI), [28](#)
 - malicious QR code alerts, [111](#), [112](#), [114](#)
 - North Korean IT job applicants alert, [178](#)

- video job interviews alert, [177](#)
- U.S. Health Sector Cybersecurity Coordination Center (HC3), [161](#)
- U.S. Internet Crime Complaint Center (IC3) video job interviews alert, [177](#)
- U.S. National Institute of Standards and Technology (NIST), [211](#)
- U.S. Secret Service, [21](#)
- U.S. State Department
 - North Korean IT job applicants alert, [178](#)
- U.S. Treasury
 - North Korean IT job applicants alert, [178](#)
- Ubiquiti Inc., [45](#), [46](#)
- Ume, Chris, [203](#)
 - Tom Cruise deepfake videos, [179](#), [203](#)
- uranium centrifuges
 - Iran, [61](#)
- URLs, [46](#), [48](#), [49](#), [74](#), [110](#), [111](#), [114](#), [117](#), [119](#), [129](#)
- USB drives
 - bad/malicious, [35](#), [59–66](#), [67](#), [75](#), [76](#), [101](#), [259](#)
 - plugging in unknown, [61](#), [65](#), [78](#), [98](#), [99](#), [101](#), [256–57](#), [260](#)
 - port lockdown of, [65](#)
 - Wi-Fi enabled, [62–63](#)
 - See also* [Rubber Ducky \(USB drive\)](#)

V

- vehicle entry
 - fixed codes, [53](#)
 - keyless, [53–54](#), [55–57](#)
 - rolling code mechanisms, [53–54](#), [55–57](#)
- victim blaming, [227–53](#), [258–59](#), [261](#)
 - culture of, [230](#), [233](#)
- victims, [227–34](#), [243](#), [250](#), [258](#)
- videos
 - deepfake, [177–208](#)
 - deepfake detection, [190](#), [194–208](#)
 - deepfake supremacy, [195–96](#), [198–99](#)
 - real, [189–90](#), [199](#)
- vigorous, [63](#)
- virtual private networks (VPNs), [35](#), [48–49](#), [74](#), [87](#)
- vishing, [103](#), [154](#), [155–208](#)
 - control techniques, [204–5](#)
 - hybrid, [161](#)
- vocal cord paresis, [173](#)
- voice cloning, [156–77](#), [202–3](#), [219–21](#)
 - consent and, [220](#), [221](#), [225](#)
 - of dead people, [220](#), [221](#), [223–24](#)
 - disclosure of, [221–22](#), [225](#)

- platforms, [158](#), [162](#)
- red flags, [221](#)
- technical glitches, [160](#)
- unapproved, [219–20](#), [225](#)
- voice disorders, [170–73](#), [222](#)
- voice filters, [164](#)
- voice recognition, [167–68](#)
- voiceprints, [164–65](#), [196–98](#)
- voices
 - AI-generated (See [voice cloning](#))
 - actors, [174–75](#)
 - samples of, [154](#), [156](#), [197](#)
- VPNs. See [virtual private networks \(VPNs\)](#)

W

- wallets
 - crypto, [4](#), [236](#)
- Warren, Elizabeth, [88](#)
- watermarks
 - authentication, [199](#)
 - digital, [199](#), [214](#)
- Web of Make Believe* (documentary), [23](#)
- websites, [48](#)
 - company, [154](#)
 - dating, [25–26](#), [140](#), [144](#)
 - fake, [45](#), [78](#), [128](#)
 - imageboard, [6](#)
 - used to capture usernames and passwords, [45–46](#), [47](#), [111](#), [112](#), [113](#)
- Werewolf By Night #32* (comic book), [116](#)
- West, Erin, [234–35](#)
- white hats. See [hackers: ethical](#)
- Wi-Fi networks, [44](#), [45](#)
 - denial-of-service attacks, [52](#)
 - public, [45](#), [47–49](#), [74](#)
 - service set identifiers (SSIDs), [45](#)
- Wi-Fi Pineapple (router), [9](#), [10](#), [35](#), [43–50](#), [67](#), [74](#), [76–77](#), [78](#), [256](#), [257](#), [260](#)
- Wire, The* (TV show), [155](#)
- work from home (WFH)
 - deepfake video job interviews for, [177](#)
 - technical controls for equipment, [243](#)

Y

- Year to Quantum (Y2Q), [210](#), [211](#), [214](#)
- YubiKey, [131](#)

Z

zero-day exploits, [114](#), [256](#)

zero-day vulnerability, [114](#)

Zuckerberg, Mark, [89](#), [90](#)

ABOUT THE AUTHOR



Frank Riccardi is a cybersecurity and privacy expert who's passionate about empowering people and companies with the cyber-savvy needed to repel cyberattacks. With twenty-five years of experience in health-care compliance and privacy, he has led the response to high-risk data breaches and ransomware cyberattacks. Grappling with one cyberattack after another has led Frank to embark on a new journey and mission: Helping everyday people—whom he affectionately refers to as “non-geeks”—protect themselves from financially devastating and soul-crushing cyberattacks that can ruin their lives.

When Frank is not preaching the gospel of cyber hygiene, he indulges in his love for music as an audiophile and a vinyl record hoarder—or, as he prefers to call himself, a hobbyist. Notably, Frank guarantees that he is irrefutably human and not an avatar, bot, or AI. He lives with his wife in the charming city of Belmont, North Carolina.

PRAISE FOR



“Covering cybersecurity since 2004, I’ve watched the same core scams—impersonation, credential theft, confidence tricks—continually reinvent themselves. What began as crude phishing and identity theft now resurfaces as ransomware, business email compromise, and AI-driven deepfakes. To anyone outside the field, each wave can feel entirely new. Headlines warn of the latest threat, yet few resources step back to explain how these tactics evolve—and what that means for everyday consumers. In *CTRL+ALT+PWN*, Frank Riccardi brings welcome clarity. He demystifies modern cybercrime and connects the psychology, the tools, and the technology in plain English. This is the kind of contextual, up-to-date understanding consumers have long needed.”

—**BYRON ACOHIDO**, Pulitzer Prize-winning journalist and
Editor-in-Chief of *The Last Watchdog on Privacy & Security*

“In a field crowded with noise, *CTRL+ALT+PWN* stands out as a rare combination of technical accuracy and everyday accessibility. Frank Riccardi provides a much-needed roadmap for navigating the modern threat landscape with confidence. *CTRL+ALT+PWN* is a must-read for anyone who wants to stay safe online.”

—**BOB LORD**, creator of Hacklore.org

“Frank Riccardi’s book is a great book on hacking, distinctive in how well it is written and its storytelling. People learn through stories, and his book has plenty. Along the way, Frank shares how hackers hack and what you can do to best protect yourself.”

—**ROGER A. GRIMES**, CISO Advisor for KnowBe4
and author of *A Data-Driven Computer Defense and How
AI and Quantum Impact Cyber Threats and Defenses*

AUTHOR PHOTO COURTESY OF ROSA K. GOLDSMITH
COVER DESIGN AND ILLUSTRATION BY BEN PRIOR

TURNER
PUBLISHING COMPANY

X | @TURNERPUB
f /TURNER.PUBLISHING
TURNERPUBLISHING.COM