CYBER CURIOSITY

A BEGINNER'S GUIDE TO CYBERSECURITY

HOW TO PROTECT YOURSELF IN THE MODERN WORLD

LAKEIDRA SMITH

CYBER CURIOSITY

A BEGINNER'S GUIDE TO CYBERSECURITY HOW TO PROTECT YOURSELF IN THE MODERN WORLD

LAKEIDRA SMITH

New Degree Press

Cyber Curiosity

A Beginner's Guide to Cybersecurity How to Protect Yourself in the Modern World

ISBN
978-1-63676-869-4 *Paperback*
ISBN
978-1-63730-173-9 *Kindle Ebook*
ISBN
978-1-63730-313-9 *Ebook*

This book is dedicated to my beloved family and friends. Thank you for believing in me even when I didn't believe in myself.

Contents

Introduction

Your name, social security number, address, date of birth, driver's license number. Vital pieces of information that create your identity. Combined, they make you who you are to others. You need them to identify yourself when you go to work or school, apply for credit cards and bank accounts, or get a passport or ID. They're essentially your keys to the world.

Without them, who would you be? How would you prove who you are to the world?

Dave Crouse was forced to face that

"I have no identity," said fifty-six-year-old Crouse in an interview with "I have no legacy. My identity is public knowledge, and even though it's ruined, they're still using

In six short months, the criminals had slowly but surely charged over $900,000 to his debit card. He fought tirelessly against the attacks and attempted to salvage his finances. However, ultimately, he wasted almost $100,000 in his attempts to regain his identity, and he drained his retirement and savings accounts in the process. Even his once stellar credit score, formally a 780, had

Crouse was a favorable target for a cybercriminal. He was a frequent online shopper, and he did the majority of his banking

online. He would frequently use his debit card during his online shopping sprees without using any additional protection measures such as PayPal. One of his favorite pastimes was downloading songs from file sharing websites, which are notoriously riddled with

The first suspicious activity on his account occurred in February of 2009. However, Crouse dismissed the charges since they were for relatively small amounts of money, only $37 and

Crouse was financially secure, and at the time, he had a job in the construction industry making $180,000 a year. The account he did most of his spending out of typically had around $30,000 in it at any given

In March, he was laid off from his job. This sudden change of events caused his $2,300 a week income to shrink to $780 biweekly unemployment

Unfortunately for Crouse things really took a turn for the worse in August. “All of a sudden it really got bad,” he recounts. “In August, the charges hit big time—$600, $500, $100, $200—all adding up from $2,800 to $3,200 in one

Once he discovered the fraudulent charges, Crouse immediately contacted his bank and began the long process of filling out affidavits, forms swearing he was not responsible for the charges on his account. He says he filled out about twenty affidavits, and

one day he filled one out concerning a charge and the following day, the bank accepted similar charges nearing

“At that point, I was going to the bank every day and looking at everything,” he

Even after he closed his debit account at that bank, his other accounts were still getting drained daily. Crouse then decided to go to a new bank and open a new account, hoping his information would be safe there. The following day both accounts, the new and old one, were fraudulently charged for

Crouse felt

His new bank explained to him that he was very likely a victim of a cybercrime. His bank advised him it was likely a malicious program that had been installed on his computer without his knowledge while he was visiting one of the file sharing sites he frequented. They theorized he was a victim of what is called “keystroke

If this was the case, the cyberattacker was tracking every key he struck on his computer—from his passwords to his banking information—and that’s how they picked up all his personal

Malicious software or malware, such as keystroke malware is often not a targeted attack. When this type of malware is created, it is created to produce as much impact or financial gain as possible with as little effort as possible. It is sent to as many people as

possible, so it is given a greater chance of giving the attacker a return on his investment.

It's also possible that Crouse's information was being sold on the dark web. He reported that people in multiple locations in Florida; Brooklyn, NY; and North Carolina were using his identity to make

It's common for cybercriminals to sell personal information on the dark web for as little as one dollar for a social security number. Prospective criminals can also buy what's known as a '"Fullz," a full package of someone's personal information (including the victim's full name, social security number, birthdate, account numbers, and other sensitive information) for about thirty

"It was nasty," he said, admitting he even contemplated suicide. "I just couldn't take it. I didn't feel like a man anymore. I was violated, and I didn't know what to

His identity—social security number, address, phone numbers, name, even his old information—is still being used in attempts to open new credit cards and bank

You might believe that Crouse's case is an outlier, but unfortunately, you would be mistaken. His case is much more common than you may think.

The Internet Crime Control Center (IC3)—the FBI's department for cybercrime reports and investigations—reported that in 2019 alone,

there were 68,649 victims of personal data breaches, identity theft, and credit card fraud, and they lost a total of

Perhaps you believe you have no reason to be concerned about your personal cybersecurity because you believe there is nothing you can do to protect yourself or that it is the responsibility of corporations to worry about cybersecurity. Yet I spoke to some experts who believe we can all become more responsible cyber citizens.

This book explores some techniques that can help you secure your identity as you navigate through the modern world. No one can reduce their risk of being a victim of cybercrime to zero, but you can be one step ahead.

The Power of Connection

Our world is becoming more interconnected by the minute, and this is a good thing in many ways. We use our devices and the applications they host to connect with the people that we care about.

Our phones and computers have become a gateway for connecting with amazing people and learning wonderful, new things. The Internet and the devices we have been able to create and connect to it have improved our lives in many ways.

Today, most of us would not be able to imagine our world without the joys of our smartphone, social media, and the

Internet.

In 2020, currently, around fifteen billion Internet of Things (IoT) devices are connected to the Internet. IoT devices are defined as devices "connected to the Internet and so can share data or otherwise communicate with each other and with

In the consumer space, these "things" are most commonly smartphones, laptops, wearable devices like smart watches and connected medical devices, smart home devices, and connected vehicles.

It is projected that there will be forty-one billion IoT devices connected to the Internet by 2027, and in 2019 there were only eight billion devices As you can see, the Internet of Things is growing at an exponential rate, and it's showing no signs of slowing down.

As more everyday items in our lives become connected to the Internet from our refrigerators to our watches to our light switches, every device you connect becomes a potential access point for a hacker or malicious actor. This increases your chances of becoming a victim of a cyberattack if you don't consider the risks of these devices and take steps to minimize them.

According to a study done by Pew Research in 2019, 81 percent of Americans admit to going online daily. This includes the 28 percent of people who reported that they are online "almost constantly" and the 45 percent that claims to log on several times

a day. Eight percent of the population only gets connected a few times per week or less. Only 10 percent of American adults reported they did not use the Internet at

Looking at these statistics, you're likely someone who goes online every day, just like I am. I would actually put myself into the "almost constantly" online category.

However, that level of connection and near-constant use of the Internet and Internet-connected devices comes at a cost.

"Cyberattacks are occurring every single day, targeting anybody from somebody who has five dollars in their bank account to up to fifty million," said Dr. Eric Cole, former chief technology officer at McAfee, former chief scientist at Lockheed Martin, and member of the commission on cybersecurity under President Obama, in an interview with me.

Regardless of who you are, what your income level is, or what type of job you have, you could be the target of a cyberattack. This is why it is important for every individual who uses the Internet to learn how to use it responsibly and take personal control of their cybersecurity.

Many people think and believe cyberattacks only affect companies, and therefore individuals don't really need to think about cybersecurity.

It's also a common belief that everyday people don't need to have any knowledge of technology or cybersecurity. Many individuals

have developed an indifference toward the security of their private information, and they believe they don't care what happens with their cybersecurity.

When I became aware that my online activity increases my risk of being a victim of a cyberattack, I changed my online behavior and adopted healthier cyber habits. I realized that increased exposure is equivalent to increased risk.

However, I have come to believe something else.

Cyberattacks can and very likely will affect you. Anyone can be a victim of a cyberattack, it's just a matter of the impact and the timing, which is why everyone can benefit from having knowledge of technology and cybersecurity in their daily lives. I learned this lesson first-hand during my junior year of college.

In 2019, IC3 reported that cybercrimes accounted for $3.5 billion in victim losses. The IC3 received over 1,200 complaints concerning cybercrimes or a suspected cybercrime per Not all victims of cyberattacks report their situation to the IC3, so the figures are an underestimation of the true impact of these crimes.

Fortunately, I also learned you don't have to trade the enjoyment of being connected for enhanced cybersecurity.

Discover Your Curiosity

Living in the modern world is hard enough without having to worry about the safety of your personal information, but you can no longer make the choice to opt out of understanding the fundamentals of technology and cybersecurity. This is why everyone needs to develop a sense of cyber curiosity.

If you use the devices, you have to know how to operate them safely for your own protection. This book will teach you how to better secure your personal data from attackers, how to assess the risks and benefits before you buy or install a new smart device or application, and straight-forward tips to tighten your cybersecurity.

In preparation for writing this book, I have curated research from scholarly sources, first-hand accounts of cybercrime victims, insider knowledge from my peers in the cybersecurity community, and primary interviews and exclusive insights from some of the brightest minds in the industry. Many of the people who I've chosen to interview for this book have been working in cybersecurity since before it was considered a "real" thing. They've previously lent their skillsets to organizations like Pinterest, IBM, McAfee, and the White House.

My hope is that you will have a better understanding of cybersecurity as a multidisciplinary subject and understand why considering it a problem for the IT department is an off-base assumption.

Don't wait until you've become a victim of a cyberattack to make a change to your habits, as it may be too late. Anticipate risks and take the measures needed to protect yourself and your family.

Topics this Book will Explore include:

•How to Define Cybersecurity
•Cybersecurity in Business
•How and Why the Internet Was Created
•Why Personal Cybersecurity is Important
•Cybercrime and the Dark Web
•Personal vs. Identifiable Information
•Malware and the Booming Spyware Industry
•How to Avoid Being Scammed Online
•The Privacy Paradox
•Big Data and Ethics in Technology

My intention is for this to be a guidebook for those wanting to protect themselves and their families as they navigate cyberspace in their daily lives. This is why Part 3 is dedicated to tips, and Chapter 13 is dedicated to protecting vulnerable populations like children and the elderly. I will also explore and explain how psychology, human behavior, ethics, and privacy play a large role in the study of cybersecurity.

1 Jennifer Waters and MarketWatch, "Identity Fraud Nightmare: One Man's Story," MarketWatch, February 10, 2010.

2 Ibid.

3 Ibid.

4 Ibid.

5 Ibid.

6 Ibid.

7 Ibid.

8 Ibid.

9 Ibid.

10 Ibid.

11 Ibid.

12 Ibid.

13 Ibid.

14 Ibid.

15 Ibid.

16 Brian Stack, "Here's How Much Your Personal Information Is Selling for on the Dark Web," *Experian* (blog), December 6, 2017.

17 Jennifer Waters and MarketWatch, "Identity Fraud Nightmare."

18 Ibid.

19 US Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report* (Washington, DC, 2019).

20 Bethany Groff Dorau, "Internet of Things: Overview," *Points of View: Internet of Things* 1, no. 1 (October 2019): 1–3.

21 Peter Newman, "The Internet of Things 2020: Here's What over 400 IoT Decision-Makers Say about the Future of Enterprise Connectivity and How IoT Companies Can Use It to Grow Revenue," Insider Inc., March 6, 2020.

22 Andrew Perrin and Madhu Kumar, "About Three-in-Ten US Adults Say They Are 'Almost Constantly' Online," Pew Research Center, July 25, 2019.

23 US Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report* (Washington, DC, 2019).

Part 1

What is Cybersecurity

Chapter 1
Redefining Cybersecurity

"The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction, and Resilience. Do remember: Cybersecurity is much more than an IT topic."

—Stephane

Cybersecurity isn't simply a buzzword that has gotten a lot of press lately. It also represents a multibillion-dollar issue with the FBI reporting $10.2 billion in total victim losses over the last five

Alongside problems come profits. According to the global cybersecurity market was worth $173 billion in 2020, and it is expected to grow to $270 billion by

Like Stephane Nappo, 2018 Global Chief Information Security Officer of the I recognize that cybersecurity is so much more than a growing multibillion-dollar subsection of the IT industry. It can be argued how much of the discipline of cybersecurity is even directly IT-related, and as you will see as we define cybersecurity in modern terms, this field has a human element at its core.

Therefore, I believe the best cybersecurity solution is one that emphasizes the human element. We, the users of the devices,

hold a lot of power over our security—far more power than we realize or care to admit.

Unlike other IT industries like software development, which mainly rely on the proper input from the human and the proper output from the machine, cybersecurity was defined and is constantly evolving because humans are curious. It's just our nature.

Some of us use that curiosity for good, and others, not so much.

We like to tinker with things, to test their limitations. Some of us are motivated by fame, others by fortune, some by pure delight at finding out how something works.

Because of this, with the invention of the Internet and therefore a worldwide interconnected network of computers, we brought about new avenues for humans to explore their curiosity, sometimes at the expense of other humans.

Defining Cybersecurity

Before we look at the modern definition of cybersecurity, let's take a trip back in time to recount the closest thing the cybersecurity community has to an origin story.

It was November 2, 1988. Robert Morris, a Cornell University computer science graduate student, hacked into an MIT computer and changed the way we view the

For months, Morris had been developing a program he believed would spread slowly and secretly across the Internet. He'd written an experimental worm, a self-replicating program, just to see if it was possible. His plan was to release the worm from MIT to disguise his identity as a Cornell

At around 8:30 p.m., Morris unleashed the worm, and soon after, he discovered the program was spreading far faster than he anticipated. There was a bug in his program. The computer worm was spreading at an extremely high speed and bringing computer speeds to a crawl in its

"We are currently under attack," wrote a concerned University of California, Berkeley student in an email later that night. In the span of twenty-four hours, it's estimated that 6,000 of the 60,000 computers connected to the Internet at the time had been

Even though the worm didn't destroy or damage data, it managed to greatly harm productivity. Essential military and university systems were halted, and emails were delayed for

Technologists worked tirelessly to figure out how the worm functioned and how it could be removed. Given the nature of the attack, exact damages were difficult to estimate, but they range anywhere from $100,000 to

Immediately following the attack, Morris contacted two of his friends in a panic. He admitted he was responsible for launching

the worm, but he never intended it to get this out of

He requested one of his friends to deliver an anonymous message from him across the Internet. He wanted to issue an apology and a guide on how to remove the worm. Unfortunately, because of the damage that the worm had done to the network, few people received the message in

Unbeknownst to Morris, his other friend made an anonymous call to *The New York Times*. The friend blabbed to the reporter that he knew the person responsible for creating the program, but it was only meant to be a harmless experiment. The creator had no idea the extent of the damage that would be caused and that its spread was due to an error. It was the information gained from this call that would make the attack front-page

The friend had many follow-up conversations with the reporter. During one of the conversations, the friend accidentally referred to the creator of the worm by his initials, RTM. The *Times* used that information to connect the dots and publicly confirm the identity of Robert Tappan Morris as the creator of the

The Morris Worm inspired a new generation of hackers and a wave of Internet-driven assaults that continue to plague our digital systems to this day. Whether accidental or not, the first Internet attack thirty years ago was a wake-up call for the country and the cyber age to come.

The Worm highlighted security flaws that technology users and leaders were previously oblivious to because the Internet was still in its infancy; this was a year before the invention of the World Wide

This attack sparked the conversation for the necessity of security measures for this newly connected world called the Internet. Many people consider the Morris worm to be the beginning of cybersecurity and the event that made institutions pay closer attention to the possibility of attacks on computer networks.

Minor malware programs had been created prior to the Morris worm, however, it was the first to garner widespread media attention primarily because the targets were prominent universities and institutions, such as Harvard, Princeton, Stanford, John Hopkins, and

* * *

This is where cybersecurity begins to get defined as what we know it as today. However, the definition of cybersecurity still varies depending on your source:

According to Merriam-Webster Dictionary, cybersecurity is defined as “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or

During the White House Cyberspace Policy Review in May 2009 conducted by the National Security Council and Homeland Security

Council, cybersecurity was defined as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or

Sam Curry, chief security officer of Cybereason (an end-to-end cybersecurity solution), explained to me in an interview that a simple way to define cybersecurity is using the acronym CIA:

•Confidentiality: making sure that when you interact with other you have only the people you want involved
•Integrity: nobody who isn't the intended party can modify information without permission
•Availability: you can't be denied the ability to interact with others or access your data

According to the 2020 edition of *The Cybersecurity Body of Knowledge,* "Cybersecurity is a combination of the words cyber, meaning computer, and security. We understand the reason for the cyber part...Security implies the act of safeguarding

Many of these definitions focus on the computer or computer system that needs to be protected. However, many of them miss the core element that drives all cybersecurity problems and solutions: the human element. The human element of cybersecurity is critical to its practice because the devices aren't the issue; it's the way we use them that results in problems. Computers can only act as they are programmed or commanded to, and we, the humans lead the charge in the programming.

This fact alone shows that cybersecurity is much broader than an IT topic. It spans into criminology, psychology, healthcare, and many other fields.

Humans are the facilitators of cybercrime, and they are also the victims. They are the targets of phishing schemes, but they are also the ones doing the social engineering. (We will learn about social engineering in Chapter 8).

Understanding how to navigate "cybersecurity" is much more complex than installing a piece of software and being safe forever. Unfortunately, there isn't a cybersecurity equivalent to a house alarm, especially with the rise and increased sophistication of social engineering attacks that use manipulation to trick people into becoming cybercrime victims.

My definition of cybersecurity is "the measures individuals and organizations take to protect themselves, their personally identifiable information, and their digital, physical, and financial assets from unauthorized use, damage, or exploitation."

Today, cyberspace is a key aspect of modern life, with broadband signals, wireless networks, local networks in schools and businesses, and heavy use of the power grid to support millions of computers, tablets, and cell

Education Is Everything

Anticipation of threats and user education should be at the forefront of cybersecurity efforts, not prepackaged antivirus software—those are great for detection of a threat that is already on your device.

However, there lies the issue. The threat is already on your device.

I'm not saying to go and uninstall your antivirus software from your computers or unplug every device in your home. However, I'm urging you to not fall into a false sense of security just because you have those measures in place.

As we will explore in this book, a lot more is at play when it comes to your security than viruses or digital threats. The way our world has meshed with cyberspace has created an entirely new category of threats, and prevention is always the best medicine.

If you bought a car and you got into a car accident because you didn't know where the brakes were, is the manufacturer at fault? What if you were seriously injured because you didn't know how to use a seatbelt—is that their fault?

Of course not, but the answer to that question is only rhetorical because we have normalized user education and anticipation of threats when it comes to the car industry.

I grew up seeing "BUCKLE UP" ads everywhere, which then became "Don't drink and drive," and later "Buzzed driving IS drunk driving." We as a society have invested a lot of time, effort,

and money into user education for things we use every day—even trivial things like infomercials about how to properly use a new flat iron.

Then, why is it that we haven't done the same for cybersecurity? After all, it is a skill that can save people money, time, and resources by giving them the tools to be able to avoid falling victim to scams, cyber-crimes, and malware.

Is it because we've decided that there's nothing we can do about the issue, it isn't our issue to solve, or do we simply not care? Possibly, it is a combination of all of the above, and we have resigned ourselves to that reality—even though that isn't our only choice.

A New Perspective

The first day of a new semester is always chaotic. I had just signed up for this class just days before the beginning of the semester because someone dropped it, and I was so excited that I was able to get a spot. It was the last elective I needed to fulfill my cyber criminology minor, and it seemed to be on a pretty interesting topic: legal and ethical issues in computing.

At one point in my life, I wanted to be a lawyer, and I guess my interest in policy and legal matters never really left me. Ethics also intrigued me, because I believe we have a responsibility to make sure that the technology that is being created is ethical and not being misused or abused.

On my first day, I attempted to push up the stairs of Lloyd Hall, iced caramel latte in hand, past the crowd of students that had formed between class times.

Buzz.

I looked down, and my Apple Watch said, "CS340 Legal and Ethical Issues in Computing in 5 mins."

"Excuse me," I said with a sense of urgency in my voice. Showing up late on the first day of class is in poor taste.

My path slowly cleared, and I started to hurry up the second flight of stairs to the third floor. My pink backpack felt like a brick strapped to my back as I walked swiftly down the hallway until I finally reached the doorway. *Room* I made it, and just in time. I sat down at one of the desks in the front of the small classroom and plopped my backpack down beside me.

Unbeknownst to me, this class would change the way I would think about the real ethical issues plaguing the computing industry, and it triggered me to explore how many of those were linked to cybersecurity and privacy.

The class involved creating a final project that showcased your research around a niche technology subject and the related legal and ethical issues around that subject. I chose Internet of Things (IoT) devices as the subject for my project. It was a topic I

wanted to learn more about, and I thought what better time to do a deep dive into the topic than for a project worth 40 percent of my final grade.

As I began my research, I found many articles that confirmed my overall feelings about IoT devices. IoT devices offer users great functionality, accessibility, and sometimes even improve the user's quality of life; however, they collect large amounts of data and user information, which can lead to privacy and security concerns from improper security within the device, a breach, or the device maker selling the user's information to a third party.

A 2019 survey by Consumers International and the Internet Society found that "75 percent of people distrusted the way data is being shared, 63 percent found data collection by connected devices "creepy" and 53 percent did not believe connected devices could effectively protect their

Yet year after year, IoT device ownership has grown exponentially.

Why was that if people didn't trust these devices?

I began delving deeper into scholarly research about the privacy and ethical concerns with IoT devices, and I was intrigued by the information I found.

If I asked you if you value your security and privacy, what would you say?

You would say, “Yes, of course, I do.”

What would you say to me then if I told you that you actually didn’t?

When asked if they would share their date of birth with a complete stranger, most people would answer, “No.” However, if given an incentive to share their date of birth like a coupon or exclusive access to a new app, they’d be more willing to provide their information.

This is known as the privacy paradox. A theory that demonstrates the “disjointedness between self-reported privacy concerns and actual privacy protecting The privacy paradox is the reason why millions of people own smart devices that they don’t think are secure or they would refer to as “creepy.”

Many people fall into this trap of owning and using products they don’t trust or doing things that if they thought hard about, they wouldn’t normally do. Why do we do it? *Well, everyone else is.* If we see others doing an action or buying a new device, we begin to think it’s safe, and we don’t want to feel left out.

Going into a new decade bound to be filled with floods of technical innovations, we must practice caution as consumers when making purchasing decisions.

We’ve woven technology into our lives, and the brightest ideas have brought us a long way from the landline. However, we must

remain aware that fast-paced innovation sometimes comes at a cost and that not all devices and software were created equally or with safety in mind.

The Future of Cybersecurity

"The future depends on what we do in the present."

—Mahatma

In the modern world, cybersecurity is a multifaceted force. It's is no longer only relevant to people who want to pursue it as a career.

In the grand scheme of the world of technology, cybersecurity as its own discipline is in its infancy; for example, it is still not decided within the community whether the proper spelling for the word is cybersecurity, cyber security, or cyber-security. Any of the above are generally accepted, but I personally prefer the compound word—cybersecurity.

Personally, I view cybersecurity from a couple of different lenses. However, the lens I'll be focusing on is the lens of the technology consumer.

From a consumer's point of view, cybersecurity is not their life. It's not their gig. I do my best to remember that when making decisions and choosing my verbiage, the majority of people are casual technology consumers, not technology fanatics or STEM majors.

Whether we realize it or not though, many of us have immersed ourselves in cyberspace and created virtual versions of our lives within this domain.

Cybersecurity for technology users is often seen as an afterthought. Many people feel like their computer's security is taken care of once they've installed their new antivirus software. Or, they feel their privacy concerns are eliminated once they put that cute little sticker over their webcam. However, as Sam Curry so aptly put it during our discussion, "It's not just a green lock somewhere; it's a fight."

The issue of cybersecurity is not a mystical magical idea hidden somewhere in the "cloud." Even some IT professionals who don't specialize in cybersecurity still don't realize its full value.

If you haven't put much thought into the security implications of using the Internet and smart devices, I invite you to start now.

I think people being safe and secure in their interactions on the web is the most pressing issue in cybersecurity today. It's a real, pervasive issue that's here now and for the foreseeable future.

I began this project toward the beginning of the COVID-19 pandemic. As the months pass by and we continue to transition into this new post-pandemic world, one of the things we must consider is the impact that this pandemic has had on the cybersecurity industry. Tens of millions of employees are now

working from home, and for some this change is permanent. As Forbes puts it, "Remote workers' identities and devices are the new security

With this in mind, learning to protect our own networks is becoming more crucial than ever with not only our own data on the line but also that of our employer's.

No matter how much innovation we achieve in technology, if we don't feel safe using it, what's the point?

So, as consumers, we must start taking responsibility for our own cybersecurity today.

24 Ian Warner, "24 Best Cybersecurity Quotes That Will Blow Your Mind," *The Habit Stacker* (blog), *Habit* accessed January 11, 2021.

25 US Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report* (Washington, DC, 2019).

26 Louis Columbus, "2020 Roundup of Cybersecurity Forecasts and Market Estimates," *Forbes,* April 5, 2020.

27 Ibid.

28 Stephane Nappo, "Stephane Nappo," LinkedIn, accessed January 16, 2021.

29 "The Morris Worm 30 Years since First Major Attack on the Internet," *US Federal Bureau of Investigation* (blog), November 2, 2018.

30 Ibid.

31 Ibid.

32 Ibid.

33 Ibid.

34 Ibid.

35 Ibid.

36 Ibid.

37 Ibid.

38 Ibid.

39 Ibid.

40 Ibid.

41 Merriam-Webster.com Dictionary, Online ed., s.v. "cybersecurity (n.)," accessed January 11, 2021.

42 "Cybersecurity Glossary," Cybersecurity and Infrastructure Security Agency, last modified July 21, 2020.

43 Daniel Shoemaker, Anne Kohnke, and Ken Sigler, *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in* (New York: CRC Press, 2020), EBSCOhost.

44 *Salem Press* s.v. "Cybersecurity," by Kathy Warnes, PhD, accessed January 11, 2021.

45 Noura Aleisa, Karen Renaud, and Ivano Bongiovanni, "The Privacy Paradox Applies to IoT Devices Too: A Saudi Arabian Study," *Computers & Security* 96, no. 101897 (September 2020): 1.

46 Ibid.

47 Asad Meah, "35 Inspirational Quotes on The Future," *Awaken the Greatness Within* (blog), *Awaken the Greatness* accessed January 11, 2021.

48 Columbus, "2020 Roundup," *Forbes*.

Chapter 2
Cybersecurity in Business

"Cybersecurity is treated a lot like the weather; everybody talks about it, but little is done to seriously address it."

Cybersecurity Body of

Two hundred million dollars in estimated costs. Secret Service investigations. Testimonies before the US Senate Judiciary Committee. The adaption of chip-and-PIN technology. Seventy million customer records

The year 2013 set off a series of events that would change the landscape of technology forever. A year that would define cybersecurity's future. When the year began, none of us could have imagined this series of events would unfold. Certainly not Target, as they believed they were doing everything correctly. Despite this, they will proceed to become the main character in this series of unfortunate events. Their missteps in the handling of this situation have been analyzed by top cybersecurity analysts since it occurred in 2013, and it still presents itself as an excellent case study to showcase business cybersecurity failing on a large scale.

During the peak of the 2013 holiday season, Target became the victim of a cyberattack. The method of attack used against them

wasn't a new one, and judging by its design, it shouldn't have been as successful as it turned out to be.

Days before Thanksgiving 2013, an attacker installed malware onto Target's security and payments system. The malware was designed to steal the information of every credit card used at the corporation's 1,797 US stores. Once the customer swiped their card to pay for their holiday gifts, the malware would capture the card information, and store it on a Target server that had been infiltrated by the malicious

On Saturday, November 30, the hackers had sent out the malware to retrieve the credit card information, and all that was left was to establish where the data would go after they stole it. As they began uploading malware to move the stolen card numbers, Target's computer security firm, FireEye, caught them in the

Just six months prior to them being the target of one of the most infamous data breaches in US history, Target made an investment of $1.6 million in a malware detection tool by the network security firm FireEye, a firm trusted by the CIA and the Pentagon. FireEye is an advanced cybersecurity system; unlike traditional antivirus systems, FireEye doesn't simply flag malicious or suspicious activity that has been used in the

FireEye is capable of detecting never-before-seen tools and customized attacks, which is why Robert Bigman, the CIA's former chief information security officer, says the system is so valuable: "It's a very smart approach. When we first started working with them several years ago, no one ever thought of doing it this

FireEye had a team of security specialists at their office in Bangalore, India, constantly monitoring Target's computers. If they noticed any suspicious activity, they would notify Target's security center in

So, on that fateful Saturday, the team in Bangalore received an alert to suspicious activity and immediately notified the team in

No one

Minneapolis didn't react to the sirens. They were also alerted again on December 2, when the attackers installed another version of the malware onto the

These alarms were not only impossible to miss, but Target was alerted of the threat early enough that no private information had been stolen from their network. If they had acted on these alerts, there would have been no headlines, no monetary loss, and no loss of personal

The one in three American consumers affected wouldn't have to be concerned about who has possession of their personal

When asked about the incident and the company's lack of an immediate response, Target chairman, president, and chief executive officer Gregg Steinhafel issued an emailed statement that said, "Target was certified as meeting the standard for the payment card industry (PCI) in September 2013. Nonetheless, we

suffered a data breach. As a result, we are conducting an end-to-end review of our people, processes, and technology to understand our opportunities to improve data security and are committed to learning from this experience. While we are still in the midst of an ongoing investigation, we have already taken significant steps, including beginning the overhaul of our information security structure and the acceleration of our transition to chip-enabled cards. However, as the investigation is not complete, we don't believe it's constructive to engage in speculation without the benefit of the final

A critical fact is that the breach could have been eradicated without any human intervention. FireEye's system has an option to automatically delete any malware that the system detects. However, Target's security team opted to turn off that function so they could have full control of what would be

Edward Kiledjian, chief information security officer for Bombardier Aerospace, an aircraft maker says, "Typically, as a security team, you want to have that last decision point of 'what do I

In this case, the decision on *what do I do* was made far too late. It is now known that Target also received warnings from their antivirus system, Symantec Endpoint Protection, alerting them to the same threat that FireEye detected. These alerts rang out on multiple occasions before

Still no action was

“The malware utilized is absolutely unsophisticated and uninteresting,” says Jim Walter, director of threat intelligence operations at security technology company McAfee. He adds that if Target had a firm grasp on its information security, “they absolutely would have observed this behavior occurring on its

On December 12, federal investigators warned Target that they were experiencing a massive data breach. Not only did they have evidence of the fraudulent charges, but they also had the data the attackers recklessly left on the servers. Still, it was not until December 15 that Target confirmed the breach to the public and eradicated the malware after forty million credit card numbers were The information from the stolen cards was ultimately sold on the dark web for a price that “ranged from

Stephen Cobb, a senior security researcher, said, “The combination of time and place was a perfect storm, reaching a significant percentage of the United States population. The odds are very good that if you lived in the US in 2013, even if you yourself were not affected, you probably know plenty of people who

Target’s action and inaction during this breach went on to normalize the data breaches to come in the following decade and changed the landscape of cybersecurity forever. Before the Target breach, information security wasn’t seen as a priority by many large corporations. Cyberattacks were seen as something that only happened to smaller shops that didn’t have the resources to defend themselves against an attacker. This breach showed that it was possible for well-known, large companies with significant

security defenses in place to fall victim to an attack. It also put into perspective the impact that data breaches can have on

Before these events, many companies didn't see the profitability in maintaining security in their operations. It was seen more so as a checkmark on an audit sheet or just something that had to be done to comply with regulations and to continue operations. Nothing big enough had happened to scare them into wanting to put the security in place to protect their customers.

The policies, the procedures, and everything else that goes along with security in cyberspace weren't well understood. In addition to not understanding the fundamentals, the consequences of not having proper cybersecurity were underestimated because no one had seen a breach like this on such a large scale. There hadn't been an event that demonstrated the value of proper cybersecurity practices in business for organizations to take it seriously and to understand that the benefits of hiring security professionals outweigh the risk and that the cost of security would eventually pay off.

The Target breach showed large companies that they, just like smaller companies, were vulnerable. Even if they did have considerable security defenses in place, failure on these security measures would give them an unfavorable outlook from the perspective of consumers and investors.

No one wants to purchase from a company that they believe doesn't take their privacy and their personal information seriously. People didn't want to continue to swipe their cards at a store

that could still be under attack by malicious actors. They didn't want to take that type of chance.

Many people were scared after this attack to shop anywhere with their debit cards or credit cards. Many people stopped shopping online for a period of time. This breach has scared many people from making online purchases entirely.

This led to the adaptation of chip and pin technology, which promised to increase the security of the cards we already had in our pockets and increase the security of the payment processors giving consumers more peace of mind in the

"Probably the biggest change is that this is what got payment processors moving toward chip & PIN in the United States," said Aryeh Goretsky, a distinguished security

This change helped consumers become more comfortable, but it didn't completely regain consumer trust. Even after spending sixty-one million dollars in response to the breach, Target had a difficult time regaining the full trust of their consumer base. Target's profit fell 46 percent during the 2013 holiday season from the same period the year prior, and the number of transactions fell more than it had since Target began reporting it in 2008. In this case, Target drastically dropped the ball on their security, and they cost themselves money and their reputation in the process. They failed their consumers, their investors, and themselves by not implementing security in the fullest form that they

They had multiple security systems in place to alert them to potential attacks, but they didn't act on those warnings. According to the 2020 edition of *The Cybersecurity Body of* "A protection scheme that is unable to guarantee the reasonable confidentiality, integrity, and availability of its protection objects has not achieved its basic purpose. It should be noted here that there is no exception to this The protection scheme used by Target Corporation failed to protect and defend the confidentiality of its customers' data and therefore failed its purpose.

Negligence in cybersecurity is not always just a matter of pure ignorance on that cybersecurity systems are necessary, but it also is a matter of not acting upon alerts to threats in a timely matter.

They had the systems in place to detect a threat, but they didn't have the protocols in place to actually eliminate that threat once it was detected. They didn't take it seriously enough to say, *this issue might be a serious threat that needs to be deleted immediately when detected because we handle the data of millions of people, instead of waiting on a human to take initiative and delete it.*

So, this brings us to the point that we have to practice—not just knowing that things pose a threat but actually taking all of the precautions that we need to take. In Target's case, they should have had their security system enabled to kill the malware as soon as it was detected. They dropped the ball, and they cost their customers money and their identities.

Prevention Over Reaction

"We should treat personal electronic data with the same care and respect as weapons-grade plutonium—it is dangerous, long-lasting and once it has leaked there's no getting it back."

—Cory

Only 38 percent of the organizations surveyed by Information Systems Audit and Control Association (ISACA) felt they were taking substantive steps to address the problem of Over half of the organizations surveyed thought they were not doing their part in the fight against cyberthreats.

So why aren't organizations taking cybersecurity seriously? Is it a lack of resources? A lack of caring? Clearly, they understand that they could be doing more to protect themselves and their customers by their responses to the survey. While the cybersecurity policies at some organizations fail because they were never adequate in the first place, in many cases, especially with large, well-established organizations, the problem arises not with the policy itself but with the implementation of the policy.

Organizations know that they are not taking enough action in protecting themselves from cyberthreats. And why is that? Why are they not taking enough action?

"The biggest problem in cybersecurity is the lack of alignment of security with the business or with the mission of an organization. They don't understand each other very well," said Cybereason

CISO Sam Curry when I asked him about the biggest challenge in cybersecurity today.

Currently, cybersecurity and information security as a whole aren't widely understood, especially by those outside of the field. This leads to cybersecurity being seen as an IT issue instead of a human issue.

Cybersecurity is a continuous, always-on, proactive activity—not a task or a single point in a process. As such, it calls for a holistic strategy including people, processes, and technologies that integrate security at every level instead of downstream, which is often too When organizations fail to look at cybersecurity from a holistic lens, their strategy often fails.

The technology implemented is very important, but as we saw in the Target breach, the people acting upon the technology often play an even larger role in the cybersecurity strategy. Cybersecurity policies and procedures must take into consideration possible human error.

"There are two highly credible types of attacks that are unavoidably part of the overall attack surface: human and physical exploits...Current research shows that electronic exploits constitute less than one-third of the threat. The rest of the protection problem involves such real-world factors as insider threats and social engineering or even natural complications like fire or

Too often, when organizations and individuals think about cybersecurity, they think about something directly digital, electronic, or IT related—that the threat has to be by someone using something electronic to exploit their security protocols. This mindset is what leaves large gaps in security policies. “In many organizations, human or physical types of threats are often not included in traditional cyberdefense planning. Most active cyberdefense solutions do not even consider the need to embody tightly integrated, well-defined, and uniformly applied behavioral controls as a fundamental part of the overall cybersecurity

An information security policy that doesn’t consider human behavior and natural disasters isn’t one that has the ability to prevent an exploit from being carried out.

There’s also the issue that some companies don’t think that preventive cybersecurity measures are a profitable solution. They don’t see that prevention is profitable enough, so they’d rather react to the issue than to prevent it. They think, *Well, I haven’t been hit yet. I haven’t had a breach yet.* So, they think they’ll be okay. If they do have a breach, they’ll be able to react to it. It’s more costly to put in all the preventative measures needed to properly protect themselves from a cyberthreat than to react and just pay for victims to have LifeLock for a year. Then it’ll blow over in a few months, and someone else will be the star of the news cycle.

However, this is not a bright idea. If we continue to normalize and ignore cybercrime, it encourages hackers and shows them that their behavior is acceptable. This is the way to commit the crime, get rich, and never get caught. Why shouldn’t I just be a

cybercriminal? It makes all the sense in a world for me to do it. It's much less likely that I'll be caught, it's much less likely that anyone's even going to care. There are far fewer physical boundaries to it than me going out and robbing a bank.

It makes no sense for companies to not put in these security measures in cyberspace. Companies do it in the physical space all the time, sometimes at extreme costs. We put in security cameras. We put in gates. We put in locks. We do all of these things that cost money and resources because we care about securing our physical space. We can see the physical world, so we have a grasp on what's going on, and the dangers that go along with it. However, since we can't "see" cyberspace, many times we choose to ignore the dangers and the need for security, but shouldn't we want more security for something we can't visualize in the physical space?

Cyberspace and cybersecurity are just as important as our physical space and physical security because today we spend as much time in our physical space as we do in cyberspace. So, we have to ensure we are maintaining security in both.

As a result of negligent corporations, millions of people now have their personal information exposed and waiting to be sold to someone in cyberspace. The only way to avoid the side effects of data breaches, which is widespread exposure of sensitive data to people with malicious intentions, is practicing prevention instead of reaction. As we can observe in the case of Target, if they would have acted earlier to prevent the attack, they could have

saved themselves $200 million, and they could have saved the identities of seventy million of their customers.

Once a cyberattack has occurred, there's no recovering data that has already been exposed to threat actors. Therefore, it's best to prevent a cyberattack before it can occur instead of simply using reactionary measures, like offering identity theft protection to victims.

What It Means for You

Due to misaligned and mismanaged cybersecurity policies, the personal information of millions is on the dark web or elsewhere on the Internet. This is a common side effect of data breaches, and the primary reason they occur in the first place. The goal of malicious actors is to get as much valuable, personal information as possible, so they can exploit it for monetary gain. The only way this can be avoided is by practicing prevention instead of reaction.

I emphasize this sentiment because I believe it is the key to changing our relationship with cybersecurity.

Being reactionary will not help as you can't reverse what's already been done. Once your information is out there, it's out there forever.

Yes, new information considered personally identifiable is generated all the time or can be changed, whether that's GPS locations or

changing credit card numbers. But key identifiers like your social security number, your birthday, and other very private very sensitive data about you are stagnant and not (easily) changeable. You can't use a reactionary measure to reverse that damage. Once the damage is done, it is done.

If any customer data or information is lost or exploited, the organization's cybersecurity protocol is considered a failure. It doesn't matter what fraction of the information is compromised. Nevertheless, it doesn't matter because if any information is lost in a breach, then the cybersecurity protection scheme

In this case, Target attempted to downplay the number of customer records lost and the number of credit card numbers stolen to attempt to downplay their accountability. However, if even one customer's information was compromised, their cybersecurity team failed at their job of protecting the confidentiality of their client's

The reason cybersecurity is important in business is because at the core of both fields lies the same element: humans. You, whether you're an intern, an entrepreneur, or a C-Suite executive, are the most important part of the cybersecurity strategy of any business.

Across corporations, many people agree that cybersecurity is a high priority. However, they also believe the cybersecurity or IT department of their company holds sole responsibility for defending them from cyberattacks.

A Leader's Guide to Cybersecurity explains the viewpoint that nontechnical leaders have toward cybersecurity: "They don't see cybersecurity as part of their job description. Backing up this view is the idea that cybersecurity is so complicated that laypeople are simply incapable of making any meaningful contribution to their company's defenses. Cybersecurity, they think, is a matter best left to the

This, however, couldn't be further from the truth. Cybersecurity is something that you as an employee at your organization plays an active role in every day, whether you're aware of it or not.

When your co-worker Jake asks you to send him the password to the company computer via text. When you forget to log out of your computer during your lunch break and potentially compromise a client's confidential information. These actions put the confidentially, integrity, and availability of your company's information at risk.

Also, doing things like choosing a secure password, opting to use two-factor authentication, and strictly following your company's security policies improves the security of your organization.

We have to hold each other accountable.

We've all received an alert on our phone or computer that says we need to install a security update, and we ignored the alert and said we'd take care of it later or it's not that important. We have

to remind ourselves that alerts are there for a reason, and we have to take them seriously. In a modern world filled with devices, noise, and notifications—alert fatigue is real. So, we have to remember that security alerts are important and shouldn't be ignored.

The cybersecurity of an organization is only as strong as the compliance of the members of that organization. We have to make security a high priority for ourselves and for our organizations.

Remember that cyberthreats can come from any level of an organization.

It's our responsibility to take the cybersecurity protocols of our organization seriously, whether we are leaders in our companies or new hires, and it is the responsibility of the organization to create these protocols and ensure they are strong and well enforced.

49 Daniel Shoemaker, Anne Kohnke and Ken Sigler, *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in Cybersecurity* (New York: CRC Press, 2020), EBSCOhost.

50 Meagan Clark, "Timeline of Target's Data Breach and Aftermath: How Cybertheft Snowballed for the Giant Retailer," *International Business Times,* May 5, 2014.

51 Michael Riley, Ben Elgin, Dune Lawrence and Carol Matlack, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," *New* March 17, 2014.

52 Ibid.

53 Ibid.

54 Ibid.

55 Ibid.

56 Ibid.

57 Ibid.

58 Ibid.

59 Ibid.

60 Ibid.

61 Ibid.

62 Ibid.

63 Ibid.

64_Ibid.

65_Ibid.

66_Ibid.

67_Ibid.

68_Ablon, Lillian, Martin C. Libicki, and Andrea A. Golay. 2014. Markets for Cybercrime Tools and Stolen Data. Washington, DC: Rand Corporation.

69_Lysa Myers, "Target Targeted: Five Years on from a Breach That Shook the Cybersecurity Industry," WeLiveSecurity, December 18, 2018.

70_Ibid.

71_Ibid.

72_Ibid.

73_Riley, "Missed Alarms," *New*

74_Shoemaker, *The Cybersecurity Body of*

7.5 Cory Doctorow, "Personal Data Is as Hot as Nuclear Waste," *The* January 15, 2008.

7.6 Shoemaker, *The Cybersecurity Body of*

7.7 Cyril Perducat, "Rethinking Cybersecurity as a Business Priority," *Industry* February 1, 2019.

7.8 Shoemaker, *The Cybersecurity Body of*

7.9 Ibid.

8.0 Ibid.

8.1 Ibid.

8.2 Thomas J. Parenty and Jack J. Domet, *A Leader's Guide to Cybersecurity: Why Boards Need to Lead--and How to Do It* Vergne: Harvard Business Review Press, 2019), chap. 6, EBSCOhost.

Chapter 3
The Birth of Cyberspace

"If at first the idea is not absurd, then there is no hope for it."

—Albert

Today, over 3.96 billion people use the Internet US households own an average of eleven IoT Cyberspace has become an essential part of our modern world. We engage with the Internet daily and stay connected through "broadband signals, wireless networks, local networks in schools and businesses, and heavy use of the power grid to support millions of computers, tablets, and cell There's no sign of turning back now that we've had a taste of what a hyper-connected world can offer us.

However, this hasn't always been the case, and the Internet hasn't always been such an expansive and widely accessible tool.

The Internet we know today originated from a research project funded by the federal government of the US Advanced Research Projects Agency (ARPA) in the 1960s. The project was named the ARPANET, and it was commissioned to fulfill the need for a system that gave researchers from different geographic locations the ability to share resources. ARPANET was created as a small network meant only for researchers and academics. The first computers on the network were connected in

On October 29, 1969, Charley Kline was a graduate student at UCLA. At 10:30 p.m., he attempted to send the first message via the ARPANET from his computer science professor Lenard Kleinrock's computer. Kline told PBS, the computers at the time were "room sized...with under-floor air His intended message—to one of only four other computers in existence at the time—was the word "login." However, the computer crashed before it could transmit the entire message and only ended up sending [90]

"I had no expectation that what I was doing that evening would be particularly significant," Kline

However, it was extraordinarily significant. That evening and that message marked a turning point in the history of communication. When that fragmented message traveled from Kleinrock's computer at UCLA to a computer at Stanford Research Institute, the way we would exchange communications and information would be changed

In 1985, the National Science Foundation established its own academic network called the NSFNET. In 1989, British computer scientist Sir Tim Berners-Lee invented the World Wide Web along with the technology required to access, create, and share web pages. Berners-Lee published the first web page in [94]

Shortly thereafter, the two networks merged causing the ARPANET to be decommissioned in 1990. In 1991, NSF began allowing restricted access to the NSFNET to Internet Service Providers

(ISPs), or commercial networks as they were known then. The NSFNET was decommissioned in 1995 as the privatization of networks began to occur. This resulted in the birth of what we know as the modern-day

Tim Berners-Lee said about the World Wide Web, “The original idea of the web was that it should be a collaborative space where you can communicate through sharing Berners-Lee intended for the Web to be a place where people could freely express themselves and engage their right to free speech.

Berners-Lee said, “What was often difficult for people to understand about the design was that there was nothing else beyond URLs, HTTP, and HTML. There was no central computer ‘controlling’ the Web, no single network on which these protocols worked, not even organization anywhere that ‘ran’ the Web. The Web was not a physical ‘thing’ that existed in a certain ‘place’. It was a ‘space’ in which information could

Essentially when Berners-Lee created the World Wide Web, he created a “host” where people could put their information. The World Wide Web was the land, but the creators had to come to build the properties themselves. It made for a highly customizable platform with endless possibilities, just the way Berners-Lee imagined it.

Since the Internet was built with the intention to be an open platform, it was designed so that any device can connect and can communicate with all other

As Paxton and Branca said, “The inherent flaws of the Internet are complex because of its development history...The Internet has been evolving for over fifty years, addressing issues of the moment. The foundational systems, methods, technologies, and protocols of the internet trace their beginnings to the ARPANET project. The Internet was not built considering today’s requirements, nor was security built in from the

While Berners-Lee’s dream of a World Wide Web free of restrictions might have sounded great when he invented it in 1989. Today, we can see how this framework, while great for creatives, is also great for attackers.

“I have some regrets,” Kline told PBS. He wishes they had “built more security into

Hindsight is 20/20 as they say. The pioneers of the Internet’s design couldn’t have realized at the time what ramifications an open platform could bring, and that failing to build security into their design was a recipe for disaster.

However, today we know better as we are currently witnessing the consequences. As we continue to add more functionality to the Internet and entrust it with more of our personal information, these design flaws become more worrisome.

If we continue to ignore the importance of cybersecurity, we will have to face more issues in the future. We are currently in a

vicious cycle of reacting to security issues after they occur instead of preventing them from happening in the first place.

Prevention and addressing things from the beginning—before something has been created, implemented, or worse of all exploited—is always the best way to go about it. Since after the creation process is complete or the software has been exploited, it is much more tedious and costly to repair the damage than it would have been to implement security from the onset.

The most worrisome Internet flaws are ones that affect privacy, security, and safety issues. When the Internet was originally designed, privacy, safety, and security considerations were naively Regrettably, Internet-connected devices inherit the flaws of the Internet that powers them. According to Paxton and Branca, "These flaws allow cybercriminals to search for, access, exploit, steal, modify, and even destroy data and devices of unsuspecting victims." This is incredibly troublesome for medical devices that contain sensitive data that can be directly linked to the

Even the Department of Homeland Security has openly recognized these faults in the Internet's infrastructure: "Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyberthreats and

The Internet continues to evolve today as we continue to push the limits of the Internet's utility with the spread of IoT devices. When innovations constantly push the Internet's limits the inherent flaws of the Internet become even more

The Age of Information

We live in the age of information. The age of the Internet. The age where the Internet is connected to nearly everything we touch and interact with. We are constantly interacting with our IoT devices. It's how we stay in contact with our friends, our family, and even complete strangers.

It has become such a normal part of life that we often take it for granted. At times we don't even remember the fact that what we're doing would be impossible without the Internet. When we lose power in our homes or our Wi-Fi is disconnected, we notice how worthless our devices are without the Internet.

Right now, I'm writing using a cloud-based writing program that saves my progress as I write so I never lose any content, very similar to Google Drive. However, when I'm writing, it rarely occurs to me that I'm using the Internet.

Does it usually occur to me that I'm using the Internet? No. That's because we take for granted the functionality the Internet has provided us with.

Often, we wake up and we turn on our phones and we get on social media, and it's not a mindful thing that this is the Internet. From the Fitbit on your wrist to the smartphone in your pocket to the tablet on your dresser, their function would be rendered virtually useless without the Internet.

The capabilities of cyberspace have expanded far beyond an Internet browser on your desktop. But still, so much of our lives is powered by the internet.

Bridging a Divide

It's a cool Spring Tuesday on the campus of the University of Alabama. Squirrels dart across the quad, and bicycle traffic races around me and my friend as we walk from our management class.

"What's your next class?" he asked.

"Oh, it's my cyber criminology class," I replied.

"What do you do in that class?" he asked while looking both interested and confused.

"Well, you know cyber criminology is my minor and this class is on cyber law and privacy rights. I'm actually doing a video project on IoT devices and the impact they are having on privacy," I said with enthusiasm.

"What's an IoT device?" my friend asked as he grew more confused.

As I struggled to juggle my iPhone, iced coffee, and notes from my previous class, my Apple Watch buzzes as I walk across the

quad. It was 2:55 p.m. Five minutes until cyber criminology 330, it said. *I'm going to be* I thought.

I replied, "An example of an IoT device is this smartwatch that knows exactly where I am and exactly where I should be, and it just told me I've got to go!" I exclaimed as I took off across the quad in pursuit of class.

* * *

"How many IoT devices exist, with how many computing devices do they share data? How many others have access to that data, and what decisions are being made with this data? No one really knows. We just don't know."

—Rebecca Herold, Author and CEO of The Privacy

The term Internet of Things (IoT) was first established in 1997. The Internet of Things refers to the network of physical objects, especially hardware devices, that are connected to the Internet and can share data with each other and with users.

According to Dorau, "It includes not only devices typically used for browsing the internet, such as laptop computers and smartphones, but also anything else equipped with sensors and network If the device or thing has a non-connective counterpart, like a watch, the item will often be labeled "smart" to indicate its ability to connect to the Internet and collect and share

Examples of IoT devices include:

include: include: include: include: include: include: include: include:

The list goes on, and it is growing by the day.

The invention of IoT devices has restructured how we live our lives, and they have become a significant part of our everyday activities. We have smart cars, TVs, refrigerators, vacuums, even the basics like light bulbs have become internet connected. We've entrenched ourselves into cyberspace. There isn't much of a physical barrier between us and it. Our world is cyberspace now. We live in it. The Internet of Things is our world.

By the late 1990s, the Internet dominated the global communication landscape. In 1993, only about 1 percent of telecommunications networks sent information over the Internet, but by 2000 over 51 percent of these networks did. This was mostly due to the Dot Com boom of the late 1990s. By 2007, the Internet conveyed over 97 percent of telecommunications information. The Internet continues to grow in the twenty-first century, propelled by massive amounts of online information, commerce, entertainment, and social

It is expected that more than 38.6 billion IoT devices will be connected by 2025 and that connections will increase to over fifty billion in the year 2030 according to estimations published by Statista Research In coming years, the influence of 5G will cause the Internet and the number of devices owned to grow

Today, the line between our online and offline lives is virtually invisible.

Your online identity is your offline identity, from geographic data to personality traits to your recent purchases. Most people have a trail that connects their online and offline life in a very direct way. It's difficult to escape interacting with technology in today's world.

When we think about interactions in cyberspace, we, of course, think about the positive effects that these interactions bring. The ability to socialize with people who are far away, exchange currency, or shop from your favorite store from the comfort of your couch. However, we understand this convenience is associated with risks, and therefore we have a give and take relationship with digital interactions.

Jen Ellis, Board Member for The Center for Cybersecurity Policy and Law, explained, "When I think about how risk is changing, and how we think about new trends, developing IoT is one of the most interesting areas because of a number of factors, but one of the key ones, and the most critical, is that we are bridging the divide between the physical and virtual

Florence Hudson, Executive Director of the Northeast Big Data Innovation Hub at Columbia University, expressed a similar sentiment in an interview with me "The biggest issue we have is the increased risk with all the attack surfaces that cybersecurity

needs to address because of the human and cyber physical connection. That's what I'm most concerned about."

This pertains especially to now, post COVID-19, where a lot of our interactions are virtual and we are in our homes, interacting with people who are outside of our households. We use our IoT devices to FaceTime, text, and call. We're constantly scrolling through endless TikToks, using Zoom for distance learning, and working remotely.

This has created a new layer to our already thriving digital ecosystem. We are relying on the Internet more than ever to fulfill our social and economic needs. This growth in Internet usage is increasing the need for cybersecurity in our everyday lives. We needed cybersecurity in our lives before, but now we need it more than ever.

The Cybersecurity and Infrastructure Agency stated, "As Americans become more reliant on modern technology, we also become more vulnerable to cyberattacks such as corporate security breaches, spear phishing, and social media

As we transition into remote working and learning and these practices become more commonplace, we need to be able to ensure our private and personal information remains secure. These activities transmit so much private and personal data like student, client, or even patient files.

Working from home on your own device increases the likelihood of this important data being mishandled, which is why if you are working from home, it is extremely important you learn how to navigate basic cybersecurity principles to keep your company's information safe.

In this age of digital information, we must make sure that we don't lose the confidentiality, integrity, or availability of any of the information that we have access to.

According to the Cybersecurity and Infrastructure Security Agency (CISA), "increased connectivity brings increased risk of theft, fraud, and

Therefore, you should be vigilant about your cybersecurity because we all own these devices and the more your own the greater your risk becomes. The issue is pervasive, and everyone in society must be responsible for their own digital welfare.

Technology is now a vital part of our ecosystem and we must treat it as such.

83_"Albert Einstein Quotes," Goodreads, accessed January 31, 2021.

84_ITU, "Number of internet users worldwide from 2005 to 2019 (in millions)," chart, November 30, 2020, Statista, accessed January 31, 2021.

85 Todd Spangler, "US Households Have an Average of 11 Connected Devices—And 5G Should Push That Even Higher," *Variety,* December 10, 2019.

86 Daniel Shoemaker, Anne Kohnke and Ken Sigler, *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in Cybersecurity* (New York: CRC Press, 2020), EBSCOhost.

87 Napoleon Paxton and David Branca, *Delivering Superior Health and Wellness Management with IoT and Analytics* (Switzerland: Springer, Cham, 2020), 447-467, Springer Link.

88 McDowall, Mike, "How a Simple 'Hello' Became the First Message Sent via the Internet," *PBS NewsHour* (blog), February 9, 2015.

89 Joshua Bote, "The Internet Is Now 50 Years Old. The First Online Message? It Was a Typo," *USA* updated October 29, 2019.

90 Nancy E. Marion and Jason Twede, *Cybercrime: An Encyclopedia of Digital Crime* (Santa Barbara: ABC-CLIO, 2020), EBSCOhost.

91 Bote, "The Internet Is Now 50 Years Old."

92 Ibid.

93 Ibid.

94 "Sir Tim Berners-Lee," World Wide Web Foundation, accessed January 31, 2021.

95 Paxton and Branca, *Delivering Superior*

96 "Tim Berners-Lee Quotes," Goodreads, accessed January 31, 2021.

97 Ibid.

98 Paxton and Branca, *Delivering Superior Health.*

99 Ibid.

100 McDowall, Mike, "How a Simple 'Hello' Became the First Message Sent via the Internet," *PBS NewsHour* (blog), February 9, 2015.

101 Paxton and Branca, *Delivering Superior*

102 Ibid.

103 "Cybersecurity," dhs.gov, accessed January 31, 2021.

104 Paxton and Branca, *Delivering Superior Health.*

105 Bruce Sussman, "Top 20 Cybersecurity Quotes You Need to Hear," *Secure World Expo* (blog), *Secure World* November 14, 2018.

106 Nancy E. Marion and Jason Twede, Cybercrime: An Encyclopedia of Digital Crime (Santa Barbara: ABC-CLIO, 2020), EBSCOhost.

107 Paxton and Branca, *Delivering Superior Health*.

108 Shoemaker, Kohnke and Sigler, *The Cybersecurity Body of*

109 Strategy Analytics, "Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030 (in billions)," chart, May 16, 2019, Statista, accessed January 31, 2021.

110 Todd Spangler, "US Households Have an Average of 11 Connected Devices—And 5G Should Push That Even Higher," Variety, December 10, 2019.

111 *Duke University School of* "Cybersecurity Law and Policy: What Are the Top Issues for 2019?," February 6, 2019, video, 57:19.

112 "Combating Cybercrime," cisa.gov, last modified November 20, 2018.

113 Ibid.

Chapter 4
The Cyber Curiosity Mindset

"No serious commentary will say that the user has no responsibility. We all have responsibilities to lock our doors in our homes and to buckle up when we get in cars."

—Spokesman, Information Technology Association of

According to IBM, 95 percent of successful cyberattacks are the result of human Nineteen out of twenty. Not the result of a technical mishap, but a human lapse of judgment.

The core issue here is that we as a society have yet to correlate our behaviors with our online security. When discussing cybersecurity, practicing responsible cyber behavior is often dismissed in favor of improving technical capabilities, although an astonishing number of successful cyberattacks are due to human error.

In the International Journal of Information Security and Cybercrime, Campean stated, "Cybersecurity aspects are too often regarded as purely technical and confined to the realm of IT departments, thus resulting in a limited general knowledge and awareness of the risks

This lack of risk awareness and public knowledge surrounding cybersecurity leads to a variety of concerning issues including general indifference toward cybersecurity, deferring the responsibility of our cybersecurity to another party, and a lack of awareness that cybersecurity is an issue at all.

We often prefer to defer the blame to the organizations and corporations that we entrust with our information. Instead of searching for solutions, we surrender to what we consider our fate. Our information will never be secure in the modern world, *so why should we bother?*

This apathy isn't the way we should approach our cybersecurity. While it's true there isn't a way to make yourself bulletproof from cyberattackers, you can minimize your risk of being a victim of a successful attack in many ways—the keyword there being "successful." You may receive phishing messages, malware may attempt to infect your system, and your small business may even be targeted in a ransomware attack. (We will dive deep into different types of attacks in coming chapters.)

However, I'm here, along with tips from some of the top experts in cybersecurity, to arm you with the insights and guidance to navigate these threats, so you can keep your identity and data secure.

We live in a modern world where everything is readily accessible. We can make a purchase with the click of a button or even a tap of the finger. We clamor after the latest and greatest smart devices. Communicating and sharing moments with friends, family,

and co-workers is easier than ever and always available to us from our pockets. Spending and transferring money now are primarily a digital affair with physical money and check payments becoming an antiqued idea.

No one can argue against the fact that we have entered the Information Age, and this is the new normal. In this new normal, we must realize that remaining apathetic toward our cybersecurity is no longer an option that we can take lightly.

Alongside the indifference toward cybersecurity, the lack of basic technical skills among the public is contributing to the phenomenon of human behavior leading to cyberattacks. In a 2020 survey done by the European Commission, over 40 percent of participants reported they lack basic digital skills, yet 82 percent of participants use the Internet on a regular

Earlier I stated that improving technical capabilities shouldn't be the focus of cybersecurity, however, having at least some basic digital skills are important when using any digital device. If I didn't have basic driving skills, it wouldn't be safe for me to operate a vehicle. The same thing applies to digital skills. A lack of basic digital skills can lead to unsafe cyber behavior. This is one of the main reasons that researchers have frequently stated that humans are "the weakest link of

If we fail to educate ourselves as a society on the importance of cybersecurity and the many ways we can protect ourselves from the dangers we may encounter in cyberspace, then we will never rise above being the weakest link in the cybersecurity chain.

I learned that lesson the hard way.

My Wake-up Call

"We do not learn from experience...we learn from reflecting on experience."

—John

It was a beautiful Thursday morning. The dying grass outside of my office window was covered in red and yellow leaves. I sat at my desk, staring at my computer, scrolling through technical support tickets. My co-worker and I began talking about our weekend plans when I got a slew of text messages that stopped me in my tracks,

As a result of a card transaction your available balance is -$255.17.

Then, *As a result of a card transaction your available balance is -$455.17.*

Then a moment later, *As a result of a card transaction your available balance is -$655.17.*

Someone had overdrafted my checking account by over $600 in a matter of minutes. I was in complete shock. At first, I thought it

must have been a mistake, but when I attempted to log into my online banking app, I was completely locked out.

"Oh my god," I exclaimed. "My account is over-drafted $655, and I can't get into my account!"

My co-worker looked at me, stunned, and asked, "What are you gonna do?"

"I guess I have to go to the bank, and hopefully, they know I didn't do this," I said.

"Good luck, girl," my co-worker said to me as I grabbed my keys and hurried out the door.

I rushed out to my car, and I was able to text my bank back and get the information from the last transaction. I Googled the ATM that the money was withdrawn from, and it was in Baton Rouge, Louisiana. I was in Tuscaloosa, Alabama. I had no ties to Louisiana. My stomach sunk even further to the floor.

How could this be happening? I thought as I drove to my local bank.

When I arrived at the bank, I approached the bank teller, and I told her about the text messages I had received.

"You're going to need to talk to her," she said pointing to a lady in a suit, sitting at a desk behind me.

I looked back to see where she was pointing, then turned back and managed to utter, “Thank you.”

I walked over to the lady’s desk. I was so nervous and jittery. I explained to her exactly what happened. She began to pull up my information using my bank account number and social security number.

“Is this your email?” she asked as she showed me her computer screen.

“No,” I said, as I shook my head.

It was clearly an email that was made just to break into my account. It was a random series of letters and numbers attached to a Yahoo account.

We started exchanging small talk as she continued to investigate the charges.

“I’m so embarrassed that this happened to me,” I said, as I really felt at the time that I should’ve been immune to an attack due to my knowledge of cybersecurity. I knew what not to do, and still, I wasn’t doing the best job I could of securing myself.

As she was resetting my email and password, she said very cavalierly, “It’s approaching the holidays. These types of things

have been happening a lot lately."

That's very I thought sarcastically.

"Yes, it does look like they withdrew the money from an ATM in Baton Rouge. So, we're going to file a claim with our fraud department, and your money should be back into your account in two-to-four weeks," she said with a smile.

"Thank you so much for your help," I said as I got up to walk out.

Thankfully, my story had a fairly happy ending. My money was returned to my account about three weeks after the hack, and since then I've improved my passwords and security questions on all my accounts. I also use a password manager to securely store my passwords for me and generate strong, unique passwords for every account I own.

However, my story could have ended a lot differently. Many people live paycheck to paycheck. They cannot afford for someone to steal money from their account and then wait two-to-four weeks for the money to be returned. Bills will still be due, food still must be put on the table, but cybercriminals don't care about you as an individual.

Cybercrimes are typically just traditional crimes carried out in a new venue. What happened to me is the cyber equivalent of someone stealing my wallet. We all learned at some point to keep

your purse close to you, or not to walk with your wallet or money in your hand. Not practicing proper cybersecurity is the Internet equivalent of walking and waving hundred-dollar bills around.

If you're not careful, eventually, someone is going to take it.

The Growing Need for Cybersecurity

According to The Cybersecurity and Infrastructure Security Agency, "Every time we connect to the Internet—at home, at school, at work, or on our mobile devices—we make decisions that affect our

In our modern world, technology is all around us. With that technology, comes risks that we often don't take into consideration when purchasing or using these products. From apps to new devices, we freely install, apply for, and begin using new technology on a whim. We don't think of cybersecurity as synonymous with our personal security, but as a society tethered to our devices, we should.

Your email address alone holds a treasure trove of information about yourself. If I got full access to your email account, I have your full name, possibly your banking information, and if you don't use two-factor authentication, the access to change the passwords on any account linked to that email. There's a lot at stake here.

Now more than ever, there is a growing need for cybersecurity education in our society.

The COVID-19 pandemic has caused a massive increase in remote learning and working. This drastic and abrupt shift has taken everyone, both employers and employees off-guard, and has left many employers in an odd situation. Most organizations were not fully prepared to send employees home to work remotely full-time.

Aside from companies that already offered remote working days, this change has been uncomfortable, to say the least. Due to the urgency of the situation, sorting out cybersecurity protocols has been an afterthought for many organizations. Companies are concerned about the security of their data and their client's data as the employees take their work home—many for the first time ever. Unfortunately, attackers are keenly aware of this.

Since people are spending more time than usual at home and on their devices, cyberattackers have taken this as an opportunity to launch more attacks during this time. They are also aware that working remotely comes with reduced security and a more relaxed environment. Getting you to let your guard down and make a mistake is exactly what they want.

Bring Your Own Device (BYOD) is when you are allowed to access your company's data and systems via your personal mobile devices such as your smartphone or laptop. The level of access granted depends on your company's policy and can range from full access to all company data, access to only non-sensitive data,

access without the ability to download or store the data onto your device, and many levels in

With the trend of BYOD becoming more popular in the workplace, ensuring employees take the same amount of precaution while they are home as they do at work is more important than

A top consulting firm, McKinsey & Company, predicts that based on trends observed early in the pandemic, companies will spend more on security overall in 2021 since fiscal 2020 budgets were solidified prior to the crisis occurring. Companies will also increase spending dedicated to improving remote access for workers, cybersecurity training, and automating routine

Today, Internet-connected devices drive most of our communication, work, school, and entertainment. They store our memories, our personal information, and our location. In the modern world, protecting our devices is protecting our lives.

In this rapidly changing environment, it benefits you to learn about cybersecurity. The Department of Homeland Security stated that "our daily life, economic vitality, and national security depend on a stable, safe, and resilient

Cybersecurity isn't the future. It's the present.

What is Cyber Curiosity?

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

—Bruce Schneier, Internationally Renowned Security Professional and Author of *Click Here to Kill*

Cyber curiosity is a mindset and a lifestyle. Embracing your cyber curiosity means you are aware of the dangers of cyberspace and what can happen to your information; therefore, you approach online links, attachments, webpages, other online interactions with a healthy level of suspicion.

You must do three simple things to build your cyber curiosity, which we will address in-depth in Part Three: What to Do to Protect Yourself.

In your online interactions, you must:

Cyberaware (learn the risks)
Caution (think about the risks)
Curiosity (ask about the risks)

The most important thing, and ultimate goal, is for you to take personal responsibility for your cybersecurity.

"Awareness trains individual learners how to properly perceive, judge, and respond to cybersecurity risks," according to *The*

Cybersecurity Body of "Awareness is the building block on which all other levels of learned security behavior

This is why it is not enough to simply be "aware" of the risks you might encounter in cyberspace; you must also have cyber curiosity so you have the skills and know-how to perceive, judge, and respond properly to the wide range of cybersecurity risks you will come across.

I asked Dr. Eric Cole, former chief technology officer at McAfee, what he perceived as the biggest challenge in cybersecurity today. He chuckled and said he couldn't pick just one.

"To me, what it really comes down to is understanding what are the potential threats or bad things that could happen to your critical data," Dr. Cole stated was his "number-one challenge" in cybersecurity today.

He said the second biggest challenge was people accepting responsibility for their cybersecurity.

"The second biggest challenge with cybersecurity is recognizing that people need to accept responsibility that cybersecurity is their responsibility. So, I think people as they're getting aware are like, *Okay, it's the bank's responsibility. It's Microsoft's responsibility. Somebody* said Dr. Eric Cole.

A focus on actionable solutions is what sets the cyber curiosity mindset apart. When given only awareness and no solutions, that's

how people grow apathetic to the problem and believe that it shouldn't be their responsibility because there isn't anything, they can do about it. When that is far from the case.

"Really for things to change, everyone has to recognize that they have to take action and that cybersecurity is their responsibility, to protect their data, their children, and their business," Dr. Cole continued.

According to The Cybersecurity and Infrastructure Agency (CISA), "Emerging cyberthreats require engagement from the entire American community to create a safer cyber environment—from government and law enforcement to the private sector and, most importantly, members of the Studies have indicated that up to 90 percent of the overall cybersecurity problem are the result of "simple human error and noncompliance with As CISA stated, we the public hold a great responsibility in the faith of the future of our cyber environment.

Our engagement, advocacy, and participation are needed as we face unprecedented threats to our cyber systems. My hope is that by making cybersecurity education more accessible and comprehensible, we can lower that percentage in the years to come.

When there is a threat, we do what is necessary. We lock our doors; we fasten our seatbelts. Even if we don't enjoy doing it, or it's a bit annoying, we still do it because we know the precaution is there to keep us safe. If we don't, then we know we are responsible for our own undoing. If we practice unsafe behaviors

like driving drunk, we assume the risk associated with it and understand we are at fault if something bad happens to us. If we leave our wallet on the street, we will assume someone will steal our money, our credit card, or our driver's license. However, for some reason, we don't treat our cybersecurity in the same manner.

According to the *Cybersecurity Body of* "Cybersecurity is often perceived as either belonging to the State or to organizations who can afford to implement We often ignore the risks associated with our actions in cyberspace, and when faced with the consequences, we prefer to defer the blame to the creator of the technology or the technology itself.

This step—taking responsibility—is often ignored. When examined, it makes perfect sense why. We as humans often don't enjoy admitting we've done something wrong. It is much easier to blame someone else than admit that our circumstances are our own responsibility. Owning our cyber behavior is difficult because it requires us to change how we think about and approach our own online interactions, and let's face it none of us particularly like change.

Change is hard.

This is especially true when that change requires you to point out your mistakes and what you need to improve. Bad habits are hard to break, and good habits take time to build. Nonetheless, good cyber habits will last a lifetime and save you from becoming a case study in my book.

114 "Security Quotes," Native Intelligence, Inc., accessed March 13, 2021.

115 Sorana Campean, "The Human Factor at the Center of a Cybersecurity Culture," *International Journal of Information Security and Cybercrime* 8, no. 1 (June 2019): 51-58, HeinOnline.

116 Ibid.

117 "Human Capital and Digital Skills," European Commission, accessed January 31, 2021.

118 Campean, "The Human Factor."

119 "Learning from Mistakes Quotes," Goodreads, accessed January 31, 2021.

120 "Cyber Safety," cisa.gov, last modified February 27, 2019.

121 "What is Bring Your Own Device (BYOD)?," IBM, accessed January 31, 2021.

122 Ibid.

123 Venky Anant, Jeffrey Caso and Andreas Schwarz, "COVID-19 Crisis Shifts Cybersecurity Priorities and Budgets," *Our Insights* (blog), *McKinsey &* July 21, 2020.

124 "Cybersecurity," dhs.gov, accessed January 31, 2021.

125 "Security Quotes," Native Intelligence, Inc.

126 Daniel Shoemaker, Anne Kohnke and Ken Sigler, *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in Cybersecurity* (New York: CRC Press, 2020), EBSCOhost.

127 "Cyber Safety," cisa.gov, last modified February 27, 2019.

128 Shoemaker, Kohnke and Sigler, *The Cybersecurity Body of*

129 Ibid.

Part 2

What to Know About Cybersecurity

Chapter 5
A New Threat Landscape

"In the underworld, reality itself has elastic properties and is capable of being stretched into different definitions of the truth."

—Roderick Vincent, *The*

Daily, millions of people worldwide browse the World Wide Web. Thanks to search engines such as Google, we can find exactly what we are looking for on the Web exactly when we need it. However, the part of the Web archived by Google only accounts for "6–10 percent of the whole

That small section of the Web is known as the surface web. The surface web includes all of your favorite websites, from Amazon to Netflix to Wikipedia. Anything that is publicly accessible is categorized as the surface web.

The remaining 90–94 percent contains web content that is neither indexed nor cataloged in any search This content is known as the deep web and the dark web.

The deep web and the dark web are commonly confused as being synonymous or interchangeable. They are not, however. Dark web content is contained within the deep web, but not all deep web content is considered a part of the dark web.

The deep web is broadly defined as the webpages and content that are not indexed or cataloged by search engines. Therefore, if you cannot search for it and get a result, it is considered a part of the deep

However, not all deep web content is hidden because it is illegal or immoral. The deep web includes content from normal sites that require registration, login, or payment to gain access to the protected areas of the website. The deep web would also include anything that the site admin has made intentionally private or restricted the access to only allow certain users. The exact size of the deep web is impossible to measure, but some experts estimate that it is “hundreds of times” larger than the surface

Within the deep web is the dark web. The dark web houses many underground markets selling everything from malware to drugs to child pornography. The marketplace is so large that the dark web community has created its own search engines and discussion forums to mirror the surface

“It’s here that bad actors of all stripes—script kiddies out to deface websites; professional hackers who break into corporate and government networks to steal data, wreak havoc, and commit extortion; pedophiles circulating child pornography; drug, arms, and human traffickers; terrorists spreading propaganda, recruiting fighters, and planning attacks; digital media pirates; and cyber mercenaries for rogue-state intelligence services—communicate with one another and trade in hacking tools, malware, ransomware, and

various illegal goods and services," said George Hurlburt, chief scientist at

To access the dark web, users must use an onion router such as Tor Browser or peer-to-peer This is why the .onion top-level domain is used at the end of dark web websites.

"The onion router or Tor, the onion meaning there's multiple layers to get to the center. ... And that's the way that Tor works... There are multiple computers that one has to go through in order to reach that content, the center of the onion," said Austin Berglas, former assistant special agent in charge, FBI NY Cyber

Computer scientists, Roger Dingledine and Nick Mathewson, founded Tor Project Inc. Tor Brower is used to connect to the dark web, and it is used to facilitate illegal activities, but it itself is not illegal. Tor was originally created to protect the security of its users and ensure users weren't being subjected to tracking and surveillance by government

"The Tor network...was created for the purpose of allowing people to communicate on the Internet without anyone having the ability to know who or where they were," said Vincent D'Agostino, an FBI agent in the cyber division, said to CBS

Tor is simply the portal being used to allow criminals to participate in the illegal

Diving into the Deep Web—The Silk Road

Ross Ulbricht grew up in Austin, Texas. He was raised in a tight knit family. He was always a smart and charming kid, so it surprised no one when he earned a scholarship to the University of Texas at Dallas to major in physics. He would receive a scholarship to earn his master's degree in materials science and engineering from Penn State. No one would have guessed that just five years later, Ulbricht would be arrested for running a multimillion-dollar black-market website that sold everything from illegal drugs, weapons, and even murderers for

"The idea was to create a website where people could buy anything anonymously, with no trail whatsoever that could lead back to them," Ulbricht documented in his journal toward the end of 2010. He continued and wrote that he had "been studying the technology for a while but needed a business model and

As a libertarian, Ulbricht held the belief that drug use was an individual's choice. After he saw that the drug market was extremely lucrative, he decided his new enterprise would center around

"I was calling it Underground Brokers," Ross journaled, "but eventually settled on Silk

As his first product, Ross decided to use his scientific knowledge to cultivate his own psilocybin

In January 2011, Silk Road finally launched. The sales came rolling in. Eventually, all ten pounds of Ross' homegrown mushrooms were sold. Then, other sellers wanted to join the website. At the time, Ross was handling all the transactions by hand. However, before too long, there were enough buyers and sellers to make Silk Road a fully functioning

"In 2011," Ross wrote to himself in his journal, "I am creating a year of prosperity and power beyond what I have ever experienced before. Silk Road is going to become a phenomenon, and at least one person will tell me about it, unknowing that I was its

Ulbricht was correct. Silk Road did become a phenomenon beyond anyone's wildest dreams. From 2011 to 2013, Silk Road experienced tremendous success. The site attracted millions of customers, hosted thousands of sellers, and allegedly garnered over one billion dollars in

However, by the end of 2011, law enforcement had caught onto Ross' (or Dread Pirate Roberts, as he was known online) operation. Mail carriers were seeing a massive increase in the number of drugs being shipped through the postal service. Although the Silk Road website included instructions on how to package the drugs to evade detection, some packages were still discovered and traced back to the website. Some Silk Road customers and vendors were arrested, and law enforcement worked diligently to find the identity of "Dread Pirate

Ulbricht was reportedly making over half a million in sales a month by the end of 2011. Unfortunately for Ross, Silk Road's

activities had attracted the attention of the FBI. Prompting the New York cyber branch to open a case in September 2012 dedicated to finding the server that ran the Silk Road

“Silk Road was the Amazon of drug sites,” said former FBI Special Agent Milan Patel to CBS

Just like Amazon, Silk Road allowed third-party vendors to sell their products to customers, and something that made their marketplace feel even more like your typical e-commerce experience was the user ratings and product

One customer with the username “Cantfeelmyface” left a review of the product they received and said it had “a nice shine” and delivered “a rush of euphoria and

Another customer going by the username “Ivory” left a review for some crystal MDMA they purchased, and they stated had “a nice fizz and wisp of smoke

Living up to its name as the Amazon of drug sites, Silk Road sold every drug imaginable plus a few more for good measure. Their catalog included over 13,000 listings, spanning dozens of

The reviews, high community standards, and extensive catalog of offerings showed potential customers that Silk Road offered exceptional value and superior customer service. This gave them a competitive advantage as customers saw them as trustworthy and

reliable. This leg up on their competitors is what made Silk Road the premier online illegal drug

“They trafficked in anything you could get in the black market—poisons, things like that,” Vincent D’Agostino

Silk Road’s customers weren’t only people already involved in illegal drugs or activities in the physical world. Silk Road made purchasing in illegal drugs so effortless some people did it just to see if it was that easy.

“Silk Road took drug trafficking into the twenty-first century. This was so easily accessible that it ended up getting into the hands of people that never really would have touched it.” D’Agostino said that this led to overdoses and

While drugs were Silk Road’s main market, they were not the only thing for sale on the underground marketplace.

“We saw murder-for-hire postings, hacking-for-hire postings, which was, ‘Hey, pay me two Bitcoin, and I’ll hack into your ex-wife or ex-husband’s email account’...and I suspect people were using it because it made a lot of sense. It was totally anonymous. And you could never trace it back to the person who asked for it,” said Special Agent Milan

You might wonder how this type of website was able to remain in operation for as long as it did. Two words: Bitcoin and Tor.

At the time that Silk Road was online, Bitcoin was believed to be a traceless form of payment that allowed complete anonymity. It has since been proven that the cryptocurrency is not completely anonymous; however, Bitcoin transactions don't involve the transmission of personal information, making them more private than using a debit

Former Special Agent for Homeland Security Investigations, Jared Der-Yeghiayan stated, "There's a computer somewhere—that actual website's running off of, and when the internet's trying to direct traffic to the website, it has to know where to go to. And what Tor does is it protects that information, it protects the IP

An IP address is an Internet Protocol address. It's a server or device's identification number, and it can tell you a few things about the server or device it is connected to, such as the ZIP code the device is located in, what type of device it is, or if it's attached to any Wi-Fi networks.

When you're connecting to the Web through Tor Browser, Tor constantly changes your IP address to ensure your anonymity. The goal of Tor is to offer users "as much privacy as possible" when This is why it is the only way to access dark web websites where illegal transactions take place that you would want to keep anonymous.

"Those traditional techniques that an investigator would use were useless in an online drug market—they didn't work," said Vincent

Milan Patel said their team was “always one step behind. Sometimes by

Even with the FBI desperately trying to track him and his server down, Ross refused to shut down the site. Silk Road was trafficking millions of dollars’ worth of illegal goods every month, and Ross was pocketing a cut of each

“If you take away the technology, it’s like any other enterprise, organized crime or otherwise,” said Milan

Ulbricht ran the Silk Road in a similar fashion to an organized crime enterprise with him at the helm. He employed henchmen to act as site administrators, moderators, and customer service agents.

One of these men was Curtis Green, a forty-seven-year-old grandfather. Green used the site under the username “Chronicpain,” a nod to his extensive knowledge of prescription narcotics. He eventually became a paid moderator for Silk Road. Green was arrested by the FBI during their hunt for Dread Pirate

It was required that moderators reveal their true identity to Ulbricht, so when he found out that Green had been arrested, he immediately feared that Green would become an informant. Ulbricht was especially troubled when he found out that $350,000 in Bitcoin had been stolen from multiple Silk Road accounts that were traced to Green’s

In an effort to protect himself from being unmasked, Ross asked one of his other online associates, known online as "Nob," for a favor. The favor was to execute Green. Unfortunately for Ross, "Nob" was an undercover Drug Enforcement Administration (DEA) agent named Carl Force. Force decided to stage Green's killing to further his relationship with Ulbricht, and Ulbricht paid the hefty price of $40,000 for the supposed

With Ross feeling his troubles had been eliminated, he paid a visit to a San Francisco public library one October afternoon. Using one of the available computers, he logged onto Silk Road using his administrator account under his online alias, Dread Pirate Roberts. He unknowingly began chatting with an undercover FBI

The FBI was able to infiltrate Silk Road by working alongside many of Ulbricht's closest associates and using their identities. They finally connected Ulbricht and Silk Road when a Google search connected Dread Pirate Roberts with another alias, "Altoid" which was used on a drug forum. The FBI then found that Ulbricht used the "Altoid" alias in a Bitcoin forum where he had posted his personal email

He'd finally been caught, and his online drug scheme was coming to a dramatic end.

Silk Road was shut down within a few hours of Ulbricht's arrest, and the domain was seized by law The attempted murder charges —for the incident with Green—were removed from the indictment. After his arrest, Ulbricht "pleaded not guilty to seven charges of

narcotics trafficking, criminal enterprise, computer hacking, and money laundering," according to *BBC*

Today, Ross Ulbricht remains in prison for his role in Silk Road, serving two life sentences plus forty years without the possibility of

US Attorney Preet Bharara said the conviction sent a clear message: "The supposed anonymity of the dark web is not a protective shield from arrest and prosecution." [178]

Not Your Traditional Crime

"Let's face it: the future is now. We are already living in a cyber society, so we need to stop ignoring it or pretending that is not affecting us."

—Marco Ciappelli, Co-Founder of [179]

There's nothing new under the sun.

An idiom you've probably heard repeated many times because its relevance reigns true for so many things we encounter in our lives. While we may reinvent the wheel, we can trace the issues we face in the modern, hyper-connected world to those of our formerly more analog one.

In the past, we have been trained to recognize threats by their proximity to us. The monster under our bed, the robber sneaking in through the window, the purse thief sneaking up behind you on the sidewalk.

However, we cannot use these same techniques for recognizing threats in cyberspace.

A cybercriminal can plan and execute an attack from anywhere in the world, and their victim doesn't have to be from the same country as them—let alone the same neighborhood. So, cyberspace gives criminals more free range to commit crime than they ever had before, whereas before, criminals had limitations—whether those limitations were the distance they were willing to or could afford to travel, their knowledge and skillset, or their physical strength and abilities.

Technology makes those limitations nonexistent. You no longer have to travel to steal from someone in another neighborhood or even another nation; you can purchase the malicious technology from illegal online vendors at negligible prices, and your strength isn't a factor in the virtual world.

There are two main categories of cybercrimes: cyber-dependent crimes and cyber-enabled

Cyber-dependent crimes, as the name implies, are crimes that can only be facilitated by means of a computer, computer network, or another IoT device. These types of crimes weren't possible prior

to the invention of computing technology. Examples of cyber-dependent crimes include spreading computer viruses and other malicious software or accessing a computer or network without permission, otherwise known as

Cyber-enabled crimes are traditional crimes that criminals have adapted to cyberspace to scale, simplify, or lessen the risks of their operations. Cyber-enabled crimes differ from cyber-dependent crimes because they can be performed in the absence of a computer, computer network, or another IoT device. For example, fraud and theft can be done in the physical world, but a criminal can use the Internet to increase how many people he reaches or decrease his likelihood of being

In our hyper-connected, modern world, what traditional, physical crimes don't already have a "cyber" equivalent? Most of the financially motivated crimes already do—fraud, identity theft, ransom. In addition to those, we've seen an increase in cyber harassment, stalking, and child sexual offenses to the point that it is often assumed that the crime was facilitated online even if it isn't explicitly

"Bad guys will always find a way to use technology for malicious purposes. It's just the way it is," said Austin Berglas, assistant special agent in charge of the cyber branch in the FBI's New York

Traditional criminals and cybercriminals have a lot in common. They don't follow societal norms or "conventional rules of engagement," as *The Cybersecurity Body of Knowledge* calls all, what makes a criminal a criminal is the fact that they have broken a law or a perceived social norm.

Criminals are motivated to commit cybercrimes for three main reasons: low barrier to entry, low chance of being caught (and convicted), low to no physical interaction with your victim.

"Having to play the game of being a bad guy or gal, you have options of which attack vectors in cyber is cheaper, less risky, reaches everyone, then no to very little chance of ever being found guilty...You're really a stupid criminal if you're just holding people up," Sam Curry, chief security officer at Cybereason, said at a discussion at Duke University about the top issue in

There is a common misconception among some people that all cybercriminals must be "hackers" with excellent programming skills to successfully execute a cyberattack. This idea would be false and misguided. "The term 'hacker' has become a catch-all phrase for any person who violates the security of a computer or its information...Although the common perception is that all hacking attempts are electronic in nature, the actual loss of data indicates that modern cybercriminal attacks tend to also be physical and human-centered exploits," according to *The Cybersecurity Body of*

While some cybercriminals are very skilled programmers, others are far from it. Many are referred to as "script kiddies." Script kiddies use the code of other more advanced programmers and hackers found online to perform malicious online acts. These criminals are particularly dangerous because of their lack of technical skills. They are typically only committing a cybercrime for

monetary gain, unlike some other hackers who might be driven by ego or personal or political agendas. Their lack of technical skills means that they are more likely to cause more damage than they anticipated with their attacks because they didn't fully understand what they were doing and the potential consequences.

Other cybercriminals don't utilize any code in their scheme at all. They weaponize their intellect, social, or communication skills to create a social engineering attack. (We will talk about social engineering further in a later chapter.)

"Let's just face it; most of this stuff is just cons at scale," Sam Curry told me when talking about malicious cyber activity.

The attribution problem that occurs with cybercrime is well known within the cyber community and is one of the things that draws criminals to the cyberspace domain. We will talk about the attribution problem more at the end of this chapter.

Even if you are introverted or reluctant to commit a crime, you can disconnect yourself from the consequences of your actions because you never have to physically see your victim when committing a cybercrime. Few people have the nerve or lack the morality to walk up to an old lady and steal her purse, but unfortunately, more people have the audacity to steal from an old lady's bank account or trick her into thinking she's giving her money to a good cause when she's handing it over to a thief.

Due to the COVID-19 pandemic, cybercrimes have become even more enticing for criminals because of the number of people spending more time at home, and in turn more time on their

devices. The pandemic has caused projections for cybersecurity spending, remote working, and IoT device purchases to increase. With more people than ever working, learning, and entertaining themselves at home, cybersecurity must be an important facet of our lives now more than ever.

The Attribution Problem

"In our digital age, nearly anything can be learned, compromised and/or fabricated to look exactly like someone else did it."

—Travis Farral, Author of *The Attribution Problem with Information Security Attacks* [188]

Law enforcement is supposed to keep us safe from criminals, hunt down the offenders, and take our complaints seriously when we file them.

The judicial system is supposed to be effective at deterring criminals from committing crimes by imposing sanctions on them that are reasonable for the crime committed but will deter others from committing them.

The legislative system is supposed to create laws that match our current circumstances yet manage to outpace future threats.

Unfortunately, this is not currently the case, as we are currently facing one of the largest crises our modern world will have to overcome, and it is growing exponentially year by year. Millions of

Americans and organizations have been financially and emotionally impacted with no relief in sight. The projected cost is expected to double to a massive six trillion dollars by 2021 from the 2018 expense of three trillion

Over the past few years, many organized cybercrime groups have formed that have thousands of members from all over the world. This makes attributing cybercrimes and attacks to a particular individual or group more difficult for law enforcement since they have resources spread across the globe. Even if they are the perpetrator of an attack, they are able to deflect the investigator's attention away from their own organization.

The more connected our society becomes the more avenues for obtaining and releasing sensitive details there are. The challenges of protecting all these potential attack avenues are far-reaching and will become broader as more options become

But attribution is not just possible; it has been happening successfully for a long time. Attackers cannot assume that they can cause serious harm and damage under the veil of anonymity and get away with

Just like with traditional crimes, there isn't a foolproof formula to finding the culprit who committed a cybercrime. While with physical crimes, evidence, eye-witness accounts, and testimonies can become reliable evidence to build a case around, when dealing with cybercrimes most criminals are smart enough to cover their tracks.

Helpful evidence like IP addresses can be quickly disguised using software that is easy to obtain, such as a VPN. This leaves cybercriminologists having to use deductive reasoning skills to solve the case.

Starting by asking, "Who would have the means, motive, and opportunity to do so? How easy or hard would it be for another actor or actor group to use these same tools and techniques and procedures? What is the evidence telling me alongside what I already

This is remarkably similar to the deductions that detectives must make during investigations into physical crimes. Starting with the people who have means, motive, and opportunity to commit the crime.

However, in cybercrime, it is much harder to eliminate suspects because you cannot rely on evidence such as GPS data or DNA evidence to narrow your search. Also, since cyberattacks are often committed by groups, it makes it even more difficult to track down the offenders. Attackers can commit these attacks from anywhere in the world and can have partners on the other side of the globe.

The real attacker may also deliberately lead investigators in the wrong direction during their investigation to protect

"Due to the circumstantial nature of the typical types of evidence used for attribution, there is only *suspicion* that a particular actor or group was behind the attack. But generally, nothing that can definitively prove those suspicions. This is true even if the evidence does happen to point in the true attacker's direction," said This means that even if the evidence is pointing in the right direction, there is typically no way to prove it beyond a suspicion that a particular person committed the attack.

Often, law enforcement will use top secret or highly controversial techniques to apprehend an offender or bring down illegal websites, and in some cases, they have decided to not take the case to trial in order to evade revealing the technology that was

Overall, it is evident that not only is the collection of evidence in cybercrime cases an issue, but so is attributing the crime to an offender and prosecuting that offender properly. If physical crimes were being ignored by the justice department in the same way the cybercrimes were, the public would be appalled. Currently, as local, state, and federal law enforcement fight over the jurisdiction of cybercrime cases and we try to figure out how to hold cybercriminals responsible for their criminal acts, someone else becomes a victim of a cybercriminal.

In the words of Shoemaker, Kohnke, and Sigler, let me pose a question to you: "If you could commit a crime that nobody knew about, would

130 "Cybersecurity Quotes," Goodreads, accessed January 31, 2021.

131 George Hurlburt, "Shining Light on the Dark Web," *Computer* 50, no. 4, (April 2017): 100-105.

132 Ibid.

133 Andrew Norry, "The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin," *Blockonomi* (blog), October 17, 2017.

134 Ibid.

135 Hurlburt, "Shining Light on the Dark Web," 100-105.

136 Ibid.

137 Norry, "The History of Silk Road."

138 "Inside the FBI Takedown of the Mastermind behind Website Offering Drugs, Guns and Murders for Hire," *CBS* November 10, 2020.

139 "History," Tor Project, accessed February 1, 2021.

140 "Inside the FBI Takedown." *CBS News.*

141 "History," Tor Project, accessed February 1, 2021.

142 "Inside the FBI Takedown." *CBS News.*

143_Joshuah Bearman and Tomar Hanuka, “The Untold Story of Silk Road, Part 1,” May 2015.

144_Norry, “The History of Silk Road.”

145_Bearman and Hanuka, “The Untold Story of Silk Road.”

146_Ibid.

147_Ibid.

148_Ibid.

149_Ibid.

150_Ibid.

151_Ibid.

152_“Inside the FBI Takedown.” *CBS*

153_Ibid.

154_Ibid.

155_Bearman and Hanuka, “The Untold Story of Silk Road.”

156 Ibid.

157 Ibid.

158 Ibid.

159 Ibid.

160 "Inside the FBI Takedown." *CBS News.*

161 Ibid.

162 Ibid.

163 Oliver Dale, "Don't Forget—Why Bitcoin Is Not Truly Anonymous," *Blockonomi* (blog), August 10, 2017.

164 "Inside the FBI Takedown." *CBS News.*

165 "History," Tor Project.

166 "Inside the FBI Takedown." *CBS News.*

167 Ibid.

168 Ibid.

169 Ibid.

170 Ibid.

171 Norry, "The History of Silk Road."

172 Ibid.

173 Ibid.

174 Ibid.

175 Ibid.

176 "Ross Ulbricht: Silk Road Creator Convicted on Drugs Charges," *BBC* February 5, 2015.

177 Norry, "The History of Silk Road."

178 "Ross Ulbricht: Silk Road Creator," *BBC*

179 "The Cyber Society," ISTP Magazine, accessed February 2, 2021.

180 Steven Furnell and Samantha Dowling, "Cybercrime: A Portrait of the Landscape," Journal of Criminological Research, Policy and Practice 5, no. 1, (February 2019): 13-26.

181 Ibid.

182 Ibid.

183 Ibid.

184 "Inside the FBI Takedown." *CBS News.*

185 Daniel Shoemaker, Anne Kohnke and Ken Sigler, *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in* (New York: CRC Press, 2020), EBSCOhost.

186 *Duke University School of* "Cybersecurity Law and Policy: What Are the Top Issues for 2019?," Feb 6, 2019, video, 57:19.

187 Shoemaker, Kohnke and Sigler. *The Cybersecurity Body of Knowledge.*

188 Travis Farral, "The Attribution Problem with Information Security Attacks," *Network Security* 2017, no. 7 (May 2017): 17–19.

189 Shoemaker, Kohnke and Sigler. *The Cybersecurity Body of Knowledge.*

190 Farral. "The Attribution Problem."

191 Ibid.

192 Ibid.

193 Ibid.

194 Ibid.

195 Farral. “The Attribution Problem.”

196 Shoemaker, Kohnke and Sigler. *The Cybersecurity Body of Knowledge*.

Chapter 6
What is PII?

"The diverse threats we face are increasingly cyber-based. Much of America's most sensitive data is stored on computers. We are losing data, money, and ideas through cyber intrusions. This threatens innovation and, as citizens, we are also increasingly vulnerable to losing our personal information."

—James Comey, Former Director of the

As you'll see in this chapter, when cybercriminals obtain your personal information and commit identity fraud, it can cost you more than just your lifestyle—it can truly cost you your life.

After a long day at work, you pull up to your home and you check the mail as you do every day. You take the mail inside and see an envelope that catches your eye. "Confidential" is written on the front of the crisp white envelope in big, bold, red ink. You open the letter thinking it could be something important from your job. To your shock, it's a $44,000 hospital bill for a surgery.

However, you've never had surgery before. In fact, you've never even been hospitalized.

For Joe Ryan, a pilot and business owner, this was his reality. Ryan was a victim of medical identity theft. Medical identity theft

is “when someone uses your personal information to collect money, prescription drugs, goods, or health

It’s similar to other versions of identity theft in that it can cause severe financial damage to the victim, but this type of identity theft can also have unforeseen medical consequences. If your medical records are changed, this can cause your chart to include inaccurate medical history, diagnoses, or If someone changes your chart to no longer include that you’re allergic to codeine and you seek emergency medical care without knowing that has been changed, that can have serious consequences.

This is especially vital today when many health systems share data and records between many different hospitals, doctor’s offices, and clinics across the country. Therefore, if your medical information is tampered with at one healthcare facility this can have a cascading effect on your records beyond just that specific hospital or hospital system.

Pam Dixon, executive director of the World Privacy Forum, estimates that up to 500,000 Americans may be victims. Dixon says, “Medical identity theft causes terrible harm, both financial and

After Ryan received the bill, he pursued an investigation into the case, and the investigation proved to be very revealing. It was uncovered that a previously convicted criminal had used Ryan’s Social Security number to check into the hospital and have his surgery. The ex-con got his procedure done without raising any

red flags, and in the end, he successfully carried out his efforts to leave the real Ryan holding the

When interviewed over two years later by WebMD, Ryan said, "I still can't get my medical records straightened out." According to WebMD, he says the event has emotionally scarred

What is PII?

The term "PII" stands for personally identifiable information. PII is considered anything that can be traced back to you alone or when combined with another piece of personal information.

According to McCallister, Grance, and Scarfone PII is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records and (2) any other information linked or linkable to an individual, such as medical, educational, financial, and employment

US General Services Administration says PII is "not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available—in any medium and from any source—that, when combined with other available information, could be used to identify an

So, what types of information are considered PII?

PII includes information that can directly identify an individual, such as a social security number. In addition to directly identifiable information, PII is also comprised of information that can be used to trace an individual's specific activities.

Specific Examples of PII include, but are not limited to:

•Name, such as an individual's full name or their mother's maiden name
•Street address, email address, and IP address

•Identification numbers (i.e., social security number, passport number, bank account number, driver's license number, credit card number)
•Telephone number
•Passwords or answers to security questions
•Information that can be combined with one of the above to trace an individual (i.e., gender, race, birth date, geographic indicators, activities, employment information, medical information, education information, financial information)

Why is this information considered personal and identifiable?

Information is considered identifiable because the information can be used to verify your identity. Social Security numbers, driver's license numbers, and passports are all widely used forms of identification. If yours falls into the wrong hands, one can easily

impersonate you, especially in cyberspace where you most times cannot verify that the person putting in your social security number is actually you by looking at the picture on your ID.

What fits into the category of personal information is going to vary based on the individual. Your passwords and the answers to your security questions are your personal information, but those are going to be different for everyone (hopefully!).

Your personal information includes anything that would be deemed sensitive and could be used by a cybercriminal to directly identify you and your habits. This can include the fact that you go to brunch with your friends every Sunday at that expensive diner on street or that you recently got a promotion working for Y company, and you'll be making X amount more money now.

Making this type of personal information public can increase your likelihood of being the target of a cybercriminal, because you're presenting yourself as a suitable target by disclosing your habits and income level.

It also should be noted that not all PII is created equally. A large percent of the world's population is the same gender as you, so if you disclose that information to someone it doesn't hold the same risks as you disclosing your social security number, which is unique to you.

Despite this, every piece of your PII should be treated with care and protected because you never know what might happen if it

falls into the wrong hands.

Just Another Case of Stolen Identity

"Criminals look at identity theft and say only one in 700 criminals gets convicted of it. And they look at check forgery and they know that for every 1,400 forgers arrested, only about 123 get convicted and about twenty-six go to jail. So, the rewards are great, but the risks are very slim. So that's one of the reasons that make it very popular."

—Frank Abagnale, Security

One of the biggest risks associated with stolen PII is identity theft. According to the United States Department of Labor, "The loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of the

You very likely know someone who has been a victim of identity theft. When surveyed, one out of fifteen consumers reported being a victim of identity theft. One in

According to the FBI, "Identify theft involves a perpetrator stealing another person's personal identifying information, such as name or social security number, without permission to commit fraud." The Bureau also separately defines account takeover as "when a perpetrator obtains account information to perpetrate fraud on existing

Unfortunately for Simon Bunce, he's a part of that Not only was his financial freedom being threatened, but his physical freedom as well.

In 2004, one of Bunce's favorite pastimes was online shopping. Like so many of us, he loved the excitement of having his packages delivered to his doorstep and being able to avoid taking an unnecessary trip to a brick-and-mortar store. Although he loved the thrill of shopping online, he felt that he was doing his best to only shop with stores that he deemed were

To his surprise, he would become involved in the UK's controversial police hunt against online pedophiles, Operation

UK police arrested him on "suspicion of possession of indecent images of children, downloading indecent images of children and incitement to distribute indecent images of children." After his arrest, the police confiscated his computer, flash drives, and CDs, including the ones he used for

News of Bunce's arrest spread like wildfire as the community began to learn more details about Operation Ore. The effect the arrest had on Bunce's life was swift and dramatic. As soon as his employers discovered the reason for his arrest, he was terminated from his 120,000-euro-a-year job. His family members disowned him because of the

"I made the mistake of telling my father, and he cut me off," Bunce said to "He then told all my siblings and they also cut us

The only person who remained by his side and supported him in his attempt to clear his name was his wife, Kim. Unfortunately, the gossip showed no signs of slowing

In cases like this, the police's computer technicians can take several months to look through all of the digital evidence, but Bunce didn't want to wait that long for his name to be vindicated.

"I knew there'd been a fundamental mistake made, and so I had to investigate it," he

The gateway site Landslide, used to purchase the illegal content, was based in the United States and was under investigation

Through the US Freedom of Information Act, Bunce was able to gain access to all of the information that he needed about his case to track how his credit card had been used. By tracking his IP address, Bunce discovered that the person who used his card to purchase the lewd material was in Jakarta,

At the same time, Bunce was in South London swiping his card for a meal at a restaurant, and he had the credit card bills to prove

"I can't be in two places at once, so somehow my data had got to the man in Indonesia," he

Later that year, the police told Bunce they wouldn't be proceeding with the investigation against him. They failed to find any indecent material on his hard drives and accepted that he wasn't the one who made the online

Thankfully, he's made amends with his family after explaining to them how this happened to him, "I've forgiven them [my family]—there's no point in bearing a

However, the damage to his public reputation was already done. After an extensive six-month job hunt, he secured another job. However, his salary is one-fourth of what he was earning prior to his

Tragically, Simon Bunce is far from being alone. In 2019, 16,053 victims reported identity theft to the FBI. Those cases had a combined $160,305,789 in

Awareness Is Everything

As we navigate today's interconnected world, we must be aware of the value of our identity.

To cybercriminals, your identity is a ticket to endless possibilities from opening credit cards, committing crimes, to having medical procedures without having to foot the bill. With the growing number of cases of identity theft, individuals need to safeguard their personal information now more than ever. In a world that is

being more interconnected by the minute, criminals are gaining more ways to obtain your

Routine activity theory usually measures the victim's exposure and proximity to a motivated offender as time spent outside the home and area crime However, in the modern world, your proximity to someone is merely an illusion.

Unlike in 1942, we can't simply observe our physical surroundings and assure ourselves that there isn't a motivated offender in our midst, ready to take our personal information. Factors that typically protect you from traditional crimes, like a low rate of crime or unemployment in your community, won't save you from becoming a victim of a cybercriminal.

When surveyed, American consumers were 22 percent more concerned about their PII being stolen than the death of themselves or a loved one, and their concerns are This is a massive issue that can't be resolved by installing security monitors in your home or avoiding high crime areas, and for most people avoiding the Internet is simply not an option today.

So, we must take the route of awareness and prevention by adopting a cyber curiosity mindset.

Your PII is important, and it is your responsibility to protect it. You are—and will always be—your first defense against a cyberattack.

197 James B. Comey, *Homeland Threats and the FBI's Response* (Washington, DC: Federal Bureau of Investigation, 2013).

198 R. Morgan Griffin, "The Scary Truth about Medical Identity Theft," *Feature Stories* (blog), accessed February 9, 2021.

199 Ibid.

200 Ibid.

201 Ibid.

202 Ibid.

203 Erika McCallister, Tim Grance and Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (Pii): Recommendations of the National Institute of Standards and Technology* (Gaithersburg, MD: US Department of Commerce, National Institute of Standards and Technology, 2010), Government Documents Electronic Resources.

204 "Rules and Policies—Protecting Pii—Privacy Act," US General Services Administration, last modified on October 8, 2019.

205 "Frank Abagnale Quotes," BrainyMedia Inc, accessed February 9, 2021.

206 "Guidance on the Protection of Personal Identifiable Information," US Department of Labor, accessed February 9, 2021.

207 Bob Sullivan, "Identity Theft Is Skyrocketing, and Getting More Sophisticated," *Credit.com* (blog), *MarketWatch* February 27, 2018.

208 US Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report* (Washington, DC, 2019).

209 Marc Sigsworth, "I Was Falsely Branded a Paedophile," *BBC News*. April 3, 2008.

210 Ibid.

211 Ibid.

212 Ibid.

213 Ibid.

214 Ibid.

215 Ibid.

216 Ibid.

217 Ibid.

218 Russ Smith, *IP Address: Your Internet Identity,* (US Department of Commerce: Washington, DC, 1997).

219 Sigsworth, "I Was Falsely Branded."

220 Ibid.

221 Ibid.

222 Ibid.

223 Ibid.

224 US Federal Bureau of Investigation, *2019 Internet Crime*

225 US Federal Bureau of Investigation, *2019 Internet Crime*

226 Bradford W. Reyns and Billy Henson, "The Thief with a Thousand Faces and the Victim with None: Identifying Determinants for Online Identity Theft Victimization with Routine Activity Theory." *International Journal of Offender Therapy and Comparative Criminology* 60, 10 (August 2016): 1119-1139.

227 Steve Symanovich, "What Is Personally Identifiable Information (Pii)?," *ID Theft Resources* (blog), *NortonLifeLock* September 6, 2017.

Chapter 7
Malicious Intent

Computer virus. Ransomware. Malware. What do you think of when you hear those terms? You might not think of the $10,974,966 in victim losses from 2019 reported by the FBI or the threat they pose to your personal safety, but you

Malicious software. A vague yet also self-explanatory name.

How can software be malicious? What makes software malicious—the user or the software itself? Well like most cybersecurity concepts, it's not a black-and-white subject. As you find out in this chapter, sometimes software is malicious by nature. Other times, the intent of the human operating the software determines if the software is malicious and how malicious it will be.

Gone Viral

"I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We've created life in our own image."

—Stephen

What is considered “malicious software?” You’ve probably heard it referred to as a “virus,” and while a virus is a type of malicious software, it is not the only type of malicious software that exists.

Malicious software is often referred to as malware. According to Kaspersky Lab, “Malware usually appears in the form of a useful program that is available for download from a genuine-looking company website, email or pop-up advertisement. The malware program is written into the program and can cause harm to the user’s computer, as well as monitor computer use and copy sensitive Common types of malware include viruses, worms, Trojans, spyware, ransomware, adware, and rootkits.

Computer viruses, worms, and Trojans are similar types of malware, but they have very distinct differences. So, what are the differences between them?

According to Cisco, “Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected email

It is important to remember that viruses cannot spread without human action. A virus spreads by inserting a copy of itself into another program and becoming a part of it. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program.

The virus must be spread by a human sharing infected files (oftentimes unknowingly) through emails, attachments, and other means. Just like a human virus, computer viruses can vary in the amount of harm they cause to the system they infect, ranging from a mild annoyance to a complete destruction of data.

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. Worms are often considered a sub-type of a virus. Unlike viruses, worms are standalone software, and they don't require a host program or human interaction to

An example of a worm's self-replicating ability would be a worm infecting your system, then sending a copy of itself to everyone on your email contact list. Once the worm makes it to the recipient's device, the worm would then replicate itself again and send itself to everyone in the recipient's contact list. The worm would continue to spread until it is

In Chapter 1, we discussed the Morris worm, one of the first known malware attacks, and its destructive nature because of how fast it was able to spread on its own after being deployed.

A Trojan is another type of malware. The Trojan gets its name from the wooden horse that the Greeks used to infiltrate Troy. Like viruses, Trojans require user interaction to spread. Unlike viruses and worms, Trojans don't infect other files, and they don't have the ability to

Trojans often look like legitimate software, like an antivirus or a software from a trusted organization. This trickery leads users to download the malicious software onto their system thinking that it is something of value. After it is on the user's device, it can perform any number of attacks from being a mere nuisance—creating pop-ups or shutting down windows—to damaging the device or data on the device—deleting files, stealing private information, spreading other malware. Trojans can also create backdoors that can give malicious users access to the

Viruses, worms, and Trojans are just one category of tools that malicious actors can use when employing a cyberattack using malware. Within the umbrella of malware, there are many more tools at a malicious actor's disposal.

Held for Ransom

"Ransomware is unique among cybercrime because in order for the attack to be successful, it requires the victim to become a willing accomplice after the fact."

—James

One thousand four hundred and nine-three victims in the US alone and $3,621,857 in reported losses. Two thousand and forty-seven victims. Eight million nine hundred and sixty-five thousand eight hundred and forty-seven dollars in losses. An over 37 percent increase in victims. An over 147 percent increase in

losses. These figures represent the impact and exponential growth of ransomware from 2018 to

Ransomware is a type of malware, installed onto a computer or network designed to block access to a device or network—and all of its data—until money, a ransom, is paid to the attacker. More sophisticated attacks use more advanced encryption at the disk or file level making it nearly impossible to decrypt the files without paying the [240]

When I clocked in on the early morning of October 1, 2019, it was a typical fall day in Tuscaloosa. We were experiencing one of our signature pop-up rainstorms, and my co-worker, JT, and I were sitting in the office talking about classes.

"Isn't your assignment due Thursday?" I asked JT.

"Yeah, but it's Tuesday, so I'll start on it tomorrow," JT said, as we both chuckled. "What time is it?"

"11:02."

Our supervisor, Matt, came into the dark room. JT and I seemingly in unison said, "Hi!"

Matt asked, "Have you guys seen the news?"

JT and I flash each other a confused look. “No, what news?” I asked.

“DCH Hospitals got attacked by ransomware. They’re not taking any new patients, and they’re having to use all paper for everything. Everything electronic is down,” Matt said. “Look it up.”

We went online to search for information about the attack and found a news article from *Tuscaloosa*

In the article, a DCH spokesperson said, “The network became infected when someone opened an email with an infected attachment. No patient data has been

The article went on to say that staff was waiting for FBI and Secret Service agents before opening the file containing the hacker’s monetary demand to release control of the

“Wow,” I said. “That doesn’t sound good.”

“Yeah, it’s not,” Matt said. “I wonder who opened that attachment.”

“Do you think they’ll pay the ransom?” JT asked.

“They’ll probably have to,” I said. “It’s not a good option but staying closed isn’t either.”

“That’s true,” JT said.

In cases of ransomware, “the FBI does not advocate paying a ransom,” according to their This is because paying the ransom does not guarantee that the organization or victim will regain access to its data. There have been cases where victims paid the ransom and were never provided with the decryption key to decrypt their files.

Even with a valid decryption key, it is possible that the victim may not be able to recover some or all the data. Paying the ransom also encourages criminals to continue to target organizations and individuals with ransomware, and it makes the attack method more alluring to other

The DCH Hospital System serves a large portion of West Alabama. The three hospitals—DCH Regional Medical Center, Northport Medical Center, and Fayette Medical Center—house about 850 beds and admit more than 32,000 patients in a

“Our hospitals have implemented our emergency procedures to ensure safe and efficient operations in the event technology dependent on computers is not available,” a statement on the DCH System site said, in

All but the most critically ill or injured patients were being diverted to hospitals in Birmingham or Mississippi, but staff at the Tuscaloosa, Northport, and Fayette hospitals continued to care for existing Days passed by as the public grew anxious about what would happen. We were essentially living in a community

without a fully functioning hospital system, and the nearest hospital is almost an hour away from our crowded college community.

It seemed like a lose-lose situation for DCH. If they surrendered and paid the ransom, they would be giving the attackers exactly what they want, therefore fueling future attacks. Paying the ransom also didn't ensure that the attackers would release the decryption key to unlock the system. However, this is not public knowledge, and every day they don't pay the ransom the public is suffering as a result, and so is their image. If they decided against paying the ransom, they would have to find a way to decrypt the ransomware themselves, which can take weeks or even months.

On Saturday, October 5, DCH Hospitals paid the ransom to receive a decryption key from the attackers that would expedite system recovery. They did not release an amount

These attacks on our critical infrastructure will become more common especially if we do not take steps to prevent them and the damage they can cause. Given the delicate nature of the healthcare system, they are perfect targets for ransomware attacks because they are very likely to pay the ransom to get their files back. They cannot afford to lose the sensitive data that their systems hold.

While the method used to attack DCH Hospital's system was ransomware, their means of facilitating the attack was via a phishing scheme. An employee opened an email with an infected

attachment, and it unleashed this malware onto the hospital's network.

In order to prevent attacks of this type in our own lives and to recognize them in workplace settings, we must be aware of our personal responsibility for our cybersecurity. This case demonstrates why having a personal awareness of cybersecurity is so valuable.

Employee training focused on identifying and avoiding potential cyber threats should be offered to all employees. However, it is also the employee's responsibility to absorb the information and use it to assess real-world risks. The employee should have been made aware of the cybersecurity risks of opening an email attachment from an unknown source, especially at his workplace.

If you are ever unsure about an email or text message you've received, a link, or an attachment, ask someone with expertise to view the message and give their opinion. If the message claims to be from a reputable company, like your bank, or someone you know, call them directly to confirm they sent you a message and confirm the contents of the message before opening any attachments or links.

Most universities have on-campus IT departments that will take any reports concerning a phishing attempt directed at a university email address, and they can confirm whether the email is legitimate for you. Many businesses have an in-house IT department as well. If you ever second guess the legitimacy of a

message, especially one sent to you on the company's email, you should let them know immediately.

As a preemptive measure, DCH Hospitals should have had a backup of their critical files created before the attack. This would have mitigated the damage caused by the ransomware and allowed the hospital to maintain normal operations.

This is also a great tip for individuals, as well. In the case of a ransomware attack where you do not want to pay the ransom or some of your files are lost in the attack, you will want to have a backup of your most important data. We will discuss how to pick the right storage solution for your situation, in a later chapter.

Ransomware, while not happening more frequently, is becoming more costly and also increasingly dangerous to our physical well-being as our critical infrastructures are targeted.

As an employee, you need to be aware of these threats because if your company is targeted, you need to be able to recognize the attack and report it to your IT department immediately.

In our daily lives, we must be cognizant of cyber threats. We as a society have come to believe that cyber threats are not as real as physical ones, and we often forget the damage that can be caused.

Don't Ignore the Risk

Commonly, when ransomware is depicted in the news, the stories focus on the impact the ransomware has had on corporations, large organizations, or healthcare systems. Rarely do you hear about the ransomware attacks waged against individuals, but this is not because these cases are few and far between.

When I asked Sam Curry what he was most concerned about when it comes to individuals using IoT devices, he said, "I worry about their safety. I worry about the ransomware affecting them. I worry about scams."

This is because ransomware targeted toward individuals is a real threat to our safety when engaging with the Internet.

There are two main methods used when deploying ransomware: encryption and lock

Encryption ransomware specifically targets certain files saved locally on the device. These files are typically hand-picked beforehand by the attacker using phishing techniques or other forms of malware to research their target. After the files are encrypted, the victim will be asked to pay a fee in exchange for a decryption key to access their files. This technique typically targets information that is either confidential or sensitive. This is the way that most businesses or companies are targeted. From the description of the attack, this was the type of ransomware used on DCH's

On the other hand, lock screen ransomware doesn't just encrypt certain files but renders a user's device virtually useless. With lock

screen ransomware, the device will display a full-screen message that cannot be closed, minimized, or moved asking for payment for the return of their device.

These programs may include scare tactics to expedite payment, like a countdown timer that threatens to erase your files when it hits zero. Other scare tactics may include alleging that the attacker knows that the device has been associated with illegal activities or extreme pornographic material and that they will contact law enforcement if they are not paid. A different strategy is that the ransomware itself includes pornographic imagery and the message claims they cannot be removed unless the ransom is paid in

John was a successful lawyer who knew his way around a computer. He ran his own law practice and relied on his computer heavily to keep track of client data and information. Even though John was aware of the risks, he used the same computer that he used to store confidential, personal client information to do personal tasks like web browsing. He chose to ignore the risks, and ultimately John was attacked by a case of lock screen ransomware. When John turned on his computer, he was shocked by what was displayed on his screen. A threatening message written in red text was demanding ransom for his computer files. The message said that he had only fourteen days to pay a ransom in Bitcoin, or his files would be deleted

Understandably, John is startled by this, “My first reaction was panic. My second reaction was to get on another computer and figure out exactly how much 1.71 Bitcoin was worth in US

John didn't have a backup of the data on his computer which stored important files containing the personal information of his clients and details of cases he worked on. He was "terrified at the thought" of losing this valuable

After doing some digging into the going rate for Bitcoin, he found out that 1.71 Bitcoin would cost $600 in 2016. At this point, John felt anger and frustration set in. The situation reminded him of the invasion of privacy he felt when his home was burglarized a few years

So, he decided to take matters into his own hands: "I decided I was not going to give them a penny and was going to find some way around this," he

He consulted with several local computer security companies about his situation, but he only found one that was willing to help him. However, the price of their service was over ten times the cost of paying the ransom, $7,000, if they were able to decrypt the ransomware—or zero dollars if they were unable

John agreed to their terms as he refused to pay the attackers a dime, and he didn't trust that their demands would end there, "I thought, what's to stop them from asking me for more money?" He continued, "If it had been my personal computer, I probably wouldn't have paid, but this was absolutely necessary for my business and my

Three days later, he got his computer back from the security company with his files intact and the ransomware removed. He paid them the

However, he was still paranoid, so he bought himself a new computer. Now, he stores files from his old computer on an external hard drive not connected to the Internet as a precautionary

"I think I always understood the risk but just ignored it. Now, I'm much more cautious about security and software updates and always make sure that I do regular backups. I also use a cloud-based software with the highest security protections for all my client files," John

While John never reported the crime to law enforcement, he did call his insurance company, and they were able to reimburse him the $7,000, as they classified it as

Anyone can be a target of ransomware: individuals, government entities, hospitals, or private businesses. You must take steps to protect yourself against these types of attacks as their frequency increases.

iSpyware

Look around. Are you alone in your room? If you answered yes, I want you to think about it again. Are you *truly* alone? You should probably check to make sure.

Spyware. It's a twelve-billion-dollar, unregulated industry, and it's rapidly

Spyware is a type of malware designed to monitor the digital activities of the user, usually without their consent or knowledge. It is often secretly packaged with another program or disguised as legitimate software. On a phone, it is most often an app installed with or without your knowledge by someone who has access to your phone.

Unlike a virus or ransomware, the main objective of spyware is typically not monetary gain or complete control of the electronic device. When a malicious actor employs spyware, the goal is to monitor the target in some way either by listening, watching, or tracking their movements without their knowledge or consent.

Today, spyware has become widely available to consumers. You will often see ads claiming that they will help you catch your cheating partner or monitor your child's online activities and location. These apps are a form of spyware that can be purchased and used to monitor the inspecting party.

But how far is too far when it comes to spyware?

With the widespread availability of spyware, the risk of the product being used in malicious ways increases. As ease of access to consumer options increase, spyware will increasingly be used to

compromise individual's privacy and personal information while being a beacon for digital account compromises, harassment, and

From the use of keyloggers in financially motivated cybercrimes to covert surveillance software in domestic violence and harassment cases, spyware's use cases are wide ranging and damaging for those subjected to them. As a society, it seems we have mostly accepted the fact that these services are available, and many people use them proudly and openly on their children or other loved ones.

However, with these services so widely available, if you didn't sign up to have your every move watched and monitored, how can you be sure no one's watching? And how can we be sure that the person watching doesn't have malicious intent?

While spyware is the most used type of malware in personal or domestic attacks, not all spyware cases have specific

In 2018, an Ohio man, Phillip Durachinsky, was charged in a sixteen-count indictment for allegedly creating and installing a type of malware, spyware, onto thousands of computers over the span of thirteen years. From 2003 to January 20, 2017, Durachinsky allegedly illegally accessed thousands of computers owned by individuals, companies, schools, a police department, and the

He was using the spyware to watch, listen to, and obtain personal information about the victims without their knowledge. The software he allegedly developed would also function as a keylogger

and turn the camera and microphone on whenever the victim walked away from the computer. He also allegedly used the malware to produce child

The twenty-eight-year-old used the spyware to gain access to a variety of very personal information about the victims including their passwords, tax records, medical records, personal pictures, banking records, and private communications. According to his indictment, Durachinsky also allegedly saved millions of images from the compromised webcams and “kept detailed notes of what he

For his cybercrimes, Durachinsky was charged with Wiretap Act violations, Computer Fraud and Abuse Act violations, production of child pornography, and aggravated identity

While Durachinsky’s case is on the extreme end of the spectrum not only because of the number of people he victimized, but also how heinous his crimes were. His case shows the capabilities of spyware when malicious intent is involved.

It is important to address that the spyware software itself is simply computer code. Therefore, alone it is morally The way in which the software is used is what makes it spyware.

If you were to install a keylogger on your own computer to keep track of how many letters you type in a day, that is not spyware because you are aware that you are monitoring your own actions. However, installing a keylogger on the device of an unsuspecting

person and collecting their usernames, passwords, and other sensitive information so you could use it to hack into their accounts would be spyware.

The difference is the malicious intent of the user and lack of knowledge of the person in the second example that they were being monitored.

Spyware differs from legitimate applications that share data from smart The main differences are the lack of consent, targeting and monitoring of individuals or groups of individuals, and the full disclosure of private information found with spyware.

With legitimate applications, if your data will be shared with a third-party it is typically disclosed in the privacy policy, which users are required to sign before using the application. The intent of applications like social media platforms or online map services is not to target specific individuals or groups and monitor them, they collect data from a variety of users.

Most websites and applications encrypt sensitive or private information, like passwords, so they are not readable by the naked eye. With spyware, private information is fully disclosed to the operator of the spyware.

Many popular consumer spyware products claim to have millions of users, but this cannot be proven. The numbers surrounding how many people use consumer spyware widely vary, from hundreds of thousands to millions of users, depending on your

[273] One thing that can be agreed upon, however, is that the issue is prevalent.

From spyware installed onto devices by a stranger—like the Durachinsky case—or specifically targeted spyware installed by someone that you know, the impact and implications of spyware vary widely. However, one fact remains the same. Spyware is a threat to personal privacy rights, because of the possible malicious intent involved if you have spyware installed on your device by a third-party, it is a threat to your cybersecurity.

In our modern world, there are very few people who don't own a cellphone. A Pew Research poll showed that 96 percent of Americans owned a cellphone, and 81 percent owned a smartphone, a drastic increase from the 35 percent of American smartphone owners in

For most of us, our smartphone has become our main computing device, and we wouldn't be caught without it by our side. This makes our phone the perfect host for spyware because the operator of the software can be almost certain that you have the device with you at all times.

Another thing that makes phones vulnerable to domestic attacks is ease of access. We often leave our phones unattended around our partners, family, and friends without a second thought.

However, according to a Pew Research study, many smartphone users haven't taken adequate steps to protect their devices. Twenty-eight percent of smartphone owners claim to not use a

screen lock or any other security features, such as fingerprint, facial recognition, or a passcode, to access their

This careless behavior leaves their device more vulnerable to an attack because the attacker doesn't even have to take the time to crack the passcode to their device.

Our phones track and store so much personal information about ourselves, from our GPS location to our personal communications. For this reason alone, we should want to secure our devices from finding their way into unfavorable hands and being compromised with malicious software.

Unfortunately for Android users, Androids are more susceptible to consumer spyware products than iPhones. According to research from Deakin University, "This is a consequence of the Android operating system being more permissive of software functionality, allowing third-party developers greater latitude to build programs of less-restrained Android's OS allows for more freedom—which users of the platform adore—but it also allows for more freedom amongst malware creators.

It is more difficult to install spyware onto an iPhone that can gain camera access of the device. You would need to jailbreak the iPhone first, which is a process that involves installing third-party software that overrides the iPhone's built-in security features and voids any existing warranty you may

In comparison with Android phones, applications available for purchase on the Google Play Store can provide real-time photo or video from the device without the target's reasonable However, this does not mean that iPhone users are completely safe from being victims of spyware.

The researchers at Deakin University in Australia decided to do a lab test on a jailbroken iPhone X to show the full capabilities of consumer spyware. On the modified iPhone, they were able to install a spyware application called

On FlexiSPY's website, they claim their goal is "to keep your loved ones, your business, and your personal information On the site, they describe the experience of being able to spy on an iPhone from the comfort of your couch.

"Imagine being able to remotely see everything that's happening on an iPhone from the comfort of your armchair or on the move using our unique mobile viewer app. Imagination just became reality. After it's installed, FlexiSPY silently captures all information coming and going from the phone and allows you to view or listen to that information—any time, any place—no matter where you are," says the homepage of FlexiSPY's

As we will see, the application delivers on its promises to remotely capture information, but they may have forgotten about their main goal in the process.

After installing the spyware onto the phone, the research team simulated normal phone use. Making calls, running errands around town, checking emails, using social media, snapping photos, and sending text messages.

While a "target" was using the phone, an "operator" was sitting and accessing all of the private data from the phone, thanks to an Internet portal that the spyware vendor provided.

During this experiment, it was found FlexiSPY could obtain the following types of data without the target's knowledge:

knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge: knowledge:

In addition to gathering that data, the application had a number of other alarming functions including acting as a keylogger, remotely controlling the camera, taking pictures or video from the target device, listening to the audio, and impersonating the user in text messages. None of these functions have any practical usage, except in cases where the user is unaware that the software is installed on their device.

The harm that can be done by allowing an application with this type of functionality to be sold to consumers far outweighs any benefit that can be perceived.

Unfortunately, this is not the only application for iPhone or Android devices that offers similar capabilities. There are spyware applications that only offer a fraction of the functions that this software does. However, even if only a small number of device functions are compromised (for example your location data and text messages) this could still have huge consequences on your cyber privacy and aid in harmful activities such as cyberstalking, if the information is being used by someone with malicious intent.

Confidentiality, integrity, and availability of information. How can we ensure them? The presence of consumer spyware undermines our confidence in security and privacy of our IoT Someone can easily install software that has the ability to disrupt the confidentiality of the information on your device by monitoring it without your permission, disrupt the integrity of information by allowing the attacker to impersonate the user and send text messages as them, and disrupt the availability of information by taking pictures or video from the target device.

However, it should also be emphasized that spyware is an even greater threat to victims of domestic violence, abuse, or

The National Network to End Domestic Violence conducted a poll that found that 54 percent of US domestic violence victims were being monitored and tracked by their abusers using spyware. That means on average, one out of every two domestic abuse cases in America today is supported by some form of

Beyond domestic and family violence, spyware is also a threat to general privacy. Deploying spyware against an individual without

their knowledge is a clear violation of their human right to privacy. With the extent that spyware can be abused for malicious purposes, it can be questioned why spyware is so easily accessible to consumers.

How is it still legal?

Well, firstly, it's highly profitable. Secondly, not everything used for illegal purposes is itself illegal. As we've seen, spyware is only as dangerous as the operator makes it. Third, not everything that is bad is illegal or even well regulated.

A great example of this is Tor browser, which we discussed earlier in Chapter 5. Tor can be used to carry out criminal activities. However, people also use it to browse the internet anonymously without criminal intentions. There are also cases of Tor being used by whistleblowers who want to connect to the press without disclosing their The human using Tor makes Tor into a vector for illegal activities.

Should a product or service that has a high rate of misuse, abuse, or associated illegal activity be banned or highly regulated, although some people benefit from the product or service? I think society has agreed that the answer is currently no.

In addition to any ethical bindings there may be, government regulations surrounding technology typically lag far behind the rapid pace that technology advances at today.

In 2013, a UN Special Rapporteur suggested that the spyware industry "is virtually unregulated as States have failed to keep pace with technological and political

Academic researchers Burkhart and McCourt have also stated that "the commodity chain for hacking products and services has evaded comprehensive, or even substantial, regulation to

Government officials and industry leaders have been aware of the lack of regulation surrounding spyware products for several years. So, why is it still being ignored?

It's possibly because many instances of spyware usage go unreported, and therefore the number of complaints associated with spyware are drastically skewed.

Andrea Charron recounted an instance after a speech she gave about cyber-stalking and spyware at the Diana Initiative in Las Vegas, "What was so moving is that after the talk—we spent probably two hours in the hallway after a 30-minute talk—having conversations with people who had experienced something like this. People for whom the topic rang true and who had never heard it discussed in public before. And the more I have these conversations, and particularly after giving that talk on stage, I think whatever numbers are out there, it's something that is seriously underreported. And I hope the more we talk about it, the more we can define just how much of a problem it

Many victims feel no one will believe their story or their experience wasn't severe enough to report, so they aren't compelled to tell their story publicly or report it to authorities. The statistics on this issue do not reflect what is the reality for many people because they don't feel comfortable reporting their stories.

However, when there is a demand for a product, we know someone will supply it. Whether it is made available commercially or not, people will find a way.

It begs to question, why a society that holds the human right to privacy in such high esteem has a thriving enterprise built on violating the privacy of others. We claim to savor our own privacy, but at the same time, we're enticed by marketing campaigns that promise to show us who our boyfriend has been texting in the middle of the night.

We must be aware that if we accept this type of application being sold commercially, we must also accept the consequences.

228 US Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report* (Washington, DC, 2019).

229 Pattyl Vartanian, "99 Inspiring Cybersecurity Quotes," *Online Security* (blog), August 8, 2019.

230 "Essential Malware Protection Advice for Families," Kaspersky, March 30, 2020.

231 "What Is the Difference: Viruses, Worms, Trojans, and Bots?," Cisco, last modified June 14, 2018.

232 Ibid.

233 Ibid.

234 Ibid.

235 Ibid.

236 "New Malware Threats: Ransomworm Is Coming, Are You Ready?," *Sentinel One* (blog), *Sentinel* February 1, 2017.

237 US Federal Bureau of Investigation, Internet Crime Complaint Center, *2018 Internet Crime Report* (Washington, DC, 2018).

238 US Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report* (Washington, DC, 2019).

239 Ibid.

240 James Sanders, "Ransomware: A Cheat Sheet for Professionals," *Security* (blog), *Tech* October 22, 2018.

241 Stephanie Taylor, "DCH Hospitals Closed to New Patients after Ransomware Attack," *Tuscaloosa News,* October 1, 2019.

242 Ibid.

243 US Federal Bureau of Investigation, Internet Crime Complaint Center, *High-Impact Ransomware Attacks Threaten US Businesses and Organizations* (Washington, DC, October 2019).

244 Ibid.

245 Taylor, "DCH Hospitals Closed."

246 Ibid.

247 Staff, "Cyberattack Still Affecting DCH Hospitals," *Tuscaloosa News,* October 4, 2019.

248 Jessica Davis, "3 Alabama Hospitals Pay Hackers Ransom to Restore System," *Cybersecurity News* (blog), Health IT Security, October 7, 2019.

249 Jim Greene, *Salem Press Encyclopedia of* Academic ed., s.v. "Ransomware," accessed February 8, 2021.

250 Ibid.

251 Ibid.

252 Mozilla, "Story of a Ransomware Victim," *Internet Health Report* (blog), April 2018.

253 Ibid.

254 Ibid.

255 Ibid.

256 Ibid.

257 Ibid.

258 Ibid.

259 Ibid.

260 Ibid.

261 Ibid.

262 Ibid.

263 Ran Levi and Lodrina Cherne, "How is Spyware Legal?," October 2019, in *Malicious Life* produced by Cybereason, podcast, MP3 audio, 42:00.

264 Diarmaid Harkin and Adam Molnar, *The Consumer Spyware Industry an Australian-Based Analysis of the Threats of Consumer* Australian Communications Consumer Action Network: Sydney, August 2019.

265 Levi and Cherne, "How is Spyware Legal?"

266 The United States Department of Justice, "Ohio Computer Programmer Indicted for Infecting Thousands of Computers with Malicious Software and Gaining Access to Victims' Communications and Personal Information," press release no. 18-21, January 10, 2018, on the Department of Justice website.

267 Ibid.

268 Ibid.

269 Ibid.

270 Harkin and Molnar, *The Consumer Spyware Industry.*

271 Ibid.

272 Levi and Cherne, "How is Spyware Legal?."

273 Harkin and Molnar, *The Consumer Spyware Industry.*

274 "Mobile Fact Sheet," *Internet & Technology* (blog). *Pew* June 12, 2019.

275 Monica Anderson, "Many Smartphone Owners Don't Take Steps to Secure Their Devices," *FactTank* (blog), *Pew* March 15, 2017.

276 Harkin and Molnar, *The Consumer Spyware Industry.*

277 Ibid.

278 Ibid.

279 Ibid.

280 "FlexiSPY Unique iPhone Spy App—Reveals Secrets Others Cannot," FlexiSPY, accessed February 9, 2021.

281 Ibid.

282 Harkin and Molnar, *The Consumer Spyware Industry.*

283 Ibid.

284 Levi and Cherne, "How is Spyware Legal?."

285 Ibid.

286 Harkin and Molnar, *The Consumer Spyware Industry*

287 Patrick Burkart and Tom McCourt, *Why Hackers Win: Power and Disruption in the Network Society* (Oakland, California: University of California Press, 2019).

288 Levi and Cherne, "How is Spyware Legal?"

Chapter 8
So Social

Socialization. Love. Attention. These are needs we all have, and throughout history, we've gone about finding ways to fill these needs in a variety of different ways. Most recently, with the invention of social media we have found a new venue to supply these needs.

The Cybersecurity Body of Knowledge states, "The average person spends up to a quarter of their daily lives on social This statistic seems exaggerated at first glance, but when examined it isn't difficult to imagine. Social media is the source of our daily news, entertainment, and most of all, socialization.

Social media is an invaluable tool that has changed our lives in a million ways. However, social media is also "one of the major threats to personal and organizational security in decades" according to *The Cybersecurity Body of*

Social networks have grown beyond the days of Myspace where your profile was merely for fun. These platforms have evolved from a fun place to connect with friends to multibillion-dollar platforms that allow us to communicate with strangers from around the globe.

In our modern world, it seems that social media users have begun to forget that the other users they are socializing with are humans too.

What happens when the world is connected in such an intangible way?

You've Been Scammed

She just wanted to find happiness. That was all. It seemed so simple, yet her quest ultimately left both her heart and saving account

The woman, who we'll call "Jane," lives with her husband in Texas. She is in her 50s. She is a devout Christian, and she publicizes her faith openly on her Facebook

Over the past few years, she had been experiencing problems in her marriage. Jane said she found herself "in an emotionally abusive marriage, and things had not been good for probably at least ten

Then "Charlie" requested to be Jane's friend on Facebook. Charlie claimed they had a mutual friend. Jane, being the trusting person she is, took him at his

"I'm very active on Facebook," she said. "I thought it was

Charlie and Jane began to form a bond over the social platform. "He would read my wall; I would read his wall. We would post things; he would like things. Then it got to where we would share emails. We started sharing pictures," she

When Charlie made his way into Jane's life, it felt like faith had brought them together. Charlie and Jane's relationship appeared to be growing closer, and Jane felt that she was building a true connection with

"I was looking for happiness. I thought I could find that with

"I felt a real soul connection with him right away," Jane said. "We sang to each other. We prayed with each other. We'd talk about what happened at church on

So, when Charlie asked Jane to loan him $30,000, she agreed, thinking of it as a "statement of

"He was trying to finish up a job in California," she said, "and he needed some money to help finish the job. I thought about it long and hard. I prayed about it. I've always been a very giving person, and I figured if I had money...I could send him some [money]. And he promised to have it back within twenty-four to forty-eight hours. I thought, *I could do*

Jane wired Charlie $30,000. He said he would pay back within a couple of days, but the days ticked by and she didn't get her money

“I still thought everything was okay, just that he was the victim of some bad luck,” she

Now, Charlie told Jane he needed another $30,000, but he promised he would pay her back. He never

Charlie continued to tell Jane stories of his misfortune. “One thing kept happening after another. He’d need more money because he was coming in over budget. Things didn’t get done on time. He needed a lawyer. He had to take a money loan, and it needed to be paid back,” she said as she recalled some of the

To a lovestruck Jane, his stories made all the sense in the world. She continued to fund his every need because she cared about him and believed that he would repay one

Over the next two years, the loans kept accumulating until Jane had given Charlie over two million

Although her estranged husband had yet to notice the missing funds, Jane’s financial advisor became concerned about how quickly her once substantial savings accounts were deteriorating. He suspected she was a victim of fraud and urged her to contact the FBI

When Jane reported her case to the FBI, they confirmed her financial advisor’s suspicions. This wasn’t their first encounter with a case like Jane’s. She’d been a victim of a romance scam.

Romance scams typically target older, widowed, or divorced women who are active on social media where they post details about themselves that make it easier for criminals to manipulate their

FBI Special Agent Christine Beining is a veteran financial fraud investigator in the FBI's Houston Division, and she said, "The Internet makes this type of crime easy because you can pretend to be anybody you want to be. You can be anywhere in the world and victimize people." Agent Beining highlighted, "The perpetrators will reach out to a lot of people on various networking sites to find somebody who may be a good target. Then they use what the victims have on their profile pages and try to work those relationships and see which ones

According to the IC3, a romance scam, also known as confidence fraud, begins when "a perpetrator deceives a victim into believing the perpetrator and the victim have a trust This can be achieved by building a friendship, convincing the victim the perpetrator is a family member, or like in Jane's case sparking a romance.

After the perpetrator gains the trust of the victim, they immediately use that trust to convince the victim to send money, personally identifiable information, launder money for the perpetrator, or give them something else of

When compared to other cybercrimes, romance scams have consistently resulted in the greatest financial losses to In 2019, IC3 reported that confidence fraud and romance scams cost victims over $475 million. Only 19,473 victims are included in this

statistic, since the FBI estimates that only around 15 percent of romance scam victims report their crime or losses to the

That's quite a high price for love.

The investigation led by Special Agent Beining led to the arrest and conviction of two Nigerian men for their role in the crime. The two men came to the US posing as South African diplomats to collect money from Jane on Charlie's behalf. In July 2016, the men pleaded guilty to their charges and were sentenced to three years in

Charlie, however, has never been identified. Authorities assume he is in Nigeria, but there is little chance he will ever be brought to justice, and a high likelihood he is currently victimizing someone

"This is a very difficult crime to prove," Beining said. "When someone is using a computer to hide behind, the hardest thing to find out is who they are. We can find out where in the world their computer is being used. It's identifying who they actually are that's the hard part. That is why this individual remains a

This is also the reason that romance scams are so popular. It's a low risk, high reward crime. There's a very low barrier to entry: All you need is a computer, an Internet connection, and a social media or dating account to get started. No technical knowledge is required.

"It's not like going in a bank and holding a gun to the teller," Beining explained, "because there are so many leads that you provide law enforcement when you do that. Even if you are able to get out of the bank, we can probably find out who you are and track you down. But with an Internet crime like this, it's much more

Unfortunately, Jane was unable to get her money back. The two million dollars she lost to Charlie was her entire life's savings. She felt that the financial hurt she felt was not as painful as it was for her emotionally, however. "The loss of money was my future and knowing that I wouldn't have to work, that I could just make it to the ripe old age of whatever and be perfectly comfortable. The loss that I've suffered emotionally I think has even been more traumatic," she

The psychological and emotional toll that romance fraud takes on its victims is intense and very real. Some people find it hard to believe that you can fall in love with someone you've never met before if they've never done it themselves. Jane said that she never saw Charlie's face, and probably never will. Yet she felt a deep connection and love toward him, without meeting him, touching him, or even being able to put a face or voice to his name.

Psychologist Monica Whitty, author of *Truth, Lies and Trust on the* explained that cyber-based relationships can be "hyper personal"—stronger and more intimate than physical relationships. When we form bonds with people through online interactions, we are often

able to idealize the other person. Each party can craft the perfect reply and edit away any red flags that would have slipped out in person. Then a cycle begins. “What happens is, you can see the written text and read it over and over again, and that makes it stronger,” wrote Whitty, chair in human factors in cybersecurity at the University of

It isn’t hard to imagine how you could quickly fall for someone after spending days rereading picture-perfect text messages from them expressing how much they care about you, especially if you are already in a vulnerable position.

The tone of voice, body language, and responsiveness of the speaker is removed when communicating solely through text messages or social media DMs. Since we can control our image in this way through virtual communication, we are often able to build trust and intimacy easier online than we do face-to-face.

Jane said she wanted to tell her story “because I don’t want this to happen to anybody else. I not only invested money in this man, but there is a big, huge piece of my heart that I invested in him.” She said she wanted to save other women the pain of “being embarrassed, being ashamed, being

If you think you’re immune to this type of attack, you should think again. “No one is immune to being scammed,” psychology professor Stephen Lea of the University of Exeter. “We need to be on our guard both for ourselves and for our friends and family. If you have any worries that something might be a scam...it very likely

Many people dismiss crimes like romance scams because they lack an "ideal victim." In these cases, the victim and perpetrator have willingly communicated with each other, the victims have willingly taken action to give the perpetrator their money or personal information, and often even after they have discovered they have been defrauded, the victim still feels a connection to the perpetrator.

For these reasons Dr. Cassandra Cross, who has studied the impact on romance scam victims wrote, this is a "unique" kind of fraud. She said, "Victims of fraud are seen to actively violate the notion of an ideal victim and hence, are typically understood as blameworthy and culpable for their own victimization." Cross added, "Do not confuse the word 'typically' in the last sentence with

In Jane's case, from the way she speaks about her experience you can tell that she still hasn't accepted that Charlie was the culprit. "Even though she knows Charlie doesn't [really] exist, there are times when she thinks the two men we arrested acted alone," Beining Unfortunately, in some cases, the connection that is built is so strong the victim cannot accept that the person they talked to every day, loved, and idealized conned them.

"I can't think of him that way," Jane said. "There can't be a man in this world that could be this horrible to have purposefully done what he's done to

Jane has contemplated suicide since Charlie defrauded her, according to

True stories like Jane's remind us that cyberthreats have no borders in their impact. They can affect us mentally, emotionally, and financially, and we may not even realize that we are falling victim to a cybercrime if we are not cyberaware. This is why it is important to understand the mental aspects of cybersecurity and know what signs to look for to perceive a threat.

Gone Phishing

Throughout this book, we've discussed that cybersecurity is not a purely technical subject.

"Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems, or data," wrote Josh Fruhlinger, writer for

Social engineering is the perfect example of how an understanding of psychology, communication, and criminology are arguably as important as technical ability within cybersecurity.

Social engineering is any man's game. So, it's no surprise that social engineering has become so popular. Phishing was the most frequently reported cybercrime to the IC3 in 2019 with 114,702 victims reporting phishing, vishing, smishing, or pharming attacks accumulating to a total loss of

Phishing is a type of social engineering scam that typically tricks you into clicking a malicious link, opening an attachment, or

disclosing personal information under the guise that the message is from a legitimate sender. Phishing messages often look like they've come from a sender you recognize and trusts, such as your bank, a popular brand, or even your mother.

"For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password," Josh Fruhlinger

The barrier to entry is low since this type of attack involves using social skills to achieve the attacker's goal. Phishing can be used to get the victim to send the perpetrator money or personal information like their social security number or a password to their account.

Phishing scams have also become popular on social media. Social media is the perfect platform for this type of attack because users are likely to click on a link to an article with a click-bait title without giving it a second thought.

However, as writer for Tech Cocktail Rick Delgado said, "Social engineering scams are a particular concern. With these scams, attackers present a post intended to get the target user to click on a link. That link usually leads to the user downloading some malicious code that has the potential to steal information on the user's computer or mobile device. These scams are sometimes also called phishing and baiting, as well as click-jacking." Delgado continued, "Whatever they're called, just know that not every post

on social media is safe to click on. You should take special care to treat every link with suspicion, especially those that look like

Smishing is a phishing scam that uses SMS messages, commonly known as text messages, as a form of

Vishing is when phishing is combined with voice communication, most often via a phone call. This technique can be used in a few different ways and combined with other social engineering techniques to get a victim to disclose their personal information.

For example, you may receive a call from a number that starts with your local area code. Although you don't have the number saved, you answer the phone because it may be someone you know calling from a new number. The caller says, "Your social security was involved in a crime, and the DEA has issued a warrant for your arrest. In order to stop this action, please give me your social security number...."

Now I know reading that it seems crazy to think that anyone would give these scammers their SSN over the phone, but this was a real scam that was going on in 2020, and some people felt pressured to give up their personal information when confronted in the moment with a scary situation.

If you're wondering how scammers acquire so many different phone numbers, they use Voice over Internet Protocol (VoIP) solutions. With VoIP, the scammer can change the caller ID to match the identity they want to

For this reason, you should not trust that just because the caller ID matches the number of a legitimate organization such as your bank, the Social Security Administration, or a business that the call is coming from them.

Similarly, spoofing is when scammers duplicate a legitimate website and lure victims to the website by using familiar logos and a similar or nearly identical website address. This is done to get the victim to submit personal information on the website, thinking that the website is legitimate, when it is not. Victims are often lured to the fake site via a phishing message. Attackers may also use web address shortening services like bit.ly to avoid detection by spam and malware

If you receive a message that claims to be from a reputable company and includes a link to their website, type in the web address of the company directly into your web browser to visit the site.

Another way to detect if the link is legitimate is to scroll over (not click!) the link to the web address that the link goes to will appear in the bottom left corner. Be careful with this technique, because as we learned before, attackers can use web addresses that are nearly identical to those of the company they are impersonating. Look out for misspellings or added symbols in the web address.

A basic rule of thumb to go by to avoid falling for phishing attempts is to never open a link or attachment in a message that you did not plan to receive. If you do not know who the sender is, don't open the message. If the sender is impersonating someone you know or a business you trust, give that person a call directly or send them a text asking them if they messaged you. If they didn't, you can report the message as spam and delete it from your inbox.

Do not give anyone any personal information (your Social Security number, password, birth date, etc.) over the phone, text message, or email. Reputable companies and organizations will never ask for personal information from you, especially not over insecure forms of communication like email. Do not give anyone calling and claiming to be a bank or the Social Security Administration your information; you can hang up and call them directly so you can be sure you are not talking to an impersonator.

There's Harm in Oversharing

"It's critical that people know and understand the risks they face when they put themselves out there on social media."

Cybersecurity Body of

Mark Zuckerberg infamously stated that he no longer considered privacy to be a social norm. Perhaps he was preparing the 2.8 billion active monthly users of Facebook for what was to

Around 270,000 Facebook users were paid to take a quiz called "thisisyourdigitallife." The first step for those filling out the questionnaire was to grant access to their Facebook

It was presented to users as a simple, fun quiz. Quizzes are very popular on Facebook and other sites like Buzzfeed where the user answers questions about themselves, and at the end, the quiz guesses something about them, from what Harry Potter character they are to what their favorite color is.

This quiz was different, however, as it led users to a lengthy psychology questionnaire hosted by Qualtrics, a company that manages online surveys. The questionnaire was created by a British company by the name of Cambridge Analytica, which specialized in data

After the users filled out the questionnaire, an app then harvested their data and their friend's data as well. The company employed cookies to track users' every move around the web. The information obtained from the cookies included every website visited, every search term typed, and every video the users [341]

This led to a massive collection of data. The data was then used to help understand their emotions and gauge their true feelings surrounding the 2016 US election. Then, Facebook political campaigns and advertisements were targeted to them based on their data to manipulate their feelings toward certain [343]

Christopher Wylie, a Cambridge Analytica employee, admitted in an interview with *Business Insider* to the company's exploitation and revealed the full extent of the scheme to the media, "We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner

This exploitation of user data shows a blatant lack of care for privacy of Facebook users; however, this is far from the only instance in which this has happened. The Better Business Bureau (BBB) has issued a scam alert addressing the hidden dangers of Facebook quizzes.

The BBB wrote on their official website, "These quizzes ask seemingly silly or meaningless questions, but scammers can use that information for nefarious

These quizzes get your information by asking you questions like, "What street did you grow up on?" or "What was the name of your childhood best friend?" or "What's your mother's maiden name?" All of these are common security questions for important accounts such as your bank account or credit card. By sharing this information with an unknown source, you put yourself at risk of being a victim of a cybercrime and having your personal or financial information

You should take a cautious approach to taking online quizzes, but not all social media quizzes are a scam to collect your personal information. If you don't know and trust the brand who created the quiz, don't take it. If any of the questions sound suspicious

or require you to disclose personal information, don't answer them.

When navigating social media, it is easy to fall into the trap of oversharing. After all, social media is the place where everyone comes to celebrate milestones and major life moments. However, these major life moments are often filled with personal information that can tell a potential attacker everything they need to know about your life. From birthdays to getting a new pet to pictures of family members, you're curating a portfolio of your life, and if your profile is public, anyone in the world can access it.

If you are concerned about your privacy (and if you've made it this far, I assume you are), you should set your privacy controls on your social media accounts where only friends or followers can see your personal information. How to do this varies by social media platform, but generally, you can change these settings by going into your profile settings and changing your profile from public to private.

In general, it's best to avoid sharing your birthday, your place of birth, the schools you've attended, the car you drive, and names of your family members or pets publicly on social media. These details about your life are enough for most attackers to break into your accounts or apply for credit card accounts using your

289 Daniel Shoemaker, Anne Kohnke and Ken Sigler, *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in Cybersecurity* (New York: CRC Press, 2020), 417-418, EBSCOhost.

290 Ibid.

291 “Romance Scams,” fbi.gov, February 13, 2017.

292 Ibid.

293 Ibid.

294 Ibid.

295 Ibid.

296 Ibid.

297 Ibid.

298 Ibid.

299 Ibid.

300 Ibid.

301 Ibid.

302 Ibid.

303_Ibid.

304_Ibid.

305_Ibid.

306_Ibid.

307_Ibid.

308_Ibid.

309_Ibid.

310_Ibid.

311_US Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report* (Washington, DC, 2019).

312_Ibid.

313_"Romance Scams," fbi.gov.

314_US Federal Bureau of Investigation, *2019 Internet Crime Report.*

315_Ann Brenoff, "How a Billion-Dollar Internet Scam Is Breaking Hearts and Bank Accounts," *Life* (blog), updated July 27, 2017.

316 "Romance Scams," fbi.gov.

317 Ibid.

318 Ibid.

319 Ibid.

320 Ibid.

321 Brenoff, "How a Billion-Dollar Internet Scam."

322 "Monica Whitty," The Conversation, accessed February 24, 2021.

323 "Romance Scams," fbi.gov.

324 Brenoff, "How a Billion-Dollar Internet Scam."

325 Ibid.

326 Ibid.

327 "Romance Scams," fbi.gov.

328 Brenoff, "How a Billion-Dollar Internet Scam."

329 Josh Fruhlinger, "Social Engineering Explained: How Criminals Exploit Human Behavior," *Social Engineering* (blog), September 25, 2019.

330 US Federal Bureau of Investigation, *2019 Internet Crime*

331 Fruhlinger, "Social Engineering Explained."

332 Nate Lord, "101 Data Security Tips: Quotes from Experts on Breaches, Policy, News & More," *DataInsider* (blog), *Digital* updated August 5, 2020.

333 "Avoiding Social Engineering and Phishing Attacks," cisa.gov, last modified August 25, 2020.

334 Ibid.

335 Lord, "101 Data Security Tips."

336 Shoemaker, Kohnke and Sigler, *The Cybersecurity Body of Knowledge.*

337 Monica Anderson, "Fast Facts on Americans' Views about Social Media as Facebook Faces Legal Challenge," *FacTank* (blog), *Pew Research* December 10, 2020.

338 Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," *The New York Times,* April 4,

2018.

339 Ibid.

340 "Facebook Pays $643,000 Fine for Role in Cambridge Analytica Scandal," NPR.org, October 30, 2019.

341 Confessore, "Cambridge Analytica."

342 Confessore, "Cambridge Analytica."

343 "Facebook Pays," NPR.org.

344 Alexandra Ma and Ben Gilbert, "Facebook Understood How Dangerous the Trump-Linked Data Firm Cambridge Analytica Could Be Much Earlier Than It Previously Said. Here's Everything That's Happened up until Now," *Tech* (blog), *Business* March 19, 2018.

345 "BBB Scam Alert: Bored at Home? Think Twice before Taking That Facebook Quiz," Better Business Bureau, last modified on April 10, 2020.

346 Ibid.

347 Serena Dorf, "7 Ways Social Media Sabotages Your Cybersecurity," *Cybersecurity* (blog), accessed February 24, 2021.

Chapter 9
The Privacy Paradox

Privacy.

You might ask if there is such a thing as "privacy" data in the age of Internet of Things devices and machine learning. Well, I can tell you there still is. In that case, you're probably thinking, *Why should consumers care about their personal data, now?* Well, new privacy data is being generated every day, so you should protect yourself.

I asked Sam Curry, chief security officer of Cybereason what his opinion was on the matter. "I was on a panel once with someone who said, 'Well, you already lost all the privacy data. It's over.' No. New privacy data is being created all the time," he said.

Privacy data is more valuable than ever before. Data has been compared to being the new oil, and there's no wonder why given how much of society is becoming data driven. From machine learning to highly targeted advertisements, everything is fueled by our data input.

Despite the fact that our current world is driven by the constant production of data, there hasn't been an effort in our society to establish a framework or universal understanding of the value of

our data, how that data is being used, and when and why it is being collected.

Sam Curry described this lack of a universal understanding surrounding privacy data: “I don’t believe it’s been established, a. that it has value and b. that it belongs to you. There’s neither jurisprudence like a law or ethical frameworks that are applied or technical models that make sense to people to describe that.”

We can no longer escape the conversation of personal cyber privacy because the practice of data collection is ubiquitous and woven into our daily lives.

Can privacy and hyperconnectivity coexist? Well, that depends. What is your definition of privacy?

Traditionally, we think of privacy as being free of prying eyes or snooping ears. We think of locked doors on homes, enclosed fences on properties, and blinds on your windows. You’re keeping yourself and your property private from your neighbors, safe and secure.

There are obvious cultural and generational differences when it comes to physical privacy and how strict our boundaries are concerning it, and generally, especially in the western world, we have come to expect physical privacy as a basic human right. Why then have we not created firm, clear, easy-to-understand boundaries surrounding our digital privacy as well?

Also, while the terms are often used interchangeably, cyber privacy, anonymity, and security have different meanings and imply different intentions.

Digital Privacy Terms Compared

Compared

Compared Compared
Compared Compared Compared Compared Compared Compared Compared Compared

It's a Paradox

The privacy paradox is a theory that describes the discrepancy between an individual's actual privacy practices and their described privacy preferences. It explains the relationship between an individual's intentions to disclose personal information and their actual personal information disclosure behaviors, which often differ

I first learned about the privacy paradox while doing research for an essay. The theory fascinated me for a variety of reasons. It combined the concepts of psychology, sociology, and technology to explain the evolution of human behavior that we see exhibited in cyberspace.

I wanted to know why people often made the trade of personal privacy for accessibility, functionality, or convenience. I realized that this concept is prevalent even in my own life.

I remember one holiday season; I was shopping at the outdoor mall with my sister. It was a breezy day in a suburb of Memphis, Tennessee.

As we walked past the Macy's, I said, "Oh, let's go in here. I haven't been to Macy's in forever."

By the time we made it to the checkout line, we had amassed a collection of clothing, accessories, and other miscellaneous items we could give to friends and family as Christmas gifts.

"Mission accomplished," my sister said as we headed to the checkout line.

It was a fairly busy day at the mall, so we waited until it was our turn to checkout.

"Next," said the cashier at the clothing register.

I approached the register with my items, and she began ringing me up as we made small talk.

"Ooh, that's a really cute dress," she said as she scanned the merchandise. "I love that shade of pink."

"Thank you!" I exclaimed, as I looked closely at the prices ring up on the tiny monitor as she continued to scan. *I really got a lot of stuff didn't* I thought to myself.

"Your total is $256.23. Would you like to sign up for our rewards card? We have a special offer going where you save 10 percent if you sign up today!"

"Well, sure."

"Great! I just need your name, phone number, and email address, and I can get you signed right up."

Just that easily, I had given my name, phone number, and email address away for a rewards card, at a store I don't even frequent. You're probably wondering, *How does this tie back into cyber privacy? This was an interaction at a physical* Well, these same techniques are used online, and the decisions that we make online are even more rash and uninformed than the ones we make in person.

Even though before entering the store I knew my privacy preferences, during that brief exchange I felt pressured, by peer pressure, the offer of a discount, the time constraint of others waiting in line, and me wanting to leave the store. On your favorite online store, a pop-up offering a discount if you sign up

with your email will often be the first thing that you see on the landing page.

The disclosure of your personal information typically comes with an immediate benefit—access, social engagement, or convenience of some kind.

“There’s always going to be some give and take, between functionality and security,” security consultant and instructor Chris Silvers said in an interview with me.

However, the risks that accompany the disclosure of personal information are often not discovered until much later. When thinking about the immediate benefits, we don’t think about the long-term risks that could be associated with the action of disclosing the information. For this reason, we tend to overvalue the short-term benefits of disclosure while greatly discounting any risks that might be incurred in the future. This is a cognitive bias known as hyperbolic

When examining the Privacy Paradox, most researchers believe one of two theories. Humans are always rational thinkers who perform a cost-benefit analysis prior to determining the price they are willing to pay to give away their data, or humans are inconsistent and largely inaccurate when determining the price of their personal data due to Based on recent research studies, it seems that the latter is the more accurate assessment of human behavior.

In research studies, people have been willing to give up their entire browsing history for the value of a Big Mac meal. In similar studies, people have been willing to give away their password for the cost of a chocolate

In everyday life, people are willing to give away their entire shopping history at a specific store in return for rewards, discounts, and bonuses—usually in the form of a rewards However, we have become so comfortable with this exchange that it feels natural, and the customer feels like they are making an even exchange (if they even realize they are making an exchange at all.)

From this perspective, it seems like people place very little value on their privacy. However, that is exactly why it is a paradox because although people think they protect their privacy, in reality, they are quite lax about it.

People are more likely to reveal their personal information if they see that other people are doing the same. It is believed that if most others reveal their information, then it is safe for me to disclose it as This is labeled the "bandwagon heuristic" and can explain why consumers make certain seemingly irrational decisions regarding their data. It is almost a domino effect, once someone sees another person disclosing their data for a nominal reward or discount, they believe that the behavior is safe, or they should participate out of the fear of missing

Going forward, the Privacy Paradox, and the biases associated with it, are such important theoretical constructs for framing future debates about data privacy protection. For one, the Privacy Paradox raises questions about the types of biases and inconsistencies that tend to cloud people's perceptions of privacy. It also helps stimulate debate about the moral and ethical ramifications of privacy regulation. If future regulators do not take into account morality and ethics when crafting new data protection laws, they would be going about it all wrong, and in so doing, fail to protect the very people they hope to

While it's virtually impossible to live in today's world and never disclose your personal information to any companies, service providers, or government institutions, knowing and acknowledging that the privacy paradox exists can make you more cognizant of your decisions when it comes to your own cyber privacy.

So, the next time you are faced with the decision of whether or not to disclose your personal information to a company or website, you can remind yourself of your personal privacy preferences first, and remember the cognitive biases that might be affecting your decision making.

Your Digital Footprint

"Privacy is not actually about keeping things private. Privacy is about choice. The choice of what we tell other people about ourselves."

Allan, Artificial Intelligence

Denelle Dixon is the former chief operating officer of Mozilla Foundation, the creators of Firefox, a free and open-source web browser. She ascended to the C-Suite of the company after occupying several legal roles including chief business and legal officer and associate general counsel. Dixon currently serves as the chief executive officer of Stellar Development Foundation, a fintech company dedicated to making financial institutions more

This is simply a very brief overview of Denelle's most recent accomplishments, and given Dixon's background in technology, you would think she'd be one of the last people to struggle with controlling her digital footprint. Nevertheless, the TEDx Talk she gave in October 2017 centered around this loss of

Her sense that she was losing control of her digital identity began in 2016 after she was invited to debate at the Oxford Union about cybersecurity. A recording of the debate was uploaded to YouTube, and the comments quickly came flooding

Her son saw the comment section and said, "Hey Mom, you should take a look at the comments," with an embarrassed look on his

The top comment read, "I'd fuck

The next one read, "Yeah, I'd fuck that,

A feminine-sounding alias interjected and said, "Hey, not cool. This is an articulate woman, and we should focus on the

argument," and then added, "but I'd fuck that

After her son showed her the comments, she was mortified. She'd worked so hard to be invited to this prestigious debate society, to then be torn down by internet trolls in the comment section. And now her family, friends, and colleagues would be able to see these public comments about her. Not because of her argument, but because of her

Dixon said, "It was then that I realized I can't control my online persona or how I want others to see me, because the trolls get to contribute to

Dixon considers herself a "pretty private person outside of work," a description that many people would claim to relate to. Even so, after hiring a professional to dive into her digital life with just her first and last name, they were able to compile a massive dossier about her

According to Dixon, they were able to dig up "my physical addresses for the last twenty-five years. My email addresses for the last twenty-five years, where I live, where I intend to live. What cars I drive. What cars I own. Hundreds of pages from my divorce and custody proceeding that contained highly personal information about me and my

The fact that Denelle Dixon's digital life could be hunted down so easily might come as no surprise to you. You might say to yourself, *She has high profile job; she's a relative celebrity. Of course,*

it's easy to track her private information down. However, studies suggest it's just as easy for someone to take your information and identify you just like they did

As we've learned in previous chapters, no one is immune from becoming a victim of a cybercrime. No matter your level of notoriety, you have a digital footprint. Everyone who uses the Internet does.

Dixon explained that "Everything that you do online leaves behind a breadcrumb. It's a piece of you. You might be sitting there saying, I don't care. I'm so boring. Nothing like this matters to me." She continued, "But what about your name. Your search for abortion, pregnancy, divorce...What about all those videos you watch? What about the private support groups for addiction, for cancer? Religion. It's so personal. And then, let's think about the information I can find out about you, offline. Where you work. Where you live. Where you go, and when you go there. The list goes on and

The list could truly go on and on because many of us have massive digital footprints that we don't ever think twice about. Think back to the new account you opened at a local store the other day. They were offering a discount to anyone who downloaded their app and signed up with their email address. You did it then and there at the checkout and created the new account using one of your trusted, easy to remember passwords.

When navigating cyberspace, we often minimize the ripple effects that our actions can have. Today, one viral social media post can

be life changing. For some people, these events have brought them fame and fortune, for others, they have gotten them fired from their jobs.

We also live in a world where we are no longer the only ones in charge of our personal narratives. In Dixon's case, commentators were able to weigh in on her appearance on a professional video, attempting to change her narrative from one of the accomplished professional women debating in a distinguished venue to just someone to look at. And, yes, we've all experienced this type of treatment in our lives, and while it's hurtful, it goes away.

However, on the Internet, nothing ever goes away. *The Cybersecurity Body of Knowledge* compared the Internet to the Wild West because "every online move you make leaves cyber footprints that are making yourself fodder for third-party research about you, without you ever realizing It's all cataloged, archived, and searchable, even once "deleted."

Dixon said in her TEDx Talk, "I imagine a world where we are in control of all of our personal information because, in the future, it's going to become harder and harder for us to disconnect our online and our offline

This is the reason why cybersecurity is so important for all of us to value and understand. We are surrounded by amazing technology, and the scope of that technology is only getting wider with the popularization of IoT devices, and the connectivity that we are bringing into our lives.

Ayana Miller, a privacy specialist who built and managed in-house privacy programs at Facebook, Snapchat, and Pinterest, told me in an interview, "I think a lot of people feel helpless right now. But what do you do? I think the biggest challenge is this sense of helplessness that now I know. I'm educated. I understand that there's risk with privacy. What am I supposed to do?" She continued, "We haven't figured out the tooling, the communication, the language, the legislation to kind of address how to handle the feeling of loss of control over data."

The future of our data privacy is in our hands as consumers of technology.

Dixon continued, "We need to demand that the products that we use that they actually hold up to the control standards that we want. We need to use our voices, there's strength in numbers. Call them, contact them through their websites, use social media. And if that doesn't work, stop using the products, vote with your loyalty, and show them your value. So, this is all in our

We must make the decision to take back control of our data, take control of our digital identities, and hold companies accountable when they mishandle our data or when their products don't live up to our expectations. We also must hold each other accountable by reporting bad behavior that we encounter on the web that could endanger our privacy or the privacy of someone else.

For now, until we have a solution to our data privacy woes, we must do our best to manage the risks associated with exposing our personal data.

Chris Silvers said to me in our interview, "So, I believe the key is really to look at it from a risk management standpoint. And, you know, develop your own personal risk tolerance and risk appetite. What are you willing to risk, and then make those educated decisions on your own...If you really want this particular feature or set of features, then you have to be willing to take that risk."

This means we must educate ourselves about the companies we are using products from and the features that these products have. Are all 300 apps on your phone really necessary or could you do without some of them? What permissions do those apps have access to that are not required for their functionality? Does the puzzle app actually need access to your location, camera, and microphone? You should ask yourself these questions before signing up for a new product or service or purchasing a device.

348 "The Privacy Paradox and How You Can Use It to Increase Conversion," KeepitUsable, accessed February 24, 2021.

349 Ari Waldman, "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'," *Current Opinion in Psychology* 31, (February 2020): 105-109.

350 Nicole Lindsey, "The Privacy Paradox Could Determine the Next Evolution of Privacy Regulation," *News* (blog), *CPO* November 30, 2018.

351 Ibid.

352 Ibid.

353 "A Privacy Paradox: Why Do People So Readily Give Up Information Online?" Technology Networks, April 27, 2020.

354 Ibid.

355 *TEDx* "The Coming Privacy Crisis on the Internet of Things | Alasdair Allan | TedxExeterSalon," November 28, 2017, video, 13:46.

356 *TEDx* "Online Privacy: It Doesn't Exist: Privacy and What We Can Do about It," October 18, 2017, video, 14:14.

357 Ibid.

358 Ibid.

359 Ibid.

360 Ibid.

361 Ibid.

362 Ibid.

363_Ibid.

364_Ibid.

365_Ibid.

366_Ibid.

367_Ibid.

368_Ibid.

369_Daniel Shoemaker, Anne Kohnke and Ken Sigler, *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in Cybersecurity* (New York: CRC Press, 2020), EBSCOhost.

370_*TEDx* "Online Privacy."

371_Ibid.

Chapter 10
The New Oil

"Convenience is the product. Data privacy is the cost."

—Lauren Bass, author of *The Concealed Cost of*

In December 2017, Kashmir Hill converted her small San Francisco apartment into a "smart home." She connected as many of her belongings as she could to the Internet, everything from the lights, to her toothbrush, and even her

"Our bed?" her husband asked, appalled at the thought of sleeping on a mattress connected to the Internet. "What can it tell

"Our breathing rate, heart rate, how often we toss and turn, and then it will give us a sleep report each morning," she

"Sounds creepy," he said, as he plopped onto the

However, Kashmir's husband isn't alone in thinking that the level of tracking that smart homes are capable of is creepy. We discussed this briefly in Chapter 1, but here's a refresher. Consumers International and the Internet Society conducted a survey including consumers from Australia, Canada, France, Japan, the UK, and the US. They asked the participants what they felt

mattered most when purchasing connected devices. The findings showed that 75 percent of people distrusted the way data was being shared. While 53 percent of people didn't believe that connected devices were capable of effectively protecting their

After Congress in March 2017 gave Internet Service Providers the right to monitor and sell their customers' Internet usage data, we were all warned that the ISPs could now sell our browsing activity or records of what we do on our computers and smartphones. But in fact, they have access to more than that. If you have any smart devices in your home—a TV that connects to the Internet, an Echo, a Bluetooth-connected scale—your ISP can see and sell information about that activity

Knowing when you turn on your lights or whether you do so with a switch or through a voice assistant might sound like pretty banal data to give up. But even anonymized data can be used with other troves of available information to figure out other personal details about you. The fear is not only that this information could fall into nefarious hands but that it might be sold or shared at

Consider an Amazon or Google smart speaker voice assistant. It knows where you're located, what you buy, as well as your taste in music and movies. It knows when you're at home, what your voice sounds like compared to, say, your roommate's—and, if you've paired it with other smart devices, some of what those devices are sensing. In short, it knows a lot about

“Whenever you make functionality decisions. There’s a security risk associated with it, and to ask that second question. What I mean by that is most people, whether it’s putting Alexa in their home, or doing Amazon home delivery. They ask a single question, which is, what is the benefit, what is the value, but they never ask that second question, which is, what is the exposure, what is the risk, what is the impact,” said security expert Dr. Eric Cole in an interview with me.

Internet of Things devices are expanding into nearly all facets of our lives, and as new technology emerges, we are often eager to try the “next big thing” without considering the risks that bringing that technology into your home might pose.

“I think the ease of technology just in general has really kind of made it where it’s almost too easy to implement technology,” Chris Silvers said when I asked him what people should be most aware of concerning IoT and home security. He continued, “And I think we have to be a little wary of that, to where when you bring some technology into your house. It’s really easy to just plug it in, turn it on and, you know, walk through whatever it tells you to do, and you know it’s really easy and set it up and then forget about it.”

In your home, you probably have at least one IoT device whether that’s an Amazon Echo, a Smart TV, or a Roomba. Amazon’s voice assistant Alexa is already integrated into more than 100,000 smart home products from over 9,500 brands. Over half of Americans own an Alexa-enabled device or another artificial intelligence (AI) enabled

The Roomba can compile a map of your home and figure out where it is within it. This can be a helpful utility if used correctly, however, in July 2017 iRobot announced they would be sharing those maps with their commercial partners, including Apple, Microsoft, and Google's parent company, Alphabet. No worries though, because you gave them permission to map your home's floor plan, store the data, and share it with tech giants when you clicked agree on their Terms of

Therefore, it's extremely important to purchase hardware (IoT devices, laptops, smart TVs) and download software from companies and websites that are reputable, and you know you can trust.

Choosing a device from a company with a reputation for taking privacy seriously, like Apple, is a safer bet than an unknown start-up company that hasn't proven itself in the market yet. While any company big or small can be the target of a cyber-attack, more established companies with a reputation to uphold typically hold themselves to a high standard and make sure that their products follow and sometimes exceed security and privacy regulations.

"When a security breach happens, a lot of the impacts are borne by device owners and wider society," as opposed to the device maker, Olshansky, internet technology program manager at the Internet Society, a nonprofit

This makes personal cybersecurity habits more important than ever as we integrate these technologies into our homes giving them access to not only our family's sensitive data but also in many cases, the ability to monitor their every movement.

You Are the Product

She is a twenty-six-year-old British Asian woman, and she has a career in media. She lives in Southwest London in a recently converted flat that she shares with a roommate. She previously lived in Suffolk, and prior to that, she stayed in Northeast London. As a child, she lived in a detached house with her family, and they went on vacation to India every year. Murgia does most of her shopping online, and she is

Her interests include movies and start-ups, and she has taken five vacations in the past year. She is about to purchase plane tickets within the next fourteen days. Her annual salary is between thirty and forty thousand British pounds a

She doesn't own a TV, but she does enjoy watching shows on Netflix. Last week, she passed through Ofton Street in North London on Monday and Wednesday evening at 7 p.m. She cooks a little, but she tends to eat out or get takeaways often. Her favorite cuisines are Thai and Mexican food. She doesn't own any furniture, and she doesn't have

Her name is Madhumita Murgia, and this list of characteristics, behaviors, and attitudes comes very close to defining her as a

person. However, this list wasn't written by Murgia. It wasn't even written by someone she knows. This is a snippet of the characteristics that personal data tracking companies, like Eyeota, had compiled about

According to their website, "Eyeota works with marketers, data owners, and research companies to provide distinct, comprehensive and qualified audience

Eyeota's primary source of consumer data is their third-party partners, ranging from Adobe to the credit rating agency Experian, who maintains the demographic and credit information on approximately 220 million [390] [391]

While she was working in journalism, Madhumita became curious about what these companies truly knew about us, and she began her journey to uncover the truth behind the multi-million-dollar industry.

"I decided to write about it for Wired Magazine. What I found out shocked me and reinforced my anxiety about a profit led system designed to log behaviors every time we interact with the connected world," Madhumita said. "I already knew about my daily records being collected by services such as Google Maps search, Facebook, or contact-less credit card transaction. But you combine that with public information, such as land registry council tax or voter records, along with my shopping habits and real-time health and location information and these benign data sets begin to reveal a lot," she

In some instances, large datasets can be used for useful reasons such as medical research or city planning, however, the majority of the data that is being collected by these companies are being purchased by advertisers or other third parties.

In 2020, businesses will likely spend $336 billion in digital advertising worldwide. The content and audience for digital advertisements for major corporations are determined almost entirely by data targeting and tracking.

Data is the new oil, and companies are mining it directly from you, the consumer. So, why shouldn't you be apathetic? Why should you care?

For starters, the data companies are profiting from your data, and if they are, you deserve a share of the profits; they generate from something that is yours.

"We shouldn't be doing that because there's people making a lot of money off, and you should be able to determine how it gets us in should have to give you," said Sam Curry, CSO at Cybereason in our interview.

"Data. We love it. And we also know just how important it is to keep it safe. These days we're plugged in anywhere and all the time. Sometimes, we may not even realize how plugged in we actually are while our apps, web searches, and credit card purchases are constantly storing our actions in the background."

—Katie Atkinson, Survey

"If you think you don't care about being unmasked, you may want to reconsider. Personalized browser ads may be harmless, but connecting disparate aspects of your life to predict your future behavior could lead to unexpected consequences. For instance, decisions on whether your child gets to go to a certain university," Madhumita

As organizations collect more data about you, how you live, and your medical conditions, you lose your right to free choice as those companies make decisions on your behalf without your

Ayana Miller, former privacy engineer at Facebook, Snapchat, and Pinterest, explained this concept further in an interview with Shine Hard Family: "A lot of people think of AI as this scary robot or something. That's not what it is." Miller continued, "It's your data being regurgitated combined with other people's data to give you more personalization and experiences, but it's based on an assumption. It's based on a formula so there's opportunity, an incentive not to ever delete any of your data because the more history it has, the more accurate the predictions are going to be. My biggest fears are that we will get to a place where there's predictions made about you already like, say, your credit

Companies and organizations are already beginning to use user data to make inferences about a user's future behavior. These inferences can go far beyond predictions about your location. The

data industry has become capable of using data to determine whether an individual will be a hard-working employee, a risky driver, a credit risk, or even a criminal. These predictions can be made based on metrics from social media, health data, location, or even your home energy

We've seen police departments in the US attempt to implement AI in the form of "predictive policing" with the aim to predict crimes before they happened. Using historical criminal data as a way to predict future crimes creates a bias against poor, minorities, and low-income communities according to the *MIT Tech* Concerns about these biases were brought forward, and the majority of these systems have been shut

I had a conversation with Ayana Miller about the future of machine learning, big data, and her hesitations about the technology.

Miller explained, "It's just the notion that you can derive intent from someone's message data, [or] you can derive intent from location. And like where you may go based on where you've gone in the past. All those things are based on inferences."

This is the basis of the privacy problem that exists when it comes to artificial intelligence and big data. Ostensibly, these data points are used to make your smart device experience better and more personalized. In the wrong hands, it's a treasure trove of personal

372 Lauren Bass, "The Concealed Cost of Convenience: Protecting Personal Data Privacy in the Age of Alexa," *Intellectual Property Law Commons* 30, no. 1 (2019).

373 Surya Mattu, and Kashmir Hill, "The House That Spied on Me," *Gizmodo,* February 7, 2018.

374 Ibid.

375 Ibid.

376 Ibid.

377 Consumers International and the Internet Society, "The Trust Opportunity: Exploring Consumers' Attitudes to the Internet of Things," accessed February 24, 2021.

378 Mattu and Hill, "The House."

379 Rani Molla, "People Say They Care about Privacy but They Continue to Buy Devices That Can Spy on Them," *Recode* (blog), May 13, 2019, 5:40pm EDT.

380 Ibid.

381 Rhett Jones, "Roomba's Next Big Step Is Selling Maps of Your Home to the Highest Bidder," *Privacy and Security* (blog), July 24, 2017.

382 Ibid.

383_Molla, “People Say They Care about Privacy.

384_TEDx Talks, “How Data Brokers Sold My Identity | Madhumita Murgia | Tedxexeter,” May 23, 2017. Video, 16:19.

385_Ibid.

386_Ibid.

387_Ibid.

388_“The Audience Technology Platform,” Eyeota, accessed on February 24, 2021.

389_TEDx Talks, “How Data Brokers.”

390_Ibid.

391_“The Audience Technology Platform,” Eyeota.

392_TEDx Talks, “How Data Brokers.”

393_Nate Lord, “101 Data Security Tips: Quotes from Experts on Breaches, Policy, News & More,” *DataInsider* (blog), *Digital* August 5, 2020.

394_TEDx Talks, “How Data Brokers.”

395 Ibid.

396 Brandon Alexander, "Protecting Your Privileged Information with Ayana Miller," *Shine Hard Family,* accessed February 24, 2021.

397 TEDx Talks, "How Data Brokers."

398 Yvette Hammett, "Predictive Policing Is Predictably Controversial," *The Legal* last modified September 16, 2020.

399 TEDx Talks, "How Data Brokers."

Part 3

What to Do to Protect Yourself

Chapter 11
The 3 Cs of Cyber Curiosity

Part Three of this book has been designed as a guide to be referenced repeatedly. Part Three is broken into three chapters. Chapter 11, this chapter, covers simple cybersafety tips that are valuable to everyone. Chapter 12 covers easy, safe password management and data storage solutions. Finally, Chapter 13 is dedicated to cybersecurity dangers and tips that are relevant to vulnerable groups including children, teens (and their parents), and the elderly.

The cyber curiosity mindset is made of three basic principles. The three Cs of Cyber Curiosity: cyberawareness, caution, and curiosity. In this chapter, we're going to dive into what these terms mean for how we approach cybersecurity in our lives.

Practicing Cyberawareness

"Security in IT is like locking your house or car—it doesn't stop the bad guys, but if it's good enough they may move on to an easier target."

—Paul Herbka, Security

Dr. Eric Cole told me in an interview, "The main thing they [the users] should be aware of is that the good news is that

cybersecurity is built into most products. Most technology, whether it's online banking or e-commerce, the operating system has security built-in." He continued, "They need to recognize that they need to turn it on. It's not turned on by default."

While most applications include security features, they will often be turned off by default. Building your cyberawareness is the most important part, and you have taken a huge step in that process by reading this book. Practicing cyberawareness in your everyday life and making Cyber Curiosity a lifestyle is the next step.

I recommend implementing only a few of the recommendations I mention into your life at a time. Removing a negative habit from your routine and replacing it with a positive one. Then, the next week, come back and pick another habit you want to add to your routine. It has been shown that making small changes to your routine gives a more lasting effect than trying to change everything at once. I like to compare it to starting a diet and telling yourself that you're going to cut out all junk food and have no cheat days, when your baseline is eating a bag of chips while watching Netflix every day after work.

It won't stick.

Building a positive cybersecurity routine is not just about forming new, healthy habits. It is also about breaking old, damaging habits. Breaking old habits is often the hardest part of making any lifestyle change, and cybersecurity is no different. While it may be difficult at first, it will get easier over time, and the peace of mind of knowing your information is secure is priceless.

You also need to set realistic expectations for yourself. No one is a perfect cyber citizen. I'm certainly not claiming to be, but I believe you don't have to be perfect to see results. Even if you only change one bad cyber habit today, you are taking more personal responsibility for your cybersecurity than you were yesterday. That is a step in the right direction.

Here are some more general habits to cultivate:

cultivate: cultivate:

cultivate: cultivate:

Balancing Caution and Curiosity

Caution is the second of the three basic Cyber Curiosity principles. Caution does not mean we should be afraid when using the Internet. Actually, practicing caution will make you safer and more confident as you enjoy cyberspace.

Caution means to stop and think before acting.

This is at the core of the practice of mindfulness. I know mindfulness sounds like something your yoga instructor would tell you to practice, not a cybersecurity consultant, but hear me out. Research done at the University of Virginia showed that mindfulness training was 38 percent more effective in preventing successful attacks than traditional anti-phishing

Ryan Wright, the C. Coleman McGehee Professor of Commerce in the University of Virginia's McIntire School of Commerce said, "Even the briefest pause alerts your instincts, leading to a better decision the majority of the time," Wright said. "We often use technology fairly mindlessly; if you pause and are more mindful for just a second, then you have already

So, whenever you're checking your emails or scrolling through your Facebook timeline, practice caution by taking a moment to stop and think before you take any action. Think before you click a link, open an attachment, or even make a post.

Yes, you should be mindful about what you post on social media because as we've discussed before, cyberattackers can use information from your social media accounts to craft a targeted attack against you.

Today's phishing scams are very targeted, unlike the days of mass messages. According to Wright, the average phishing scam today targets around nine people and uses information from their social media profiles to customize each message, posing as family members, friends, and These targeted attacks are more likely to be successful because they are disguised as a message from someone you trust.

Curiosity is the third piece of the Cyber Curiosity mindset. It ties into practicing caution because when you stop and think, you should use your curiosity to ask yourself questions about the situation or message in order to make the best judgment.

Always ask questions.

Some questions that you could ask yourself or the sender include:

include: include: include: include: include: include: include: include: include: include: include: include: include: include: include: include:

include: include:

In all of the above questions, “person” can be substituted with “organization” or “business.” It is not necessary that you ask yourself all of these questions, or even some of them, each time you read an email. However, this gives you an idea of where to begin when thinking about phishing messages.

If after practicing caution and curiosity, you’re still unsure if the message is safe or not, ask someone else for their opinion. If you’re at work, ask someone from the IT Department to take a look at the email with you.

However, if you decide to ask someone for help, don’t forward the suspicious message to the person you want to ask. If the message does contain a malicious attachment or software, you don’t want to spread the malicious message to someone else. If it doesn’t feel right and you can’t verify the sender, it is best to delete the message.

Most reputable organizations, such as banks, universities, companies, etc., won’t ask for any personal information via email or text message. However, if an email seems to be from a reputable company like your bank or a retailer, but you are not sure if the email is legitimate or they are asking for personal information, you can contact them directly and verify that they were the senders of the email. If they indeed need your personal

information, you can provide it to them directly after you have called them.

Other Signs of a Phishing Scam:

•Seemingly reputable organization asking for personal information via email.
•Offer of a "free" gift, prize, or vacation.
•Requests to update or confirm your personal information or password.
•Unexpected email that appears to be from someone you know.
•Poor grammar, misspelled words, and inconsistent formatting.

We've discussed how devastating falling victim to a phishing scam can be for both individuals and companies. From the infamous Target breach to DCH Hospitals, we've seen how one click can leave corporations and communities in distress. Practicing caution and curiosity in your daily life from work to home significantly reduces the risk that you will fall victim to a phishing attack that can put your family's financial future in danger.

Protect Your Privacy

Vet everyone you meet online before you meet them in person. Make sure they are who they claim to be. If they claim to work for a particular company or attend a certain school, do your due diligence and check to see if their stories match with the results of their web search.

Cyberspace is forever. You might "delete" that picture from your phone but the digital forensic evidence of it will exist forever. Taking risky pictures of yourself that you wouldn't be comfortable getting leaked on your smartphone isn't wise as you never know what could happen if they fall into the wrong hands. I'd recommend if you want to take explicit pictures, to get a cheap polaroid camera that isn't connected to any of your IoT devices that you can use to print your own pictures (only if you're over eighteen years old, of course).

A Virtual Private Network or VPN is great for your online privacy and security. Like we talked about in Chapter 5, a VPN can disguise your computer's IP address. This isn't just useful for people trying to hide their cybercrimes from law enforcement. A VPN can help protect you if you have to connect to untrustworthy public Wi-Fi hotspots.

Recently, VPNs have seen a rise in popularity because of their ability to give users access to online content from different countries that might not be available to the user. For example, a US user can connect to a VPN and change their location to Canada to access the Canadian version of Netflix or Hulu which has different

Tips for Protecting Your Online Privacy:

•Delete your cookies on a regular basis.

•Avoid applications that are known to not store your data safely and securely.
•Use a VPN to protect your privacy.

•Use DuckDuckGo.com To Protect Your Privacy While Searching Online.
•Set your phone to not show a preview of your text messages on the lock screen.

Shop Safely

Online shopping has become the norm for many people nowadays. While we love this convenient pastime, we know that it comes with its risks. However, there are ways to mitigate those risks if you implement some simple tips from these experts.

When using online banking services, check to be sure the sites you use are secure. One quick clue to determine whether a website is safe is if the URL begins with "https://." The "S" in https stands for secure. Sites that only have http are not secure which means the information transferred is not encrypted, and you should not input any personal information into that website. Look for the padlock icon next to the URL in your browser which means the website uses encryption.

Some attackers may create a malicious website that looks like a legitimate website to trick customers, according to The Cybersecurity and Infrastructure Security Agency. If this is your first time hearing of the site, double check and do some research prior to

The Better Business Bureau (BBB) is a good place to start when looking for business reviews, and you can usually find individual

experiences online as well. If you type the business name into the search engine and the first suggestion is “scam” you shouldn’t trust them with your personal information.

Instead of clicking on links in emails or copying and pasting, type the URL directly into the address bar. When using a public computer—such as one at your local library—avoid typing your personal

It isn’t recommended for you to use a debit card when shopping because if someone steals your debit card information, the money comes out of your account immediately, like in my personal cybercrime story. This can leave you without that money for weeks or months until the bank sorts your situation out.

That’s why fraud expert and ex-con artist, Frank Abagnale, stated in an interview with “Want to avoid identity theft? Never, ever use a debit card.” Abagnale continued, “I don’t own one. I never have and I never will. I don’t recommend them to anyone—not my family, not my friends, not

What does Abagnale suggest you use instead? “Instead, use a credit card,” he

Abagnale also commented on the protections that credit cards offer the consumer, “With credit cards, federal law limits my liability if there’s an unauthorized use of my card. When I use a credit card, I’m spending the credit card company’s money every day until I pay my bill at the end of the month. Meanwhile, my money is earning interest in a bank

While your credit card company has some protections that your bank doesn't, like the ability to question any unusual charges, you should still check your credit card statements regularly for any fraudulent charges so you can report them immediately.

It is a good idea to keep track of your receipts, in either digital or physical form, for this purpose. If you make frequent purchases, you likely won't remember the exact amount that you spent on UberEats last week or at H&M last month. So, it is best to keep receipts, so you'll know if anything is out of place.

If you must use a debit card online, use a service such as PayPal. PayPal acts as the middleman between your card and the merchant. PayPal hides your card's information from the merchant, making your transaction safer and often easier. PayPal also offers easier charge disputes than most banks, and they often side with the customer in the event of a complaint.

If you notice any fraudulent charges made to your account, notify your bank or financial institution and local law enforcement immediately.

Sign up to get text message alerts whenever a purchase is made on your credit card or debit card. This way, you will know immediately if any fraudulent charges are made using your card.

Avoiding Malware

Mike Danseglio, program manager in the security solutions group at Microsoft said, “We’ve seen the self-healing malware that actually detects that you’re trying to get rid of it. You remove it, and the next time you look in that directory, it’s sitting there. It can simply reinstall

Sometimes it is very difficult or impossible to get rid of malware on your device. Therefore, preventing malware from getting on your device is the best way to protect yourself.

Ways to Prevent Malware from Getting on Your Device:

Device: Device:

Device: Device:

What to Do If You Detect Malware:

•Stop all online activities that involve usernames, passwords, or other personally identifiable information, especially banking and shopping.
•Update your antivirus software and scan your computer for malware. If any is detected, delete it immediately.

* * *

Now that you are armed with the tools to defend yourself against cyberattackers, go put your new skills to good use. Go have a conversation about cyberawareness with your co-worker. Get into the habit of practicing the three Cs. Find an antivirus software and VPN you love. Have fun with your Cyber Curiosity journey, and you'll know you and your family are safer because of it.

400 "Security Quotes," Native Intelligence, accessed March 5, 2021.

401 Caroline Newman, "How Mindfulness Can Help Prevent Hacks, and Four More Cybersecurity Tips," *The University of Virginia* August 28, 2018.

402 Ibid.

403 Ibid.

404 Chris Hoffman, "What Is a VPN, and Why Would I Need One?" last modified October 15, 2020.

405 "Holiday Online Shopping," cisa.gov, accessed March 5, 2021.

406 Ibid.

407 Frank Abagale, "'Never, Ever Use a Debit Card,' Warns Fraud Expert and Ex-con Artist—Here's What to Do Instead," *Make It* (blog), last modified August 30, 2019.

408 Ibid.

409 Ibid.

410 Ryan Naraine, "Microsoft Says Recovery from Malware Becoming Impossible," April 4, 2006.

Chapter 12
Protecting Your PII

"Any computing device is a potential target."

—Lauren Bass, author of *The Concealed Cost of*

Every day, you could be letting strangers into your home, your bedroom, even your private conversations without your knowledge. Alan and Jean, an elderly couple from the United Kingdom, learned that lesson the hard way.

One day, someone broke into their shed and stole Alan's bike. So, Alan made the decision to buy smart cameras and install them outside to monitor their

"When we moved over here, somebody broke into my shed and took a bike so I realized it would be a good idea to have some more cameras outside. So, I put two more cameras out, better quality ones enabled me to see in more detail what was going on," Alan

Alan installed seven cameras in his home all with remote access so that only he and his wife could view the footage on their Or so he thought.

“I’m not a person that feels threatened anyway, so I just let him get on with it,” Jean said. “But he went away for a week or two, and I was here on my own. So, I think then I thought to myself, *Well, that’s good, you*

Unfortunately for the elderly couple, everything was not good. As it turns out, it was not good at all. When a security analyst examined the cameras to see the number of times they’d been viewed by someone other than Alan or Jean, the results were

The cameras had been accessed by third parties almost five thousand times from seventy different countries. By the time they discover the breach, strangers had watched the couple for a total of 366 hours, with one person watching for nine hours

If you’re wondering how such a massive breach like this can happen, the answer is default passwords.

Default passwords are one of the top vulnerabilities of IoT devices. Default passwords are particularly susceptible to attacks.

Sometimes they are simple phrases such as “admin” or “password.” Even if the default password to your device deviates from this pattern, these websites are dedicated to hosting default passwords to common devices.

These websites were created for ethical purposes such as someone being locked out of their own device, but like many

tools, when in the wrong hands they can be used for malicious purposes.

In 2018, connected cameras and Internet routers were the most infected IoT devices accounting for 15 and 75 percent of the IoT device attacks respectively. Routers are targeted so often not because attackers want to gain access to your Wi-Fi, but because they provide a gateway for attackers to gain access to other valuable personal information on the devices connected to your router. It acts as a very effective jump-off point for a

Practicing caution is so important when thinking about your cybersecurity. Alan and Jean would have never guessed that neglecting to change the default password on their smart cameras would have led to such a massive breach of their privacy and security.

“I think it’s definitely pointed us to having everything really screwed down,” Alan said. “Starting with better passwords, that’s my next

Passwords Are Your Protection

According to a survey done by Avast, 83 percent of Americans are using a weak Today, most of us have too many online accounts to keep track of. We can’t memorize unique, strong passwords for every website we’ve ever signed up for.

However, making sure that your accounts and devices are properly password protected is a very important part of a healthy cybersecurity routine.

To be honest, I wouldn't be able to memorize the passwords for the accounts I've set up in past month. It's impossible. We all live busy lives buzzing with information, and remembering the password to our LinkedIn account is not a good use of brainpower.

If you're able to memorize all of your passwords, I'm going to bet they're too similar to each other and therefore not unique and not secure. I'm not judging because I'm speaking from experience. I, too, was the woman of the one password with many variations.

A word that means something to me capitalized at the beginning, add a number at the end, and if the site required it, I'd slap a special character in for some razzle dazzle.

However, that password and its variations were found in a breach just a few years ago.

I wasn't the only one. According to Avast, 53 percent of Americans reuse passwords to protect multiple accounts and of those that do, 88 percent said they were aware that "the practice is risky." When asked why they still do it, 54 percent said, "they can only memorize a limited number of

Cybercriminals know it takes a conscious effort to create new passwords for all of your online accounts, and they exploit that vulnerability. Therefore, we cannot be complacent and think that simply because nothing catastrophic has happened yet, we can continue our routines and remain safe.

Luis Corrons, security evangelist at Avast said, “Creating strong and unique passwords for each online account is nearly impossible, which is why people create weak passwords that are easy to remember or re-use passwords for multiple online accounts.” Corrons continued, “Cybercriminals take advantage of this behavior to try to infiltrate accounts by brute force, attempting to use personal information to guess other passwords, or purchasing leaked credentials on the darknet to login into further

We now know that a strong password is important because your password is one of the main things that protects your PII from cyberattackers.

Luis explains why you shouldn’t use personal information in your passwords, “Cybercriminals collect personal data, like login credentials, from various sources including data breaches and sell it on the darknet for other cybercriminals to

In January 2019, a large list of breached information, Collection #1, was discovered being circulated on a hacking forum. The data contained 2,692,818,238 (nearly 2.7 billion) records including 1,160,253,228 unique combinations of email addresses and This is from only one collection of stolen information. There are several

others with a similar amount of data included, and countless others as the numbers dwindle.

With the sheer amount of personal information circulating in public domain, it is likely that your email address or password has been breached already, especially if it is a weak one. To check to see if your email address or password has been included in Collection #1 or any public data breach you can visit: https://haveibeenpwned.com/.

Since we know we need unique passwords for all our accounts, we need a system for keeping up with and managing our passwords too. No, it cannot be pen and paper, a notebook in your desk drawer, or that sticky note on your computer monitor. Those behaviors put your cybersecurity at risk.

If you're thinking, *Well, no one has access to my password book* but me or *I trust my co-workers not to read the sticky notes on my* is secure until it isn't.

And storing sensitive, personal information where it can be seen by bystanders or taken from your desk when you're on your lunch break puts you at a higher risk of becoming a victim of a cybercrime.

Therefore, I recommend that everyone implements an online password manager into their cybersecurity routine. A password manager will not only help you create strong, new passwords but also stores your existing ones in a secure place with only one master password that you need to remember. It can also help you update your existing passwords and change them to something

stronger than your current middle name, plus your favorite number combination.

You will want to choose a password manager that uses two-factor authentication since it will be storing very important information.

Using a password manager can be an uncomfortable switch for many of us because it is a change in how we do our daily online activities. This is one of the reasons that only 2 percent of people use a password manager, according to a study by However, you can join that select, extra-secure group of people because you know the Cyber Curiosity mindset.

Once you make the switch, you'll wonder why you didn't do it sooner.

Ways a Password Manager Can Make Your Life Simpler:

Simpler: Simpler:

There are built-in password managers on many devices and browsers now, but having a standalone password manager allows you to use your password manager on devices not made by the brand of the device with the built-in password manager (i.e., you can't access your passwords from your Apple iPhone on your Windows PC) and many of them offer better security and features.

I personally use and recommend LastPass. Other password managers like Keeper, Dashlane, and LogMeOnce are top picks by the online tech review company,

Another layer of security protection that many companies now provide is two-factor authentication or 2FA. 2FA is when you are required to give two different forms of authentication when logging into an account.

The three types of authentication are:

•Something you have (device, text, call, email).
•Something you know (password, pin).
•Something you are (fingerprint, facial recognition).

For example, being required to enter your username and password then being asked to enter a code that is sent to you via text or email. You presented something you know, your password, then you showed that you have ownership of the device or email that is linked to the account by entering the code.

Use 2FA whenever it is available so that your password is not the only thing you are relying on to stop cyberattackers from

breaching your account. 2FA being offered is a clue that the information that is being protected is valuable, and the extra layer of protection is needed.

How Do I Create a Good Password?

If you choose to manually create your own password, there are some simple rules for what you should and shouldn't include in your password.

Most importantly, every one of your passwords should be unique. While duplicate or similar passwords are easy to remember, they leave you vulnerable if your information is stolen in a data breach. Therefore, it is important for your passwords on different accounts to have variety, so if your account information happens to be leaked in a breach, your other accounts will not be compromised.

Another important rule for creating secure passwords is to never use any personally identifiable information in your password or any information about yourself that you have made public.

"Cybercriminals can use personal details, such as your favorite color, the last four digits of your credit card, and your email addresses to make educated guesses about your sign-in credentials," said Larry Alton from Entrepreneur.com. "They might contact a service provider posing as a user, provide identifying details and gain even greater access to

This can include your name (first, middle, or last), your pet's name, the year you were born, address, or anything else that an attacker can easily deduce from a simple scroll through your social media profiles or web search.

It is also wise to use a variety of characters when crafting your password including upper and lowercase letters, numbers, and symbols. While the length of your password plays a role in how easy it is to guess, the main factor of how hard it is to guess is the complexity of the password.

Attackers often use computer programs to attempt to crack your password if it isn't guessable from your personal information, so it should be long and randomized (which shouldn't be a problem if you're using your password manager.)

If you find yourself in a situation where you need to create your own password, here are some tips to make your password as strong as possible:

•Use at least sixteen or more characters.
•Contain both numbers and special characters, if possible.
•Have a mix of both uppercase and lowercase letters.
•Unrelated to yourself, the website, or the service the password is used for.

If you need a trick to help you make a strong, memorable password, string together a few unrelated words and make a phrase. For example, tUrtle_tOuches_tOeso. It may feel silly, but

it's memorable. We used capital letters in a pattern that is memorable, but not as predictable as the first letter of each word being capitalized and incorporated numbers and special characters.

This is a great trick to use when setting up the master password for your password manager. Make sure it is random and unrelated to your life, if you owned any turtles, my example password wouldn't be a good fit for you. Try it. Be creative and see what you can come up with.

Storing Your Data, Securely

How you choose to store your data is very important, and it can have a huge impact on the overall security of your private information. ensuring your storage is backed up in the case of an emergency. Storing your sensitive or important data files improperly or carelessly can cost you time, money, intellectual property, or privacy.

Your local drive is the storage drive inside your device, whether it is a desktop, laptop, tablet, or smartphone.

Your local drive should never be your only data storage solution. If you only have one copy of your files, and it is on your local drive you are putting your information at high risk. You should always back up your data.

Now that we know that we need a backup, we need to choose how we are going to back our data up. Just like most things in

technology, there's not just one way to back up your information. Sorting through all of the information can be quite overwhelming, so let's try to keep it simple.

When it comes to backing up your data, you have two basic categories to choose from: cloud-based storage and physical storage. The one you choose is based on what you want and need from your storage solution.

Everyone is different and has different needs when it comes to storage, but before we get to that let's discuss what "the cloud" is.

I hate to tell you that when you store your data in "the cloud" it isn't being sent into outer space or taking a nap with the stars.

Companies like Google, Microsoft, and Apple host a network of servers (computers) with massive storage capacities. The cloud is when these companies rent us a share of that storage. Your data is saved to their server and not your device's local drive, so you can back up, sync, and access your information from any device as long as you have an Internet

These features give cloud storage solutions a lot of pros. You don't have to worry about losing your information if your device is broken, lost, or stolen. The cloud makes it easy to share documents, photos, and other information with classmates, co-workers, friends, or family. The cloud is great for collaboration, and best of all you don't have to manage the storage yourself.

Many cloud storage providers also offer free accounts with a limited amount of storage capacity, so you can try out the platform.

Examples of cloud storage solutions include Dropbox, OneDrive, Google Drive, and iCloud. However, cloud storage solutions come with some cons.

You can only access your cloud storage if you have Internet access, so if you are in a place without Internet, you won't be able to pull up your documents to continue your work or access your photos. The speed of your Internet connection can also affect your cloud experience, if your Internet speed is slower, it might take longer for documents to upload and download to the cloud.

Also, since cloud storage gets its capabilities from the Internet, cloud storage solutions can be subject to a cyberattack. In 2012, Dropbox fell victim to a cyberattack where over 68 million user accounts were breached, stolen, and then sold on the dark web for bitcoin, or around $1,141 at the time. The full details of the attack didn't emerge until four years

Dropbox then asked all its users to reset their passwords, and they made a statement about their ongoing commitment to data

I would not recommend saving confidential documents, personally identifiable information, or anything else that would be devastating to you, if breached, to the cloud.

While the cloud isn't the most secure, it is great for saving and sharing non-confidential documents, files, and photos. I have worked on countless group projects that would never have happened without Google Docs. So, just practice caution when using the cloud. Stop and think before you decide to upload your Social Security card or driver's license into the cloud because you are one breach away from someone having that information.

Next, there is physical storage. We're going to talk about physical storage in terms of portable external drives.

Nonportable drives exist, but they are not very popular. Especially since today you can get a portable drive with up to sixteen terabytes (TB). One TB can hold 6.5 million document pages. That's enough pages to fill 1,300 physical filing cabinets. (For reference one TB = 1,000 gigabytes

So, unless you have extraordinary data needs, you should be able to find a portable drive that works for you and your data. However, this is one of the pros of external drives. They offer larger storage capacities than cloud storage solutions, often at a lower price. Cloud storage providers often charge by the month for storage, and the rate climbs alongside the storage capacity, while an external drive is a single purchase.

Another pro of physical storage is having access to your data even if you don't have Internet access.

Physical drives have their cons, however. They are known to be fragile and should be handled carefully. Like a laptop, if it takes

too many falls, it can destroy the device or corrupt the data. You can buy a protective case to mitigate this issue, but you should still be cautious. They also have a lifespan, similar to other electronic products. They will go bad at some point, so it's always good to have a backup for your backup just in

Many manufactures have implemented precautionary measures to recover data if anything unfortunate happens to the external

If you are looking into getting an external drive, there are two options: a hard disk drive (HDD) and a solid-state drive (SSD). When buying or building a computer, you will face these options as well.

HDDs have been around since the dawn of computers, and comparatively, SSDs are a new technical innovation only dating back to the late 2000s. SSDs are much smaller than HDDs of the same storage capacity, allowing manufacturers to create the ultra-light laptops we have

HDDs are more affordable than SSDs per gigabyte of storage. For this reason, it is uncommon to see SSDs with capacities larger than two TB because consumers are unwilling or unable to pay the price. SSDs are desirable to some because they are faster, quieter, and more reliable than HDDs. SSDs can also stand rougher handling because they don't have any moving

So, which one is best? That depends on your preference. If you need a lot of space or you're on a budget, I'd recommend an

HDD. If you're someone who is constantly on the go, wants a fast drive, and is rough on their belongings, you should opt for the

If you want a fully "private" secure backup, storage system, I recommend using an external drive not connected to the Internet and doesn't backup to the cloud. Then, you only have to worry about your data being physically damaged, compromised, or stolen. If you want to backup important documents like tax documents, health information, etc., this would be a way to do it that is safer than the cloud.

As you can see, there is no clear winner in the battle of storage solutions. How you store your data should be based on what works best for your lifestyle.

The only wrong choice is not backing up your data.

Failing to back up your data can cost you valuable time, memories, and money. As we discussed in our chapter on malware, if your device becomes infected with ransomware or any type of malware that corrupts or erases data from your device, if you don't have a backup, you will lose your valuable data.

Now, it's time to take the tips from this chapter and apply them in your life. Figure out what data you have stored in the cloud. Look through your local drive and see if you have any important but not private files that you need to backup. Sit down and think

about which storage option would be right for you. Following these steps is important in developing your Cyber Curiosity.

411 Lauren Bass, "The Concealed Cost of Convenience: Protecting Personal Data Privacy in the Age of Alexa," *Fordham Intellectual Property, Media & Entertainment Law Journal* 30, no. 1 (Fall 2019): 261-324.

412 *BBC* "Security Footage 'Viewed by Thousands'," May 14, 2018, video, 2:06.

413 Ibid.

414 Ibid.

415 Ibid.

416 Ibid.

417 Ibid.

418 Bass, "The Concealed Cost."

419 *BBC* "Security Footage."

420 Avast, "83% of Americans Are Using Weak Passwords," May 2, 2019.

421 Ibid.

422 Ibid.

423 Ibid.

424 Troy Hunt, "The 773 Million Record "Collection #1" Data Breach," *Troy Hunt* (blog), January 17, 2019.

425 Avast, "83% of Americans."

426 Neil J. Rubenking and Ben Moore, "The Best Password Managers for 2021," last modified February 17, 2021.

427 Nate Lord, "101 Data Security Tips: Quotes from Experts on Breaches, Policy, News and More," *DataInsider* (blog), *Digital* updated August 5, 2020.

428 Ibid.

429 Contel Bradford, "7 Most Infamous Cloud Security Breaches," *Recovery Zone* (blog), accessed March 5, 2021.

430 Ibid.

431 "How Much Is 1 TB of Storage?" Dropbox, accessed March 5, 2021.

[432] Michael Moodie, “Pros & Cons of External Hard Drives You Should Know,” January 24, 2019.

[433] Ibid.

[434] Tom Brant, “SSD vs. HDD: What’s the Difference?” last updated September 2, 2020.

[435] Ibid.

[436] Ibid.

Chapter 13
Protecting Vulnerable Populations

I strongly believe that a one-size-fits-all approach is not appropriate in most situations, and cybersecurity is no different.

I've broken this chapter into sections that specifically address the issues that children, teens, and the elderly face in cyberspace. I decided not to include an "Adult" section in this chapter, because I don't believe as an adult, we face any special circumstances when approaching cyberthreats, and the general resources in the other chapters will work great for us. However, adults will benefit from this chapter if they want to learn how to shield their children or elderly loved ones.

Someone who has been raised with technology from birth is going to face different hurdles than someone who is still adjusting to the changing technical landscape. There are also specific scams and predators preying on these vulnerable groups. This is also why it is vital for parents to play an integral role in helping their children develop good cybersecurity habits from a young age. It is never too early to encourage someone to adopt the Cyber Curiosity mindset.

Children & Teens

Stranger Danger

Every year, millions of children are targeted by predators. Over 25 percent of minors receive sexual messages from adults on the Internet each In 2020, The National Center for Missing & Exploited Children's (NCMEC) CyberTipline, the United States' centralized reporting system for the online exploitation of children, received over 21.7 million reports of suspected child sexual exploitation, the highest number of annual reports

These statistics represent a real and growing threat to the safety and well-being of our children. This threat is often forgotten, overlooked, or underestimated by our society, which can leave children vulnerable to becoming a victim of sex trafficking or exploitation for child pornography.

This is a fact that Attorney General Andy Beshear of Kentucky knows too well. In early 2018, Beshear's Cybercrimes Unit began an investigation into Ernest Anziana, after they discovered he was attempting to solicit sex from an underage girl in

Anziana was a forty-nine-year-old man living in Fredonia, Kansas. He allegedly offered $500 and seven grams of meth to purchase the young

"The details involved in this case are disturbing, yet our office encounters human trafficking cases in every county, city, and community across Kentucky," Attorney General Beshear stated. "Human trafficking represents the worst form of abuse, most often in children, as we have in this case. Every part of my office

is committed to investigating and prosecuting predators seeking to harm our children and

Anziana was served with an indictment warrant on February 7, He was extradited to Kentucky, where he was sentenced to five years in prison and designated as a lifetime sex

Protecting Your Children

The Internet has unfortunately become a breeding ground for sex trafficking and child exploitation. Stranger danger no longer only applies to people you meet in person.

According to the NCMEC, online enticement involves "an individual communicating with someone believed to be a child via the internet with the intent to commit a sexual offense or

Online enticement is a broad category of online exploitation of children, "including sextortion, in which a child is being groomed to take sexually explicit images and/or ultimately meet face-to-face with someone for sexual purposes, or to engage in a sexual conversation online or, in some instances, to sell/trade the child's sexual images," according to the NCMEC website. This type of cybercrime takes place on every platform, from social media, messaging applications, gaming platforms,

So, how is this happening? When the NCMEC analyzed CyberTipline data, they found that most often predators used these methods to entice children:

Most Common Methods Predators Used to Entice Children:

Children: Children:

These criminals were often motivated by acquiring explicit content (60 percent), meeting the child to participate in illegal and inappropriate acts (32 percent), and having explicit conversations with the minor (8

The children often are tricked into believing they are talking to someone closer to their age, like an older teen. "Someone who wants to take advantage of kids will pretend to be younger than they are, and obviously lie about their identity," says Prevention Director at The National Children's Advocacy Center Pam

The predator will then try to gain the child's trust by taking advantage of the child's natural need to belong or have someone who understands them. Clasgens said, "They might ask kids a lot of personal questions, give lots of compliments—they might even offer to send kids a gift." Clasgens continued, "They might be curious, someone might take advantage of their curiosity. Even kids that aren't depressed or lonely can be taken advantage of pretty easily by someone who is very

If you don't know what apps your child has on their devices, you should find out. Especially when it comes to social media and messaging apps like Facebook, Instagram, WhatsApp, Snapchat, etc. I can't name every social media and messaging app here, but you should do your research on the apps your child has installed on their devices.

You should also talk to your kids about what they do online. What apps are they using? Do they have any online friends? What do they talk about with their online friends?

However, too much prying will prompt your child to become defensive, so ask like you're genuinely interested, because you are. Clasgens suggests talking to your child in a way that won't scare

Clasgens recommends asking "what if" questions like, "What if someone started talking to you online that you don't know in real life?" These types of questions create an open dialogue and don't come off as accusatory. You can also use "what if" questions to set expectations for how you would like your child to behave

For example, if your child answered that "they would continue the conversation if they were nice" to the previous question, you could tell them that the rule you have about not talking to strangers applies online as well.

"Offenders are able to take advantage of children when their activities are secret," Kennedy said. "This happens often when

children are not comfortable or even afraid to go to adults in their lives when something is happening online, especially when they feel that they have done things they regret or know they shouldn't have

Creating a safe space for your children to express themselves about their experiences online is essential to their online safety. Whether they are experiencing sextortion, cyberbullying, or just need help to navigate the Internet, you want them to feel comfortable confiding in you with their concerns. Your children want to be able to talk to you about their online activities, but they are often afraid of how you will react to what they will

So, make sure you are open to receiving their answers and not overly critical when responding. Children can also pick up on body language and tone, so your words must match your tone and

"The best thing you can do to protect your child online is to be involved in their online life," said Susan Kennedy, prevention program manager at NCMEC. "Ask about what they are doing online and take a genuine interest. Provide guidance but try not to be overly punitive or

Reports of online enticement to the NCMEC nearly doubled from 2019 to 2020 showing a 97.5 percent increase in So it is more important than ever to protect your children as they navigate cyberspace.

Children and teens today haven't known a world without the Internet. So, cyberspace isn't a separate, new, place for them. It's just their life. So, as a parent it's important to think from that perspective when approaching your child about an issue they're facing online.

Consistent parental involvement is the best protection kids have against online threats.

Educate yourself and talk to your kids about appropriate and inappropriate online behavior. Make sure your children know what type of pictures or videos are inappropriate to take of themselves and send to others, and be sure to tell them that if anyone asks for those types of pictures from them to not answer and tell you what happened. Teach them how to spot red flags in messages such as sexual language or a stranger asking to meet them somewhere.

For younger children, you can limit the risks further by installing parental controls that allow you to set criteria for Internet content, programs used, time spent online, and online chat partners. Configuring security settings on your children's device is an important part of good cybersecurity hygiene. Don't rely too heavily on parental controls and security settings, however. As always, a strong focus on teaching healthy behaviors and cyberawareness should be at the core of your cybersecurity routine.

As State of California Department of Justice, Office of the Attorney General stated, "For younger children, install parental control

software that limits the Web sites kids can visit. But remember—no software can substitute for parental

Emphasize cyberawareness in your household and ingrain the values of the Cyber Curiosity mindset into your children and teens from an early age. This will encourage them to make smart decisions when interacting in cyberspace because they are cyberaware and know they should always approach cyber situations with caution and curiosity.

The Cybersecurity and Infrastructure Security Agency stresses, “It is important to add only people you know on social media sites and programs like Skype; adding strangers could expose you and your personal information to Emphasize to your children that adding people that you don’t know on social media platforms can make them vulnerable to predators and cybercriminals.

“Online enticement can happen to any child using the internet,” said Lindsey Olson, executive director of NCMEC’s Exploited Children Division. “Offenders are very effective at grooming children, gaining their trust, isolating them from their parents, and then exploiting them. Parents often think that it would ‘never’ happen to their child, but we know that is simply not

The warning signs that a child may be being exploited are rapid changes in mood, weight, and grades, however warning signs can vary by

It is important to remember it is never the child's fault. "They [the child] often think it is their (sic) fault. Of course, it is not their fault," says

Now more than ever, we all must be cyberaware and spread awareness to keep the children in our lives safe online.

Protecting Their Devices

In our modern world, making sure that our loved ones are safe and protected online is a top priority, but it is also harder than ever.

Texting, video chatting, and social media have quickly become one of our main sources of communication with our family, friends, and loved ones. An influx of new applications has made it easier than ever to connect with people.

A million smartphones are lost. Only 7 percent of them are ever The other 93 percent never return to their rightful owner, but that doesn't mean they didn't find a new home.

Young children and teens are the most likely to misplace or lose their devices. With those devices, they lose valuable PII, if the device is not password protected or able to be wiped clean before it is found by someone else. Therefore, it is very important for them to learn about cybersecurity from a very early age. We are introducing children to technology at a very young and naïve age without considering the implications.

A survey was conducted on teens and young adults, 74 percent of respondents said that their smartphone was always with Children, teens, and young adults are connected to their devices more than ever before. This is the time to emphasize the importance of cybersecurity in our society.

Richard Power, distinguished fellow at Carnegie Mellon CyLab stated, “From cyberbullying to sexting to prowling predators, the Information Age has brought with it a new spectrum of risks and threats for parents to guard their children against, and now that spectrum of threats has expanded to include child identity

Minors are especially vulnerable to becoming victims of identity theft. Cybercriminals see them as a great target because of their clean credit histories, and the fact that parents are unlikely to monitor their children’s identities for signs of theft makes it easy for them to fly under the radar for years without being

Research conducted at Carnegie Melon CyLab based on identity scans of 40,000 children found that someone else was using the Social Security Number of 10.2 percent of the children. The children’s IDs were being used to do everything from purchasing homes and cars to getting jobs and driver’s

Children and teens should be aware they should not give out their personal information to anyone over the Internet. They should be aware that they need to password-protect their devices and have proper passwords for their accounts, which you can find more

information about in Chapter 12. Teach your children that they should never give their information to a company or application that you don't know and trust. Always look for a sign that the website is trustworthy, refer to Chapter 11 for ways to tell if a website is secure.

The Elderly

The elderly are frequent targets of cyberattacks. As the elderly population grows, elder fraud will grow with them. Every year, millions of elderly Americans become victims of a financial fraud or confidence scheme. Annually seniors lose more than three million dollars to elder

Cybercriminals prey on the perceived vulnerability of the elderly to increase their chances of executing a successful cyberattack. They are also targeted because of their trust in the Internet and their politeness. Seniors are also less likely to report fraud because of shame that they fell

Elders are targeted because they typically have more money saved than the younger population who are just starting their careers. The elderly are also more likely to own their home and have good credit making them an attractive target for attackers.

Press 1 to Report a Scam

Most phone owners have experienced a spam call before. Collectively, Americans receive over forty-eight billion spam calls

every One in three Americans reports they have fallen victim to a phone scam, and $19.7 billion was lost due to phone scams in 2019, according to research by The attackers making the calls are getting smarter as well. According to a report by First Orion, more than 80 percent of scam calls in the US used the recipient's local area code. This increases the likelihood that the recipient of the call will answer, and one out of three scam calls are answered because the phone number is

The elderly are particularly vulnerable to phone scams. They are often targeted because of their age, and if they are not aware of the signs of a scam, it is easy for them to fall prey because of their trusting nature.

Gina Murray is the co-founder and director of Aware Senior Care. She was aware of scams that targeted seniors, yet a convincing scam phone call from the "Internal Revenue Service (IRS)" rocked her

Gina was just arriving home when she answered her phone. It was the "IRS." She says the man on the line sounded "very

Gina wrote, "He told me his name and said this was a courtesy call." She continued, "The man explained that my name was pulled from a random audit, and they found a 'miscalculation' during the years 2008–2013. I owed $12,562 immediately, and since I had not answered their [sic] certified letters, the case was now in federal

She acknowledged that as she recounted the situation, it clearly sounds like a scam, but at that moment, Murray said, "it felt very

The man on the phone covered all of his bases to present himself as a true professional who worked for the

Gina wrote, “He asked that I have a pen and paper ready to write down his information. He spelled his name, gave me his badge number as well as my case number.” She continued, “He told me that if at any time I felt pressured or intimidated, I could call the IRS main number to report him. He gave me the number —while he spoke, I did a reverse lookup, and the number was indeed the main number to the

Gina asked the man if he could tell her “when and where the miscalculation

He told her all the papers were sent to the court and Gina had missed her time to do the research. His call was simply to let her know she owed this

Gina recalled, “He also said if I went to court and ‘lost’ to the IRS, I would owe

Gina felt trapped. She had never had any issues with the IRS, and the threat of lawsuits and 6-figure payments terrified

She recounted how she felt during the call, “My head was spinning, and I kept trying to tell him I had not received any letter from the

Although Gina is the co-founder of a senior facility and has knowledge about elder scams and phone scams, the call still felt incredibly real to her. Gina wrote, “The conversation lasted about ten minutes and I was pretty upset. It sounded very plausible, very real, and very

“Just as he started to tell me how I could ‘resolve’ this problem, [my husband] Tim arrived home,” Gina wrote. “He could see that I was shaken by this caller and stopped to listen. I pointed to the notes I had been taking,” she

Her husband, Tim, calmly took the phone away from her and told the man on the line, “The IRS never calls. Do not ever call this number

Tim proceeded to hang up the phone as Gina began rattling off the details of her conversation with the

Her husband repeated, “The IRS does not

While she knew her husband was right, she still has second thoughts about the call. “Part of me still worries, ‘What if it’s true? What if I really do owe the IRS?’” Gina

However, it isn’t true. That is the purpose of social engineering: it is used to make us question our best instincts in the heat of the moment and make rash decisions we wouldn’t otherwise make.

Knowing these scammers are using social engineering tactics to prey on the elderly makes Gina upset because she is an advocate for seniors and their

“Then I feel angry at the thought of this caller preying on anyone else—especially the elderly,” Gina said. “I was truly shaken by that call. We are law abiding, tax-paying citizens, and to have that questioned was upsetting,” she

We can use Gina’s story as an example of how scammers use different tactics to lower your defenses and build your trust.

The scammer used a specific number, not an even one like ten thousand, for the payment amount (I owed $12,562) to make the situation feel realistic. The scammer drew from common public knowledge and adapted his strategy, he addressed the commonly known fact that the IRS will send you correspondence by mail to his

When someone presses a sense of urgency (I owed $12,562 stop and Why does this person need this money or thing right now? Why can’t it wait? If their explanation doesn’t feel right to you, ask a friend or family member for their advice. You don’t have to tell them that the advice is for you if you don’t want to; you can tell them you saw a similar situation on TV or read about it and wanted their opinion.

The scammer gave Gina the IRS number to make her feel like the call was legitimate when she looked up the number and found it was real. He hedged his bets on the fact that she was too polite to hang up on him and call the number. Don't be afraid to hang up and call the verified number of an organization. As we've talked about in earlier chapters, scammers can spoof phone numbers. Also, check all case numbers, badge numbers, and all other information given to you by the caller with the respective

As humans, we do everything that we can to avoid losses. This is called loss aversion, and the scammer in Gina's story played into our human instincts extremely well. The scammer gave Gina two options: pay the $12,562 now or wait, go to court, and possibly lose (if I went to court and "lost" to the IRS, I would owe

When presented with this situation, most people would choose the first option, because no one wants to go to court or gamble that much money.

However, the scammers know that, which is why they frame their scams this way. In the end, they are still $12,562 richer.

Remember, the IRS never calls you, neither does the Social Security Administration

Now that you can recognize some tactics used within a scam call, let's go over some more quick facts to remember when receiving a possible scam call.

Common Senior Scams

Scams Scams Scams Scams Scams Scams Scams Scams Scams Scams Scams Scams Scams Scams

Be cautious and curious. Stop and think before you give your money or personal information to anyone. You can reference Chapter 11 for more tips on how to spot a phishing message or call.

Ways You Can Help

One way to help seniors avoid scams is to reduce loneliness. Loneliness increases the likelihood that seniors will fall for a scam. It also makes it more likely because they don't have anyone to consult with about it before making their decision.

Many seniors don't understand the significance of cybersecurity, so we must help them create positive cybersecurity habits.

According to research done by Home Instead, Inc., half of seniors don't have passwords on at least one of their IoT devices. This leaves them vulnerable to identity theft if their device is lost or stolen or spyware being installed onto their device by whoever may pick it

Pass your knowledge along and help a senior that you love to become cyberaware, and work with them on building their cyber

skills. You can do this in a variety of ways. You can teach them about common scams that are being used on the elderly. You can help them set up their devices with the best security settings for them, help them set up a password manager, and teach them how to operate their IoT devices in the safest way possible.

Adapting to the new and exciting world of cyberspace is challenging for many people, but it poses a unique set of challenges for digital immigrants, especially elders. For this world of technical innovations to be introduced to them at a later stage in their life, it can be challenging to say the least.

It can be daunting to be expected to shift from an analog world to a digital one, and without guidance, there will be missteps. Those missteps can end in heartbreak, financial ruin, and emotional trauma for seniors. With the proper guidance, we can help seniors avoid these missteps and have a pleasant Internet experience.

While adapting to our modern world is a big adjustment for many, it does not have to be a fearful or uncomfortable one for seniors. Cyber scams against seniors can be prevented from being successful. We shouldn't accept that our grandparents are more likely to fall victim to a scam.

With the proper tools and a Cyber Curiosity mindset, seniors can advance their cybersecurity skills and understanding of cyberspace to be equipped to not only embrace technology but to conquer it.

437 Salem Press Encyclopedia, Academic ed., s.v. "Child Pornography," accessed March 8, 2021.

438 Brenna O'Donnell, "Rise in Online Enticement and Other Trends: NCMEC Releases 2020 Exploitation Stats," *Missing Kids* (blog), *National Center for Missing & Exploited* February 24, 2021.

439 Mike Stunson, "Kansas Man Tried to Purchase Kentucky Child for $500 and Meth. He's Going to Prison," *Lexington* last updated October 23, 2018.

440 Ibid.

441 Ibid.

442 Ibid.

443 WBKO News Staff, "Kansas Man Sentenced after Attempting to Buy Kentucky Child Online," *WBKO,* October 23, 2018.

444 O'Donnell, "Rise in Online Enticement."

445 Ibid.

446 "What Is Online Enticement and How Is It Happening?" MSN, May 14, 2018.

447 Ibid.

448 Ibid.

449 Ibid.

450 Ibid.

451 Ibid.

452 Ibid.

453 Ibid.

454 Ibid.

455 Ibid.

456 Kailey Schulyer, "Spike in Online Enticement Reports Amid Pandemic," *WAFF News*, January 27, 2021.

457 Ibid.

458 Ibid.

459 O'Donnell, "Rise in Online Enticement."

460 Schulyer, "Spike in Online Enticement."

461 Ibid.

462 O'Donnell, "Rise in Online Enticement."

463 Ibid.

464 State of California Department of Justice, "Protect Your Computer From Viruses, Hackers, and Spies," accessed March 13, 2021.

465 US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Cybersecurity and Older Americans* (Washington, DC, 2019).

466 O'Donnell, "Rise in Online Enticement."

467 Schulyer, "Spike in Online Enticement."

468 Ibid.

469 Frank Breitinger, Ryan Tully-Doyle and Courtney Hassenfeldt. "A Survey on Smartphone User's Security Choices, Awareness and Education." *Computer & Security* 88, no. 101647 (January 2020).

470 Ibid.

471 Richard Power, "Child Identity Theft," CyLab, accessed March 8, 2021.

472 Ibid.

473 Ibid.

474 "Elder Fraud," US Federal Bureau of Investigation, accessed March 8, 2021.

475 Ibid.

476 Sam Cook, "35+ Phone Spam Statistics for 2017—2021," *Comparitech* (blog), last updated February 8, 2021.

477 Kim Kok, "Truecaller Insights 2020 US Spam & Scam Report," *Truecaller* (blog), April 16, 2020.

478 Ibid.

479 Gina Murray, "IRS Scam Phone Call: How to Protect Your Loved Ones," *Aware Senior Care* September 15, 2016.

480 Ibid.

481 Ibid.

482 Ibid.

483 Ibid.

484 Ibid.

485 Ibid.

486 Ibid.

487 Ibid.

488 Ibid.

489 Ibid.

490 Ibid.

491 Ibid.

492 Ibid.

493 Ibid.

494 Ibid.

495 Ibid.

496 Ibid.

497 Ibid.

498 Ibid.

499 Ibid.

500 Ibid.

501 Ibid.

502 Ibid.

503 "Elder Fraud," US Federal Bureau of Investigation.

504 "10 Cybersecurity Best Practices for Older Adults," Protect Seniors Online, accessed March 8, 2021.

Conclusion

A total of 4,883,231 cybercrime complaints have been filed with the IC3 since its inception just over two decades ago. In 2019 alone, cybercrime victims lost $3.5 billion, and these numbers are just those who reported their case to the

The true number is millions more. Over 1.5 million phishing sites are created every Approximately 67 percent of Americans have never checked to see if they were affected by a security breach. IoT devices experience an average of 5,300 attacks monthly. One in thirty-six mobile devices had high-risk apps installed. In 2019, nearly 11,000 malicious mobile apps were blocked per day. The number is set to increase by 3.9 percent per year. One in thirteen web requests leads to I think you get the point.

Despite these shocking statistics, a study done by Enjoy Safer Technology found that nine out of ten Americans saw cybercrime as a challenge to the country's security and that it was "bigger than drug trafficking, money laundering or other major However, as we've learned, cybercrime is not any different from traditional crime, but a natural evolution of traditional crime and criminals taking their activities to a new venue: the Internet. Drug trafficking, money laundering, identity theft, and many other traditional crimes formerly performed in the physical world are now capable of being done in cyberspace.

This, combined with the uptick in cybercriminal activity, is the reason that no one is immune to becoming a victim of a cybercrime—especially if you are not taking active steps to protect yourself.

As I stated in Chapter 1, my definition of cybersecurity is "the measures individuals and organizations take to protect themselves, their personally identifiable information, and their digital, physical, and financial assets from unauthorized use, damage, or exploitation."

This book was never meant to be a complete, comprehensive guide to cybersecurity. Cybersecurity is constantly evolving, and there is something new to learn every day. This book is a guide on how to protect yourself in our hyperconnected world and is packed with valuable personal cybersecurity lessons hand-picked cybersecurity experts and myself.

I live by the belief that knowledge is power, and the more you know about a threat, the better you can defend yourself against it. No one would go into a boxing ring blindfolded. You could be entering the ring to fight a ten-foot-tall beast or a baby rabbit, but you'll never know until you remove the blindfold. This book is removing that blindfold.

Without knowledge of social engineering, sextortion, malware, the privacy paradox, and the many other topics covered in this book, you wouldn't be prepared to defend yourself against them.

Initially, my goal was to change the mindset that surrounds cybersecurity—how we think about cybersecurity, how we talk about cybersecurity, and how we approach cybersecurity in our daily lives.

I've met many people over the years that didn't know what cybersecurity was, and for a long time I didn't know how to explain it in a five-minute conversation. However, I knew deep down that cybersecurity could be and should be for everyone. I'd taken the classes and understood the concepts and how they're helpful for everyone, but I couldn't put it into words.

So, I set out to explain cybersecurity in a way that was enjoyable and demonstrates how to implement positive cybersecurity habits in ways that don't disrupt our daily lives and activities.

That is why building a cyber curiosity mindset is so important. The cyber curiosity mindset takes the "scariness" and the often-gloomy tone around cybersecurity and reimagines it as a topic that is not only approachable but for everyone. Using the three Cs of cyber curiosity (cyberawareness, caution, and curiosity) anyone can learn cybersecurity. No matter your age, your background, or your apprehension coming into this book, you can adopt the cyber curiosity mindset and use it to successfully protect yourself.

Please don't wait until you've fallen victim to a cybercriminal to make the changes to your cybersecurity habits.

If you want a quick fix, then you can find an antivirus service that will sell you the dream of being bulletproof from cybercrimes.

However, we know those solutions don't look at the full picture.

We learned, from the mistakes of businesses, that simply having expensive security software is not a full cybersecurity solution if the humans fail to act on the warnings. Therefore, we must take alerts seriously, no matter how much of a nuisance they may feel like and pair cybersecurity software with good cybersecurity habits.

If you don't change your habits and practice the three Cs of cyber curiosity—cyberawareness, caution, and curiosity—an antivirus software will fall short of protecting your PII in the case of a breach, or your bank account in the event of identity theft. If you truly want to protect yourself and your family, you must take ownership of your personal cybersecurity, which you can't do with the click of a button. It is an ongoing commitment to security. However, if you've made it to this conclusion, I'm sure you agree it's worth it.

Now that you have the tools, you can understand, articulate, and anticipate the risks that come with living a modern, digital life. You're ready to continue to build and strengthen your cyber curiosity mindset.

Since we understand these risks, you can take the needed cybersecurity measures to protect yourself and your family and

create a personal cybersecurity routine that works for your unique lifestyle.

If you haven't done so already, grab a pen and notebook (I know, that's very 2000s—a Word document works just as well). Go back to Part 3 and create your own personalized cyber curiosity calendar.

As we said in Chapter 11, it's not recommended that you rush in or add all the tips into your life at once. The ultimate goal is that you will implement all of the tips, tricks, and techniques that apply to you and your lifestyle.

My recommendation is to break your guide into time periods. These periods can be weekly, bi-weekly, or monthly. Just choose a schedule that you can commit to and stick to it.

For example, "Amy" decides that on week one she is going to set up her password manager, get an antivirus software, and set up a VPN on her browser. She's a busy woman and has a lot of passwords so she wants to give herself time to get her password manager in order. She decides to do bi-weekly time periods. Amy also has an eleven-year-old child, so in the next time period she wants to talk to her child about stranger danger online, go through their apps with them, and help them establish healthy habits. Amy continues to set up her cyber curiosity calendar until she has filled in all the positive habits she wants to adopt.

Your cyber curiosity calendar will act as your guide as you continue to develop your cyber curious mindset. As you find new tools or resources, you can add them to your calendar as well.

Seems simple right? Now it's time for you to complete your own, and I'd love to hear from you when you do. If you need any help, extra guidance, or just want to chat about cybersecurity, please feel free to reach out to me on my website: https://www.lakeidrasmith.com.

Resources

I've decided to include these resources at the end of this book for reporting cybercrimes, missing or endangered children, and child exploitation. There are also resources where you can learn more about cybersecurity or find facts to share with friends. Be cyberaware, stay safe, and be kind to one another.

Internet Crime Complaint Center (IC3)

https://www.ic3.gov/

Internet Crimes Against Children Task Force

https://www.icactaskforce.org/

Safe Online Surfing Game

A game by the FBI for children in the third to eighth grades that teaches them safe online surfing skills. It's fun for adults too!

https://sos.fbi.gov/en/

If You Are A Victim of a Cybercrime:

•File a report with the FBI's Internet Crime Control Center (IC3) at https://www.ic3.gov/.
•File a complaint with the Federal Trade Commission (FTC) at www.ftc.gov/complaint.
•You can report a suspected phishing message to the Cybersecurity and Infrastructure Security Agency at https://www.us-cert.gov/report-phishing.

To learn more about common scams and how to avoid them visit the FTC at consumer.ftc.gov.

To Report a Missing Child or a Kidnapping Involving a Child:

Call your local FBI field office or the closest international office immediately.

You can also contact the National Center for Missing and Exploited Children (NCMEC) at 1-800-THE-LOST.

To Report Online Child Sexual Exploitation:

The Cyber Tip Line is operated by the NCMEC in partnership with the FBI and other law enforcement agencies.

Call 1-800-843-5678 or report online at https://report.cybertip.org/.

International Abduction by a Family Member and Not Yet Abroad:

If you believe your child is in the process of being abducted by a parent, legal guardian, or someone acting on their behalf, call the US Department of State at 1-888-407-4747 or 202-501-4444.

505 US Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report* (Washington, DC, 2019).

506 Dhwani Meharchandani, "Staggering Phishing Statistics in 2020," *Security Bloggers Network* (blog), Security Boulevard, December 7, 2020.

507 Marija Lazic, "39 Worrying Cyber Crime Statistics," *LegalJobs* (blog), February 26, 2021.

508 "ESET Cybersecurity Barometer," We Live Security, accessed March 10, 2021.

Acknowledgments

If you are seeing this page, that means you made it to the end of this book, and you should be acknowledged.

When writing down my goals for 2020, I put down that I would write a book before the year was finished. In my vision I thought it would be a fiction book, but God had other plans for me. I wish I could say writing this book was an easy process, but I simply cannot. I also can't say I did it alone.

Thank you to my family and friends who have supported me throughout this journey. You've listened to my ranting, complaining, and insecurities. You all have helped me battle my perfectionism and imposter syndrome. I love you all more than you know. I couldn't have picked a better support system.

A special thank you to my mom and dad, who've always supported whatever crazy thing I wanted to do 100 percent even if they didn't understand it.

Thank you to those who encouraged my writing abilities. A special thank you to my freshman year college English professor Mickey Mitchell. You believed in my writing even when I did not.

Thank you to the amazing cybersecurity experts I interviewed for this book. You helped guide my vision: Ayana Miller, Florence

Hudson, Sam Curry, Dr. Eric Cole, and Chris Silvers.

To my amazing team at New Degree Press, without you this book wouldn't be possible. Thank you for helping make my dream come to life: Eric Koester, Brian Bies, Adam Burkhart, and John Chancey.

Thank you to all my amazing friends and family who pre-ordered my book and continuously support me in everything I do. To you, I am eternally grateful. Here are all their names in alphabetical order:

Aalieyah Finley, Alberta Washington, Alyssa Price, Andrew Nelson, Angela Hill, Angie Watt, Antonio Smith, Betty Gardner, Bonnie Dodson-Taylor, Bylivian Anderson, Carlos Jones, Carolyn Melvin, Chandra Edwards, Charlene Wolf, Charles Carter, Christopher Sodd, Chrystal Burton, Cleo Washington, Clifford Martin, Clifford Martin, Cloria Thompson, Craig Wilson, Curtis Augustus, Daniel Hill, Danny Lewis, Danton Taylor, David Lee Taylor, Dessie Lee Honor, Detra King, Dondrick Taylor, Dorothy Cox, Earnestine Cleaves, Elaine Stewart, Epsie Collins, Eric Koester, Eric Steward, Evelyn Jones, Freddy Mack Tunstall, Gladys Cheairs, Gwendolyn Bynum, Jaliyah Tabb, James Lewis IV, Jean Anderson, Jenny Ramos, Jeweles Moton, John Smith, Johnnie Taylor, Jonathan Clark, Jose Hernandez, Josie Thomas, Kalisha Carter, Kenisha Hymon, Kenya Cato, Kimberly Malone, Kwesi Twum, Lenora Smith, Leslie King, Jr., Lillian Jones, Lincoln Martin, Loretha Cole, Mae Lay, Marcus Liggins, Marilyn Martin, Marketta Steward, Mary Gray, Melvin Fifer, Michael Crenshaw, Michael Edwards, Micheal Mull, Michele White, Mike Laboe, Milton Burton, Morgan Taylor, Nikkia Jones, Pastor

Andrew Cheairs, Phillip Martin, Queen Martin, Rodney Lucas, Rovenia Dockery-Cotton, Sabrina Taylor, Shelia Sims, Sherry Taylor, Shondra Bassett, Terry Howell, Tina Wallace, Warren Taylor, Willie Peoples, Yolanda Williams

And to those who are no longer with us, but who I know are smiling down at me from Heaven: The thought of how proud you would be if you could witness this moment has been my encouragement throughout this journey. For every lesson taught, every book read, and all the love you lit my world with, this is for you.

Adolphus Davis, Allie Mae Smith, Dorothy Mae Taylor, Euretha King, Mary C. Jones, Frank Shaw Smith, Leslie King, Sr., Lester Jones, Robert Taylor, Sr., Robert Taylor, Jr.

Appendix

Introduction

Dorau, Bethany Groff. "Internet of Things: Overview." Points of View: Internet of Things 1, no. 1 (October 2019): 1–3.

Newman, Peter. "The Internet of Things 2020: Here's What over 400 Iot Decision-Makers Say about the Future of Enterprise Connectivity and How Iot Companies Can Use It to Grow Revenue." Insider Inc., Mar 6, 2020. https://www.businessinsider.com/internet-of-things-report.

Perrin, Andrew, and Madhu Kumar. "About Three-in-Ten US Adults Say They Are 'Almost Constantly' Online." Pew Research Center, July 25, 2019. https://www.pewresearch.org/fact-tank/2019/07/25/americans-going-online-almost-constantly/.

Stack, Brian. "Here's How Much Your Personal Information Is Selling for on the Dark Web." *Experian* (blog). December 6, 2017. https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

US Federal Bureau of Investigation. Internet Crime Complaint Center. *2019 Internet Crime Report.* Washington, D.C., 2019. https://pdf.ic3.gov/2019_IC3Report.pdf.

Waters, Jennifer, and MarketWatch. "Identity Fraud Nightmare: One Man's Story." MarketWatch, February 10, 2010. https://www.marketwatch.com/story/the-rise-of-identity-theft-one-mans-nightmare-2010-02-10.

Chapter 1

Aleisa, Noura, Karen Renaud, and Ivano Bongiovanni. "The Privacy Paradox Applies to IoT Devices Too: A Saudi Arabian Study." *Computers & Security* 96, no. 101897 (September 2020): 1. https://doi.org/10.1086/690235.

Columbus, Louis. "2020 Roundup of Cybersecurity Forecasts and Market Estimates." *Forbes,* April 5, 2020. https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/?sh=22371351381d.

Cybersecurity and Infrastructure Security Agency. "Cybersecurity Glossary." Last modified July 21, 2020. https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.

Meah, Asad. "35 Inspirational Quotes on The Future." *Awaken the Greatness Within* (blog). *Awaken the Greatness* Accessed January 11, 2021. https://www.awakenthegreatnesswithin.com/35-inspirational-quotes-on-the-future/.

Merriam-Webster.com Dictionary. Online ed. s.v. "cybersecurity (n.)." Accessed January 11, 2021, https://www.merriam-

webster.com/dictionary/cybersecurity.

Nappo, Stephane. “Stephane Nappo.” Linkedin, accessed January 16, 2021. https://www.linkedin.com/in/stephane-nappo/.

Salem Press Encyclopedia. 2nd ed. s.v. “Cybersecurity.” Hackensack, NJ: Salem Press, 2019. Accessed January 11, 2021, Research Starters.

Shoemaker, Daniel, Anne Kohnke, and Ken Sigler. *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in* New York: CRC Press, 2020. EBSCOhost.

US Federal Bureau of Investigation (blog). “The Morris Worm 30 Years since First Major Attack on the Internet.” November 2, 2018. https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

US Federal Bureau of Investigation. Internet Crime Complaint Center. *2019 Internet Crime Report*. Washington, D.C., 2019. https://pdf.ic3.gov/2019_IC3Report.pdf.

Warner, Ian. “24 Best Cybersecurity Quotes That Will Blow Your Mind.” *The Habit Stacker* (blog). *Habit* accessed January 11, 2021. https://thehabitstacker.com/cyber-security-quotes-that-will-blow-your-mind/.

Chapter 2

Clark, Meagan. "Timeline of Target's Data Breach and Aftermath: How Cybertheft Snowballed for the Giant Retailer." *International Business Times,* May 5, 2014. https://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056.

Doctorow, Cory. "Personal Data Is as Hot as Nuclear Waste." *The* January 15, 2008. https://www.theguardian.com/technology/2008/jan/15/data.security.

Myers, Lysa. "Target Targeted: Five Years on from a Breach That Shook the Cybersecurity Industry." WeLiveSecurity, December 18, 2018. https://www.welivesecurity.com/2018/12/18/target-targeted-five-years-breach-shook-cybersecurity/.

Parenty, Thomas J., and Jack J. Domet. *A Leader's Guide to Cybersecurity: Why Boards Need to Lead—and How to Do* La Vergne: Harvard Business Review Press, 2019. EBSCOhost.

Perducat, Cyril. "Rethinking Cybersecurity as a Business Priority." *Industry Week,* February 1, 2019. https://www.industryweek.com/technology-and-iiot/article/22027084/rethinking-cybersecurity-as-a-business-priority.

Riley, Michael, Ben Elgin, Dune Lawrence, and Carol Matlack. "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It." *New Yorker,* March 17, 2014.

https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.

Shoemaker, Daniel, Anne Kohnke, and Ken Sigler. *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in* New York: CRC Press, 2020. EBSCOhost.

Chapter 3

Bote, Joshua. "The Internet Is Now 50 Years Old. the First Online Message? It Was a Typo." *USA Today,* updated October 29, 2019. https://www.usatoday.com/story/tech/2019/10/29/first-internet-message-sent-50-years-ago-ucla-using-darpa/4062337002/.

cisa.gov. "Combating Cybercrime." Last modified November 20, 2018. https://www.cisa.gov/combating-cyber-crime.

dhs.gov. "Cybersecurity." Accessed January 31, 2021. https://www.dhs.gov/topic/cybersecurity.

Duke University School of "Cybersecurity Law and Policy: What Are the Top Issues for 2019?" February 6, 2019. Video, 57:19. https://youtu.be/q6SaCWh4QCY.

Goodreads. "Albert Einstein Quotes." Accessed January 31, 2021. https://www.goodreads.com/quotes/110518-if-at-first-the-idea-is-not-absurd-then-there.

Goodreads. “Tim Berners-Lee Quotes.” Accessed January 31, 2021. https://www.goodreads.com/author/quotes/428754.Tim_Berners_Lee.

ITU. “Number of internet users worldwide from 2005 to 2019 (in millions).” Chart. November 30, 2020. Accessed January 31, 2021.

Marion, Nancy, and Jason Twede. *Cybercrime: An Encyclopedia of Digital* Santa Barbara: ABC-CLIO, 2020. EBSCOhost.

McDowall, Mike. “How a Simple ‘Hello’ Became the First Message Sent via the Internet.” *PBS NewsHour* (blog). February 9, 2015. https://www.pbs.org/newshour/science/internet-got-started-simple-hello.

Paxton, Napoleon, and David Branca. *Delivering Superior Health and Wellness Management with IoT and* Switzerland: Springer, Cham, 2020. Springer Link.

Shoemaker, Daniel, Anne Kohnke, and Ken Sigler. *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in* Cybersecurity. New York: CRC Press, 2020. EBSCOhost.

Spangler, Todd. “US Households Have an Average of 11 Connected Devices—And 5G Should Push That Even Higher.” *Variety,* December 10, 2019. https://variety.com/2019/digital/news/u-s-households-have-an-average-of-11-connected-devices-and-5g-should-push-that-even-higher-1203431225/.

Strategy Analytics. "Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030 (in billions)." Chart. May 16, 2019. Accessed January 31, 2021. https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/.

Sussman, Bruce. "Top 20 Cybersecurity Quotes You Need to Hear." *Secure World Expo* (blog). *Secure World* November 14, 2018. https://www.secureworldexpo.com/industry-news/top-20-cybersecurity-quotes.

World Wide Web Foundation. "Sir Time Berners-Lee." Accessed January 31, 2021. https://webfoundation.org/about/sir-tim-berners-lee/.

Chapter 4

Anant, Venky, Jeffrey Caso, and Andreas Schwarz. "COVID-19 Crisis Shifts Cybersecurity Priorities and Budgets." *Our Insights* (blog). *McKinsey &* July 21, 2020. https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets.

Campean, Sorana. "The Human Factor at the Center of a Cybersecurity Culture." *International Journal of Information Security and* 8, no. 1 (June 2019): 51-58. HeinOnline.

dhs.gov. "Cybersecurity." Accessed January 31, 2021. https://www.dhs.gov/topic/cybersecurity.

European Commission. "Human Capital and Digital Skills." Accessed January 31, 2021. https://ec.europa.eu/digital-single-market/en/human-capital-and-digital-skills.

Goodreads. "Learning from Mistakes Quotes." Accessed January 31, 2021. https://www.goodreads.com/quotes/tag/learning-from-mistakes.

IBM. "What is Bring Your Own Device (BYOD)?" Accessed January 31, 2021. https://www.ibm.com/services/digital-workplace/byod.

Native Intelligence, Inc. "Security Quotes." Accessed January 31, 2021. https://www.nativeintelligence.com/resources/security-quotes/.

Shoemaker, Daniel, Anne Kohnke, and Ken Sigler. *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in* Cybersecurity. New York: CRC Press, 2020. EBSCOhost.

Chapter 5

BBC News. "Ross Ulbricht: Silk Road Creator Convicted on Drugs Charges." Accessed February 1, 2021. https://www.bbc.com/news/world-us-canada-31134938.

Bearman, Joshuah and Tomar Hanuka. "The Untold Story of Silk Road, Part 1." May 2015. https://www.wired.com/2015/04/silk-road-1/

CBS "Inside the FBI Takedown of the Mastermind behind Website Offering Drugs, Guns and Murders for Hire." November 10, 2020. https://www.cbsnews.com/news/ross-ulbricht-dread-pirate-roberts-silk-road-fbi/.

Dale, Oliver. "Don't Forget—Why Bitcoin Is Not Truly Anonymous." *Blockonomi* (blog). August 10, 2017. https://blockonomi.com/bitcoin-not-anonymous/.

Duke University School of "Cybersecurity Law and Policy: What Are the Top Issues for 2019?" Feb 6, 2019. Video, 57:19. https://youtu.be/q6SaCWh4QCY.

Farral, Travis. "The Attribution Problem with Information Security Attacks." *Network Security* 2017, no. 7 (May 2017): 17–19. https://doi.org/10.1016/S1353-4858(17)30051-X.

Furnell, Steven, and Samantha Dowling. "Cybercrime: A Portrait of the Landscape." *Journal of Criminological Research, Policy and Practice* 5, no. 1, (February 2019): 13-26. https://doi.org/10.1108/JCRPP-07-2018-0021.

Goodreads. "Cybersecurity Quotes." Accessed February 1, 2021. https://www.goodreads.com/quotes/tag/cyber-security.

Hurlburt, George. "Shining Light on the Dark Web," *Computer* 50, no. 4, (April 2017): 100-105. https://doi.org/10.1109/MC.2017.110.

ISTP Magazine. "The Cyber Society." Accessed February 2, 2021. https://www.itspmagazine.com/the-cyber-society/.

Norry, Andrew. "The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin." *Blockonomi* (blog). October 17, 2017. https://blockonomi.com/history-of-silk-road/.

Shoemaker, Daniel, Anne Kohnke, and Ken Sigler. *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in* Cybersecurity. New York: CRC Press, 2020. EBSCOhost.

Tor Project. "History." Accessed February 1, 2021. https://www.torproject.org/about/history/.

Chapter 6: What is PII

BrainyMedia Inc. "Frank Abagnale Quotes." Accessed February 9, 2021. https://www.brainyquote.com/quotes/frank_abagnale_530058.

Comey, James B. *Homeland Threats and the FBI's* Washington, D.C.: Federal Bureau of Investigation, November 14, 2013. https://www.fbi.gov/news/testimony/homeland-threats-and-the-fbis-response.

Griffin, R. Morgan. "The Scary Truth about Medical Identity Theft." *Feature Stories* (blog). accessed February 9, 2021. https://www.webmd.com/a-to-z-guides/features/scary-truth-medical-identity-theft#1.

McCallister, Erika, Tim Grance, and Karen Scarfone. *Guide to Protecting the Confidentiality of Personally Identifiable Information (Pii): Recommendations of the National Institute of Standards and* Gaithersburg, MD: US Department of Commerce, National Institute of Standards and Technology, 2010. Government Documents Electronic Resources. https://permanent.fdlp.gov/gpo28832/sp800-122.pdf.

Minniti, Robert K. "I Didn't Commit That Crime!" *Fraud Magazine,* July 2016. https://www.fraud-magazine.com/article.aspx?id=4294993877.

Reyns, Bradford W., and Billy Henson. "The Thief with a Thousand Faces and the Victim with None: Identifying Determinants for Online Identity Theft Victimization with Routine Activity Theory." *International Journal of Offender Therapy and Comparative Criminology* 60, 10 (August 2016): 1119-1139. https://doi.org/10.1177/0306624X15572861.

Sigsworth, Marc. "I Was Falsely Branded a Paedophile." *BBC News.* April 3, 2008. http://news.bbc.co.uk/2/hi/uk_news/magazine/7326736.stm.

Smith, Russ. *IP Address: Your Internet Identity.* US Department of Commerce: Washington, D.C., 1997. https://www.ntia.doc.gov/legacy/ntiahome/privacy/files/smith.htm

Sullivan, Bob. "Identity Theft Is Skyrocketing, and Getting More Sophisticated." *Credit.com* (blog). *MarketWatch* February 27, 2018. https://www.marketwatch.com/story/identity-theft-is-skyrocketing-and-getting-more-sophisticated-2018-02-27.

Symanovich, Steve. "What Is Personally Identifiable Information (Pii)?" *ID Theft Resources* (blog). *NortonLifeLock* September 6, 2017. https://www.lifelock.com/learn-identity-theft-resources-what-is-personally-identifiable-information.html.

US Department of Labor. "Guidance on the Protection of Personal Identifiable Information." Accessed February 9, 2021. https://www.dol.gov/general/ppii.

US Federal Bureau of Investigation. Internet Crime Complaint Center. *2019 Internet Crime Report*. Washington, D.C., 2019. https://pdf.ic3.gov/2019_IC3Report.pdf.

US General Services Administration. "Rules and Policies—Protecting Pii—Privacy Act." Last modified on October 8, 2019. https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act.

Chapter 7: Malicious Intent

Anderson, Monica. "Many Smartphone Owners Don't Take Steps to Secure Their Devices." *FactTank* (blog). *Pew* March 15, 2017. https://www.pewresearch.org/fact-tank/2017/03/15/many-smartphone-owners-dont-take-steps-to-secure-their-devices/.

Burkart, Patrick, and Tom McCourt. *Why Hackers Win: Power and Disruption in the Network* Oakland, California: University of California Press, 2019. https://doi.org/10.2307/j.ctvr00xbr.

Cisco. "What Is the Difference: Viruses, Worms, Trojans, and Bots?" Last modified June 14, 2018. https://tools.cisco.com/security/center/resources/virus_differences.

Davis, Jessica. "3 Alabama Hospitals Pay Hackers Ransom to Restore System." *Cybersecurity News* (blog). Health IT Security, October 7, 2019. https://healthitsecurity.com/news/3-alabama-hospitals-pay-hackers-ransom-to-restore-system.

FlexiSPY. "FlexiSPY Unique iPhone Spy App—Reveals Secrets Others Cannot." Accessed February 9, 2021. https://www.flexispy.com/en/iphone-tracker-spy-on-iphone.htm.

Greene, Jim. *Salem Press Encyclopedia of* Academic ed. s.v. "Ransomware." Accessed February 8, 2021, Research Starters.

Harkin, Diarmaid, and Adam Molnar. *The Consumer Spyware Industry an Australian-Based Analysis of the Threats of Consumer* Australian Communications Consumer Action Network: Sydney. August 2019. http://accan.org.au/files/Grants/2017%20successful%20projects/Deakin%20-%20Consumer%20Spyware%20Industry%20%20-%2030Jul19%20WEB.pdf.

Levi, Ran, and Lodrina Cherne. "How is Spyware Legal?" October 2019. In *Malicious Life* Produced by Cybereason. Podcast, MP3 audio, 42:00. https://malicious.life/episode/episode-58/.

Lord, Nate. "101 Data Security Tips: Quotes from Experts on Breaches, Policy, News & More." *DataInsider* (blog). *Digital* updated August 5, 2020. https://digitalguardian.com/blog/101-data-security-tips-quotes-experts-breaches-policy-news-more.

Mozilla. "Story of a Ransomware Victim." *Internet Health Report* (blog), April 2018. https://internethealthreport.org/2018/story-of-a-ransomware-victim/.

Pew Research. "Mobile Fact Sheet." *Internet & Technology* (blog). *Pew* June 12, 2019. https://www.pewresearch.org/internet/fact-sheet/mobile/#mobile-phone-ownership-over-time.

Sanders, James. "Ransomware: A Cheat Sheet for Professionals." *Security* (blog). *Tech* October 22, 2018. https://www.techrepublic.com/article/ransomware-the-smart-persons-guide/.

Sentinel One (blog). "New Malware Threats: Ransomworm Is Coming, Are You Ready?" *Sentinel* February 1, 2017. https://www.sentinelone.com/blog/new-malware-threats-ransomworm/.

Staff. "Cyberattack Still Affecting DCH Hospitals." *Tuscaloosa News.* October 4, 2019.

https://www.tuscaloosanews.com/news/20191004/cyberattack-still-affecting-dch-hospitals.

Taylor, Stephanie. "DCH Hospitals Closed to New Patients after Ransomware Attack." *Tuscaloosa* October 1, 2019. https://www.tuscaloosanews.com/news/20191001/dch-hospitals-closed-to-new-patients-after-ransomware-attack.

The United States Department of Justice. "Ohio Computer Programmer Indicted for Infecting Thousands of Computers with Malicious Software and Gaining Access to Victims' Communications and Personal Information." The United States Department of Justice press release no. 18-21, January 10, 2018. The United States Department of Justice website. https://www.justice.gov/opa/pr/ohio-computer-programmer-indicted-infecting-thousands-computers-malicious-software-and.

US Federal Bureau of Investigation. Internet Crime Complaint Center. *2019 Internet Crime Report*. Washington, D.C., 2019. https://pdf.ic3.gov/2019_IC3Report.pdf.

US Federal Bureau of Investigation. Internet Crime Complaint Center. *2018 Internet Crime Report*. Washington, D.C., 2018. https://pdf.ic3.gov/2018_IC3Report.pdf.

US Federal Bureau of Investigation. Internet Crime Complaint Center. *High-Impact Ransomware Attacks Threaten US Businesses and Organizations*. Washington, D.C., October 2019. https://www.ic3.gov/media/2019/191002.aspx.

Vartanian, Pattyl. “99 Inspiring Cybersecurity Quotes.” *Online Security* (blog). August 8, 2019. https://pinngle.me/blog/99-inspiring-cybersecurity-quotes/.

Chapter 8 Appendix: So Social

Anderson, Monica. “Fast Facts on Americans’ Views about Social Media as Facebook Faces Legal Challenge.” *FacTank* (blog). *Pew Research* December 10, 2020. https://www.pewresearch.org/fact-tank/2020/12/10/fast-facts-on-americans-views-about-social-media-as-facebook-faces-legal-challenge/.

Better Business Bureau. “BBB Scam Alert: Bored at Home? Think Twice before Taking That Facebook Quiz.” Last modified on April 10, 2020. https://www.bbb.org/article/news-releases/16992-scam-alert-that-facebook-quiz-might-be-a-big-data-company-mining-your-personal-information.

Brenoff, Ann. “How a Billion-Dollar Internet Scam Is Breaking Hearts and Bank Accounts.” *Life* (blog). updated July 27, 2017. https://www.huffpost.com/entry/romance-scams-online-fbi-facebook_n_59414c67e4b0d318548666f9.

cisa.gov. “Avoiding Social Engineering and Phishing Attacks.” Last modified August 25, 2020. https://us-cert.cisa.gov/ncas/tips/ST04-014.

Confessore, Nicholas. “Cambridge Analytica and Facebook: The Scandal and the Fallout So Far.” *The New York* April 4, 2018. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Dorf, Serena. “7 Ways Social Media Sabotages Your Cybersecurity.” Cybersecurity (blog). CCSINet, accessed February 24, 2021. https://www.ccsinet.com/blog/social-media-cybersecurity.

fbi.gov. “Romance Scams.” February 13, 2017. https://www.fbi.gov/news/stories/romance-scams.

Fruhlinger, Josh. “Social Engineering Explained: How Criminals Exploit Human Behavior.” *Social Engineering* (blog). September 25, 2019. https://www.csoonline.com/article/2124681/what-is-social-engineering.html/.

Lord, Nate. “101 Data Security Tips: Quotes from Experts on Breaches, Policy, News & More.” *DataInsider* (blog). *Digital* updated August 5, 2020. https://digitalguardian.com/blog/101-data-security-tips-quotes-experts-breaches-policy-news-more.

Ma, Alexandra, and Ben Gilbert. “Facebook Understood How Dangerous the Trump-Linked Data Firm Cambridge Analytica Could Be Much Earlier Than It Previously Said. Here’s Everything That’s Happened up until Now.” *Tech* (blog). *Business* March 19, 2018. https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3#how-is-facebook-implicated-5.

NPR.org. "Facebook Pays $643,000 Fine for Role in Cambridge Analytica Scandal." October 30, 2019. https://www.npr.org/2019/10/30/774749376/facebook-pays-643-000-fine-for-role-in-cambridge-analytica-scandal.

Shoemaker, Daniel, Anne Kohnke, and Ken Sigler. *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in* Cybersecurity. New York: CRC Press, 2020. EBSCOhost.

The Conversation. "Monica Whitty." Accessed February 24, 2021. https://theconversation.com/profiles/monica-whitty-452539.

US Federal Bureau of Investigation. Internet Crime Complaint Center. *2019 Internet Crime Report.* Washington, D.C., 2019. https://pdf.ic3.gov/2019_IC3Report.pdf.

Chapter 9 Appendix: The Privacy Paradox

KeepitUsable. "The Privacy Paradox and How You Can Use It to Increase Conversion." Accessed February 24, 2021. https://www.keepitusable.com/blog/privacy-paradox-and-how-you-can-use-it-to-increase-conversion/.

Lindsey, Nicole. "The Privacy Paradox Could Determine the Next Evolution of Privacy Regulation." *News* (blog). *CPO* November 30, 2018. https://www.cpomagazine.com/data-privacy/the-privacy-paradox-could-determine-the-next-evolution-of-privacy-regulation.

Shoemaker, Daniel, Anne Kohnke, and Ken Sigler. *The Cybersecurity Body of Knowledge: The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in* Cybersecurity. New York: CRC Press, 2020. EBSCOhost.

Technology Networks. "A Privacy Paradox: Why Do People So Readily Give Up Information Online?" April 27, 2020. https://www.technologynetworks.com/informatics/news/a-privacy-paradox-why-do-people-so-readily-give-up-information-online-333948.

TEDx "Online Privacy: It Doesn't Exist: Privacy and What We Can Do about It." October 18, 2017. Video, 14:14. https://youtu.be/LgWrD3EJ1Do.

TEDx "The Coming Privacy Crisis on the Internet of Things | Alasdair Allan | TedxExeterSalon." November 28, 2017. Video, 13:46. https://youtu.be/yG4JLoZRmi4.

Waldman, Ari. "Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'." *Current Opinion in Psychology* 31, (February 2020): 105-109. https://doi.org/10.1016/j.copsyc.2019.08.025.

Chapter 10

Alexander, Brandon. "Protecting Your Privileged Information with Ayana Miller." *Shine Hard Family*. Accessed February 24, 2021. https://www.shinehardfamily.org/interviews/protecting-your-privileged-information-with-ayana-miller?rq=ayana%20miller.

Bass, Lauren. "The Concealed Cost of Convenience: Protecting Personal Data Privacy in the Age of Alexa." Intellectual Property Law Commons 30, no. 1 (Fall 2019): 261-324. https://ir.lawnet.fordham.edu/iplj/vol30/iss1/6.

Consumers International and the Internet Society. "The Trust Opportunity: Exploring Consumers' Attitudes to the Internet of Things." Accessed February 24, 2021. https://www.internetsociety.org/wp-content/uploads/2019/05/CI_IS_Joint_Report-EN.pdf.

Eyeota. "The Audience Technology Platform." Accessed on February 24, 2021. https://www.eyeota.com/.

Hammett, Yvette. "Predictive Policing Is Predictably Controversial." *The Legal* Last modified September 16, 2020. https://www.legalexaminer.com/home-family/predictive-policing-is-predictably-controversial/.

Jones, Rhett. "Roomba's Next Big Step Is Selling Maps of Your Home to the Highest Bidder." *Privacy and Security* (blog). July 24, 2017. https://gizmodo.com/roombas-next-big-step-is-selling-maps-of-your-home-to-t-1797187829.

Lord, Nate. "101 Data Security Tips: Quotes from Experts on Breaches, Policy, News & More." *DataInsider* (blog). *Digital* updated August 5, 2020. https://digitalguardian.com/blog/101-data-security-tips-quotes-experts-breaches-policy-news-more.

Mattu, Surya and Kashmir Hill. “The House That Spied on Me.” *Gizmodo,* February 7, 2018. https://gizmodo.com/the-house-that-spied-on-me-1822429852.

Rani Molla, “People Say They Care about Privacy but They Continue to Buy Devices That Can Spy on Them.” *Recode* (blog). May 13, 2019, 5:40pm EDT. https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security.

TEDx Talks, “How Data Brokers Sold My Identity | Madhumita Murgia | Tedxexeter,” May 23, 2017. Video, 16:19. https://www.ted.com/talks/madhumita_murgia_how_data_brokers_sell_your_identity.

Chapter 11

Abagale, Frank. “‘Never, Ever Use a Debit Card,’ Warns Fraud Expert and Ex-con Artist—Here’s What to Do Instead.” *Make It* (blog). last modified August 30, 2019. https://www.cnbc.com/2019/08/27/debit-cards-are-dangerous-warns-fraud-expert-and-ex-con-artist-frank-abagnale.html.

cisa.gov. “Holiday Online Shopping.” Accessed March 5, 2021.

Hoffman, Chris. “What Is a VPN, and Why Would I Need One?” last modified October 15, 2020. https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/.

Naraine, Ryan. “Microsoft Says Recovery from Malware Becoming Impossible.” April 4, 2006. https://www.eweek.com/security/microsoft-says-recovery-from-malware-becoming-impossible/.

Native Intelligence. “Security Quotes.” Accessed March 5, 2021. https://www.nativeintelligence.com/resources/security-quotes/.

Newman, Caroline. “How Mindfulness Can Help Prevent Hacks, and Four More Cybersecurity Tips.” *The University of Virginia* August 28, 2018. https://news.virginia.edu/content/how-mindfulness-can-help-prevent-hacks-and-four-more-cybersecurity-tips.

Chapter 12

Avast. “83% of Americans Are Using Weak Passwords.” May 2, 2019. https://press.avast.com/83-of-americans-are-using-weak-passwords.

Bass, Lauren. “The Concealed Cost of Convenience: Protecting Personal Data Privacy in the Age of Alexa.” *Intellectual Property Law Commons* 30, no. 1 (Fall 2019): 261-324. https://ir.lawnet.fordham.edu/iplj/vol30/iss1/6.

BBC “Security Footage ‘Viewed by Thousands’.” May 14, 2018. Video, 2:06. https://www.bbc.com/news/av/uk-44117337.

Bradford, Contel. “7 Most Infamous Cloud Security Breaches.” *Recovery Zone* (blog). accessed March 5, 2021.

https://blog.storagecraft.com/7-infamous-cloud-security-breaches/.

Brant, Tom. "SSD vs. HDD: What's the Difference?" last updated September 2, 2020. https://www.pcmag.com/news/ssd-vs-hdd-whats-the-difference.

Dropbox. "How Much Is 1 TB of Storage?" Accessed March 5, 2021. https://www.dropbox.com/features/cloud-storage/how-much-is-1tb.

Hunt, Troy. "The 773 Million Record "Collection #1" Data Breach." *Troy Hunt* (blog), January 17, 2019. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/.

Lord, Nate. "101 Data Security Tips: Quotes from Experts on Breaches, Policy, News and More." *DataInsider* (blog). *Digital* last updated August 5, 2020. https://digitalguardian.com/blog/101-data-security-tips-quotes-experts-breaches-policy-news-more.

Moodie, Michael. "Pros & Cons of External Hard Drives You Should Know." January 24, 2019. https://sleeklens.com/pros-cons-to-external-hard-drives-you-should-know/.

Rubenking Neil J., and Ben Moore "The Best Password Managers for 2021." *PCMag,* last modified February 17, 2021. https://www.pcmag.com/picks/the-best-password-managers.

Chapter 13

Breitinger, Frank, Ryan Tully-Doyle, and Courtney Hassenfeldt. "A Survey on Smartphone User's Security Choices, Awareness and Education." *Computer & Security* 88, no. 101647 (January 2020). https://doi.org/10.1016/j.cose.2019.101647.

Cook, Sam. "35+ Phone Spam Statistics for 2017—2021." *Comparitech* (blog), last updated February 8, 2021. https://www.comparitech.com/blog/information-security/phone-spam-statistics/.

Kok, Kim. "Truecaller Insights 2020 US Spam & Scam Report." *Truecaller* (blog), April 16, 2020. https://truecaller.blog/2020/04/16/truecaller-insights-2020-us-spam-scam-report/.

MSN. "What Is Online Enticement and How Is It Happening?" May 14, 2018. https://www.msn.com/en-us/news/missingchildren/what-is-online-enticement-and-how-is-it-happening/ar-AAxgr85.

Murray, Gina. "IRS Scam Phone Call: How to Protect Your Loved Ones." *Aware Senior Care* (blog), September 15, 2016. https://awareseniorcare.com/new-irs-phone-scams/.

O'Donnell, Brenna. "Rise in Online Enticement and Other Trends: NCMEC Releases 2020 Exploitation Stats." *Missing Kids* (blog). *National Center for Missing & Exploited* February 24, 2021. https://www.missingkids.org/blog/2021/rise-in-online-enticement-and-other-trends--ncmec-releases-2020-.

Power, Richard. "Child Identity Theft." CyLab, accessed March 8, 2021. https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf.

Protect Seniors Online. "10 Cybersecurity Best Practices for Older Adults." Accessed March 8, 2021. https://www.protectseniorsonline.com/resources/cybersecurity-best-practices/.

Salem Press Academic ed. s.v. "Child Pornography." Amenia, NY: Salem Press, 2019. EBSCOhost.

Schulyer, Kailey. "Spike in Online Enticement Reports Amid Pandemic." *WAFF News,* January 27, 2021. https://www.msn.com/en-us/lifestyle/parenting/spike-in-online-enticement-reports-amid-pandemic/ar-BB1d902f.

State of California Department of Justice. "Protect Your Computer from Viruses, Hackers, and Spies." Accessed March 13, 2021. https://oag.ca.gov/privacy/facts/online-privacy/protect-your-computer.

Stunson, Mike. "Kansas Man Tried to Purchase Kentucky Child for $500 and Meth. He's Going to Prison." *Lexington* last updated October 23, 2018. https://www.kentucky.com/news/local/crime/article220490995.html.

US Department of Homeland Security. Cybersecurity and Infrastructure Security Agency. *Cybersecurity and Older Americans.*

Washington, D.C., 2019. https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20and%20Older%20Americans.pdf.

US Federal Bureau of Investigation. "Elder Fraud." Accessed March 8, 2021. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud.

WBKO News Staff. "Kansas Man Sentenced after Attempting to Buy Kentucky Child Online." *WBKO*. October 23, 2018. https://www.wbko.com/content/news/Kansas-man-sentenced-after-attempting-to-buy-Kentucky-child-online-498339231.html.

Conclusion

Lazic, Marija. "39 Worrying Cybercrime Statistics." *LegalJobs* (blog), February 26, 2021. https://legaljobs.io/blog/cyber-crime-statistics.

Meharchandani, Dhwani. "Staggering Phishing Statistics in 2020." *Security Bloggers Network* (blog). *Security* December 7, 2020. https://securityboulevard.com/2020/12/staggering-phishing-statistics-in-2020/.

US Federal Bureau of Investigation. Internet Crime Complaint Center. *2019 Internet Crime Report*. Washington, D.C., 2019. https://pdf.ic3.gov/2019_IC3Report.pdf.

We Live Security. "ESET Cybersecurity Barometer." Accessed March 10, 2021. https://www.welivesecurity.com/wp-

content/uploads/2019/01/ESET_BAROMETER_USA.pdf.