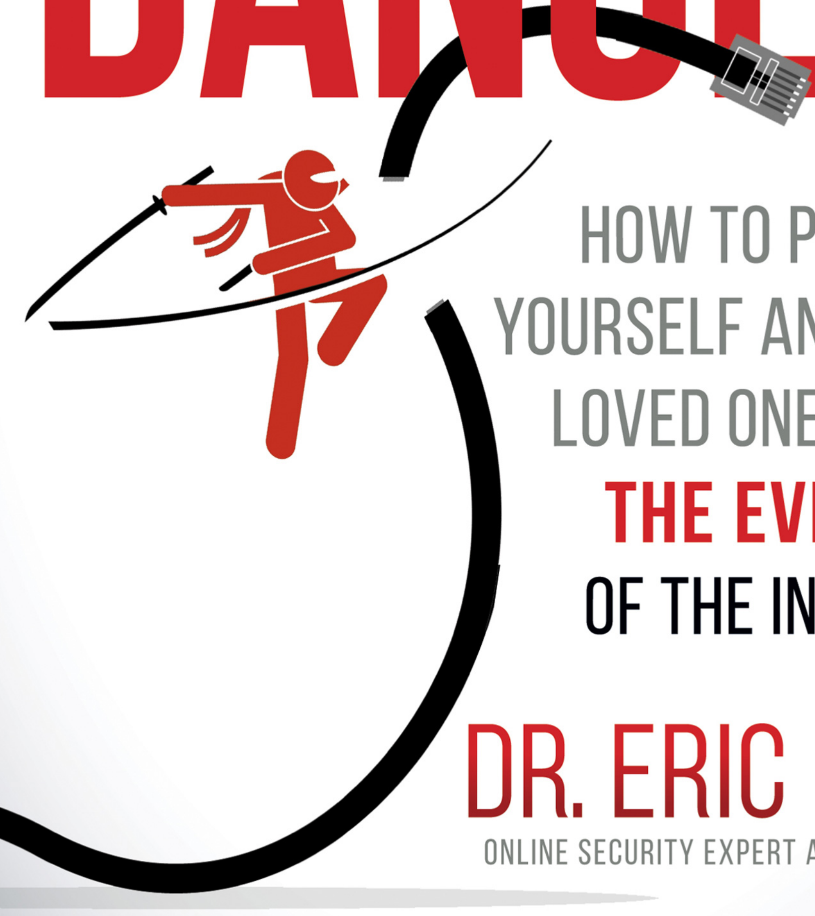
ONLINE DANGER



HOW TO PROTECT YOURSELF AND YOUR LOVED ONES FROM **THE EVIL SIDE** OF THE INTERNET

DR. ERIC COLE

ONLINE SECURITY EXPERT AND CYBER NINJA

CHAPTER 1

THE NEW WORLD ORDER

Do you spend more money on coffee and treats at Starbucks than you do on cybersecurity? In the grand scheme of things, which one is more important? When it comes to your and your family's cybersecurity, do you opt for a skinny latte or a double shot of espresso?

In a world that is changing at a pace never before seen in our history, astonishing advances in technology play out before our eyes. With the advent of personal electronics, I often wonder, how did we ever survive without cell phones, tablets, and computers? How did we occupy our days, nights, and weekends?

My teenagers spend most of their time in front of a device, communicating with their friends. And hell hath no fury like a teenager grounded from cell phone privileges. When you take away electronic devices from teenagers or children, it is as if you are taking away their identity and, in fact, their very existence. Today's kids have no idea what to do, or in a scarier sense, how to operate without their electronics.

Whether we realize it or not, and most often kids do not, these devices have us living in a fully connected world in which almost every action we take leaves behind a digital fingerprint. It is easy for us to focus on all the new and enhanced functionality in our interconnected world, but we also need to consider the new dangers that accompany the technological advances.

Behind every email, every website, every packet that your computer receives, lurks the possibility of a malicious code with the potential to rock your world. Embarrassment, legal implications, financial loss, and even your identity are at stake. There is a new world order, and if you are not prepared, you can wind up on the short end of the stick, the victim of cyber criminal activity.

Organizations in Russia, China, and other locations work 24/7/365 to steal and exploit your digital information. The only question you have to ask: do you want to be a target? If you are not actively addressing online security, your default answer to that question is YES.

Most of us have done little to protect ourselves in a digital world. From experience, I can tell you that the cyber adversary plays a very effective offense. If you're not prepared to respond—or even better—to counter with a comparable effective defense, you are going to lose, and the losses can be significant. This book will teach you the tips and tricks of a vigorous cyber defense.

PERCEPTION OF SECURITY

When I meet people at parties or airports, and they ask what I do, I tell them that I work in cybersecurity. Many people exclaim that it must be the coolest job. But people's responses have not always been so positive. Fifteen years ago, that same career conversation garnered me some weird looks, like I was the smelly kid on the school bus.

Old-school thinking was that cybersecurity existed only for governments with classified information and for large companies with proprietary secrets to protect. Today, everyone—every single individual of any age—needs cybersecurity, and I consider myself blessed to work in an industry that is helping to make the world a safer place.

If you are not convinced that everyone needs cybersecurity, please turn on the television or pick up a newspaper and read the most recent—and the ongoing—reports about cybersecurity breaches. No company or government is immune to today's cyber adversaries; it seems that every aspect of commerce or communication, government or global entity can be compromised. And, are you ready for the scariest information of all? Most breaches pass undetected or unreported, so what you see or read about reflects only a small piece of the problem.

Those of us who work in cybersecurity call this perception the "iceberg effect." What you can see of an iceberg above the waterline represents a small percentage of the overall problem because most of an iceberg hides underwater, invisible and dangerous. The state of cybersecurity looks bad, but like the looming iceberg, the problem is a lot worse than most people realize.

Despite more than twenty years of rapid technological change, the average person only recently began recognizing cybersecurity as a problem to be addressed. The dangers in online interactions have always existed, but the problems are just now unfolding as an epidemic. No matter your age, background, or location in the world, if you use electronic devices, you must be vigilant about cybersecurity, and this book is written for you.

FALSE PERCEPTIONS MAKE YOU A TARGET

Leaked photos from a celebrity smartphone. A presidential candidate's leaked emails. Embarrassing voicemail messages left by a future king. Only celebrities get hacked, right?

WRONG.

Just like celebrities, you own a bank account, carry a credit card, and fill out online shopping forms—creating digital data in a wide variety of other ways. That personally identifiable information, or PII, forms your electronic identity. PII is priceless, regardless to whom it belongs.

Cybersecurity lingo includes the word "harvesting." Think of the cyber adversary as a farmer. Cyber crime is a risky business, and not every seed will sprout into a profit-yielding crop. But, just like in legitimate farming, a bigger harvest usually equals a better profit.

A massive field might be too much for one farmer to handle, and the same holds true for the cyber criminal. Breaking the harvest into smaller parts, and different plants, makes for an easier yield. This strategy, too, works for the hackers.

To be more specific, breaking into one large organization to steal 5,000,000 records works for cyber thieves, but larger companies can deploy tough defenses. On the other hand, most individuals have little-to-no security protecting their online identities and assets, making it much easier for hackers to break into 5,000,000 individual computers to steal personally identifiable information. The net effect remains the same: big profit for cyber criminals and big losses for their victims.

Cyber adversaries also favor so-called "watering hole attacks." Hackers target large sites accessed daily by millions of people, infiltrating cyber defenses for short periods of time. Even when the compromise of a major site lasts for just sixty minutes, it will net a significant harvest for the cyber thieves.

Wherever you go in cyberspace, and whoever you are, evil exists, and you need to be prepared.

And, instead of getting better and safer, the dangers and challenges of cyber defenses multiply every day.

Twenty years ago, I worked a compromise of 10,000 stolen records (i.e. credit cards, personal information), which was considered a large-scale incident. I told a friend that if we ever got to the point when 100,000 records could be stolen, that would signal trouble.

A few years later, working a case with 100,000 stolen records, I insisted that a million stolen records would signal that the situation was out of control. Just a few years later, we reached that million-records breached mark. Still, I would not give up. I contended that tens of millions of records stolen would result in chaos. Sure enough, a few years later it happened, and today we're edging towards a billion stolen records as the new norm.

It might be easy to blame third parties—banks, retail stores, the government—for not protecting your information. Certainly, those institutions and companies should be held accountable. But ultimately, each one of us, each individual, must accept responsibility for keeping our personally identifiable information properly protected.

The bottom line: when your identity and personal information are compromised, you are the one left to deal with the repercussions. Not the credit bureau, the retailer, or the government agency—though they may take steps to support your recovery. Nonetheless, if you want to win in cyberspace, YOU must take responsibility for your own protection and implement security today.

DEFENSE IN DEPTH

No single solution can make you 100 percent secure. That lack of absolute protection fuels a billion-dollar cybersecurity industry, where cyber breaches dominate consumer news.

Long ago, I coined a key phrase, “Prevention is ideal, but detection is a must.” Truly, you will not be able to stop all attacks, but you should make it your goal to minimize or control the damage. You can start by implementing a variety of defenses, such as endpoint security, but you must also recognize those measures—all of them—can be bypassed by expert cyber criminals. You must always be alert for signs of an attack. When you notice unusual activity, do not ignore it; take immediate action.

Traveling through an airport, you often see signs imploring, “If you see something, say something.” The same philosophy holds for personal protection. If you see strange activity, call the bank or credit card company and investigate the questionable charges. The sooner you detect an intrusion and take action, the more you can control—and perhaps limit—the damage.

“Defense in depth” is another common term in the cyber industry, and the term means to deploy multiple defense measures to protect your system. Defense in depth is all about diversifying your portfolio.

Consider your 401k or other savings: No smart investor puts 100 percent, or even 90 percent, of their assets in one fund; that plan would be way too risky. Instead, investors diversify, so that if one fund fails, the other investments minimize the impact on the total portfolio.

When you think of security, you need to identify multiple levels of protection and never depend on a single mechanism to make you secure. Take a moment and think of the possible layers of physical security for your home: You might live in a gated community, have an alarm system installed, and own a large dog named Fido that roams the halls. You might also sleep with a pistol in your nightstand and possess the martial arts skills of a certified ninja. Think of cybersecurity in the same manner: Be a cyber ninja.

Can you think of at least three different measures that you have put in place to protect your personal information online? If you cannot, this book is for you.

If you can name three measures that you've implemented to protect your PII, continue reading because there is no such thing as too much security. The ultimate question is: how effective is your overall security?

No matter your answer, do not let yourself become complacent. Adversaries are very smart and constantly aggressive, and the moment that you take your online security for granted, you make their job easier.

SECURITY 101

This entire book focuses on security and powerful knowledge to keep you, your family, and your company as safe as possible. Every chapter contains actionable steps that you can take to minimize your chance of compromise. To start, let's look at four basic cybersecurity principles.

1. **Always run the latest version of any software you install**. This principle applies to all software, including a device's operating system. Most software vendors, especially Microsoft, constantly improve product security and add new levels of protection.

   For example, Microsoft made huge changes and increased security from Windows XP to Windows 10. If you are running Windows XP, and you connect to the Internet, your system is highly vulnerable and probably has been compromised. Outdated software is the greatest gift you can give the adversary. Keep reading to understand why.

2. **Do not put off installing patches from software vendors.** Bugs, vulnerabilities, or exposures constantly pop up in software. Vendors release fixes, or patches, to eliminate these problems. A patch is the vendor telling the world that a weakness exists in its software. Adversaries, who recognize that many people do not properly patch their systems, actively develop exploits and try to quickly break into the vulnerable software. The longer it takes you to patch, the greater the chance of compromise.
3. **Uninstall any software that you do not use.** Software programs, especially unused and outdated ones, create opportunities for adversaries. Think of each software program like a window in a house. The more windows in a house, the more opportunities an adversary has to break in. It only takes one unlocked window for your house to be vulnerable to a robbery.

   A computer is like a house. The more software programs installed, the more points of potential exposure an adversary can try to exploit to break in. Install and use as much software as you need, but get rid of any programs that go unused or are replaced by new or different ones.
4. **Never log in using an administrator account for daily activity; always log in as a normal user with limited access or privileges.** An administrator can do anything on a system and can bypass most of the security controls. When (notice I use the word "when," instead of "if") your account gets compromised, the adversary will have the same level of system access you have. If the administrator account gets compromised, the

adversary gains total access to everything on your system. On the other hand, if an adversary gains access to your system as a simple "user," there will be some information that cannot be compromised.

You always want to operate with the least amount of privileges. Follow the golden rule of "never, ever surf the web or check email as administrator." Surfing the web as an administrator is like driving a motorcycle without wearing a helmet. You might not get into an accident today, but it is a very risky thing to do. Do not take chances when it comes to your personal protection.

THE TWO MOST DANGEROUS APPLICATIONS

In fact, can you name the two most dangerous applications on planet Earth? What programs have caused more harm, more damage, more identity theft, and more monetary damage than any other applications? Nope, it's not Angry Birds or Candy Crush. The answer: email clients and web browsers.

Yes, email and web browsers are the conduits of most evil and are the tools of choice for the adversary to cause harm. More specifically, the harm and damage lie in opening email attachments and clicking on links to illicit websites.

Many people do not realize that email is not an authenticated method of communication. The source address listed has little to do with who the email came actually from. This information can easily be spoofed, and your mail server does nothing to authenticate the origin of the email. Even though an email might look like it came from a trusted source, do not believe it.

The good news is that receiving a standard email typically does not cause harm directly. Instead, the danger lies in opening an attachment that allows a system to be infected. In fact, users are their own worst enemy, as they are tricked into actions that ultimately cause harm to themselves.

A wide variety of trusted online repositories, like Dropbox, offer a much better way to transfer documents. These sites require both parties to authenticate their identities in order to upload or download documents.

While there is a wide range of attacks that can be done via the web, security advice can be reduced to, "Be careful what links you click on." Adversaries like to send a link (via email) that looks legitimate but when you click it, malicious code activates that can compromise your system or steal your credentials. For any site that you visit on a regular basis, it is much safer to bookmark it rather than click on an embedded link.

I will cover this in more depth later, but here is one of the most critical pieces of advice I can offer: do not click on attachments or web links unless you are 300 percent sure they are legitimate. And here's more essential advice: Never, ever click on a link that looks like it came from your bank or the IRS. If you implement only these two practices, you will be saved a lot of money and heartache.

BUT I HAVE ANTIVIRUS SOFTWARE

After I speak at conferences, people often tell me that they feel safe because they have endpoint security or antivirus software installed on their systems. While a very important thing, installing these programs does not give you permission to be careless—or foolish. Endpoint security and web-filtering programs minimize common types of attacks, but more advanced malware can bypass these mechanisms and infect your system.

To return to our car analogy, wearing a seat belt in a car is a good idea, but it does not mean that you will not get into an accident or get hurt. Even when you wear a seatbelt, you still should be very careful when you are driving. Navigating the complex world of cyberspace is no different: even when you have antivirus software, you need to be careful.

Additionally, remember that adversaries are very clever and very smart—they do not like to get caught. Therefore, they constantly look for ways to get around antivirus and endpoint security protection. The game, often referred to as "attacker leap frog," works like this:

- The bad guys constantly look for ways to bypass current security measures and compromise your system.
- When the adversary is successful, the cyber defenders at security software companies actively work to figure out ways to defend against these attacks and stop the adversary.
- When the cyber good guys successfully stop the attacks, the adversary figures out a different way to bypass the software. And, the game continues indefinitely.

So, in addition to installing these measures, you must also keep your antivirus and endpoint security software up to date. Do not let the annual license costs deter you—these programs play an important role in cybersecurity.

WHO IS TARGETING YOU?

Slime balls.

Scum of the earth.

Just as immoral and unethical people populate our physical world, they also exist in cyberspace.

My blood still boils when I think of a particularly nasty cyber attack that targeted widows of police and firefighters after the terrorist attacks of September 11, 2001. An email circulated, which appeared to offer help to those families with their loss and to handle compensation benefits for free. In reality, the adversary gathered PII, accessed bank accounts, and wiped out the savings of many survivors.

Essentially, the slime balls stole the financial security of many defenseless people and targeted people who had just lost their loved ones. If people who behave like that are not the definition of the scum of the earth, I do not know who or what is.

We all face similar types of danger in the cyber world. Adversaries will strike when you are most vulnerable; they search for those weaknesses and exploit them as opportunities. Be suspicious. This is not to say you have to be miserable, but truly, trust no one.

CONSIDER YOUR CHILDREN

Kids have not been exposed to evil, and therefore they do not understand or anticipate it, especially in cyberspace. That naiveté can lead to unwise social media choices and relationships. Over several months, the predator builds a relationship with your child, and at some point, the slime ball will ask for your child's address or will discover where the child attends school. The cyber stalking now gets real by becoming physical stalking, and the predator either approaches and/or abducts the child. I wish this scenario was a one-off case, but it happens a lot more times than you would believe.

I know that some readers do not want to accept that such horrible things could happen, or worse, that you could unwittingly play a part in it. Those readers will dismiss this section. Or perhaps as a defense mechanism against the overwhelming evil of such situations, some readers will try to convince themselves that this kind of scenario is simply not true, but rather it is the result of Internet myths. Either way, denying the potential evil and harm that exists in cyberspace is a very unwise thing to do.

The golden rule of being safe online is that anything you say and do, can and will be used against you by slime balls. One of the main goals of this book is to offer new, real-world perspective and to re-train people's brains and behaviors to respond to what's really happening online.

For readers in denial: Please, you need to accept that the way you currently see the world is naïve and incorrect. Based on this newfound insight, you must continually ask yourself, "What do I gain and what do I lose by performing these actions?" It is also a good idea to always ask, "How could this information be used to target me or my family?" You absolutely must start to change your activity.

SURVIVAL OF THE FITTEST

Two general types of attacks exist in cyberspace: opportunistic attacks and targeted attacks. Most attacks, with monetary impact and negative outcomes, are opportunistic attacks that can be avoided. Opportunistic attacks target a large population, recognizing that only five percent of the targeted group will become actual victims—but five percent of 10,000,000 is a significant number.

The good news? You do not have to be in that five percent of victims.

On the other hand, targeted attacks are specifically aimed at an individual or entity, and they are often the work of a foreign government or organized crime. I will be honest: if you are the sole target of a cyber attack, you have bigger problems than the state of your cybersecurity. You need more help than this book can provide.

Fortunately—or not—targeted assaults typically focus on large organizations with significant amounts of valuable information. If you follow the tips and tactics in this book, you should be able to avoid, or at least minimize, the potential of ever being the focus of a targeted attack.

And, with that in mind, we will concentrate on implementing protection against opportunistic attacks.

If you are alive, which I am assuming you are since you are reading this book, you already know something about how to survive.

Like in nature, cybersecurity bases itself on survival of the fittest. If you do not adapt, you do not survive. A key component of survival is common sense. Common sense tells you not to stick a fork in an electrical socket or to open the door to a stranger at two o'clock in the morning.

Most people acquire and build a strong, robust set of intelligence that enables them to make good choices and avoid bad decisions. The key to a safe and happy life: do not do stupid things. If you apply those very same principles to cyberspace, you will win and the adversary will lose. Summarizing this entire book in one phrase: remember, everyone on the Internet could be out to get you, use your common sense.

For some puzzling reason, when many people connect to the Internet, they act as if all common sense goes out the window. Because of this mindset, the amount of stupidity that occurs in cyberspace is mind-boggling. If people behaved in the real world the way they do in cyberspace, the population of planet Earth would be significantly less.

The Internet is a completely open, untrusted network. Most forms of online communication contain little-to-no built-in authentication, which would verify a degree of safety. Spoofing, or impersonating, another individual is simple and effortless to perform with online communications.

Let's take social media for example. Go ahead, pick one of your favorite social media platforms and ask yourself a simple question: when I setup my account, what did they require to authenticate or prove that I am actually who I claim to be? The answer: absolutely nothing. Anyone can set up almost any account without verification. Yet most people accept social media accounts at face value and believe those accounts to be authenticated and verified.

INSTANT CYBERSECURITY

Are you intimidated by—or wishing you possessed—the skills of elite cybersecurity specialists? Let me quickly introduce you to one of their most powerful strategies: Limit the external exposure of your system and devices.

When you buy a brand new computer, unpack it, and turn it on, the computer most likely exists in a secure state. (Sure, as you see in spy movies, shrink-wrapped software can be infected with malware, but it usually happens on specialized devices and is discovered quickly.)

If you use that computer in its isolated state—never connect it to the Internet, never install any software—it will stay in a secure state. External contact causes infections and exposes personal information. The most common external source of contact is the Internet, closely followed by external devices like USB devices or storage devices. If you can control those two items and carefully monitor any external software introduced to your computer, you have essentially mastered the tools of the elite.

MAJOR COMPROMISE VERSUS MINOR COMPROMISE

The idea of abstaining from all Internet connection is enough to make the average person's head explode. How would we get anything done?

While not practical for everyone, I will share one easy and effective solution for your personal devices.

First, ask yourself what a major cyber compromise versus a minor cyber compromise would look like in your life. What is the difference between a computer infection that leaks personal information compared to an annoying yet minor virus? The personal value you attach to your data determines the gravity of the compromise.

Cybersecurity and cyber hygiene come down to a simple principle: protect your data. The best method, if you can afford it, starts with owning two computers or personal devices.

Use one device for all of your personal information: taxes, bank accounts, passwords, and more. Use that device ONLY for those purposes. If you bank online, connect to the Internet and only go to the bank site, nothing else. When you are done, disconnect from the Internet—no email, no web surfing.

The other device should NEVER contain sensitive or personal information. Use it only for email and web surfing. If this electronic gets compromised, the impact is minimal because all of your high-risk data resides on a separate drive—on the other, secure-use-only device. If you can swing that second device, you can sit back, smile, and say “I got this.” Who knew that cybersecurity was so easy?

WHY IS THIS HAPPENING?

When I attend cybersecurity conferences or deliver corporate keynote addresses, I am often asked, “With all of the security software and technologies available, why does cyber crime continue to grow?”

It is true. Even with the vast sums invested in security, and an increasing focus on embedding security into software, the problem seems to be getting worse, not better. There are many reasons for this.

First, just like in the physical world, dangers exist all around us, and we have learned to operate in a manner that minimizes our exposures to those threats. In the real world, we have history, experience, and an extensive knowledge base of how to operate to avoid getting hurt. The problem is, in cyberspace, we have a very short history, few experiences, and a small or non-existent knowledge base.

Many of us are the first generation exposed to cyberspace, and therefore, we have little to no knowledge to pass on to our children. In fact, in many cases, our children are smarter and more efficient on technology than we are, but because they are also naïve about the dangers in the world, they often become targets of cyber stalking, cyber bullying, and other cyber crimes.

Second, sophisticated adversaries constantly adapt and change how they compromise systems. Each time the good guys introduce new security measures, the bad guys identify weaknesses and develop ways to bypass increased controls.

FUNCTIONALITY LEADS AND SECURITY FOLLOWS

A third reason for the continued growth of cyber crime reflects the very powerful concept, which is worth understanding in any area of our lives, that functionality leads and security follows.

When new technology emerges, vendors and users focus on functionality, and in general, they either do not consider security or view it as an unneeded expense. They have a mentality of, “Look what we can do now!” versus one of “How can this open new doors to harm?” Or, “How can this great new product be used against us?”

As time passes and people engage with the product, users begin to understand the potential—or actual—dangers, and then, people become willing to pay for security and solutions. Of course, the problem with this approach is that people have to be negatively impacted before vendors implement change. We are reaching that point in cyberspace.

We see this progression in the auto industry. When first manufactured, cars did not have seatbelts, airbags, or anti-lock brakes. Only after people started suffering harm did we realize that cars needed these safety features. I remember when the seatbelt law passed in New York in 1984. People were freaking out—they actually used bolt cutters to remove seatbelts, as a form of protest.

Today, that mentality seems galactically stupid. A seatbelt serves to help you and increase your security, but people hate change. I am assuming that since you are reading this book, you want to change. When you read the advice I give, do not fight it, but instead, embrace it and recognize that it is meant to help you.

Like cars and other innovations, computers, electronics and software were built with an eye on functionality and life-enhancing features; security developed as a response to problems discovered in usage. And, truth be told, many vendors are reluctant to change their focus to include more security features. Software companies that make operating systems want to make money. Those companies make money by making customers happy. Customers are happy when things work. Customers are angry when things do not work.

Facing those basic demands, manufacturers believe they are left with two options. Option one, turn on all functionality and turn off security, so everything works out of the box, and everyone stays happy (well at least initially, until they get compromised).

Option two, turn all connected functionality off, properly securing the application, but nothing works, and customers get angry. The second solution will cost software companies less money in the long run, with fewer patches and fixes. Just talk to an identity theft victim and ask them how much of their time a compromise cost them. They will quickly agree option two is better in the long run.

Unfortunately, the short-term drives most decisions, and option one wins. Do not feel hopeless. Most software today contains embedded, or built-in, security with features you can maximize. However, remember that while most computers, most operating systems, and most applications hold the potential to be secure, that security usually does not exist in the default state.

Don't leave your personal security entirely in the hands of someone else. Whenever you use any technology keep telling yourself, "This is not secure, and it can hurt me if I am not careful." The more you think about the negative consequences, the more protected you will be, and the smarter the decisions you will make.

CYBERSECURITY CAN BE AS PAINFUL AS PARENTING. THAT SAYS A LOT.

Quite honestly, a lot of security products miss the mark and neglect the root causes of cyber risk. Some applications do good things, but focus on the wrong things.

In fact, when I work with CEOs after major cybersecurity breaches, I often think of situations that parents encounter.

This year, when my son started high school, he came home the second week of classes and asked for my help. He said, "Dad, I just found that we are having a surprise quiz tomorrow, and I was wondering if you could help me study?"

Being the supportive dad, I said yes, but I was confused. Unless they changed the definition of "surprise," how did he know he was having a surprise quiz?

I asked him, with some hesitancy, how he knew about this alleged, surprise quiz. To be totally honest, I was cautious because like his dad, my son knows quite a bit about cybersecurity. Did he hack the teacher's computer? Being a security professional, I feared I faced a moral dilemma. If he broke into the system, should I high-five him for being clever or should I punish him for hacking?

Fortunately, the answer did not lie in cyber crime (whew), so I did not have to resolve that inner conflict. Apparently, the teacher told the students about a planned quiz on a surprise TOPIC.

I asked my son which subjects the teacher emphasized. He thought for a moment and answered mathematics. So we studied math. I gave him sample problems, and he got them all wrong. We worked together for three hours before it finally clicked. The next day he woke up for school confident and ready to take the surprise quiz.

I happened to be working from home that day, and I greeted him at the door when he arrived home. With a big smile I asked about the surprise quiz.

With his head hung low, he said it was rough. I tried to be encouraging—he knew that math inside out! "Dad," he said, "the quiz was on history. I wasted three hours studying when I could have been doing something much more useful like playing video games." (You have to love the mind of a sixteen-year-old and what he thinks is important.)

Undaunted, I tried to explain to him that the time he spent studying mathematics was still a good investment of his time, regardless of the surprise quiz and his score on it. He is going to need that math knowledge not only in high school but also in college. I am not sure he agreed.

This conversation is very similar to the ones I have at a corporate level. Organizations spend millions of dollars on security, and still, their systems get compromised. Despite best intentions, it can be impossible to know exactly how that "surprise" cyber attack will surface.

I walk into offices after a breach and the CEOs have their heads down. After a big sigh, they assert that the millions of dollars spent on security were wasted because systems were compromised anyway. As with my son, I explain that, without the investment, the damage would have been worse. The protocols deployed laid a solid foundation; however, in terms of stopping the adversary, it was not the right thing to do, and that is the fundamental problem.

You might be asking, what is the right thing to do when it comes to personal security? I refuse to leave you in too much suspense: protect and minimize the exposure of your sensitive information. The more you protect your critical information, the less overall damage an adversary can cause.

Some simple questions you should frequently ask yourself:

- What is my critical information or data that would cause harm if exposed?
- Where does that information or data exist?
- How can I better control or manage it?

As you think about and protect your data, you become a more and more unattractive target for an adversary.

READY, SET, GO!

Our new, interconnected world order presents boundless opportunities. But the same tools and technology present themselves to adversaries. In cyberspace, much as in the real world, anything that can be used for good can also be used for evil purposes. On the other hand, as long as we remind ourselves every day that we can become a target, and if we think before we click, we can reduce the harm that awaits us on the next website.

We CAN protect ourselves, our families, our companies, and the world we live in. The same skills that allow us to survive in the real world will protect us in cyberspace.

Here is what you need to remember to earn your cybersecurity black belt:

- The potential payday in cyber crime is enormous, so attacks will only worsen. As soon as investigators shut down one method of attack, adversaries adapt and find new techniques.
- Cybersecurity is often an afterthought. Designers first build devices that work well, and then consider security. Safety measures are often restrictive, so in the struggle between security and functionality, an efficient device comes out ahead.
- When your most commonly used programs issue new versions, upgrade. Instead of pinching cyber pennies, invest in improved software that is often more secure than older versions.
- Do not ignore those update reminders. When patches and updates to current versions of software are released, it usually is in reaction to known problems. Do not leave your systems vulnerable.
- When spring cleaning, do some cyber scrubbing, too. Uninstall all unused programs and eliminate potential problems.
- Always be yourself, and never be the administrator. Limiting use of the administrator account limits opportunities for major disaster if a system is breached.
- Email clients and web browsers are the two most dangerous applications in cyberspace. Email was never designed to be secure, and web links are vehicles for serious cyber attacks.
- Antivirus software is an important cybersecurity tool, but it should not be your only one. Adversaries work to circumvent the safety measures in software protections. Keep your antivirus software current and supplement your cybersecurity with some of the other tools and strategies I will introduce in later chapters.

- ✦ As dangerous as cyberspace is for you, the potential dangers for children are even greater. Never let go of a child's hand in this digital world.