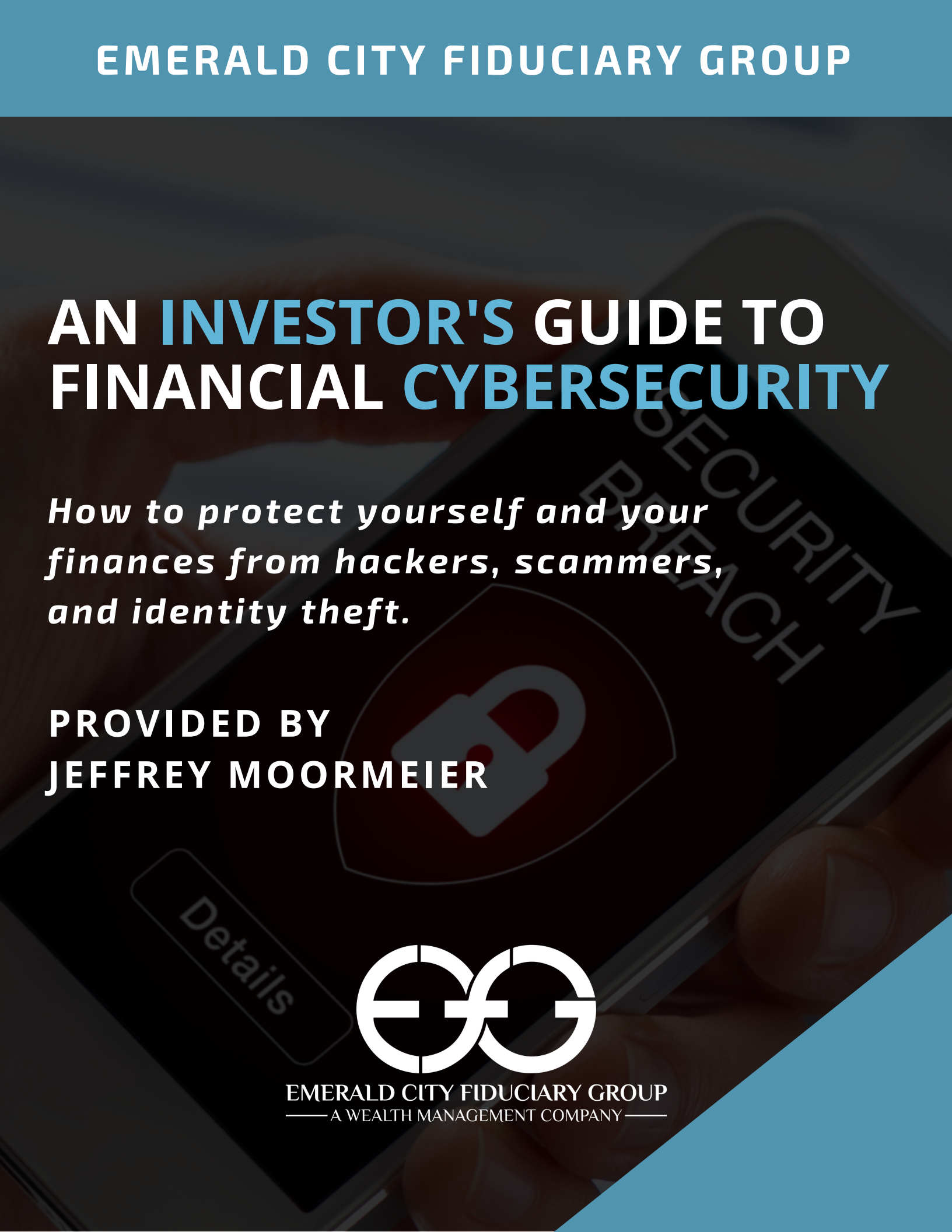
EMERALD CITY FIDUCIARY GROUP

AN INVESTOR'S GUIDE TO FINANCIAL CYBERSECURITY

How to protect yourself and your finances from hackers, scammers, and identity theft.

PROVIDED BY
JEFFREY MOORMEIER



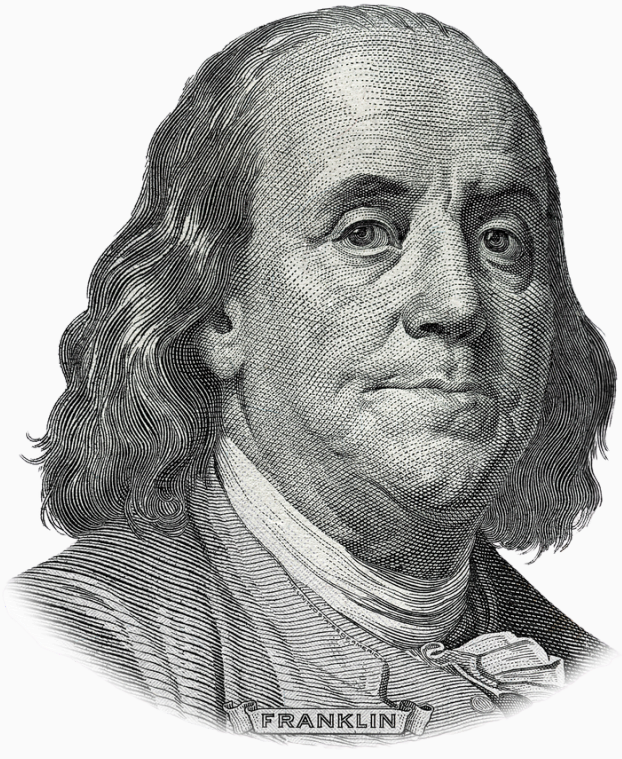
EMERALD CITY FIDUCIARY GROUP
A WEALTH MANAGEMENT COMPANY

It's time to understand…

THE IMPORTANCE OF FINANCIAL CYBERSECURITY

"An ounce of prevention is worth a pound of cure."

- Benjamin Franklin



INTRODUCTION

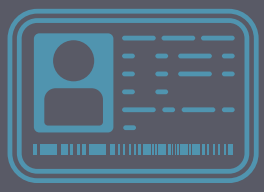
It has become far too common an occurrence to turn on the evening news and hear a story about another scam that's made its way into our community. Or to switch on the radio during your morning commute and learn that some massive corporation has been hacked.

Technology has changed dramatically over the last couple of decades. Most of those changes have been for the better. Personal computing makes it easier to get more work done. The internet has put a wealth of knowledge at everyone's fingertips. Thanks to smartphones and other mobile devices, it's easier than ever to stay connected with friends and family. And because credit and debit cards have largely replaced cash and checks - not to mention the rise of mobile payment apps like Venmo and PayPal - we now have greater access to our money whenever and however we need it.

But these same advancements have also made it easier for hackers, scammers, and fraudsters to steal from people. When it comes to protecting ourselves from theft, we now worry less about a masked burglar stealing the family jewelry. Instead, the greater danger is that someone thousands of miles away will steal something even more important: Our very identity.

As a financial professional, the rise of threats like identity theft, fraud, and malware have added a unique element to my job. In addition to helping people grow their money and plan for their future, I now also help people safeguard their money and protect their future.

I call it financial cybersecurity - the practice of protecting yourself and your finances from hackers, scammers, and fraudsters. Nowadays, financial security has become as important as financial planning. Why? Because few things in life are as painful as planning for your goals, only to see those plans ripped away because of someone else's dishonesty. The scariest thing is that most people don't even know they're a target until it's too late. Just take a look at these stats:



IDENTITY THEFT

- In 2023, over 1.4 million consumers fell victim to identity fraud.
- The average loss suffered by fraud victims in 2023 was $500.
- People between the age of 60 and 69 led the way in terms of most money lost due to fraud, with $980 million stolen in 2023 alone.

CYBERCRIME

- Cybercrime is estimated to cost $9.5 trillion in losses in 2024, rising to $10.5 trillion in 2025.
- In the United States, a cyberattack occurs approximately once every 39 seconds.
- "Phishing" attacks – one of the most common ways that cybercriminals attack individuals – rose by 1,265% in 2023. The rise of generative AI in recent years has contributed to this trend.

Those are sobering numbers! When you dive into the statistics, it becomes clear that identity theft, online scams, and overall fraud are threats that everyone faces. It doesn't matter whether you're young or old, male or female. And due to the increase in in technology use, these threats are only going to get worse. In fact, online scams and data breaches have increased dramatically since the pandemic began. That's why it's more important than ever to keep your finances "scam-safe" and "cyber-secure."

The good news is that while the threat is real, the solution is simple

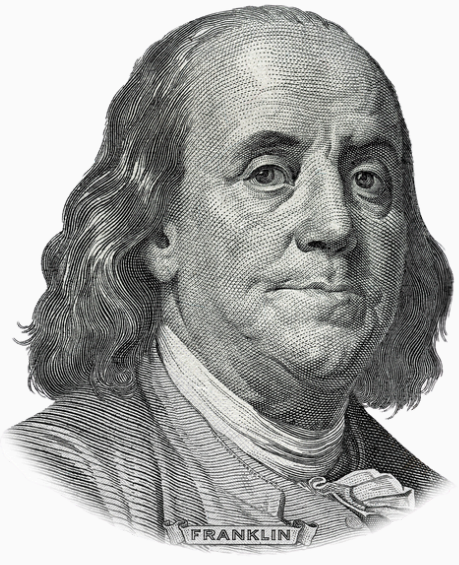
When pondering all the various types of scams, fraud, and malware out there, it's easy to feel overwhelmed. But here's the good news: Achieving financial security doesn't have to be hard. In fact, it's relatively simple!

With a little proactivity, you can strengthen your financial defenses to the point that most criminals will see you as simply not worth the effort. That's because, just as regular burglars prefer houses that are left unlocked, scammers and cybercriminals look for easy targets who've taken little-to-no steps to protect themselves.

To help you and your family become more financially cybersecure, I am sharing this short eBook. Inside, you'll find some simple steps you can take to protect your data, your money, and your identity. You'll also learn a little more about how to recognize the different types of fraud, scams, and cybercrimes that investors need to look out for.

Understand, this eBook is not meant to be an exhaustive compendium of every possible threat that investors and retirees face. Instead, it's a quick and handy guide to making yourself just a little more secure. Think of it as the virtual equivalent to simply locking your doors when you leave the house. These steps are easy, basic, and oftentimes, no-brainers - but they can go a long way to protecting yourself and your finances.

As Benjamin Franklin once said, "An ounce of prevention is worth a pound of cure." By taking steps today to protect your finances and your identity, you'll be saving yourself months of grief and frustration in the future. Because it's not just your money you'll be protecting.



It's your dream financial future.

Let's get started with…

IDENTITY THEFT

"People need to be more aware and educated about identity theft. You need to be a little bit wiser, a little bit smarter, and there's nothing wrong with being skeptical. We live in a time when if you make it easy for someone to steal from you, someone will."

- Frank Abagnale, former con-man and subject of the movie *Catch Me If You Can.*

IDENTITY THEFT

Identity theft is "the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name."

Usually, identity thieves are looking to apply for a loan, get medical services, or receive a tax refund in your name. Or, they may be hoping to go on an online shopping spree using your credit card. Either way, while identity theft may not be as shocking as, say, burglary, it can be equally devastating -- and even more time-consuming to recover from.

The good news is that protecting yourself from identity theft isn't hard. It simply requires you to be proactive and vigilant when it comes to your finances. On the following pages, you'll learn about some common forms of identity theft, who is most vulnerable, and how to spot the warning signs. Finally, you'll also learn some simple-but-effective steps for protecting yourself and your loved ones. Let's begin!

COMMON FORMS OF IDENTITY THEFT

Oftentimes, we only think of getting our identities stolen when we hear about a massive data breach -- think Target in 2013 or Equifax in 2017. But there are many ways that thieves can steal and exploit a person's personal information. Check out a few of the most common techniques on the right. We'll discuss a few of these in greater detail later in the book.

Did you know?

According to one study, only 1 in 700 identity theft suspects were caught by federal authorities.

Dumpster diving

Rummaging through garbage and recycling cans to find documents containing personal information like bills, medical forms, and statements.

Mail theft

One of the oldest forms of identity theft, mail theft is when a thief steals your mail looking for checks or documents that list your contact info, Social Security number, or credit card/bank information.

Online shopping

Online merchants often require customers to set up accounts. This makes shopping convenient, but these accounts contain everything thieves need to use your money…and they're often protected by weak, overused passwords that are easy to guess.

Phishing

Ever receive an email or phone call from someone that looks or sounds legitimate, but isn't? It could be a phishing attempt, where thieves try to "fish" for personal information by posing as your bank, the government, or some other authority.

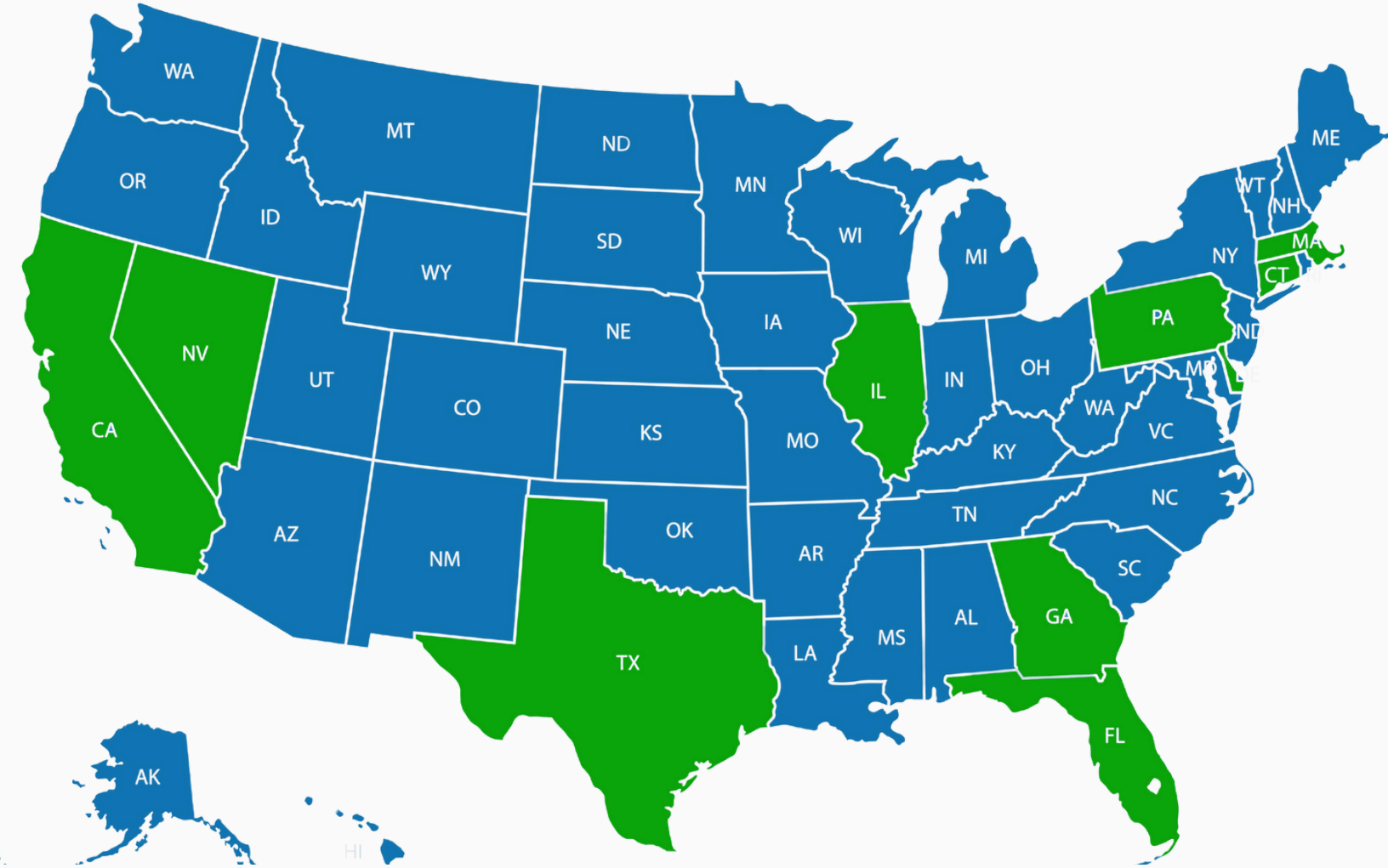
Malware

Malicious software like worms, Trojan horses, spyware, and ransomware can give hackers access to your personal information, including passwords.

WHO IS MOST VULNERABLE

By state

Identity theft is a threat to every American's finances, regardless of who they are or where they live. But some people are more at risk than others. For example, these ten states have the highest rates of identity theft per 100,000 residents.



1) GEORGIA
2) FLORIDA
3) NEVADA
4) CONNECTICUT
5) DELAWARE
6) MASSACHUSETTS
7) TEXAS
8) PENNSYLVANIA
9) ILLINOIS
10) CALIFORNIA

SOURCE: Business Insider

WHO IS MOST VULNERABLE

By demographic

Certain demographics may also be more vulnerable to identity theft, either because they represent potentially easy targets, or because they have exactly what identity thieves are looking for. If you or a loved one fall into one of these groups, it's worth taking extra steps to protect yourself.

CHILDREN AND TEENS

Children are vulnerable to identity theft because their Social Security numbers are "clean" of any credit card applications, job history, mortgages, etc. Furthermore, parents often fail to check their child's credit score, so theft can go undetected for a long time.

HIGH-INCOME EARNERS

Adults who earn a high income are often targets precisely because they have so much money! In addition, high-income earners often have more financial data that can potentially be exposed.

THE ELDERLY

The elderly tend to be targets because:

1) They may not be as internet-savvy as younger demographics

2) They often have a good deal in savings

3) They may depend on caretakers. A dishonest caretaker has ample opportunity to steal information.

HOW TO KNOW IF YOU'RE A VICTIM OF IDENTITY THEFT

Many victims do not even realize their identity has been stolen until months or even years later. Here are some indicators that you may have been targeted.

SUSPICIOUS ACTIVITY

Often, the first indicator of identity theft is if there is suspicious activity related to your credit or debit cards. For example, charges for goods or services you never ordered, receiving cards you didn't apply for, or getting a call from your credit card company asking about unusual purchases are all major red flags. For these reasons, you should inspect your bank accounts and credit card transactions frequently.

CREDIT SCORE

Your credit score can also serve as an early-warning indicator of identity theft. If your credit score has suddenly changed, or if you receive notification that your score was recently investigated, it could be a sign that thieves have either stolen your credit cards or applied for loans in your name.

UNEXPECTED EVENTS

Whenever something unexpected happens with your money, it should make you sit up and take notice. In this case, any sudden changes to your bills, unusual data on your tax returns, or even a check unexpectedly bouncing are all potential symptoms of identity theft.

WHAT TO DO IF YOU SUSPECT YOUR IDENTITY HAS BEEN STOLEN

If you think your identity has been stolen, the first thing to do is take a deep breath. Dealing with identity theft isn't fun, but it's not the end of the world! With some patience and persistence, you **WILL** be able to recover your identity.

The second step is to call my office right away. Let us know what happened. We will do everything in our power to assist you!

From there, the situation will require you to be methodical and thorough. The Federal Trade Commission (FTC) has listed some useful steps on what to do if your identity is stolen. I've listed the basic steps below, but you can read more about each by visiting the FTC website.

Step #1: Call any companies where you know fraud occured

Ask to speak to the company's fraud department if it has one. Explain that your identity was stolen, and request that your account(s) be frozen or closed. Then, change any logins, passwords, or PINs you have for those accounts. That way, no new charges can be added without your knowledge.

Step #2: Place a fraud alert with one of the three main credit bureaus

Next, contact one of the main credit bureaus: Experian, TransUnion, and Equifax. Ask for a free credit report so you can better monitor your credit score, and then place a free, one-year fraud alert. This makes it harder for someone to open new accounts in your name. NOTE: It doesn't matter which bureau you choose, as each is legally required to inform the other two.

Step #3: Report the theft of your identity to the Federal Trade Commission (FTC)

The FTC will help you create an Identity Theft Report and recovery plan. The report proves to businesses that your identity has been stolen and guarantees you certain rights. To create your report, fill out the online form here.

Step #4: Close fraudulent accounts and remove bogus charges

Once you have your Identity Theft Report, call the fraud departments of each business where an account was opened or money was spent. Again, ask that all accounts be closed and bogus charges canceled. Give a copy of the Identity Theft Report if necessary, and then ask each business to send you a letter confirming they removed the fraudulent charges.

Step #5: Correct your credit report

Victims of identity theft have the right to remove fraudulent information from their credit report. The next step is to write to each of the three credit bureaus. Include a copy of your Identity Theft Report and provide proof of your identity. Explain which information on your credit report is fraudulent, and ask them to block that information. Use the FTC's sample letter if you need help.

Step #6: Add an extended fraud alert or credit freeze

Finally, consider placing an extended fraud alert or even a credit freeze on your credit report. An extended fraud alert lasts for seven years and limits access to your credit report by mandating that inquiring companies provide proof of their own identity. A freeze goes even further. It prevents any access to your credit report, and lasts for however long you want until you decide to lift the freeze.

IDENTITY THEFT PROTECTION CHECKLIST

Now that you know what identity theft is, what it looks like, and who is most vulnerable, it's time to learn how to protect yourself from it. Here are some simple steps you can take to safeguard yourself and your loved ones.

- Keep all your personal documents in a safe place. Don't carry them around with you, especially not your Social Security card.
- Don't open emails from senders you don't recognize, and never open attachments. These can be disguised as special offers for things such as weight loss products, miracle cures for ailments, or merchandise at "unbelievably low prices." Scammers keep coming up with new subjects to hook you.
- Remember that neither your bank or the government will ever ask you to provide sensitive or personal information via email or text. Messages that look like they are from these institutions are likely "phishing" scams. (More on these in the next section.)

IDENTITY THEFT PROTECTION CHECKLIST

- Similarly, if you are ever concerned about the credibility of a call or email from any institution, search for their contact information online and ask them to verify whether the message you received is legitimate.
- In short, don't share personal information (like your birthday, Social Security number, or bank account number) just because someone asks for it!
- Don't publish the date of birth or death in obituaries. Thieves can use that information to obtain a death certificate, which usually includes the Social Security number for the deceased individual.
- Collect your mail every day. Place a hold on your mail when you're away from home.
- Shred all your receipts, credit card offers, account statements, expired credit cards, and other sensitive documents. This prevents dumpster divers from getting your information.

IDENTITY THEFT PROTECTION CHECKLIST

- Regularly review your credit card and bank account statements. Compare receipts with account statements. This can help you find unauthorized transactions.
- Review your credit report annually for discrepancies. If your credit has dipped without any good reason, investigate immediately.
- Install firewalls and malware-detection software on your computer and mobile devices. (More on this in the next section.)
- Don't reuse passwords! Every online account should have a different password. Furthermore, change your passwords regularly, and don't leave them all in one place. You can use a password manager like **1Password**, **Bitwarden**, or **Dashlane** to help keep track of all your passwords.

Next, let's look at...

CYBERCRIME

"Passwords should be like underwear: Don't let people see it, change it very often, and never share with strangers."

- Chris Pirillo

CYBERCRIME

Viruses. Trojan horses. Phishing. Malware. The internet is littered with scary-sounding terms that make it seem like shadowy hackers are watching every keystroke and mouse click we make, looking for ways to break into our devices the moment we're not looking.

It's widely known that cybersecurity and financial security are closely related. But the reason why doesn't really have anything to do with images like the one to the right.

While it's true that there are indeed many skillful and nefarious hackers out there, the best of them tend to work for cybercrime "syndicates" that target large corporations and even entire governments.

For individuals like you and me, the real risk comes when we make one of these three basic mistakes:

- Fail to recognize basic scams and fraud, many of which are old as time and have been merely adapted to the digital age.
- Fail to keep our "digital doors locked" when using our computer or mobile devices.
- Engage in unsafe practices or visit insecure websites -- the virtual equivalent of finding yourself in the "wrong part of town."

What is cybercrime?

Cybercrime is essentially **any crime that involves the internet to some degree**. There are many types of cybercrime, and some of the worst don't involve money at all. But for the purposes of this book, we will focus on those that can negatively affect your finances -- often via identity theft -- and by extension, your financial goals.

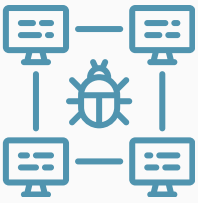
Specifically, we will look at two broad categories of cybercrime: Online crimes that use your electronic devices as a **tool**, and crimes that use your devices as a **target**. Once we've covered both categories, and how they overlap, we'll examine what makes people vulnerable to cybercrimes and how you can protect yourself. Let's dive in!

COMMON FORMS OF CYBERCRIME

Your computer as a target

The term is **MALWARE**, which is a portmanteau for **MALICIOUS SOFTWARE**. Think viruses, worms, Trojan horses, etc. Malware is the classic example of a cybercrime, in which your **computer** is the primary target rather than your identity or your bank account (although these may be indirect targets, and the lines between the two are becoming increasingly blurred). Malware has been around for decades, but it was the rise of the internet that made it the preferred toolkit for a new generation of thieves. Here are six of the most common types.

Computer viruses



A virus is a type of program that replicates itself by modifying other programs and inserting its own code. One of the oldest types of malware, viruses are less common than they used to be since antivirus software has become more effective. But they still cause billions of dollars worth of economic damage each year, and can corrupt your data, slow down your devices, or even cause a complete system failure. As a result, dealing with viruses can be very expensive.

How you get them: Email attachments, internet downloads.

Trojan horses

A Trojan horse is a malicious program that looks normal, benign, or even helpful, in order to convince the user to install it. But once installed, Trojans can give hackers **backdoor access** to your computer, enabling them to steal information, spy on you, install more malware, and more.

How you get them: Internet downloads

Worms

Worms are an extremely common form of malware. These spread over computer networks like the ones in offices, college campuses, or other institutions. Unlike viruses, they don't require any user action to replicate. Some worms do little damage while others can give hackers access to your system, similar to Trojans. All worms, however, can spread very easily.

How you get them: Email attachments, visiting bad websites, running out-of-date software.

Spyware

Spyware tracks your internet activity: browsing habits, Google searches, login information, even your keystrokes! While it may sometimes be just an annoyance, it can also represent a serious threat to your privacy and the security of your bank account.

How you get it: Spyware often comes from Trojans but can also be bundled with legitimate software.

Adware

Adware is software that persistently and aggressively puts unwanted advertisements on your computer screen, often in the form of a "pop-up" or browser window that can't be closed. It can redirect you to advertising websites, change your internet browser settings, search settings, homepage, and more. Most ominously, adware can also collect your data. Some of the newest forms of adware can even disable your anti-malware protection.

How you get it: Using an out-of-date browser, clicking on certain ads or visiting disreputable websites.

Ransomware

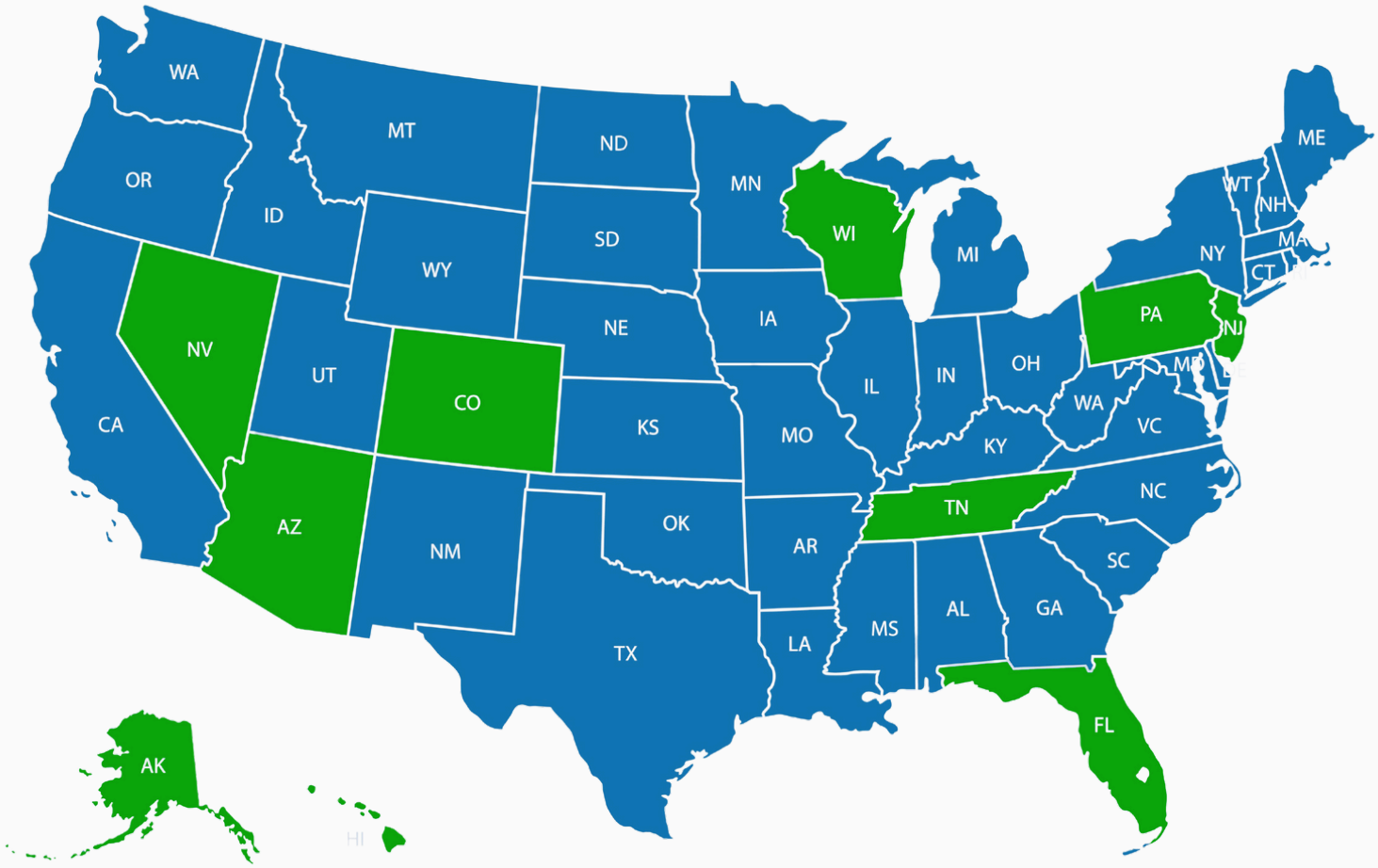
Ransomware tends to dominate the news, and for good reason: It can hold entire corporations hostage. It's a type of malware that essentially locks you out of your data, or even your device, until you pay the ransom. Sometimes it's merely a scam designed to trick you, and sometimes it's not.

How you get it: Ransomware is often installed on your device via Trojans or worms. Like most other forms of malware, the main culprit is opening unexpected emails and attachments.

WHO IS MOST VULNERABLE

By state

Anyone who uses the internet is potentially vulnerable to cybercrime or data breach. But just as with identity theft, some states seem to be particularly at risk. Here are the top ten, based on FBI data and the National Governor's Association.



1) HAWAII
2) PENNSYLVANIA
3) NEVADA
4) FLORIDA
5) WISCONSIN
6) ARIZONA
7) NEW JERSEY
8) ALASKA
9) COLORADO
10) TENNESSEE

SOURCE: Security.org

COMMON FORMS OF CYBERCRIME

Your computer as a tool

Rather than a target in and of itself, more and more thieves are seeing your computer and other devices as a tool to target you. These types of crimes don't require as much technical expertise, and range from sophisticated to crude. In fact, most of the crimes in this category have been around for centuries. The internet simply represents a new and more dangerous tool for them to use against their victims.

The main crime we will discuss here is known as **PHISHING.**

Phishing

Imagine this scenario. You get an email that appears to be from your bank. You open it and read a message that either looks extremely convincing, or is riddled with misspelled words. Either way, you are directed to "click the link below." You click the link, and are taken to a page that looks almost exactly like the website you're used to visiting.

Almost.

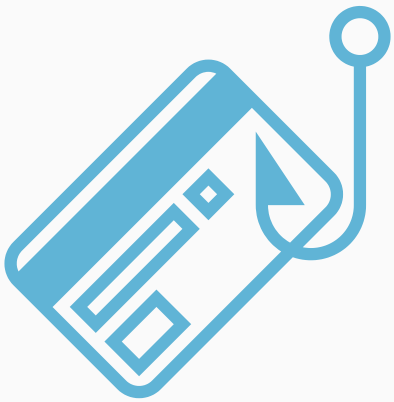
You've been phished.

Hopefully, this scenario has never happened to you. Or if it has, you recognized the warning signs and knew to stay away. Unfortunately, many people don't recognize those warning signs, and so fall prey to a particularly insidious form of internet fraud called phishing.

Phishing is when hackers and cyber-thieves try to trick people into submitting their personal information by creating fake versions of existing websites and/or sending emails and text messages that look like they are coming from a legitimate bank, business, or government agency. Sometimes, phishing can even take place over the phone!

A play on the word "fishing" (with regular people as the prey and the fake message/website as the bait), the crooks behind phishing try to dupe people into giving out sensitive information, like their Social Security numbers, account passwords, credit card numbers, or even bank PIN numbers.

Often, victims of phishing are directed to websites that automatically install malicious software onto their computer or mobile device. Either way, phishing poses a major threat to your finances, your identity, or your data.

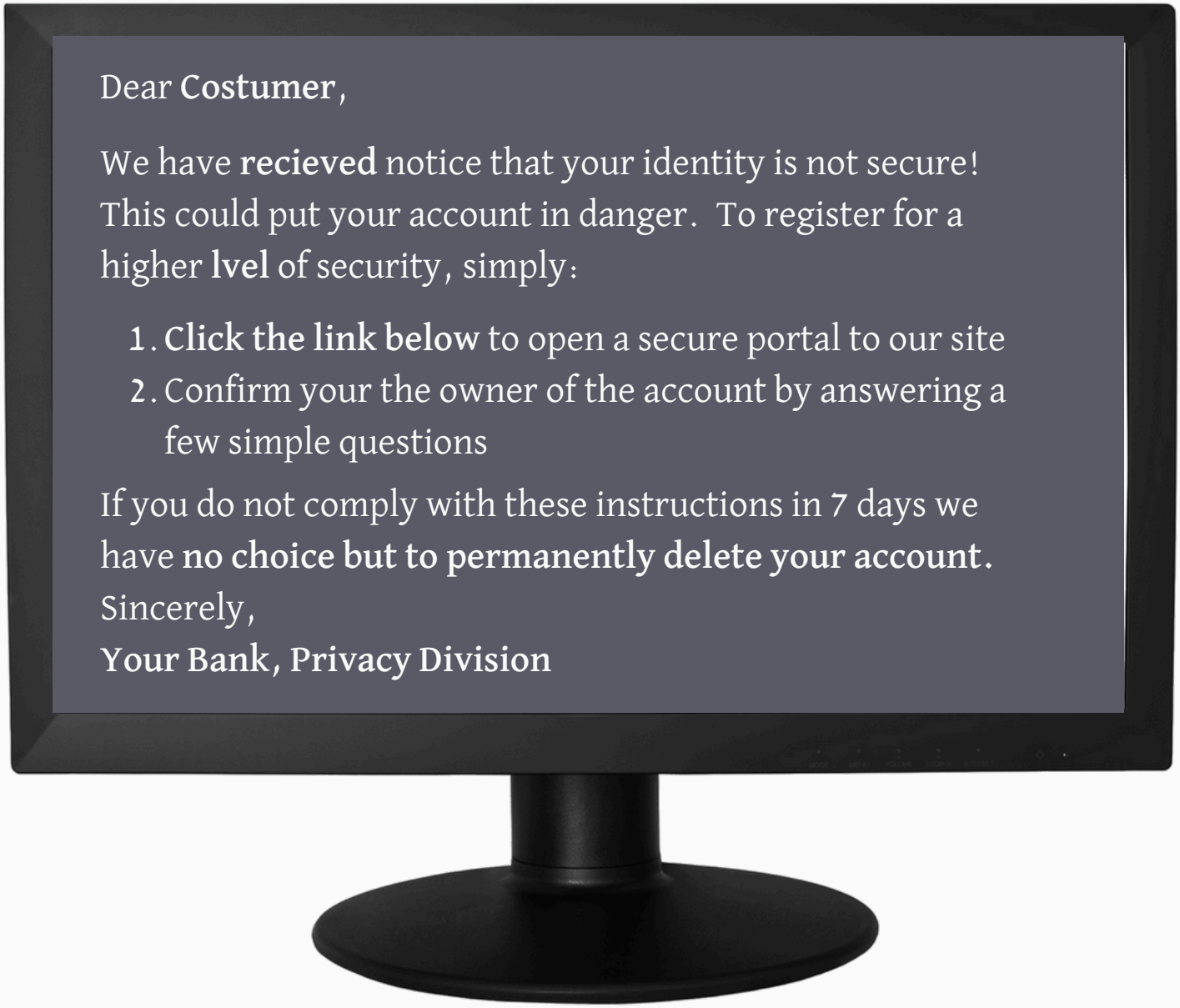


Thankfully, phishing is easy to avoid if you follow a few common-sense rules:

- Legitimate banks, retailers, and agencies will never ask for your personal information via email. If you receive a message from someone asking for this, assume it's a scam.
- Furthermore, as a general rule of thumb, do not reply to any message, electronic or otherwise, that requests your personal information.
- Never use links in an email to connect to a Web site unless it's an email you expected from a source you KNOW is trustworthy. Instead, open a new browser window and type the site address in directly.
- Always double-check the URL of any site you intend to visit. Some thieves set up sites with URLs that look very similar to a legitimate site. For example, "amzon.com" instead of "amazon", or "facebok.com" instead of "facebook." You get the idea.
- When doing business online, look at each website's address. Secure websites should have a small symbol of a lock next to their URL, or the letters https (instead of merely http) at the beginning of the address. Both indicate that the site has been verified as secure.

RECOGNIZE WHAT COMMON PHISHING MESSAGES LOOK LIKE

Some phishing messages may be extremely sophisticated and be virtually indistinguishable from the real thing at a glance. But there are often some telltale signs, and most phishing messages tend to be crude if you pay attention.



The warning signs in this email -- a real phishing attempt that was caught -- aren't hard to spot. Notice the misspelled words? **(Costumer, recieved, lvel.)** The link to click on? Or what about the threat? **("If you do not comply…")** And of course, there's the reference to your bank or some other well-known organization.

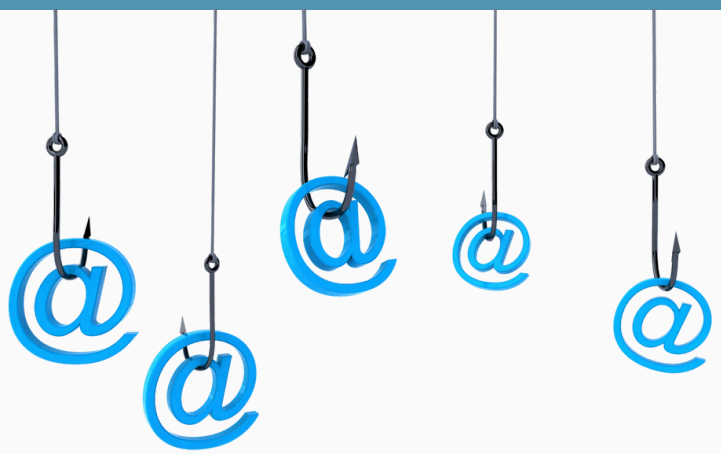
Here is the message again. Spot the red flags?

Dear **COSTUMER**,

We have **RECIEVED** notice that your identity is not secure! This could put your account in danger. To register for a higher **LVEL** of security, simply:

1. **CLICK THE LINK BELOW** to open a secure portal to our site
2. Confirm **YOUR** the owner of the account by answering a few simple questions

If you do not comply with these instructions in 7 days we have **NO CHOICE BUT TO PERMANENTLY DELETE YOUR ACCOUNT.**
Sincerely,
YOUR BANK, PRIVACY DIVISION



STEPS TO PROTECT YOURSELF FROM PHISHING

REMEMBER THIS

Legitimate banks, retailers, agencies, and institutions should never ask for your personal information -- like passwords, PINs, and Social Security Numbers -- via email. If you receive a message from anyone asking for this info, assume it's a scam. Furthermore, as a general rule, don't reply to any message, electronic or otherwise, that requests your personal information.

DON'T DO THIS

Don't click on a link in an email to connect to a website unless it's from a source you know is real and trustworthy, like a family member. Instead, hover your mouse over the link to verify the address, or search for the site on Google. And NEVER click on an attachment you're not expecting! The same is true for any links you see on social media, like Facebook.

ALWAYS DO THIS

Always double-check the URL of any site you intend to visit. Sometimes, scammers create sites with URLs that look very similar to real sites. For example, "amzon.com" instead of "amazon". Also, check to see if sites have a symbol of a lock next to their URL, or begin with the letters https (instead of merely http). Both indicate the site has been verified as secure.

WATCH OUT FOR THIS

Phishing emails and websites may look legitimate at first glance, but the warning signs often stick out upon closer inspection. In particular, watch out for misspelled words, broken English, and threats. Variations on "If you don't comply" is a common phrase.

CYBERCRIME PROTECTION CHECKLIST

Now that you know a little more about cybercrime, here are some simple -- but crucial -- steps to keeping yourself and your finances "cyber-secure".

1) Keep all of your software up to date.

What does this have to do with cybersecurity? Everything. You see, one of the easiest targets for hackers to attack is outdated software. That's because older applications often contain weaknesses that hackers can use to gain access to your devices. Your web browser -- Chrome, Firefox, or Safari, for example -- can be especially susceptible. That's why you should always:

- Turn on automatic system updates for your computer, tablet, or smartphone.
- Download updates and software patches when prompted.
- Frequently review the apps on your devices. Remove the ones you don't need and update the ones you do.
- Familiarize yourself with your browser's extensions. (For example, Flash, Java, AdBlocker, etc.) Keep these updated, too.

CYBERCRIME PROTECTION CHECKLIST

2) Use stronger passwords via a password management tool.

Your email. Your bank. Your Facebook account. These days, we all have to juggle dozens of passwords. There's no way to memorize them all, so many people resort to using the same two or three passwords for everything. To make matters worse, these passwords are often extremely simple. (Please don't be the person who uses "1234" or "password" as their password.)

As a rule of thumb, your passwords should always:

- Contain at least eight characters.
- Contain at least one uppercase letter, one lowercase letter, one number, and several symbols. (Symbols include exclamation points, question marks, and asterisks.)
- Be different from one another. Don't use the same password twice.
- Change at least once per year.

To help with this, consider downloading a password management app. These are handy tools that make managing passwords a breeze.

CYBERCRIME PROTECTION CHECKLIST

With a password manager, you only need to memorize one password -- for the manager itself -- instead of dozens. The app will do the rest, automatically inserting the right password whenever you need it. Popular password managers include LastPass, Dashlane, 1Password, and Bitwarden.

3) Embrace two-factor authentication.

Two-factor authentication is a technical term for a simple concept. Think about the front door of your home. It probably has two locks - a handle lock and a deadbolt. While the deadbolt is a second layer of security for your home, two-factor authentication is a second layer of security for your identity.

Normally, when you log into an app or website, you type in your username and password. Two-factor authentication goes a step further by requiring you to enter at least one additional form of authentication. This is often a personal identification number, like a four-digit code. It can also be a second password, the answer to a question only you would know, or even your fingerprint. Only by entering two different forms of authentication can you login to the app or website.

CYBERCRIME PROTECTION CHECKLIST

Yes, two-factor authentication adds another five seconds to the process. But it also makes it much harder for thieves and hackers to access your email, Facebook profile, or Amazon account. Use it!

4) Use antivirus (AV) protection software.

Back to basics here. It's been around for decades, but good AV software is still critical to protecting yourself from viruses and malware. Be advised, though, that it's better to use one program than two or three. Multiple AV programs can clash with each other, slowing your device and paradoxically leaving you more open to attack. So, rely on one good program you can trust, and remember to keep it updated!

5) Backup your data regularly.

Backing up your data will make your life much easier if you do become a victim of malware. Oftentimes, restoring your data via backup is the only way to return your device to normal. Keep three copies of your data. One can be kept on your local hard drive. The second should be kept on an external hard drive. The third should be kept in the cloud. Google Drive, Microsoft OneDrive, Apple iCloud, and Dropbox are four popular examples of cloud storage.

CYBERCRIME PROTECTION CHECKLIST

6) When in doubt, keep out.

In the outside world, it's usually healthier to be positive than cynical. But the internet is not the outside world. It's the Wild West. A little cynicism or skepticism can go a long way toward keeping you safe. So:

- If you aren't sure an email is legit, don't read it.
- If you weren't expecting an attachment, don't open it.
- If you weren't purposefully shopping online, ignore any and all ads you didn't search for.
- If you're not sure where a link goes, don't click on it.
- If you feel uncertain about a website, don't visit it.
- If you're ever asked to do or share something that you're not comfortable with, SAY NO!

Remember, you can always open that email, visit that website, or click that link later after you verify it's real. But undoing something you wish you hadn't done? That's a lot harder. So, when it comes to keeping your device, your data, your finances, and yourself cyber-secure…

WHEN IN DOUBT, KEEP OUT!

TIMES TO BE ESPECIALLY WARY

While financial security should be a priority 365 days a year, there are certain times when people are more susceptible to fraud and identity theft. Here are three times you should be particularly vigilant:

AROUND THE HOLIDAYS

The holiday season -- Christmas especially -- is a magical time of year. But it's also a stressful one. Because people have so many things to do, they often fail to pay attention to the warning signs we discussed earlier. Thieves know that, and act accordingly.

Here are some potential scams you may encounter around the holidays:

Phishing Scams

During the holiday season, the twist on this scam may include thieves posing as shipping companies or online retailers, asking for personal information to resolve a shipping error. Their goal is to get personal information from people who are worried their online purchases won't ship in time for Christmas. Another holiday flavor to this scam is individuals posing as a legitimate organization asking for charitable donations, hoping to capitalize on your holiday generosity.

Gift Card Scams

With this scam, thieves will go into retailers and find gift cards that are yet to be purchased. They write down the numbers to the gift cards and track them electronically until they are purchased. Once activated upon purchase, the scammer will drain the funds leaving the gift card empty for its rightful owner. To avoid this scam, avoid purchasing gift cards that are either damaged or do not have packaging.

If you feel uncomfortable buying a gift card you find in a store, you can always ask the staff if they have any in the back that haven't been accessible to the public. Also, to further protect yourself, avoid buying gift cards from third party vendors you aren't familiar with.

Fake Coupons

With everyone trying to save a little money on their Christmas shopping, coupons can be a handy resource. Unfortunately, there are scammers who set up websites that provide fake coupons in order to steal personal information. Be wary of websites offering coupons or discounts to third parties in exchange for personal information.

Counterfeit Gifts

Just as everyone is trying to save money with coupons, people are also on the hunt for deep discounts. Another scam to avoid this year is the sale of counterfeit goods. If this year's newest smartphone or gadget is being sold for a price that seems too good to be true, it probably is! To avoid this type of scam, do your research on how to identify authentic goods, or purchase these items directly from the manufacturers.

TAX SEASON

Tax season is another stressful time. With so many people desperate to get their filing done in time, swindlers and con artists know this is the perfect time to go after your identity. Don't let them! Here are some common tax-season scams.

Phishing Scams

Yep -- phishing again! During tax season, watch out for emails purportedly from the IRS promising a refund or threatening some sort of penalty or legal action against you. They're all bogus! The IRS will never contact you by email, text message, or social media to request any personal or financial information from you.

Phishing by Phone

This is similar to the scam above, except it's by phone. If you get a call from someone claiming to be an IRS agent who is making threatening calls demanding money, hang up. Same if you get a call asking you to "verify your information." Instead, if the IRS needs to get in touch with you, they'll usually do it via the regular mail.

Refund Scams

Watch out for people who promise a bigger-than-usual refund if you'll only let them prepare your taxes -- all you have to do is sign a blank check or allow them to take a percentage of your refund. Legitimate tax preparers should never ask for these things. Nor should they make outlandish promises before they even look at your tax situation. Often, these are scammers who will try to file a false return in your name so they can claim your refund for themselves.

DURING A CRISIS

Scams often go up whenever there is a crisis. Sometimes the crisis could be a natural disaster, like after an earthquake or hurricane. Or it could be a health crisis. During the coronavirus pandemic, for example, data breaches and online scams went up dramatically. The same was true during the 2008 financial crisis. Again, **phishing** is the method of choice. Thieves will often pose as government officials, either via email, text messages, or even robo-calls, requesting your personal information in order to qualify you for government assistance. Given that the government often does provide some sort of assistance during a crisis, these scams can often seem very convincing.

In addition to the steps you've already learned, the best thing you can do to protect yourself is to simply stay informed about what the government is and is not doing to help during a crisis. While the media -- like almost everything else -- has become a contentious political topic in recent years, the fact remains that national news outlets, or your local news organizations, are simply more reliable than any email, text message, robo-call, or post on social media when it comes to this sort of thing.

WHAT TO DO NEXT

Take a few minutes to think about everything you just read. Think about your long-term goals and your short-term needs. Has anything changed? Does anything need to change? Are you as prepared as you should be?

If you feel it's time to become more "financially secure", then let's talk. We can meet in my office, over the phone, or through video conferencing to determine what areas need to be addressed. If you need expert help on any of these topics, I can also put you in touch with professionals I know and trust.

In the meantime, I hope you found this information to be interesting and helpful. As always, please let me know if there is ever anything I can do for you. Above all, remember to be vigilant. Be careful.

Be financially cybersecure.

TIME TO REVIEW YOUR STRATEGY OR UPDATE YOUR GOALS?

Call, email, or visit our website to schedule an appointment today!

206-448-9107

jeff@vstrickler.com

www.emeraldcityfg.com

MEET JEFFREY MOORMEIER

For three decades Jeff Moormeier has been aiding families and friends navigate the road to pursue their financial goals and objectives. His philosophy begins with helping clients define their perfect day and then aligning their money to support that lifestyle.

He began his financial advising career at Merrill Lynch in 1988 after spending 8 years serving in the U.S. Army as a computer programmer with top-secret clearance. During his 14 years at Merrill Lynch, he worked his way up from an entry level financial advisor to Vice President. In 2002 he started his own firm, Quantum Advisors, to focus his efforts in an entrepreneurial environment that more closely fit his style of advisory work.

In 2018 he affiliated his independent practice with City Fiduciary Group in Vancouver, Washington. In 2020 he acquired the financial planning practice of Vivienne Strickler in Seattle, Washington, and relocated his office from Mukilteo, WA, to Mercer St. in Seattle. His firm, Emerald City Fiduciary Group, now manages more than $250,000,000 for clients across the country.

He is an avid snow skier and PSIA Instructor. Jeff has been married to his wife Jean for 40 years. Jeff and Jean are both U.S. Army veterans. They have four children and many grandchildren (8 and counting as of 2024).

DISCLAIMERS

Securities offered through Osaic Wealth, Inc. member FINRA/SIPC. Osaic Wealth is separately owned and Emerald City Fiduciary Group and Arbor Point are independent of Osaic Wealth.