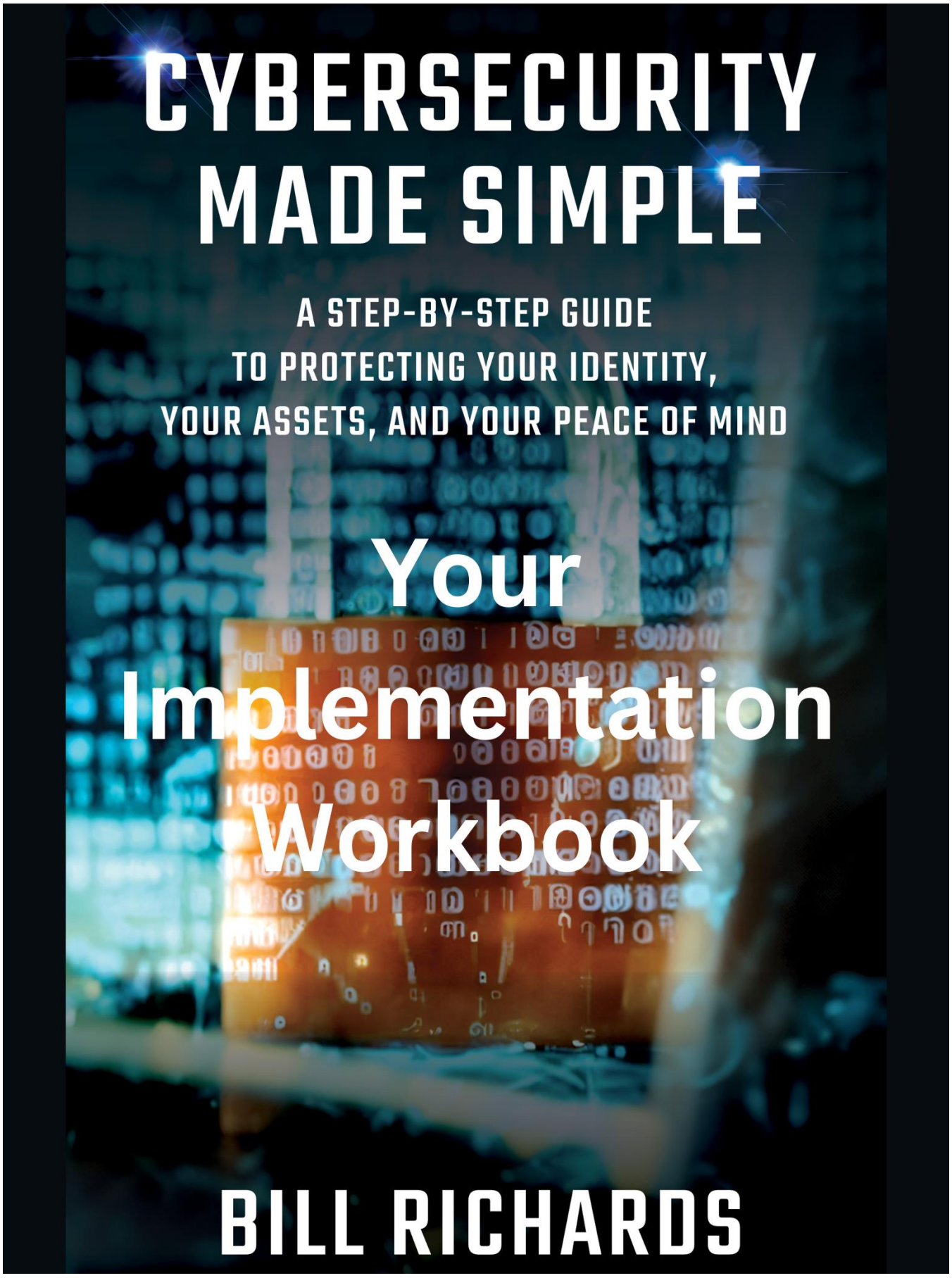

CYBERSECURITY MADE SIMPLE
A STEP-BY-STEP GUIDE TO PROTECTING YOUR IDENTITY, YOUR ASSETS, AND YOUR PEACE OF MIND
Your Implementation Workbook
BILL RICHARDS

Table of Contents

Introduction

In the late 1990s, the internet exploded. Many of us were caught flat-footed, and found ourselves running to catch up, not sure perhaps if we were even running in the right direction!

These days most folks have at least a basic knowledge of the internet, using it for emails, social media, searching for this or that, and perhaps ordering Thai delivery from DoorDash. But despite a growing comfort level, we can't afford to grow complacent, as we are currently in the midst of another technological explosion: an explosion of hacking and fraud which now pervades the internet.

If you've already read Cybersecurity Made Simple: A Step-By-Step Guide to Protecting You Identity, Your Assets, and You Peace of Mind, then you have some idea of the sheer number of cyberattacks occurring each month. Equally concerning is that attacks have grown ever more varied and sophisticated. Some phishing emails can lead the unwary to surprisingly authentic-looking spoof sites, where user IDs, passwords, and other sensitive information can be collected and used to steal one's money or even identity.

(If you don't recognize terms such as "phishing" and "spoof sites", I encourage you to stop now and return to the main book, at least skimming its glossary, before attempting to complete this workbook, which assumes some baseline knowledge.)

The unfortunate truth is that there are unscrupulous people who will try to make money by any means available. They act without conscience, and without concern for the harm they do to others.

I do not wish for you or someone close to you to become a victim of one of these predators, and I'm sure that you don't want that either. That's why I created Cybersecurity Made Simple and this workbook.

And why exactly did I create this separate workbook? After all, Cybersecurity Made Simple purports to be "A Step-By-Step Guide to Protecting You Identity, Your Assets, and You Peace of Mind". So why this companion workbook?

While I strove to make Cybersecurity Made Simple as complete as I could (and there will be updated editions in the future with even more information), feedback from some initial reviewers indicated a lack of certainty about how to proceed after reading the book.

Yes, they certainly understood that creating a cybersecurity safety plan based on best practices is an important first step to safeguarding themselves and their loved ones. But they wanted more direction on how to actually implement their plan.

And unless you actually implement your plan, you are just as exposed as if you had no plan at all.

This workbook is therefore designed to close the gap, to help you actually implement an effective cybersecurity plan, step by step.

This workbook contains three main sections:

Prepare. We've all heard the adage "An ounce of prevention is worth a pound of cure." That old saw has never been truer than when contemplating your online safety. Following best practices and implementing a personal cybersecurity plan will go a long way toward protecting you and your loved ones. Make it harder for the predators, and they will likely move on to an easier target.

Be aware. Even with a solid cybersecurity plan in place, you shouldn't let your guard down – and that is true for every member of your household, as the security practices of one so often affect the others. You need to be aware, e.g., of common tactics like phishing emails and spoof sites, mentioned above. If an email, text, or QR code looks suspicious, tread carefully.

Respond. Unfortunately, despite your best efforts, you may still find yourself the victim of a cyberattack. Your home network may be accessed by an outsider, or perhaps your personal data resides in the databank of a company or institution which was hacked. Regardless of the cause, you need to know what steps to take to protect yourself to the degree possible after the fact.

Some steps recommended in this workbook should be straightforward and easy to accomplish quickly. Others tasks, such as reviewing all existing passwords and updating them as necessary, may take considerably more time. Regardless, I encourage you not to skip tasks because they may seem tedious, unpleasant, or too time-consuming. Instead, keep your eyes on your goal: Ensuring your safety.

To that end, you'll find a checklist of tasks toward the end of this workbook, to help you monitor your progress and to ensure that you don't overlook any steps.

With that, let's dive in!

(Yes, that's me, maaany years ago.)

Prepare

Later in this workbook we'll discuss what to do if you find that you've been the victim of an attack, but obviously you'd like to avoid one in the first place. How do you begin? In this section we'll discuss a number of steps that you can take to avert cyberattacks.

The very first step to take, if you have not already done so, is to ensure that **all** of your devices are password protected, either by a PIN or by fingerprint biometric reader.

Next, strengthen your passwords. Weak passwords are a major source of hacks. Fortunately, implementing stronger ones is an easy process. We'll cover this topic in depth in the next section.

You can further reduce your exposure by closing out memberships that you no longer use, and by pruning contacts on social media.

You'll also want to be very sure that you make a modest investment in your security by subscribing to a VPN and by installing virus-protection software on all of your devices. Yes, even you Mac users!

You can be more proactive by subscribing to a service which will help remove your personal information from the many databases which – legally – buy and sell it.

Let's look at each of these topics in turn.

Set Up Secure Log-In

You likely set up password or PIN authentication when you first got your device, but if not, do it now.

I've noticed that most folks use either a PIN or fingerprint to access their smartphones, but are less apt to secure their computers. Even if you use a desktop, or rarely take your laptop out of the house, you're better off securing it.

And if you haven't changed your PIN or password in some time (Still using "Fluffy1234"?), now may be the time to change it.

The exact navigation to setting up and changing login in credentials will depend on the specific device and its operating system. But you'll first go into Settings, then look for something like "Security and Privacy", "Sign-In Options" or similar.

You should find options to create or change your PIN or password. Newer devices, including most smartphones, also allow you to set up biometric scans. Usually this involves scanning your fingerprint on the main camera lens. Although I have set up fingerprint scanning on my smartphone, frequently it cannot read my fingerprint, and I have to use my PIN. For this reason, even if you use fingerprint scanning – or perhaps facial recognition – I encourage you to also set up a PIN as well.

While in Settings, also review your settings for how long your device must be inactive before it is automatically locked. Don't set too long of a delay. Yes, having to log back in – again – can be a minor irritation, but it's a small price to pay for the protection afforded, especially when in public places.

Let's move on now to the next topic – and it's an important one: password management.

Password Management

Creating strong passwords – and periodically changing them – is one of the most effective ways to head off hackers. However, we've probably all been guilty of creating passwords based on personal information simply because they're easy to remember.

But the fact is that hackers can easily gain a wealth of information about you from social media and data brokers. Using a child's name or birthday, the name of your pet, or your mother's maiden name is not nearly as secure as you might wish to believe. According to Norton (https://us.norton.com/blog/privacy/password-statistics):

"More than 80% of confirmed breaches are related to stolen, weak, or reused passwords."

That statistic should rattle you a bit, and motivate you to strengthen your passwords.

To be truly secure, a password needs to be long, and it needs to be nonsensical. This is why so many websites list requirements for creating a password, such as

- Must contain a minimum of 8 characters
- Must contain numbers and letters, both upper- and lower-case
- Must contain special characters

However, this makes remembering all of your many passwords virtually impossible. What's the solution? I recommend using a password manager, which we'll discuss next.

Password Managers

I recommend using a password manager to store your passwords. These typically reside in your computer's browser. They come standard in the more common browsers, such as Google Chrome and Firefox.

But this begs the question: Are password managers, which store passwords in the cloud, really secure? The answer is, "Yes." If not absolutely, 100%, no-way-can-they-ever-be-hacked secure, certainly using browser-suggested strong passwords stored in the cloud is better than using "Fluffy1234" as your standard go-to password.

Further reading:

Simple explanation of "the cloud":

https://edu.gcfglobal.org/en/computerbasics/understanding-the-cloud/1/

Additional information about password manager security:

https://www.forbes.com/advisor/business/are-password-managers-safe/

In my opinion, if you aren't using a password manager already, you should strongly consider doing so. The next time you are asked to create (or reset) a password, put your cursor in the Password field and when the browser suggests a strong password, accept it. Then, wait a couple of seconds, and a box should appear in the upper right of your screen asking if you want to store or update the password; always select "Yes", as that's the whole idea. Let the system remember those cryptic passwords for you.

Strengthening Existing Passwords

You should also explore what is already stored in your password manager. It may be enlightening! I did this recently and was amazed at how many passwords were stored there – and how many of them were weak. (And I should know better!)

I use Chrome as my browser, as I'm sure many of you do as well. To access Chrome's Password Manager, click on the three stacked dots at the far right of the Chrome bar. In the drop-down menu, click Passwords and Autofill, then Google Password Manager. (If you use another browser, the steps will be similar; Google if you need assistance.)

Once inside Chrome's Password Manager, you'll see a laundry list of websites for which your browser has already saved passwords. Now, just for fun, look to the left, find and click on "Checkup". Chrome will spin for a few seconds and then present to you lists of:

- Compromised passwords
- Reused passwords
- Weak passwords

If any passwords are compromised, jump on those right away. Go to the site(s) indicated and change your password.

Reused passwords are, in my view, less critical – unless you're using the same easy-to-crack password on lots of web-sites. Still, best practice is to have a unique password for each website you access. That way, if one is compromised, the damage will be contained.

Now we come to "Weak passwords", such as "Fluffy1234". I was stunned by how many of these Chrome found among my saved passwords, so I set about updating them. I will confess that there were way too many to do in one sitting. The process – which should be essentially the same regardless of which browser and password manager you use – goes like this:

Run the Checkup, then:

1. Open the list of weak passwords. What you'll actually see is the list of websites, rather than the passwords themselves.
2. Go to each website in turn (you can just click the URL displayed in the listing).
3. Update the password for that website. There are a couple ways to do this:
    - Log in using the current password, and then go into your profile and update your password with a more secure one, or
    - At the login step, click "Forgot password?" and enter your email address. An email will be sent to you (which usually arrives immediately, but might be delayed two or three minutes), click the link within the email which says "Reset password", and on the screen that's pulled up, allow the Password Manager to suggest a stronger password.
    - Either way, after updating your password, your browser should ask you if you'd like it to save the new password. Be sure to confirm "YES"!

    If you have many passwords to update, I suggest you prioritize. Begin, for example, with financial institutions first, e-tail sites next, etc.

Tip: If your browser does not automatically suggest a password when you need to create one, just position your cursor within the Password field and right click. A dropdown menu should appear and "Suggest a strong password" should be the top selection option.

Note that simply deleting a password within the Password Manager does **not** eliminate your exposure. The weak password no longer resides in your browser's Password Manager, but it still resides on the website.

While in the Password Manager, check your settings and see if there is anything you want to change. If the setting "Offer to save passwords" isn't already switched on, definitely switch it on!

There are a few passwords which are so critical that you might want to write them down. Examples:

- Microsoft (which will also be your Skype and/or Teams password; changing one changes the others)
- Your email service, such as Gmail, plus any alternate email services
- Your bank(s)

These are just a few examples. There may be others which you wish to always have access to, if your computer should become lost, damaged, or stolen. (Although you should be able to eventually access your information from another computer, it will likely be easier if you have the relevant passwords.)

Printing a Hard Copy List of Passwords

As another option, once you've strengthened your passwords, you can download the remaining list. In the case of Chrome, this list (which will be in CSV format) will include the name of each website, its URL, your username for that site, and your password for the site.

Needless to say, if you print out this list, it needs to be kept in an extremely safe place. Should an intruder find this list, you would be extremely compromised.

Also be sure that if you update any key passwords, that you either rerun this listing, or annotate the list with the new password. Nothing is worse than finding (as I have) that the password on your list is no longer valid.

Creating a Master Password

If printing out a list of your passwords makes you nervous – which I certainly understand –another option is to create a master password, which is just what it sounds like: one password which will allow you access to all of your accounts and websites. This is done by linking individual passwords to the master, so the master is the only one you need to remember.

I am not personally a fan of master passwords, as having one password seems to me to undo the purpose of having individual passwords for different sites and accounts. If anyone got hold of that master password, you'd be in a world of hurt. A master password needs to be long and complex, something which can't ever be guessed – and therefore will be difficult for you to remember. So why not rely on strong passwords suggested by, encrypted by, and saved by your browser?

However, if you would like to pursue this option, you can learn about how to set up a master password in Chrome or Firefox in this article:

https://www.computerhope.com/issues/ch002030.htm

Regardless of whether you opt to use a master password or a list – or neither - **I suggest that you go into your browser's password manager right now and run a check of weak and reused passwords.** Like me, you might be surprised at how many there are. Then schedule time very soon to update the passwords with strong ones.

Multifactor Authentication

To enhance your security even further, you may choose to implement – and in some cases, be forced to implement - multifactor authentication (MFA).

MFA, also referred to as two-factor authentication or 2FA, requires a second step in the log-in process. For example, let's say that you enter your user ID and password on your banking website. A window then displays which says that the bank needs to call, email, or text you; you then select an option. You will receive a code by the method selected, which you enter online to confirm your identity.

MFA is often required if you log in from a different device or location than usual. Yup, the bank – or other company – can actually determine that.

And yes, MFA can be annoying if you're in a hurry, but it greatly enhances your security for the extra seconds it requires. MFA is becoming more and more common these days, for the unfortunate reason that it's necessary in today's hacker-happy world. So if it is offered to you as an option by a website you frequent, I suggest that you enable it, especially if sensitive data might be at risk.

Reduce Your Exposure

Consider how many websites have a profile for you. Stop and think for a moment. Financial sites, travel sites, sites relating to hobbies, social media sites, e-tail sites...and the list goes on.

You can reduce your exposure to hacking and data breaches by cancelling memberships and opting out of sites you no longer wish to visit. You can do this at the same time as you are strengthening your passwords. So, update passwords for those sites you intend to visit again, and cancel your profiles on the rest.

Similarly, it could be time to prune your friends in Facebook, Instagram, etc. Facebook in particular seems to be prone to hacks. You may have been hacked yourself – as I was just recently – or received a message from a Facebook friend saying "It wasn't me…!" You might head off some hacks and certainly reduce visibility by doing some spring cleaning. And who knows? During the process of weeding out old "friends", you may stumble across some actual friends that you haven't contacted in a while and want to reestablish contact with.

You might also consider signing up with https://incogni.com/, a subscription service which contacts data brokers and requests that your information be scrubbed from their databases. I subscribed recently and was amazed at how many data brokers had my information (well over 100!). Incogni got to work immediately, sending out requests to purge my information, and sending follow-up requests as needed. For more information about Incogni, visit www.CybersecurityMadeSimple.net.

Let's move on now to discuss another layer of protection: virus-protection software and VPNs.

Virus-Protection Software and VPNs

Most of what we've discussed so far can be accomplished at no cost other than a bit of your time. Now I'm going to ask you to part with a bit of your hard-earned money. I want to encourage you to invest in virus-protection software and a VPN. Consider them to be cheap insurance, and essential components of your overall cybersecurity program.

Antivirus Software

Hackers are clever folks, and have created many inventive ways to invade your devices. Antivirus software seeks to prevent malware from entering your devices, and also to neutralize any that does manage to get through.

There are many companies providing such software, including Norton, Bitdefender, AVG, and Kaspersky to name only a few. Very likely you already have antivirus software installed on your computer, but if not, you really should subscribe to a reputable service as soon as possible. Note that today most companies offer antivirus protection for all of your devices. Because smartphones and tablets are as vulnerable as computers – and are often used more frequently than your computer – be sure to get coverage for **all** of your devices.

(If you happen to use a Mac user and still cling to the notion that Macs are immune to viruses, please read this article: https://www.digitaltrends.com/computing/does-your-mac-need-antivirus/.)

Whichever virus-protection software you opt for, be sure to run thorough scans frequently. You can set up most antivirus software to scan automatically at a preset time when you are not likely to be using your computer. That way, you don't have to worry about forgetting to run a scan, and the scan won't interfere with your work. (Some scans, especially "deep" scans, can slow down processing while they are running, and may require you to exit programs, close your browser, and restart your computer after the scan.)

New viruses pop up all the time. Accordingly, antivirus software is updated frequently, and you need to be sure that you are accepting updates regularly. You should be prompted to accept updates automatically, but it's a good idea to check for them periodically – certainly before running a deep scan.

VPNs

In addition to installing antivirus software on your devices, I recommend that you also consider having a VPN. A VPN – which stands for "virtual private network" – acts as a shield to block many attacks. VPNs reroute your data through their own secure servers and also provide end-to-end encryption, making them more secure than standard ISPs (internet service providers).

I consider a VPN an absolute necessity if you frequently use public wifi (think cafes, airports, hotels, etc.). But even if you only log in from home, a VPN provides extra security. Antivirus software and a VPN together are like a moat and strong castle walls.

You can toggle VPNs on and off. Be sure to keep the VPN turned on as a general rule. Some companies – Netflix is one example – may require you to turn off your VPN to access their site. (They are trying to prevent the sharing of user logins, which a VPN could facilitate.) Be sure to turn the VPN back on later – and absolutely before doing anything sensitive online, such as banking.

For a comparison of various companies and their offerings (some also offer VPNs and other associated services), visit www.CybersecurityMadeSimple.net.

Having a VPN plus virus protection software
is like having a moat and castle walls.

Backup and Recovery Plan

As Scottish poet Robert Burns observed, "The best laid plans of mice and men often go awry."

Despite religiously following best practices, you might be the target of a data breach outside of your control, or fall victim to a sneaky new virus that evaded your antivirus software, or lose your computer to a sneak-thief at the airport. Or it could be something more prosaic like your hard drive crashing. (Sigh.)

Regardless of the cause, the result is the same: your data may be compromised and lost, through no fault of your own. And for many of us, losing data is not just an inconvenience. It might put our livelihoods at risk if we aren't prepared.

So I encourage you to schedule regular back-ups. In fact, in the spirit of my late father, who often wore suspenders **and** a belt, I encourage you to back up your critical data both on an external hard drive and in the cloud.

External drives become cheaper every year, so this is one time when it's fine to supersize. There are countless brands on the market. I would, however, look for one that specifically says "fast" or "fast loading". Its load speed may depend in part on its cable, so take a minute to read the product description and reviews. Oh, and make sure that the cable will fit your specific device!

As far as cloud storage, again there are countless providers. I use Google Drive (buying extra space for $9.99 per month), but you may have your own preference. With servers now very dependable and memory increasingly cheap, price is often the determining factor, but do check reputation as well. For a discussion of various cloud storage providers, visit our companion website: www.CybersecurityMadeSimple.net.

Just as having expensive golf clubs means nothing if you've never taken a lesson, having the means to back up your data means nothing unless:

1. You in fact regularly **do** back up your data, and
2. You know how to restore data should that ever be necessary.

Your cloud storage provider should provide step-by-step instructions on how to restore your data. In fact, be sure that any cloud storage service you are considering does provide clear instructions before subscribing.

Restoring data from an external drive likewise shouldn't be difficult provided that you are organized when backing up your data. This is largely a matter of clear and consistent naming of folders and files, and then actually doing the backups to the correct folders. I make backups as a part of my Friday end-of-week routine, along with cleaning my keyboard and clearing my browser of cookies and unwanted cache.

I encourage you to create a backup plan. Note that all data is not created equal. Some is less critical, some more so; some is more static, some updated daily. Use these factors to help you determine how often to back up your data. Monthly might be just fine for some folders, while daily may be right for that book or contract that is still being amended. It's all a matter of balancing risk of loss against the time to do the backup – which, let's be honest, isn't much.

To help get you started, follow these steps:

1. Take a look at the folders on your computer.
2. Ask yourself which ones are essentially static. Backing these up monthly may be fine.
3. Which folders are updated frequently? Examples might be presentations, contracts, proposals, or an article or book you're writing. Backing these up weekly means that you shouldn't lose more than one week's worth of work.

4. You may even want to back up some files daily. If that's the case, consider making things easier on yourself by keeping these work-in-process files together in a single folder which can be easily dragged and dropped into an external drive.
5. Also check to see if your cloud storage does backups automatically or needs to be manually launched.

If you implement all of the recommendations in this section, you will be much more secure. The simple steps discussed here will greatly reduce the chances of your becoming a victim. However, that doesn't mean that you are wearing a suit of impenetrable armor and are impervious to cyberattack. (If only if were that simple!)

No, you must still remain vigilant, which we consider in the next section.

Be Aware

In the first section we discussed the importance of preparation in averting cyberattacks. While having a solid cyber-security plan in place is of course critical to your safety, you'll also want to remain vigilant and cautious whenever you are online. You really can't afford to let your guard down, even when you are scurrying about and multitasking.

In this section we'll look at several behavioral best practices and also offer some tips about what to watch out for when online. Specifically, we'll cover:

Social media awareness. How can you avoid problems while still enjoying your favorite social media platforms?

Smartphone best practices. Given that more and more folks are accessing the internet via smartphones, it's important to understand the special threats involved.

Social engineering. This is a blanket term for tricking people into revealing sensitive information through trickery and gaining trust. We'll focus on one of the most pervasive types of social engineering: phishing emails.

Shopping online. While shopping online provides us with many more options and allows us to save time versus running from store to store, it can also open us up to potential scams.

Staying safe in public places. Being able to access the internet from just about anywhere has made our lives easier in many ways. (Does anyone remember life before GPS?) But just how safe is accessing the internet while in public, and how can you best secure your connection?

You can greatly reduce your exposure by doing two things:

1. Always being vigilant when online, and
2. Staying up-to-date on current scams.

Let's move on now to look first at social media.

Social Media Awareness

Social media truly is a double-edged sword. Social media platforms can be fun, entertaining, and a great way to stay in touch with friends and family. But social media can also expose you to risks such as being called out or even cancelled, or inadvertently revealing too much personal information.

Fortunately, adjusting your settings and observing a few common-sense rules will help you sidestep most potential issues. Even if you don't use social media very much, others in your household, including your children, may; if this is the case, you will definitely want to practice social media awareness in your home.

First, adjust the privacy settings for all users. All of the major social media platforms – including Facebook®, Instagram®, TikTok®, X® (formerly Twitter), and YouTube® - allow users to adjust their privacy settings. Go into Settings, then Privacy or something similar; if you can't find what you are looking for, just go to Settings and search "Privacy".

(A special note regarding TikTok. At the time of this writing, there is a concerted effort by members of the US Congress to limit TikTok in the US, or to ban it altogether. The fear is that TikTok, which is owned by a Chinese company, may collect data on users which it could be forced to share with the Chinese government. Whether the threat is real or high is open to debate, but it is something to bear in mind. You may opt to ban TikTok in your home.)

And when logged into social media, regardless of the platform, it is wise to keep in mind what has been dubbed "Digital Permanence." Whatever happens in Vegas may stay in Vegas (maybe), but whatever goes online, stays online (definitely). Posts, photos, and all other content can spread rapidly and soon becomes impossible to remove completely. The message should be clear: Think before you post.

It's worth noting here that the areas of the brain which oversee control and restraint are some of the last to mature. What this means in practical terms is that teens – who love to be online, often on social media – will often want to react to comments before giving due thought. If you have youngsters in your home, talk to them about the important of not reacting rashly, and of measured responses.

In addition to **what** you post, you should also be careful about **when** you post. Sure, you might want to make your co-workers and obnoxious sister-in-law jealous by posting photos of your wonderful daytrip in Bali as soon as you're back in the hotel. But doing so could also be alerting bad actors that you are away from home, and likely to be away for several days yet.

For more about Social Media Awareness, refer to Chapter 1 of Cybersecurity Made Simple.

Smartphone Best Practices

We sometimes forget what a "smartphone" really is: a handheld computer, nothing more nor less. These days, many folks use their smartphone more than they do a desktop or laptop – meaning that it is their primary point of exposure to cyberthreats.

More smartphones run on Android than any other system, so it should be no surprise that a wide variety of malware targets Android devices. That said, iOS devices aren't immune from attacks, despite what some Apple adherents want to believe.

Fortunately, as noted earlier, most antivirus software options available today protect a variety of devices, including smartphones. Many safeguard both Android and iOS devices. So when shopping for virus protection, make sure to get one that covers all of your devices, including your smartphone.

But even with built-in virus protection and additional antivirus software, you should still exercise due care in the moment. While that should be obvious, it's all too easy to forget when you are running late, juggling multiple tasks, or about to board a plane and trying to handle business before having to put your phone on airplane mode. But you need to force yourself to think before automatically pushing buttons.

Here are some warnings which apply specifically, or mostly at least, to smartphones:

If you receive a text from an unknown sender with no subject, don't open it; simply delete it. If you do open it (curiosity can be a powerful thing) and see an attachment, for goodness sake do not open it! But I personally would not even open the message.

While on the topic of texts, a scam that I've seen a few times recently is the sending of a text to some unknown (and likely fictitious) person at my number. I typically reply that there is no one by that name using my number. After all, the text may actually have been sent in error. (I do **not** give the sender my name, of course.) However, if the sender then replies with an apology and tries to engage me in an exchange, I block them and delete the message string.

Spam calls are also a common threat. These could be legal – if annoying – calls from salespeople or donation solicitors. But they might also be something more insidious. My elderly mother has on two occasions received calls by someone purporting to be her grandson, asking her to send money to handle some imagined emergency. Don't humor these people. Just hang up. You could also file a complaint on the FBI's IC3 website. If you receive a lot of spam calls, consider downloading Robokiller, a free app that blocks many such calls.

You might receive phishing emails on your smartphone as well as your computer. Phishing emails or texts fall under the general heading of Social Engineering, which we'll discuss below.

A possible threat which you may not have considered before is QR codes. QR codes, if you didn't know, is the name for those odd checkerboard squares which you can scan with your smartphone. They can be quite useful, allowing you to claim product discounts, board a plane without a paper coupon, or learn more about a product simply by scanning the code. You might even pay to park your car by scanning a QR code.

But although QR codes may look innocuous, they can actually be quite dangerous. They might, e.g., send you to a spoof site and steal that parking fee – and perhaps more. One reason that QR codes can be insidious is that, while we humans can read a URL, we can't read a QR code, and so we can't know where we are actually being routed when we scan a code. To head off potential problems, simply do not scan suspect QR codes, including:

- Codes in random places, such as a bus stop or lamppost
- QR stickers which appear to have been physically altered in some way, perhaps by adding one sticker (perhaps fraudulent) on top of the original sticker

- Codes in unsolicited snail mail

Typical QR code

Let’s now turn our attention to one of the most common threats out there: Phishing and other social engineering attempts.

Phishing and Other Social Engineering Attempts

One of the most common types of cyberattacks is "phishing". It's one form of what is termed "social engineering", which are attempts to manipulate people into providing sensitive information. We are going to focus on phishing, but if you'd like to dive into the broader topic of social engineering, here is a good article: https://www.fortinet.com/resources/cyberglossary/pretexting.

Phishing attempts most often are emails which purport to be from a legitimate entity and attempt to elicit sensitive information from you, such as your Social Security number or a password – often to "prove" to the sender who you are.

Sometimes the phishing email will request the information directly. Other times it might direct you to a "spoof site" which is a phony site designed to look like a legitimate one, such as the site of your bank, a utility, or perhaps an e-tail store you have purchased from. You are supposed to log in to the spoof site – thereby providing your log-in credentials to the scammers.

How do you deal with phishing attempts, and the related "pretexting" attempts? (Pretexting is quite similar to phishing but the scammer seeks to build rapport before asking for sensitive information– think "long con".) First, you should learn to recognize them.

Understand that legitimate entities are **not** going to send you an email requesting sensitive information (Social Security number, account PIN, user ID or password), so any such request is suspicious, in and of itself.

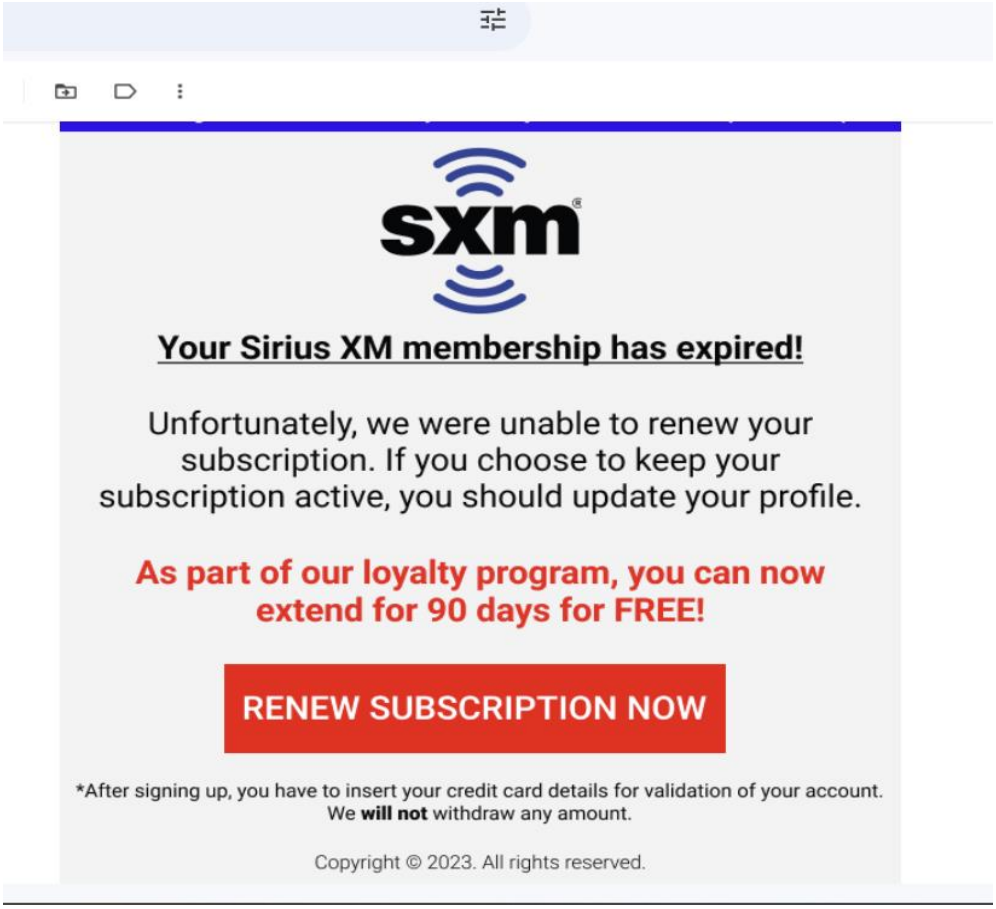
Other tip-offs include:

- The sender's email address doesn't look right. It either doesn't reflect the supposed sender at all, or contains misspellings such as transposed or duplicate letters.
- Images, such as the company's logo, are fuzzy or of low quality.
- The sender expresses urgency, trying to get you to act rashly before thinking the situation through.

If you receive such an email, contact whichever entity supposedly sent you the email. Do so through their known website, **not** through any link or phone number provided in the suspicious email. You may also wish to file a complaint through the FBI's IC3 site.

Phishing emails are common. As I matter of fact, I received a few just recently. I'll post two of these on the following pages as examples, so you can have a better idea of what to watch out for:

Example of a Phishing Email



There were a few tip-offs that this was not a legitimate email:

1. I don't have an SXM account!
2. This email was sent to a few email addresses which contained my first and last names with various other characters – clearly, the sender had my full name, but was guessing as to what my email address might be.
3. Also, the sender's email address was odd, and definitely not from SXM:
   - SiriusXM® <contact_support.asv@news.usifalow.co.uk> via upnorthswipe.com
4. Finally, the copyright notation at the bottom was clearly added to try to lend some credibility to the email, while in fact doing just the opposite.

What did I do? I took a screenshot so that I could show this example to you, and then clicked the Spam icon in Gmail (which is at the upper left and looks like a stop sign with an exclamation point inside). I saw no risk of a virus or mal-ware, but I certainly wasn't going to click the button and enter my credit cards details!

Scammers can be clever, and often introduce urgency into their pleas. Don't' be fooled.

Another Example of a Phishing Email

Below is another actual phishing email I recently received.

Brie Hassan <hassanzbricenoj2085@gmail.com> 7:03 AM (2 hours ago)

to me

GEEK RECEIPT

Date : Mar 04, 24

Hey, richards.bill

We appreciate having you in our family and respect your decision.

You may rest easy knowing that your device is protected since your automatedly update plan is enabled.

Details are mentioned below:

Receipt No : **#C93060550**

Description	Tenture	Total Value	Payment Mode
GT Global	l2 months	$ 523.12	Online

Status : **Successful**

Your e-statement will display the amount in Up to 24 hours billed for the plan..
To call off your plan, phone us at:

<+ l.801.305.32 6l

Comments:

Again, I don't have an account with GT Global, so I immediately clicked SPAM. No doubt you can also spot, as I did, several mistakes in the email. It's just sloppy, which is common in phishing emails.

Let's turn our attention now to shopping online safely.

Shopping Online

Let me share something personal about myself with you: I really hate going to the mall – pretty much shopping in general, in fact. I embraced online shopping long before many of my friends and family simply because of my distaste for shopping the old-fashioned way.

You may or not share my sentiment. Regardless, we must exercise care when shopping online. Excitement over finding a hot deal can easily turn to disappointment and anger if our purchase never arrives, but a charge still appears on our statement.

Here are a few tips to help keep you (and your credit card) safe online:

- Be wary if you are clicking on an ad for a company that you've never done business with before – perhaps never heard of. Yes, most of such ads are probably for legitimate companies. Just proceed with caution.
- If a website looks amateurish, or in any way suspect, that's a major red flag. It might be a spoof site (a rip-off site designed to mimic a legitimate site). Just close the tab or window.
- Never buy anything from a website that doesn't begin with https. That "s" is important, as it indicated a secure website which has been verified.
- Make purchases using a credit card rather than a debit or gift card. Fraud laws grant you greater protection if you use a credit card. For details, read this article: https://www.nerdwallet.com/article/credit-cards/credit-card-vs-debit-card-safer-online-purchases.
- If given the option on an e-tail site, don't save your card information. Even if the e-tailer is a known, legitimate entity, and you plan to make future purchases on their site, remember that they could be hacked and your card information stolen in the resulting data breach. Even large companies are hacked.

For more about safe online shopping, you can review Chapter 6 of Cybersecurity Made Simple.

Staying Safe in Public Places

No doubt you often find yourself accessing the internet while in public. You may be on your computer or tablet while at a hotel, in the airport, or in a coffee shop. Or you may be on your cell phone at the mall or in some other public space.

So, how do you stay safe online when in public?

If you're accessing the internet via your cell phone, you'll be safer if you use your cell's data plan than a public wifi (aka, a "hot spot"). Not that you'll be 100% safe, but you will be much safer than using public wifi.

However, you may be out of, or low on, data. Cell service can also be slower than wifi. These factors make it tempting to use wifi, even if it's public. Or you may be accessing the internet via a tablet or laptop, in which case may the public wifi be your only option (unless you can use your phone as a virtual hot spot). If you really must use public wifi, I suggest that you:

- Enable your VPN. (Hopefully you have one now!)
- Restrict your activities to the minimum. **NO** banking or online shopping!

For a good rundown of accessing the internet via cell or wifi, you might want to read this article: https://www.wilsonamplifiers.com/blog/cellular-vs-wifi-how-safe-is-cellular-data.

One final note: Technology aside, practice common sense. If there is someone lurking behind you, it's best to move. The name of this section is, after all, "Be Aware".

Keep yourself informed

The world of technology is fast-paced, and there's no reason to think that it's going to slow down. Likely just the opposite, in fact.

One consequence of the relentless advance of technology is that hackers exploit changes almost as soon as they arrive.

That means that you have to view your cybersecurity as something that you must actively maintain. Updating your social media privacy settings and strengthening your passwords is a good start, but you have to treat your online security as an ongoing process, not a one-time task. You need to make best practices **habits**.

Besides implementing what we've covered in Cybersecurity Made Simple and this workbook, you should strive to stay updated about current threats. Here are a few suggestions:

Visit the companion website, www,CybersecurityMadeSimple.net. On the blog you'll find updates about the most recent threats and data breaches. You can also compare various antivirus and VPN software offerings to find the one that's best for you.

I also plan to create a monthly newsletter recapping the most important news. You may find it easier to stay current by perusing it once each month rather than by visiting the blog. You can sign up for the newsletter on the website.

You should also become familiar with the FBI's Internet Crime Complaint Center, or IC3 (https://www.ic3.gov/). You can file a complaint there, and there are also pages devoted to topics like Elder Fraud and Common Scams.

If you, or someone you know, belongs to AARP (the American Association of Retired Persons), then check their newsletter, which frequently included alerts about new scams.

Finally, just remain alert to updates in the popular media. For example, the next time you read or hear about a data breach, stop a moment and consider whether **your** data might have been accessed.

Cyberthreats have become a part of modern life. Playing ostrich won't keep you safe, so make up your mind to be vigilant.

Respond

It can still happen: You might one day find yourself the victim of a cyberattack. Perhaps it wasn't even due to your own negligence. Perhaps your information simply resides in the database of a company which was targeted and breached by hackers.

In the end, it is still up to you to take control of your online security, and to respond in an appropriate manner.

When you need to respond, you'll want to be able to do so quickly, but in a calm and deliberate manner. Getting flustered and rambling while speaking with someone at your bank or other institution isn't going to help get your issue resolved faster; quite the opposite.

So in this section, we'll look at:

- Pulling together your system and contacts' information so that it will be at your fingertips if needed,
- Dealing with data breaches, which unfortunately happen fairly frequently, and
- How to complete an incident log, to keep yourself organized during the resolution process.

There are also some training exercises to test your knowledge.

Be prepared to respond if need be!

System and Contact Information

Record below the requested information, so that it will be immediately available if needed.

Internet Service Provider (ISP) information:

Company name (e.g., Comcast): _____

Customer Service Number: _____

Website URL (for problem reporting): _____

Note:

Your ISP is the company which connects you to the internet and likely installed your router. A few of the larger ISPs are AT&T, Comcast, Charter, Verizon, and CenturyLink.

System and wifi Information:

Router ID: _____

Modem ID: _____

Wifi network name: _____

Wifi password: _____

Guest wifi network (if applicable): _____

Guest wifi password (if applicable): _____

Notes:

IMPORTANT: Be sure that your wifi system password is long enough and impossible to guess – so not the name of your child or dog, or a simple string like 0123456789. If someone manages to guess your wifi password – and this could be someone parked on the street outside your home – then your castle wall has been breached.

If you change your wifi password, sure to record the new password here.

If you frequently have guests, you may wish to create a separate network for their use. Likewise, you may wish to have separate networks for parents and children, with differing permissions and security features in place.

Virtual Private Network (VPN) information:

Company name: _____

Customer Service Number: _____

Website URL (for problem reporting): _____

Note:

A VPN provides a strong layer of security for your system by encrypting your data and routing it through its own servers rather than your ISPs. Many companies provide VPN services at modest costs. To compare various VPN offerings, you can visit www.cybersecuritymadesimple.net.

Virus protection software + contact info.

Company name: _____

Customer Service Number: _____

Website URL (for problem reporting): _____

Note:

Some well-known names in virus protection are Norton, McAfee, Bitdefender, and AVG, among many others. Many antivirus software companies also provide VPN services, so this information may be the same as what you entered above for your VPN provider.

The FBI's Internet Crime Complaint Center: https://www.ic3.gov/

Note:

You may want to familiarize yourself with this website today.

Local technical support contact information:

Company name: _____

Customer Service Number: _____

Website URL (for problem reporting):_____

Note:

Don't wait until you have an emergency to look for local tech support. Ask people you trust to recommend a trustworthy, responsive company. Do it today.

Financial institutions contact details:

Record here the information for your bank(s), credit card issuers, and other financial companies, such as IRA servicers. You'll need this information should you become a victim of fraud.

Company **Phone number** **Website address**

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Dealing with Data Breaches

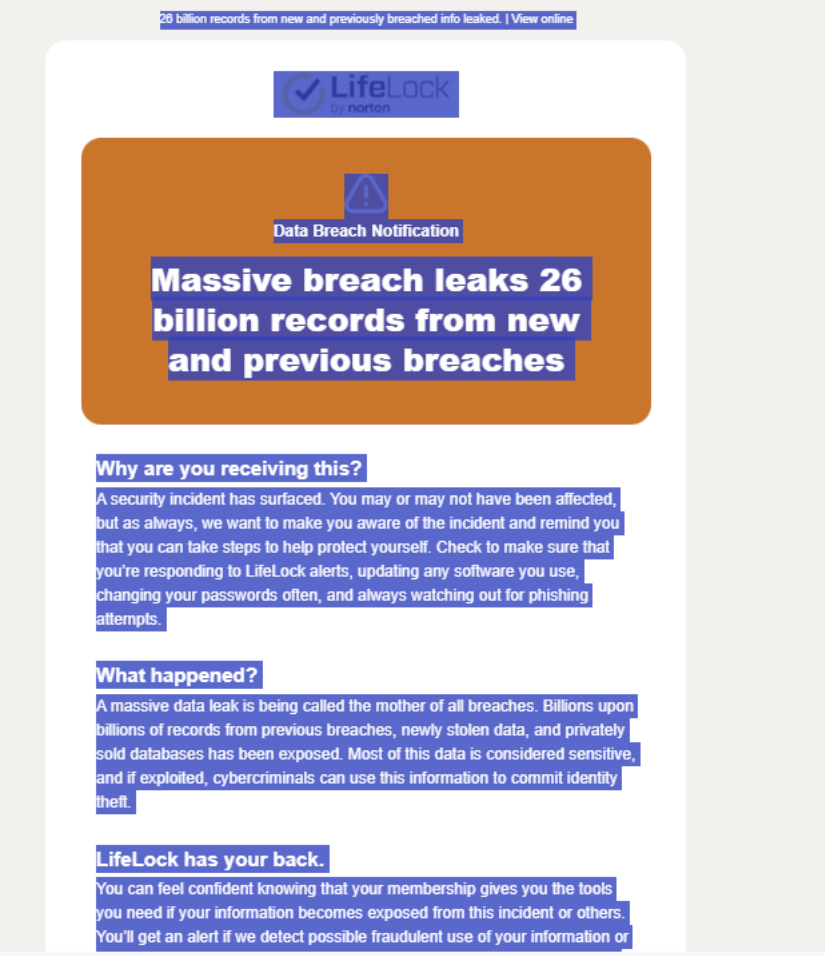
As noted earlier, even if you do everything you can to head off cyberattacks, you can still become a victim. One common way this might happen – through no fault of yours – is a data breach.

We've all read or heard about data breaches. Don't make the mistake of thinking that breaches only happen to big companies and so aren't your concern. Yes, companies are the typical targets, but they can hold data about thousands, perhaps even millions, of individuals just like you.

Here is a screenshot of an actual notification I received recently from Norton LifeLock regarding a massive data breach:

Example of a Data Breach Notification

26 billion records from new and previously breached info leaked. | View online



Earlier, in the discussion about passwords, I posed the question, "How does a password become compromised?" It might well have been through a data breach, meaning a hacker gained access to a website on which you used that password. Regardless of the source of the issue, you'll want to change any compromised passwords ASAP.

What else can you do when you receive a notice about a data breach? Unfortunately, not a lot. These notifications go out after the breach has been discovered and damage done. Sometimes the breach isn't discovered for quite some

time, so it may have happened long before you received a notification. Beyond updating any password(s) which may have been compromised, also check for any unauthorized charges or other activity on accounts which may have been accessed.

Incident Response Log

Suppose one day it happens: One of your accounts – let's pray it's just one – is hacked. You might receive a text or email alert from your bank, credit card issuer, or other service alerting you to suspicious activity involving your account. Or you try to log into an account and find that you can't.

What do you do?

First, take a deep breath, and don't panic. Yes, you'll want to act quickly to contain the situation and hopefully avert or contain damage, but getting worked up will not help you to think clearly and act appropriately. So take a few deep breaths.

Next, write down exactly what happened. I know, this step may seem a waste of time at this juncture, but when you go to report the issue, you will want to be clear and concise. Also, when we are flustered, it's easy to become a tad confused. So while the details are fresh, record the time, exactly what you were trying to do and the result, and any actions you may have already tried, such as entering various possible passwords.

Believe me, this information can become very helpful later when reporting the issue. You won't have to recall the details of exactly what happened while on a call or in a live chat. You can read confidently from your notes, or cut and paste them. It's quite likely that you'll have to speak to more than one person, and a written record helps you to be clear and consistent in each conversation.

Next, get in contact with the particular entity involved, whether it's your bank, an e-tailer, Facebook, or whomever. I prefer, whenever possible, to speak to a person; however, these days it can be difficult to reach someone by phone – if you can even find a number for Customer Service. As email exchanges can be slow, your next-best alternative to speaking with a person is live chat. Hopefully you can reach a real person. If you are instead connected with Suzy the AI Assistant, ask in the chat to be connected to a real person.

Once connected (or via email, if that is the only option available – and be sure to copy yourself, if you must use email), lay out the facts. Be as clear and succinct as you can be. You are seeking help, and you want to make resolving your issue as straightforward as possible. Avoid giving unnecessary details or repeating facts, and try to present events in chronological order.

Also, avoid ranting, and be careful about blaming any individual or company at this point. Your focus is on getting the issue resolved, and you want folks in your corner. Putting someone on the defensive won't help you.

You'll want a record of having reported the issue. If you spoke to a live person, get his/her name (sometimes an ID number is provided instead), and immediately after the call, while all is fresh, make relevant notes on the incident log. If you had a live chat exchange, you can typically request that a transcript be sent to you via email when ending the chat.

You can find an example issue log at the end of this section.

The old adage is that the wheels of justice turn slowly. That is true not only in the courthouse, but is often true in cases of online fraud as well. Now that the incident has been reported, stop and decide on your next steps.

- Do you need simply to be patient while you wait for a reply? Is the matter now squarely in someone else's court?
- Do you need to take steps to prevent further spread of the damage? This might involve, for example, checking other accounts which might also have been hacked, making additional phone calls, or updating passwords.

- If you have reason to believe that your router has been hacked, you may want to disconnect it physically from the internet until it is determined that it is safe to reconnect. If you do decide to take this step, first be sure that you provide the people working your case with an alternate way to contact you.
- Depending on the nature of the attack, you may wish to report it to the FBI's Internet Crime Complaint Center at https://www.ic3.gov/.

Once the cause of the attack is established, consider what steps you can take to prevent another such incident.

It's normal to feel angry, violated, and even guilty after suffering an attack. But thousands of people suffer cyberattacks every year – even me, the author of a book about cybersecurity! Yes, I was recently a victim.

Just last week (as I write this) my Facebook profile was hacked; it has not been established yet how this occurred. The clever perp not only changed my password, blocking me from accessing my account, but also changed the email address associated with my account. Since the email address is one way Facebook uses to verify a member's identity, I was again blocked: I entered my (absolutely valid) email address as requested by Facebook, but it wasn't recognized, having been superseded. Receiving a text message from Facebook at the phone number associated with your profile is supposed yet another way to confirm identity, but for some reason the Facebook page was not letting me enter it, defaulting repeatedly to the email.

Finally, I had to upload a jpeg image of my driver's license to verify my identity. I'm still waiting for a resolution.

Morals:

- Even social media passwords need to be strong. (Mine wasn't. I know, shame on me.)
- Always have readily available a jpeg or gif of a photo ID. It may be the only way to prove your identity in case one of your accounts is hacked.

Incident Log

Date: **Time:**

Description of incident:

Who was contacted:

How was contact made (phone, live chat, email)?

Resolution or actions to be taken:

When and how should follow-up take place?

Emergency Response Training Exercises

Let's see if you can apply what you've learned from this workbook. How would you handle the situations below? Answers and discussion are presented on the following pages.

What is the single most effective – and simplest – way to protect yourself from cyberthreats?

What is "multifactor authentication" and how does it help protect you?

How often should you scan your computer for viruses and malware?

How often should you back up your data?

What is a VPN is, and how it helps safeguard you?

Name two things that you can do to reduce your chances of problems on social media?

You receive a text from an unknown number. There is no subject but there is an attachment. What do you do?

You park your car. On the parking meter there is a QR code sticker – but there appears to be another sticker underneath. What do you do?

What is "phishing"?

Follow-up questions: What are some clues that an email may be a phishing attempt? What steps should you take to verify the authenticity of the email and protect yourself from potential phishing scams?

You sit at your computer to do some Christmas shopping online. What are some ways that you can protect yourself. ? (known e-tailers only, use CC not debit, don't allow site to save your info)

You are logged in at a café using their public wifi. What steps can you use to protect yourself?

Suppose that you are notified by email or letter of a data breach. What actions should you take?

Have you completed the System and Contact Information form?

What are some key components of any individual's personal cybersecurity protection plan?

I encourage you to think through these questions, and perhaps jot down some thoughts, before reading the answers on the following pages.

Q: What is the single most effective way to protect yourself from cyber threats?

Answer: Using strong (cryptic) passwords, preferably a unique one for every website you access. Weak passwords are a major source of hacked accounts. Strong passwords make hacking your accounts much more difficult. They should include a mix of upper and lower-case letters, numbers, and special characters, and should not make any intuitive sense, making them essentially unguessable. So how do you remember them? Let your browser's password manager do that for you.

Q: What is "multifactor authentication" and how does it help protect you?

A: Multifactor authentication (MFA) requires a second step when you are logging into a site. This is especially common if you are logging in using a new device, or from a location which is different from your usual one. After entering your user ID and password, the system will ask either to call you or send you a verification code by email or text. Upon receiving the code, you enter it on the website to finish the login process. MFA is increasingly common these days, and while is can be a minor inconvenience, it greatly improves your security.

Q: How often should you scan your computer for viruses and malware?

A: Frequently. If you go online often, daily is not too often. Scans, especially "deep scans" can slow some computer programs though, so you will want to run them when you are not using your computer; your antivirus software will almost certainly allow you to schedule a scan for a convenient time.

Q: How often should you back up your data?

A: It depends on how often you update your data. Some data will likely be more or less static, and monthly backups may be just fine. However, for work in progress, you may wish to back up daily. To make the backup process easier to do (so you'll actually do it!), you may wish to keep all work in progress in a single folder until it's completed.

Q: Can you define what a VPN is, and how it helps safeguard you?

A: VPN stands for Virtual Private Network. A VPN reroutes your data from your ISP's servers through its own, and encrypts your data as well. You should always use a VPN if you are using a public wifi, such as one at a café or hotel, and always use one when accessing sensitive information, such as financial data. VPNs cost little compared to the protection they provide; they are often licensed bundled with virus-protection software.

Q: What are two simple things that you can do to reduce your chances of problems on social media?

A: First review your privacy settings in all of the social media platforms that you use. And think before you post, especially if you are angry or upset. Remember that you can't be sure who all will see your posts, and that the internet is forever.

Q: You receive a text from an unknown number. There is no subject but there is an attachment. What do you do?

A: The safest thing to do is to fight curiosity and simply delete the text. You don't know who the text is from, or what it is supposed to be about. But you do know (or should) that malware is often embedded in attachments. So just delete the text. If it truly is legitimate and important, the sender will get back in touch with you.

Q: You park your car. On the parking meter there is a QR code sticker – but there appears to be another sticker underneath. What do you do?

A: Don't scan the QR code! A QR code can be covered by a bogus sticker which directs the person scanning it to a spoof site (fake site designed to look legitimate). In fact, this is a common scam these days. Unfortunately, this will likely require you to move your car, unless another method of payment is available.

Q: What is "phishing", and how can you recognize a phishing attempt?

A: Phishing is a fraudulent activity involving sending emails that appear to be from reputable companies to trick individuals into disclosing personal information. The sender typically poses as a trusted entity you know, such as your bank or a utility. Here's a typical scenario: You receive an email claiming to be from your bank, asking you to click on a link to update your account information.

Q: Follow-up questions: What are some clues that an email may be a phishing attempt? What steps should you take to verify the authenticity of the email and protect yourself from potential phishing scams?

A: The first thing you may notice is that the English in the email isn't quite right. Any logos may be fuzzy, as if scanned in. Also check the email address of the sender. It may not reflect the supposed sender at all, or it may contain misspellings or transposed letters which aren't immediately noticeable without careful reading.

If the email appears to be a phishing attempt, you may wish to post a complaint on the FBI's I3C website. You should also contact the supposed sender (your bank, utility, etc.) to notify them of the fraudulent scheme. Do **not** under any circumstances reply to the email – even to tell them that you've reported them – or click any links contained in the email.

Q: You sit down at your computer to do some Christmas shopping online. What are some ways that you can protect yourself?

A: There are several simple things that you can do. It's safest to limit your shopping to known e-tailers. Never buy anything from a website if the URL doesn't begin with https; the "s" indicated a secure, verified website. Pay using a credit card rather than a debit card, as you'll have greater legal protection in case of any issues. And if asked, don't allow the site to save your card information.

Q: You are logged in at a café using their public wifi. What steps can you use to protect yourself?

A: Turn on your VPN. Even with that, it is advisable not to make any financial transactions. Also be careful of old-fashioned spying. Could someone see you enter a password, or overhear a sensitive conversation?

Q: Suppose that you are notified by email or letter of a data breach. What actions should you take?

A: First, reread the communique carefully. Rereading may take a few minutes, as such communications are often lengthy, but be sure that you understand the communication. If there is any question as to the authenticity of the communication, contact the sender – and not via any information provided in the letter or email you received, but via an alternative, trusted source. If the communication seems genuine, follow the steps suggested if they seem reasonable and not apt to expose you; but do not supply any sensitive information such as user ID, etc., because it's possible the notification could itself be a phishing attempt. Also update any of your passwords which might have been compromised, and monitor any accounts which might have been compromised during the breach.

Q: Have you completed the System and Contact Information form?

A: If you haven't, you need to do this right away. You don't want to be scrambling to locate needed information in the middle of an urgent situation.

Q: What are some key components of any individual's personal cybersecurity protection plan?

A: I'd say the three main components are:

1. using strong and unique passwords. You've read again and again that using strong passwords (not Fluffy1234) is one of the simplest things that you can do to thwart hackers. Make it difficult for them, and they will likely seek an easier target.
2. implementing a VPN paired with reputable virus-protection software. Virus-protection software is an absolute must for anyone who goes online – yes, even Mac users. And if you use public wifi (think cafes, hotels, or airports, to name only a few common spots), you need a VPN as well. Consider these measures to be cheap insurance which you hope that you never need – but you may well.
3. being vigilant. Does a text or email look suspect? Then don't open its attachment. Does the nature of an email seem odd? Be suspicious. Did you get an official letter about a data breach? Change the passwords of accounts which may have been compromised. Does the shopping website you were directed to not begin with https? Then hop to another, known site. (That "s" is important!)

None of these steps is difficult nor expensive, and together they greatly reduce your risk of becoming a victim.

Checklist

Below is a list of key tasks which you should attend to right away.

Password protect (via PIN or fingerprint scan) all of your devices.

Record your important system information and emergency contact information.

Implement password management via your browser:

1. Turn on password management in the browser settings.
2. Run a check on your existing passwords.
3. Update weak or non-unique passwords with new, stronger passwords suggested by you browser.

Cancel unused memberships and purge contacts/friends on social media.

Install antivirus software on all of your devices – including your smartphone.

Install a VPN on all of your devices.

Create a back-up and data restoration plan:

- Subscribe to a cloud service.
- Buy an external drive for manual back-ups.
- Assess your data and devise a daily/weekly/monthly plan.
- Know how to restore data if it be necessary.

Find a reputable local tech support company. Don't wait until you have a problem.

And practice vigilance daily!

Practice vigilance!

Final Comments

Unfortunately, online scams are ever-evolving. Therefore, I encourage you to visit our companion website, www.CybersecurityMadeSimple.net. Read the blog to learn about current threats and data breaches. You can also read more about some of the software and services which I've recommended in this workbook and in the main book.

I provide this workbook in PDF format so that you can print out pages as needed. Be sure that you print out the System and Contact Information pages and fill them in; do this soon. I suggest also printing out a copy or two of the Incident Response Log. Keep these documents where you can find them, ideally near your home computer.

On a personal note, I wish to add that online book reviews are always welcome. They help not only me as the author, but help prospective purchasers of a book to understand better if a book is what they are looking for. We are all busy, but taking a couple of minutes to write your thoughts would be greatly appreciated. You can leave a review on Amazon by clicking this link:

https://www.amazon.com/review/create-review/?ie=UTF8&channel=glance-detail&asin=B0CV99VFGG

Of course, word-of-mouth comments to friends and acquaintances are also welcome. You may also write to me directly at info@cybersecuritymadesimple.net.

All the best, and stay safe.

Bill