



# **Cybersecurity Essentials For Everyone**

**Protecting your Small Business Systems  
In The Age of Artificial Intelligence**

**PJ Networks Computer Services**  
**(434) 975-0122**  
[info@pj-networks.com](mailto:info@pj-networks.com)  
[www.pj-networks.com](http://www.pj-networks.com)

Written by Phil Jaderborg  
CEO, *PJ Networks LLC*

Copyright 2024 - PJ NETWORKS LLC

<b>Introduction</b>	<b>4</b>
<b>The Top 7 Cybersecurity Threats</b>	<b>5</b>
1. Install OS/+Software Updates	5
Unsupported Software	6
2. Run Good Endpoint Protection Software	9
3. Prevent Identity Theft	10
4. Turn On Personal Firewalls	11
5. Avoid Spyware/Adware	13
6. Protect Your Passwords	14
7. Back Up Important Files	15
Additional Security Recommendations	16
Two-factor or Multi-factor Authentication:	16
Leaving your laptop unsupervised:	17
User account and password:	17
Installing unnecessary programs:	19
Encrypt your local hard drive:	19
Annual computer tune ups	20
Additional Cybersecurity Considerations	20
Phishing Scams	21
GIFT CARDS	23
Fake News	23
Fake Pop-up Alerts	24
Public Wi-Fi and Social Media Use	28
What is even easier than that?	29
Keep an Eye on Your Social Media Accounts	30
Security recommendations for Mac users	30
<b>Impact of Artificial Intelligence on Cyber Threats</b>	<b>32</b>
Deepfakes	33
Watch out for scammers using Deepfakes to trick you into giving away sensitive information.	33
AI Generated Phishing E-mails	34
Traditional Phishing E-mails vs AI-generated Ones	35
Hacking Kits	37
Business E-mail Compromises (BEC)	38
EvilProxy Phishing Bypasses MFA	40
Targeted Attacks	41
Cybercriminals are Exploiting TeamViewer to Infiltrate Networks.	41
How to Determine if Your Credentials Are On The Dark Web	42
The Dark Web	43
<b>Quantum Computing</b>	<b>44</b>
Quantum computing to spark cybersecurity Armageddon, IBM says.	44
Quantum's potential impact:	45
The concept behind Quantum computing is fairly basic	45

Quantum Hacking and Malware	48
<b>So, How Do You Protect Your Business?</b>	<b>49</b>
First, educate your employees	49
Restrict access to company data	50
Business-class Firewalls	50
Consolidate your data	50
Good endpoint protection	50
Back up your data	51
Encrypt your data	51
Multifactor Authentication	51
STOP – LOOK - THINK	52
DO NOT fall for pop-ups	52
Use common sense	52
DO NOT LET ANYONE CONNECT INTO YOUR COMPUTER	52
Watch out for DEEPFAKES	52
<b>What To Do Next</b>	<b>53</b>
Here is a Golden Rule to help keep yourself from getting compromised:	54
<b>Cyber Insurance</b>	<b>55</b>
The Next Steps You Should Take...	56
<b>Special Thanks:</b>	<b>56</b>
<b>Additional Resources</b>	<b>57</b>
More Resources from PJ Networks:	57
<b>Afterword</b>	<b>58</b>
<b>Addendum 1 to <i>Cybersecurity Essentials for Everyone</i></b>	<b>59</b>
CMMC 2.0 Compliance	59
<b>Addendum 2 to <i>Cybersecurity Essentials for Everyone</i></b>	<b>63</b>
Microsoft Copilot Overview	63
<b>Addendum 3 to <i>Cybersecurity Essentials for Everyone</i></b>	<b>68</b>
A Few Words of Caution About Microsoft Copilot and Generative AI	68
Start Slowly with Copilot	68
Generative Feedback	69
Some Final Considerations: Power Requirements for Artificial Intelligence	70

# Introduction

It probably feels like everybody in the world is trying to tell you about cybersecurity these days.

Many of them are trying to sell their services, but some of them are honestly just trying to help get the news out to the public about what they need to be aware of and to be cautious about. My intention is to provide a review and explanation of the many ways that everyone – including businesses as well as everyday home computer users – can better protect their data and their assets from falling prey to the most common online scams and forms of data compromise, including ransomware attacks.

So, the list of topics we are going to go through together includes the more traditional threats that we have been talking about for the last 10 years, and then we will discuss some of the newer things that are coming up in the Age of Artificial Intelligence.

Many articles on cybersecurity begin with a long list of statistics about cybersecurity incidents, but my intention is not to scare you into reading this book. I am going to assume that you are reading it because you are already interested in learning more about this topic, and learning about ways that you can protect your computers, your data, and if you run a business, ways that you can protect your business assets.

However, there is one statistic that is worth presenting right here at the beginning of this book:

## **60% of small businesses close within six months of a data breach**

If you own a business, that should be enough to keep your interest kindled as we delve into our discussion about data protection and cybersecurity.

However, if you happen to be an avid fan of statistics, then Norton™ has put together this very extensive list of the top cybersecurity statistics to know in 2024: [115 cybersecurity statistics + trends to know in 2024 \(norton.com\)](https://norton.com/cybersecurity-statistics)

I am writing this book with the intention of providing actionable tips and recommendations, and to share valuable information that any small business can

use to help protect themselves, but most of this advice is also applicable to anyone who uses a computer. I'm not necessarily going to spend the entire time dwelling on the traditional forms of cyber threats that we've been dealing with in the past, but I do feel like they are worth discussing, since they are still an active part of the cyberthreat landscape and account for the majority of data breaches and ransomware attacks going on right now.

## The Top 7 Cybersecurity Threats

The top seven traditional cybersecurity risks that we will talk about are:



### 1. Install OS/+Software Updates

Outdated software is not considered to be secure, particularly computer Operating systems (OS). Vendors regularly release updates for their products, and usually those are security-related patches. So, it is important to install updates when they become available for applications like Windows updates, Mac OS updates, Adobe Acrobat updates, QuickBooks, and other line-of-business software applications. If a program is going to touch or contain any information related to your business, then you want to keep it as up-to-date as possible.

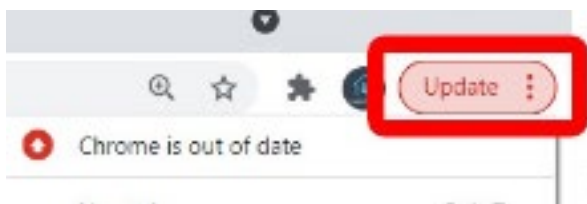
While it is important to install updates, **you want to make sure you look carefully at any prompts that you get to update your software**, just to make sure that they look legitimate – hackers often disguise their malware to look like legitimate updates. A prompt is typically going to be a message that pops up on your computer screen when you launch an application, but they can also appear when you access websites or try to open certain types of files. Look for anything unusual or suspicious that might indicate something out of the ordinary, such as a misspelled product name, typos, or anything else that makes you feel that it might not be coming from a legitimate source. Trust your intuition – if something doesn't feel right, then stop and take a moment to look carefully at what you're being prompted to do.

## Unsupported Software

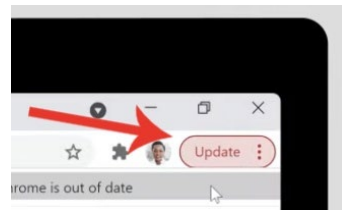
Software that has officially reached “end of life”, such as Windows 7 or older versions of Adobe Acrobat, are considered to be unsupported. If the vendor no longer supports it, then you really should stay clear of it. Retired/unsupported software is no longer considered to be secure, so please make sure that you are running a current version of whatever software packages you happen to be using at your business.

Most software companies release regular updates that include security patches, and web browsers (Google Chrome, Microsoft Edge, Mozilla Firefox) in particular are prime targets for hackers to attack through infected websites and malicious downloads. So, when you get prompted to install those updates, please accept them. (Assuming they look legitimate)

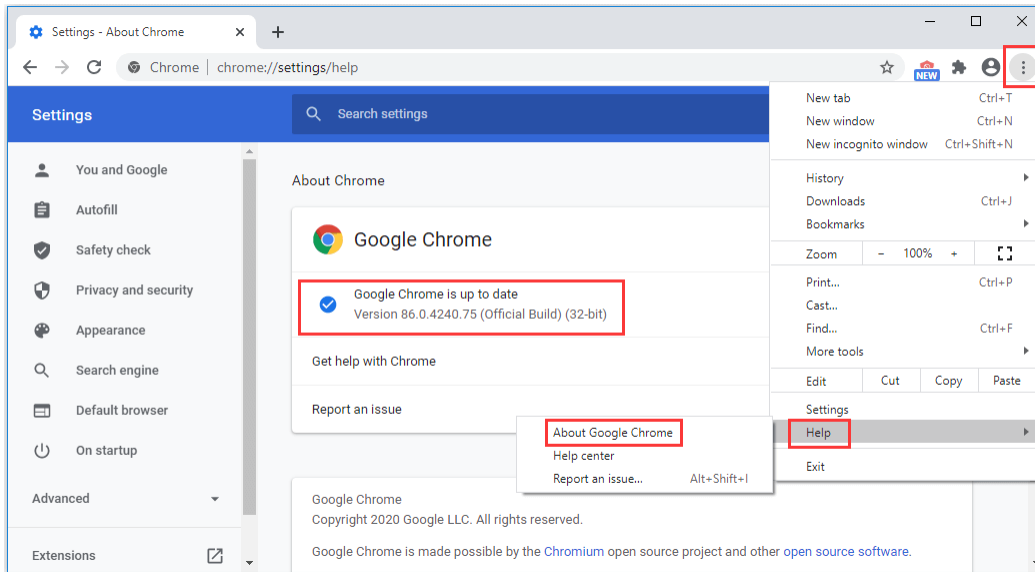
However, it is also important to know that hackers will often release infected software through fake updates, so try to be cautious about where you get your patches from. Google Chrome, for instance, will always release updates with a notification in the upper-right corner of Chrome, up where your user account name and the settings options are located.



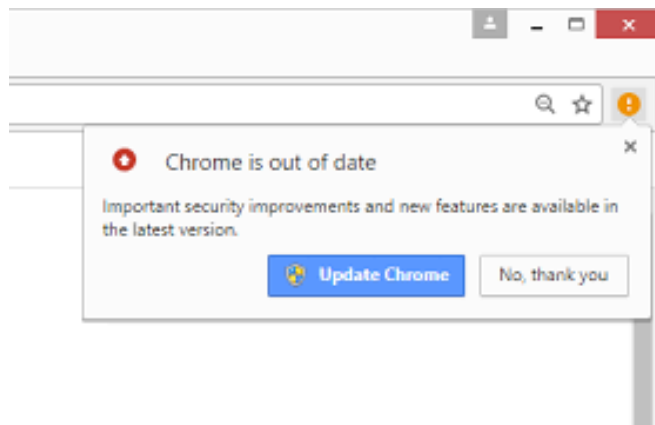
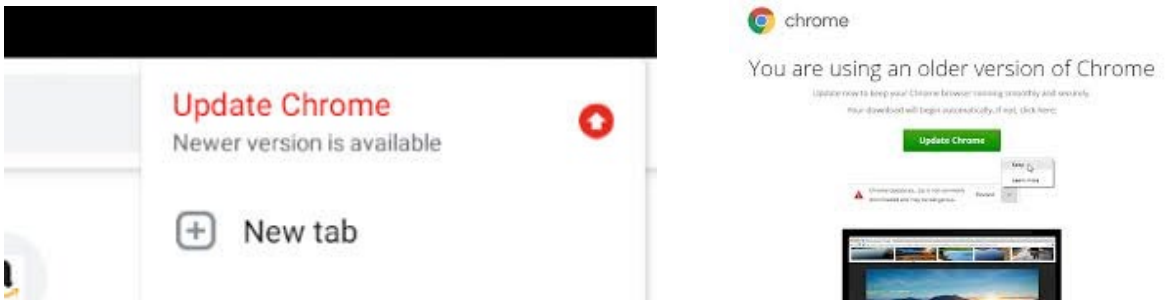
or



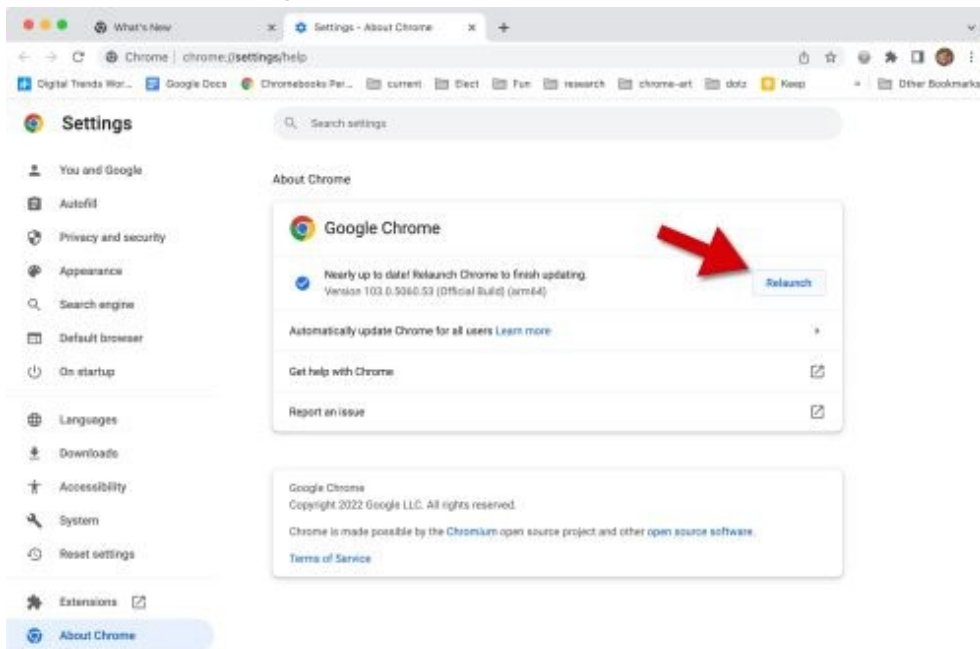
If you go into your Google Chrome Settings (the 3 dots) and choose Help→About Google Chrome, it will tell you if it is up to date, or if there is an update waiting for it:



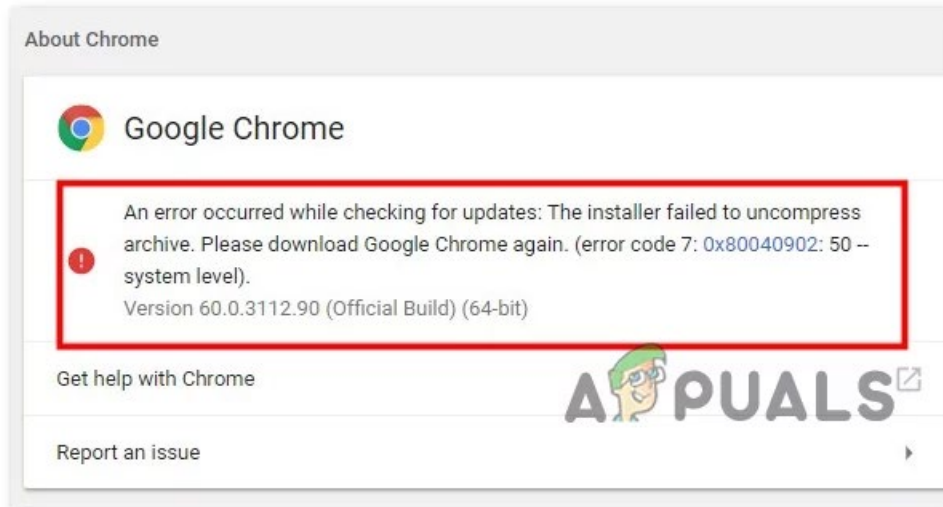
or



...and don't forget to relaunch Chrome when it has finished updating:



If for some reason you cannot install a Chrome update, don't just ignore it. Uninstalling and reinstalling Chrome will usually fix that kind of problem:



If you are a Microsoft Edge user, then here are instructions for keeping it up to date: <https://support.microsoft.com/en-us/topic/microsoft-edge-update-settings-af8aaca2-1b69-4870-94fe-18822dbb7ef1>

Here you'll find the steps to keep Mozilla Firefox updated: <https://support.mozilla.org/en-US/kb/update-firefox-latest-release>



All set? Great – let's move onto the next security tip.



## 2. Run Good Endpoint Protection Software

Make sure you have good antivirus software at a bare minimum, but even more importantly nowadays, we advise you to be running **endpoint detection and response software (EDR)**, which is a more robust form of protection.

Traditional antivirus solutions look for viruses based on virus definitions and known infections, and they try to match what is running on your computer against a database of millions of known threats; they can block those when they recognize them. But, newer endpoint protection software solutions such as Sentinel One, that use Artificial Intelligence to determine whether or not something is malicious, are part of a growing number of much more robust next-generation solutions.

What you really want to be using is an EDR (Endpoint Detection and Response) solution. This is more advanced than a traditional antivirus software program, because it looks at what the software on your computer is trying to do, and then decides if it is malicious or not. Many of the older traditional antivirus software programs now have evolved into being full EDR solutions, and that's good news.

It turns out that Microsoft **Windows Defender Antivirus**, which is built into Microsoft Windows 10 and 11, is not considered to be an EDR solution. It has proven itself to be top-rated antivirus solution, but it is limited in its ability to detect and block other types of malware. So, if all you are running is Windows Defender AV on your computer for security, you might want to consider upgrading to **Windows Defender Endpoint**. It is considered to be one of the top-rated EDR solutions on the market, now, and a number of third-party security solutions work in conjunction with Windows Defender, instead of replacing it. The standard version only costs \$3/month as part of a Microsoft subscription, and then Windows will pretty much manage it for you.



### 3. Prevent Identity Theft

Well, that's an obvious statement, but how do you do that?

Do not give out your information anywhere that you do not need to, which includes online forums, telephone calls, text messages, or on social media. **Be careful what you post online.** Keep an eye on your security and activity on your online accounts. Check your credit reports from time to time.

Keep an eye open for any suspicious activity, such as people saying that they're getting e-mails from you that you know you didn't send, or if you're seeing bounce-back e-mails from people that you never sent messages to; that's a good indication that your e-mail account somehow may have been compromised, and identity theft on some level is going on. If someone has infiltrated your account, then they can send messages directly from your e-mail account.

However, hackers can also “spoof” your e-mail address and send messages from their own accounts with your e-mail address as the reply address. Unfortunately, there isn't a whole lot you can do about that. Your IT support provider can set up [DMARC, DKIM, and SPF](#) records for your company that will tell the rest of the world if e-mails that are claiming to come from you are actually coming from a source authorized to send on your behalf.

**Facebook and other social media accounts are also a prime target for hackers and scammers.** They find ways to gain control of your account, usually from compromised credentials they purchase on the Dark Web, and then they use your account to post online content or to run advertising campaigns through your Facebook account that you may not even be aware of.

Our company has one client that had their Facebook advertising account compromised several years ago, but instead of posting unauthorized content, the scammers set up their own credit card payment method and ran unauthorized Facebook ads that the client never knew about. The client stumbled across a bogus account in their Facebook profile one day when they wanted to run the first

advertising campaign of their own. Even though they deleted the bogus admin account and removed the unauthorized credit card from their Facebook account, Facebook still permanently disabled their Facebook advertising account, and they are still trying to get it re-authorized 6 months later.

So, the lesson to be learned here: **keep an eye on all of your online accounts.** Log into them from time to time and just look around to make sure that everything looks okay, and investigate if you see any suspicious activity.

An ounce of prevention is worth a pound of cure!



#### 4. Turn On Personal Firewalls

Windows comes with a built-in firewall, as does Mac OS. Additionally, most antivirus software packages also include a built-in firewall. It is important to keep those enabled and not disable them for the sake of convenience, as they serve an important purpose. They block unauthorized connections from coming into the computer. If a firewall is installed locally on a computer, it is usually referred to as a “personal firewall”, which is different from a physical firewall device that protects an entire business network from unauthorized connections coming in from the Internet. (We’ll talk more about physical firewalls later.)

Understanding firewall security benefits is the first step in facilitating safe business growth in the constantly evolving digital era. Regardless of whether your business depends on technology and networks for only a small portion of its activities, or for most of its operations, it is crucial to proactively safeguard your assets. Firewalls are usually considered the first line of defense against malicious access to network devices.

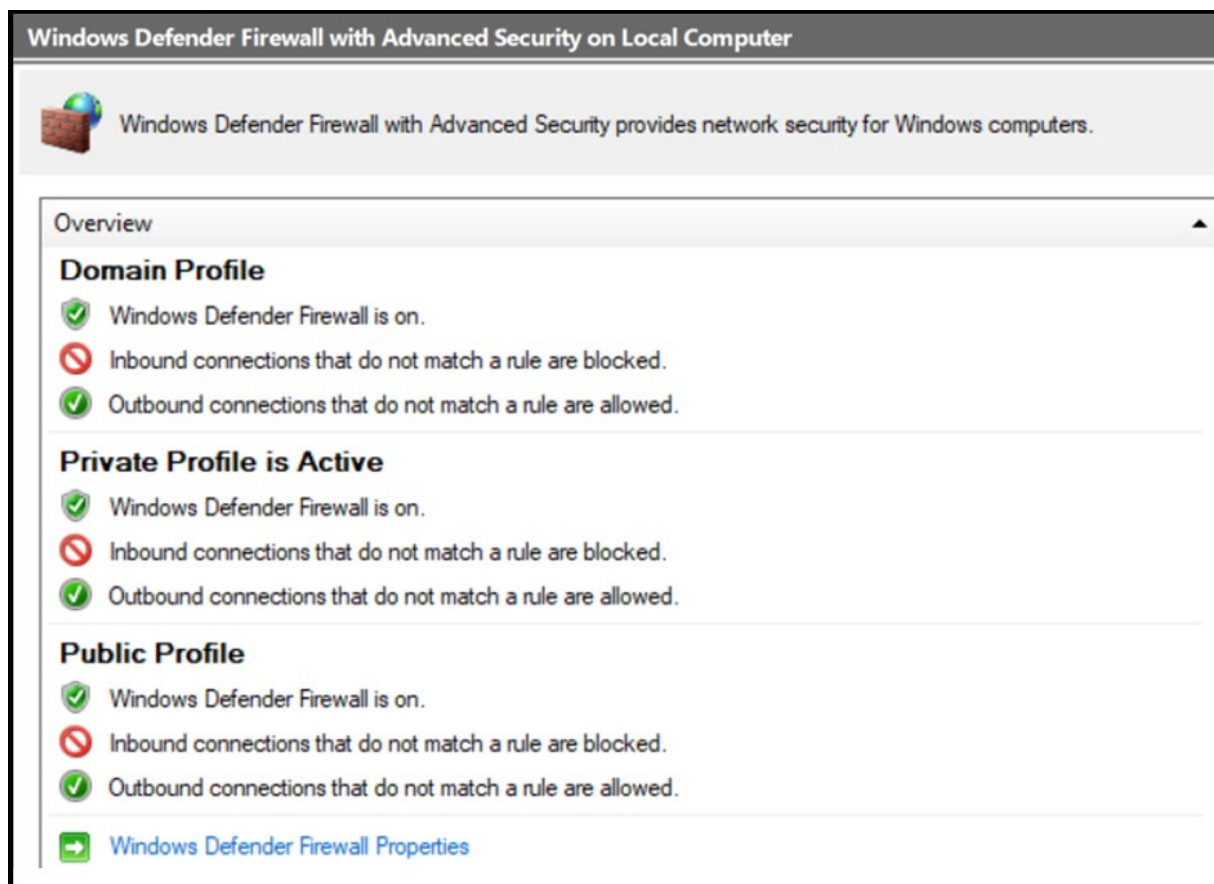
Firewalls offer security against external cyber threats by safeguarding your computer and network from harmful or unwanted network traffic. On a local computer, they block traffic from other systems on the same network. An Advanced Threat Protection (ATP) firewall can also stop malicious software coming from the Internet from infiltrating a computer or network. Firewalls are customizable to restrict

data from specific locations, applications, or ports, while permitting approved data and authorized connections to pass through. Ports are like channels that specific types of data and services use to communicate across networks and across the Internet; there is a total of 65,535 distinct ports that are available for use.

For example, a standard website communicates on HTTP port 80, but few websites use that unsecure port. Most websites now use port 443, which is for HTTPS traffic; the “S” stands for “Secure”. Those websites are protected by an SSL (Secure Socket Layer) certificate, and offer a much higher level of security than standard HTTP traffic.

Anyway, the point here is that a personal firewall monitors all traffic across all ports, and it only allows the traffic through that has been approved by the firewall (which can be configured and customized).

Here’s an example of what a standard Microsoft Windows Firewall configuration looks like:





## 5. Avoid Spyware/Adware

Recommendation number five is quite interesting, because we all want to avoid spyware and adware, so that seems like a no-brainer. Spyware and adware are malicious software programs that can compromise your privacy, security, and overall computer performance. So how do you avoid them?

The simplest way to achieve that is to avoid downloading free or unnecessary software onto your computer. Be especially cautious about downloading software from a website that urges you to do so when you weren't expecting to install anything.

For example, if you click on a link in Google News to read an article about Taylor Swift, there is no good reason why you should be prompted to install an application just to read it, so just hit the "back" button and go somewhere else to read the story. This is a clear indication that someone might be attempting to trick you into installing something harmful on your computer. Therefore, **do not simply install software because you are prompted to.**

Take the time to research and understand what you are installing. Look up the software's credibility, security threats, and any linked spyware or adware. Exercise caution when accessing any Internet link, particularly those in e-mails or messages from unfamiliar sources; malicious links are commonly used by cybercriminals to spread spyware. Install a trustworthy endpoint protection and anti-malware program. Schedule regular scans to maintain system security. Keep your operating system and software up to date. Enable automatic updates for ongoing protection.

Those are ways to help protect yourself from malicious software if you accidentally hit "OK" when prompted to install something, but **stopping to think before you click** is really the best way to do that.



## 6. Protect Your Passwords

Ensure the security of your passwords by refraining from using the same ones across multiple websites and platforms. Create passwords that consists of a combination of letters, numbers, and symbols, and is at least twelve characters long, to reduce the risk of compromise. Better yet, create a passphrase.

A passphrase is a combination of random words that you put together to create a simple phrase, like **HairyBacksArePopularTheseDays!** or **HoolaHoopsCanBeFun#**.

Select a password or passphrase that is new to you but easy to remember. Refrain from sharing your password with anyone, and avoid writing it down in an easily accessible location (like a Post-It note under your keyboard). Avoid using personal information such as birthdays, pet names, song lyrics, or famous phrases in your password. Regularly update your passwords for all your accounts and devices. Consider using a password manager to securely store all your login details in a single digital vault, such as BitWarden or 1Password. Then, you only need to remember one password to access all of your other ones.

I will confess that over the years, I have sometimes used the same “burner” password when I felt that it really didn’t matter if a hacker got into the account in question. So, I just used a simple, easy to remember password across multiple “no-risk” websites, such as signing up for blog posts or to be able to access a website with recipes. However, in recent years I have even stopped doing that, because you never can be sure which organizations out there might be affiliated with each other or share login permissions, so I have stopped doing that altogether.

I have also historically used an old “burner” e-mail address whenever I have had to provide an e-mail address in order to log into something that is not work related, so that even if that organization were to get hacked, my work e-mail address would not be part of the data that gets stolen. When hackers get your e-mail address, you then get added to their growing list of targets for their phishing e-mail campaigns. Recently, there was a HUGE dump onto the Dark Web of a database containing nearly 10 BILLION (with a “B”) passwords that was compiled from data that had

been leaked in previous data breaches over the years. You can read more about that here: [Nearly 10 Billion Passwords Leaked in Biggest Compilation of All Time \(techrepublic.com\)](https://techrepublic.com)

Later in this book, we will discuss Dark Web platforms where hackers can sell and exchange compromised passwords and login details. If a hacker gains access to your YouTube password, it may seem harmless at first, since YouTube accounts typically do not contain sensitive information. However, if you use the same YouTube password for multiple accounts such as Amazon and your banking website, the hacker can potentially access all of them. So, please be careful to protect your passwords and refrain from reusing them across multiple websites.



## 7. Back Up Important Files

The fallback in our industry is that if something happens to a client's data and it gets compromised or it gets corrupted, then the safety net is that you should always have a good backup to recover from. All of our clients have that, and in most cases, they have multiple types of backup in place, just to be safe.

So, not only is it important to make sure you've got your data files backed up, but you also want to make sure that you **test those backups** occasionally, meaning you want to go and look at your backup files, confirm where they're being stored, and perform a test restore to make sure that one of the recent files that you backed up can be successfully restored from backup. If you can't restore one file from backup, then you probably can't restore any of those files.

***Do not just take it for granted that your backups are good – seeing is believing.***

If you're only going to be backing up your data to an external USB drive (including thumb drives), then **make please sure that you keep at least one copy offsite at all times**. We recommend having at least two backup drives that get rotated out with each other, with one copy always being stored somewhere other than where the computer is kept. That way, if the building burns down (heaven forbid) or

someone breaks in and steals your computer along with your backup drive, you still have a good recent backup of your important data that you can restore from.

If you're a business owner and you're paying somebody else to back up your data, I suggest that every month you find a data file that you store in your main network data locations (or local drive), a file that's not critical, for example a PDF file that you that you don't really need (or even a copy of this PDF), delete that file, and then request from your IT support provider that they restore that file from backup back to its original location.

That is the only way you will know for certain that your files are getting backed up and that those backups are working properly - especially for programs like QuickBooks, which are particularly important. If for any reason they cannot restore that file, then you have a serious problem on your hands.

Do your own legwork, do your own homework, and make sure that your data files are successfully being backed up regularly, and that you keep one recent backup copy offsite.

## **Additional Security Recommendations**

### **Two-factor or Multi-factor Authentication:**

Use multifactor authentication (MFA) anywhere online that it is offered to you.

For years, most banks have required a secondary form of authentication where they text you (in most cases) a security code that you need as part of a 2-step login process, or they might want to e-mail you a security code instead of texting it. If you log into your banking website and you are able to log in without any extra form of authentication besides a username and a password, then you need to figure out how to get multifactor authentication turned on, even if it means contacting the bank and asking them about it.

A big risk for people using their home computers or business computers to access online banking is that most web browsers will ask you if you want to save your password, so that the next time you go there, you do not need to



enter it. The problem is that if somebody gets into your computer, they also now have to all your passwords and credentials for all your websites.

Having MFA enabled will help to deter most kinds of unauthorized access whether you receive your MFA code via text, by e-mail, or by using an authentication application like Google Authenticator, Microsoft Authenticator, or Duo Mobile. Several password managers, like BitWarden, now also allow you to use them to provide MFA codes. Of these MFA methods, e-mail is considered the least secure, followed by SMS text messages. Authenticator apps are generally considered to be the safest method to use.

When traveling to another country, you may find that you will be unable to receive text messages, due to your particular cellphone plan. In most cases, you can get around this issue by temporarily switching your method of MFA/2FA authentication to deliver your security code via e-mail. This is not a good long-term arrangement, because hackers can gain access to your e-mail much more easily than your text messages, but for a short-term solution, it is probably not a major risk for you to do that.

### **Leaving your laptop unsupervised:**

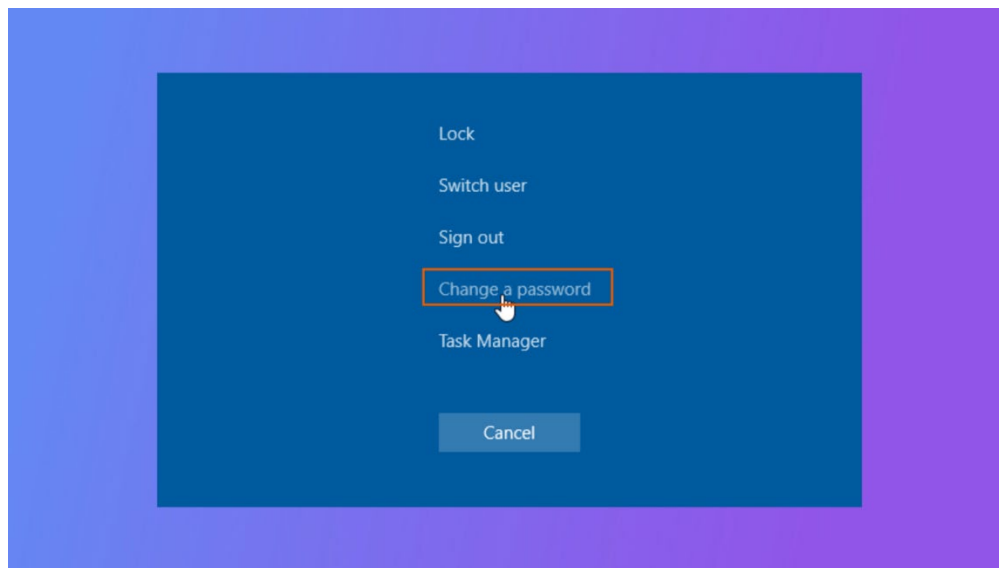
Avoid leaving your laptop unsupervised and in plain view, especially when you are at a public place. Avoid walking away from your computer with the screen unlocked; this leaves your laptop vulnerable to theft, or someone gaining unauthorized access to the system. If you cannot avoid leaving your laptop unattended, at least lock your computer screen. This can be done by pressing the Windows key and L key at the same time to lock it ( [WIN] + [L] = Lock ). When you are ready to log back in, press [CTRL] + [ALT] + [DEL] and then enter your password.

### **User account and password:**

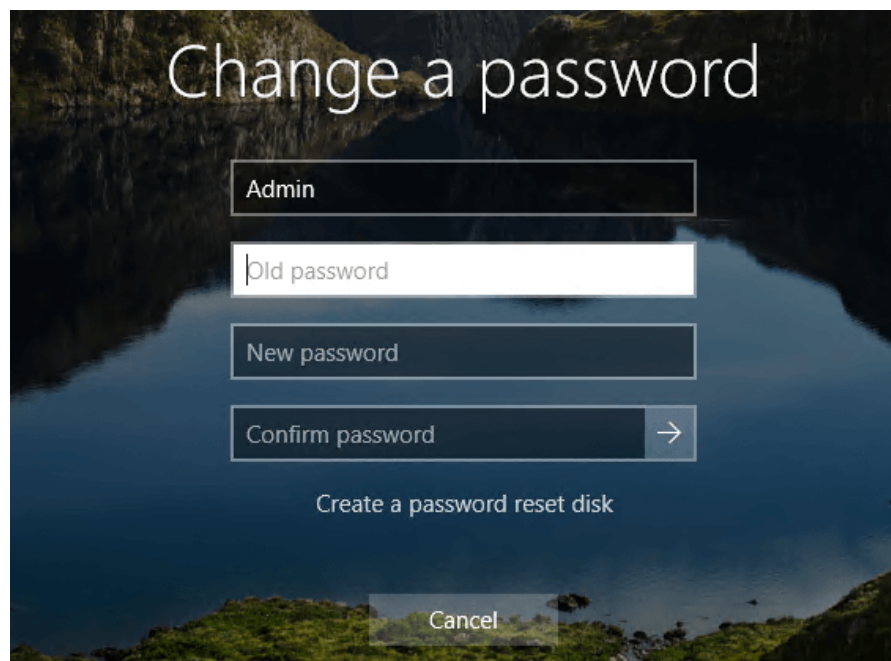
Okay, so we've talked about using secure passwords on the Internet, but if you don't protect your computer itself by using a password-protected account, anyone can just turn it on and then they're into your computer. If that is currently the case – that when you turn on your Windows computer, it boots

up straight into the desktop with no login required – then you pretty much have no security at all if it gets lost or stolen.

It is really easy to add a password to your Windows computer account: Simply press [CTRL] + [ALT] + [DEL] and choose “Change a Password”, and then create a secure password using the method that we discussed earlier:



You will be prompted for your old password, but if you don't have one, then just leave that blank and enter what you want your new password to be:



That's it! Now you can securely lock your computer, and when it gets rebooted or turned on, it will prompt you for that password.

Problem solved!

### **Installing unnecessary programs:**

Try not to install unnecessary programs on your computer, especially the free ones. The most common way that hackers get malicious software onto your computer is to offer free games or free software online that you download and install. When you download the program, their malicious software comes along with it. Make sure you are installing software that is coming from a trusted website and publisher, and be sure to get the latest version. If it gives you options when you install it, do not take the default installation; click on the advanced option, and look at all the different components that are getting installed. Uncheck any of them that you don't want or need.

A common example of unwanted software would be McAfee programs. McAfee likes to put their free software bundled in with other software packages that gets installed on your computer. When that happens, it can leave you with multiple versions of security software that not only can conflict with each other, but they can also cause performance issues.

***Bonus Tip:*** Software that installs itself without asking you or without you knowing is also known as a ***"PUP"***, which stands for ***Potentially Unwanted Program***.

### **Encrypt your local hard drive:**

There is hard drive encryption available on most modern computers. In Windows, it is BitLocker by default. Mac's version is File Vault. If you encrypt your hard drive, and then somebody else gains access to that device, without the password to unlock it, they cannot get into your data files - even if they pull out the hard drive out and stick it in another computer.

Most IT people know that connecting a hard drive to another computer is often the easiest way to recover data files from a crashed computer. You remove the hard drive from the original computer, insert it into a different computer, boot it up, and then gain access to the files. If the hard drive is encrypted, however, then whoever has access to that computer will not be able to gain access to the files without the encryption code. This security feature is particularly important for businesses, because if somebody breaks into your place of business and they walk away with your server, they will not be able to log onto it, and all your data will be safely protected if the hard drive(s) is encrypted.

***Important: When you encrypt a hard drive, you will either be given a long encryption key or you will be asked to create – WRITE IT DOWN OR PRINT IT! If you lose it, and your computer crashes, your data may not be recoverable without that encryption key.***

Keeping your confidential data on an encrypted hard drive is called “Safe Harbor” from a legal and compliance perspective, so that if a security incident happens and your server is stolen, you will not be fined or penalized by the government for not protecting your data. This is called **Safe Harbor encryption**.

### **Annual computer tune ups:**

Unwanted software will always somehow manage to infiltrate your computer system; that’s just the way things work. When cleaning and optimizing your computer, consult with a coworker or professional computer support engineer. Regular cleanups, ideally annually, will enhance performance and bolster your security posture.

## **Additional Cybersecurity Considerations**

There are many traditional cyber threats, and I think that we have covered most of them fairly well. Keep in mind that even though Artificial Intelligence has recently become known as a potential cause for cybersecurity concerns, many threats that

are still actively used today already existed 10 or more years ago; they just weren't as sophisticated as they are now. The old tricks still work, to some degree, and as long as they do, the hackers will continue using them, so we will continue talking about them whenever we discuss cybersecurity with our clients.

Malware (any kind of malicious software), denial of service attacks (a focused attack on a website), and phishing attacks (see next section) have been around since the beginning of e-mail. There are so many kinds of traditional cyber threats. We are covering them here, but you might be served well by watching one of the previous cybersecurity presentations on our [PJ Networks YouTube channel](#). Later in this book, I'm going to be focusing specifically on how Artificial Intelligence is taking some of these more traditional cyber threats, putting them on steroids, and then pushing them back out to the general public.

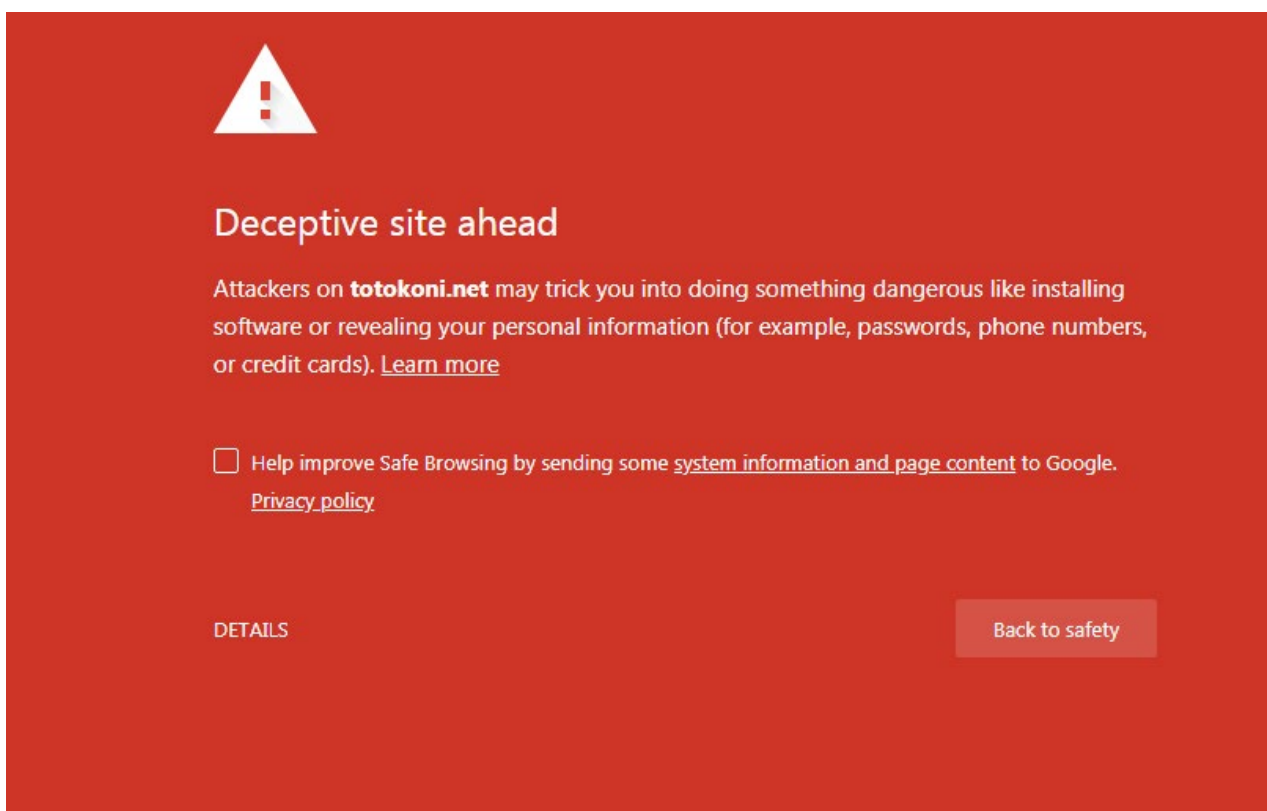
## Phishing Scams

Recently, a phishing scam was sent to one of our clients and forwarded to us for review. It was disguised as an e-mail from “MSN-Docs”, but the sender was **Natalie@ypas.org.uk** in the United Kingdom (presumably); I quickly recognized it as a phishing e-mail due to the sender's e-mail address. As I have always recommended, I hovered over the link in the e-mail and saw that it was pointing to a suspicious website.

It was not a site I wanted to visit.

However, since I have multiple layers of security on my computer, and therefore feel fairly confident about my protection from malicious content, I clicked on the link (please don't do that) to see what website that link was pointing to.

This is what I then saw:



That site was blocked because phishing and malware detection are turned on by default in Google Chrome. (We strongly recommend against turning that feature off.)

To be clear, we would never recommend to a client that they click on any link in a suspicious e-mail; we always tell them to forward the message to us if they are unsure whether it is legitimate or not.

However, my computer was not connected to our network at work, and I felt confident that the protections that I have in place would prevent anything ugly from happening. Besides, I was curious about what would happen. Had I been wrong, and a ransomware attack or other nasty virus had been unleashed on my computer, then I guess I would have had to restore it from the previous night's backup.

Luckily, that didn't happen.

Take a look at that warning message for a moment. If this e-mail message really had been sent from Microsoft, you would expect to see the website address end in Microsoft.com – not **totokoni.net**.

When I clicked on the link, even though I have multiple layers of protection on my computer, Google Chrome blocked it and popped up the warning message above, before any of my other security protections could spring into action.

Google Chrome was doing its job.

If it had failed, I would have expected either that my Sophos firewall would have stopped it dead in its tracks, or my endpoint protection would have stopped it. However, Google Chrome caught it before I could even get to the malicious content. For the record, both Microsoft Edge and Mozilla Firefox also both have their own built-in protections that are enabled by default. We recommend leaving those **turned on at all times**, even if they try to block you from going to a website that you think you want to visit.

So, please leave your default security settings turned on in all of your web browsers, if you want to at least have what we consider to be a bare minimum level of protection.

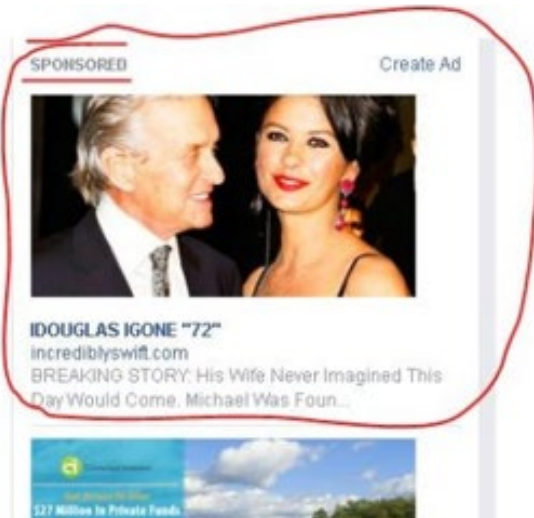
**GIFT CARDS: By the way, if you ever get an e-mail requesting that you purchase gift cards for any reason, it is almost definitely some kind of a scam, so proceed with extreme caution.**

## **Fake News**

The more traditional fake news headlines are still very commonly used, and we see them on a regular basis. Usually, they are embedded in a **sponsored ad**, whether it is on Facebook, or when you are searching for the latest online news.

You will see some little headline that shows the picture of somebody famous, like Michael Douglas, and it will say he has passed away. Arnold Schwarzenegger has passed. Ronald Reagan is back from the grave. Ryan Reynolds married Lady Gaga.

These are sensationalized headlines that make you immediately want to click on the link to see what's going on.



The image above was from a fake “news article”. All I needed to do was open a separate Google search window and type “Michael Douglas dead”. Immediately, I got back several results confirming that he was still alive and well.

If Michael Douglas had really passed away, there would have been headlines everywhere. So, try to avoid clicking on news articles that are coming from sponsored links, because **sponsored links are not to be trusted**; those are paid advertisement spots. Anybody can purchase an ad to put a sponsored link out there claiming anything they want to claim. The hosts of those websites are supposed to verify their content, but that doesn’t always happen.

So, be careful clicking on anything that says it is a sponsored link (unless you’re shopping for that item), because it may lead you to a malicious website or prompt you to download some kind of malware.

## Fake Pop-up Alerts

Every month or so, sometimes more often than that, somebody will bring in their computer to our repair shop that has been infected because they saw a warning pop-up message with a 1-800 number and they called it. They called the number, and the person on the other end told them their computer was infected. **Do not call any toll-free numbers that pop up on your screen - ever.**



Here is how that type of scam usually works: The hacker tells the victim that their computer is infected, and they can clean up for free or for a small fee. However, they need to connect into to the computer in order to do that. The victim is instructed to navigate to a specific website for the hacker to gain remote access. The person then lets the outsider in, and that hacker now has access to everything on that local hard drive while they are connected into it. To add insult to injury, at the end of these sessions, the hacker will often say, “Okay, I have cleaned up your computer, and now we need a credit card number to pay us for doing that work”.

What they have actually done is pulled all of the passwords and login credentials that were saved to the local hard drive, like in Google Chrome or Microsoft Edge, and then they immediately go out from their own systems and start accessing the victim's online accounts, usually starting with their bank account – sometimes while still on the phone with the victim. We have seen people's entire life savings wiped out just because they let somebody into their computer, all because of a fake pop-up warning.



The general rule of thumb with these kinds of pop-ups is to simply turn your computer off and turn it back on in a few minutes, or you can simply close your browser and clear your cache, if you're able. Do be sure to clear your web cache, just to be safe. If you don't know how, you can Google "how to clear my browser cache" and you'll find plenty of easy-to-follow articles on how to do that.

To reiterate, **do not let anyone connect into your computer for any reason if you do not know them personally.** You need to have some way to positively confirm their identity, first, and a legitimate reason to let them connect into it.

If somebody states that they are calling from your bank and says, "We need to look at something on your computer, because the last time you logged into your bank account, we detected there was something wrong with your computer," **end the call immediately.** Then, call your bank's confirmed support phone number and ask to speak to customer support to find out if they did, in fact did, call you. Chances are you were being scammed.

**Google searches are not guaranteed to give you the results you want.** I have many times in the last few years seen situations where people have had a problem with their computer or with their printer and they will Google "HP printer support" or "Microsoft support". Some of the first links and phone numbers they will see are actually from hackers who are paying for sponsored advertisements in order to get their listings elevated to the top of the search results, so that people will call them before they see the actual support number that they need.

If you need to call HP tech support, go to "HP.com" and get their tech support number there. Do not call numbers that pop up in any kind of a web search for tech support, unless you go to the actual website from the real vendor and make sure that it is legitimate.

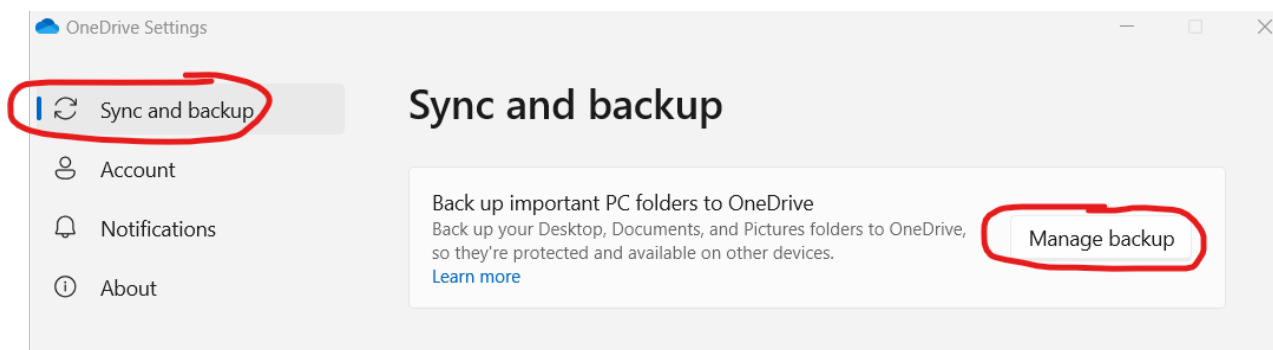
The final big reminder from this section is to **back up your important files**, because if you have those backed up, then you can recover from almost any data loss scenario. QuickBooks data is the most common thing that we see people panicking about when they have lost their files, or when they have become corrupted. Normally, you would just go back to the previous backup copy, but if you do not have that, you're stuck. (and possibly out of luck)

*Please* back up your important files and keep them in a safe location. If it is a home computer, then either back them up to a thumb drive and then pull that thumb drive out and keep it somewhere safe, or keep a backup copy online in your OneDrive or Google Drive account.

**BE AWARE:** Database files like Quickbooks cannot be synchronized to cloud folders like OneDrive or Google Drive when they are in use. Instead, back up your databases to a local folder (like OneDrive) that gets backed up or synchronized to the cloud – those backup files can be safely synchronized online like any other file.

If you own or run a business, **we strongly recommend that you back up your company data files to the Cloud** and allow somebody else to manage them for you - they are that important.

Make sure that you have backups, and then test them on a regular basis to make sure that the backups work. If you have a OneDrive account, which comes along with most Microsoft 365 subscriptions, all you need to do is to click on the little cloud icon in your system tray, or pick OneDrive from the Start Menu, then click on Settings→Sync and Backup→ Manage Backup.



You will then get a list of different items stored on your local hard drive that you can choose to back up. Choose all of the folders that you want to back up, which in most cases will include your Documents and Desktop folders. You probably also want to include Pictures and Downloads, as well. Click on “Save Changes”.

Automatically, your files will start backing up to Microsoft OneDrive, and they will synchronize every time you make any changes. You can get more storage if you need more; it only costs a few dollars per month.

It's that easy! OneDrive is likely already installed on your computer, so please take advantage of that readily available backup option.

There is also a **full image Windows Backup** program available in both Windows 10 and Windows 11, which allows you to back up your *entire computer*, including

programs, operating system, data files, and settings. You will find instructions on how to set that up here: [How to backup Windows 11 to external USB drive - Pureinfotech](#)

That's the type of backup you want to have if your entire computer crashes and it needs to be restored from scratch.

## **Public Wi-Fi and Social Media Use**

So, why is public Wi-Fi generally not considered safe?

If you walk into Panera Bread and you decide that you are going to use their free public Wi-Fi, another customer there could be a hacker who has brought their own hotspot with them and titled it "Panera Guest." If you select this option instead of clicking on the legitimate Panera Bread hotspot, you will then be connected to the hacker's router, and then everything you do online is now visible, trackable and recordable by the hacker - and you don't even know that you clicked on the wrong one.

Even if you did click on the right wireless network, hackers can attach to the same one that you are connecting to. Depending on how that public hotspot is configured, they may still be able to see all of your activities, because in most cases, your connection is unencrypted, unless you're using your own VPN solution.

What are the rules of thumb for using public Wi-Fi?

- Do not do anything of value when using free public WiFi. (Banking, shopping, business e-mail, etc.)
- Do not go to McDonalds or the local mall to connect to their free Wi-Fi and then do your banking online. That would be very unwise.
- Make sure you have good endpoint protection - that you have a robust EDR solution installed.
- Make sure that your personal firewall is turned on.
- Make sure you're following all of the standard best practices that you would follow for any other Internet activity, and also try to use some kind of personal

VPN. There are plenty of them - ExpressVPN, NordVPN, PrivateVPN, Private Internet Access. There are all kinds of VPN solutions available; just try to choose a reputable one. VPNs create a secure encrypted connection between your computer and the Internet that is much more difficult to hack into than just using an open public WiFi hotspot. Research and find the ones that have the best reviews and the best ratings - those will usually be a good choice.

## What is even easier than that?

Use your cellphone as a wireless hotspot.

If you use your cellphone as a hotspot and ensure that you have a secure password to connect to it, that will be a fairly safe way to get onto the Internet everywhere you go, without having to use a public hotspot.

I do that often when I go to restaurants, conferences, etc. If I need to do something quick online and I need it to be secure, I just turn on the hotspot on my cell phone, connect to it with a (very) secure password, and away I go. Even then, though, I am cautious about what I do online. In many cases, people have unlimited Internet usage on their cellphone accounts, but you should verify that if you're unsure. However, I wouldn't recommend using your cellphone hotspot all the time for Internet access, even if you have an unlimited data plan; the main purpose is to provide you an alternative to public WiFi hotspots if you need to do something quick online that you want to keep secure, like purchasing something.

So, that is a super easy, more secure way to conduct your online activity without using a public hotspot, because it is going to be much harder for a hacker to get into your cell phone hotspot. **However, using a cellular hotspot is not 100% hacker proof.** Hackers now have the ability to "clone" the SIM chip in your cellphone, thereby allowing them access to your connection, but you would need to be a targeted victim, and it would require much more work on the hacker's part.

Also, if you have ever shared your WiFi hotspot password with anyone, then always remember to change it, afterward.

This article provides some valuable tips for making your cellular hotspot as secure as possible: [https://www.astrill.com/blog/are-mobile-hotspots-secure/#Risks\\_of\\_Using\\_a\\_Mobile\\_Hotspot](https://www.astrill.com/blog/are-mobile-hotspots-secure/#Risks_of_Using_a_Mobile_Hotspot)

## **Keep an Eye on Your Social Media Accounts**

We discussed this briefly earlier, but it is worth a quick recap.

It is crucial to have unique and complex passwords for your social media accounts in order to help prevent unauthorized access to your personal information – use the guidelines that we provided earlier; passphrases are the best way to go.

Remember that there are other applications on your phone that may have access to your social media data, as well. Don't automatically grant every application you install full access to all of your accounts – they will often prompt you to grant them those permissions. Be cautious about what you share online, and regularly review and update your social media details.

In 2018, Facebook experienced a security breach that exposed the information of [50 million user accounts](#). This breach occurred due to the exploitation of “access tokens”, which are a type of security key that allows users to stay logged into Facebook over multiple browsing sessions without entering their password every time. Unfortunately, this loophole was used to compromise the accounts of Facebook accounts worldwide. Personally, I only realized the impact of this breach years later when my own account was compromised.

It serves as a reminder for everyone to stay vigilant and monitor their online presence closely.

## **Security recommendations for Mac users**

Throughout my 30-year career, I have worked in over a thousand business network environments. While Macs are great for doing creative work such as websites, audio, video, and graphics, they are not typically used as the primary business computers in a business; I know that from personal observation.

This is primarily because standard business applications like QuickBooks and the Microsoft Office suite work differently on Macs than on Windows computers, and file transfers between Macs and Windows computers can sometimes be problematic; files don't always look or behave the same between the two platforms. Word documents can appear to be formatted differently, and Excel macros don't always work as expected.

Macs used to be considered "the safe alternative" to Windows, but security has now become a real concern for Mac users, too, and we have seen an increase in infected or compromised Macs coming into our repair shop in the past few years. In the more distant past, meaning 10 or more years ago, only about 3% of Macs were affected by viruses, but now the number has skyrocketed to between 15% and 18%. Hackers noticed that Mac users tend to feel more confident and secure than Windows users, making them easier targets because they tend to employ fewer protections in general, due to a false sense of security.

More here on Mac security: [Apple quietly drops its claims that its computers don't get viruses | WIRED](#)

For Mac users, it is now recommended to use third-party antivirus software in addition to the built-in protection in MacOS. Ransomware infections targeting Apple computers are on the rise, so it is important to take more precautions than in years gone by. Many security guidelines for Windows users also now apply to Mac systems. You can find more Mac-oriented security tips online these days than in the past. Additionally, our shop loves working on older Apple systems that Apple stores may no longer service, so feel free to bring in your older Macs for repair! ☺

Signs that your Mac (or Windows) computer may be infected:

1. The system is running at a slower pace than normal.
2. The browser has a different homepage or additional extensions that you did not install.
3. An increase in the number of pop-up ads is noticeable.
4. Security alerts are being received without initiating a scan on your Mac.
5. Your contacts are receiving spam from your accounts.

If any of these signs are present, it is an indication that your computer or e-mail account may have been compromised. Unauthorized access to your contacts or being unable to access your personal files, along with ransom demands or warnings, are clear indicators of a security breach.

Finally, I was recently asked by a friend if you can easily lock a Mac computer screen like you can on a Windows computer, and the answer is “Yes”. There are several ways to lock the screen on a Mac computer:

- **Keyboard Shortcut:** Press Control + Command + Q to lock your screen immediately.
- **Apple Menu:** Click on the Apple logo in the top-left corner of your screen and select “Lock Screen.”
- **Hot Corners:** You can set up a hot corner to lock your screen. Go to System Settings > Desktop & Screen Saver > Hot Corners and assign a corner to “Lock Screen.”
- **Touch ID:** If your Mac has Touch ID, you can press the Touch ID button to lock your screen.

My thanks to Copilot for providing me with that handy information.

I think that’s all that I have right now for you regarding Mac computers, but I will be happy to provide more information in future revisions of this book as it becomes available.

## **Impact of Artificial Intelligence on Cyber Threats**

One comment that caught my attention from a fellow MSP (Managed Service Provider) during a recent conference was likening AI-driven cyber attacks to a town of 3,000 residents with 10,000 burglars attempting to break into their homes. AI is powering more and more efforts by cyber criminals to compromise computers and networks, and the situation is getting pretty dire.



AI is empowering hackers to be able to engage in numerous malicious activities simultaneously, and making those attacks more effective than ever before. The rise in cyber threats due to AI is growing rapidly, and it is only expected to get worse as we move forward in time.

## **Deepfakes**

Deepfakes are on the rise, as well. A Deepfake is a synthetic voice or image where a person's likeness (voice or face) is replaced with someone else's using Artificial Intelligence technology. This technique can create highly realistic fake videos, images, or audio, often making it appear as though someone is saying or doing something that they never actually did.

Here is a great example: <https://www.youtube.com/watch?v=oxXpB9pSETo>

That video was created more than three years ago, and the ability for AI to create Deepfakes like that has just continued to improve since then.

### **Watch out for scammers using Deepfakes to trick you into giving away sensitive information.**

I believe that it is only a matter of time before we find ourselves bombarded by telemarketing callers who sound like real people, but they are just Deepfakes. Even worse, using a voice sample or image of someone you know, hackers will be able to simulate a friend or loved one calling you in distress and asking you for financial assistance.

Imagine your nephew or cousin or child calling you from a jail in Mexico, telling you that they need you to wire them \$1,000 immediately in order to get them released. Or imagine a video call from a parent telling you that they need urgently \$500 transferred using Venmo in order to get them out of a serious problem.

It would look like them, and sound like them – but it is really a Deepfake.

An example of Deepfakes that you can create on your own can be found on a website called Synthesia. (<https://synthesia.com>) If you visit that website, you will find a number of examples of virtual “avatars” that you can create for your own uses. Presumably, you would only use them for training materials or educational purposes, but nobody is stopping cyber criminals from using that same kind of technology to scam people out of their money.

At our company, we have a secret passphrase that we all know, so that if someone on our team makes a request to change permissions or gain access to a system they haven’t accessed before, they have to know the passphrase, or else we will assume that it is not a legitimate request. Short of that, if you receive that kind of communication from someone you know, but it seems suspicious, try texting or calling them from another line to verify that it really is them.

## **AI Generated Phishing E-mails**

Be prepared to encounter an increasing number of Deepfakes and AI-generated phishing e-mails in the future. Be cautious of the sender and subject line. Congress has recently issued a critical security alert [requiring stricter data protection measures for all government agencies](#). That same caution needs to be followed by businesses, as well as individual computer users.

An example: You receive an e-mail that claims to be from a reputable source - they are requesting your password. The message is sent from a generic IT security account, though, which may not be familiar to you.

What do you do? Ignore, delete it, move on.

I realize that may not be an easy practice to follow, but once you’ve done it a few dozen times, it will become a healthy habit that you can get used to. If the e-mail was somehow genuine (unlikely), then you will either get a follow up e-mail with additional information explaining who is making the request and why they need a response, but 99.99% of the time, you will not hear back from them – or you’ll simply

receive the exact same e-mail later on, which would also be suspicious. You can always call the sender (assuming you know who they are) to try to verify whether the request was sent by them, and why.

This is AI, after all; it never gets tired or bored, it doesn't get paid overtime, and it can be relentless. Get used to the rising number of spam e-mails and texts arriving into your Inbox and on your cellphone, because it is only going to get worse. I have labeled this incoming wave of AI-assisted attacks a **CyberStorm**, and I have started writing a book about it. Time permitting, I will try to have that finished and published by the end of this year.

My experiment with AI: I used Microsoft Copilot to generate an e-mail template that would prompt the recipient to click on a link to change their Microsoft 365 password. If hackers had generated it, the link would take the victim to a fake Microsoft website designed to steal their login credentials. The e-mail template it produced was flawless - no typos, no grammatical errors. It would have appeared completely legitimate, with the only potential giveaway being the sender's e-mail address.

This is the risk of AI - it does not make the same basic mistakes that human hackers make.

## **Traditional Phishing E-mails vs AI-generated Ones**

This is what a traditional "handwritten" phishing e-mail might look like:

## Scenario: Traditional Phishing E-mail

What are the “tells”?

**REMEMBER! BE SUSPICIOUS!**

### Password Review

System Administrator <sysadmin@it-security-group.com>

Sent: Tue 10/13/2015 7:01 AM

To: [REDACTED]

### IMPORTANT SECURITY NOTICE

Due to a recent rise in security breaches in our industry, Congress has mandated higher information security standards. As passwords are the primary mechanism of defense against unauthorized access, we are being required to check the complexity of all employees' passwords and recommend changes if they fall short of the standards.

Please assist us in being compliant and visit <https://passwordtest.it-security-group.com> to test the strength of your passwords. Failure to do so may result in your account being locked out.

Thank you for your co-operation,

IT Security

### Subject and Sender

- Messages regarding passwords
- Generic e-mail addresses / unrecognizable addresses. EVEN if it looks legitimate, hover over it to see the actual address

### Supposed Authority

- Often cites some authority as the reason for the request

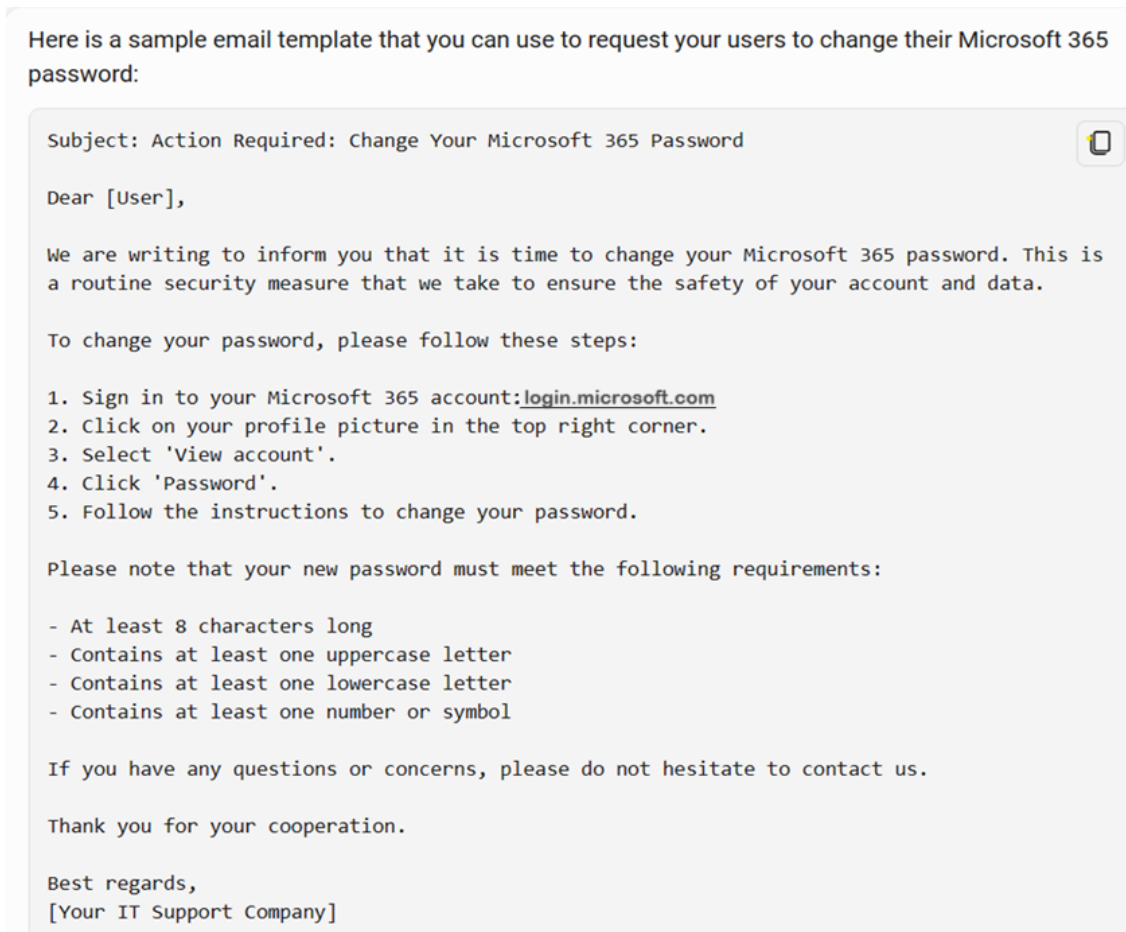
### Asking for your password

- Most legitimate organizations will not ask
- Nothing legitimate will ask for multiple passwords

### Spelling and Grammar

- VERY rare that a legitimate organization lets an e-mail go out with a misspelling

This is an example of an AI-generated phishing e-mail template:



As you can see, there are many “tells” that give away the first example as being a fake phishing e-mail.

The second one was written using Microsoft Copilot from a single prompt, and if distributed widely, it guarantees a yield of thousands, possibly hundreds of thousands of dollars. So, hacking is a thing that can now be bought as a phishing kit, and phishing e-mails are now more convincing than ever with the assistance of Artificial Intelligence.

## Hacking Kits

Hackers now also design and sell “hacking kits” - a complete phishing attack kit that includes everything an amateur (or lazy) hacker needs to run a complete phishing campaign without knowing how to write any code or program AI themselves.

A phishing kit typically contains a counterfeit domain and a counterfeit login page that closely resembles a popular website, like Amazon or Microsoft. Using their own e-mail server (included in the kit), they can distribute harmful e-mails without being detected. Utilizing a bulk mailer software program, they can send out millions of e-mails in a single blast.

By purchasing these phishing kits, a hacker can acquire thousands to millions of potential targets. After importing the e-mail addresses, the kit disperses a huge volume of spam and phishing e-mails in a very short period of time. Even if only a small fraction of recipients falls for the scam, the hackers can profit significantly. If only 1% of 1% of the recipients fall for it (0.01%), the hackers have a bountiful payday.

This type of phishing kit could cost a hacker as little as \$250 to purchase.

## **Business E-mail Compromises (BEC)**

Recently, we have seen a dramatic rise in the number of successful BEC attacks against small businesses.

Our Chief Technology Officer put together this urgent warning that we sent out to all of our managed business clients:

In the last few weeks, we've noticed a significant increase in hacked email accounts, in what the IT industry calls a "Business Email Compromise." In its most common form, the attacker will find a way to hack into your email account, will read and snoop on all your correspondence, and then use your account to impersonate you and scam your coworkers, clients, and business partners.

PJ Networks has been rolling out additional protections to all of our customers, especially "multifactor authentication", which can go a long way in stopping these attacks. However, the criminals do still have ways of bypassing these protections, and we expect the problem to get worse, not better. With that in mind, here are a few tips that we recommend you drill into your employees, that can help with preventing this kind of account hacking.

- If you are emailed a document that you did not directly expect, treat it with extra suspicion  
Attackers try to send documents that look similar to ones you already handle or work with, and want to slip under the radar.
- If someone sends you a document via Dropbox, ShareFile, or another system that they don't normally use, don't try to open it
- If someone sends you a document, and when you open it there's a QR code or link to another website, don't scan the code or follow the link  
Often a document will even have text saying that you need to follow the link to "get permission" to open it, or something like that.
- If you see anything suspicious about something that you get via email, don't reply to the email. Instead, call the sender via phone to ask them about it  
If an attacker is controlling the sender's email, they'll even respond to you and convince you to open the thing they sent.
- If you get a screen that prompts you to "sign in", especially signing into your email or Office 365 account, check to make sure it's a legitimate site  
Microsoft usually uses the website address "login.microsoftonline.com", and anything else is very likely to be a scam.
- If you suspect something is afoot, ask for help

We'd rather review 100 different suspicious emails, than have you get hacked and lose money.

PJ Networks is continuing to explore more ways to keep you and your systems safe, but with the recent rise in cybercrime, staying vigilant is the best defense.

Nathan Kipps  
Chief Technology Officer, *PJ Networks*

The FBI provides an excellent overview of what a BEC is and how they work:  
<https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/business-email-compromise>

## EvilProxy Phishing Bypasses MFA

Cyber criminals are now utilizing a method known as EvilProxy phishing.

An example: You receive a phishing e-mail prompting you to visit your banking website to address an urgent matter with your account. The hackers behind this scheme will often have knowledge of which bank you are affiliated with. Once you click on the link provided, a fake login webpage closely resembling your bank's site will appear.

This webpage is a doppelganger, an exact imitation designed to deceive you into entering your login credentials. Unbeknownst to you, as you input your information, the hackers are intercepting it, and then transmitting it in realtime to the legitimate banking website you intended to access.

As you are entering your username and password, **hackers are already accessing your banking login site**. Soon, a multi-factor authentication code will pop up on your phone or in an e-mail. The fake login screen will ask you for the code, which you will unknowingly provide.

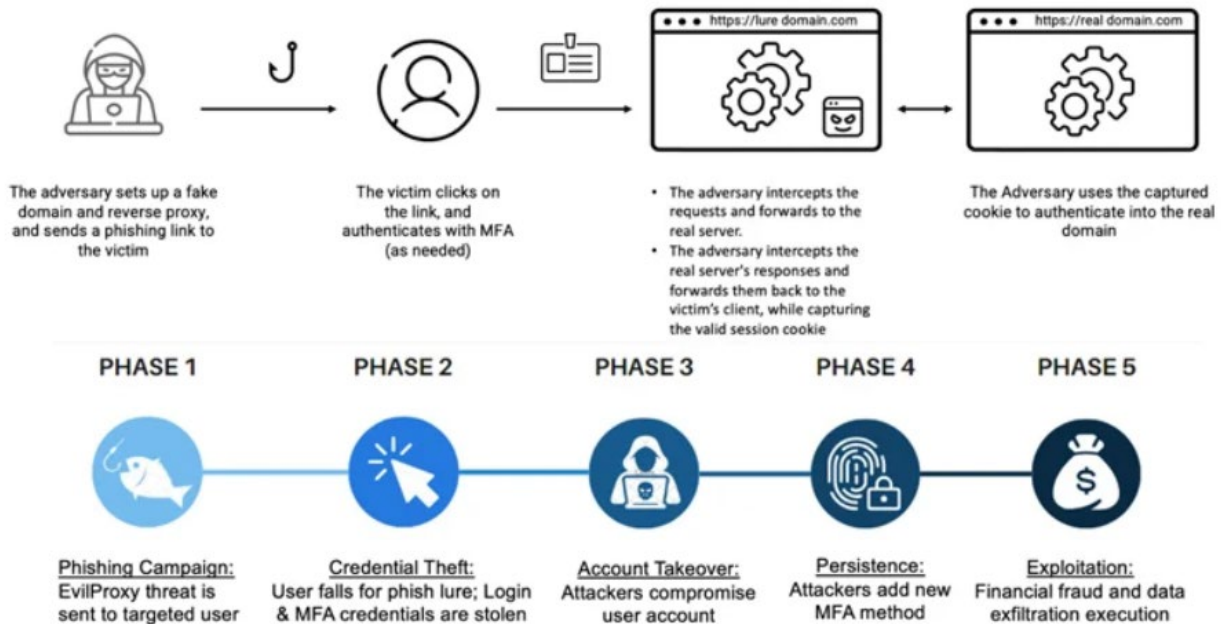
Once you enter the code into the MFA screen, the fake web page will relay it back to the real website, and the hacker will then have access to your account. Before you know it, they will start draining your bank account while showing you a fake screen indicating that everything is fine with your account.

So, that's EvilProxy.

Everything about it looks legitimate, and they have a way to get around MFA by having you provide it to them.



This diagram shows how EvilProxy works:



## Targeted Attacks

Hackers are also using AI to target specific victims based on their personal profile or demographic information. Last year, there was a [hack of 23andMe's genetic database](#), and hackers managed to access their customer data – about 7 million accounts. Shortly thereafter, they were caught attempting to use that data by targeting individuals with Jewish ancestry that they obtained from the 23andMe breach. The hackers targeted them by sending them personalized phishing e-mails to deceive them into thinking the e-mails were legitimate.

## Cybercriminals are Exploiting TeamViewer to Infiltrate Networks.

Many organizations opt for free or low-cost remote access tools like TeamViewer to remotely connect to their computers, which can pose unforeseen security risks. At PJ Networks, we ensure that our clients connect into a VPN with MFA authentication for secure remote access to their business networks. This way, they can access company data files and control their work computers remotely without any additional monthly fees or third-party software. It is all included in the initial cost of the

firewall. Avoid using cost-free or low-cost methods to establish remote access to your company systems, as there is a risk of them being compromised.

## How to Determine if Your Credentials Are On The Dark Web

There is a website called **haveibeenpwned.com** where you can search for your e-mail address and find out if it appears in any reported data breaches:

### Search results from **haveibeenpwned.com**

The screenshot shows the search interface of haveibeenpwned.com. The search bar contains the email address 'philjaderborg@gmail.com' and a 'pwned?' button. Below the search bar, a green banner displays the message 'Good news — no pwnage found!' followed by the text 'No breached accounts and no pastes (subscribe to search sensitive breaches)'.

...and the big one:

The screenshot shows the search interface of haveibeenpwned.com. The search bar contains the email address 'phil@pj-networks.com' and a 'pwned?' button. Below the search bar, a red banner displays the message 'Oh no — pwned!' followed by the text 'Pwned in 15 data breaches and found no pastes (subscribe to search sensitive breaches)'. The number '15' is highlighted with a red box.

The first e-mail account I checked was my Gmail account, which apparently has not experienced any breaches or security issues. Next, look at my Yahoo account, which I have had for a very long time; it has been involved in seven data breaches over the past 25 years. I can see exactly where the breaches occurred and what information was compromised by clicking on the results.

Lastly, I can see that my e-mail address associated with my business at **pj-networks.com** has been involved in 15 data breaches.

It is important to note that these breaches were not caused by me. These breaches are often due to companies like Target, Equifax, Aquarian, or Dell being compromised, and I happened to have an account with one or more of them. For example, Dell recently experienced a data breach, and since I have a Dell account, there is a possibility that my e-mail address and password were compromised. By checking for your accounts at [haveibeenpwned.com](https://haveibeenpwned.com), anyone can determine if their important e-mail addresses have been compromised and where the breaches occurred.

If there has been a compromise of your credentials, it is crucial to change all passwords associated with the affected account(s) immediately. For added security, consider setting up multi-factor authentication as a precautionary measure on every account where that is an option. If you are unsure how to enable MFA on specific platforms like Amazon or YouTube, simply search online for step-by-step instructions on how to do so.

## **The Dark Web**

### **The Dark What?**

Most people have heard about the Dark Web, but really have no idea what it is, so I would like to take a moment to explain it.

The Dark Web is a part of the internet that is not indexed by traditional search engines (not included in search results when you perform a Google or Bing search), and it requires specific software, such as Tor (The Onion Router), to access it. It is known for its anonymity and is often associated with illegal activities, such as the sale of drugs, weapons, and stolen data.

However, it also hosts legitimate uses, such as providing a platform for whistleblowers and activists in oppressive regimes to communicate securely.

Basically, the Dark Web is a place that you should never need to visit, but if you ever do, then you need to be exceedingly cautious – it is like visiting a very bad neighborhood in a big city that most people would stay clear of. However, if you would like to learn more about the Dark Web, this is a good place to start: [Dark web - Wikipedia](#)

What's scarier than the Dark Web? If you really want to know, then read on...

## Quantum Computing

This section on Quantum Computing is going to get a bit heavy, so if you're only interested in learning about Cybersecurity Essentials, feel free to skip to the next section. The only reason I am including it in this book is because Quantum Computing will be powering Artificial Intelligence in a few years, and when you put those two together, well, you get a *CyberStorm*.

### Quantum computing to spark cybersecurity Armageddon, IBM says.

How's that for a [headline](#)?

Governments and businesses are not prepared for the havoc that quantum computers will create in the cyber landscape by the end of the decade, according to that IBM corporate executive. The advent of quantum computing and generative Artificial Intelligence could potentially pose new risks to the US financial system, warned the Board of Governors of the Federal Reserve System in a [report](#) issued to Congress on August 1, 2023.

Just do an Internet search for “the risks of quantum computing” and you can find dozens (hundreds, really) of articles on the topic. I will try to explain the fundamental risks that it creates.

From Wikipedia: “**Shor's algorithm** is a [quantum algorithm](#) for finding the [prime factors](#) of an integer. It was developed in 1994 by the American mathematician [Peter Shor](#).<sup>[1][2]</sup> It is one of the few known quantum algorithms with compelling potential

applications and strong evidence of superpolynomial speedup compared to best known classical (non-quantum) algorithms”.

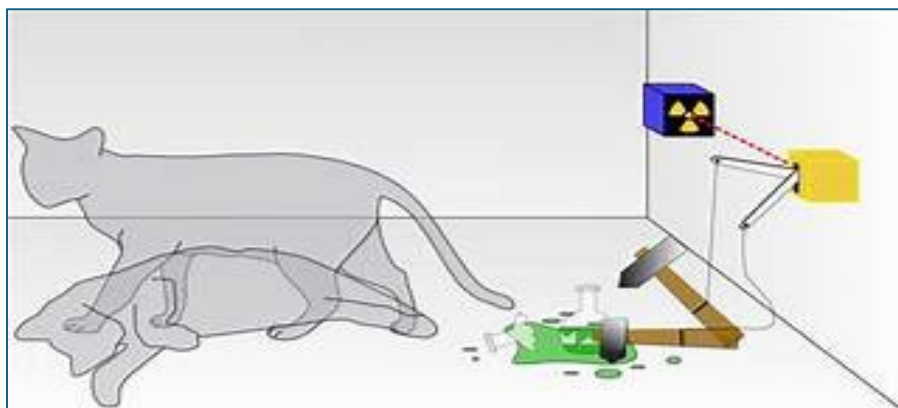
### Quantum's potential impact:

Exponential advantage: For specific problems like factoring large numbers (used in encryption), quantum algorithms like Shor's can work **millions or even billions of times faster than classical algorithms**. In 2019, Google's Sycamore achieved "quantum supremacy" by *solving a specific problem in 200 seconds that would take the world's fastest supercomputer 10,000 years to solve*.

Wow – that is truly mind-boggling.

### The concept behind Quantum computing is fairly basic

You've probably at least heard of Schrodinger's cat, even if you don't know what it is. It's a thought experiment where an imaginary cat (not a real cat, of course) is put in a box that's totally sealed. Inside, there's a vial of poison and a hammer mechanism that has a 50-50 chance of getting triggered and falling and breaking the glass vial, which will kill the cat.



The person on the outside of the box has no way of knowing if the vial has been shattered at any point in time. So, at any given moment in time, you do not know if the cat is alive or if the cat is dead.

That scenario is called “Schrodinger's Cat”, meaning the cat is at any given point in time **both alive and dead**, from the point of view of physics, and you cannot confirm whether it is alive or dead until you open the box. Until you do, from a quantum scientific point of view, **the cat is both alive and dead at the same time.**

Weird, huh?

Well, when you move that concept into the realm of quantum computing, the equivalent would be that any given digit, one value, one piece of data, one bit, can be broken down to being either a zero or a one.

A **bit** is the smallest unit of digital information that can be processed by a computer. It can have one of two values: 0 or 1. In binary notation, 0 represents the absence of an electrical signal, while 1 represents the presence of an electrical signal.

0 or 1 = 1 bit

All data can be broken down into these two digits, or bits, and a byte consists of 256 bits. There are 256 combinations of zeroes and ones possible in an 8-digit binary sequence called a byte, starting with 00000000 and going all the way up to 11111111.

00000000, 00000010, 00000100, 00001000, and so on. There are 256 combinations of zeroes and ones that you can put together in a sequence of 8 digits.

You get the idea.

Sorry – I digress.

Microsoft Copilot explains it like this:

1. **Bits vs. Qubits:** Traditional computers use bits, which can be either a 0 or a 1. Quantum computers use **qubits**, which can be both 0 and 1 at the same time due to a property called **superposition**<sup>1</sup>.
2. **Superposition:** Imagine a coin spinning in the air. While it's spinning, it's both heads and tails at the same time. Similarly, a qubit can be in multiple states simultaneously<sup>1</sup>.
3. **Entanglement:** Qubits can be **entangled**, meaning the state of one qubit is directly related to the state of another, no matter how far apart they are. This allows quantum computers to process complex problems more efficiently<sup>1</sup>.
4. **Interference:** Quantum computers use **interference** to amplify the correct answers and cancel out the wrong ones. This helps in solving problems faster than traditional computers<sup>2</sup>.  
In essence, quantum computers leverage these unique properties of qubits to perform calculations that would take traditional computers an impractically long time to solve<sup>3</sup>.

The key point here is that a quantum computer can process every bit as being **both a zero and a one at the same time** – those are called qubits. It then performs computations based on this assumption. *It can do simultaneous calculations based on two different unique conditions.* Instead of going sequentially through an encryption code, it can try millions of them simultaneously.

This is from Google Search Labs™: *Quantum computers can break encryption by performing computationally intensive operations, such as factoring large prime numbers, very quickly. This could put asymmetric encryption at risk, which uses two keys, a public key and a private key, to encrypt messages. Deriving one key from the other requires factoring large prime numbers, which is difficult for a standard computer to do in a practical amount of time. However, a quantum computer could potentially take a publicly available public key and derive the associated private key from it.*

Quantum calculations are going to be used to break encryption codes so that hackers can gain access to encrypted data more quickly; most encrypted hard drives using current encryption methods can be hacked in seconds using quantum computing.

Fortunately, quantum computing is not yet generally available to the public, and quantum protections are in the process of being developed and integrated into encryption algorithms to address this vulnerability. Hopefully, those protections will become available before quantum hacking technologies become widespread.

## **Quantum Hacking and Malware**

There are new dangers that are emerging in the form of quantum hacking, quantum malware, and quantum sabotage. Regulations are struggling to keep up with the rapid advancements in quantum computing technology. The combination of Artificial Intelligence, with its immense processing power, only adds to the complexity of the situation. There is an exponential advantage where quantum computing works millions or even billions of times faster than classical algorithms can protect encrypted content.

As mentioned before, in 2019, Google's Sycamore achieved quantum supremacy by solving a specific problem in just 200 seconds, a task that would have taken the world's fastest computer 10,000 years.

This extreme example highlights the incredible power of quantum computing. On a similar note, archeologists spent 200 years trying to decipher 5,000-year-old cuneiform tablets, but last year, they were able to use AI to decipher them in just a matter of *minutes*, providing them with translations that had been frustratingly elusive for centuries.

So, combine the power of Quantum Computing with the advanced analytical and trouble-solving skills of Artificial Intelligence, and it certainly seems like there is a storm brewing that we will need to learn how to control, navigate...or suffer the consequences.



## So, How Do You Protect Your Business?

The bottom line is that the average business is not even adequately protected from the cyber threats that are already out there, so how are they going to be prepared for the threat that AI is bringing, or that quantum computing is going to add to that threat? If a business has not even adopted the most basic protections available to them today, then how are they going to protect themselves against the more advanced ones that are on the way?

Here are some simple guidelines to start with:

- Educate your employees
- Only give your employees access to the data they need
- Use business-class firewalls (not home routers)
- Use the best EDR protection you can find
- Consolidate your data into one host platform
- BACK UP YOUR DATA (securely)
- Use encryption where possible
- Use MFA everywhere you can
- STOP – LOOK – THINK
- DO NOT FALL FOR POP-UPS
- Use common sense
- **Don't allow anyone to connect to your computer**

**First, educate your employees.** You need to give your employees resources to know what to be on the lookout for. Your employees are your last line of defense when a threat makes it past all of your other safeguards, especially from the things that your computer protection cannot protect you from.

When someone calls your employee pretending to be from Microsoft or the bank, trying to trick them into revealing a password, no security measure from PJ Networks (or any other security provider) can prevent that. **It is crucial to train your employees on how to spot and handle such social engineering attempts, including Deepfakes.**

PJ Networks has a program called “CyberLookout Sentry™” that educates our clients about the many different ways that business systems and company data can

be protected by employee vulnerability awareness. It does this through short weekly training videos, quizzes, and phishing e-mail simulations. However, there will be links provided for you at the end of this book for **free online resources** that you can use to give your employees access to cybersecurity training, and provide your staff with some no-cost cybersecurity education.

**Restrict access to company data:** When companies are first starting up and there are only a few employees, there is a tendency for everyone to have access to all company data – that’s something we see all the time. However, businesses really need to start thinking about only giving access to the data that each employee actually needs in order to get their work done. That way, if one user account gets compromised, the only data at risk is whatever that user has permission to access.

**Business-class Firewalls:** A TP-Link or Netgear wireless router that you can purchase from Best Buy for less than \$100 is not considered to be a business-class firewall, nor is the modem that your Internet Service Provider (ISP) gives you when you subscribe to their services. A real business or enterprise-class firewall provides Unified Threat Management (UTM) and has advanced protection features, such as website filtering and malicious content blocking, which you won’t normally find in most home routers.

**Consolidate your data:** Safeguarding data that is spread across the vast stretches of the digital world can be quite challenging. We work with clients who store data in Dropbox, Google Drive, OneDrive, on their local hard drives, on their servers, on their laptops, and they even hold onto unneeded data left behind by former employees. Managing and securing all of that data is a challenge, let alone backing it all up. We help them to consolidate their data. We recommend having a client choose **one primary location** to keep all of their important company data (a local server, OneDrive, Google Drive, etc.), and then we provide good backups and as much protection as possible for that storage location.

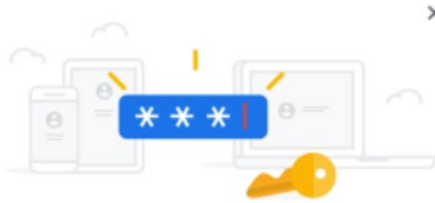
**Good endpoint protection:** For home users and smaller businesses, Windows Defender will provide a solid level of protection against viruses, ransomware, and malicious code. However, for larger companies (more than 10 employees), companies that work with Personally Identifiable Information (PII), and companies that work with high-value financial data, we recommend a higher level of protection

with multiple layers of security that are managed and monitored by a professional third party IT support company.

**Back up your data:** We've covered this several times already, so this is just one more reminder that if you back up your data and keep multiple backup copies, safely encrypted and isolated from where you store your company data, you can then recover your data from just about any disaster scenario. (However, you can't get it back from hackers if they steal it.)

**Encrypt your data:** When data is encrypted properly, it is unreadable and unusable to anyone that steals it, and ransomware cannot typically do anything to data that is already encrypted. Backups should be encrypted, as well.

**Multifactor Authentication:** Enable and enforce MFA (also called 2FA) anywhere and everywhere you can; banking websites, stock trading websites, shopping websites are all good places to turn on MFA. If all you need to log into a website is a username and password, then you do not have MFA turned on (or it isn't working properly). **BONUS TIP:** DO NOT allow your browser to save your passwords for you, unless you have MFA turned on for your browser, but then you need to remember to log out of your browser when you're not using it. Otherwise, anyone who gains access to your computer also gains access to your passwords.



Save password?

Username

Password

Passwords are saved in your Google Account so that you can use them on any device

**STOP – LOOK - THINK:** Many data breaches occur because people are in too much of a hurry to stop and look at what they are clicking “Okay” to. When you receive an unexpected prompt to approve a software installation, or asked by a pop-up to provide personal information, please take a moment to stop and figure out why you are being prompted for that information before you give that approval.

**DO NOT fall for pop-ups:** Many people have mindlessly clicked 'OK' on pop-ups without taking a moment to assess the situation or read the message, and that can eventually result in a data breach. Had they taken the time to read the content, they would have recognized that a visit to a website for information on Taylor Swift should not be met with a suspicious software installation prompt. Remember: **always stop, look, and think before interacting with pop-ups**. Most of them are likely to be harmful or questionable. Pop-up messages, fake virus warnings, and unexpected prompts are some of the most common ways that people get compromised or breached, so if you see a pop-up, be extra cautious about what you decide to do next.

**Use common sense:** You absolutely do not have to be a computer geek or even slightly tech-savvy in order to avoid 95% of the most common scams; you just need to use a little common sense. If something seems suspicious, then there is probably a good reason for it. Hopefully, this book has helped you to realize how simple it can be to protect yourself online just by using a little common sense.

**DO NOT LET ANYONE CONNECT INTO YOUR COMPUTER:** Microsoft is not going to call you and ask to connect into your computer, nor will the IRS, HP, or your bank. So, don't give anyone access to your computer, either locally or remotely, unless you know them and confirm that it *is* them. (Remember Deepfakes)

**Watch out for DEEPFAKES!** Hackers and scammers can now use Artificial Intelligence to create audio that sounds just like someone you know – a child, a sibling, a parent, just about anyone. They can also create videos that mimic someone you know, as well. If you get a call from “someone you know” asking to connect into your computer, first ask them why. Then, tell them that you'll need to call them back, first, and then hang up and call them back. There haven't been a whole lot of successful Deepfake scams that have made it into the news, yet, but

they are on the rise, and I predict that it won't be long before it becomes a very common thing.

## **What To Do Next**

PJ Networks, as well as other Managed Service Providers, offers a wide range of cybersecurity services that are typically too expensive for small businesses to afford on their own. We offer 10 different layers of protection for our business clients, bundled together into a package that even smaller businesses can budget for. Purchasing these services individually would be costly for most small companies. To obtain the necessary licenses at an affordable price, we must buy them in bulk, and then we can pass along discounted pricing to our clients.

Even if they could afford them on their own, the other challenge for a small company would be to manage so many different security solutions. With that many solutions available, it would practically be a full-time job for an employee. We manage our cybersecurity stack as a team.

So, start implementing the strategies that you can handle on your own – don't delay or wait until you can get all of them implemented at the same time; just start with the basics and work from there. Use good passwords, enable MFA where you can, turn on your personal firewall and use good endpoint protection; those are all things that you could take care of in the next few days, if you really intend to boost your security.

So many small businesses have practically no security measures in place because they don't know where to start, and so they never do anything – not even the most basic things, like giving each user on their network their own unique password. If everybody on your business network is logging into their computers with the user name "Administrator" and the same password, you have a disaster just waiting to happen.

So, begin with the measures that you can manage independently without any cost, and then consider implementing the ones that you may still need help with.

When that time comes, seek out a reliable service provider like PJ Networks or another trusted IT services company to help you take the next steps.

Here is a Golden Rule to help keep yourself from getting compromised:

Do not let  
**ANYONE**  
connect into your computer  
**FOR ANY REASON**  
if you do not  
**KNOW THEM!**

or have some way of positively confirming  
their identity

(Call your bank, call them back, e-mail them)

Google searches are **\*not guaranteed\*** to connect you  
to the *actual company* you are trying to reach.

(You might want to print that out and post it on the wall somewhere)

## Cyber Insurance

Cyber insurance is a great safety net; it can help a small business recover from a business e-mail compromise or data breach incident.

Just be aware that if you apply for a legitimate cyber liability or cyber insurance policy, it should require that you fill out a questionnaire that asks security questions about your computers and network environment. If it doesn't, then you probably aren't looking at a very good policy.

Remember that you have to answer those questions **accurately and truthfully**. If you do not answer the questions honestly, then you run the risk that your claims could be denied, so if any of the answers are a "No", answer no. It may make the policy a bit more expensive, but at least you will get valid coverage.

If you are going to fill out a cybersecurity questionnaire for an insurance application, make sure you answer it fairly and honestly. If you don't know the answers, work with someone who does or can help you find them out, so that your policy is valid.

For example, if one of the questions is (and it should be): are you enforcing MFA for all your online business accounts?

If you answer "Yes", and then one of those accounts gets compromised, when you go to make that claim with your cyber insurance company, **they will be able to tell whether or not you had MFA turned on at the time of the incident**. If you had answered yes on the questionnaire, but that wasn't true at the time of the compromise, then they're going to deny your claim, because you said that you had multi-factor authentication enabled when, in fact, you did not.

Otherwise, you are just throwing away your money and getting no real protection.

## The Next Steps You Should Take...

Further your cyber education, assess your company's security posture, improve the situation where you can...or do nothing and hope for the best.

Keep in mind that **60% of small businesses close within six months of a data breach**. Businesses that do nothing now will regret that decision within the next 12 to 24 months, because if you suffer a ransomware attack that takes down or exposes all of your data, the odds are better than not that your company will never recover.

**YOU HAVE BEEN WARNED!** Now, let's be careful out there.

-PJ

## Special Thanks:

I would like to thank the following people for providing assistance with this book:

- Jason Flint, Director of Managed Services, *PJ Networks LLC*
- Jennifer Hoppe, Marketing Assistant, *PJ Networks LLC*
- Kelly Jaderborg, Director of Administration, *PJ Networks LLC*



## Additional Resources

You can start by checking out the cybersecurity resources offered for free on the Virginia and Michigan SBDC websites.

By visiting <https://www.virginiasbdc.org/programs/cybersecurity/> you'll find a tool to create your own cyber risk program. Additionally, there are a variety of recorded cyber webinars available to assist in training your employees.

Michigan offers an impressive library of videos, training programs, and tutorials. Additional resources for Cyber Security are available from the Michigan SBDC: <https://michigansbdc.org/small-business-big-threat-home/>

See? You can educate your employees and secure your business without spending a dime.

Lastly, please **visit our website at** <https://pj-networks.com/> and select the pull-down menu for “Security and Compliance” and then choose “Free Cybersecurity Tools and Resources” from the list. There you will find a variety of free resources from public and government organizations providing information on how to protect your business.

### **More Resources from PJ Networks:**

Schedule a complimentary Cyber Security Business Network Assessment: [Network Vulnerability Assessment](#)

**Weekly Blog Posts (typically on Cyber Security):** [PJ Networks Blog](#)

**Facebook:** New posts almost daily on the latest cyber threats and warnings: [PJ Networks Facebook Page](#)

**LinkedIn:** New posts weekly on the latest cyber news: [PJ Networks LinkedIn Page](#)

**YouTube:** Cyber Security Videos: [PJ Networks YouTube Channel](#)

If anyone has any additional questions or comments, please feel free to reach out to me directly at [phil@pj-networks.com](mailto:phil@pj-networks.com).

We hope that you have found our complimentary e-book informative and helpful.

And once again: ***Please be careful out there!***

## Afterword

So, that concludes my summary of the core Cybersecurity Essentials that I believe everybody should know. If your curiosity has been satiated, then I hope you have enjoyed reading this compilation of best cybersecurity practices and my own observations on how cyber threats are impacting the cyber landscape.

However, I have added several appendices to cover the topics of CMMC Compliance, Microsoft Copilot, and a few cautions to consider concerning Generative AI.

If any of those topics are of interest to you, then please read on!



Network Support \* Security and Compliance \* Managed Services

**Phil Jaderborg**

Chief Executive Officer

[phil@pj-networks.com](mailto:phil@pj-networks.com)

(434) 975-0122 ext 105

It's All Good!

[www.pj-networks.com](http://www.pj-networks.com)

*Whatever It Takes!*

# Addendum 1 to *Cybersecurity Essentials for Everyone*

## CMMC 2.0 Compliance

Content provided by Matthew Griffith, CISO, *PJ Networks LLC*

The Cybersecurity Maturity Model Certification (CMMC) 2.0 is a framework established by the U.S. Department of Defense (DoD) to enhance the cybersecurity of contractors within the Defense Industrial Base (DIB).

Starting in October of 2025, the federal government is going to officially begin enforcing CMMC compliance standards for businesses that engage in federal government contracts. (Unless they change the deadline, again.)

That means that if you go to a federal government website to apply for contracts and get awarded them, you are going to need to be able to show (or claim and back it up) that you have done a CMMC compliance self-assessment and received a passing score, which may eventually lead to a certified government compliance auditor coming to your business to perform an official CMMC compliance audit.

According to Microsoft Copilot:

Falsifying your CMMC compliance self-assessment score can lead to serious consequences, including:

1. **False Claims Act (FCA) Violations:** Submitting false information can result in liability under the FCA, which may include civil fines, penalties, and even treble damages (three times the amount of damages)<sup>12</sup>.
2. **Loss of Contracts:** If discovered, your business could lose existing DoD contracts and be barred from securing new ones<sup>3</sup>.
3. **Whistleblower Actions:** There are programs that reward whistleblowers who report businesses falsifying their cybersecurity compliance<sup>1</sup>.
4. **Reputational Damage:** Being caught in such a violation can severely damage your company's reputation, making it difficult to regain trust and secure future contracts.

Ensuring accurate and honest reporting in your CMMC assessments is crucial to avoiding these risks.

In other words, do whatever it takes to get yourself into compliance if you plan to continue to engage in federal government contracts, or go and find work that you can do in the civilian sector that doesn't have such hefty requirements.

You will need CMMC Level 2.0 in most cases if you work with [Controlled Unclassified Information](#) (CUI). Level 1.0 compliance is lighter and easier to achieve, while Level 3.0 is a very high level and requires some extremely high-level security standards and protocols. If the government holds steady to their deadline, then all government contractors will need to be able to demonstrate that they satisfy all of the security controls that go along with being CMMC compliant to one of those levels.

That day is not the day that you want to start preparing for being CMMC compliant - that day is already here if you're a government contractor and plan to continue being one in the future. It takes about 6 months of steady work to achieve CMMC 2.0 compliance, and your budget should be aligned with this goal.

The government estimates that achieving and maintaining a Level 2 certification for CMMC compliance will cost smaller companies around \$105,000 and larger entities approximately \$118,000, which includes having assessments every three years, and additional affirmations from outside entities.

It is crucial to start planning today for a successful implementation. To secure a government contract, you should aim to ***begin the process at least six months prior to needing to be compliant***. Aligning yourself with a company like PJ Networks, that is knowledgeable in NIST 800-171 and CMMC 2.0 compliance, will help to ensure a smooth and efficient certification process.

There are 110 individual controls divided into 14 categories in the requirements:

- 3.1 - Access Control**
- 3.2 - Awareness and Training**
- 3.3 - Audit and Accountability**
- 3.4 - Configuration Management**
- 3.5 - Identification and Authentication**
- 3.6 - Incident Response**
- 3.7 - Maintenance**

**3.8 - Media Protection**  
**3.9 - Personnel Security**  
**3.10 - Physical and Environmental Protection**  
**3.11 - Risk Assessment**  
**3.12 - Security Assessment**  
**3.13 - System and Communications Protection**  
**3.14 - System and Information Integrity**

From access control to data security, your employees must be trained and knowledgeable, and your auditing procedures documented and accountable.

You will need to consider questions like these:

- Who is responsible for managing, monitoring, and documenting your configurations?
- How do you identify and authenticate your employees into your systems?
- What kind of incident response plans do you have if your data does get breached?
- How do you maintain your systems?
- How do you protect any media that your company owns?
- How do you secure your personnel?
- How do you secure your physical environment?
- Who is doing your risk assessments and how are they conducted?
- Who does your security assessments?

Those would be starter questions for a compliance assessment – there are about 100 more controls to be accountable for, and each control can include multiple specific questions within them.

There will be dozens and dozens of hours of work required, possibly more than a hundred hours, in order to achieve full CMMC 2.0 compliance, depending on your organization's existing cybersecurity posture. The good news is that there is a plethora of information available online about it, and a myriad of organizations that can assist you in the process. Depending on how much assistance your business needs, you can expect to spend anywhere from \$10,000 to several hundred thousand dollars in order to get you into full compliance.

As with any other type of professional service offering, there are consultants who will charge you fairly for their work and their expertise, and then others who might charge you five times as much for the same amount of work – so research your options thoroughly and carefully.

Getting external help is almost always going to be necessary, because you need to involve a third party to assist in monitoring your network, logging all data activity, and providing services such as SOC/SIEM. Remember, some controls require thorough monitoring of your network, data access, and application usage, and each process must be precisely defined and documented. This means that no one can simply appear out of nowhere and provide you with everything that you require if they have not invested the time, energy, and resources into becoming a qualified compliance consulting resource.

Again, the CMMC compliance levels are: (1) the most basic, (2) which can be covered by a self-assessment, and then (3) which is the level at which you are assessed by the Department of Defense. (yikes)

There will be some serious work required on your part as a government contractor in order to continue to be eligible for those kinds of engagements, but it is not an impossible task. However, it does require time, diligence, and a monetary commitment. The good news is that PJ Networks can absolutely help you to get there, and so can a number of other External Service Providers (ESPs) located around the country. We have helped other companies to reach their compliance goals, and we can assist you with yours, as well.

Please do yourself a favor and don't wait until the week before you need to apply for a contract until you start the process of becoming compliant. There are extensive resources available online concerning NIST and CMMC compliance, but we recommend sticking to the ones that are being provided directly by the federal government.

Here is the main site for information on becoming CMMC compliant; this is an excellent place to start: [CMMC Model \(defense.gov\)](https://www.defense.gov/compliance/cmmc/)

## **Addendum 2 to *Cybersecurity Essentials for Everyone***

### **Microsoft Copilot Overview**

Content provided by Joseph Melendez, Senior Systems Engineer, *PJ Networks LLC*

Microsoft Copilot is an AI-driven virtual assistant that seamlessly integrates with a variety of Microsoft 365 components to offer help with everyday tasks. It is even capable of tackling more advanced tasks, such as creating an entire PowerPoint presentation for you. For example, I asked Microsoft Copilot to create a ten-minute PowerPoint presentation on Microsoft Copilot, complete with images, and it created a seven-slide Powerpoint presentation for me.

However, you do not want to have Microsoft Copilot (or any other tool) writing or doing all of your work; you really only want to use them for assistance. You may want to use Copilot to start an initial draft presentation for a client, but then you should personalize and expand upon it, adding your own style and content. Copilot can currently be connected to many of the Microsoft 365 applications: Excel, PowerPoint, OneNote, Word, Outlook, and now it also integrates with Microsoft Teams.

Having Microsoft 365 Premium and a paid Microsoft Copilot Professional subscription is going to give you the same set of tools that we have access to at PJ Networks, and that will give you the best set of resources for accomplishing some of the more advanced tasks.

Copilot can turn creating a one-hour presentation into an easy task if you provide it with some initial content to work with, like an existing Microsoft Word document, because it can write the original draft for you. It can enhance the collaboration of a work team in many ways, but first you have to take the time to learn how it works and practice using it for various tasks.

If you go to <https://aka.ms/copilotlab>, you will find some short tutorial videos that show you how to start using Copilot, for example how to create a prompt. You will learn about some of the things you can do with it, and you will get an introduction to the most common uses for it.

There is a free version of Microsoft Copilot which is available to the general public. You can check out at <https://copilot.microsoft.com>. Just go to that website (preferably using Microsoft Edge) – you don't need to install any special software in order to access it and start trying out different prompts and queries.

You can find plenty of additional information about Copilot on Microsoft's website. It is important to note that Microsoft requires a one-year subscription commitment with an upfront payment if you want the Professional version, but you can use the free version to your heart's content.

I like to visit the Copilot website just to ask it questions, sometimes, like this:

**Provide step-by-step instructions for turning on the firewall in Microsoft Windows.**

Sure! Here are the step-by-step instructions to turn on the Microsoft Defender Firewall in Windows:

1. **Open Settings:**
  - Click on the **Start** menu (Windows icon) at the bottom-left corner of your screen.
  - Select **Settings** (gear icon).
2. **Navigate to Windows Security:**
  - In the Settings window, click on **Privacy & security**.
  - Then, select **Windows Security** from the left-hand menu.
3. **Open Firewall & Network Protection:**
  - In the Windows Security window, click on **Firewall & network protection**.
4. **Select a Network Profile:**
  - You will see three network profiles: **Domain network**, **Private network**, and **Public network**.
  - Click on the network profile that is currently active (it will be labeled as "Active").
5. **Turn on Microsoft Defender Firewall:**
  - Under the selected network profile, find the **Microsoft Defender Firewall** option.
  - Toggle the switch to **On**.



Sure, you can find those instructions elsewhere on the Internet, but Copilot will go out and scan for articles and content that relate to your question, compile it into a straightforward and concise answer, and then present you with it. This saves you time by eliminating the need to go out and look at multiple websites to find the content you are looking for – Copilot does that for you and delivers what it “believes” are the answers you are looking for.

Here’s another example:

**Provide a list of the 10 most common cybersecurity threats to small businesses.**

Here are the 10 most common cybersecurity threats that small businesses face:

**Phishing:** Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity in electronic communications.

**Ransomware:** Malicious software that encrypts a victim’s data, demanding payment to restore access.

**Malware:** Various types of malicious software, including viruses, worms, and trojans, designed to damage or disrupt systems.

**Insider Threats:** Risks posed by employees or other insiders who intentionally or unintentionally compromise security.

**DDoS Attacks:** Distributed Denial of Service attacks overwhelm a network with traffic, causing it to crash.

**Man-in-the-Middle (MitM) Attacks:** Intercepting and altering communication between two parties without their knowledge.

**Advanced Persistent Threats (APTs):** Prolonged and targeted cyberattacks where an intruder gains access to a network and remains undetected.

**Cross-Site Scripting (XSS):** Attacks that inject malicious scripts into content from otherwise trusted websites.

**Password Attacks:** Attempts to obtain or decrypt passwords to gain unauthorized access to systems.

**Data Breaches:** Unauthorized access to confidential data, often resulting in the exposure of sensitive information.

Copilot is really good at searching the Internet for information from multiple online sources and then putting it together in abbreviated fashion, like in the example above.

Feel free to experiment with AI, but be cautious about relying on it too heavily for important tasks, like writing term papers or final reports. It is best used for rough drafts and as a reference tool, not for producing final work – that’s our advice, anyway. Again, you can go to <https://copilot.microsoft.com> and quickly engage with Copilot to assist you in generating content or templates. For additional features and integration with Microsoft 365 Suite, you can opt for Copilot Pro at \$30 per month.

With Copilot Pro, you'll be able to do more, including integrating with Teams and customizing Copilot to your liking. Unfortunately, government and nonprofit pricing is not available at this time, but we anticipate that it will be, eventually.

Microsoft Copilot, as part of the government process, strictly adheres to data protection policies if you are using the right version. By utilizing Microsoft 365 Premium or Enterprise, users benefit from the high-level security protocols that are integrated into those subscriptions.

The transparency in Microsoft's governance of Copilot usage, along with the accountability of tracking all actions and integrations, ensures that any potential data breach can be thoroughly investigated and traced back to its origin. This level of detail is exactly what the government looks for in their requirements, and they are necessary during data breach investigations.

You can find more information here: <https://copilot.microsoft.com/sl/kNuF4Llxywe>

Microsoft Copilot is integrated with several important third-party applications, and as time passes, an increasing number of other companies (not only Microsoft) are incorporating Microsoft Copilot into their applications as an AI assistant. Additionally, Microsoft Copilot ensures data protection through secure government principles, guaranteeing that your data is always encrypted and secure.

Ready to learn more about Copilot? Great!

You can start your journey here: <https://copilot.cloud.microsoft/en-US/prompts>

## **Addendum 3 to *Cybersecurity Essentials for Everyone***

### **A Few Words of Caution About Microsoft Copilot and Generative AI**

Content provided by Nathan Kipps, CTO, *PJ Networks LLC*

Generative AI is defined as AI that is capable of creating unique content, not just searching existing content and compiling or manipulating it. You should keep a healthy skepticism and cautious perspective on the use of generative AI; generative AI simply has not been thoroughly tested and proven, yet. It is well known that generative AI has a tendency to “hallucinate” facts and data when actual data is not available on a given subject, or if there is conflicting information available to it.

It is important to ensure that employees only use AI tools that have been approved and monitored by your IT department, whether it is an in-house team or a third-party provider.

Make sure that employees are not casually utilizing *any* AI tools, including the free ones, without the knowledge of others in the company. You never know the potential consequences of unleashing an AI engine on your company's data. As Copilot and AI are relatively recent technologies entering into the business market, they are facing intense scrutiny from attackers who are seeking to exploit any vulnerabilities due to their innovative and unproven nature.

Society is already experiencing social media platforms flooded with AI images, e-commerce sites with AI descriptions, and Amazon is being flooded with AI written books. The issues arise when AI starts learning from this publicly available information, and then retrains itself on data generated by AI rather than from human or historical data. This feedback loop can lead to confusion, as AI only knows the practices it has been following, not necessarily understanding what good practices are.

### **Start Slowly with Copilot**

A business should not start using and investing in Copilot subscriptions unless they specifically know how they want to use it, what they want to use it for, and how they

can leverage it within their business. Make sure you have a specific intention in mind before signing up for a paid subscription, not just for the sake of acquiring it.

A good way to start small is to get one person in your company a subscription and let them begin using it to explore its capabilities; I would not recommend that a ten-person organization purchase ten Copilot subscriptions. Begin with one, test out its usefulness, and if the benefits justify the cost, then consider expanding your usage to more people within your organization.

For security reasons, keep in mind that if you integrate Copilot into a user's Microsoft Teams application in your company, it will then provide the user access to **all of your OneDrive and Sharepoint company folders that the user has access to**, even ones that they didn't know they have access to.

Therefore, always verify what OneDrive files and folders a user has been granted access to *before* empowering them with Copilot. If a user is unaware of certain company folders being available to them in OneDrive, Copilot will know, and it will search them when presented with a query or prompt.

Failure to secure your payroll and HR data from unauthorized users may result in Copilot retrieving payroll information and providing it to users who should not have access to it. Even if access has not been explicitly granted, Copilot will access it if the user has access to it, either implied or explicit.

## **Generative Feedback**

One risk with AI is the potential for receiving “feedback” when the model is allowed to retrain on data it has already generated. For instance, if you employ AI to revise the e-mails you compose, you may run into issues. As you prepare to send an e-mail, you begin to rely on AI for improved phrasing; this is a useful application for it.

However, if your AI system begins to analyze the e-mails it has previously composed on your behalf, you could reach a point where it is examining more of its *own* generated content than yours, resulting in e-mails that do not reflect your style and voice at all. These e-mails will not look or sound like you wrote them, which is not what you want.

## Some Final Considerations: Power Requirements for Artificial Intelligence

If you're looking to protect the environment, remember that generative AI requires a LOT of processing power. Using AI solutions can be costly, and the energy consumption from training and running these models on powerful computers is incredibly high. For example, a large AWS data center can require around 100 megawatts (MW) of power. In comparison, a small town with a population of around 5,000 to 50,000 people typically consumes between 1 to 5 MW. (Copilot told me that)

And, in fact, on the news Atlas website, Elon Musk recently said that AI will run out of electricity and transformers to power it in the year 2025. By next year, Elon Musk is claiming that the rate that AI is growing and the amount of processing power that it requires is going to be more than the world can generate.

From Elon Musk: "The Artificial Intelligence compute coming online appears to be increasing by a factor of 10 every six months. Like, obviously that cannot continue at such a high rate forever, or it'll exceed the mass of the universe, but I've never seen anything like it. [The chip rush is bigger than any gold rush that's ever existed](#)"

An Amazon Web Services data center is being established in Louisa and Fluvanna counties in Virginia. I attended the county board meeting where they discussed finalizing an agreement. One of the factors behind choosing these sites is the proximity to the Lake Anna nuclear power plant, which can provide some of the power – *but not enough for the data center*. There was mention that the plant alone cannot supply sufficient power, and that additional power would need to be sourced in from neighboring counties.

It was truly surprising to learn that an entire nuclear power plant could not produce sufficient power for just one Amazon Web Services facility. The next shortage will be electricity, said Elon Musk, and also the transformers to step it down to the proper voltage. Industry will not be able to find enough electricity to run all of the AI chips. It sounds like the big shortage of the future will not be over gasoline or water - it will be electricity that we will all be wishing that we had more of.

OpenAI and Google DeepMind employees made headlines recently (6/4/24) by issuing a [cautionary open letter](#) about the potential risks within the AI industry. They highlighted the absence of proper safety regulations and advocated for increased safeguards for whistleblowers. It is a stark reminder that there may be a mysterious and concerning side to AI technology that remains hidden from our view.

It is important to exercise caution when utilizing Artificial Intelligence, as hackers and cyber criminals are relentless in exploiting every available tool, including AI. Despite the odds being against us, rest assured that we folks in the Business Technology industry are working tirelessly to maintain strong and effective security measures from any and every kind of threat to data privacy and integrity.