SECURITY REBOOT GUIDE FOR TODAY'S SMALL BUSINESS

Two Modern I.T. Stories

CRAIGPETERSØN

me@craigpeterson.com

855-385-5553

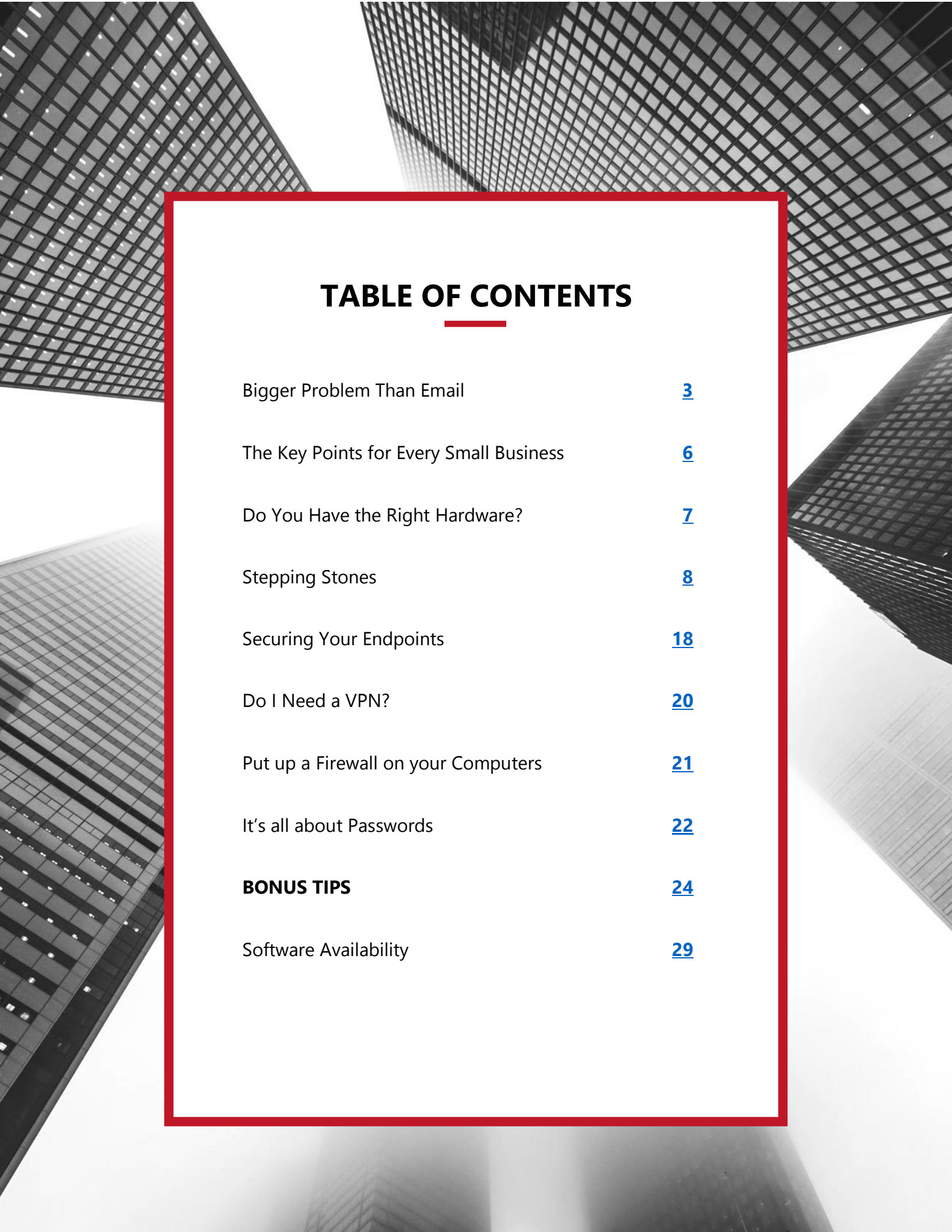


TABLE OF CONTENTS

BIGGER PROBLEM THAN EMAIL

I have a client, a relatively new client, who called me because he had heard me on the radio and he was experiencing some odd behavior with his email. He runs a tiny manufacturing firm with 8 computers and 6 employees. His office manager, who has been with him for over a decade, acted as his in-house IT person, although he also employed an outside IT firm to help her. The outside firm installed a basic firewall, security software and a router. The office manager did regular scans of their systems using the installed security software.

How common is this type of setup? Who is handling your computer systems' security? If it's the person with the most computer experience in your company, you're normal.

ISACA, a non-profit information security advocacy group, predicts there will be a global shortage of two million cybersecurity professionals by 2019.

Wow! Will we be able to fill this gap? Let me tell you about Josh, a 23-year-old who is hoping for a better job.

Josh works at McDonald's, and he makes about 23,000 a year. Josh's best friend Ken drives a new car and doesn't eat at McDonald's. Ken's making over $90,000 working IT for a company and tells Josh that he "can take an online course, and he will share his study materials it will only take a month," and Josh can start making $90,000 too.

Josh is so excited, he jumps in with both feet, and in just about a month, he knows all the buzzwords, and it turns out he knows just enough to convince the boss at a small company that he is qualified to take over computer security. The boss is impressed, hires him, and Josh begins working for the company as their in-house IT person.

Have you met a Josh? Have you hired a Josh? Can you tell the difference between him and someone who has years of experience, when you don't speak the same technical language (jargon, TLA's)? They can sound the same -- so how do you tell?

When there's a shortage of IT professionals, there's bound to be an over-supply of wanna-bees. Real professionals are demanding a hefty salary and benefits package that put them out of reach for many small to medium businesses.

Let's get back to my new client and his weird email problem --

It turns out that one of his customers also needed a security verification form filled out. He asked us to check things out further to make sure, but he was sure that he was all set. He just wanted to know why he was getting so much weird spam email and wanted his systems verified.

I started a scan of his systems, and the scans provided some horrible news. His computer systems had Chinese malware infecting them, including three backdoors that allowed the PLA (Chinese Army) complete access to his plans, drawings, finances, customer records, technical specifications and other research, and even his pricing.

After this, we started a more in-depth "Indication of Compromise Scan," which found even more bad news that included a live, ongoing exfiltration of his data.

When his in-house IT person, Maria, found out that he had called me in, she became very defensive. She called her outside IT company who came in to look at her systems and talk to one of my engineers. Their technician verified that what we were doing was in fact, legitimate. To prove everyone wrong, Maria began running more of her scans which returned "No Infections or Malware." All systems are safe. Of course, both Maria and her "Professional Grade" anti-virus software and systems were utterly wrong.

Employees Running Software They Shouldn't Cost Thousands

GDPR, CCPA, PCI, HIPAA and more privacy and security regulations come out every day. Per usual, the rules and laws can't keep up with the ever-changing state of technology. For the small business, complying with this matrix of rules, regulations and laws is taxingly expensive in time and scarce resources. Let me tell you about a small 20-person medical testing company in Atlanta GA.

How many of us have employees running software that exposes your confidential company information? Were you aware that these programs create two-way tunnels that allow all sensitive data to leave your network?

After a drawn-out two-year discovery battle there was a 12-page Civil Investigative Demand (CID) letter issued requiring them to provide detailed information on every aspect of their computer systems and organization practice. After complying with this demand letter, they filed a formal complaint in August 2013 against them, requiring that the company institute a comprehensive information security program and submit to third-party security audits twice yearly for the next 20 years.

It's hard enough to compete with these new online businesses. But now we have to "compete" with Hackers and Thieves. What are your chances of business survival in this environment of burdensome and unclear regulation?

Now back to my new client and their security verification form.

Remember this my new client had received a security verification form from one of their customers, well it turned out that their customer was a defense contractor, who was purchasing their products to put into military and avionics systems. This whole thing turned out now to be a national security issue. I worked with the client, contacted the FBI, and they came in and met with the client and made them aware of the gravity of the situation.

Thankfully, the owner had called us, and we were able to stop the leak, update their systems and install business-grade network hardware and security software. Although he did lose some of his data, in the end, it turned out relatively well so far.

Since the Chinese now apparently have his designs, he may end up competing against his very own designs being manufactured in China and sold a such a steep discount that he will not be able to compete.

THE KEY POINTS FOR EVERY SMALL BUSINESS

1) Document Everything

You can no longer run your small business informally with decisions made as you walk to the break room. Today's regulatory environment requires documentation of every step of every decision in such exacting detail even a stranger could understand it. Yes, this means that you document every operational procedure, every technology purchase and that you have a complete blueprint of your network. It is an arena in which electronic alternatives or reliable services that specialize in regulation can be especially helpful to keep any potential for exposure (for theft or liability) to a minimum.

2) Install a Comprehensive Security Program

Make sure you have a comprehensive data security plan in place. Sometimes this means having a trusted partner who watches your security for you. Cyber theft of every kind is a growing risk for small business, and just by taking the short and straightforward steps such as applying malware and security software and putting sufficient physical access and password protection in place is of great benefit.

3) Consider the Implications – all of them – Including the staffing and outsourcing

How does a company's liability shift when it employs directly versus work fulfillment through an external agency? There are implications to every storage decision including where they store client data (and particularly data such as medical records) on site or outsourcing that storage to the cloud. If you outsource, where is the cloud located? What is your company's liability? Likewise, how much liability do you have for the actions of in house employees versus those you engage through outside services? Be sure that you research these alternatives with care in advance.

4) Be a Savvy Business Consumer

Make sure you are aware of any regulatory issues that could affect your business. Stay abreast of the changing regulatory climates that affect their industries and business. This rapidly evolving environment presents a need for small businesses to stay flexible as they work not only to keep their organization as safe as possible but to capitalize on the opportunities to meet new market needs.

5) The Security Success Path

Although you can throw a lot of expensive hardware and software at the problem, that alone can't protect you, and especially if you have not taken the time to understand how to operate and tune those systems effectively.

DO YOU HAVE THE RIGHT HARDWARE?

Were you aware that there are differences in the grade of components? Well, there are, and it makes a huge difference when it comes to security. You will find that a computer designed for use in a business will have large amounts of additional memory to deal and a larger heavy-duty and more powerful processors which are capable of providing increased processing capacity and are often custom designed for running unique business applications.

Whereas, computers sold at big box consumer stores have components that have been cost reduced, to meet the price point necessary for that retail market and mass designed for personal use meaning reasonably light computing resources in both memory and processing power. When used in a commercial or business application they are quite underpowered and many times not readily upgradable.

Let's spend a few minutes and discuss what you must do to get your company on the security success path.

STEPPING STONE 1:

Security Audits from the Top to the Bottom

Every company should have in place a policy for conducting regular security audits on all of their Information Technology assets and practices. These audits should review and test all the security practices and procedures from the heart of the IT department to the peripheral edges of your enterprise (includes off-site manufacturing, third-party services, mobile devices, IoT devices, access control systems, and phone systems.) Every audit should review the hardware, firmware, and software security protection techniques but also evaluate personal employee habits and their compliance with corporate security policies.

Security Audits/Assessments: If you don't know you have a problem, then you don't know where to start.

There are four types of assessments that I recommend:

Risk Intelligence - We begin by performing a Risk Intelligence scan to look for unsecured data across your network—even in persistent storage.

Indication of Compromise - Next, we run Indication of Compromise Scans. These allow us to look for existing hacks/viruses/ransomware threats and locate any activity that may have occurred that appears suspicious, and to confirm any presence of either known or unknown malware found on devices attached to or off the network.

Vulnerability Scans - Vulnerability scans and vulnerability assessments search systems for known vulnerabilities. The most important thing is that the Vulnerability scan you run is accurate, because like my new client found out, you have a worse problem than you thought. An inaccurate vulnerability scan that misidentifies issues too often can be more trouble than it's worth. Make sure that the version of the vulnerability scan you use is the most current available, that way you are not picking up "previously patched vulnerabilities or ones that a recent release of the operating system or application corrected." However, you need to remember that if you have not patched the vulnerability or ignored the notice of or failed to install the patch or update, it will flag the deficiency.

Penetration Tests - A penetration test is test that actively attempts to exploit any weaknesses within your environment. These types of tests require specific levels of security expertise.

STEPPING STONE 2:

Don't forget your Human Factor – Dangers of Social Engineering

How much value will tempt an employee to give up confidential information? Part of your audit must look at how vulnerable your employees to being tricked or lured into revealing information they should not. How trusting are they? How gullible are they? How efficient do they try to be? How much do they like to talk? Each of these is traits that can be exploited by a black hat social engineer. In many breach investigations, it turns out were the result of a human factor failure that led to the breach.

A loss of vital information might occur by leaving a computer open and unattended running quickly to get something off the copy machine or to answer a co-worker's question. A phishing email might get acted upon because an employee was trying to get through their email rapidly and skimmed over the email not realizing that there were fake headers and clicked through, compromising your network to a piece of malicious malware.

STEPPING STONE 3:

Establish a vendor and business partner Audit policy

Do you use third parties to help offload your employees and increase efficiency? If so, when you are completing your audits be sure to include them. You need to have a policy in force that requires all your IT vendor and business partners to submit regular security audit reports on a biannual basis.

STEPPING STONE 4:

Security Education and Training – New and Continuing

When employees join your company, they should receive as part of their onboarding program, basic cybersecurity training as well as an introduction of the cybersecurity policies and procedures and employee expectations. They should sign off on their understanding of your cybersecurity policies. Most companies who have any regulatory compliance requirements must conduct regular cybersecurity training for their employees. Annually, there should be a company-wide cybersecurity refresher that includes a review of security policies and practices, as well as an explanation and discussion of any policy additions or changes.

STEPPING STONE 5:

Monitoring the Edge

Much manufacturing is being done using automated systems, and sometimes the plants are remotely located from the central facility. These situations require that all security maintenance for the hardware and software be done, not by qualified IT specialists, but by local employees who must adhere to all corporate cybersecurity policies and procedures. These remote sites can result in security exposures if the employees are not well trained in security practices and procedures and vigilance by the IT department and IT auditors.

STEPPING STONE 6:

Backups 3-2-1 and Verification

One of the most crucial security protections you can insist on is complete backups of your system. If a compromise to your data occurred or some black hat held it ransom would you be able to continue your business activities? If you were conducting regular nightly data backups, you might only lose 24 hours worth of data. One problem that many companies have is that they don't do them or if they do, they don't verify that the data written out, can be restored. Putting a backup policy in place that includes a requirement for all data backups and disaster recovery to be full-tested on a biannual basis will help to ensure that everything is working correctly.

STEPPING STONE 7:

Physical Security of all Information Assets

Having hardware, software and network security can not help you if a computer, can walk off the floor of the plant or off of the conference room table. Locking down the physical technology assets of the company is essential. It is also necessary that you have access control for specific equipment. All policies and procedures need to address both the physical and visual appearance of the asset.

Never Leave Your Computer Unattended: It is no longer good enough to set a lock screen when you walk away from your desk. Now I recommend that you turn off your computer. If you only have a lock screen enabled, it can not stop someone from connecting a device and stealing your data.

Encrypt your disk: Many computers come with pre-installed software and web-plugins - Remove these immediately. If you decide you need to use them later, install the latest copy of them directly from the company so that you have the latest security patches. Next, make sure that you use an Ad-blocking program. These programs can prevent advertisement tracking cookies and drive-by malware from being installed without your knowledge.

You should consider encrypting your computer which offers some great privacy benefits, but you don't have to be a techie to understand. All major operating systems have built-in full-disk encryption, and it is a way for you to protect your data from theft or in case someone gets physical access to your computer. A password will not help in this situation because they can break-in by using a USB device with another copy of the operating system on it, or using just a screwdriver, they can remove your hard disk.

With all the personal and private information that is on our computers today it is hazardous not to have it encrypted. Think about all the information that is on your computer, photos, videos, work and personal documents, databases and spreadsheets, password files, browser histories and information that belongs to you and is not for anyone else. By using encryption, you can protect this information from falling into the hands of a thief, a criminal or even a foreign government agent (for those who travel abroad - remember you don't have the same rights in other countries that you do here in the U.S.) If Border agents search your equipment, then disk encryption can protect your data.

What does disk encryption do? If someone gets access to your computer files, it will appear as a series of jumbled ciphertext instead of your actual data files.

However, disk encryption only thwarts those who have physical access to your computer. Network attacks are still a threat. It also does not prevent internet surveillance.

STEPPING STONE 8:

Compliance with Industry standards

IT security is crucial when it comes to regulated industries. Companies who are heavily regulated must review their security compliance requirements, annually and make changes to their security policy and procedures as they are needed.

STEPPING STONE 9:

Keep the Bosses informed

For a CEO nothing can be worse than being front of the cameras looking like a deer in the headlights while news reporters and angry customers pepper him with questions about how someone was able to breach his systems and why he did not keep their information safe. Nothing will put your job in more jeopardy than allowing the CEO to be unprepared when talking to the media. Whenever there is any cybersecurity incident, you must make sure that the CEO and the Board of Directors are aware of the situation and what is being done to remedy it. Often security systems operate flawlessly and never have an issue, and that is why when something does happen, those in the know about cybersecurity, must address the non-technical c-suite with a detailed explanation that they can understand. It also applies when enacting new policies, or when you need new equipment, be prepared to explain why that is necessary, its use and why now.

The path to Security Success is never complete – It goes on and on

Sorry to break it to you but security success is an ongoing process. You will have more updates, new security patches, new hardware, additional software, monitoring, and more training. But at least now you are on the right track and for what it is worth that is in itself a measure of success.

Make sure that all Systems and Softwares Are Up-to-Date

For most manufacturers and vendors, security patches and updates get issued when there is a discovery of a security vulnerability, and they are needed to protect their devices from being used as an attack vector against their customers. But, what if the customers IT department does not apply the patch or do the update? How can companies be assured that their systems are safe? Due to the volume and the speed at which the black hats are launching cyber attacks, I now recommend, that companies require patches and updates to their systems by not giving employees the options to not take the update. I know that it may be inconvenient, but it is the surest way to make sure that all the systems are patched and up-to-date.

By keeping all your devices and applications current with the latest releases you can reduce the chances of becoming the victim of a black hat hacker. Did you know that you increase your chances of being a victim with each additional application or service that you install? No software is inherently safe and “bug” happen when you

code and even more when more than one person is adding features to the software code. It is essential that you keep your system software and all apps on your system up-to-date to help avoid the chance of a security breach.

When software updates are released, it is because the manufacturer needs to address many different tasks within the operating system and individual software programs. Once they installed, they revise the software on your computer by removing outdated features and adding new ones, fixing “bugs” and patching security holes as well as updating software drivers and enhancing performance features. Black hats often rely on security loopholes within the system that they have discovered to deploy their malicious payloads.

An efficient way to keep your computers and mobile devices safe and secure is to keep their software up to date. Updates help manufacturers patch security vulnerabilities quickly.

Updating your Operating System (OS) to the latest version

I know we have all done it. The latest release comes out, and we are too busy to install it, afraid it will break things, or we have a lot of things to get done and can’t have the system down for an update. However, in today’s world and with the increased number of attacks against our business systems, it is no longer a good idea to not take an operating system update when it is released. Many times older but operational operating systems are not eligible for security updates. It means that they are wide open for the black hats to exploit with their malicious software. That also means that should a

breach occur we are at risk of having to waste a lot of valuable time and lots of effort to correct issues and recover data caused merely by our failure to adhere to best practices of updating our operating systems on schedule.

Function: The most current versions of the operating system have the newest security and stability patches, bug fixes and new features, which, if installed, can save your employees both time and energy. They may have more optimization of the user interface, enhances software tools.

Keep all your software and applications up to date

In the business world, and especially for small and medium businesses one of the most aggravating things they must deal with is patches and updates to their technology and technology tools. Many times, you are forced to stop your work and let the software update. Occasionally, this results in a crash of the system or need for a reboot. However, with the increasing number of vulnerabilities and malicious exploits, it is something that is best not ignored.

Function: Keeping your technology current, allows the installation of all security patches, bug fixes and software enhancements for optimal operation. Programmers and Software engineers work diligently to support the software while increasing its functionality and operability of the hardware for their customers. Unfortunately, sometimes technologies come installed with vulnerabilities and exploits. Often this occurs when some piece of the code has hooks in it from its initial manufacture. With the hackers becoming increasingly more sophisticated security that was good last month may not work now. If you regularly update your technology, you are inoculating your machine and reducing the chances that a black hat hacker can get into your system using some yet undiscovered vulnerability or infect other computers by manipulating an exploit.

Get a good anti-malware program

Anti-malware software runs in the background to keep a tab on all activities on your system and helps to avoid any virus attack. These tools work using advanced techniques and powerful search engines to find and remove all malicious threats.

- Check to see if you have an active anti-malware program on your computer.
- Make sure you have the latest version installed.
- If you don't have one installed, download one.
- Have the program scan your computer, then restart
- It is the best way to avoid all current and latest virus threats.

Patch and Update your system, to prevent black hats from using the "known holes" to launch their attacks

These include Computers, Servers, IoT devices, Switches, Routers, Firewalls, VPNs, Intrusion Detection/Intrusion Prevention systems, Applications and all your security software (Anti-Malware, Anti-Virus, Anti-Exploit, Anti-Ransomware, Anti-Rootkit, Pop-up Blockers, and Adware Blockers.) You should always go back and check your privacy settings after taking an update to make sure no changes occurred during the update. Go to your Settings or System Preferences menu on most digital devices to check your privacy settings.

While some phone and computer manufacturers are right on top of their security updates, others are not. The better companies have automated updates available for your devices which makes a lot of sense. However, many manufacturers who make routers, security cameras, carbon dioxide/monoxide, radon monitors, security lights, etc. do not.

For this reason, I recommend that every few months you assign someone to check for software and firmware updates for those items. You can locate instructions on how to update these devices either online or in the user's manuals for these devices.

SECURING YOUR ENDPOINTS

What are Endpoints? And why must we secure them?

Endpoints are end-user devices that connect to any network, in this case, your business network. They include servers in a data center as well as mobile devices, laptops, and desktop PC's but also may include other devices.

What is their Function?

Endpoint security is the act of securing the myriad of hardware devices and mitigating the risks that those connections present to your business network. Endpoints are many times the primary entry point for threats. Securing access to these endpoints at the perimeter of your system, substantially reduces the risk to the sensitive data that lives in the network by both monitorings the status of the hardware, all software that the equipment uses and all activities carried out on that hardware to block malicious activities. It also encompasses securing and protecting the data on those devices from misuse or theft, if the device gets lost, or stolen or otherwise end up in the wrong hands. First - do not confuse endpoint security with anti-virus protection. Anti-virus protection is just the most straightforward and most essential components of an endpoint security program which is responsible for the safety of every aspect of network access by any endpoint. As a business, your level of endpoint security varies significantly in scope from those available as a consumer version. When you employ a robust endpoint security program, all functions of your security begin to work in unison to create a more efficient system of protection. A full endpoint security system will incorporate management of all devices and the safety of all applications and programs running on those devices. It will include

and the safety of all applications and programs running on those devices. It will include antivirus/anti-malware scanning features, behavioral analysis (API hooking and DLL injection prevention for the identification compromise indicators. As well as a verdict decision engine that employs real-time analysis utilizing a global threat engine and access to human analysis for those files and applications that may be problematic, host intrusion protection for the monitoring of system processes and application activities to stop any actions capable of damaging critical system components. Also, it will have a packet filtering firewall that provides detailed management of all network activity (inbound or outbound), keeps your network hidden from malicious scans and provides warnings if any suspicious activity is detected.

How do you select an Endpoint Security System: What should you use?

Endpoint security systems come in a few varieties, and you will need to evaluate your needs before you select the type of system that is right for you. Here are some general guidelines.

Unmanaged Solutions are for Companies:

- Who have between 2 and 10 endpoints, (not people - endpoints (includes, mobile devices, networked computers, networked printers, etc.) and a non-centrally managed domain file server, Small offices that utilize standalone computers that are not networked at all or rely on a tiny, simple, network
- Who employs a third party network management solution of their centralized system and do not require any additional endpoint management solutions
- Who manages operations through a scalable network management solution
- Retail businesses and franchises
- Remote users that do not use a central network.

Managed Solutions are for Companies:

- Companies who employ a dedicated centralized solution to deploy, configure and report on all endpoints
- Small to Medium enterprises which maintain a single headquarters location
- Those who use a centralized network without a reliable, high bandwidth or permanent dedicated connection or VPN tunnel to smaller remote office networks.
- Companies who maintain a headquarters location and regional offices that utilize a Centralized network, plus smaller satellite networks for remote offices which connect to the centralized network via a permanent dedicated connection or virtual private networking (VPN).

Hybrid Solutions are for Companies:

- Who utilize a centralized network plus remote users, or users that do not connect to the centralized network on a regular basis. (examples: Schools/universities supporting facilities (classrooms/libraries/labs), staff and students)

DO I NEED A VIRTUAL PRIVATE NETWORK (VPN)?

A virtual private network will help keep your information private from one computer to another which makes hard to eavesdrop on your browsing habits or identify your real-world location. It acts as a tunnel to block the view of the traffic using encryption. However, once it is no longer travelling but arrives at a computer or server, it is no longer encrypted.

VPNs help reduce the risk of security breaches and cyber attacks because when your employees use it, your business data is not on a public network which means your company is less of a target for the black hats hanging around on free public wi-fi. Having VPNs for your employees helps them increase their productivity especially if you have been stressing the importance of internet security and they are now wary of working when they are offsite and only have public wi-fi available.

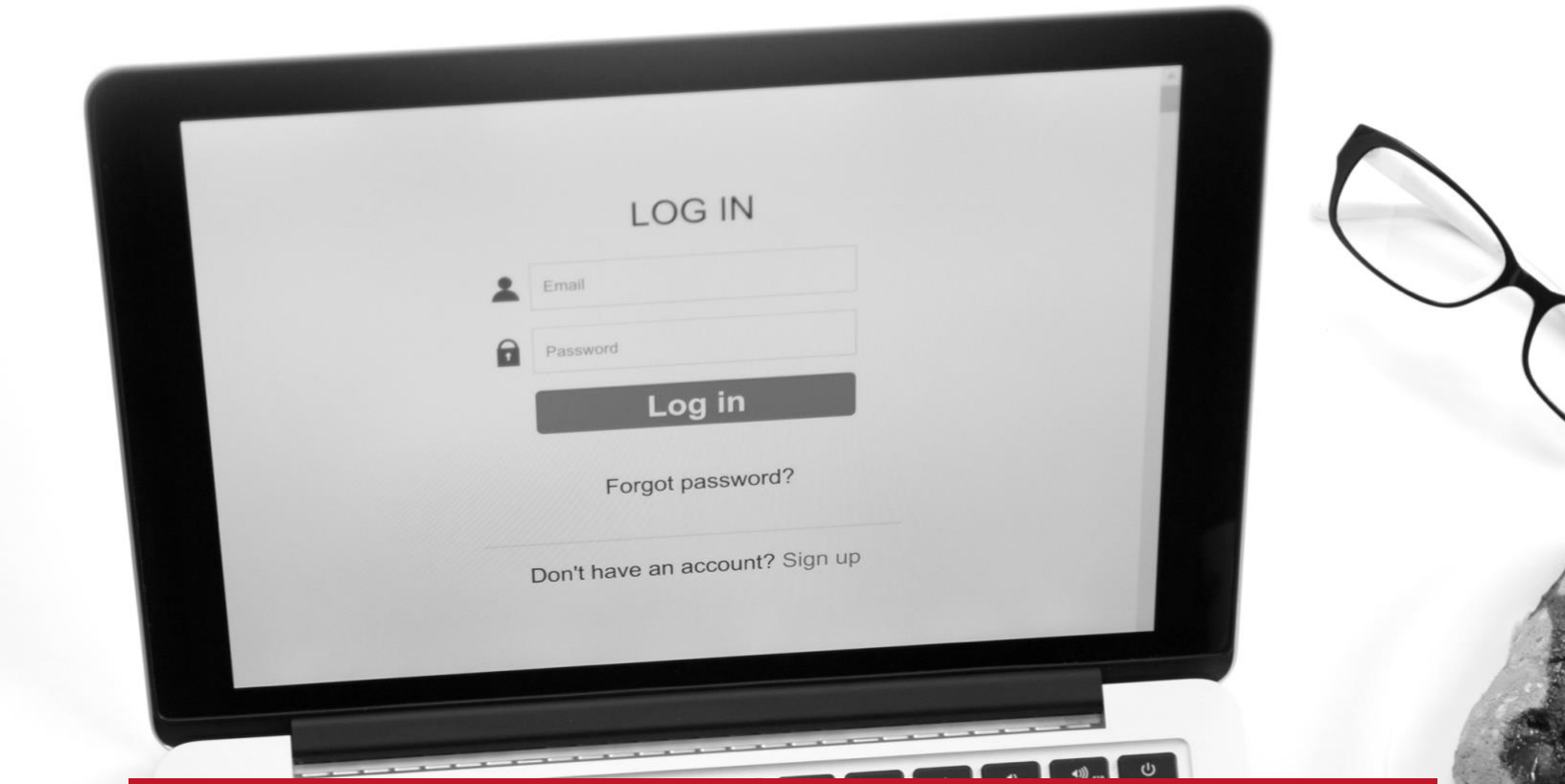
It is especially important if they are on the road, feeling secure in their communications with the office helps with their productivity. Using VPNs can help assure your clients that you are concerned about the data you collect from them and are trying to keep their data safe. If you have employees that travel out of your home country, then your VPN can be set to give them a "home network address" when they are out of the country. Your VPN will act as their IP address. It also allows these employees to connect with clients and customers who might not trust an email that arrives in another country. With a VPN, you can make sure all your company emails, posts will be identified as coming from your local office. VPNs are an affordable, worthwhile investment in your security.

However, remember that using any VPN, other than an entirely private one, means all your traffic is carried by a third party using their tunnels. Yes, all of it, and while it may be encrypted and unreadable, there is a lot of information about you available in the metadata, such as your location and which unencrypted sites you visit -- is still readable. You need to remember that VPN providers control your traffic, and they can not only see your traffic, but they are also able to inspect that traffic, and even modify it. They also can log it. What does that mean -- you guessed it - they will be able to determine very readily of what you are doing. If you choose to use a VPN, then do your research and find one you trust, to not abuse that trust and one that is capable of resisting demands by agents of their government to reveal your data. Free VPN services are free because they monetize your traffic using trackable ads so opting for a paid service is always better.

PUT UP A FIREWALL ON YOUR COMPUTERS AND DEVICES (ENDPOINTS):

An endpoint firewall consists of policies and rules that dictate the actions of traffic on your network. It means that depending on the rule or policy traffic will be allowed in or blocked or quarantined for further inspection.

Routers need to be protected by a Firewall:
Routers need to be protected by either a piece of hardware or a piece of software that blocks the unwanted traffic from entering and while allowing the right traffic through. Just because your internet provider supplies you with a router, does not mean that there is a firewall protecting it. You need to assure that you put a decent firewall on it to protect your connection to the internet from allowing everything in.



ITS ALL ABOUT PASSWORDS, PASSCODES AND THE USE OF A PASSWORD MANAGER:

First of all, you all know that you need a secure password, but it does not need to be hard to remember. As one of the bonuses, you will be getting my special report on Passwords and Password Management. Creating a password is a rather straightforward process. One that is a minimum of 12 characters in length, and I prefer 16 characters will make it hard to guess, but also easy for you to remember. After you create your strong and different passwords for all of your accounts, you do not need to change them. Previously recommendations included replacing them every 60-90 days. However, recent studies have revealed that this is terrible advice and now security experts are suggesting that you keep your passwords unless there is a reason to believe a compromise occurred.

Now, you need to keep that password safe which means, not on your desk, your drawer, in an excel spreadsheet, but in your head. Also, be sure that you don't use the same one on every site. Sites don't always keep your password secure, so you need to be aware of that by using different passwords on each site. To keep track of these, I recommend using a password manager such as 1Password or Last Pass. These also have a built-in password generator, which will allow you to create unique, complicated passwords for every site you visit.

You can think of a password manager like an electronic bank vault for all your passwords. You can put in passwords you have created, have the password manager generate a secure and complicated password for all your accounts. These are not expensive and are a well-worthwhile investment in your security.

Unfortunately, a password manager will not automatically replace passwords on all the sites you access. The process of locking down all your accounts is a manual one and requires that you individually log into every website, separately and change your password to the one that your password generates for that site. It is a time-consuming process, and so I recommend that you begin with your most vital and essential accounts first and work through them systematically as you have time.

- Now think about your mobile device: How secure is your passcode? I have a 16-digit passcode on all my mobile devices, and I NEVER use the thumbprint as an unlock feature. Why? At least in the US, you can be compelled to give your fingerprints if they suspect involvement in a criminal act. That act might only be a misdemeanor, but if the police can demand your fingerprint, they can demand that your mobile device, be unlocked. However, the courts have held that they cannot require your passcode. Most current mobile devices allow you to make the passcode as long as you want.

Give your company a security reboot. It begins with this booklet that will outline what you need to do, why and how to do it.

BONUS TIPS:

For preventing future infections of your system

Bonus #1 - Avoid Suspicious Attachments:

Attachments to emails are one of the primary ways that black hats use to launch their phishing scams and they also are how viruses get into your system. You must open these attachments for them to begin their malicious trek through your system. If you are not explicitly expecting an attachment from someone you know, then don't open it. Verifying the authenticity of any attachment is as easy as a quick phone call to the sender.

Bonus #2 - Avoid Suspicious Links:

Ignore unfamiliar links from unknown sources. Often these unexpected or random arriving links are sent to get you to open up a site whose purpose is to launch data breaches to your system that will result in loss of your sensitive data. Black hats use spoofing techniques that will hide a malicious and dangerous site as a real website. Even when you are browsing the internet on your system, check to be sure that any links you are using are safe links.

Bonus #3 - Practice Safe Downloading:

You should only download software and applications from reliable and reputable companies. Additionally, this is true for any updates to the software or applications you use. Be sure If you download from a third-party developer, that they are a highly rated company who is not known for creating harmful software.

Bonus # 4 - External Media Safety:

External media sources such as CD's, DVD's, Cameras, External Drives, and USB's can be the source of malicious software. If you do not know the origin of the media or question how you got it, you should not install it or use it on your system. You can scan the external media for viruses by inserting the media and using your anti-malware to examine it before you click start or open of any of the files which they contain.

Bonus #5 - Watch where and how you Browse:

Browsing the internet is not only a single function. While you navigate, you are being tracked by ad networks - who follow you from site to site, your internet provider - who keeps old logs on places you visit and even hackers who hope to target you. There are many browsers, and some offer more security than others.

Although you might see browser updates as a chore and not an important one at that, you need to understand how important those updates are. Updates to browser software will include updates and fixes which occur mainly hidden from the user's view but can assure additional safety and security from black hats who are trying to attack you. As I said before, some browsers are more secure than others. Browser updates offer new functions and features and when you use them will encourage the developers to create innovations and improvements in their products.

If you are not sure if you are using the most current version of your browser you can check here: https://updatemybrowser.org

Many popular browsers allow you to install a plugin called HTTPS Everywhere which encrypts your communications with many major websites and thereby helping you to browse the internet more securely.

Watch where you browse - avoid untrustworthy sites: There are sites out there that are just there to lure you in. They may have worms or other malware that will infect your computer if you visit the site. Keeping your anti-malware up-to-date is an excellent way to stop infections if you do happen upon an infected website.

Bonus #6 - Keep your servers and clouds secure:

Ok, you are now well on your way to being secure in your technology, but there is this thing called "The Cloud." What that amounts to is - SOMEONE ELSE'S COMPUTER! Have you thought about, how much information that you have entrusted to "the cloud?" What information do you store on these servers? Servers that belong to someone else, and ones you do not have control over. You also need to evaluate and ensure that you maintain a level of security and access control on those cloud servers meets your expectations.

Bonus #7 - Connectivity

Do you need to be connected to the internet all the time? Not every computer function requires internet access. When you don't need it, you should probably disconnect it. Having a connection to the internet, especially when you are not using it, is like leaving the door to your home wide open. One of the typical tactics of hackers is to watch for "always on" connections. If you have a sporadic use pattern, they are less likely to be attracted to you. If you do have to have your internet on at all times, then make sure that you have a robust firewall on your router.

Bonus #8 - Secure your mobile devices

When you think of an endpoint, What is your ultimate endpoint? For most of us, it is our mobile phone. That small device holds more sensitive and personal information than anything other technology we own. To make matters worse, we always have it with us. If you carry an iPhone, you carry among the safest mobile devices available as the iPhone encrypts your data as soon as you lock your screen, and if you have protected your device with a long passcode on the lock screen, you are even better off. Now if you chose an Android device, you must make sure to contact the manufacturer to make sure you have the latest operating system release and security patches, additionally you should check with your carrier to make sure that any patches to their custom software get installed on your device. Unfortunately, for Android, they do not have universal encryption available so to encrypt your device you must shut it down completely.

Bonus #9 - Make sure you are messaging securely

Have you considered how secure your data is during transfer through the internet? Today there is a struggle for keeping our data safe, and the reasons for keeping it secure are critical. Governments can't get enough, marketers and companies need it, and black hats want it the most. Currently, some laws allow for the monitoring of voice, text messages and data at any time. Additionally, police can use stingrays, or simulated cell sites to downgrade your cell connection from an LTE signal to one that is non-encrypted so they can more easily listen in. Think about this: When you are in a city or other densely populated place, and you suddenly lose LTE connectivity consider that your phone might have fallen victim to a stingray connection. Oh, they are not just interested in your conversation but in but all the additionally generated data (you know, that metadata, stuff they like to collect, but has no value) like who you are speaking with, when you

spoke with them, how long to talk, and where the conversation took place. It is the surveillance data on which these intelligence services thrive.

When you use end-to-end encryption, it keeps your conversation out of the hands of the black hat criminals who want to steal your information by making it available to third parties. When utilizing an app, the data is shared by only those communicating and no one else and protected from surveillance and tampering during both transmission and storage. I recommend Signal for encrypted communications. In Signal any communication carried out is encrypted end-to-end by default.

Our world is one of the digital data, and now more than ever keeping our that data secure and private is essential. One way to assure that privacy is by the use of encryption messaging app to secure your communication from criminal spies and malicious hackers.

Bonus #10 - Watch where you store your encryption keys

Just because you have the option of uploading your encryption keys to the developer's server, does not mean that it is wise to do so. If a compromise to their cloud servers occurs, your privacy is at risk. I recommend keeping a backup of your encryption key or your recovery key on your computer.

Bonus #11 - Using unsecured public Wi-Fi is not recommended

These networks are becoming ubiquitous. Treating them as though they are wide open and monitored is wise. When on these networks everything that you browse through, every action you take, and all information, including any usernames, passwords, security questions/answers, is openly available for access by anyone on the network.

Bonus #12 - Your secure phone's data

Most data plans today, offer LTE or 4G data. Some allow you to make your phone as a personal hotspot. If you are out and need to have a secure network, you are best off, using your cellphone vs public wi-fi.

Bonus #13 - What's App

What's App is an end-to-end encrypted messenger that is owned by Facebook and works on a variety of mobile devices. Communications carried on using this app are secure from being read by anyone other than the intended recipient including the developer or facebook. Make sure that you turn off all online backups. Online backups are available to be searched by law enforcement under warrant. I also recommend that you monitor any critical changes by enabling your security notifications. However, What's App collects quite a bit of metadata that can be turned over to the authorities just by simple subpoena.

Bonus #14 - iMessage

iMessage is an Apple application that was designed with Security in mind and is encrypted end to end. However, if you back up your messages to iCloud, Apple could be forced to that data to law enforcement. You should perform a regular encrypted local back up of your device.

Bonus #15 - Two-Factor Authentication:

Two-Factor Authentication Is one way that you can add additional protection to your accounts. It works because it relies on something you know and something you have. After you enter your password, you will be sent a code over an encrypted channel that you also will have to enter in to gain access.

Depending on the level of security you require you can have an authenticator app send the token to you. For most people, receiving tokens via their texting app is good enough. To secure your phone account, call your provider and set up a secure and lengthy passcode for your cellular phone account.

Two-factor authentication is available from almost every online service provider although the form it takes may differ from site to site.

Bonus #16 - Remove Old Unaccessed Accounts

It is a problem to keep accounts open that you no longer use. Blackhat hackers love to find old accounts that you are not using. They have the information they can glean about you and your habits, and they don't need to worry about getting caught. You should log in to them and shut down your account. Some mail accounts, allow anyone to register that email address once it is no longer in use.

Bonus #17 - Put a Priority on Privacy

Choosing the most robust privacy protections available is especially important when you get any new hardware or just a new application or service. These settings can protect your private information from being pilfered by companies who collect and then share it for a profit and from black hat hackers who want to steal your private information. If you sign up with a company and they ask for information that you don't want to give them -- don't. If there is not a good reason that an app would need particular details to complete its standard functions, you can turn off the permissions for the app to access those functions.

Whenever possible choose "opt out of data collection" and use companies that offer that option. When customers begin to demand privacy protection of their information, more companies will start to follow suit.

Bonus #18 - Fingerprint Sensor and Your Privacy

No passwords required, just a press of your fingertip and your phone unlocks - In the voice of "The Church Lady" - How Convenient. Like many another technological wizardry that come out -- security was not in the design and frankly may have gotten overlooked in a rush to market. If you use a fingerprint to unlock your phone and you get arrested the police can take your prints. Since they have the authority to require your fingerprints, you can be compelled by them to unlock your phone. I recommend using a very long, 16-digit passcode, to unlock your phone and using the fingerprint to open your apps. The courts have held that you can not be compelled to provide your passcode to the police.

In a recent study, they uncovered that digitally composed features of human fingerprints could fool these fingerprint sensors. While full human fingerprints are near to impossible falsify, tricking these phones is possible due to the small sensor size that only scans a partial print.

I recommend that you do not use fingerprint authentication for your most sensitive application such as mobile payments and banking apps.

You can Turn off Touch ID by going to Settings > Touch ID & Passcode > Turn off iPhone Unlock. (Android users can go to Settings > Security > Lock Screen or Nexus Imprint.)

Bonus #19 - Working together

One person alone can do quite a bit to protect their data privacy and personal security for themselves. But if we are going to make a difference, we need to work together, by telling everyone we know, to do the same. By working together, we can increase security and put a wrench in the cog of the black hats.

Bonus #20 - Ask for professional help

If you get bogged down or have no idea where to start, there are security professionals who are willing to help you. They can offer you suggestions on how to remove malware, install anti-malware software and even discuss ways you can prevent future attacks from happening.

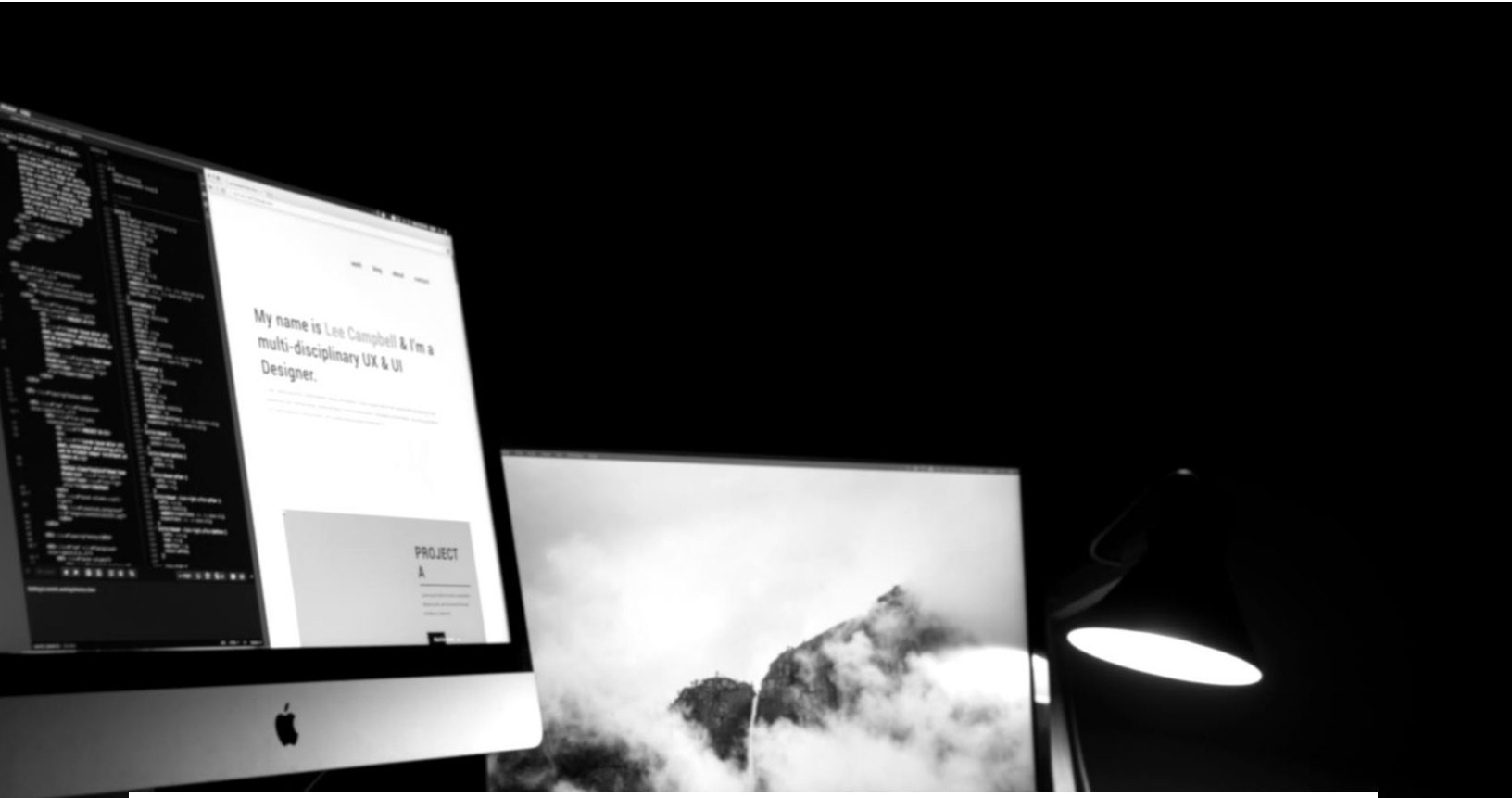
Bonus #21 - Have you been hacked - Freeze Your Credit

With some of the massive data breaches that occurred in the last year or so and all the information that is available on the dark web, there is not much you can do if your information was part of those breaches. However, you can put an alert on your credit so that you get notified if someone tries to get credit in your name.

If you do not need to use your credit you can stop all credit inquiries and any new credit from being opened by Freezing your account.

When you have a freeze on your account, it blocks lenders from accessing your credit history and without that they are unable to extend credit or approve any loan. However, this is a dangerous move because it will prevent any legitimate use of your credit history while it is in effect.

Each credit bureau must be contacted individually to put a freeze in effect or to remove it. The credit bureaus do charge for this service, but the fee is reasonable.



Software Availability:
Let's talk about the software available to you.

If you have a Windows machine:

Installing and Running Windows Defender will protect you 30%
Adding Windows Firewall will give you 20% more protection --- Now you are 50% protected
Add Malwarebytes - (affiliate link), and you can bring your effective protection up to 80%

If you have a Mac:

Configuring and using the Mac Firewall will protect you 50%
Add Malwarebytes - (affiliate link), and you can bring your effective protection up to 80%

Or you can contact Craig's company, Mainstream Call 855-385-5551 and get the Security Stack that he uses for all his enterprise clients.

Mainstream Security Stack = 98%
With Backup gets you close to 100%

CRAIGPETERSØN me@craigpeterson.com 855-385-5551

The Mainstream Difference

Our product is a stack of the best in breed security products that are integrated seamlessly into each other to amplify your level of protection and provide you with a comprehensive security strategy previously unavailable to the small and medium business sector.

No matter where your employees go on the internet we are there providing you with the first line of defense against threats by blocking malicious destinations before a connection is ever established thereby providing more effective security.

We stop malware before it reaches your endpoints or network by directly enforcing rules using your domain name server to find threats over all ports and protocols — even direct-to-IP connections.

We intelligently route any traffic from risky domains for a more in-depth inspection thereby protecting your network doing it without delay or performance impact.

If a device becomes infected through other means, we prevent any connections back to the attacker's servers. What this means is that none of that data will be exfiltrated avoiding any execution of these malicious programs as is the case with ransomware encryption.

Our systems are intelligent and learn from other internet activity to rapidly and automatically identify attacker infrastructure staged for current and emergent threats. We capture and understand relationships between malware, domains, IPs, and networks across the internet.

Our security platform is part of a global threat intelligence network that analyzes millions of malware samples and terabytes of data per day providing our platform with a context-rich knowledge base to proactively defend against known and emerging threats.

Our sandboxing capabilities allow us to perform an automated static and dynamic analysis of all your files against more than 700 behavioral indicators. It is this analysis that helps us uncover stealthy threats and block sophisticated attacks.

We block malware trying to enter your network in real time. We do this by employing best in breed AV detection engines that included one-to-one signature matching, machine learning, and fuzzy fingerprinting all at the point of entry allowing us to catch known and unknown malware. The result? Faster time to detection and automatic protection.

We also offer a roaming client for Laptops that are not connected via your enterprise VPN to extend protection beyond the corporate network.

Also, our security platform never lets you get behind on the latest patches.

When you employ our security platform, all your endpoints will be configured, patched, and maintained at the same level, regardless of geographic location.

We will be able to know precisely how many endpoints your enterprise has and the location of each one. We will be able to see the configuration, the installation of updates/patches, whether it is still vulnerable and if it is compliant with your company policies.

And it does not matter to us what Operating system your enterprise employs. We know that keeping all of your endpoints patched up and compliant with all regulations and policies is an expensive, time-consuming, and reactive job. These jobs require time and staff that you may not be able to spare. That is why we identify AND remediate patches for all OS's, critical software, and even some custom needs.

With all of the regulations that govern business and more coming on the horizon our security platform allows us to control endpoint configurations according to your organizational and best-practice plans and other regulatory mandates. When you are undergoing our onboarding process, we will help you customize policies to meet the many different needs within your infrastructure. Then we continuously evaluate every one of your computers checking for compliance. If an endpoint is out of policy, we automatically take action to reestablish compliance per your policy set. We log every activity and inform you in real time when we execute an operation.

So, what about our Mobile devices? Well if they are Apple devices we have a solution for all your enterprise supervised iOS devices, iPhones and iPads, using our mobile device management solution.

We will ensure compliance of mobile users and their enterprise-owned iOS devices, during incident investigations, by rapidly identifying what happened, whom it affected, and the level of risk exposure.

We will protect users of iOS devices from connecting to malicious sites on the internet, whether on the corporate network, public Wi-Fi, or cellular networks.

We will facilitate the protection of your corporate data and users by filtering and encrypting internet (DNS) requests.

Concluding Thoughts

Having information on the status of your systems is vital, so we make sure that you receive reports on endpoint status and every action taken.

What does all this mean to you — Speedy detection and automatic protection with all your devices protected from the first day.

For the first time ever, the world's best and simplest security system is available for your small business. We're so sure that you will find it the most straightforward and powerful security system you will ever use, that we'll give it to you free for three weeks.

Email me@CraigPeterson.com for more information.

Try the world's best Small Business Security System Free for 21 days!
We're betting that you will never want to let it go!

Reach out by email to:
me@craigpeterson.com