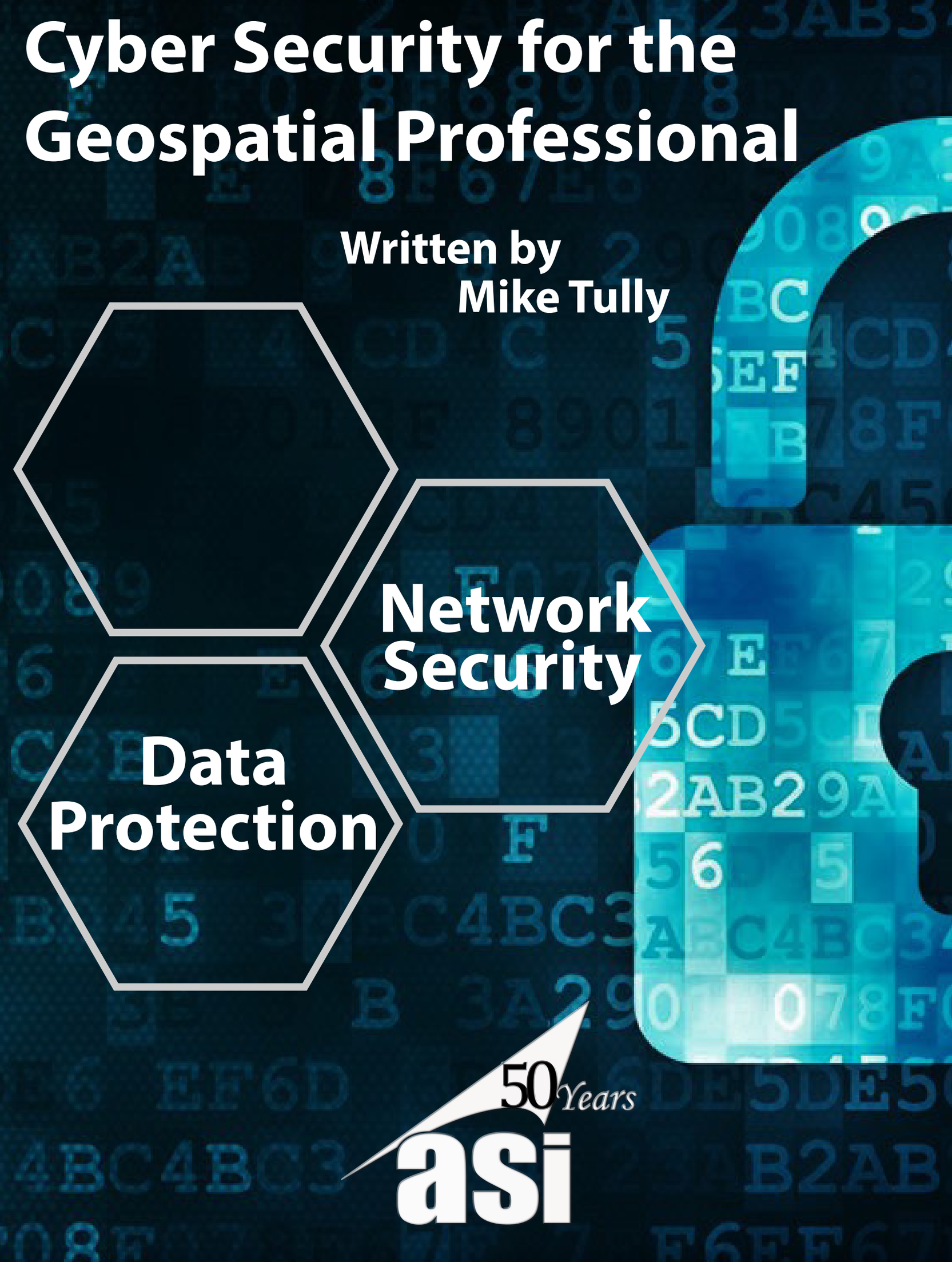
Cyber Security for the Geospatial Professional

Written by
Mike Tully



50 Years
asi

The Internet has lost its innocence. It is a dangerous place! Our antivirus scanners catch less than 5% of current threats to our safety and privacy. The 2016 Presidential election will certainly be remembered for raising the national awareness of how the hacking of our private email can be catastrophic. The wise will put their ears on and take note. This article encourages the reader to adapt the "best of the best" behaviors and tactics that anyone can, and should, use to stay reasonably safe on today's rapidly changing Internet.

But first, a few unalterable, universal principles. Like the laws of nature, these "laws of computing security" hold us accountable. As much as we wish it otherwise, there are no shortcuts or ways around these laws. They are:

Law #1: Complexity is the enemy of security.
Law #2: Security is hard. Absolute security is impossible.
Law #3: Security is inconvenient.

First, complex things are very hard to secure. More complex things are more difficult to secure. The Internet is the most complex machine ever created by a lot … by a huge margin! Second, absolute security is a worthy goal but can never be achieved. We must learn how to manage our risk and adopt behaviors and an awareness that provides maximum protection in an adverse environment. Last, security is the enemy of convenience. To be more secure means you will be inconvenienced. That's why we have keys to our cars. It's a pain to have to carry them around and when we lose them it doubly inconvenient. But we don't want just anyone to drive our vehicles. Our safe use of computers and the Internet will mean more inconvenience. Get over it!

Technical Illiteracy may be Your Problem

There is a type of growing "illiteracy" today. Many geospatial professionals are competent with advanced technologies like digital cameras, mapping software, and LiDAR systems. We can wield our smart phones like none other. But we may still have a technical illiteracy about Internet security. This illiteracy, much like low English language literacy, puts us at a great disadvantage and at much greater risk. If you are a computer user (and we all are) you first must understand the basic "language" (terms) of computing. If these recommendations or terms in this article seem foreign, confusing, or difficult you may be technically illiterate. It is imperative you assimilate a much larger technical vocabulary and expertise to understand the risks and garner increased protection from others who wish you harm.

The New Internet of Things Era

Every 10-15 years we enter a new era of computing. Each era comes with a new menagerie of threats. As of a few years ago, we left the Internet of Things (aka, IOT) era. The IOT refers to our global network of "smart" devices of all types connected to the Internet and each other. Computers are now so small, inexpensive and powerful that we can embed them inside anything for pennies. Wireless communication between devices using Bluetooth and RFID enable these trillions of connected smart (computerized) devices to talk with each other. These technologies have enabled a new era of computing where we have thermostats, light bulbs, appliances, mobile phones, laptops, Fitbits, GPS dog collars, baby cams, video doorbells, and all manner of gadgets embedded with smart computers and connected to the web.

Bruce Schneier, a computer security expert, says it helps to think about our connected devices differently to appreciate the gravity of this new IOT era. Our connected car is not a car but a computer with wheels and engine to move us around. The video doorbell is not a doorbell but a computer that allows us to see who is at our door from anywhere on the planet. Your cell phones are computers that allow us to talk to other people. ATM machines are computers with money inside. Everything is being connected to everything via the internet. But as our homes, our lives, and our devices are wired to the "Internet of Things" it fosters a growing dependence on it and leaves us vulnerable in ways that very few of us can even begin to comprehend.

"Technological progress is like an axe in the hands of a pathological criminal."

-Albert Einstein

"Technological progress is like an axe in the hands of a pathological criminal. ...Albert Einstein"
Why? Because criminals are early adopters of technology. All of this fast, powerful technology that benefits us so much is complex and "complexity is the enemy of security". Criminal hackers are experts at finding the vulnerabilities in our devices. They use them to steal our private information and money, and increasingly, cause physical harm in the real world of connected devices. It is generally acknowledged that, on average, there are 20-30 bugs per 1000 lines of code. Our cars today, for the most part are not connected to the Internet and are not part of the IOT, there are 100 million lines of code. Do the math! That works out to be up to 3,000,000 bugs. When your car becomes part of the IOT perhaps as early as this model year and is hacked, it may crash, be stolen or emptied of its contents. As Albert Einstein said long ago "Technological progress is like an ax in the hands of a pathological criminal." For these reasons, we all must decide today to practice responsible computing … to, digitally speaking, stop leaving the keys in our unlocked cars.

Consider these stats:

• 95% of malware is undetected by antivirus software
• 90% of malware infections come from hacked popular web sites the moment the unsuspecting visitor stops by
• 91% of all targeted cyber-attacks are done by "spear phishing"
• 99% of all mobile malware is targeted against Android phones.

[Full stop! Full disclosure: I'm not an Apple fanboy, but use IOS devices! The Android operating system (OS) is as secure as any. But our cell phone providers use their own flavor of this OS and fail to push out to their users the timely updates to that OS and often stop updates for unsupported models just a couple years old. The effect is that your phone becomes less secure with time and easily exploited by criminal's intent on your harm. Apple IOS device users don't share this same attack surface (if they regularly apply the OS updates) because all 1 billion Apple devices use the same core OS and updates are regularly and frequently pushed out to every single device. This makes a HUGE difference in reducing your security vulnerabilities.]

Below are the top 10 things you can do at home and at work to eliminate 85% of the threats. These were compiled adhering to two criteria:

1. Keep it easy to understand (even for a moderately literate technologist).
2. Focus on the "few" that afford the "most" protection.

If followed, these behaviors will protect you from 85% of cyber threats. Absolute security can't not guarantee (Security Law #2). But just as if you wash your hands it does not guarantee you'll avoid someone else's cold, good hygiene certainly decreases the odds that you will get sick. And besides, there is a certain joy and professional satisfaction knowing "you've been responsible and diligent protecting what's valuable in your life".

But just as general illiteracy exposes one to great disadvantage, so does technical illiteracy. If you don't understand the following recommendations or they seem too obscure or scary, you are probably illiterate and are inviting harm and difficulty to yourself, your family and your business. Spend some time and get comfortable with these recommendations and the technical skills behind them. [Refer to this glossary of cyber security terms as needed.]

Top 10 Things to Do to Eliminate 85% of Threats

ONE: Apply Operating System updates

Perhaps the single most important thing you can do is apply operating system updates as they are released on all devices: Windows, Mac, Android, & IOS. As discussed above, operating systems and applications are complex. And "complexity is the enemy of security."

New vulnerabilities in these systems are discovered every day. As developers identify flaws they are fixed and updates are pushed out to users. These should be applied as quickly as possible. And just as importantly: as updates for apps are released, apply them too.

TWO: Block / Disable flash, scripting, and ads

Flash is one of the most dangerous technologies on the Internet. Avoid it. Use browser extensions like Ad Block Plus and UBlock Origin to disable all flash. Delete flash players from your computer. Most websites don't require flash players any longer. If you use one that does, stop using it. Flash is simply too dangerous.

Most websites now track your Internet behavior. Aside from the privacy implications, these tiny "tracking" programs stored on your device require time to run and eat bandwidth. Disabling this tracking and the ads on sites speeds up your browsing and saves you money on data charges. Sites like petsmart.com and myspace.com (by no means are these two sites unusual) have upwards of 50 trackers on them. Each tracker consumes bandwidth and time and tracks your activity while online. Using Ublock Origin while browsing is equivalent to drinking out of a clean glass. Why would you choose to drink out of a dirty glass if you could get your water easily enough from a clean glass? Likewise, why browse knowing there are 10 or 50 trackers in the background wasting your time, money and privacy.

As for scripting: the best advice is to disable all scripting in your browsers. This, however, invokes Security Principle #3: Security is inconvenient. Most websites deploy script in the background that do many useful things. Unfortunately, invisible running scripts do many very bad things too and are a very common attack vector. The best advice is disable all scripting and "whitelist" the 20-50 sites you regularly visit. Our browsers allow us to create a "whitelist" of websites that we trust and will then allow their scripts to run. Additionally, both of these apps allow you to temporarily enable scripts on any website with a single button click. This feature is a good compromise with "convenience" so sites that don't work correctly because scripting has been disabled can resume working by enabling scripts on that site if needed.

Three: Use a password manager

LastPass The rule of thumb is: If you can remember your password it's weak and easily hacked. It doesn't matter how long it is. Password managers like LastPass generate random passwords and remember all your credentials for every website you visit. When you are prompted for a site's username and password, LastPass will enter those credentials for you. LastPass is very secure because your credentials are stored in an encrypted vault and you are the

only person that has the “keys” (the “master password”). They are always accessible on your devices with or without an Internet connection. Password managers are an indispensable requirement for cyber security today.

Stop what you’re doing now! Stop using weak passwords and configure LastPass today. It is that important!

However, you also must use passwords correctly for the password manager to be effective. Use 14-character passwords generated for you by LastPass. Never re-use any password. Change the passwords to the sites you frequent every few months.

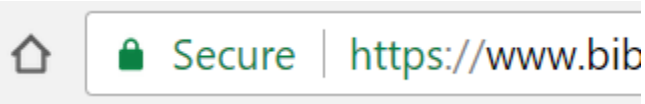
In 2013 a team of hackers demonstrated that they could crack up to 90% of cryptographically hashed passwords (many 16 characters) in under 1 hour using a commercially available computer that could guess (“brute-force”) 350 billion passwords per second. With this power, they were able to crack most 8-char passwords in under 6 minutes. Many much longer non-random passwords were similarly cracked in short order. NSA-strength computers were not needed! These same powerful cracking devices would take over 380 million years to crack a 14-character “random” password that LastPass will create for you.

While we’re talking about passwords, enable 2-factor authentication for your most important sites like Apple, Google, Facebook, Evernote, your bank, your 401k site, etc. While you’re at it, download the LastPass “Authenticator” app that makes using 2-factor authentication as easy as a single button click. Single-factor authentication is what you’re using when you are required to enter a username and password only. To login to that site, you must “know” something …. your password. But because passwords can be cracked or stolen “Single-Factor” security, especially when your financial information or personal information is at risk, is just not sufficient. Multi-factor authentication requires the user to have to “know” something and “have” something, like a mobile device. Before anyone can log into your account they must know the password and must have your mobile device that receives a code that must be entered. The criminal might steal your password, but they will not have your mobile device. So, you are the only person on the planet that will ever be allowed access to your site … unless you don’t have your mobile device! [Note: Most sites allow you to print “one

time passwords" after enabling multi-factor authentication. These are handy in case you don't have your mobile device and need access.]

BTW: it is even more important that you ensure your System Administrator (at work) is also using the same techniques for all the same reasons.

Four: Practice secure browsing habits



Look for "*https*" on all sites and double check each url to verify it is legitimate. Phishing attacks will try to cleverly fool you and present website addresses that look like: https://www.amason.com instead of the real address: https://www.amazon.com. Knowing that this is how they trick you is the first step in defeating them.

Don't click on links in emails unless you are certain they are legitimate or you trust the person that sent you the email. If your friends forward you an email chain with links, send them straight to your trash. Just don't click on links inside emails. Period.

Phishing is a technique by which criminals masquerade as a legitimate website to acquire information such as passwords and credit card numbers. "Spear phishing" is similar but is phishing targeted to you personally. This has become the preferred method of attack for online criminals and digital spies, responsible for a full 91% of all targeted cyber-attacks. Criminals are now using "social engineering" to help engineer spear phishing attacks designed just for you that will appear that they are coming from your best friend or perhaps your mother. This is a very serious threat and is another great reason to use multi-factor authentication. I consider myself to be very cautious when browsing and have been fooled by phishing attacks! These attacks are often extremely difficult to identify as "fake". Be smart!

By the way, Hillary Clinton's campaign manager's email was hacked and its contents leaked to the world during the 2016 presidential election. This was the result of a phishing attack on John Podesta, her campaign manager. It was totally avoidable if these best practices had been employed.

Five: Change your default login on your Windows machine to "user" not "administrator"

This is called practicing the "Principle of Least Privilege" where it is best to operate with the least amount of privilege. Each of us at home and at work should log into our computers with "user" privileges NOT as "administrator". Many times, "administrator" is the default account setting. Logging in as a user with "Administrator" privileges malware and other attacks have "full privileges" to run malicious software on the computer. Conversely, if logged in with user privileges, the malware is prevented from most harm and saves you from countless exploits!

Six: Don't ever attach USB drives to your computer

Unless you trust the person that gives you a USB drive, don't ever already outright banned these very convenient devices from their networks. Many firms fill their USB ports with glue to permanently disable them. There are new exploits that will electrically fry your computer the instant the USB is attached.

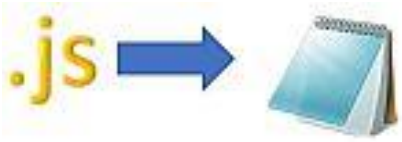
Seven: Ensure your System Administrator stays current on risks.

They should subscribe to the US-CERT weekly Vulnerability Summary. This report details every known exploit discovered and lists them by severity. This is an excellent resource to review regularly and will keep your SysAdmin current.

Related to #1 on our list, it is critically important that your SysAdmin stays current with the updates and patches available for the computers and applications on your firm's network. Patches for Windows, Linux, switches, routers and other devices need to be applied as they are released. Because these attack surfaces can be very large, this is very important.

Eight: Change the ".js" file type association to NOTEPAD.

Files on your Windows computer with the .js file extension are typically "javascript" routines. This ubiquitous Internet code is used on virtually every web page and is the code of choice for many nasty exploits. WSH is a very powerful, low level application that has elevated privileges to run operations on your computer. By default, .js files are associated with Windows Scripting Host (WSH). Anytime a user clicks on a .js attachment WSH executes the code. POW! Game over if its malicious. However, if these files are associated with Notepad then they are not executed by WSH but harmlessly opened in this text editor and cause no harm.



Nine: KNOW you have good backups all the time.

Good backups have always been essential for protection of data loss or corruption. But today, If you are a victim of ransomware attack, there is NO protection except a backup. Period! Game over!

Ransomware is a type of malicious software that infects a computer and restricts users' access to all the user files on it until a ransom is paid to unlock it. Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and

installed without the user's knowledge. The past several years ransomware threats have only grown in size and numbers. Your only protection today from a ransomware attack is a good backup of your devices.

Ten: Encrypt your PC / Mac.

Vercrypt is open-source software that encrypts data. It recently completed a security audit and provides very good, very secure encryption of all the data on your computer. Veracrypt (formerly TrueCrypt) is very easy to use and it only takes 10 minutes to encrypt your hard drive. Instructions are here and here.

Bonus: Practices that provide even more security and safeguard your privacy

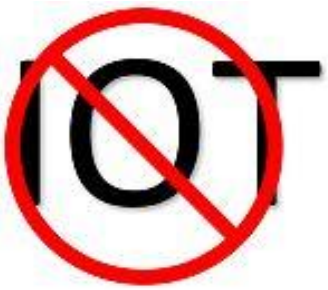
Eleven: Use a VPN all the time.

It's nearly free (Hotspot Shield costs 10 coffees for a year of use on all your devices. Virtual Private Networking (VPN) encrypts all data traversing to and from your device across an untraceable connection. You should never connect to public Wi-Fi (like in airports or hotels, or any network you don't own, manage, or trust who manages) without using a VPN. A great bonus when using a VPN is your surfing is anonymized and you can no longer be tracked by the zillions of sites that like to track you and build up scary detailed profiles of your life.

Twelve: Don't buy and use IOT devices

Most IOT devices manufactured today have been shown to have little or no security. What this means is that they create a door to your network that Crime, Inc. can use to waltz into your private life or business and cause mayhem. The only exception to this rule is if you know how to secure them

behind an impenetrable router like the amazingly solid and inexpensive Ubiquity Edge router or similar.



Americans now own an average of 3.4 IOT devices. By 2020, there will be an estimated 50 billion connected to the internet. Without any security standards in place and few manufacturers using any meaningful security design, IOT devices are dangerous. They have already been used to take down major sites on numerous occasions. Nest thermostats, baby cams, video doorbells, smart lightbulbs, and many other devices are now commonly available. Think of these as computers that control your furnace or as computers that show you who is at your door, or computers that enable lighting.

There are no security standards for these deviceds yet and most of them are being sold with particularly poor security that are quite dangerous for your networks at home and work. The best advice is "don't buy any" until manufacturers enable much better security. NOTE: most of these devices claim they use strong encryption and protect privacy. They don't! The U.S. Government is beginning to take these manufacturers to court and suing them for false advertising.

Remember this: Just because a manufacturer uses "strong encryption" does not necessarily mean it affords good security. There is much more to security than simply whether encryption is used.

If you have any other suggestions for cyber security, please add them to the comments below.

A very helpful glossary of cyber security and privacy terms can be found here (compliments to komando.com).

Sources for this eBook:

1. Years of listening to "Security Now" podcast at grc.com

2. Future Crimes: Inside the Digital Underground and the Battle for our connected World, Marc Goodman, Anchor Books, 2015

3. Bruce Schneier, 'The internet era of fun and games is over'. The Daily Dot, 16 Nov 2016

4. Austin Powell, Experts issue dire warning to government about the Internet of Things. The Daily Dot, 16 Nov 2016