WIPFLI LLP

30 TIPS in DAYS

Table of Contents

INTRODUCTION

Don't Be the Next Headline

Before the technological revolution and advent of the digital age, threats like identity theft, fraud and data breaches were no more than Hollywood plotlines – stories that flew under the radar, masked by more immediate dangers.

But then, the landscape *changed.*

Today, cybersecurity is a full-blown policy issue, underscored by high-profile breaches at major, seemingly untouchable corporations like Equifax and Target. This year alone, 60 million Americans have been affected by identity theft, compared to 15 million in 2017.[1] A recent Juniper Research study claims cybercrime will cost businesses $2 trillion by 2019.[2] And damage related to cybercrime is projected to hit $6 trillion annually by 2021.[3]

There's no question that the impact of cybercrime can be emotionally and financially devastating.

The costs can be extensive, including forensic investigations, reputational damage, fraud and the damages resulting from the theft of personal and financial data, money or intellectual property. But prevention is possible – and if you become a victim, you can prevail and recover. It starts with taking some basic preventative measures.

In October, we joined millions across the nation in honoring National Cybersecurity Awareness Month with the launch of our annual campaign, *30 Tips in 30 Days*. The initiative is designed to help everyday consumers and business owners take proactive, impactful steps toward becoming more cybersecure and stay vigilant in the face of potential online dangers.

This eBook is a continuation of the campaign, with the goal of helping you make cybersecurity part of your day-to-day life at home and in the office. At Wipfli, our cybersecurity specialists and thought leaders are committed to creating a safer digital world, one that encourages users to communicate, collaborate and connect freely and without fear. We encourage you to take action on these tips and keep the conversation going well beyond October. Let's make cybersecurity a priority – *together.*

[1] LifeLock, "How Common Is Identity Theft? The Latest Stats," April 13, 2018, https://www.lifelock.com/learn-identity-theft-resources-how-common-is-identity-theft.html, accessed November 2018.

[2] "The Future of Cybercrime & Security: Enterprise Threats & Mitigation," James Moar, Juniper Research, April 25, 2017, https://www.juniperresearch.com/researchstore/innovation-disruption/cybercrime-security/enterprise-threats-mitigation, accessed November 2018.

[3] Cybersecurity Ventures and Herjavec Group, 2017 Cybercrime Report, p. 3, https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf, accessed November 2018.

TIP #1

Keep Kids Safe With Parental Controls

Young people today are more connected than ever before, which also makes them a vulnerable target for cybertheft. Fortunately, there is a wide variety of parental control software available to help ensure your children stay safe online. For many parents, the biggest question is identifying which software is right for them. There are so many apps and products out there that claim to simplify the monitoring process, which can make it difficult to know which option to choose.

The best way to answer this question is to ask yourself what kind of control you need to have over your children's cyber activity. Look for common, helpful features like text message, phone call, email and website monitoring. Some products even offer more advanced features, such as disabling your child's cell phone while they are in a moving car or locking their phone until they respond to a call or text. Certain types of products work on both mobile devices and computers. The most important benefit is that you can have control over which apps and activities your child has access to, as well as the ability to monitor everything they do on their devices.

Here are some of the most popular options used by parents:

- **Qustodio**
- **OpenDNS FamilyShield**
- **KidLogger**

(Not all software includes every feature described above, and the list is not exhaustive.)

Remember These Important Takeaways:

- **Explore Your Options:** In June, PCMag.com published an excellent review and comparison of many popular parental control software choices – **be sure to check it out here**.
- **See the Software in Action:** Most packages have free trials, so you can test drive the products before you purchase them.
- **Practice Cyber Safety at Home:** Some internet service providers, such as Xfinity xFi, also provide parental controls as part of their packages. Check with your provider to see if parental controls are available for you to leverage.
- **Stay Safe On-the-Go:** Most cell phone manufacturers and service providers offer their own variant of parental controls. Google and Apple both have features that allow you to enable parental controls on mobile devices.

PRO Tip

Your children may be resistant when you introduce parental control software to them. Take the "trust-but-verify" approach when talking to them about parental controls and let them know why you feel it's an important tool to implement for their safety.

TIP #2

Beware of Oversharing on Social Media

Social media is a great medium for interacting and communicating with friends and family over the internet. Unfortunately, many social media users don't understand the importance of limiting what they post on these sites. Attackers use social media sites as reconnaissance tools on a regular basis. It's no longer surprising to hear about people falling victim to identity theft or networks being infiltrated because of information gathered from social media sites.

Many social media sites allow users to create profiles that can include their name, date of birth, the companies they've worked for, duration of their employment, the duties they performed on the job, the schools they attended and so much more. Hackers also can use the personal information users include in their social media profiles – the names of their children or spouse, for example – to guess the answers to security authentication questions and gain access to their personal accounts. The more information hackers expose, the easier it is for them to craft credible attacks. Sites such as LinkedIn allow users to create connections with co-workers, which can be beneficial from a professional or cultural perspective. However, this also gives hackers the information they need to determine a company's organizational chart in a matter of minutes. All of these entry-points provide potential hackers with the sensitive – and valuable – material they need to craft their attacks.

Like diamonds, the actions you take online last forever.

The idea that you can completely "delete" or "remove" your social media presence is a fallacy. Every time you post, update or engage online, your content is backed up, repeated, linked, indexed and spread across the internet. Search engines actively gather this content and store it in their databases, even storing the pages themselves. Organizations like **Archive.org** and the Library of Congress make it their mission to preserve the internet by copying billions of pages. So, one way or another, the content you post, comment, tweet or share is captured immediately by something you don't control – and can't delete!

How Can You Protect Yourself?

Employ what you learned during communications class about the responsibility of the sender and the perspective of the receiver. Sharing quick phrases without context, mixed with emotion and combined with a lack of nonverbal cues can be easily misread by your audience. Always think about how you want to be viewed by the world around you, and don't believe that your online presence is irrelevant when you step away from the keyboard. If it's posted online, it reflects on you! In today's digitally driven world, most potential employers review their candidates' online presence as part of the hiring process.

Online gaffes are played out publicly all the time, whether they're made by a politician, a celebrity or even one of your friends. Odds are, you know someone whose personal relationships have been affected by something they said – or read – online. Remember to step back and take a moment before you press "enter." Exercise a strict rule about how and when you engage online. Remember, your online footprint is ink for the entire world to see – not only immediately, but likely until the end of time.

Remember These Important Takeaways:

- Be cautious about what you post because hackers can use any information to carry out attacks.
- Review your privacy settings and restrict who is able to view your profiles.
- Only connect with people you know outside the realm of the internet.
- Assume that anything you post online is public and permanent.
- Don't post information that may damage your reputation or that of your employer.

PRO Tip

Your online "friends" are not always *real* friends. Limit access to your private information to only those you know personally, away from the keyboard!

TIP #3

Be Diligent About Backing up Your Data

While it's impossible to predict when your hardware will fail, it's safe to assume that, at some point, it will. What would happen if your phone and computer were caught in a fire? Would you still have access to your pictures? How much work would you lose? The best time to implement a backup strategy is before you need it.

What Can You Do?

The standard backup strategy is "3-2-1" — in other words, you should keep three copies of all your important files on two different mediums (on hard drives and DVDs, for example) and one copy off-site. You can implement this strategy fairly easily by keeping important data in a designated folder on your computer. Once a week, make a copy of that folder and store it on a cloud data storage drive as well as on an external hard drive; your cloud storage drive will act as your off-site copy. A great benefit to using a cloud storage drive is that most providers have their own backup processes and redundancy for their infrastructure.

When we think about the process of backing up data, we often think about the information stored on our workstations or personal computers. But you should also have a backup strategy in place for irreplaceable items, such as photos saved on your smartphone or tablet device. When looking for a backup solution, check to see if the provider offers an app for your Android or Apple iOS device as well.

Remember These Important Takeaways:

- Remember to encrypt your backups to ensure you are the only person who has access to your confidential information. (If you're using an online service like Google Drive, Dropbox or OneDrive, you should also make sure that confidential information is for your eyes only.)
- Backing up your data is also a great way to defend yourself against ransomware attacks, which are attacks that encrypt the files on your computer and require you to pay for the private key to decrypt them. If you've backed up your data to an external device or cloud storage, you can easily wipe your hard drive and restore your data to that drive.

PRO Tip

Keep all of your important files on a cloud storage drive, and periodically (once a week or so) make a copy of that folder and put it on an external drive. This makes it easy for you to keep track of your data and create backups. Test your ability to download your content and make sure you can successfully obtain your backed-up data before it's too late!

TIP #4

Actively Monitor Your Data Usage

If you're like most people, you probably have a plethora of online accounts that you use on a regular basis. It can be cumbersome to keep track of – let alone understand – the seemingly endless list of your accounts, such as Facebook, Instagram, Twitter, Gmail and Microsoft. Most of us don't have time to do the digging and find out what these sites do with all of our information once they have it. Today, most online services – especially the free ones – track everything we do on their sites, and they store that information for future use. In fact, most of them sell it off to third parties for advertising purposes.

Think about it: Have you ever researched hotel rates for a trip, and then noticed that your Facebook feed is littered with advertisements for hotels? It's not a coincidence – your web activity is the catalyst for these advertisements, and service providers are more than happy to sell it to the highest bidder. In some cases, the service even takes legal ownership of the content you upload.

Stay Diligent About Tracking Your Data Usage

Before you sign up for or use a service on the internet, you should know what it will or won't do with your data. The best way to do this is to read the service provider's end user agreement (EUA), which is a binding legal document between you and the provider. This agreement explains your rights and obligations as the user of the product(s), although it typically focuses more on the rights of the provider. It's important for you to be cautious of what you are agreeing to. Before you click "agree," you should read the EUA carefully to see whether:

1. Your personal data will be sold to third parties for advertising or telemarketing.
2. Your data will become the property of the provider.
3. You can delete the data.

Though EUAs aren't exactly the most riveting reading material, at the very least, you should skim the major sections and look for anything that looks odd to you.

Remember These Important Takeaways:

- When signing up for any service, see how the provider protects your data and what they can or will do with it.
- Services that are free or really cheap are usually the ones that are most interested in the data you enter, but even paid services like to make extra cash with users' data when they can – so practice caution. You need to make sure you understand how companies will use your data, and whether or not the way they're using it is acceptable to you.

PRO Tip

We'll say it again: Read EUAs! At the very least, skim the major sections and make sure nothing jumps out at you.

TIP #5

Use Strong Passwords and Store Them Securely

Passwords often are subject to many different cyberattacks, so it's important to practice diligence. By repeating certain "styles" of passwords, you'll increase the likelihood that hackers will guess the combinations. Uncomplicated, short passwords with common dictionary words and few, or predictable, numbers (e.g., the current year) can be easily cracked by hackers with free tools and inexpensive graphics cards. Using the same password for multiple accounts *greatly* increases the risk of a breach — and if one of those accounts is hacked, there's a good chance that hackers will crack the others, too.

PRO Tip

Always create strong, unique passwords or passphrases for each of your online accounts. Secure them with a password manager to reduce the number of passwords you'll need to remember.

How Can You Protect Yourself?

When creating your passwords, avoid referencing your username, seasons, numerical years, your children's names and other guessable or easily searchable data. Instead, use a "passphrase," which is a sentence that you can easily remember and type. The longer your passphrase, the stronger it is. Making your passphrase strong and of sufficient length can limit the success of humans and/or computers in guessing it. Using only simple sentences in passwords is becoming less effective especially with the decreasing cost of consumer graphics cards, which allow hackers to attempt up to 50 billion guesses every second. Always use strong, unique passphrases for all accounts that are secured by a password.

Creating Your Passphrase

First, use your resources. The National Institute of Standards and Technology (NIST) published an excellent blog post about best practices for coming up with strong passphrases and the science behind how they should work. **You can read it on the NIST's website here**.

Finally, after creating your new, secure passphrase, you should type it into a window that will not only save your work, but also will allow you to read what you have typed to engage muscle memory. Then, you'll have a better idea of how you might type the passphrase incorrectly, which will allow you to make improvements and memorize it to ensure optimal security.

Once you have created strong, unique passphrases for all your accounts, how will you remember this myriad of information? This is where a "password manager" application can come into play.

What Is a Password Manager?

A password manager stores all of the passwords for each of your accounts, allowing you to remember only one strong passphrase that you'll consistently use to access the password manager, and consequently, your accounts. Some passwords managers can also generate completely random passwords for you and store and recall them on demand. Random passwords of almost any length, or the maximum length allowed by the system, can be used in this manner. In general, password managers use strong encryption to secure your "database" of passwords.

Click here to view a non-extensive list of password managers you may be able to leverage. Some hardware-based password storage devices, such as the **Mooltipass** and **OnlyKey**, have recently become available on the marketplace and can provide secure, portable and easily accessible password management.

TIP #6

Install and Update Antivirus Software

One of the top methods hackers use to conduct computer attacks stems from malicious software – malware. There are millions of new malware pieces created every year. Malware can be transmitted to your computer from file downloads, email attachments, USB thumb drives and other removable media. To make matters worse, malware is often disguised as something safe or even helpful like antivirus software.

How Can You Protect Yourself?

Install antivirus software. Make sure to use a product that can address all types of malware. Without appropriate anti-malware software, you're leaving your system vulnerable to a very common and prevalent attack vector. Attackers often use malware to gain access to a system, capture key strokes or utilize the system as part of a botnet.

Choose a reputable antivirus manufacturer, such as McAfee, Sophos, Symantec, AVG or eSet. With these products, you get what you pay for. With each new iteration of malware around the corner, you need a team of dedicated professionals to keep your software effective, and making a paid subscription is well worth it. Next, use that subscription and keep the software and the virus definitions/signatures up to date. Use auto-update options within the software to check at least daily for updates to both of these items – vendors often release hundreds of new definitions/signatures throughout a given day. If a new piece of malware is on the rampage, timing will be everything so make sure to stay diligent!

Remember These Important Takeaways:

Run a full scan on your USB thumb drives (or other removable media) every time you use them. You'll likely see the option to run a scan if you right-click on the drive letter in your browser window. Make sure this is the first thing you do after connecting the USB to your system. Keep in mind that USB devices and other portable media can carry all sorts of malware – before you plug it in, make sure you know where it came from.

This also holds true for email – you should scan all email attachments before you open them. Even though antivirus software may filter your emails before they are delivered to you, take the extra step to scan them again. You may see this option by right-clicking on the attachment, or some antivirus programs will run a scan as soon as you attempt to open it. There's no harm in taking the extra step.

So which antivirus software should you use? Visit the **AV-Comparatives website** or **AV-Test.org** – this site runs many different types of tests against various AV vendors' software and on different types of platforms. Check it out and see what software could work for you!

PRO Tip

Install quality antivirus/anti-malware software, and automatically update the software and definitions as often as they will allow. Like a second opinion from a doctor, you can also perform an online scan of your computer, phone or other mobile device. Look for online scanners from the vendors listed in this article or other trusted vendors (listed on **AV-Comparatives.org** or **AV-Test.org**).

“The average cost of a malware attack on a company is $2.4 million.[4]”

[4] Accenture, 2017 Cost of Cybercrime Study, p. 9, https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf, accessed November 2018.

WIPFLi LLP

TIP #7

Keep a Pulse on Cyber News

New updates or developments sweep the cyber realm every day – from the latest breach of the week, to the next huge threat that affects seemingly half the population, all the way down to the latest drama with net neutrality. It can be difficult to keep up with, even for those of us who live and breathe in the cyber world. Fortunately, there are a lot of resources available that can give you the important information you need (without subjecting you to the minute details you wouldn't want anyway).

Stay in the Know With These Resources

- **WipfliSecurity Weekly Newsletter – ** At Wipfli, we create and distribute a weekly newsletter that recaps all of the relevant headlines, trends and updates affecting the cyber world. It's an easy way for you to stay up to speed on the latest big news. **Click here** to subscribe – select *WipfliSecurity Weekly* and fill out the form.
- **Social Media – ** Social media networks have become one of the best ways to get real-time news about what's happening in the world, and cyber news is no exception. Follow professionals and businesses that work in cyber on LinkedIn, Twitter or your favorite social platform, and pay attention to what they post – it may apply to you!
- There are a number of other online resources and websites that can be valuable sources of cyber news:
  - **Naked Security by Sophos – ** Provides daily stories and newsletters for all things security and cyber-related.
  - **SANS Institute – ** Offers information repositories, newsletters and more.
  - **The Hacker News – ** Distributes articles on everything in the cyberspace, geared more toward advanced users.

PRO Tip

Pick your favorite newsletter, subscribe and actually *read* it. This exercise will keep you informed and up to date on what's happening in the cyberspace.

TIP #8

Turn Off Your Wi-Fi and Bluetooth Devices

Wi-Fi and Bluetooth wireless technologies can be very useful and are often set up to connect seamlessly to other devices or networks with no input from the user. For instance, your network connection will still work as you move from your home to Starbucks. As you transition from using a headset to taking a call from your car, Bluetooth will keep your phone calls connected. What you may not realize is that these radio protocols are constantly announcing your presence, and they are capturing information about other wireless protocols around you. These protocols operate by looking for "beacons" that match your saved connection profiles. All of this activity is happening constantly and is visible and trackable by anyone who is interested. There are even devices, such as the WiFi Pineapple, that take advantage of these beacons to "trick" your phone into connecting and monitoring your web traffic. In other words, these connections open the door for a cybersecurity breach, which can have major, detrimental consequences.

How Can You Protect Yourself?

Turn off your Wi-Fi and Bluetooth connections if you aren't actually using them. Disable "automatic" connections to your wireless profiles, and only save the profiles you actually need. When these profiles are saved to your device, your Wi-Fi radio is sending out requests for them, essentially advertising which coffee you prefer, the hotels you've stayed at, where you work, airports you've visited and the name of your network at home.

If your mobile device or computer is set for automatic connections, anyone interested could say, "I'm that network," and connect to your device, waiting for your network requests to pass through their hands. And for various smartphone applications, the combination of GPS, Bluetooth and Wi-Fi offers great data sets for companies like Apple and Google to map out where you have been and what is around.

So turn off the radios you aren't actively using to ensure that you are connecting to the appropriate network or device you intended. Doing so will decrease risk, increase privacy and, as an added bonus, improve your battery life, too.

PRO Tip

Turn off Wi-Fi and Bluetooth connections when you leave the house, and only turn them on again when you are planning on using them.

TIP #9

Phishing, Spear Phishing and Whaling ... Oh My!

Phishing is one of the most common attacks against internet users. By way of email, hackers with malicious intent will contact unsuspecting persons, asking them to click a link or download a file. Generally, the end goal is to infect the user's computer with malware or coerce them into submitting important personal information.

"Spear phishing" is a term used to describe a phishing attack that is directed toward a specific individual, usually for the purpose of identity theft or some other compromise. "Whaling" describes a phishing attack specifically targeted at high-profile end users, such as C-level corporate executives, politicians and celebrities. The purpose of this attack could be to gain information that is useful in blackmail, insider trading or simply stealing account credentials.

How Can You Protect Yourself?

Understand that "spam" and "junk" filters DO NOT catch all malicious emails. Second, know what signs to look for in a phishing email. The vast majority of phishing attempts are fairly easy to recognize and avoid. Here are a few aspects of phishing emails that can help you recognize their true nature:

- **Look at the "From" Address.** Make sure you recognize the address. Then, take a second look at the domain name (that's the name after the "@" symbol), and make sure it's spelled correctly. At the office, an internal email from your co-worker would display only his or her name. If it also shows the full email address, that means it came from the outside.
- **Watch for Inconsistencies.** Make sure that the "reply" address matches the "from" address of the sender – otherwise, it may be a spoofed email.
- **Verify the Sender's Identity.** You can do this by using out-of-band communication to contact the claimed sender. In other words, call your brother and make sure he actually sent you that cat video before you click on the link in the email (don't reply to the email and verify the identity – the attacker will just say "yes").
- **Be on Grammar Watch.** Check that the message is well-composed with the grammar and spelling you would expect from the sender, whether it's your boss, your brother or your bank.
- **Look at Links Closely.** If there is a link in the email, does it match the destination? By hovering your mouse over the link (without clicking on it), your email application will show its actual destination. Again, take a second look at the domain. Be sure it is a domain you would expect. Misspelling a domain is a very common tactic (microsft.com versus microsoft.com) used by hackers. At a glance, they may look the same, but one will take you to Microsoft, and the other will take you somewhere you don't want to go.
- **Trust Your Gut!** If something doesn't seem right, it probably isn't. If there is any doubt that an email or call is illegitimate, immediately contact that organization. *Never click the links or act on any information from a suspected phishing email* (including the phone number!).

Unfortunately, email phishing works on unsuspecting people every day. Even outlandish-sounding emails – "Send me $100,000, so I can give you my inheritance!" – work quite frequently. There are much more well-constructed emails that require a close look and keen eye to notice they are malicious. So take that second look and check before you click, download or enter your information.

PRO Tip

Always verify that the sender of an unexpected email is who they claim to be. Call them, text them or walk to their desk. You should never attempt to verify their identity through the email chain or use any other numbers or emails that are provided by the potential phishing email.

TIP #10

If You Aren't Using Data Encryption, You Should Be

All of the information we send and receive across the internet is valuable — but the data on your computer, tablet or smartphone is especially valuable, and you should take steps to protect it. Computers can be configured with full hard-drive encryption. You can also encrypt portable devices as well as their internal, removable storage devices like SD cards.

Cloud storage services like Dropbox, Box and OneDrive hold your files for you, and they are typically encrypted in transit and at rest with the provider. But these services also may have access to the encryption key, which is typically your login password. Consider what would happen if everyone in the world had access to your cloud storage folder. Would they be able to get into your bank account? Would they know when your house is empty? Encrypting this information before storing it in the cloud will provide a second, self-controller level of safety to help prevent this unwanted exposure in the event of a breach.

How Can You Protect Yourself?

- For your computer, tablet and smartphone, it is important to enable encryption on your storage devices (which is called full-disk encryption, or FDE). For Windows computers, this usually takes the form of BitLocker encryption; for Macs, FileVault 2 supports FDE.
- Enable encryption on your tablet and smartphone devices. For iOS devices, using a password on your device enables encryption by default. **Enabling encryption on Android devices** is a little more complicated, but the protection is well worth the effort.
- If you need to use a cloud storage service, create a secure container *within* your cloud storage that only you can access. At Wipfli, we recommend using **7-Zip**, which is a free, open-source file encryption and compression software program.
- Follow these steps to create a secure container inside your cloud storage that only you will have access to. If you're interested in learning more, many cybersecurity blogs and websites offer more detailed descriptions for using 7-Zip to encrypt files:

1. Download, install and launch 7-Zip.
2. On your computer, create a folder that you would like to store encrypted files in.
3. Right-click this folder and select *7-Zip*, then *Add to Archive*.
4. This will bring up a new window. Make the following changes in this window:
   - Change *Archive format:* to *zip*.
   - Enter a password. (**See Tip #5** for recommendations on selecting a password.) *Please note: This password is critical to securing your data and should be at least 20 characters long with letters, numbers and symbols.*
   - Under *Encryption method*, choose *AES-256*.
   - Click *OK* once you are satisfied with your password.
5. Once you have created this encrypted container, you can add files to it by dragging them to the folder and dropping them in. If you are using a service like Dropbox, Box or OneDrive, the changes will be copied to your cloud backup.

PRO Tip

While your encryption key needs to be long and complex, make sure that it's something you can remember. Once they're encrypted, your files will be completely inaccessible without the key. There is no compromise here — that's the point, right?

TIP #11

Keep Your Software and Devices Up to Date

Criminals and hackers are always looking to exploit holes within software to gain access to your computing devices or data. One method they use is looking for vulnerabilities within software code to target their attacks. Once these vulnerabilities are discovered, software providers rewrite or update their code to "patch" the holes so they cannot be exploited. In fact, in 2017, Microsoft released 250 patches for the various Windows operating systems.

Microsoft isn't alone in the battle to find and patch these holes. All software providers are in this cat-and-mouse game of staying ahead of criminals. That's why it is important to update your operating system and installed software regularly.

Your mobile device, in most cases, is just like your computer – you can access all the same information, store critical data and conduct a significant portion of your business from it. Just like your computer, your mobile device can be exposed to vulnerabilities in poorly written software and holes in the operating system the device runs on. The same care and consideration that are used to safely run a computer should be used on mobile devices to keep them secure.

Your mobile operating system and application providers are constantly identifying enhancements and fixes in their software and publishing updates. Applying these updates in a timely fashion removes the identified vulnerabilities and reduces the risk of someone – or something – taking over your device or accessing information that is private or confidential.

How Can You Protect Yourself?

- Know what software you have installed – if you don't, then you won't know what software to keep updated.
- Make it a habit to update your software regularly, turn on the application's auto-update feature or, at the very least, activate a setting that notifies you of available updates.
- Check to see that you have the latest versions available. Older versions of software and operating systems are often dropped from support, so be sure you use a version that is being actively maintained and monitored.
- Most smartphones and tablets have an automatic update feature for apps – make sure you turn this on. If you are doing a major update to your mobile device operating system, it's a good idea to do a backup first.

PRO Tip

If you no longer use an application, then uninstall it! Security hang-ups that arise with an application you *don't* have installed aren't an issue! This also means you'll have fewer applications to update and/or upgrade.

TIP #12

Keep Business and Personal Separate

Like most of us, organizations are creating a strong presence online. Whether it's Facebook, Amazon, eBay or another online service, businesses are leveraging many of the same platforms that individuals use. If you're like most people, you probably tie your accounts to your email for notifications and to make ongoing management easier. When your company is looking into a service you already use, it's all too easy to leverage your personal account for business purposes.

Privacy and risk are two very important issues that arise when personal and business accounts are connected. When it comes to privacy, the demarcation between your individual privacy versus company rights is blurred when accounts are comingled. From a risk standpoint, the amount of useful information for hackers to leverage as part of a targeted attack (against you or the company) can increase dramatically. The fallout from an attack against a personal account that's tied to one at the office can have serious ramifications for your organization.

A third issue that's tied to the first two is connecting with co-workers socially. This creates added personal context for attackers, and it also gives your colleagues and company an invited look into your personal online life. In addition, the personal use of social media, web-based email or other online services can sometimes violate your employer's acceptable use policy, or you may even be subject to monitoring.

How Can You Protect Yourself?

The answer to this problem is simple – but it's the execution that is more difficult. You need to clearly identify which sites, services and applications are for personal use versus business use. At points where the services cross over, establish two separate accounts (e.g., create a second Facebook account for business purposes). This is an absolute must if you are managing or contributing to any online service on behalf of your organization. Think about what would happen if you left your organization or changed positions or duties within it – how would you hand off the account to your successor?

Also, practice caution before you invite all of your co-workers to be your friends online. Consider exactly what information you want to share with them, and what you want to keep private.

In the end, when faced with the temptation to combine personal and business accounts for social, managerial or any other reasons, draw a clear line and keep them separate.

PRO Tip

Keep all of your personal social media accounts private and hidden so that only people you approve may view your profile. We also recommend that you continually review what information is publicly available by checking the privacy settings of the online service you're concerned about. This will help keep your personal life private and information about you out of the wrong hands.

“Damage related to cybercrime is projected to hit $6 trillion annually by 2021.[5]”

[5] Cybersecurity Ventures and Herjavec Group, 2017 Cybercrime Report, p. 3.

TIP #13

Before Going Mobile, Do Your Research

Mobile electronic payment solutions have gained popularity and merchant support over the past few years. Mobile phone apps like Apple Pay, Android Pay, Venmo and Samsung Pay are designed to help you stop carrying around all of your payment and loyalty cards. This convenience is not without its own security concerns; before using these apps, you should get to know the technology.

Understand Card Information Storage

A primary concern is the storage of your payment card information. Visa Checkout and MasterCard Paypass both store actual card information on your phone within the apps. While these apps use "industry-standard encryption," they are not excluded from being cracked in the future, which would put your credit card information at risk. This method is akin to storing your credit card information in an encrypted file on your phone.

There is a way to avoid these inevitable vulnerabilities: Manipulate the payment information when you're in the app. Samsung Pay generates one-time-use payment numbers you can store on your device over time and does not save your actual account information. This helps prevent your credit card information from being stolen and used indefinitely. However, in August 2016, Samsung Pay's "tokenization" method was found to be predictable, which means that if one token credit card number was intercepted, future token credit card numbers could be guessed by hackers and used from a different device. In addition, Samsung Pay is only available on Samsung cell phone models S6 and up.

Android Pay uses a tokenization process that is generated on Google's end, much like Samsung Pay, but it requires additional device security, including a PIN number, a pattern or a password-secured lock screen. Android Pay is available on nearly all Android phones.

Apple Pay has enhanced this tokenization method. At the point of transaction, Apple Pay generates a one-time credit card number on your device's specialized payment chip. This is the only time the app generates a usable credit card number. All transactions need to originate from and be approved by human input from the phone that created the number. Apple Pay is available only on iPhone models 6 and up.

What Is Card Information Communication?

All of the apps above use the same radio technology to communicate payment information: near field communication (NFC). NFC requires the radio chip on your phone to be within two centimeters of a payment terminal's radio chip. This significantly reduces the area for communication interception, but relying solely on proximity is not enough to ensure your credit card information is safe. While compatibility is an advantage for all of your favorite retailers, it means that your credit card information can be intercepted if the attacker has an NFC radio close enough.

Additionally, Samsung Pay has the ability to emulate the magnetic field produced when swiping your credit card, making nearly all credit card readers compatible. In August 2016, Samsung Pay was shown to be vulnerable to this type of attack by a security researcher, who was able to "skim" the magnetic field similar to how a physical magnetic skimmer works. Using the captured token credit card number, he was able to guess and use remaining tokenized credit card numbers from a separate device.

Remember These Important Takeaways:

Generally, all of these mobile electronic payment apps have one flaw in common: When you put all of your credit cards on your phone, you run the risk of compromising all cards when the app is compromised. Overall, Apple Pay appears to be the most secure payment app all-around, but it is only available on the newest Apple devices. Android Pay comes in at a close second for security and has a larger install base with lower barrier to entry, because it is available on almost all Android devices. Ultimately, these are relatively immature platforms with new and unknown attack vectors. Expect to hear more about vulnerabilities in these payment apps as security research and popularity increase. And as always, make sure to keep your apps up to date.

PRO Tip

If you use any of these payment apps, keep a close eye on your accounts. These services are largely secure, but it's always better to find out about a potential breach sooner rather than later.

TIP #14

Prevent (and Respond) to Ransomware Attacks

You're browsing the internet, and all of a sudden, a warning is displayed on your computer. It may tell you that you need to contact technical support at the number provided, or it may inform you that your information is encrypted and you must pay to unlock it. These types of attacks are referred to as "ransomware," and they're one of the most detrimental threats to your personal information. You probably know someone who was affected by the huge ransomware outbreak aptly referred to as **WannaCry**, which took the internet by storm overnight in May 2017.

How Can You Protect Yourself?

To protect against ransomware attacks, it is important to be curious when warnings come across a website you're visiting or your email. Similar to handling phishing attacks, you should reach out to the source directly instead of using the information listed in the alert. Here are some additional tips to incorporate into your regular routine:

- **Back up your important information regularly.** In addition, you should take this information offline upon completion in order to prevent ransomware from making its way to your backups. This should occur on a schedule so you can ensure you have the most recent information backed up.
- **If you don't trust the source, verify it.** If you want to check a link for suspicious behavior, you can use a website like **VirusTotal** to inspect for malicious content. Another recommendation is to use a browser add-on, such as **Web of Trust**, which provides a color-coded ring next to websites to show their potential risk and reputation.
- **Keep your operating system and programs up to date.** Attackers are known to prey on security flaws in older applications that are used on websites, such as Oracle Java. Make sure to disable these if they are not in use, or keep them updated. The WannaCry outbreak is a great example of this because it relied on a flaw in Windows that had been patched weeks prior.

When it comes to ransomware, never give in to the demands of the attacker. Even if your files are unlocked by paying the ransom, the likelihood of you being a victim increases because you've let the attackers know that you are willing to pay. This can lead to future targeted attacks.

PRO Tip

Back up your data (see **Tip #3**)! If you do get infected with ransomware, there is no way to recover your data unless you pay the criminal's ransom, which you should never, EVER do – unless, of course, you have a backup.

TIP #15

Plug the Leak and Bounce Back From a Breach

Over the past few years, it seems that data breaches and leaks have been stealing all the headlines. Every week, there seems to be a new company reporting that it has been hacked, or another government agency that has its deepest, darkest secrets posted on the internet. It's pretty easy for most of us to turn the other way and tune out all the noise from these constant breaches. However, in order to protect yourself and your information, it is important to keep up to date about what is going on in the cybersecurity world. We frequently find that these breaches set trends for future types of attacks and malware. Take the **very recent Vault 7 leaks**, for example – a lot of interesting information was released as part of these documents. But one of the most illuminating details to come from Vault 7 was the root for the success of the WannaCry ransomware attack. The exploit that made it easy for WannaCry to spread throughout the web was outlined, in detail, in the Vault 7 leaks.

How Can You Protect Yourself?

What if your information is compromised in a breach? With all the companies that are falling victim to attacks, there is a good chance your information will be exposed eventually. An easy way to find out if you have been breached is to check the website, **Have I Been Pwned**, periodically. You can even receive a notification if the site finds your information in a breach.

Staying up to speed with this stuff doesn't necessarily mean that you have to go out and read every piece of leaked information yourself. There are plenty of great news sources you can use to help sum up a breach and give you some insight into what the key takeaways are. Watch for information about leaks on your favorite news site, or you can read about most of them on WikiLeaks. Wipfli also publishes a weekly security newsletter that contains summaries and links to articles about high-profile breaches. You can sign up by visiting **wipfli.com/subscription** and clicking on WipfliSecurity Weekly.

PRO Tip

Go straight to the source – many sites with articles or reports may have biases or a different interpretation of what occurred.

TIP #16

Secure Your Home Network

If you work in an office environment, you are probably familiar with the notion of a firewall. At home, your router likely provides firewall protection, acting as the "security guard" that only allows the good content to enter — and keeps threats out. If you're like most people, you don't just access your home and work networks. Laptops enable us to use networks at coffee shops, airports, libraries, hotels and other public places, where we don't know what protections are being used, who is on those networks and what they can see and access.

How Can You Protect Yourself?

- You don't need to lug around a special device. Instead, you can use what is known as a "personal firewall." Oftentimes, this functionality is included with your antivirus software or your operating system. Make sure it is turned on and active!
- There are clear advantages to using a firewall that is bundled with your antivirus software. When the two work together, they can detect more behaviors and better know what to block and what to trust. You should only install personal firewalls on your personal computers at home.

What About Other Devices?

While a personal firewall is excellent at protecting the computer it is installed on, it doesn't offer protection for all the other devices on your network. If you have Wi-Fi on your home network, you likely have a firewall built in, which will safeguard your "smart" or otherwise network-enabled devices with at least one layer of protection from the Internet. This hardware firewall acts as a physical barrier that will shield your home network from unwanted and possibly malicious traffic.

The Final Takeaway

Make sure your home router has a firewall built into it. Most do, but if your router was provided by your internet service provider, ultimate control of your home network still rests with them. A router can be purchased at most retail stores for under $50, and it will allow you to take ownership of your security.

PRO Tip

Many routers on the market also include functionality for parental controls and website filtering, which can be helpful in protecting your children from inappropriate content online.

TIP #17

Communicate With Caution in the Digital Space

In today's digitally driven world, it has never been easier to shop, apply for loans, transfer money or even set up doctor appointments. We transmit all sorts of financial and personal information across the internet — and this information needs to be protected as it zigzags across cyberspace. Most of us use the web browsers on our phone or computer to interact with the internet. The easiest way to make sure the website you are using is secure is to look for the padlock icon next to the address bar (pictured below). This icon may differ slightly depending on your browser, but if you see a closed lock with no red flags or warning, then the site is secure.

The padlock indicates that the website is using SSL/TLS, which just means that it is encrypted. If you don't see the padlock, that means the website is not secure, and you're putting your data at risk by visiting it.

Email is another major communication tool many of us use every day. For the most part, we send email in clear text (i.e., information is sent as-is, rendering it readable without a keyword of some sort), store it on a server and then send it when the recipient is next available. Some security features are available for many web mail clients, but none are guaranteed to be secure because there is nothing forcing the recipient to abide by the request to send or receive the information securely. To make a long story short, it is definitely not a good idea to send sensitive data through your Gmail (or any other) email account.

Text messaging and phone calls are usually protected by the communication network protocol and providers themselves. The prevalent cell network protocols — GSM (Global System for Mobile Communications) and CDMA (Code-Division Multiple Access) — have been cracked in recent years, so you shouldn't assume they're secure. The network protocol is designed to encrypt communications to avoid easy eavesdropping using radio scanners.

The past couple of years have seen a surge in the use of third-party secure chat programs. Be wary of these apps because while many of them claim to be secure, some do not follow good practices. Do your research before using these apps for your sensitive communications.

How Can You Protect Yourself?

- Check your web browser for a padlock icon next to the URL in the browser. Most modern browsers provide a padlock icon when there is a valid certificate and a website is using an encrypted protocol. Before you enter personal information — even a password to log in — look for the confirmation that encryption is in use. If you do not see the padlock on a site you're visiting, or there are errors in the address bar where you would normally see the padlock, do *not* enter any sensitive information into it.
- Do *not* send or store sensitive information via email unless you know it is secure. If you need to send emails or files securely over the internet, you should use a secure encrypted file-sharing tool or an email service such as Sharefile or Zixmail.
- Use an app, such as Signal for Android or Signal for iOS, for secure chat and phone calls.

PRO Tip

Many routers on the market also include functionality for parental controls and website filtering, which can be helpful in protecting your children from inappropriate content online.

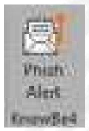
TIP #18

If You See Something, Say Something!

Have you ever received an obvious phishing email or sketchy phone call, ignored it and moved on with your day? If so, you are not alone. That time, the message may have been benign or a one-off — but how many people received that same email or call? How many people clicked on the link in the email or gave the caller information? We can all play a part in maintaining a safer world. You can help reduce response time or prevent an attack from happening altogether just by saying something or reporting suspicious activity.

How Can You Protect Yourself?

If something seems weird or out of place in an email you receive, say something. Be vigilant. For example, if you receive an email that asks you to download a patch or new software, notify someone in your IT department or your company's security officer. The same goes for physical security. If someone is loitering by a locked door or digging through a dumpster outside of your office, contact your security officer. Whether it's on your computer, the phone or around the office, follow your gut if you see something that isn't right and report suspicious activity.



A useful tool for identifying phishing emails early is the "Phish Alert" button from KnowBe4 (pictured here). This is a simple button you can add to Outlook that allows you to report suspicious emails with the click of a button, immediately alerting IT about suspicious activity. If you are interested, ask Wipfli about how KnowBe4 can help you mitigate phishing through training and awareness.

Don't be afraid to "stop, challenge and authenticate" suspicious activity. Stopping someone from committing a potentially malicious attack can be as simple as saying, "Hi! Can I help you?" The next step is to find out what the person's intentions are. If you don't feel comfortable, ask someone who works at your office for their opinion and perspective. Finally, ensure the person is who they say they are and involve the security officer when appropriate. It's better to engage someone who does belong than to ignore someone who doesn't.

PRO Tip

Better safe than sorry! You are always better off playing it safe and reporting something that doesn't seem right. Trust your gut.

WIPFLi LLP

The Equifax data breach affected 148 million consumers – one of the largest in American history.[6]

[6] Merrit Kennedy, "Equifax Says 2.4 Million More People Were Impacted by Huge 2017 Breach," NPR.org, March 1, 2018, https://www.npr.org/sections/thetwo-way/2018/03/01/589854759/equifax-says-2-4-million-more-people-were-impacted-by-huge-2017-breach, accessed November 2018.

TIP #19

So You've Been Hacked ... Now What?

It finally happened – you were one of the 148 million American citizens who were affected by the 2017 Equifax data breach, or you fell prey to one of the seemingly-endless stream of breaches that happen on a regular basis. Now what?

The 2017 **Identity Fraud Study**, released by Javelin Strategy & Research, found that thieves stole $16 billion from 15.4 million consumers in the United States in 2016, compared with the $15.3 billion stolen from 13.1 million victims a year earlier. In the past six years, identity thieves have stolen over $107 billion from their victims. It's a big business, and there is a good chance that you will become a victim at some point in your life (if you haven't been one already). Responding quickly after you're notified about an incident can limit the damage to your credit and reputation, and help you find a resolution quicker and easier.

How Can You Protect Yourself?

1. **Call the companies where you know fraud occurred.**
   - Call the fraud department – explain that someone stole your identity.
   - Ask them to close or freeze your affected accounts. This will ensure that no one can add new charges unless you agree.
   - Change login credentials, passwords and PINs for your accounts.
   - Many times, if a company is breached, it will offer credit monitoring or other identity theft protection services to consumers – take advantage of these services whenever they are available!
2. **Place a fraud alert and get your credit reports.**
   - To place a fraud alert, contact one of the three largest credit bureaus (the bureau you contact must inform the other two):
     - **Experian.com/fraudalert** – 1.888.397.3742
     - **TransUnion.com/fraud** – 1.800.680.7289
     - **Equifax.com/CreditReportAssistance** – 1.888.766.0008
   - A fraud alert is free and will make it harder for someone to open new accounts in your name.
3. **Report identity theft to the Federal Trade Commission (FTC).**
   - Go to IdentityTheft.gov or call 1.877.438.4338 – include as many details as possible.
   - Based on the information you enter, IdentityTheft.gov will create your Identity Theft Report and recovery plan.
   - Your Identity Theft Report is important because it guarantees you certain rights.
4. **You may choose to file a report with your local police department.**
   - Go to your local police office with:
     - A copy of your FTC Identity Theft Report
     - A government-issued ID with a photo
     - Proof of your address (your mortgage statement, rental agreement or utilities bill)
     - Any other proof you have of the theft – bills, Internal Revenue Service (IRS) notices, etc.
   - Tell the police someone stole your identity and you need to file a report.
   - Ask for a copy of the police report; you may need this to complete other steps.

(Excerpted from **IdentityTheft.gov: A Recovery Guide***)*

PRO Tip

Keep an updated list of all your online accounts, credit cards, bank accounts, etc., with contact or customer service phone numbers for each. Early in an identity theft incident, time can be of the essence in heading off further damage that might take additional time to rectify later. Also, consider subscribing to an identity theft and credit monitoring service. There are several good options available for around $10/month.

TIP #20

The Internet of Things: What It Is, and What It Isn't

The Internet of Things (IoT) has been a popular phrase in technology in recent years, but what does it actually mean? In a nut shell, an IoT device can be any physical device that connects to the internet. It might include things like vehicles, thermostats, appliances or even beds. Connecting any of these things to the web has its perks, but it also causes some concern. How secure are IoT devices? Is the risk worth the reward?

How Can You Protect Yourself?

The security of IoT devices is highly debated. The fact is that the market for IoT devices popped up rather quickly and, as a result, many companies rushed products through development, allowing a lot of security issues to slip through the cracks. Developers of IoT devices have matured in recent years, and security is starting to make its way to the forefront of IoT. Even though IoT devices are much safer than they used to be, there are still a lot of vulnerable products out there.

It is important to read reviews and search for any known flaws with devices you are considering using. With any IoT device, you must consider what information is going to be available to it, and whether or not you want that information exposed to the internet and possibly at risk. Ask yourself, "What type of information does this device use or monitor, and where does it send and store that information?" This will help you determine if that IoT device is right for you.

Additional security products have been released to help monitor and manage IoT devices. Products like the Bitdefender Box can help you get a handle on managing these devices securely. However, these products should be used in conjunction with good security practices and caution, as we discussed earlier.

PRO Tip

Not all IoT devices are created equal. It is vital that you research any product you are considering using. Use reliable sources, such as consumer reports, for real-world information about these products.

TIP #21

Is Your Router/Firewall at Risk?

On March 7, 2017, the website WikiLeaks exposed a series of internal CIA documents and software "from an isolated, high-security network situated inside the CIA's Center for Cyber Intelligence in Langley, Virginia."[7] The bulk of this leak was tools that referred to a "hacking arsenal" the CIA developed for cyber intelligence. These tools are now readily available to everyone – bad actors included.

One tool that was released has an impact on home and small business users: "Cherry Blossom." Cherry Blossom is a command and control system that compromises hundreds of vulnerable home and small business routers/firewalls from companies such as Belkin, D-Link, Linksys, Aironet/Cisco, Apple AirPort Express, Allied Telesyn, Ambit, AMIT Inc., Accton, 3Com, Asustek Co., Breezecom, Cameo, Epigram, Gemtek, Global Sun, Hsing Tech, Orinoco, PLANET Technology, RPT Int., Senao, USRobotics and Z-Com.

The tool finds susceptible devices and injects compromised firmware into them, even wirelessly without physical access to the device. The tool allows the attacker to monitor all traffic passing through the device, proxying any and all traffic and allowing access to the internal network and its devices via an attacker-established VPN, essentially bypassing the firewall. Once implanted, the compromised firmware is undetectable by standard antivirus and anti-malware tools.

How Can You Protect Yourself?

- Determine the brand and model of your router/firewall device. **Check it against this list of vulnerable devices**.
- If your device appears on this list, check with the manufacturer for updated firmware that specifically addresses this exploit. If your device is provided by your internet service provider, contact their technical support
- If you own your device and it's several years old, consider upgrading to a newer device that isn't vulnerable to Cherry Blossom. You might gain faster internet and wireless speeds by doing so as well.

For more information about the entire Vault 7 leak, refer to the WikiLeaks website here: **wikileaks.com/ciav7p1/**.

For more information about the Cherry Blossom tool specifically, refer to the WikiLeaks website here: **wikileaks.org/vault7/releases/#Cherry%20Blossom**.

PRO Tip

Whether or not you determine your device is vulnerable to the Cherry Blossom exploit, regularly updating the firmware on your router/firewall is essential to capture security and performance updates incorporated into newer firmware versions by the manufacturer.

[7] "Vault 7: CIA Hacking Tools Revealed," WikiLeaks, https://www.wikileaks.com/ciav7p1/, accessed September 2018.

TIP #22

Keep Your Sensitive Information Behind Closed Doors

Many coffee shops, airports, hotels, printing/shipping companies and libraries have computers and Wi-Fi available for public or guest use. Certainly, these resources can come in handy when your computer battery is dead, you're on a road trip and didn't bring your laptop, or have a bad cell signal.

Whatever the reason, if you find yourself considering using a public computer and/or connection, you may want to think again. Some public computers/networks may not have protections like antivirus software and firewalls. But even more important, you don't know what was installed prior to your session on the computer. There is no lack of opportunity for hackers to install key loggers, remote access or other monitoring tools on public computers. When unsuspecting persons use the computer and login to their email, Facebook account or banking sites, the credentials can be harvested by the hacker without any indication.

How Can You Protect Yourself?

Be careful when using public Wi-Fi; this is an opportunity for man-in-the-middle attacks, whereby your traffic could be captured, snooped, replayed, etc. (even if you use SSL/TLS to connect to the site). Additionally, the wireless network you connect to may not be what you think it is. Some attackers will use a device like the Wi-Fi Pineapple to spoof the names of wireless networks that your device may be looking for.

It is also important to understand what you are agreeing to when you sign up to use a free service or publicly available computer or connection. Almost every service or software you will ever use is accompanied by an end user license agreement (**See Tip #4**).

Avoid using public computers if at all possible. Though some are managed better than others, you just don't know the real state of that particular computer, nor do you know how well it is protected. You may want to think twice about even printing documents. If the document you're printing has sensitive information on it, is a hotel computer or printing/shipping computer the best one to use? Keep in mind that even loading a document on a computer and printing it can leave copies of that document on the computer, the print server and the printer itself. So it's better to be safe than sorry and avoid using public computers altogether.

If you need a network connection, use a VPN to connect back to the office first or back to your home. There are providers that offer VPN services for this exact reason. Use **Private Internet Access** VPN for personal use on PCs, iOS, Android and Kindle. Use your organization's VPN for business purposes.

PRO Tip

Use a VPN whenever possible. If you can't, double check that the website you are visiting is using HTTPS and has a valid certificate (typically indicated by a lock icon next to the URL).

TIP #23

Know Who You Are Talking To

It's easy to lie about who you are on social networks. Whether it's a small omission on a profile or something more nefarious, there is no question that people are generally free to create whatever identity they care to online. That freedom occasionally leads to extreme cases of complete identity creation or manipulation.

There are certainly serial predators online with fake identities waiting to victimize you or your loved ones. It's up to you to do the digging to know who is on the other end of your screen. Are they who they say they are, or someone (or something) else? Do you take the same precautions on the web that you tell your children to take?

How Can You Protect Yourself?

Protecting your personal information also extends to requesting information using email and social media as tools to gain trust. Requests for information, no matter the source, should be carefully scrutinized. Several scams over the past couple of years have come from someone compromising an email account or spoofing information in order to gain trust. While digital communication provides convenience, it does not prove to be more reliable than its predecessor. Like messages that were intercepted by opposing forces during wartime, messages can be intercepted or faked in online communications.

Contact through email and social media gains trust because it appears to be coming from a source you know. The most important way to prevent scams of this type is to adopt the "trust-but-verify" habit when evaluating requests for contact or information. This could be as simple as "out-of-band" communication. Out-of-band communication should consist of contacting the person directly using information you have rather than what is provided in the message. This will allow you to determine whether the request is legitimate. If this is a person who frequently communicates with you, developing a method of authentication, such as a call or code word, that you can send through a separate communication method will allow for more security.

All of these practices are even more important for children, seniors and other potentially vulnerable individuals, who often lack the online savvy to discern the bad from the good.

Remember These Important Takeaways:

- Always think twice!
- Remember that online friends are not the same as real-life friends.
- Never agree to meet someone by yourself if you do not know them.
- Do not give your personal information online. Keep your last name, address and phone number private.
- Profiles can be fake; simply don't trust what someone posts online.
- Understand the potentially dangerous situations that could occur online and in real life, and be certain not to expose yourself to them.
- Be aware of the online activities of potentially vulnerable individuals within your sphere of influence.

PRO Tip

Though they may seem outdated, the telephone and whitepages actually can be valuable trust-but-verify resources to ensure a person's identity is legitimate.

TIP #24

You Must Send Snail Mail Securely, Too

Postal mail can provide a wealth of information for a bad actor that is intent on committing identity theft. Account statements, bills, greeting cards and other physical mail pieces can be the start of a campaign to steal your identity. The United States Postal Service delivers over 493 million pieces of mail every day[9], each of those having the potential to assist in identity theft or other forms of theft or fraud.

How Can You Protect Yourself?

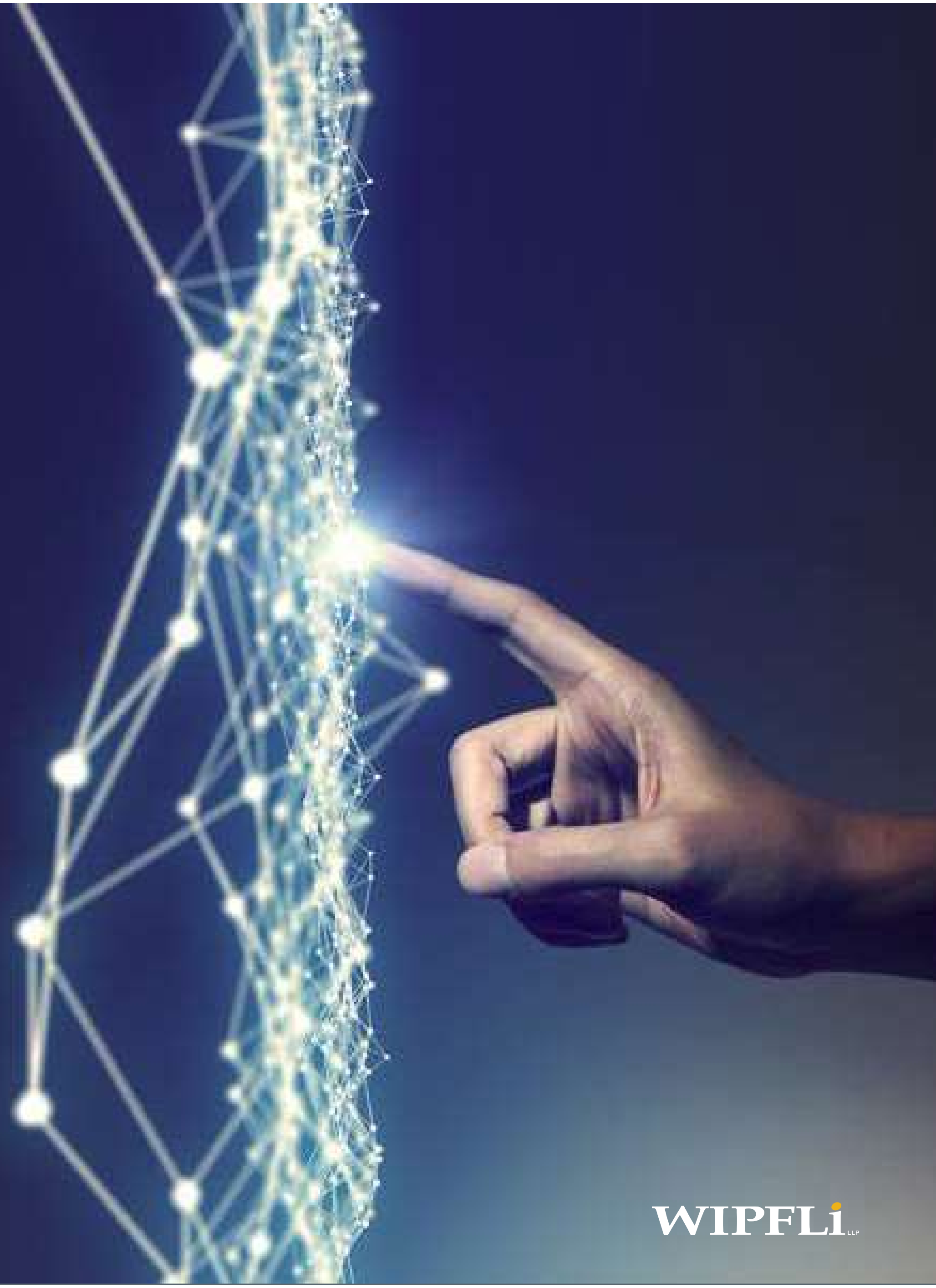
- When sending postal mail, use the letter slots inside your post office or the secure boxes located outside of it, or hand it to a letter carrier.
- Pick up your mail promptly after delivery; don't leave it in your mailbox overnight. If you're expecting checks, credit cards or other negotiable items, ask a trusted friend or neighbor to pick up your mail if you're unable to do so promptly.
- If you don't receive a check, statement, bill or other mail that might contain personal information that you're expecting, contact the issuing agency immediately.
- If you change your address, immediately notify your post office and anyone with whom you do business via the mail.
- If you're going out of town, notify your post office online or in person so they can hold your mail until you return. You can schedule the hold 30 days in advance.
- Report all suspected mail theft to a postal inspector or your local post office.
- Consider starting a neighborhood watch program. By exchanging work and vacation schedules with trusted friends and neighbors, you can watch each other's mailboxes (as well as homes).
- Consult with your local postmaster for the most up-to-date regulations on mailboxes, including the availability of locked centralized or curbside mailboxes.
- Consider installing a USPS-approved locking mailbox to secure your incoming mail or obtain a post office box for secure delivery.
- If your zip code is eligible, sign up for **USPS Informed Delivery** which will send images of most incoming mail to your email address. This allows you to see when important mail is soon to be delivered.
- NOTE: Due to the way the USPS authenticates requests to sign up for Informed Delivery, EVERY adult at your address should sign up for a USPS account and Informed Delivery.

PRO Tip

Never put outgoing mail in your unsecure mailbox with the "flag" up. This is a sure sign that there might be privileged information in there – checks to pay bills, bills themselves, greeting or birthday cards with checks, or gift cards. Always drop outgoing mail at your local post office, even if you have a locking mailbox.

[8] United States Postal Service, "One Day in the Life of the U.S. Postal Service," 2018, https://facts.usps.com/one-day/, accessed November 2018.

86% of American companies plan to increase cybersecurity spending in 2018.[9]



[9] Thales, 2018 Data Threat Report – Global Edition, p. 6, http://go.thalesesecurity.com/rs/480-LWA-970/images/2018-Data-Threat-Report-Global-Edition-ar.pdf, accessed November 2018.

TIP #25

Secure Your Wi-Fi Network

Your Wi-Fi password is broadcast over the air every time you turn on your computer. Hackers can trick your computer into resending the password any time it's connected, and they can do it from as close as across the street. When they see the password has been sent, they can go home and let their computer break it. The time it takes to crack your password could be five minutes or five months, depending on its complexity. When the hacker comes back, will the same password still work? Once they're on your network, they'll be able to watch everything you do online or engage attacks against the computers on your network.

By default, many routers or access points have weak or no security enabled for the Wi-Fi connection as well as a weak password for the device's management interface. These need to be changed from their defaults to more secure Wi-Fi settings and longer, more complex passwords. Your network's Wi-Fi connection is a potential entry point for attackers. You should know how to secure it or engage the assistance of someone who does.

How Can You Protect Yourself?

- Familiarize yourself with your device's documentation and know how to access its configuration, usually through a web browser.
- When configuring the settings for the Wi-Fi network, use:
  - A network name that does not identify you or your network personally.
  - A strong Wi-Fi password or passphrase.
  - Use WPA2 encryption at a minimum; do *not* use WEP.
- Change the device's management password to something other than the password/passphrase used for the Wi-Fi network.
- **Refer to Tip #5** to create strong passwords and passphrases.
- Some routers provide a "guest" network that is separate from your personal network. Use this to connect devices that won't need to share information with your computer. This is a great option for cell phones, internet-enabled cameras, etc., in addition to visitors.
- If you're uncomfortable configuring your Wi-Fi device, get help from someone who is knowledgeable.

PRO Tip

Many modern Wi-Fi routers/devices are very powerful and broadcast a signal far outside your space. Some have settings that can "turn down" the power of the radio. If yours does, turn down the power to no more than necessary to provide sufficient signal within your space. This will limit the ability for those outside your space to detect and access your connection.

TIP #26

Know Your Source

Software downloads are a great way to disguise malware. Numerous sites serve as repositories for independent developers and/or open-source software, which makes validating the source of the software and the download difficult. Without knowing where the software or the download originated, you could expose yourself to some very harmful threats.

We download thousands of smartphone applications every day for entertainment or to make our lives easier – but along with the fun and convenience offered by mobile devices comes increased risk for malware. Sure, there's a lot of money to be made by popular apps like Clash of Clans, but it's also lucrative to create malware disguised as legitimate applications that can mislead users into approving permissions that give access to accounts, storage, contacts, network communication, system tools and settings. Some malicious applications are known to mimic banking apps, deceiving users into entering their financial information. Looking ahead, it's only going to get more dangerous as mobile devices become more affordable. Security software companies have already made popular antivirus applications available on various mobile device platforms due to the amount of malicious software that has already been discovered.

How Can You Protect Your Computer?

- Make sure you only download software from the website of the company you know is the correct seller. Also, make sure you see the secure lock symbol next to the URL of the site (see Tip #17). Major vendors that we are all familiar with (e.g., Microsoft, Apple and Google) operate their own websites to distribute or sell their own software – so make sure you use them to download the software you need.
- Open-source projects typically have their own websites where you can safely download the software. First, search for favorable references to the project or developers from sources like industry news and review sites or software publishers you've worked with in the past. There are trustworthy software repository sites for many independent developers and open-source software. Even with trusted repository sites, it's important that you still consider the publisher of the application.

How Can You Protect Your Smartphone?

- Download applications from trusted sources such as the Google Play Store for Android, Apple's App Store for iOS and the Amazon App Store for Kindle.
- For Android users, leave the security settings option for "allow installation of apps from unknown sources" unchecked.
- Read the ratings and reviews for applications you want to download. People love to voice their opinions and frustrations, especially when money is involved.
- View the permissions that an app requires before you download or install it from the app store. This information is available in the download page in the app store, usually toward the bottom!
- Refrain from "rooting" or "jailbreaking" your mobile device, which grants administrative access and allows the installation of anything.

PRO Tip

Avoid downloading anything from "download aggregation" websites such as download.com, softpedia.com, filehippo.com, etc. These third-party websites are notorious for adding undesirable, unwanted software in addition to the software you intend to install.

TIP #27

Be Aware of and Alert to Scams

We have been taught to ignore suspicious requests made over the internet – in other words, anything that involves sending large sums of money to Nigerian princes to help get it out of the country. As our world grows more complex with new technology and more efficient ways of getting things done, scams like these also grow in their complexity. Now, scammers are claiming to represent the Internal Revenue Service (IRS), the technical support team for your office or even distant relatives.

These requests may seem trustworthy because they *appear* to be legitimate on the surface – however, it's important to practice caution. Requests may come through a method other than the telephone; others, such as requests for technical support, would be made by you rather someone else. It's also important to note that the IRS will always make initial contact with you via postal mail – it would never demand payment of a tax bill over the phone or via email.

Check out these real-life examples of scams:

- **Scammers from India target United States residents posing as the IRS (https://www.nytimes.com/2018/07/26/business/how-to-report-phone-scams-nyt.html)**
- **Scammers pose as Microsoft technical support tricking victims into giving them access (https://support.microsoft.com/en-us/help/4013405/windows-protect-from-tech-support-scams)**
- **Scammers target the elderly (http://time.com/money/5269699/2-new-scams-targeting-seniors-are-on-the-rise-heres-what-to-watch-out-for/)**

How Can You Protect Your Computer?

- Determine another method of contact (e.g., cell phone number, alternate email address, etc.,) that is publicly available.
- Check your computer and mobile devices regularly for malware.
- Check for suspicious charges to your credit card. Question charges that do not correspond to products or services you purchased.
- Don't trust caller ID or email addresses. These can be spoofed, so it is important to have another way to verify someone who is communicating with you. Callbacks are appropriate if you have a number for contacting them that was not provided to you by the scammer.
- Be aware of scams that target the elderly and check in with older friends and family regularly.

If you believe that you have been contacted by one of these scammers, or if you have been a victim of these types of scams yourself, report the incident(s) via the **Federal Trade Commission's website** or call 1.877.FTC.HELP. This will allow you to provide information to protect against future attacks on you and others. In the case of a scam involving the IRS, report the incident with the **U.S. Treasury Inspector General for Tax Administration**.

PRO Tip

If you weren't expecting to receive an email or phone call, don't answer it! Never trust the identity of somebody who contacts you when you weren't expecting them. Always turn to another source of verification by contacting someone through their published phone number or mailing address. Remember that caller ID and email addresses can be spoofed and are *not* methods of verification.

TIP #28

Secure Your Mobile Device

Technology advances have allowed mobile devices to work wonders in the palm of your hand. Smartphones and tablets have made it easier to surf the internet, check emails, VPN into work and even shop online from almost anywhere. When you add together all the stored data on mobile devices, including all of their features and abilities, you get an incredibly valuable piece of technology, which is why so many people say they cannot live without them.

Many people wouldn't trust their best friend – let alone a stranger – with using their smartphone. This is why mobile device manufacturers have implemented security controls such as passwords and timeouts. When a smartphone is stolen or left behind – which is becoming more and more common – the odds of getting it back are pretty slim. That, combined with the access capabilities and data stored on the device, explains why most companies consider a stolen or misplaced mobile device a security breach, and implement controls and policies to remotely wipe devices of the wealth of sensitive information they contain.

How Can You Protect Yourself?

- Use strong passphrases (see Tip #5). Refrain from using "pattern" passwords because they are easy to guess. Most mobile device screens have traces of skin oils, making the password pattern visible.

- Set a timeout of no longer than two minutes before a password is required to unlock the device. Better yet, immediately lock the device when you're finished using it. This keeps your device safe from not only thieves but also nosy friends and family members.

- Encrypt your device's SD card. This keeps your data safe even when your device is lost or stolen.

- Back up the data on your device. How many phone numbers could you actually memorize if you needed to recreate your contact list? Backups are especially important in the event your device is ever lost, stolen or wiped.

- Install anti-malware software to protect your mobile device from viruses, key loggers, phishing websites and other malicious activity. Many anti-malware applications also give you the ability to track your device through GPS and, if necessary, wipe the device remotely. Most anti-malware software vendors include many other features as well. Check out AV-Test.org to compare offerings from various vendors to find what works best for you.

PRO Tip

If you use a PIN to secure your device, check your settings – many devices now allow the number pattern on the lock screen to be randomized, preventing skin oils from inadvertently disclosing the numbers in your PIN.

TIP #29

Don’t Fall Prey to Fraud When Traveling Abroad

To avoid being a target for identity theft while traveling internationally (especially at checkpoints or during searches at customs)[10], there are some basic rules of thumb you should follow:

How Can You Protect Yourself?

Whether it’s for ease of travel, keeping your travel on schedule or keeping sensitive data out of a government or your competition’s hands, the best thing you can do is to limit sensitive corporate information, unpublished research, patient health data and personally identifiable data on your devices:

- Do not travel with any data that cannot be recovered, such as your lifetime research endeavors, if your computer is lost or stolen.
- Install full-disk encryption on your laptops and mobile devices. Configure automatic wipe settings for passcode entry failures, and use at least an eight-digit, unique, complex password utilizing non-dictionary words (try to make your passwords longer than eight characters if your device supports it).[11]
- Keep your devices by your side – you should *never* leave your devices in your hotel room.
- If you’re traveling for business or a conference, travel with only the materials needed for a presentation in an encrypted device; otherwise, use your company’s/university’s remote online storage to retrieve the materials via a VPN once you arrive at your destination.
- If you’re traveling for business or a conference, search for or contact your company’s/university’s travel liaison for travel guidelines and tips. Also, consider using a company/university-owned “loaner” cell phone, laptop and/or tablet to limit the loss of both corporate and personal data if the device is lost, stolen or confiscated by officials or thieves.
- Inform banks and credit card companies of your travel plans and pack only essential ID, credit and debit cards. Leave the others in a secure location.
- Update your data protection software, such as operating systems, anti-malware, antivirus, security patches and others prior to departure.
- Use the **U.S. State Department website** to prepare for your trip and familiarize yourself with the country to which you are traveling.[12]
- You have no reasonable expectation of privacy in some countries. Phone calls, electronic communications and even hotel rooms may be monitored as a standard practice. Sensitive or confidential conversations, transactions or data transfers should be kept to a minimum until you return home.[13]

[10] At all national borders, including the U.S. border for U.S. citizens, your rights (including the fourth amendment) are subject to “reasonable” searches, including at international airports. Border agents can take your devices, clone them and take steps to compel you for system passwords and encryption passwords. Identity theft is often a crime of opportunity. Don’t be a vacationer who presents a thief with that opportunity. Your personal information, credit and debit cards, driver’s license, passport and other personal information are the criminal’s target.

[11] Using numbers, symbols and a mix of upper- and lowercase letters in your password makes it harder for someone to guess your password. For example, an eight-character password with numbers, symbols and mixed-case letters is harder to guess because it has 30,000 times as many possible combinations than an eight-character password with only lowercase letters.

[12] Export control laws concerning sensitive equipment, software and technology (including encryption, a/k/a **The Wassenaar Arrangement**) security testing/hacker tools are also forbidden and illegal in some countries. The Electronic Frontier Foundation published an article on the topic titled, “**Digital Privacy at the U.S. Border: Protecting the Data On Your Devices**.”

[13] Be prepared to turn on and off devices and present all removable media for customs officials. You may be asked to decrypt data for inspection at international borders. In some countries, withholding your password is a criminal offense.

TIP #29

Don’t Fall Prey to Fraud When Traveling Abroad (Cont.)

- Be cautious of unsolicited requests and questions about your business, research, personal life or other sensitive information. Avoid speaking about or commenting on the status of research and development that is being conducted by others if you work for a university, research institution or a similar organization. Defer questions to those individuals directly.
- Avoid political conversations or offering political opinions while in foreign countries, whether in person, on the phone or online.
- Turn off geo-tagging in your camera app and on Facebook, Twitter and any other social media and public internet-related sites.
- Use safe ATMs in public areas during daylight. Cover the PIN keypad and cash output as much as possible. Even then, check for anything on the ATM that looks obviously out of place or fake; skimmers and readers can be installed easily, even in public places.
- Use trusted VPN connections as much as possible. If you don’t have a VPN available, use HTTPS connections as much as possible. Use **Private Internet Access** VPN for personal use on PCs, iOS, Android and Kindle. Use your company’s/university’s VPN for business purposes.
- Consider a prepaid local phone. They are cheaper for local calls and have better connectivity. Buying local SIMs, especially PAYG, adds a level of anonymity, which may be good for privacy/security.
- Avoid public kiosk computers for anything that can be personally identifiable or otherwise sensitive or private.
- Do not loan your device to anyone or attach unknown devices such as thumb drives. Thumb drives are notorious for computer infections.
- Report lost or stolen devices as soon as possible to whomever it concerns. Local authorities have a better chance of finding stolen property if you report it as stolen as soon as you know it is missing.[14]

When Your Journey Is Done ...

- Update the passwords on your devices and review them for malware, unauthorized access or other corruption. Do not connect them to a trusted network until you have tested them for malware. If you find that one of your devices is compromised, reformat and rebuild it from trusted sources/media, then restore data from the backups you performed before the trip.
- Let your bank or credit card companies know that you’ve returned, and review your transactions.

PRO Tip

If you use a PIN to secure your device, check your settings – many devices now allow the number pattern on the lock screen to be randomized, preventing skin oils from inadvertently disclosing the numbers in your PIN.

[14] The primary purpose of reporting, though, is for local crime statistics to drive increased policing in the area, making it a safer place for you and anyone visiting in the future.

TIP #30

Make It Multifactor

Think of a door with many different types of locks: If one is good, more are better (as long as they use different keys – see Tip #28). The same should be said of the way we secure access to the digital property we want to protect.

The first level of authentication is your password. A password is something you know, which grants you access to whatever you protect with your password. But sometimes passwords can be stolen, cracked or guessed by hackers. If you want to increase the level of protection on sensitive items such as email, online banking, password managers and any other application, there is a second layer of protection you can add – this is referred to as two-factor or multifactor authentication.

Multifactor authentication allows for many layers of security to protect sensitive information. Think of a safe in your house: You must be able to unlock an entry door, know the location of the safe and then have the key or combination to access the safe. This puts many obstacles in the way of someone who does not have permission to access your safe. A thief would need several different tools to access the safe. Multifactor authentication works in the same fashion by combining more than one type of method or information to access a resource.

The following are examples of types of authentication methods you can apply:

- **Something You Know:** A picture you remember, a password or a PIN.
- **Something You Have:** An app on your smartphone, a device that you plug in or a token.
- **Something You Are:** Fingerprints, speech or a retinal scan.

The *factor* portion of multifactor authentication is an important piece of this equation. You create unauthorized access to what you want to protect when you take two or more elements (such as something you know and something you have) and require them both to access the information. This is referred to as two-factor authentication. The more you combine elements, the less likely it is that someone will be able to access information without your permission.

Remember These Important Takeaways:

Check for websites that allow multifactor authentication and enable this feature. Many popular websites, such as Amazon, LinkedIn, Facebook, Google and Dropbox, support at least two-factor authentication. Visit TwoFactorAuth.org for a detailed list of websites that support this feature.

More current devices are allowing users to register fingerprints as a "something-you-are" method of authentication. In most cases, this also requires a password that is needed if the device is restarted. Keep in mind that a fingerprint can be combined with a PIN or password for increased security.

Smartphones are at our sides all day long. Many apps can produce a one-time password or PIN to access websites and unlock applications (such as password managers). One of the most popular applications is Authy, which is available from the Apple and Android stores; other, similar types of applications exist in the market as well. Google and Microsoft both have their own apps available. Many websites enable multifactor authentication in their own way. Check with the sites and apps you are enabling two-factor authentication for to see what they support or recommend.

PRO Tip

Enable multifactor authentication on everything – most importantly, your email, social media and financial accounts/websites. Check TwoFactorAuth.org to see which services and sites support multifactor authentication.


WIPFLi LLP
wipfli.com/cybersecurity