30 in 30

TIPS DAYS

Cybersecurity Services

Protect, Detect, Respond and Recover

WIPFLi

CPAs and Consultants

TIP 1:
Download Software Only From Trusted Sources

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 software.

Thousands of smartphone applications are downloaded each 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. Money isn't just made from popular apps like Angry Birds. It is also lucrative to create malware disguised as legitimate applications to mislead users into allowing additional permissions that give access to accounts, storage, contacts, network communication, system tools, and settings. Some malicious applications are known to mimic banks, deceiving users into entering their financial information. Looking ahead, it's only going to get worse as mobile devices become more affordable. Security software companies have already rolled out malware detection applications because of the amount of malicious software already discovered.

What can you do on your computer?

- Major software vendors that we are all familiar with operate their own websites to distribute or sell their own software. Use a major vendor's site to download its software. (e.g., Microsoft®, Apple®, Google®).
- 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 lots of independent developers and open-source software. Even with trusted repository sites, it's important that you still consider the publisher of the application.

What can you do on your smartphone?

- Download applications from trusted sources such as Google Play Store for Android, Apple's App Store for iOS, and Amazon App Store for Kindle.
- For Android users, leave the checkmark unchecked for "allow installation of apps from unknown sources" in the security settings.
- Read the ratings and reviews. People love to voice their opinions and frustrations, especially when money is involved.
- Refrain from "rooting" or "jailbreaking" your mobile device, which grants administrative access and allows the installation of anything.

PRO-TIP: Avoid installing software from "aggregation" sites such as **download.com**, **softpedia.com**, **filehippo.com**, etc. Third-party installers can carry additional payloads in addition to the software you intend to install.

TIP 2:
Don't Mix Business and Personal

Just like individuals, organizations are creating a strong presence online. Whether it is Facebook, Amazon, eBay, or other online service, businesses are leveraging a lot of the same services that individuals use. If you're like most people, you probably tie your accounts to your email for notifications, management, and the like. When your company is in need of one of those online services, 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. For 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 to leverage for a targeted attack (against you or the company) can increase dramatically. The fallout from such an attack against a personal account tied to one at the office can have serious ramifications for your organization.

A third issue tied to the first two is connecting with coworkers socially. Doing so creates added context about you for attackers, and it also gives your colleagues and your company an invited look into your personal online life.

What can you do?

The answer to this problem is simple, but implementation is more difficult. You need to clearly identify those sites, services, and applications that are for personal use versus business use. 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. Also, think about what would happen if you left your organization or changed positions/duties within it. How would you hand off the account to your successor?

When it comes to socially engaging online with coworkers, think carefully before you invite all of your coworkers to be your friends online. Consider exactly what information you want to share with them versus 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. This will help keep your personal life private and information about you out of the wrong hands.

TIP 3:
Secure Your Postal Mail

Postal mail can provide a wealth of information for a bad actor intent on identity theft. Account statements, bills, greeting cards, and other physical mail pieces can be the start of a campaign to steal your identity. The Post Office delivers over 506 million pieces of mail every day, each of those having the potential to assist in identity or other forms of theft.

What can you do?

- Use the letter slots inside your Post Office for your mail, use outdoor secure boxes at your Post Office, 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 don't receive a check or other valuable mail 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.
- Don't send cash in the mail.
- Tell your Post Office when you'll be out of town, so they can hold your mail until you return.
- Report all suspected mail theft to a Postal Inspector.
- 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 **informeddelivery.usps.com/box/pages/intro/start.action** 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.

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 there: checks to pay bills, bills themselves, greeting or birthday cards with checks or gift cards inside. Drop outgoing mail at your local Post Office.

TIP 4:
Turn Off Wi-Fi and Bluetooth

Wi-Fi and Bluetooth wireless technologies are very useful, and they are often set up to connect seamlessly to other devices or networks with no input from the user. As you move from home to Starbucks, your network connection just works, or from a headset to your car, Bluetooth keeps 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 work 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 Wi-Fi Pineapple, that take advantage of the beacons to trick your phone into connecting and monitoring your web traffic.

What can you do?

Turn off your Wi-Fi and Bluetooth if you aren't actually using them. Disable "automatic" connections to your wireless profiles, and save only wireless profiles that you actually need to save. When you have Wi-Fi profiles saved on your device, your Wi-Fi radio is sending out requests for those profiles and essentially advertising what 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, then wait for your network requests to pass through their hands. And for various smartphone applications, the combination of GPS, Bluetooth, and Wi-Fi offer 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 network or device which you expect to. Doing so will decrease risk, increase privacy, and as an added bonus, improve battery life too.

PRO-TIP: Turn off Wi-Fi and Bluetooth when you leave the house, and only turn it on again when you are planning on using it.

TIP 5:
Secure Digital Communications

It's never been easier to shop, apply for loans, transfer money, or set doctor appointments. We transmit all sorts of financial and personal information across the Internet, and it all needs to be protected (encrypted) as it zigzags across cyberspace. Most of these transactions occur within your web browser. When using a Web browser to connect to a website with the prefix HTTP, you are connecting with the possibility that someone can access the information you send to or receive from the website (i.e., your communication with the website is in the clear, "clear text"). When the website is HTTPS, the primary portion of the Web page is secure (although cookies, pictures, and ad space on the website may not be secure). This is called SSL, secure socket layers.

At its most basic, email uses simple mail transfer protocol (SMTP). SMTP is used by Web mail services like Gmail, Yahoo!, and Outlook.com. In most cases, email is sent in clear text (i.e., information is sent as-is, rendering it readable without a key of some sort), stored on a server, then sent when the recipient is next available. For many Web mail clients, some security features are available, 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.

Text messaging is usually protected only by the communication network protocol itself (e.g., GSM providers like AT&T and T-Mobile, CDMA providers like Sprint and Verizon). GSM and CDMA networks have been cracked over the past few years using technology-spoofed cell stations like law enforcement uses routinely in the United States for various purposes. The network protocol is designed to encrypt communications to avoid easy eavesdropping using radio scanners. Much like email, SMS text messages are stored by the provider and forwarded when the recipient is next available.

Cell phone calls are also protected only by the communication network protocol. Cell phone conversations are not usually stored by the network provider (in the United States as far as we know, this varies widely from country to country).

The past couple of years has seen a surge in use of secure chat programs. However, many popular online messaging services tend to lack security controls when using default settings. Like some of the electronic communication methods above, most Internet messaging programs store messages before sending. Internet messaging programs usually transmit the data via HTTPS.

What can you do?

- Check your web browser for a "padlock" icon and the protocol "HTTPS" preceding the URL. Most modern browsers provide a "green" indicator when there is a valid certificate and an encrypted protocol is being used. Before you enter personal information, even a password when logging in, look for the confirmation that encryption is in use.
- Any time there is a problem with the certificate or even the absence of a certificate, your browser should show a warning. If you navigate to a site where the browser has warned you about certificate issues, NEVER enter personal information or passwords; the site cannot be trusted.
- You may want to take steps to ensure your security while browsing the Web. The Electronic Frontier Foundation has released a great add-on for popular Web browsers. HTTPS-Everywhere **eff.org/Https-everywhere** is an extension that will encrypt your communication with most websites by forcing your browser to automatically use HTTPS when navigating to sites.
- Do NOT store sensitive data like passwords in your email.
- Do NOT send sensitive information via email unless it is known to be secure.
- Use clear text email only for communications that you are okay with having a man in the middle of the communication transmission reading your message while it gets sent to your intended recipient.
- Make sure you are using HTTPS when accessing your webmail or any other sensitive information on the Internet. Simply don't use the site for sensitive data access cases if the site doesn't have HTTPS.
- Use an app such as Signal for Android/Signal for iOS for secure chat and phone calls.
- Protect your email account! It is likely the most important Internet username and password you have. All of your other accounts on all of the other sites likely are using your email address for alerts and password resets. If your email account is compromised, not only do attackers have a history of your communication, but they can access your other online accounts! Make your password long and strong, and use two-factor authentication—it's worth it!
- When communicating with your bank, look for a secure messaging login on their website.

PRO-TIP: ALWAYS look for and be aware of the SSL/HTTPS status of any website you're browsing. When clicking on links it's easy to be quietly redirected to a site that does NOT use proper encryption.

TIP 6:
Privacy and Security Abroad

To avoid being a target of opportunity for identity theft, of snoopy nation states, and/or of snoopy economic competition, follow some basic rules of thumb to protect you while abroad.[1]

What can you do?

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 laptops and mobile devices.
- If 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. For ease and security, consider keeping your data only on a company/university server and accessing it only through a secure connection.
- If traveling for business or a conference, consider 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.
- If traveling for business or a conference, search for or contact your company's/university's travel liaison for travel guidelines and tips.
- Perform a full device backup and secure it with a strong password. Store it in a secure location while you are away.
- Inform banks and credit card companies of travel plans including dates, locations, and any special instructions. International transactions are typically flagged as fraud, and purchases may be delayed or your card may be cancelled without advance travel notice.
- Consider using virtual credit card numbers that offer one-time use and are disposable yet will display on your credit card bill.
- Pack only essential ID, credit, and debit cards. Leave the others in a secure location.
- Update data protection software such as operating systems, anti-malware, antivirus, security patches, and others prior to departure.
- Use the U.S. State Department website **State.gov/travel** to prepare for your trip and familiarize yourself with the country you are travelling.[2]
- Configure automatic wipe settings for passcode entry failures, and use at least an eight-digit, unique, non-dictionary word, complex password (longer if supported).[3]
- NEVER let your devices leave your side. This includes NEVER leaving your devices in your hotel room.
- 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.[4]
- Be cautious of unsolicited requests and questions about your business, research, personal life, or other sensitive information. It is advisable to not speak about or comment on the status of research and development being conducted by others at the institution. 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 PIN entry 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 are easily installed, 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.
- Prepaid local phones limit costs by not working after exceeding a maximum number of minutes. 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.
- Public kiosk computers should be avoided for anything that can be personally identifiable or otherwise sensitive or private, like logins, date of birth, credit card, social security number, electronic communication, etc.
- 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. This might include your company, mobile provider, hotel, airline, insurance company, and/or local authorities. Local authorities have a better chance of finding stolen property if it is reported stolen as soon as you know it is missing.[5]

When your journey is done...

- Update device passwords.
- Have all devices, media, and thumb drives reviewed for malware, unauthorized access, or other corruption. Do not connect them to a trusted network until you have tested them for malware. If a device is found to be compromised, reformat it and rebuild it from trusted sources/media, then restore data from backups performed before the trip.
- Inform your bank or credit card companies of your return, and review your transactions.

1 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.

2 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 ***"Defending Privacy at the U.S. Border: A Guide for Travelers Carrying Digital Devices."***

3 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.

4 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.

5 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.

PRO-TIP: Keep a tight grip on your belongings. Valuable, especially cell phones, are common and easy targets for thieves when you are travelling. Make sure you tracking and remote wipe capabilities enabled on your devices.

TIP 7:
Limit What You Share on Social Media Sites

Social media sites are a great way to interact with other users over the Internet. Unfortunately, a large number of social media users don't understand the importance of limiting what's posted on these sites. Attackers regularly use social media sites as reconnaissance tools. 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 name, date of birth, companies worked for, duration of employment, duties performed, experience, schools attended, and much more. Coincidentally, this is all similar information to many security questions banks and other entities use for verification, making it easier to guess or answer these questions. The more information one exposes the easier it is to craft credible attacks. Sites such as LinkedIn allow users to create connections with coworkers, but this also makes it simple to determine a company's organizational chart in a matter of minutes.

All this readily available information provides a potential attacker or bad actor much fodder with which to craft their attack.

Like diamonds, your actions online are forever. The idea that you can completely "delete" or "remove" something is a fallacy. When you post, update, or engage online, there are numerous ways that your content gets backed up, repeated, linked, indexed, and otherwise spread across the Internet. Search engines actively gather content across the Internet and store it on 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, whatever you post, comment, tweet, or share is immediately captured by something you don't control—and can't delete!

Employ what you learned during communications class about the responsibility of the sender and the perspective of the receiver. Quick phrases without context, mixed with emotion, and combined with a lack of nonverbal cues are easily misread. Always think about how you want to be viewed, and don't believe that it doesn't reflect on you away from the keyboard. If it's posted online, it does! Increasingly, potential employers are reviewing a candidate's online presence as part of the hiring process.

Online gaffes are played out online all the time, whether by a politician or a celebrity or even among your friends. Odds are you know someone whose relationship has been affected by something said online. So always take a moment before pressing "enter" and exercise a strict rule about how and when you will engage online. Remember this is ink for the entire world to see, not only immediately, but likely until the end of time.

What can you do?

- Be cautious about what you post because any information can be used to carry out additional attacks.
- Go through all your privacy settings and restrict who is able to view your profiles.
- Connect only 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: Online "friends" are not always real friends. Limit access to private information to only those you personally know away from the keyboard!

TIP 8:
Teach Your Kids to Be Good Online Citizens

The Internet is a wonderful place for kids to learn, play, and discover, but it can also be a dangerous place if not used properly and under supervision. As parents, we must teach our kids how to safely use the Internet and how to be good online citizens.

What can you do?

- Talk to your child about the potential dangers online.
- Spend time online together to teach your kids appropriate online behavior. Pay attention to the sites they use, and show interest in their online communities and friends.
- Explain the implications of their online choices. Information that is shared, including pictures, emails, and videos, can be easily be distributed to others and remain permanently online. Things that could damage their reputation, friendships, or future opportunities should not be shared online.
- Protect your children from cyberbullying by limiting where and what they can post about themselves and family. Teach them how to respond if they witness or are a victim to cyberbullying. Visit **cyberbullying.org** for more information.
- Keep the computer in a common area, not in individual bedrooms, where you can watch and monitor use. This isn't about trust; it is about protection and open communication.
- Be aware of all the ways kids connect to the Internet. Phones, tablets, gaming systems, and even TVs have become connected; teach your kids how to use each of these devices safely.
- Set up a separate account on your computer for your children to use that does not have administrator control if possible. This will prevent software programs, including malicious software/malware, from being downloaded without the administrator password. Do not share this password with your kids.
- Utilize parental controls on all Internet-enabled devices to filter, monitor, and block inappropriate activity. Onguardonline.gov gives an overview of the different types of parental controls. Most Internet service providers (ISP) have tools to help you manage your children's online experience, including blocking inappropriate websites and providing enhanced security features (e.g., pop-up blockers). There is also third-party software available that will allow you to more closely monitor and control children's online activity and notify you when a violation occurs.
- Review the privacy settings on social networks, cell phones, and other social tools your children use and decide together on which settings provide the appropriate amount of protection.
- Stay current with the technology your children use. The online world is constantly changing. It is important to understand the technology your children are using and the potential dangers that may be introduced. Be involved!
- Know who to contact in an emergency.
- If you know of a child in immediate risk or danger, call law enforcement immediately. Report instances of online child exploitation to the National Center for Missing & Exploited Children's cyber tip line. Reports may be made 24 hours a day, 7 days a week at **cybertipline.com** or by calling 1.800.843.5678.

PRO-TIP: The sooner kids understand how to safely and responsibly use the internet the better.

TIP 9:
Beware of Phishing, and Spear Phishing, and Whaling

Phishing is one of the most commonly used attacks against users. By way of email, those 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 get them to submit important personal information.

"Spear phishing" is a term used to describe a phishing attack that is directed towards a specific individual usually for the purpose of identity theft or 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 could be to gain information useful in blackmail, insider trading, or the simple stealing of account credentials.

What can you do?

Understand that "spam" and "junk" filters do not catch all malicious email. 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. Be sure you recognize it. Then take a second look at the domain name (that's the name after the "@" symbol). Make sure it's spelled correctly. At the office, an internal email from your coworker would display only his or her name. If it also shows the full email address, it came from the outside.
- Look for a "reply" address that matches the "from" address.
- 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.
- 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 vs. microsoft.com). At a glance, they look the same, but one will take you to Microsoft, and the other will take you somewhere you don't want to go.
- Does the email ask you for personal information? Most organizations would never ask for personal information in an email or ask you to "reconfirm" your password and account information.
- Trust your gut! If something doesn't seem right, it probably isn't. If you are not sure and are worried there is something urgent that needs your attention, then contact that company/organization as you normally would. Never use the email links or any information from a suspected phishing email (including the phone number!).

Unfortunately email phishing works on unsuspecting people every day. Even emails that seem farfetched ("Send me $100,000 so I can give you my inheritance") work all the time, but those aren't the only emails that get sent. There are often crafty and well-constructed emails that require a close look to notice they are malicious. So take that second look and check before you click, download, or enter your information.

PRO-TIP: The IRS and other government agencies will never contact you or ask for personal information via email.

TIP 10:
Back up Your Data

While it's impossible to predict when your hardware will fail, it's safe to assume that 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. That means three copies of all important files, on two different mediums (hard drives and DVDs, for example), and one copy off site. This can be implemented 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 a, external hard drive. The cloud storage drive will act as your offsite copy. Another great benefit of using a cloud storage drive is that the providers have their own backups and redundancy for their infrastructure.

Encrypt your backups to ensure only you have access to your confidential information. (If using an online service like Google Drive™, Dropbox™, or OneDrive®, ensure that only you have access to your confidential information.)

Backing up your data is also a great way to defend yourself from ransomware attacks, which are attacks that encrypt the files on your computer and require you to make a payment to obtain the private key to decrypt them. If you have your data backed up to an external device or cloud storage, it is easy to simply wipe your hard drive and restore your backed up data to the drive.

PRO-TIP: Keep all of your important files on a cloud 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 to keep track of stuff, and easy to create backups.

TIP 11:
Use Strong Passwords and a Password Manager to Store Them

Passwords are naturally subject to many different attacks. Shared password conventions can increase the likelihood of passwords being guessed. Shorter passwords of dictionary words with few or predictable numbers (e.g., the year) and not using all types of complexity are easily cracked with freely available tools and inexpensive graphics cards. Using the same password for multiple accounts greatly increases the risk of a breach of many accounts after the breach of one.

What can you do?

Avoid your username, the same password with just a different digit, seasons, and other easily guessable aspects to your password. Instead, use a passphrase. A passphrase is a sentence that you can easily remember. The longer your passphrase, the stronger it is. Making your passphrase strong can limit the success of humans and/or computers in guessing your passphrase. Using only simple sentences is becoming less effective with the decreasing cost of consumer graphics cards, which allow up to 10 trillion guesses to be attempted each second. Always use strong, unique passphrases for each separate account secured by a password.

How to make a strong passphrase

We start with a normal phrase that means something only to us so we can remember it. Do not use common quotes from books or other cultural artifacts. Write it down, including spaces.

Super best phrase of pass that only I can remember.

Add capitalization in odd places: *SupEr best pHrase of paSs that Only I caN remember*

Add numbers: *SupEr7best90 pH32rase of paSs th00at Only I c4aN rem9ember*

Add special characters: *(!@#$)(*&%<>?":{}|][,./;'): SupE$r7best90 pH32&rase" of paSs: th00at O,nly I c4aN re;m9ember*

That looks too hard to remember so we'll simplify.

SupE$r best90 paSs:

Finally, we should type it into a window that will not save our work but will allow us to read what we have typed a few times to engage muscle memory. Now that we've typed it a few times, we have an idea of how we'd usually mess up typing the passphrase, which we use as part of our muscle memory when typing out the passphrase. Destroy any written copy of this password-generation process that we started with. We now have a strong passphrase that we can remember.

Once you have created strong and unique passphrases for all your various accounts how will you remember this myriad of information? This is where a "password manager" application helps.

A password manager stores all of the passwords for each of your accounts, allowing you to remember only one strong passphrase used to access the password manager. Some passwords managers also have the ability to generate random passwords for you, then store those random passwords, and recall them on demand. Password managers generally use strong encryption to secure your "database" of passwords.

Here is a non-extensive list of password managers, as of August 29, 2017, from Wikipedia: **en.wikipedia.org/wiki/List_of_password_managers**.

Recently, some hardware-based password storage devices, such as the Mooltipass **themooltipass.com**, have become available and can provide more secure, portable, and easily accessible password management.

PRO-TIP: Create strong, unique passwords for each of your online accounts and secure them with a password manager to reduce the number of passwords that need to be remembered.

TIP 12:
Secure Your Mobile Device

Technology advances have allowed mobile devices to work wonders in the palm of your hand. Mobile devices such as smartphones have made it easier to surf the Internet, check emails, VPN into work, and even shop online from almost anywhere. When you add all the stored data on a mobile device with all of its 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, to use their smartphone. This is why mobile device manufactures 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 the device of the wealth of sensitive information it contains.

What can you do?

- Use strong passphrases (see Tip #11). Refrain from using pattern passwords because they are easy to guess. Most mobile device screens contain skin oils, making the password pattern visible.
- Set a timeout of no longer than two minutes, requiring a password 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 the SD card. This keeps your data safe even when your device is lost or stolen.
- Backup the data on your device. How many phone numbers can you actually memorize if you needed to re-create 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 13:
See Something, Say Something!

Everyone can 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.

What can you do?

If something seems weird about an email or someone seems out of place, 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 security officer. The same goes for physical security. If someone is loitering by a locked door or digging through a dumpster, contact your security officer. Whether it's on your computer or around the office, if you see something that isn't right, say something.

Don't be afraid to "stop, challenge, and authenticate." Stopping someone can be as simple as saying, "Hi! Can I help you?" The next step is to find out if the person should be there or not. If you don't feel comfortable, ask someone who works there what he/she thinks. Finally, ensure the person is who he/she says and involve the security officer when appropriate. It's

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.

TIP 14:
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 the screen. Are they the real thing or something else? How can you trust that they are who they say they are? Do you take the same precautions on the Web that you tell your children to take?

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 a habit of "trust but verify" with requests. This could be as simple as "out of band" communication. Out of band should consist of contacting the person directly using information you have rather than what is provided in the message provided. 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 sent though a separate communication method will allow for more secure communication.

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

What can you do?

- 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; don't trust simply what is posted 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: The telephone and white pages, though seemingly "antiquated," can provide one method of "trust but verify."

TIP 15:
Don't Forward Chain Emails

Email has become a part of daily life for most, but what many people don't know is how easily email can be taken over by hackers. Chain email messages are digital contents that are sent through email networks. A chain message, or chain email, is defined as any message sent to one or more people that asks the recipient to forward it to multiple others and contains some promise of reward for forwarding it or threat of punishment for not. Other chain messages may include a "survey," a list of questions intended for a recipient to answer and send back. This survey may seem harmless and fun, when actually you've just provided answers to most or all of your security questions that a malicious actor can now use to gain access to your accounts. More information about the history of chain letters can be found here **en.wikipedia.org/wiki/Chain_letter**.

Why do people start off a chain email?

- To see how far a letter will go
- To harass another person (include an email address and ask everyone to send mail)
- To damage a person's or organization's reputation
- To trick people into revealing their credentials
- To trick people into sharing answers to common security questions
- To trick people into sending money to the fraudster

What can you do?

- Educate your kids so they recognize messages that are over-the-top or unbelievable.
- Don't worry about messages with scary subjects—for example, "If you don't get this to 10 more people, you will die in two days"; these are hoaxes.
- Delete any chain email messages you receive; do not forward them to anyone.
- If you know the person who sent you the mail, you can respond to the sender with a request to not be included in the future.
- Block or mark as junk email addresses that send unwanted emails.

PRO-TIP: Don't forward anything you didn't write yourself. Anyone asking you to forward their message onto your friends for them they probably have an ulterior motive.

TIP 16:

Secure Your Wi-Fi with the Same Password Rules You Use for Your Computer

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 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 they come back, will the same password still work? Once on your network, they'll be able to watch everything you do online or engage attacks against the computers on your network.

Many routers or access points by default have weak or no security enabled for the Wi-Fi connection and 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. Know how to secure it or engage the assistance of someone who does.

What can you do?

- Review 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 #11** to create strong passwords/passphrases.
- If you're uncomfortable configuring your Wi-Fi device get help from someone 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 17:
Know the End User Agreement

An end user agreement (EUA) is a binding legal document between you and the service provider. This agreement explains your rights and obligations as the user of the product(s), although typically it focuses more on the rights of the provider. The "end user" is either you or your organization. Be cautious of what you are agreeing to. Before you click "agree," you should read the agreement carefully to see whether (1) your personal data is sold to third parties for advertising or telemarketing, (2) your data will become the property of the provider, and (3) you can even delete it. When you agree and use free services provided by Facebook, Google, and countless others, understand that your data is the actual payment for the services rendered; they own it.

What can you do?

When signing up for any service, see how they protect your data and what they can and will do with it. Services that are free and offer "good deals" are usually the ones that are most interested in the data you enter and your usage data. Today it's incredibly difficult to avoid these types of services. Most important, know what your personal data requirements are and the requirements of your company (if for company use) and verify that the service can meet those standards. It takes careful reading and understanding of the EUA to do so, and even services that have fees will limit the control and rights of the user. Everything costs something, and the adage, "You get what you pay for," almost always applies. Read and know your EUAs!

PRO-TIP: It seems obvious, but just read the EUA! You have no idea what they put in those things!

TIP 18:
If You Aren't Using Data Encryption, You Should

All of the information we send and receive across the Internet is valuable. The data on your computer, tablet, or smartphone is certainly valuable, and you should take steps to protect it. Computers can be configured with full hard drive encryption. Portable devices can usually be encrypted as well as their internal, removable storage devices like SD cards.

Cloud storage services like Dropbox, Box, and OneDrive are holding your files for you and they are typically encrypted in transit and at rest at the provider. But these services also potentially have access to the encryption key, 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 information disclosure in the event of a breach.

What can you do?

- For your computer, tablet, and smartphone, it is important to enable encryption on your storage devices (FDE, or full disk encryption). For Windows computers this can be enabling BitLocker encryption. For Macs FileVault 2 supports FDE.
- For your tablet and smartphone, enable encryption on the device. For iOS, using a password on your device enables encryption by default. Android is a little more complicated but 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. Wipfli recommends 7-Zip **7-zip.org**. It's 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. Detailed instructions with examples can be seen at **northeastern.edu/securenu/sensitive-information-2/how-to-use-7-zip-to-encrypt-files-and-folders/**.
  - Download, install, and launch 7-Zip.
  - On your computer, create a folder that you would like to store encrypted files in.
  - Right-click this folder and select 7-zip, then Add to Archive.
  - This will bring up a new window. Make the following changes in this window:
  - Change Archive format: to "zip"
  - Enter a password. (See **Tip #11** 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.
  - Once you have created this encrypted container, you can add files to it by dragging them to the file 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 be SURE that it's something you can remember. Once encrypted your files will be completely inaccessible without the key. There is no compromise here. That's the point right?

TIP 19:
Don't Use Public ANYTHING for Sensitive Information

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

Whatever the reason, if you find yourself thinking about using a public computer and/or connections, 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 to install key loggers, remote access, or other monitoring tools on public computers, so when unsuspecting persons use the computer and log in to their email, Facebook, or banking sites, the credentials are harvested without any indication. 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 (see Tip #4).

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 #17).

What can you do?

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 has sensitive information, is the 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!

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. Don't forget to vet the VPN provider, and know how it works and what they promise to do or not do.

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

TIP 20:
Ransomware Prevention and Response

You're browsing the Internet, and all of a sudden a warning is displayed. 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 direct you to pay to unlock it. These types of threats, referred to as ransomware, are one of the increasing threats to personal information. We all probably know someone who was recently affected by the huge ransomware outbreak this year, aptly referred to as WannaCry, which quite effectively took the internet by storm overnight in May 2017.

What can you do?

To protect against ransomware attacks, it is important to be curious when warnings come across a website or 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 make part of your regular routine:

- Back up your important information regularly. In addition, this information should be taken offline upon completion in order to prevent ransomware 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 potentially suspicious behavior, you can use a website like virustotal.com to check for potential malicious content. Another recommendation is to use a browser add-on, such as Web of Trust (mywot.com), 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, such as Oracle Java, that are used on websites. Make sure to disable these if they are not in use, or keep them updated. The WannaCry outbreak is a great example of needing to keep up-to-date 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 have let the attackers know that you are willing to pay. This can lead to future targeted attacks.

PRO-TIP: Backup your data (**see Tip #10**)! 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 had a backup.

TIP 21:
Install and Update Antivirus Software

One of the top methods of computer attacks comes from malicious software (malware), to the extent that there are tens of millions of new pieces of malware each year. Malware can be transmitted to a 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.

What can you do?

Install antivirus software. Use a product that is going to address all types of malware. A lack of anti-malware software leaves the 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[6] (e.g., McAfee, Sophos, Symantec, AVG, eSet). With these products, you get what you pay for. With each new iteration of malware just around the corner, you need a team of dedicated professionals to keep the software effective 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. Some days, vendors release hundreds of new definitions/signatures throughout a given day. Timing is everything if a new piece of malware is on the rampage!

Any time you use USB thumb drives (or other removable media), run a full scan on it. Often you will have such an option if you right-click on the drive letter in your explorer window. Be sure this is the first thing you do after connecting it to your system. Keep in mind that portable media like USB devices can carry all sorts of malware, so make sure, even before plugging it in, that you know where it came from.

This also holds true for email. All email attachments should be scanned before they are opened. Even though antivirus software may filter your email before it gets delivered to you, take the extra step to scan again. You may have this option by right-clicking on the attachment, or some antivirus programs will scan as soon as you attempt to open them. Know how your version works. Either way, give it another scan.

"Which antivirus software should I use?" Want to know who the best is? Visit **av-comparatives.org** or **av-test.org/en**. They run many different types of tests against various AV vendors' software and on different types of platforms. Check it out and see what could work for you!

6 Recently the FBI has opened an investigation of Kaspersky Labs and is recommending both government agencies and private companies discontinue use of Kaspersky software: **engadget.com/2017/08/21/fbi-kaspersky-lab-private-sector/**

PRO-TIP: Install quality anti-virus/anti-malware software and automatically update the software and definitions as often as the software will allow.

TIP 22:
Use Multifactor Authentication Wherever Possible

Many doors have many locks. Think of the door with many different types of locks. If one is good, more is better. The same should be said of the keys that we apply to the digital things we want to protect. The first level of authentication, providing that you have the right to access a file such as a tax return, picture, or document, 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 taken or guessed. 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 multifactor authentication.

Multifactor authentication allows many layers of security to protect sensitive information. Think of a safe in your house. You have to be able to unlock the door, know the location of the safe, 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. And it combines different things that are needed to access the safe. Multifactor authentication works in the same fashion by combining the many different types of information that are needed 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, a PIN
- Something you have: An app on your smartphone, a device that you plug in, a token, etc.
- Something you are: Fingerprints, speech, retina, etc.

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 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.

What can you do?

Check for websites that allow multifactor authentication, and enable this feature. A good amount of popular websites such as LinkedIn, Facebook, Google, Dropbox, and many more support at least two-factor authentication. Visit **twofactorauth.org** for more information and 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.

In our current living environment, smartphones are at our side all day. Many applications 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; others exist. Google and Microsoft both have their own apps available. Check with the sites and apps you are enabling two-factor authentication on to see what they support or recommend.

PRO-TIP: Enable 2FA on EVERYTHING!
Especially your email and social media accounts.
Check **twofactorauth.org** to see which services support it.

TIP 23:
Protection at Home

At the office, you are probably familiar with the notion of a firewall. At home, your router likely provides firewall protection, acting as the "security guard," allowing only the good in and out. If you're like many people you don't access just your home and work networks. Laptops enable us to use networks at coffee shops, airports, libraries, hotels, and other places were you don't know what protections are being used or who is on those networks and what they can see and access on your laptop.

What can you do?

- You don't need to lug around a special device. Instead you can use what is known as a "personal firewall." Often this functionality is included with your anti-virus software or your operating system. Make sure it is 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. Personal firewalls should be installed on personal computers at home.

What about your other devices?

While a personal firewall on your computer is excellent at protecting the computer it is installed on, it doesn't offer protection for all other devices on your network. If you have Wi-Fi on your home network, you likely have a firewall built in, which will protect your other "smart" or otherwise network-enabled devices to be covered by 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.

What can you do?

Make sure your router at home has a firewall built into it. Most do, but if your router was provided by your ISP, 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 you can buy also include functionality for parental controls and website filtering that can be helpful in protecting your children from inappropriate content online.

TIP 24:
Be Aware of and Alert to Scams

In the past we have been conditioned to ignore requests that involve sending money to a foreign diplomat in order to receive a large inheritance from a relative we never knew (because they never really existed). As our world becomes more complex with new technology and more efficient ways of getting things done, so do scams like these. Now the scammers are saying they represent the IRS, technical support, or even distant relatives.

While most of these requests are trusted because they appear legitimate on the surface, it is important to make sure of this. Most often these requests would be made to you by a method other than the telephone. Some of these requests, such as requests for technical support, would be made by you rather than others.

Recent Examples

- Scammers from India target Unites States residents posing as the IRS **forbes.com/sites/kellyphillipserb/2017/04/10/police-arrest-millennial-behind-multi-million-dollar-irs-phone-scam/#299b0b986ffc**.
- Scammers pose as Microsoft technical support tricking victims into giving them access **microsoft.com/en-us/wdsi/threats/support-scams**.

What can you do?

- Establish another method of contact (cell phone number, alternate email address, etc.,) that is not 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. Callbacks are appropriate if you have a number for contacting them that was not provided to you from the scammer.

If you believe that you have been contacted by one of these scammers, or if you have been a victim of this type of scam, reporting it to agencies such as the FTC **ftccomplaintassistant.gov** or calling 1.877.FTC.HELP will allow you to provide information to protect against future attacks on you and others.

PRO-TIP: If you weren't expecting to receive something, like an email or call, don't answer it! Never trust the identity of somebody contacting you when you weren't expecting them. Always turn to another source of verification by contacting someone through their public phone number or mailing address.

TIP 25:
What to do if you're HACKED!

It's happened. However you manage to find out: fraudulent credit card charges, bill collector calls, loss of access to online accounts… someone has hacked you or you're the victim of identity theft.

WHAT NOW?!

The 2017 **Identity Fraud Study**, released by Javelin Strategy & Research, found that $16 billion was stolen from 15.4 million U.S. consumers in 2016, compared with $15.3 billion and 13.1 million victims a year earlier. In the past six years identity thieves have stolen over $107 billion. Identity theft is big business and you could be next.

A swift response after the incident has been identified can limit damage to your credit and reputation AND make resolution quicker and easier.

What can you do?

(Excerpted from IdentityTheft.gov A Recovery Guide)

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 the accounts. Then, no one can add new charges unless you agree.
   - Change logins, passwords, and PINs for your accounts.

You might have to contact these companies again after you have an Identity Theft Report.

2. **Place a fraud alert and get your credit reports.**
   - To place a fraud alert, contact one of the three credit bureaus. That company must tell the other two.
     - **Experian.com/fraudalert** or call 1-888-397-3742
     - **TransUnion.com/fraud** or call 1-800-680-7289
     - **Equifax.com/CreditReportAssistance** or call 1-888-766-0008
   - A fraud alert is free. It will make it harder for someone to open new accounts in your name.
   - You'll get a letter from each credit bureau. It will confirm that they placed a fraud alert on your file. Get your free credit reports from Equifax, Experian, and TransUnion. Go to annualcreditreport.com or call 1-877-322-8228.
   - Did you already order your free annual reports this year? If so, you can pay to get your report immediately. Or follow the instructions in the fraud alert confirmation letter from each credit bureau to get a free report. That might take longer.
   - Review your reports. Make note of any account or transaction you don't recognize. This will help you report the theft to the Federal Trade Commission (FTC) and the police.

3. Report identity theft to the 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. If you create an account, we'll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.
- If you don't create an account, you must print and save your Identity Theft Report and recovery plan right away. Once you leave the page, you won't be able to access or update them.
- 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 (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.

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.

TIP 26:
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. 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 software code to "patch" the holes so they cannot be exploited. In fact, in 2016 Microsoft released 155 security bulletins about patch vulnerabilities discovered in its software.

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 the criminals. That is 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.

What can you do?

- Know what software you have installed. Take care to keep your Web browsers up to date. These days, many auto-update. Make sure Java is set to automatically update as well, and follow through with update notifications from it (since it usually requires user interaction to update).
- Check to see that you have the latest version; software and operating systems are dropped from support, so be sure you use a version that is being actively supported.
- Check for new security patches and updates on a regular basis; the more frequent, the better.
- Most smartphones and tablets have an automatic update feature for apps. Make sure it's turned on. If you are doing a major update to your operating system, it's a good idea to do a backup first.
- Whenever possible, use automatic update features, and make sure you turn them on!

PRO-TIP: If your employer manages your mobile device, you may need to consult with your IT department regarding the policy for updating your device's OS and applications.

TIP 27:
Mobile Electronic Payments

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.

Card Information Storage

The 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," the apps and the encryption used are not excluded from being cracked in the future, and this would allow your credit card information to be used anywhere else. 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 in the app. Samsung Pay generates one-time-use payment numbers to be stored on the device over time and does not save the actual account information. This helps limit your credit card information from being stolen and used indefinitely. In August 2016, Samsung Pay's "tokenization" method was found to be predictable, though, which means that if one token credit card number was intercepted, future token credit card numbers could be guessed and used from a different device. In addition, Samsung Pay is available only on Samsung cell phone models S6 and up.

Android Pay uses a tokenization process generated on Google's end, like Samsung Pay does, but requires additional device security, which requires a pin, pattern, or 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 the one-time credit card number on the device's specialized payment chip. This is the only time a usable credit card number is generated. 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.

Card Information Communication

All of the apps above use the same radio technology to communicate the payment information: Near field communication (NFC). NFC requires the radio chip on the phone to be within two centimeters of the 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 your favorite retailers, it means that the credit card information can be intercepted if the attacker has an NFC radio close enough.

Samsung Pay additionally 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 "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.

Thoughts

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 all around, but is available only on the newest Apple devices. Android Pay comes in 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. As always, make sure to keep your apps up to date.

PRO-TIP: Keep a close eye on you accounts if you use any of these services. These services are largely secure, but better to find out sooner than later if there has been a breach.

TIP 28:
Data Breaches and Leaks

In the last 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 they have been hacked, or another government agency is having its deepest darkest secrets posted on the internet. It is pretty easy for most of us to turn the other way and tune out all the noise from the constant breaches. However, it is important to keep up-to-date about what is going on with these breaches. We frequently find that the information revealed this way sets trends for the type of attacks and malware we will see in the following months. Take the very recent Vault 7 leaks for example **en.wikipedia.org/wiki/Vault_7**. There was a lot of interesting information released as a part of these documents. One of the more interesting things 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.

What can you do?

What if your information is compromised in a breach? With all the companies being breached there is a good chance your information will get out here eventually. If you follow the breach, you will know whether or not you have anything to worry about. An easy way to find out if you have been breached is to periodically check **haveibeenpwned.com**. You can even receive a notification of your information is found in a breach.

Keeping up-to-date 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 that will sum it up and give you some insight into what the takeaways are. Just watch for information about leaks on your favorite news site, or go straight to the source for most of them at WikiLeaks.

PRO-TIP: Go straight to the source, many sites with articles or reports may have biases or may have a different interpretation of what occurred.

TIP 29:
The Internet of Things

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. Having any of these things connected to the web has its perks, but it also causes some concern. How secure are IoT devices? Is the risk worth the reward?

What can you do?

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 a lot of early devices were riddled with vulnerabilities and flaws. Now that developers of IoT devices have matured, things have gotten much more secure. Even though IoT devices are much safer than they used to be, there are still a lot of bad products out there. It is important to read reviews and search for any flaws with devices you are considering using. Lastly, you must consider what information or products you might be willing to risk by putting them in the hands of an IoT device. Ask yourself what type of information does this device use/monitor, and where does it send and store that information? This will help you determine if that IoT device is right for you.

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 30:
Parental Controls

Using the parental controls made available to you go a long way in helping you make sure your children stay safe online. The biggest confusion surrounds what exactly you should be using for parental controls. There are so many apps and products out there that claim to make it easy that it can be confusing picking the best options. The best way to answer is that is to ask yourself what kind of control you wish to have. The most common features you want to look for is monitoring of text messages, phone calls, emails, and websites. Some even offer more advanced features, such as disabling their cell phone while they are in a moving car or locking their phone until they respond to a call or text. Ultimately you have the control to choose what apps and activities your child has access to, as well as the ability to monitor everything they do on their devices.

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 across all of your kid's accounts and devices. Other third-parties, such as Norton, offer products that air specially aimed at proving a more seamless experience across various devices.

PRO-TIP: The parental control features built into your devices (Android or iPhone) are usually sufficient in most cases. If you want more control, look at third-party products.

ADDITIONAL RESOURCES

Visit us at **wipfli.com/cybersecurity** to check out our video, learn more about our cybersecurity essentials packages and other resources. Stay connected by signing up for our e-communications or visiting our blog often:

WipfliSecurity Blog

WipfliSecurity brings you timely information that affects your organization's security. Connect with Wipfli's security experts and get up-to-date guidance on the latest threats and fixes. We'll discuss new ideas for improving your organization's security and tips to help you navigate your way through compliance and more.

Visit us at **wipfli.com/SecurityBlog**

WipfliSecurity Weekly e-communication

Every day Wipfli's cybersecurity team scours numerous sources to identify new exploits, vulnerabilities, and patches/updates that may be relevant to our clients. WipfliSecurity Weekly brings you the most important information, in a quick-hitting format, every week. This communication is designed for the technical user and provides links to additional information on each topic.

Sign-up at **wipfli.com/subscription**

WipfliSecurity Insider e-communication

If your days are focused on managing your business, not managing IT security and regulatory governance, then WipfliSecurity Insider is for you! We'll keep you in the know, with cybersecurity thought leadership and articles, without cluttering your inbox. WipfliSecurity Insider is delivered bi-monthly and provides a high-level overview rather than technical detail. But rest assured, we'll cover the issues impacting your business and help you make sure you're asking the right questions about your security risks.

Sign-up at **wipfli.com/subscription**

As always, contact your Wipfli Relationship Executive if we can be of assistance in any way in your cybersecurity efforts.