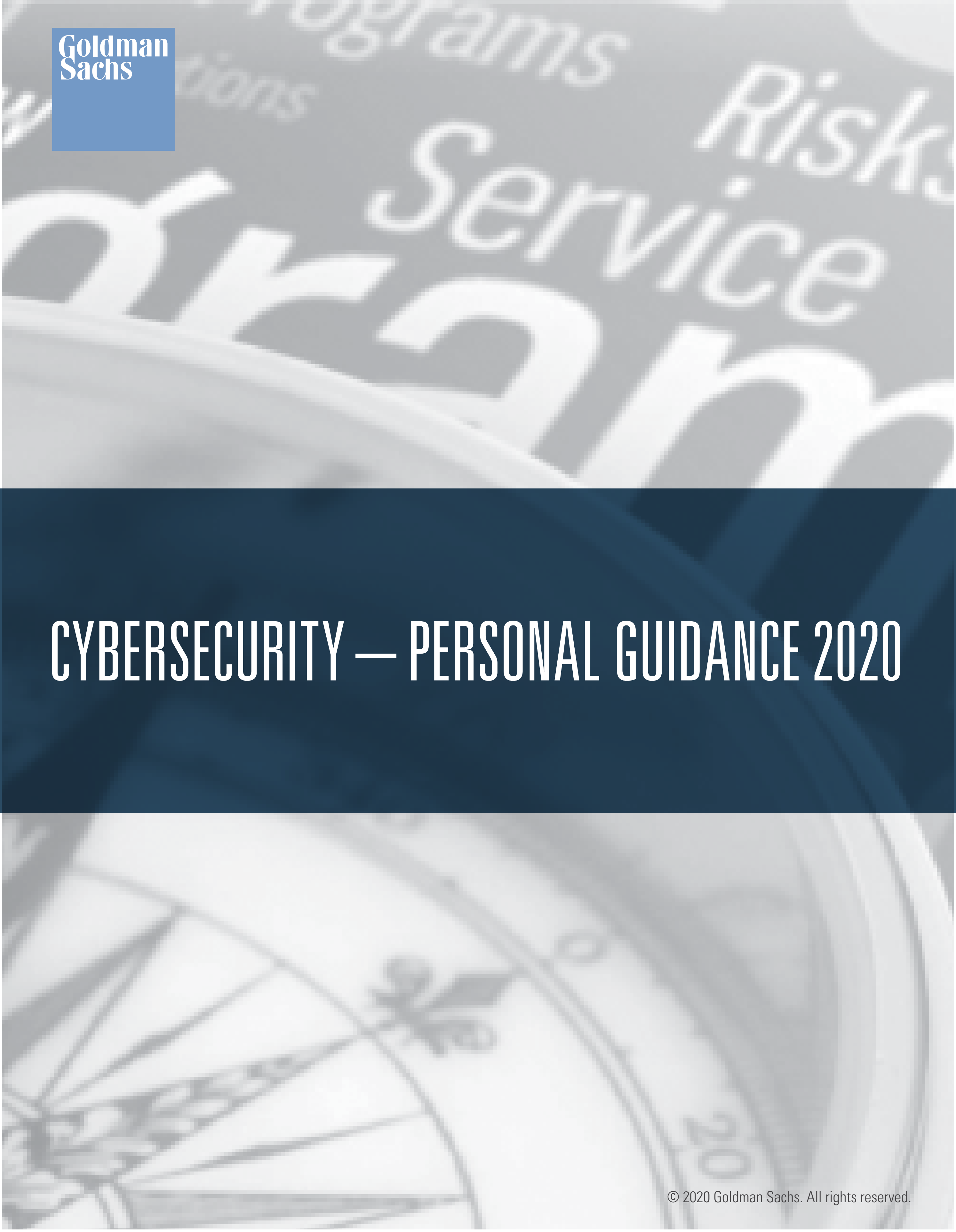


CYBERSECURITY — PERSONAL GUIDANCE 2020

CONTENTS

OBJECTIVE

Improve your personal cybersecurity posture with this guidance offered by Goldman Sachs.

Several types of cyber risks are highlighted in this guidance, along with associated controls to keep you and your family safe. This document is designed to be educational in nature, and aims to share best practices around good cyber hygiene. We encourage you to discuss this guidance with your family and personnel.

The cybersecurity risk landscape is constantly evolving and the security measures needed to respond to those risks will naturally change over time and also vary from one client to another.

As a result, you are strongly advised to stay abreast of ongoing developments in the cybersecurity space, and to consult with your own cybersecurity an technical experts.

The target audience for this guidance is Goldman Sachs clients, employees, and institutional partners looking to improve their personal cyber health.

Goldman Sachs does not represent that this document alone will be sufficient or adequate for your intended purposes.

OVERVIEW: TOP 10 BEST PRACTICES

This Personal Guidance serves as an introduction to common security threat scenarios and outlines best practices for protecting your personal and financial well-being. Before we dive into the details, here are our top 10 recommendations for personal cybersecurity.

1. ESTABLISH SECURE EMAIL PROTOCOLS

Emails continue to be a common entry point for hackers for performing online fraud. Do not click on links or open attachments from suspicious-looking emails.

Expand your communication protocol to verify sensitive information, such as wire instructions, in person or by telephone. Generally, GS will never send wiring instructions via email.

2. EMPLOY PASSWORD MANAGEMENT

Use lengthy, unique, and complex passwords — a great first step toward stopping bad actors. In fact, cybersecurity best practices suggest utilizing long, memorable, and hard-to-guess passwords such as a favorite song lyric. Avoid reusing passwords. Consider using a password application, such as LastPass, 1Password or Dashlane to help manage multiple complex passwords.

3. ENABLE 2-STEP AUTHENTICATION MEASURES

Where available, use 2-factor authentication for account login (2FA) a.k.a. two-step verification or multi-factor authentication, commonly done via a PIN sent over text message or email. At a minimum, enable this capability for your email, cellular provider, financial websites, password manager, cloud file storage and social media.

4. LOCK DOWN SOCIAL MEDIA

Periodically review and adjust social media account settings to better control who can view the content posted. Hackers and social engineers frequently obtain critical information about a target from social media sources. When posting, always consider how that information can be used against you.

5. REDUCE YOUR PUBLIC ONLINE FOOTPRINT

Periodically review all your online accounts. Reduce and/or obfuscate personal information on the internet, remove unnecessary data, delete unused accounts, and avoid sharing or reusing passwords across accounts to minimize exposure.

6. PROTECT CRITICAL DATA

Know where all your sensitive personal information is stored. Ensure that your sensitive data is always stored encrypted, to prevent someone from viewing it if your device gets lost or stolen. Also consider having a second encrypted backup of your sensitive data, whether on a flash drive stored in a safety deposit box or in the cloud using a reputable service such as Dropbox, iCloud, or Google Drive.

7. PROTECT YOUR PERSONAL DEVICES

Configure devices securely, considering what your risks would be if your device were stolen.

Use a difficult to guess passcode as a backup to biometric security such as a thumb print or Face ID, and be sure your device is encrypted. Ensure that sensitive data, such as email, does not display on the lock screen.

8. UPDATE YOUR SOFTWARE

Keep all of your software up to date. Apply software updates as soon as possible once they become available. Consider enabling automatic updates where available.

9. SECURE WI-FI ACCESS

Use Wi-FI safely. Be aware that using public Wi-Fi can expose your communications and devices to risk. If you must use public Wi-Fi, consider a virtual private network (VPN) solution to protect your communications — particularly when traveling and using public Wi-Fi at the airport or hotel. Alternatively, consider using a mobile hotspot, to protect sensitive information. At home, use a guest network for visitors.

10. FREEZE CREDIT LINES

Thwart identity theft and minimize fraud risk with a call to major credit-reporting bureaus Experian, TransUnion and Equifax, as well as Innovis, the unofficial fourth credit bureau to set a security freeze on your credit reports. Considering signing up for an identity theft protection service such as LifeLock, Kroll, or Experian, which also offers credit monitoring. These suggestions apply to all family members.

GOT HACKED: NOW WHAT? TAKE ACTION

EMAIL

MY EMAIL OR ACCOUNT HAS BEEN HACKED

Change your passwords immediately after you have cleaned your computer. Prioritize accounts that have the same password as the compromised account, or a similar one.

Consider setting up two-factor authentication if you haven't already, and if it is offered by your provider.

Immediately stop using the email account for authentication codes or approving financial transactions.

Consider setting up a new email address for sensitive transactions or email exchanges.

Run a full anti-virus and anti-spyware scan on the system(s).

Review your email account settings for new suspicious "forward-to" or "reply-to" addresses. Fraudsters sometimes add these to hide messages they are sending.

I OPENED A MALICIOUS EMAIL

Install or update anti-virus and anti-spyware software and run a full scan on your system; malicious code **(trojan horses, keystroke loggers, etc.)** may have been installed.

Contact your family, bank and financial providers if you believe personal information was disclosed, or you're worried your accounts may have been accessed.

Consider changing your passwords if you have reason to believe that any of your email or other accounts are compromised.

Trojan Horse: A program designed to breach the security of a computer system while ostensibly performing some innocuous function. Trojan horses can infect your devices in a variety of ways and can be included in software downloaded for free or as attachments in email messages. Be very cautious about running unknown software or clicking on links.

Ransomware: A type of malicious software designed to block access to a computer system until a sum of money is paid. Maintaining secure backups offline from your computer is a way to protect yourself; you can recover all your files without having to pay for them!

DATA AND CREDIT

I WAS INVOLVED IN A DATA BREACH

Consider adding a security freeze on your credit reports at Equifax, Experian & TransUnion for you and your family to restrict access and make it more difficult for fraudsters to open new accounts in your name.

Sign up for an identity theft protection service such as LifeLock, Kroll, or Experian, which also offers credit monitoring.

Protect your email and financial websites with strong passwords. Consider using password manager software and setting up two-factor authentication for your email and password manager. Also consider changing very old passwords.

Be aware of data breach-related scams; fraudsters scan headlines! Practice emergency and back-up communication and verification protocols with your family and staff.

MY CREDIT CARD WAS STOLEN

Contact your bank to block or deactivate your credit card.

Remove the card as a payment method from all apps and websites.

Review all recent activity related to the card, including Apple Pay, QR code scanning, and other smartphone payments.

Proactively monitor your credit report; consider adding a security freeze via all three main credit bureaus. Contact your bank and other financial providers to place notices on your accounts.

Sign up for an identity theft protection service such as LifeLock, Kroll, or Experian, which also offers credit monitoring.

Credit Freeze: A method by which a consumer can limit access to his or her credit report to companies with which he or she has a pre-existing credit relationship, such as a mortgage, auto loan and credit card, or a company they wish to enter into a credit relationship with.

IN ANY OF THESE INSTANCES, BE SURE TO NOTIFY YOUR BANKS AND FINANCIAL INSTITUTIONS AND CONFIRM THAT NO OTHER FRAUDULENT ACTIVITY HAS OCCURRED. CHANGE ACCOUNTS/PASSWORDS AND UPDATE ACCOUNT LOGINS AS NECESSARY. CONSIDER CONTRACTING WITH A REPUTABLE IT SUPPORT COMPANY, IF NECESSARY.

PROTECT YOURSELF: BEST PRACTICES

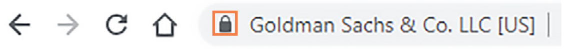
PROTECT YOURSELF WEBSITES: SECURE BROWSING HYGIENE

GUIDANCE

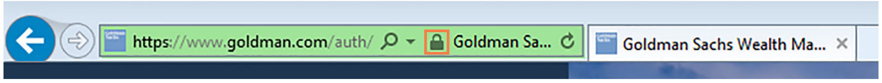
- Be careful what you click. Avoid visiting unknown websites, clicking suspicious links or downloading software from random websites.
- Log off after all online sessions on your computer or your phone.
- To make sure the websites you log into are secure, look to see “https://” and not “http://” in your browser window.
- Consider using a separate, dedicated browser to access sensitive personal or financial data.
- Be aware of third-party persistent cookies or tracking cookies which track your activity to provide a better custom experience.
- Use an ad blocker.
- Consider adjusting web browser settings to block pop-up windows by default.
- Practice safe Wi-Fi usage.

HOW DO I ENSURE CONNECTING TO A LEGITIMATE SITE?

- Only shop online with reputable vendors, and be sure your computer, network (e.g. Wi-Fi), and browser are secure.
- Be cautious with random online deals received via email or social media. If an online deal seems too good to be true, type the subject line or headline of the deal plus the word “scam” into a search engine to learn about any reported issues.
- Look carefully at a website address before you click it. If it seems even slightly unusual or unexpected, steer clear. Phishing campaigns will often create fraudulent websites with very similar website names to trick visitors into believing they are visiting trusted sites.
- When you access a website requiring that you enter a password, check that the web address starts with “HTTPS://” to be assured that data including your password is encrypted when it is transmitted to the site. Check for a padlock icon in the address bar of your browser to help confirm the login page is secure. Watch out for any certificate warnings from the browser.



Goldman Sachs & Co. LLC [US]



https://www.goldman.com/auth/

- Do not visit any sites that are identified by your search engine as possibly harmful to your computer.
- Do not provide unnecessary information. For example, does an online shopping site really need your birthdate?
- Check your bank account and credit card statements regularly for abnormal activity.
- Do not use debit cards for online purchases. Instead, consider reputable online/electronic payment services such as PayPal, Amazon, and Apple Pay when available.
- Complement your travel security with safe Wi-Fi usage. Be aware that using public Wi-Fi can expose your communications and devices to risk. If you must use public Wi-Fi, consider a virtual private network (VPN) solution to protect your communications — particularly when traveling and using public Wi-Fi at the airport or hotel. Alternatively, consider using a mobile hotspot, to protect sensitive information.

PROTECT YOURSELF WEBSITES: PASSWORD SECURITY & TWO-STEP LOGIN

GUIDANCE

- Use complex and lengthy passwords that are at least 8 characters long, using a combination of at least 3 of the 4 character sets (capitals, small letters, numbers and special characters).
- Do not reuse passwords.
- Remember, do NOT use:
  - Common number sequences like "123" or your birthdate
  - Words like "password"
  - Words commonly found in the dictionary
- Examples of strong passwords:
  - alwayz&*M1nD1NGth3*g4P
  - ARUGULa#Pl4idTshirts;wAys
- Consider using a password manager application, like LastPass, 1Password, or Dashlane, to help manage multiple complex passwords.
- Password managers usually also have a feature where you are required to enter the master password before it logs you into certain sites.
- Wherever available, leverage two-factor authentication for account login (2FA, a.k.a. two-step verification or multi-factor authentication, commonly via a unique PIN sent over text message or email). At a minimum, enable this capability for email, social media, mobile phone carrier, cloud file storage, password manager and financial websites.
- There are many two-factor authentication options currently available. In order of most to least secure: Hardware token (YubiKey), Authenticator App (Google Authenticator, Duo, Authy), SMS text, or email).

PASSWORD SECURITY

- Strong passwords you create for social media, email and financial websites should be different for each website, and should not be reused across multiple sites.
- Consider using two-step verification for any site that offers this feature.
  - Many email providers now provide an option for a second sign-in verification beyond passwords during suspicious login attempts (e.g. from a new country or a new device), usually involving a numeric code sent to your mobile phone.
  - Mobile security applications, such as Google Authenticator or Authy, are also increasingly common. They can be used with many websites, including many email and social media sites, as well as most password managers.
- Do not share sensitive passwords with anyone and consider not allowing your browser to store or retain them. If there is a need to share certain passwords (e.g. with your spouse), many password managers have secure ways of setting this up.
- Many people commonly store passwords in their browser, e.g. by linking Chrome to their Google ID, or Safari to their Apple ID. Be cognizant of how your accounts are linked to your browser and your devices.
- Request separate login IDs if others need access to your online banking or investment websites, including separate access IDs for accountants, assistants, or data aggregation software. Access provided by these IDs should be as restricted as possible, ideally read-only.
- Many online sites allow integration of common social media login IDs (like Google, Yahoo, Amazon, or Facebook IDs). There are security and convenience benefits to having a centralized login framework and not having to create individual accounts on each platform. However, be conscious that a compromised social media account that is cross-linked to other sites will allow an attacker to access the linked sites. Social media sites also do behavioral analytics, which can pose a privacy concern.

PASSWORD MANAGERS

- Password management software can help maintain passwords, generate complex passwords, provide import and export tools, and automatically complete online forms for more efficient online checkout.
- Consider making up 'not-factual' answers to easily findable authentication questions like "school attended" or "mother's maiden name" as an added layer of protection. You can store these answers in the notes field of your password manager.
- Adjust settings to require the master password to be entered before the password manager logs you into certain sites, including all financial and personal data sites.

PROTECT YOURSELF WEBSITES: SOCIAL MEDIA & ONLINE FOOTPRINT

GUIDANCE

- Assume anything posted on social media has the potential to be public and can remain online forever. When posting, always consider how that information can be used against you.
- Periodically review and adjust social media account settings to better control who can view each type of content posted, especially geotagging / location tracking features. Malicious actors who may want to target you, or your home, could use this type of data to select a time/date to social engineer you or your friends/colleagues at an event or use the data as a predictive indicator of whether your home is occupied or empty.
- Periodically review and adjust social media settings to better control who can view each type of content posted.
- Limit permissions granted to all third-party applications especially for social media, e.g. quiz apps, gaming apps, etc.
- Periodically review and get a handle on all your online accounts. An individual can have 100+ accounts, and your information could get leaked if any one of these websites gets hacked due to poor security practices. Remove unnecessary data, delete unused accounts, and avoid sharing or reusing passwords to minimize risk exposure.

HOW DO YOU BALANCE SOCIAL MEDIA USAGE & PRIVACY?

- Make sure you are aware of the risks of having a public account on social media. Set your privacy settings to ensure you are comfortable with the personal information being revealed. Anyone can see information on non-private accounts, thus information as simple as "leaving on vacation in a week" could alert robbers that no one will be at home.
- Be aware of what is posted about you through your family and friends. When available, adjust settings so that you are notified and have to approve any posting where you are tagged.
- Be aware of geotagging/location tracking/location tagging features on social media websites, which can indicate your current physical location.
- Strong passwords are especially critical on social networks, where social engineering attempts are common. Enable two-factor authentication for your account login.
- When you set answers to security questions for websites or other services to authenticate yourself for account access, to reset passwords, etc., remember exactly what information those security questions cover, and avoid sharing any of those details on social media. Ensure your responses to the security questions are not easily guessable or searchable.
- Enable notifications for when your account is accessed from a new device.
- Never respond to messages you receive from people or organizations you do not know. Scammers sign up on social media sites as ordinary people, reputable sites, and even charities.
- Be suspicious of anyone asking personal questions on social media if you don't know them. Do not respond to quizzes on social media that ask for personal information.
- Be careful with any social media features that give "permission to third-party applications" to act on behalf of the user, since cybercriminals often impersonate third-party apps.
- Clickbait is content whose main purpose is to attract attention and encourage users to click on a link to a particular page or article. Outrageous claims and "see what happened" headlines typically identify clickbait. These links often attempt to install unwanted apps or even malware on your device.
- Periodically review your old accounts and delete or disable unused accounts.
- Consider using an alias for invitations. When accepting publicly available invitations on social media or online invite websites, use an alias, a nickname or initials. While some of the invitation RSVP sites are protected, many are publicly accessible.

PROTECT YOURSELF WEBSITES: PROTECT YOUR FAMILY ONLINE

GUIDANCE

- Discuss online best practices and safety like any other important family conversation.
- Advise them to apply standards they adopt offline to the online world.
- Educate them early and often on online best practices. These include:
  - An ongoing dialogue on which sites to use and not to use
  - Knowing how and when to vet app downloads
  - Periodically applying software patches
  - Knowing how to choose strong passwords
  - Not accepting friend requests from people you don't know
  - Not agreeing to a private chat with a stranger
  - Being cautious about what you share online, including location, mobile phone numbers and home addresses
  - Reminding them that anything put online could be permanent
- Discuss cyberbullying with your children.
- Discuss and set guidelines and rules for computer use with your children.

HOW DO YOU EDUCATE YOUR KIDS ON INTERNET USAGE?

- Communication is key – be a role model, and teach your children how to safely and responsibly use the computer and the Internet.
- Educate them early and often on safe boundaries and engage in age-appropriate open discussions about your child's online activities.
- Maintain a healthy dialogue with your children about what applications they use and about appropriate online behavior, especially on social media. Use the parental control tools offered by some Internet service providers and available for purchase as separate software packages.
- Keep the computer in a central and open location in your home, and be aware of other computers your child may be using. Use a separate computer for accessing financial websites.
- Do not grant full (or admin) access to your child's account on your home computer. This is a good practice in general for all accounts.
- Many new games and toys contain elements of internet and social media connectivity — be conscious of the risks related to internet connectivity and oversharing.
- If your children have smartphones or tablets, consider taking the following actions:
  - Configure devices to control app usage and restrict app purchases and downloads. Some tablets allow you to create parent-controlled profiles that only allow your children to use pre-approved apps.
  - Install parental control software with Internet whitelisting capabilities on their devices. This can ensure that access to adult content gets blocked and limited.
- Remind your children that once something is written or posted, it can be copied and remain online forever. Controversial statements can resurface at inconvenient times, even in later life when applying for a college or a job.
- Common occurrences of inadvertent information disclosure may include younger family members posting on social media in real-time, either revealing where they are currently located — or where they are NOT currently located — which allows adversaries to determine if a home is empty because the family is on vacation. "Checking In" on Social Media platforms allows others to see exactly where you are and can allow for calculating how long you will be gone (e.g., checking in to a restaurant for dinner indicates a roughly two-hour time frame).

PROTECT YOURSELF DATA: SENSITIVE DATA PROTECTION

0100100110
1010110100
1100011001
0011100101
0101100110

GUIDANCE

- Review and be conscious of where all your sensitive information is stored, including email, chat messenger services, shared computers & personal devices, cloud file storage, flash drives and old laptops.
- Periodically review your critical data, and securely delete it from wherever it is no longer required.
- Avoid sending financial information – pictures of statements, bills, etc. – via text, instant message, or email.
- Securely back up and have multiple backup copies of your sensitive data, e.g. Data encrypted and stored in a reputable cloud service such as Dropbox; iCloud; or Google Drive, on encrypted disk at home, and on an encrypted flash drive in a safety deposit box.
- Ensure that your sensitive data is stored in an encrypted format in order to prevent another person from viewing it, if it gets lost or stolen.

HOW DO YOU PROTECT YOUR MOST SENSITIVE DATA?

- Take a moment to evaluate what sensitive personal data exists about you and where it resides. Also consider how that information can be used against you if it is compromised.
- Be conscious of how you share your sensitive data with others. A good gauge is to ask yourself why a particular company or individual needs that information.
- Avoid sending personal or financial information (including pictures of statements, bills, or other documents) via text, instant messaging, or email.
- Protect any physical or paper copies of your sensitive media as well. Remember to shred and dispose any unneeded material which has sensitive data, including credit card statements and offers, financial statements, and investment information. Consider scanning sensitive information you need to retain for a more effective archival process (multiple copies). Alternatively, a fireproof safe or safety deposit box is another option for secure storage.
- Regularly back up all of your data to protect yourself from malware or having a broken/lost device. Make sure the backup is stored in a safe place and that access credentials to the backup are protected. Consider using a third-party offline or cloud backup service.
- Consider using an escrow or secure storage of your encryption passwords to allow family or staff to access your encrypted sensitive data if you are incapacitated. A common scenario is to include the password in your safety deposit box, healthcare proxy, or will with your attorney.
- Exercise caution when using a public computer or public Wi-Fi hotspot when not at your home or office, and avoid transmitting personal or sensitive information (such as health or financial data) in these situations.

PROTECT YOURSELF DATA: EMAIL SECURITY

GUIDANCE

- Email continues to be the most common medium for performing online fraud.
- Be cautious or suspicious of unexpected email messages, particularly those that contain attachments or links, even if they are from sources you recognize.
- Always verify suspicious emails or any emails requesting financial transactions in person or over the phone, not via email.
- Set up two-factor authentication for your email provider.
- Avoid sending or storing sensitive data via email.
- Depending on your risk posture and privacy needs, consider a private or commercial email setup that offers advanced anti-spam, anti-virus, anti-phishing, or other email filtering capabilities.
- Monitor your email for suspicious activity. Periodically review your ‘sent’ folders for unknown emails, and your email rules for unauthorized forwarding.

HOW DO YOU USE EMAIL COMMUNICATION SAFELY?

- Do not click on links in suspicious-looking emails, masquerading as emails from your friends, family, financial institutions, utilities providers, social media companies, or the government. Instead, navigate directly to the site from your browser to process the request. If you suspect a link might be malicious, contact the person who sent the email by telephone or other non-email channel, or go to the organization’s website from your Internet browser and find the desired content within the site menu instead of clicking on the link in the email.
- Suspicious phishing emails may contain subtle grammatical mistakes, such as a URL or website display that looks similar to that of a legitimate site but with slight differences.
- Avoid sharing personal or sensitive information through email.
- Consider using encrypted email if available or encrypting attachments using a ZIP utility. Do not communicate the password for the ZIP file in the same email as the compressed / encrypted file.
- Periodically scrub your email accounts clean of old personal information. Consider how that information could be used against you if it landed in the wrong hands.
- Consider setting up different email accounts for online financial accounts, online purchases, and non-consequential accounts such as entertainment (e.g., Netflix).
- Never use a work email address to register for personal accounts. Work email accounts should only be used to conduct business-related activities.
- If you have reason to believe your email account has been compromised, change the password immediately and set up two-factor authentication. Review your email account settings for new suspicious “forward-to” or “reply-to” addresses. Fraudsters sometimes add these to hide messages they are sending. Additionally, you should check for auto-send messaging rules you have not authorized.
- Spam, whether or not it involves malicious intent, can take the form of chain mail or junk mail and easily builds up in your email inbox. It is important to delete the spam messages you receive.

PROTECT YOURSELF DEVICES: PROTECT YOUR PORTABLE DEVICES

GUIDANCE

- Never leave smartphones or computing devices unattended while unlocked.
- Make sure your smartphone is passcode-protected with a strong password known only to you, and automatically locks the screen when inactive.
- Configure your phone to auto-delete all information if the password is entered incorrectly too many times.
- iPhone is more secure than Android because it is patched more rapidly and all apps are reviewed by Apple. If you want to use Android, Google Pixels are the most secure as they are patched more rapidly.
- Use the most secure version of your system by regularly or automatically installing software updates.
- Disk-encrypt all your devices, including laptops, mobile phones, flash drives, and storage disks, to protect your data if it is lost or stolen.
- Enable remote phone location tracking services to help you locate your phone if it is lost.
- Check with your cellular provider if they have controls in place to avoid someone from porting or sim-swapping your mobile number to intercept authentication codes. Verify if they have a secret PIN created for you — preferably different from your Social Security number — to authenticate before a porting or sim-swap request is approved.

HOW DO I SAFEGUARD MY DEVICES?

- Use your devices safely and consider what your risks would be if your device were stolen. Mobile devices, in particular, can contain significant sensitive information and have the potential to cause considerable financial, professional, and reputational impact.
- Be aware that using your phone for a sensitive transaction is more likely to be secure than using your computer. An app on the phone (as long as it came from a trusted App Store) is more likely to be secure than a website.
- Enable automatic screen locks upon inactivity for all devices.
- Avoid using jailbroken or rooted devices. Such modified devices may disable or bypass important security controls.
- Only install applications from trusted sources and app stores, and do not open attachments from untrusted sources.
- Disable notification previews, a smartphone feature that displays the first sentence of each text, email, or notification you receive on the lock screen.
- Learn how to use ‘remote data wipe’ or lost device search features where available, in the event that your device gets lost or stolen.
- Wipe data off your old phone before you donate, resell, or recycle it.
- Evaluate which applications truly require location services. As well as providing you with accurate, local information, these services can be used to track you even when the application is not active. Disable automatic location tracking in social media apps.
- When traveling, be extra diligent. Keep your mobile devices with you at all times while in public places. Never check them in as luggage when you are traveling, and avoid leaving them unattended in your hotel rooms.
- Be conscious that when traveling to certain countries, the local laws may require you to provide your device password (and possibly email and social media passwords). Burner or backup phones and laptops are generally used under such conditions.
- Avoid connecting your smartphone to any computer or charging station that you do not control, such as a charging station at an airport terminal or a shared computer at a library, which could allow malicious software to be installed and interact with the phone in ways that you may not anticipate.
- Laptops and Desktops – Many of the best practices for smartphones also apply to laptops and desktops, and consider taking the following additional actions:
  - Install a security package (e.g., Microsoft Security Essentials) that offers firewall, anti-virus, and anti-malware protection.
  - Create standard user accounts and make sure all administrative rights are set appropriately, i.e. configured to the minimum permissions needed for a user.
  - Configure a separate guest account for visitors with limited permissions versus sharing your personal account.
  - Consider using a laptop camera cover to limit the potential impact if your computer camera gets hacked.

PROTECT YOURSELF DEVICES: SMART HOME DEVICES & THE INTERNET OF THINGS

GUIDANCE

- Smart devices are becoming increasingly common. As with any electronic device, consider how this smart device can be used against you and your family.
- Consider the tradeoffs between convenience, security, and privacy before purchasing and installing any new IoT products.
- As a general practice, consider purchasing devices from large reputable enterprises who may have the ability to bake security and privacy into the design of their products, versus smaller vendors.
- Always check privacy settings and default configurations. Change all default passwords.
- Avoid sharing unnecessary location and health information with activity trackers and other wearable devices.
- Consider configuring a separate or guest Wi-Fi network at your home for smart home devices only.
- Configure 4 digit voice PIN to protect from making accidental purchases in smart home devices like Alexa and Google Home.

HOW DO I MANAGE MY SMART HOME?

- The term Internet of Things (IoT) is used to refer to everyday devices that have the ability to communicate with each other and with people. This category of technologies includes home assistants like Google Home or Amazon Echo with Alexa, fitness monitors like the Apple Watch or Fitbit, and a diverse range of other smart home innovations – from programmable thermostats that automatically regulate temperature to Wi-Fi-connected, keyless front door locks, connected children's toys, home appliances, surveillance cameras, and home automation systems.
    - Connected devices can communicate with consumers, transmit data back to companies, and compile data for third parties such as researchers, health care providers, or even other consumers, who can then measure how your product usage compares with your neighbors'.
    - Consider the tradeoffs between convenience, security, and privacy before purchasing and installing any new IoT products. Evaluate whether or not devices such as your household refrigerator, toaster, and washer & dryer really need Internet connectivity.
- Change all default passwords set by the device manufacturer, includin any remote access passwords, which may allow a user to log in without your knowledge. Apply caution when sharing data or revealing any location details.
- Just like with your laptop or tablet, keep your IoT devices updated with the latest security patches and software versions. Consider enabling automatic software updates from the device manufacturer.
- At home, connect your devices to a Wi-Fi network which is separate from the main Wi-Fi network used by your mobile devices and computers. If your Wi-Fi router does not allow you to create multiple separate networks, consider connecting your smart devices to your Wi-Fi guest network, if available. This helps contain any damage or risk to your primary computing devices, should your IoT devices get hacked.
- If your IoT device has a web interface, use it to search for and disable the Universal Plug and Play (UPnP) feature, since UPnP can be a common security risk.
- Consider changing the device's "wake" word from the default, e.g. 'Alexa'.
- Configure your device to play a chime that alerts you when it is recording.

RESOURCE REFERENCES

GLOSSARY OF TERMS

- *Clickbait:* Content whose main purpose is to attract attention and encourage users to click on a link to a particular page or article. Outrageous claims and "see what happened" headlines typically help identify clickbait.
- *Credential stuffing:* A cybercrime technique where stolen account credentials are used to gain unauthorized access to a user's various other online accounts. Individuals who reuse passwords across different services are particularly susceptible to such attacks.
- *Email spoofing:* The forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source – a common tactic in phishing and spam campaigns.
- *Encryption:* A process that scrambles data so it can only be read by someone with the "encryption key." Encryption should be considered for handling sensitive information online. Most modern operating systems offer built-in encryption capabilities.
- *Identity theft:* The fraudulent acquisition and use of a person's private identifying information, usually for financial gain.
- *Internet of Things (IoT):* Category of everyday devices that have the ability to communicate with each other and with people – includes home assistants, programmable thermostats, and Internet-connected surveillance systems.
- *Malware:* Malicious code that installs itself and runs without the computer or mobile device owner's permission.
- *Phishing:* The practice of using online communications to lure people into divulging personal information, clicking on a malicious link, or opening an attachment.
- *Ransomware:* A form of malware where your important files are encrypted without your knowledge, then the perpetrator demands a ransom for you to gain access back.
- *Security freeze:* Also known as a credit freeze, this measure restricts access to your credit report, making it more difficult for identity thieves to open fraudulent accounts in your name.
- *Smart home devices:* See Internet of Things (IoT).
- *Social engineering:* When fraudsters and perpetrators pretend to be people they are not in order to deceive you into divulging confidential information.
- *Spearphishing:* A targeted attempt to steal sensitive information from a specific victim, where attackers often use personal details about the victim to add legitimacy to their disguise as a trustworthy friend or entity over email or online messaging.
- *Synthetic identity theft:* A cybercrime technique that involves a combination of fake and real credentials, using different individuals' names, Social Security numbers, driver's licenses, and employee identification numbers.
- *Virtual Private Network (VPN):* A safer layer of connection or "secure tunnel" for one's data and Internet activity. This typically includes encryption and other measures for improved location & browsing privacy when connected to public Wi-Fi, among other security benefits.

EXTERNAL REFERENCES

- DoD Best Practices for Keeping Your Home Network Secure
- Center for Internet Security (CIS)
- IRS: Identity Protection
- IRS: Form 14039, Identity Theft Affidavit
- IRS: Tax Fraud Alerts
- National Cyber Security Alliance: Stay Safe Online
- Federal Bureau of Investigation (FBI Cyber Crime)
- Federal Trade Commission (FTC Identity Theft)
- FTC: Credit Freeze FAQs
- FTC: Identity Theft Recovery Plan
- Get Safe Online
- Get Safe Online: General Ransomware Advice
- FCC: Protecting Your Wireless Network
- Safe and Secure Online
- SANS Information Security Resources
- US Computer Emergency Readiness Team (US-CERT)
- US-CERT: CryptoLocker Advice
- US-CERT: Cybersecurity for Electronic Devices
- US-CERT: Preventing and Responding to Identity Theft
- Equifax: Equifax.com/personal/credit-report-services – (800-685-1111)
- Experian: Experian.com/help – (888-EXPERIAN) (888-397-3742)
- TransUnion: TransUnion.com/credit-help – (888-909-8872)
- Innovis: Innovis.com/personal/securityFreeze – (800-540-2505)
- Google: https://safety.google/
- LinkedIn: https://www.linkedin.com/help/linkedin/answer/66/managing-your-account-and-privacy-settings-overview?
- Instagram: https://help.instagram.com/196883487377501
- Facebook: https://www.facebook.com/about/basics/manage-your-privacy
- Snapchat: https://support.snapchat.com/a/privacy-settings
- Twitter: https://help.twitter.com/en/safety-and-security/twitter-privacy-settings
- Pinterest: https://help.pinterest.com/en/article/edit-account-privacy
- Venmo: https://help.venmo.com/hc/en-us/articles/210413717-Payment-Activity-Privacy