Best Practices to Improve your Personal Cybersecurity Hygiene

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

1 Establish secure email protocols

Emails continue to be a common entry point for hackers to perform online fraud. Be cautious and suspicious of all unexpected communication and verify suspicious emails, especially when financial activity is involved.

- Do not click on links or open attachments from suspicious-looking emails.
- Use a different email account for online financial accounts, online purchases, and other general non-consequential accounts.
- Avoid using a work email address to register for personal accounts. Work email accounts should only be used to conduct business-related activities.
- Periodically review your sent folders for unknown emails, email rules for unauthorized forwarding, and login history for suspicious logins.
- If you are suspicious of an email that looks like it comes from your bank, call the bank and verify the content.

2 Strengthen 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, 8-10 characters in length and containing a combination of letters, numbers, and symbols. Avoid reusing passwords. Extend this good habit to family members, especially for shared accounts, which should be used with caution. Consider using a password management application, such as LastPass, 1Password or Dashlane to help manage multiple complex passwords.

3 Enable multi-factor authentication measures

Where available, you should always use either 2-factor authentication (2FA) for account login, commonly done via a PIN sent over text message or email, or the newer multi-factor authentication (MFA) process which is slowly replacing 2FA, whereby a PIN is sent via a secure 'push' your mobile app. At a minimum, enable this capability for your email, cellular carrier, financial websites, password manager, cloud file storage and social media.

4 Lock down social media

Hackers and social engineers can easily obtain critical information about a target from social media sources. 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.

October 2021

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.

- Mobile phone numbers, personal email addresses, screen names, handles, etc., all provide adversaries with a means to learn about and further target an individual.

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. Avoid using email for long-term storage of sensitive information. At home, also consider having a second 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 your devices securely. Consider what your risks would be if your devices 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.

- Enable automatic screen locks and ensure that sensitive data, such as email or text messages, does not display on the lock screen.
- 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.

8 Protect your software

Protect your software from unauthorized access by installing security software such as firewalls, antimalware and secure browsing extensions on your personal devices (particularly desktops and laptop computers). Keep all of your software up to date by applying updates as soon as possible once they become available. Consider enabling automatic updates where available.

9 Secure Wi-Fi access

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.

- At home, connect your smart devices to a Wi-Fi network that is separate from the primary Wi-Fi network used by your mobile devices and computers. Use the guest Wi-Fi network for visitor Wi-Fi access.

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. Sign 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.

October 2021