WEATHERLY
ASSET MANAGEMENT

carolyn@weatherlyassetmgt.com
T 858.259.4507 F 858.259 .0782
832 Camino Del Mar, Ste 4 | Del Mar, CA 92014
WWW.WEATHERLYASSETMGT.COM

7 Steps to Better Cyber Security

Per current events, it is an unfortunate truth that cybercrime is an ongoing threat that continues to evolve and impact our lives. As much as we want to prevent it entirely, cyber security isn't an absolute. You aren't either insecure or totally secure. There is a gradient, and it pays to ensure that you are striving to be on the "most secure" end of the spectrum. Below are 7 tips to help smoothly sail the cyber sea.

1. **Second check before you click & slow down before you share.** Although it may sound a bit extreme- trust NO ONE (online). Phishing emails often look as though they have been sent from a legitimate organization or someone who knows the end target (you), to entice clicks on malicious links or attachments. If you are ever unsure, pick up the phone to verify the validity of the email in question.

2. **Do not duplicate passwords across accounts.** When you use the same password for multiple accounts you open yourself up to a cyber-attack known as credential stuffing. All a hacker needs is your information from one poorly defended site and suddenly, they can access any other account where you use the same login information ("Are Your Passwords," 2020). Length is the primary strengthener when creating a robust password. We suggest a minimum of 10 characters and have found that using a sentence is a great way to create a long password that you will not forget!

3. **Keep your software updated.** Running outdated software is an open invitation for cyber criminals to exploit known flaws and gain access to your system. Software companies regularly push out new updates to patch identified errors, making them (and you) less likely to become a target of cybercrime. The best way to ensure your software is current is to enable automatic updates on your system(s).

4. **Back up your data.** Perform frequent backups of your system and important files and verify your backups regularly. If a ransomware infection were to occur, you can restore your system to its previous state (sans ransomware) using your recent backup(s). Store your backups on a separate network or device such as the cloud or an external hard drive. Ensure that these backups are secured with the utmost protection such as MFA (#5).
    a. Encrypted/Protected External Hard drive: These allow for fast data transfers and large storage capacities. Look for ones that are encrypted and require a padlock password.
    b. Cloud: iCloud, Google Drive, and Dropbox, are some of the most well-known cloud-based services. Many of these come with limited free storage space and a paid option for additional storage if needed.
        i. When choosing a cloud-based storage, ask; Do they have privacy and security settings I can adjust? Do they use encryption to protect my data?

5. **Enable Multifactor Authentication (MFA) whenever available.** MFA adds an additional layer of protection to the sign-in process and is widely available for many of your most sensitive logins. When accessing your data, you will be required provide additional identity verification(s), such as scanning a fingerprint, answering personalized questions, or entering a code received by phone. Use of anything beyond a password significantly increases the work for attackers to access your data, lowering the risk of you getting hacked in the authentication process!
    a. Click here to learn more about setting up MFA on your Fidelity.com login
    b. Click here to learn more about setting up MFA on your Schwab.com login

6. **Insist on Information Security (Infosec).** It is essential to ensure that when working with anyone who has your personal information (SSN, date of birth, acct #s, etc), that they will not misuse or disclose it to outside parties. Be certain that these professionals can and will safeguard your personal identifiable information (PII) to best of their ability. Take the initiative and inquire what secure method(s) they use for the bi-directional exchange of information. Some common examples include encrypted emails, secure portals (Weatherly's preferred method), or password protected documents.

7. **Upgrade your upgrade process.** Your devices (laptops, tablets, cell phones) contain more information than you may think! Whether it be financial or personal, before disposing of your old electronic devices, it is important to delete your information from the hard drive so that it does not end up in the wrong hands. Before letting go of your old devices:
    a. Back up your information (#4)
    b. Sign Out of Accounts, Disconnect Devices, and Erase Your Hard Drive
        i. After you have saved your personal information (cloud, external hard drive, etc), sign out of all your online accounts. It is also best to un-pair your computer from Bluetooth devices (mouse, keyboard, wireless display, etc.)
        ii. Erase your computer's hard drive and reset it to factory settings.
    c. Safely Dispose of your device
        i. Most devices contain hazardous materials that do not belong in a landfill. Instead consider keeping it green, and recycling or donating your old electronics. Check out the Environmental Protection Agency's Electronics Donation and Recycling page to learn about recycling or donating your computer.

When it comes to cybercrime the most harmful thought you can have is, "it won't happen to me". Cybercriminals don't discriminate, so in a way, fighting cybercrime is everybody's responsibility. At Weatherly we consider it our obligation to not only uphold our own best practices, but to be a resource for those joining the fight against cybercrime.