ASSEMBLYMEMBER

Jacqui Irwin

DISTRICT 44

Cybersecurity Guide

Please consider implementing all of these action items to secure both your personal and professional accounts, they will help minimize your vulnerability to cyber attacks. This list is only a brief introduction to steps you can take to secure yourself.

1 TURN ON TWO FACTOR AUTHENTICATION

Two factor authentication is a log-in process that requires the user to use two types of credentials; something you know (such as a password), something you have (such as a cell phone), or something you are (such as your fingerprint). The most common two factor authentication is a password and an additional code sent to a separate device. It is most often triggered when you use a new device or are at an unusual location. Two factor authentication will stop fraudulent attempts to guess your password or brute force attacks on your log-in. These services also notify you to check your accounts and change your passwords if there are unsuccessful authentications.

2 CHANGE YOUR PASSWORDS AND CONSIDER USING A PASSWORD GENERATOR AND KEEPER SERVICE

Changing passwords is a hassle, but it is one of the easiest and most effective ways to limit your vulnerability. Every day you have the same password, or use the same one for multiple accounts, the likelihood increases your accounts are already compromised. Just because you can still access your account, doesn’t mean a hacker is not monitoring your activity. By changing your password on a regular basis, and using an online password generator and keeper service, you are resetting the work of hackers. The benefits of a generator and keeper service are that strong passwords are created and you do not have to remember each unique one. LastPass and 1Password are reputable services, but be sure to look for independent reviews of any security apps before downloading.

3 DON’T CLICK ON PHISHING EMAILS

Phishing is the use of an e-mail, usually made to look official or from a trusted friend that asks you to open an attachment or click a link, resulting in a virus being downloaded to your device. These e-mails use *social engineering*, the practice of manipulating people using personal information or relationships, to trick the recipient into giving more information or access to the sender. Your first reaction to any suspicious or unexpected email should be to first delete it, and then call the sender to verify the authenticity and ask for them to resend the message if it was legitimate. For more routine messages between your co-workers or family that requires a link or an attachment utilize a secret keyword (e.g. “Sutter” or “Colusa”) that will be harder for a hacker to replicate in fraudulent e-mail.

4 UPDATE YOUR SOFTWARE

Every day, tech companies have thousands of security technicians making sure our devices and programs are secure by patching vulnerabilities. Last year, a string of vulnerabilities allowed hackers to access iPhones and read texts, e-mails, record calls, track your location, and even turn on the camera and microphone. Apple quickly provided an update (iOS 9.3.5) but that work goes to waste if, like many average users, you never download it. Whenever your device prompts you to update, take the time to do so.

5 USE ENCRYPTED COMMUNICATION

Many forms of electronic communication are at risk of interception during transmission. If written communication is required, using services like iMessage (Apple's blue text messages), Viber, Signal, or another end-to-end encryption service will limit your messages' exposure during transmission. But, it is always safer to call rather than send written electronic communication when dealing with sensitive information. The use of secure apps is especially important to share with co-workers and family because messages are only as secure as the weakest recipient.

6 TURNING OFF LOCATION SERVICES

While some applications do require location services to function, many applications' default settings go beyond what they need and track your location continuously. This increases your vulnerability as your location data is then on dozens of servers hosted by different companies around the world. This is most important for devices themselves but should also be considered for social media accounts including Twitter and Instagram.

7 DON'T USE PUBLIC WIFI

It is common for hackers to set up fraudulent open WiFi networks like "Airport WiFi" to lure victims. Connecting your device to these public WiFi services gives hackers access to your information, including the information you send and receive. Make sure that your device's settings do not automatically connect to unknown WiFi networks (for iPhones turn off "Ask to Join Networks"). If using WiFi in public is unavoidable, research VPN (Virtual Private Networks) services that can help mask your identity and the data you transmit.

You can learn more at the U.S. Dept. of Homeland Security's Computer Emergency Readiness Team (https://www.us-cert.gov/ncas/tips) & our own IT staff in the Legislative Data Center. We need to work together to make smart choices with our technology.

Questions? Please reach out to Asm. Jacqui Irwin, Chair of the Assembly Select Committee on Cybersecurity and the Co-Chair of the NCSL Cybersecurity Task Force.

Staff: Brandon Bjerke (916) 319-2044