Preventing Cybercrime

Presented by Retired
FBI Special Agent Jeff Lanza
Phone: 816-853-3929
jefflanza@thelanzagroup.com
www.thelanzagroup.com

Computer Security Tips:

1. Don't download anything to your computer that you weren't expecting to do when you got online.
2. Keep your software current with the latest updates. Both Microsoft and Apple issue updates to their operating systems that control your computer. The updates help you stay safe against the latest threats. To make it easy, go to your settings page and tell your computer to keep you updated automatically.
3. Backup your files so you can recover if your computer is compromised. For example, ransomware is an epidemic problem that effects business and home computers. It encrypts files so you can't open them without a key. Look further on this handout for ways to stay safe against ransomware attacks.
4. Consider adding an additional layer of security to your computer. Malwarebytes is a free program that does search and destroy for malware that has evaded your perimeter antivirus program.
5. Use strong passphrases. See below for more details.

Two Factor Authentication aka Two Step Verification

The following is highly recommended. You use a password **and** a PIN code (most often sent to your phone) to log in to online accounts. Use this to prevent hijacking of your accounts. In most cases you can set this up in the security/settings section of your account. Here's the thing: you don't have to use the two steps every time, only if the website wants to make sure it's you, such as when you log in from a different computer or IP address.

Be Password Savvy

It would be really bad if a hacker got access to your online accounts. A passphrase is like a password, only it's composed of a combination of words strung together. That makes them easier to create and remember. Passphrases are the new government recommendation to protect online accounts. Here are some tips to make strong passphrases:

- Use at least 12 characters to help make them uncrackable. The longer, the better.
- If a website makes you use upper/lowercase and a number and special characters (old standard), you can always add those to the passphrases that you have created. Not all sites have adapted to the new government standards.
- Here's an example passphrase: ***paranoiawillnotdestroyya***. The length is the key to making passphrases strong and a little paranoia goes a long way to keeping your accounts secure.
- Use a different passphrase for each online account. I know this is a pain, but it limits the damage if a criminal were to get access to any of your accounts. Much fraud can been committed when a victim reuses passphrases.

How to Respond to Computer Pop-ups

Be cautious of any notifications or pop-ups. Examples include emails that say you have to download something to see a greeting card or a message that says your computer is infected. Don't click on anything in these pop-ups, including the "X" inside the pop-up itself. Your best bet to remove the pop-up safely is to hold down three keys: CTL+ALT+DEL to exit a pop-up safely on a Windows computer. Use CMD+Option+Escape on a Mac. Then run your antivirus software to see if there is malware on your computer that caused the pop-up.

Fake emails:

Be careful where you click. Don't click on links or attachments in emails from an unknown sender, a suspicious sender or in emails that don't make sense. Remember that a friend's email account can become compromised and that attackers can "spoof" someone's email address to appear to be from anyone they choose. Remember, don't react emotionally to an email. The hackers count on this to overcome logic and force us into making bad decisions.

Ransomware

What it is. Ransomware is a form of malware that restricts access to data by encrypting files or locking computer screens. The criminal behind the ransomware infection then attempts to extort money from victims by asking for "ransom", usually in the form of cryptocurrencies like Bitcoin, in exchange for access to data.

How it begins. In a ransomware attack, victims will open an email addressed to them and may click on an attachment that appears legitimate, like an invoice or notification of a missed package delivery. If the victim clicks on a link in that email, it may cause malicious ransomware code to install on their computer.

What happens next. Once the infection is present, the malware begins encrypting files on a victim's computer. Users are generally not aware they have been infected until they can no longer access their files or until they begin to see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key.

How to stay safe. Be careful where you click! Also, always backup the content on your computer. If you are infected by ransomware, you can have your system wiped clean and then restore your files from your backup. Also, because ransomware can infect all hard drives, disconnect the backup drive when not in use or use cloud backup.

The Safe Way to Log in to Online Accounts

1. Don't be tricked into giving up your login credentials. Never go to a login page through a link in an email or a pop-up. Instead go to the login page directly by typing the site name.
2. Check out the site by making sure there is an "HTTPS" in the address before you enter information and that the address accurately represents the website you desire. Once you have verified the site, store it for future access in your browser's bookmarks or favorites.

Software

- Make sure that your operating system software and antivirus software is updated automatically. This can be configured in the settings/security options.
- It is imperative that Windows computers be protected with antivirus software. Popular options are **McAfee, Norton and Windows Defender** (free with Windows 10 and downloadable with some previous Windows versions.)
- Keep in mind that these programs provide one layer of perimeter security. If malware evades them, they most likely won't be able to remove it because they couldn't stop it in the first place.
- You might consider a malware removal program that does search and destroy missions. A popular free program that is very effective is called **Malwarebytes.** You can use the free version, which compliments your perimeter antivirus program. It does not replace it.
- Consider using password manager software to help keep track of all your unique passphrases. Some good options are **Keeper, Dashlane and LastPass.**
- You might try "Notes" apps on your smartphone. You can store notes and secure them with a password on your device. No one can open the note and see your passwords without the master password that you create.

Wi-Fi Networks

- Protect your home Wi-Fi network with a strong passphrase and WPA2 encryption.
- Public Wi-Fi networks are not secure. To access the internet, use a virtual private network (VPN) for a nominal fee, or use your smartphone's personal hotspot feature, which uses the more secure cellular network.

Smartphone Security

- Always use a passcode to protect your phone. This keeps the information secure if the phone is lost or stolen. Using biometrics, like Touch ID or facial recognition, is very secure and make it easier to access the device.
- Watch out for fake text messages. Don't call, click or reply unless you have verified the authenticity of the sender.
- Since there is no mouse, you can't hover on a phone or pad device. Press and hold your finger for about 2 seconds to reveal a preview of the website.
- If you use your mobile device for online banking and other financial accounts, you are using a very secure technology. Make sure that you download the apps from the actual Apple or Google store. To use this technology in the most secure way, protect your device with a password, keep the phone and apps updated and report a lost or stolen phone to financial institutions immediately.