Protecting Yourself From Malware

We have all have heard the terms: Virus, Trojan, Ransomware, Rootkits, etc. Essentially, all of these can be filed under one cyber-security title: Malware. **What Is Malware?**

The most basic definition is an app or computer program created to perform malicious and/or hostile actions. The word itself is derived from a combination of the words 'malicious' and 'software'. **Cyber-criminals (Blackhats) try and trick you into installing malware on your computers or devices to gain control over them.** Once installed, malware can enable the Blackhats to spy on your online activities, steal your passwords or files, or use your system to attack others.

Malware can even hijack all your private files, demanding you pay a ransom before you can (maybe) get them back.

Many people are under the false assumption that malware is only a problem for Windows computer owners. Nothing could be farther from the truth. Malware can infect any device, from Mac & Linux computers, to smartphones to DVRs and even your home security cameras. The more devices the Blackhats can 'own', the more money they stand to make.

Many folks think that all they need to do is install a security program, like anti-virus software, and they are protected from getting infected. **Unfortunately, no single program is capable of stopping all of the malware out there today.** The Blackhats are constantly developing new and more sophisticated malware that can evade detection so, in turn, the anti-virus vendors are constantly updating their products to try and detect the new strains. It has become a never-ending race, and the Blackhats seem to always be one step ahead. Since we are unable rely on anti-virus alone, here are some additional steps to take to further protect ourselves:

Blackhats often are able to infect devices by finding weak spots in your legitimate software programs. **The more current your software is, the fewer vulnerabilities your systems will have and the harder it is for the Blackhats to infect them.** Make sure your operating systems, applications, browser and browser plugins, and devices are always updated and current.

Another common way the Blackhats infect our devices is by creating fake programs and apps, post them on the Internet, and then trick you into installing them. It is important that you only download and install apps from trusted online stores, and avoid apps that are new, have only a few positive reviews, are rarely updated, or have been downloaded by a small number of people. **Also, if you are no longer using a computer program or mobile app, delete it from your device.**

Blackhats often trick people into installing malware by sending an email that looks legitimate but contains a hostile attachment or link. It may even appear to have been sent from their bank or a friend. Clicking on the link or opening the attachment then activates malicious code. If a message creates a strong sense of urgency or seems too good to be true, it could be an attack. Be suspicious, common sense is often your best defense. **Think before you click!**

Regularly back up your files to Cloud-based services, or external drives (disconnect the drive after each backup). This protects your backups in case malware attempts to encrypt or erase them. Backups are critical. They are often the only way you can recover from a malware infection.

To summarize, the best ways to defend against malware is to keep all our software and devices up-to-date, install a trusted anti-virus program when possible, and always be on guard against Blackhats trying to trick us into clicking on hostile links or attachments.

When all else fails, current cloud or offline backups are often the only way we can recover.