Company Resource
Malware

What is Malware?

Malware is malicious software that is designed to cause harm. It can result in cyber criminals accessing personal information and/or damaging your device.

Note: Malware is not limited to computers. It can infect almost any device with internet connectivity such as mobile phones, routers, and smart devices.

Signs of a malware infection.

- Slowed device performance
- Inappropriate/hard to close ads
- A browser toolbar that you didn't install/don't recognize
- Frequent pop-up windows

How malware spreads.

- Often, unsuspecting device users end up with a malware infection by clicking on suspicious links/attachments or downloading questionable files/software. It can also be spread by other means such as plugging in an infected USB or sending information over an unsecure Wi-Fi network.
- Without protection like an antivirus program or a firewall, malware's malicious code will begin causing problems. Malware is designed to install secretly so that the user doesn't recognize something is amiss, at least for a while.
- Once malware has infected one "host" device, the malware can easily spread to other devices connected to the same network.

Common types of malware.

- **Virus:** attaches to various files, modifying them and then executing a copy of itself when the user opens the file
- **Worm:** exploits vulnerable files and programs to spread independently by self-replicating
- **Trojan Horse:** disguises itself as a legitimate program, which contains hidden malicious code, to trick users into downloading it
- **Adware:** attempts to expose users to unwanted, potentially malicious advertisements by interfering with your browsing experience, i.e. pop ups, redirections, large banners, auto-play videos, etc.
- **Spyware:** tracks a user's activity without their knowledge, recording information such as keystrokes and login credentials
- **Ransomware:** encrypts data and holds it for ransom, demanding payment in untraceable cryptocurrency. Sometimes, the data will also be released to the public if the ransom is not paid

Best practices for malware prevention.

- Update your devices' software when prompted – don't wait!
- Install antivirus software and keep it up to date
- Be on the lookout for phishing scams, i.e. suspicious emails or texts
- Avoid questionable websites and clickbait and only install apps from reputable sources
- Back up your files. This will help in the recovery process and help limit damage in case of incident.
- Use secure Wi-Fi networks. If you must use an unsecure network, do not login to any accounts, shop online, or access sensitive data

Company Resource - Malware

- Don’t use a jailbreaked device (i.e. a device with its security restrictions removed)

What to do if your device becomes infected.

- **In the moment:** Disconnect from the internet and restart your device in safe mode. If you feel comfortable, you can take steps to restore your device to its previous state (although your files will remain encrypted).
- **Seek help:** We recommend getting professional assistance as soon as you can.
- If you’re concerned that your identity has been stolen, report the incident to the Federal Trade Commission (FTC) or Internet Crime Complaint Center (IC3).