Cyber Security Guide

Malware

Malware is a type of software that is designed to harm or exploit a computer system, network, or device. Malware is a broad term that encompasses various malicious programs such as viruses, worms, Trojans, spyware, ransomware, adware, and more.

Malware can get into a computer in several ways:

- Email attachments: Malware can be attached to an email as a file attachment. Once the user downloads and opens the attachment, the malware can install itself on the computer.
- Downloading from untrusted websites: Downloading software or files from untrusted or malicious websites can result in malware infections.
- Exploiting vulnerabilities: Malware can exploit software or operating system vulnerabilities to gain computer access. This can include visiting a trusted website that hackers have compromised; the compromised website then exploits vulnerabilities such as a web browser bug to download malware.
- Infected removable media: Malware can be transferred to a computer via infected removable media like USB drives; even phones with storage can store malware which is downloaded to a computer when connected for sync/backup or even just charging.
- Social engineering: Malware creators can trick users into downloading and installing malware through social engineering techniques like phishing, spear-phishing, and baiting.

Once installed, malware can carry out various malicious actions, such as stealing sensitive data, taking over control of the system, encrypting files and demanding ransom, displaying unwanted ads, and more. To protect against malware, use reputable antivirus software, keepi the operating system and software up-to-date, and exercise caution when downloading and opening files from the internet or email attachments is essential.

If your operating system is end-of-life, e.g. Windows 8.1, it's critical you arrange to upgrade in order to remain protected, as manufacturers stop releasing security updates for systems that are too old.