What is malware?

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of executable code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software. The term 'badware' is sometimes used and applied to both true (malicious) malware and unintentionally harmful software.

Spyware or other malware is sometimes found embedded in programs supplied officially by companies, e.g., downloadable from websites, that appear useful or attractive, but may have, for example, additional hidden tracking functionality that gathers marketing statistics.

How computers become compromised with malware

- Over-privileged users (having administrative rights on your device)
- Malicious macros (automated actions or commands) within Office files like Word documents or Excel spreadsheets.
- Email attachments, even ones that seem to be from people you know.
- Website links within in email messages.
- "Hijacked" or malicious web pages.
- Browser pop-up windows that urge you to click on links.
- Flash drives or other removable media.
- File sharing using "P2P" (peer-to-peer) software.
- Instant Messaging software.
- Free and shared software like music players, and other little web utility programs.
- Software downloads from illegal pirated software sites.

Symptoms of a Malware or Spyware Infection

- Your computer suddenly starts to behave strangely, requires frequent restarts, or begins showing pop-up ads that aren't related to the website you're visiting.

- Your browser settings have suddenly changed without your consent. Often malware changes the home page setting on your browser.

- Your web browser takes you to unfamiliar sites that you didn't choose to navigate to yourself.

- Pop-ups appear that are unrelated to the sites you normally visit.

- Additional browser toolbars appear at the top of your browser windows.

- Your computer seems unusually sluggish and unresponsive.

- Your firewall and antivirus programs are frequently turned off automatically.

- You are unable to stop the excessive pop-up windows that appear from nowhere.

- Applications appear on your machine that you did not install yourself.

- You get a lot of bounced back email and see evidence of emails being sent without your knowledge.

- Your system preferences are changed to settings you didn't select.

HOW DO I MAKE SURE MY COMPUTER IS MALWARE-FREE?

Personal vigilance, and protective tools. One of the most popular ways to spread malware is by email, which may be disguised to look as if it is from a familiar company such as a bank, or a personal email from a friend. Be wary of emails that ask you to provide passwords or emails that seem to be from friends but have only a message such as "check out this cool website!" followed by a link.

Simply being careful is not always enough. Because business security is not perfect, downloads from legitimate sites can sometimes have malware attached.

- Be cautious when downloading free software or programs.

- Carefully read the end user license agreement or EULA when installing new programs to make sure that no adware and spyware are automatically installed.

- Don't just download email attachments. Scan everything before saving files to your computer.

- Regularly update your anti-virus and anti-malware tool and scan your computer consistently.

- Ensure all your devices have the latest security patches.