Malware - Stranger Danger Refresher

The internet is a powerful and useful tool, but in the same way that you shouldn't drive without buckling your seat belt or ride a bike without a helmet, you shouldn't venture online without taking some basic precautions.

Take malware (short for "malicious software") for instance, one of the most common hazards when you're online. Malware includes any software (such as a virus, Trojan, or spyware) that is installed on your computer or mobile device. We've all heard the warnings, but we're still falling for the tricks that make us click on links or take us to malicious websites. Malware attacks almost doubled in 2021 and it looks like the upward trend will continue. Here are some examples:

- **Adware:** software that downloads or displays unwanted ads when a user is online
- **Botnets:** a network of computers infected by malware, then controlled remotely by cybercriminals
- **Ransomware:** infects your computer, locks it and holds it for ransom
- **Rootkit:** malware that opens a permanent "back door" into a computer system, allowing additional viruses to infect a computer as other hackers find your vulnerable computer exposed and compromise it
- **Spyware:** malware that quietly gathers your sensitive information and then reports it to criminals
- **Trojan:** malware that disguises itself as a regular file to trick you into clicking and downloading it, giving it access to your computer
- **Virus:** This is a program that spreads by infecting files, computers or networks, mobile devices, or routers, and then making copies of itself. Some are harmless, and others can damage data files.

Any of these can cause trouble for you at home or at work. And the steps are pretty basic that help you avoid them - probably ones you've heard before.

- Take action – the first step to peace of mind.
- Verify you have the latest security software, web browsers, and operating systems updates.
- Keep the software on all your devices up-to-date.
- Be wary of communications that want you to act immediately, offering something too good to be true, scare you into clicking on links, or ask for your personal information.
- Use strong passwords that you change regularly.
- Use Multi-Factor Authentication whenever you can (especially email and financial sites).
- Back up all your important files to another device for safekeeping should you fall victim to ransomware or other malware that can cause your device to fail.
- Finally - **Always THINK before you Click**.