WHAT IS MALWARE?

Prelude Services®

Malware, short for "malicious software," includes any software (such as a virus, Trojan, or spyware) that is installed on your computer or mobile device. This is often delivered via harmful websites and/or emails. The software is then used, usually covertly, to compromise the integrity of your device. Most commonly, malware is designed to give attackers access to your infected computer. That access may allow others to monitor and control your online activity or steal your personal information or other sensitive data. Prelude utilizes several software programs to help secure your networks including McAfee and Malwarebytes.

TYPES OF MALWARE

Adware: a type of software that downloads or displays unwanted ads when a user is online or redirects search requests to certain advertising websites.

Ransomware: a type of malware that infects a computer and restricts access to it until a ransom is paid by the user to unlock it. Even when a victim pays the ransom amount, the stolen files could remain locked or be deleted by the cybercriminal.

Spyware: a type of malware that quietly gathers a user's sensitive information (including browsing and computing habits) and reports it to unauthorized third parties.

Trojan: a type of malware that disguises itself as a normal file to trick a user into downloading it in order to gain unauthorized access to a computer.

Virus: a program that spreads by first infecting files or the system areas of a computer or network router's hard drive and then making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy files entirely.

Worm: a type of malware that replicates itself over and over within a computer.

SIMPLE TIPS TO HELP SECURE YOUR INFORMATION

When in doubt, throw it out: Links in emails and online posts are often the way criminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete it.

Think before you act: Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.

Use strong passwords. Make your password eight characters or longer and use a mix of upper and lower case letters, numbers, and symbols.