Victory Over Viruses

What is Malware?

Malware (short for “malicious software”) is a term that refers to a wide variety of hostile or intrusive software. There are a variety of reasons people create malware: to make money, steal personal information, cause trouble, or even just to prove that they can.

Most Common Types of Malware

Adware - Shows advertisements to the user. Collects data on visited sites to show relevant ads in the hopes of generated sales. Not all adware is considered malicious.

Ransomware - Restricts access to a device until the user pays money. Looks like you’ve been locked out of your computer. Sometimes it will look like it’s from a reputable source like Microsoft/Apple.

Viruses - Self replicating malware that spreads to other connected devices. Typically attached to a program and don’t activate until you run/open the program/file.

Worms - Spread over computer networks by exploiting vulnerabilities. They copy themselves over and over and don’t need to be attached to a specific program like a virus. Destroys system information and files saved on the device.

Trojan Horse - Disguises itself as a normal file to trick users into downloading and installing malware.

Spyware - As its name suggests this malware spies on the users computer and internet activity, gathering information and sending it back to an unknown source.

Devices Susceptible to Malware

Many devices can be infected by Malware. Computers, phones, tablets, and even your router.

- Computers
  - Windows
    - Most popular OS. The majority of malware is designed to target Windows.
  - MacOS
    - Safer than Windows. Only apps/programs from the app store are allowed unless given special permission.
  - Linux
    - Safer than Windows and MacOS. Only way to cause damage is to have root access. Most used OS for Servers due to its security and reliability.
  - Chrome OS
    - Most secure OS. At each reboot, software is verified and repaired if necessary. Traditional entry points for malware are closed off.
- Mobile
  - iOS
    - Very secure mobile OS. The only known malware is exclusively designed to target jailbroken devices.
  - Android
    - More common to see malware on an Android device, but overall still very secure.

Preventative Measures

- Browse Safer
  - Don’t download files or click on links if you’re not 100% sure of what they are.
    - Some viruses are sent to your email *through someone in your contacts list* to make it look as if it came from someone you know.
  - Use an Ad Blocker
    - Ads sometimes contain malicious content
    - We would suggest using an extension called uBlock Origin
  - Look for *https://* in the URL bar when giving personal information for banking or online purchases
    - Https Everywhere
  - Microsoft/Apple/Google will *never* call you.
    - If you receive a call from one of these companies, it is a scam. They will never call you, ask for money, or ask to remote desktop into your computer.
- Keep up to date
  - Operating system
  - Programs
- Firewalls
  - Monitors traffic that interacts with your system

Ad Blockers

There are thousands of browser extensions across Google Chrome, Firefox, Safari, and Microsoft Edge. Extensions can do things like change the way your browser looks, make YouTube and Facebook much more enjoyable, or automatically check the internet for coupons before you make a purchase on Amazon. The most widely used extension is an adblocker. These are two of the best options available:

Adblock Plus

uBlock Origin

Note: Having a lot of extensions (or any programs) installed at once can cause your computer to run slower.

Signs You May Have Malware

- Your System is slower than usual.
- Nothing responds when clicked on and/or your programs no longer work properly.
- Your System reboots, freezes up, or crashes for no apparent reason.
- Your antivirus software and/or firewall is suddenly disabled.
- You can no longer access your disk drives or hard drive.
- You are no longer able to print
- You start seeing suspicious pop-up windows stating you have a virus or that your computer is infected. You can not close the pop-up windows.
- Advertisements begin popping up at unexpected and random times.
- You have a problem downloading and installing any additional software
- Desktop icons and program files in your folders are missing.

Antivirus and Malware Removal

Antivirus

Antivirus software actively runs in the background of your computer looking for malware (viruses, spyware, adware, etc.). They typically scan sites as you visit them and files as you download them, trying to prevent malware from getting on your computer in the first place. These are your first line of defense. Windows Defender (Built into Windows 8, 8.1, and 10) is a decent antivirus and will work well for most people. If you'd like something a little more robust, here are five of the best free and paid antiviruses you can get.

Windows Defender

Avast

GDATA

Kaspersky

Norton

Malware Removal Software

These tools do not actively run in the background and need to be run manually. If malware gets through your antivirus, these are your best bet for finding and removing it. You should generally run a quick scan at least once a week and a full scan once a month. Below are four malware removal tools that we recommend.

Malwarebytes
www.malwarebytes.com/

SUPERAntiSpyware
https://www.superantispyware.com/

Kaspersky Virus Removal Tool
https://usa.kaspersky.com/downloads/thank-you/free-virus-removal-tool

Malwarebytes AdwCleaner
www.malwarebytes.com/adwcleaner/