Fight Against Malware

Malware, short for **malicious software**, is software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems. While it is sometimes software, it can also appear in the form of script or code. Malware is a general term used to describe any kind of software or code specifically designed to exploit a computer, or the data it contains, without consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software.

Avoid Malware

Following the tips below can help reduce your risk of downloading unwanted malware and spyware:

- **Keep your security software updated.** At a minimum, your computer should have anti-virus and anti-spyware software, and a firewall. Set your security software, internet browser, and operating system (like Windows or Mac OS) to update automatically.
- **Don't click on any links or open any attachments in emails unless you know who sent it and what it is.** Clicking on links and opening attachments – even in emails that seem to be from friends or family – can install malware on your computer.
- **Download and install software only from websites you know and trust.** Downloading free games, file-sharing programs, and customized toolbars may sound appealing, but free software can come with malware.
- **Minimize "drive-by" downloads**. Make sure your browser security setting is high enough to detect unauthorized downloads. For Internet Explorer, for example, use the "medium" setting at a minimum.
- **Use a pop-up blocker and don't click on any links within pop-ups**. If you do, you may install malware on your computer. Close pop-up windows by clicking on the "X" in the title bar.
- **Resist buying software in response to unexpected pop-up messages or emails**, especially ads that claim to have scanned your computer and detected malware. That's a tactic scammers use to spread malware.
- **Talk about safe computing.** Tell your kids that some online actions can put the computer at risk: clicking on pop-ups, downloading "free" games or programs, opening chain emails, or posting personal information.
- **Back up your data regularly**. Whether it's text files or photos that are important to you, back up any data that you'd want to keep in case your computer crashes.

Detect Malware

Monitor your computer for unusual behavior.

- slows down, crashes, or displays repeated error messages
- won't shut down or restart
- serves up a barrage of pop-ups
- displays web pages you didn't intend to visit, or sends emails you didn't write
- new and unexpected toolbars

- new and unexpected icons in your shortcuts or on your desktop
- a sudden or repeated change in your computer's internet home page
- a laptop battery that drains more quickly than it should

Get Rid of Malware

Following the tips below if you suspect there is malware is on your computer.

- Disconnect your computer from the Internet.
- Update your security software, and then perform a manual scan of your entire system.
- If the manual scan doesn’t locate and remove the infection, you may need to reinstall your operating system, usually with a system restore disk that is often supplied with a new computer. Note that reinstalling or restoring the operating system typically erases all of your files and any additional software that you have installed on your computer.
- After reinstalling the operating system and any other software, install all of the appropriate patches to fix known vulnerabilities.
- Once your computer is back up and running, think about how malware could have been downloaded to your machine, and what you could do differently to avoid it in the future.