Network Technology Resources

Malware is socially engineered, malicious software, that the user unknowingly allows onto their computer because they clicked on a link that installed the virus or rogue software. Most people don't realize their computer has been hijacked. The best defense against spyware and other unwanted software is not to download it in the first place.

Here are a few tips that will help you avoid downloading software that you don't want:

- Don't open spam email messages or click links on suspicious websites. Instead, type the website address directly into your browser, or use bookmarks.
- Watch out for fake virus alerts that show up as pop-ups warning you are infected with a virus or your computer needs updated.
- Don't click links in email messages and avoid websites that offer free software—especially free antivirus software.
- Download programs only from websites you trust.
- If you are redirected to a site wanting to download something to your computer never click **"Agree" or "OK"** to close a window. Instead, click the **red "x"** in the corner of the window or press **Alt + F4** on your keyboard to close a window.

If you're not sure whether to trust a program you are considering downloading, enter the name of the program into your favorite search engine to see if anyone else has reported that it contains spyware. Files that end in the extensions .exe or .scr commonly hide malware. However, even files with familiar extensions such as .docx, .xlsx, and .pdf can be dangerous.

Rogue security software also known as "scareware," is software that appears to be beneficial from a security perspective but provides limited or no security, generates erroneous or misleading alerts, or attempts to lure users into participating in fraudulent transactions. Cybercriminals sometimes try to trick you into downloading rogue (fake) security software that claims to protect you against malware. This rogue security software might ask you to pay for a fake product, install malware on your computer, or steal your personal information.

There are several free ways to help protect your computer against malware and scareware:

Keep JAVA and Adobe Flash Player up to date and only install updates from their websites at http://www.java.com/en/download/installed.jsp and http://www.adobe.com/software/flash/about/

Use Internet Explorer SmartScreen Filter, SmartScreen Filter is included in Internet Explorer. If you attempt to visit a website or download a file that has been reported as unsafe, SmartScreen Filter displays a warning that advises you about the potential dangers.

Install SpywareBlaster to prevent the installation of ActiveX-based spyware, adware, dialers, browser hijackers, and other potentially unwanted programs. It can also block spyware/tracking cookies in IE, Mozilla Firefox, Netscape, and many other browsers, and restrict the actions of spyware/ad/tracking sites. http://www.brightfort.com/spywareblaster.html

Download Microsoft Security Essentials, which is free http://www.microsoft.com/security/scanner/en-us/default.aspx , or another reputable antivirus and anti-malware program like Malwarebytes Anti-Malware https://www.malwarebytes.org/ and scan your computer. If you are infected already you can use this software to remove the malware.