

What is Malware?

If you are reading this, Malware may have already been introduced to you, although you may not have been properly introduced to Malware.

This is Malware:

From Malicious software, Malware is software or a set of instructions designed to infiltrate a computer, without the user's informed consent, and make the system do something that the hacker wants it to do.

Malware generally includes Spyware, Trojans, Adware, rootkits, dialers, Keyloggers, denial of service attacks, botnets, Crimeware, Badware, viruses worms and any other types of unwanted or potentially unwanted software. However, in the strictest sense, the term "Malware" expresses its purpose rather than any particular characteristic.

Unlike Spyware, a type of Malware that is written and installed strictly for financial gain or espionage, Malware can be written for any malicious purpose. In addition to financial gain or espionage, the creator of Malware may be motivated by revenge, anger, notoriety. Or, the creator might only care to see how widespread the infection could become, with little concern about the damage it could cause.

This is what Malware is NOT:

Malware is not a "bug" or a defect in a legitimate software program, even one that might have destructive consequences. Malware implies malice of forethought. Its intent is to disrupt or damage a system.

This is what Malware does:

- Changes system settings. For example, Malware can "hijack" your browser, redirecting your Web searches to a disreputable search engine that delivers unwanted, sometimes offensive search results. It can change your homepage settings, and even make surfing impossible.
- Installs unauthorized dialers. Malware can install programs that alter your dial-up settings and then dial numbers without your knowledge. Often, these numbers connect to potentially offensive sources. Once dialer software is downloaded, you will be disconnected from your Internet service provider. Dialers automatically dial "900 numbers" and you will be billed for the time used. Dialers are malicious in nature and can rack up expensive and unwanted bills

- Installs keystroke loggers. Malware can install programs that monitor and record every key stroke you type. Keystroke loggers are a grave threat to both your privacy and your security. They can monitor your e-mail and chat, capture account numbers, user names, passwords, Social Security numbers and other identifiers that you type when making purchases or doing banking.
- Collects and reports user's personal information to the developer of the software or to one or more unauthorized third parties. Once Malware has captured your personal information, it relays this information back to its creators, who use it for fraud, identity theft or other illegal purposes.
- Uses computer processing capacity without permission. If your computer processing has suddenly slowed to a crawl, you are probably infected with Malware. At the very least, Malware runs as a background application, as soon as you boot up. Unlike the makers of legitimate software, the makers of Malware do not care how inefficient their programs are with your resources. They tend to hog your computer's RAM and processing power. Sometimes, buried in the End User License Agreement, that agreement you agreed to when you installed some application, is a clause authorizing the software makers to use your computer without your permission, even to turn your computer into a "bot" that launches additional Malware!
- Delivers spam or ads without user's notice and consent. If Malware is monitoring your surfing habits, it can deliver ads that seem relevant to your search. For example, you could be searching the Web for mortgage rates when a pop-up ad for a bank or realtor is displayed on your screen. Ads relevant to your searching are much more effective than random ads. Although the ad itself may be merely a nuisance, it has been delivered at that time because your search was being monitored, and you should be concerned for your privacy.

This is how you become infected with Malware:

Malware is often transmitted by downloading freeware and shareware or swapping files. Music files, free toolbars, pictures, screen savers and other "cool" applications can infect you with Malware. Malware is also delivered via spam, when you open a malicious message or attachment.

Phishing sites often download Malware onto unsuspecting users who believe they are replying to requests for information by their banks, credit unions or merchants with whom they do business.

This is how to prevent infection by Malware:

- Do not click on pop-up advertisements.
- Do not open e-mails from unfamiliar or questionable sources.
- Do not respond to online requests for personal information, such as Social Security number, passwords, usernames or any other identifiers that could be used for fraudulent activities.
- Download only those software programs that come from reputable sources.
- Install a good anti-virus product, and make sure you are running the latest updates at all times.
- Install STOPzilla. It provides True Real-Time protection from Malware, blocks Phishing attacks and kills pop-up ads. To make sure you are running the latest updates to STOPzilla, set it to download and install definition updates automatically.