

Why Should You Be Afraid of Malware?

What is malware?

Malware is a general term for software that is meant to cause harm. Computer viruses, spyware, adware, and Trojan horses are all examples of malware. Computer security experts like to compare malware with human diseases (which is why computer viruses are called “viruses” in the first place).

The purpose of malware can be something as seemingly harmless (yet annoying) as popping up a window to show you unwanted advertizing, or as dangerous as snooping on the keystrokes as you type your internet banking password.

How do computers get malware?

Computers become infected with malware through a number of mechanisms – sharing files on jump drives or floppy disks, opening suspicious e-mail attachments, or visiting websites that are themselves infected with malware. Additionally, malware can arrive via downloaded files, such as music or videos from a peer-to-peer file sharing networks (such as Kazaa or BitTorrent), or simply by visiting a website that has been hacked and infected. No longer is it a matter of staying away from “bad” websites. Unfortunately any website that is not properly secured can be hacked and infected with malware that could infect your PC.

How do you avoid getting malware?

Doctors tell you to avoid getting the flu by washing your hands frequently, avoiding contact with those who are already infected, and by getting immunized. Precautions against getting malware are remarkably similar to trying to stay healthy.

- **The single most important step that you can take to protect your PC is to install and use well-known anti-virus software.** Update the virus definitions regularly and scan your computer regularly. Most anti-virus scanners will provide tools to automate these tasks so that they take place when you are not using your computer. This software will help you when you visit a site that has been hacked and infected.
- **Use a software firewall.** If you are using Windows XP or Vista, enable the Windows Firewall. If you have a Mac and are running OS X 10.2 or above, enable the built-in firewall.
- **Avoid fake anti-malware.** Unfortunately, there are rogue anti-malware vendors that promise to rid your computer of malware, but actually install malware instead, often holding your computer hostage until you pay them. Don't buy anti-malware software advertized in pop-up ads. Legitimate software isn't sold this way. GetNetWise.org (maintained by the Internet Education Foundation) has a list of legitimate security tools (<http://security.getnetwise.org/tools/>).
- **Don't open suspicious e-mail attachments.** Historically e-mail attachments are one of the most popular ways to spread malware. If you don't know what it is, delete it immediately rather than open it.

- **Surf the web carefully.** Malware often comes from “dodgy” web sites. Download and install software only from websites you know and trust. Scan any downloaded files for viruses before you open them.

How will I know if my computer is infected?

If you have a Mac, your chances of being infected with malware are lower than if you are running Windows, although the incidence of Mac malware is on the rise. Some security experts predict that 2009 will see a large increase in the amount of malware targeted at Macs.

It is possible that malware will make its existence known through pop-up windows or messages on your screen. If your computer exhibits this sort of behavior, your computer is certainly infected. Otherwise, you should look for the following symptoms.

Programs running slowly, crashing: many types of malware like to piggy-back on other applications, like web browsers, to monitor what they are doing. This can use a lot of your computer’s resources, causing it to slow down considerably. On the other hand, some malware is just badly written and can slow down your computer or even crash other applications.

Suspicious network traffic; slow internet connection: If you are running Windows, press the CTRL, ALT and Delete keys at the same time, then select “Task Manager” from the resulting window. When Task manager opens, click on the Network tab and see if your PC is using the internet network connection, if it shows more than a few percent usage then this could be evidence of something using your internet connection without your knowledge.

Anti-virus warnings: Antivirus software cannot be expected to find all malware, but it does detect about 75%. Some malware will attempt to download other malware to do more damage. Antivirus software may detect one of these applications but not both. An anti-virus warning, combined with other signs, is a good indication of an infection, especially if you’re not currently browsing the web or copying files.

What should I do if my computer is infected?

First, stop banking, shopping, or other online activities that involve sensitive information. Confirm that your anti-virus software is enabled and up-to-date. Scan your computer for viruses. Allow the anti-virus software to do its job, cleaning up and deleting viruses. Some malware is very sophisticated and can be difficult to remove even with the tools mentioned here. If you suspect that your computer is still infected, you may want to contact a professional. Many of the stores that sell computers also have services to repair them; this may be a good place to find assistance.

There are some helpful, legitimate (and free) resources that can aid in getting your computer healthy again:

- Malwarebytes (<http://www.malwarebytes.org/>) has a number of tools that can help identify and remove malware from your computer.
- Windows Live OneCare safety scanner (<http://onecare.live.com/scan>) is a free service offered by Microsoft that can clean up malware as well as tuning up your PC.