How to Avoid Malware

By [Justin Phelps](http://www.pcworld.com/author/Justin-Phelps/), PCWorld Nov 16, 2010

Greetings beloved PCCupid Clients,

Let’s be clear, I did not write a word of this PCWorld article. PCWorld is a well-respected magazine and online source for viable computer information. I found its content most important in today’s home computing/internet environment. I simply wanted to pass this information along to you. You can find the full online article here at this web address: <http://www.pcworld.com/article/206107/most_dangerous_places_on_the_web.html>

* *Your PCCupid, Keith Lawton*

Malware is a term used to describe a broad category of damaging software that includes viruses, worms, trojan horses, rootkits, spyware, and adware. The effects of malware range from brief annoyance to computer crashes and identity theft. Malware is easier to avoid than it is to remove. Avoiding malware involves a two-part strategy. Follow these guidelines for staying safe.

**Prevent Malware With Smart Online Behavior**

The single biggest factor in preventing a malware infection on your PC is you. You don't need expert knowledge or special training. You just need vigilance to avoid downloading and installing anything you do not understand or trust, no matter how tempting, from the following sources:

**From a website:** If you are unsure, leave the site and research the software you are being asked to install. If it is OK, you can always come back to site and install it. If it is not OK, you will avoid a malware headache.

**From e-mail:** Do not trust anything associated with a spam e-mail. Approach e-mail from people you know with caution when the message contains links or attachments. If you are suspicious of what you are being asked to view or install, don't do it.

**From physical media:** Your friends, family, and associates may unknowingly give you a disc or flash drive with an infected file on it. Don't blindly accept these files; scan them with security software. If you are still unsure, do not accept the files.

**From a pop-up window:** Some pop-up windows or boxes will attempt to corner you into downloading software or accepting a free "system scan" of some type. Often these pop-ups will employ scare tactics to make you believe you need what they are offering in order to be safe. Close the pop-up without clicking anything inside it (including the X in the corner). Close the window via Windows Task Manager (press Ctrl-Alt-Delete).

**From another piece of software:** Some programs attempt to install malware as a part of their own installation process. When installing software, pay close attention to the message boxes before clicking Next, OK, or I Agree. Scan the user agreement for anything that suggests malware may be a part of the installation. If you are unsure, cancel the installation, check up on the program, and run the installation again if you determine it is safe.

**From illegal file-sharing services:** You're on your own if you enter this realm. There is little quality control in the world of illegal software, and it is easy for an attacker to name a piece of malware after a popular movie, album, or program to tempt you into downloading it.

**Remove Malware With the Right Software**

Chances are that no matter how careful you are, you will be infected some day. That's because malware is designed to sneak onto your computer in ways you can't possibly foresee. Enlist the help of the following software:

**An updated operating system:** Use Windows Update. Take advantage of its ability to automatically notify you of updates, or better yet, to automatically download and install updates.

**An updated browser:** No matter which browser you use, keeping it current is vital to preventing infection. Take advantage of your browser's pop-up blocking, download screening, and automatic update features.

**Antivirus software:** You must run an antivirus program to be safe. Keep it updated, turned on, and schedule a scan to run at least once a month. (Don't run two antivirus programs; they will interfere with one another.)

**Anti-malware:** Also called anti-spyware, many antivirus applications include an anti-malware component. If yours does not, install and use a standalone anti-malware program that does not conflict with your antivirus program. Keep it updated.

**Firewall:** If you aren't running a third-party firewall, use Windows Firewall. (Don't run two firewalls at once; they will interfere with one another.)

**Spam filter:** If your e-mail program is not adequately filtering spam from your in-box, consider additional spam filtering software. If your security software is a security suite, spam filtering may be a feature that you need to switch on.