

# Technology Tips

March 15, 2005



## Question:

*My computer is infected with malicious software and I don't know how I got it. In fact, the infection was so bad that the technician took my computer away, cleaned it off and re-installed everything. How can I keep my computer and data safe in the future?*



## Answer:

Malicious software (malware) is designed to send you pop-up ads, direct your Internet browser to specific web sites, keep track of the web sites you visit, steal your passwords or credit card information, use your computer to send spam or other bad things, or monitor everything you type. Because your computer is doing a lot of extra work for the malware, it may become very slow, freeze up or generate error messages. Internet browser windows may pop-up on their own disrupting your work.

People who produce malware (including spyware, adware, trojans and viruses) have created a number of clever lures to get their software installed on your computer. They attach malware to programs or links that may sound helpful or fun. Malware is frequently included in “free” software, screensavers, toolbars, pop-up blockers, music or movies that you download from the Internet. Sometimes the malware is sent to you as a file attached to an email. Sometimes it is embedded in a graphic in an email. It can even be installed without your knowledge when you visit a web page. Here are some tips for avoiding malware:

- ❶ Do not click on anything in a pop-up window. To close a pop-up window, click the X in the upper right corner of the pop-up window.
- ❷ If you get an unexpected dialog box or window asking whether you want to run a program or perform a certain task, close the window or dialog box. Do not click on the Yes or No buttons in the box. Clicking on either the Yes or the No button may install malware. To close the window, click the X in the upper right corner of the window.
- ❸ Do not download free software, screensavers, cursors, toolbars, pop-up blockers, music or movies from the Internet. Before downloading anything, consult your network administrator. Many popular free programs available on the Internet contain malware. Here are a few examples of the offenders: BonziBuddy, Comet Cursor, CoolWebSearch, Gator, IEPlugin, PalTalk, Search Assistant, WebRebates, Windows Search Bar. To find out if a program is malware, go to [www.spywareguide.com](http://www.spywareguide.com) and enter the name of the program in the search box.
- ❹ Before opening any file attached to an email, be certain that you were expecting to receive the attached file from the person who sent you the email. If you have any question, call the person before opening the attached file. Malicious software may steal the email address of one of your colleagues or friends and use it to send you a friendly-

sounding message encouraging you to open an attached file containing malware or a virus.

- ⑤ If you get an email advertising anti-spyware software or pop-up blockers, do not click on any links in the email. Do not click on any link offering a free security scan for your computer. The link may actually install malware.
- ⑥ If you get an email indicating that your bank account, eBay account or PayPal account has problems, do not respond to the email. Do not click on any links in the email. These are “phishing” attempts to steal your personal information and identity. If you think that an email might be a legitimate communication from your bank, look up the telephone number to your local bank branch and call them or log in to your online account directly and check for any messages from the bank. Do not click on any links in the email.
- ⑦ In fact, you should not click on a link in an email unless you were expecting to receive that link. If you are uncertain about a link, don’t click on it. Instead, use a reputable search engine such as Google to find the web address for the site you want to visit and go directly there.
- ⑧ Avoid visiting certain types of web sites that may download malware to your computer without your knowledge. Be especially suspicious of sites that offer:
  - Pornography
  - Very low priced or pirated software
  - Free games, screensavers, pop-up blockers, graphics, toolbars, or music
  - Peer-to-peer file sharing programs
- ⑨ To protect your home computer, make sure that you have installed the following:
  - A good firewall (At least a software firewall. If you have high-speed Internet, get a router with a built-in firewall.)
  - Anti-virus software with virus definitions updated at least weekly
  - Legitimate anti-malware software such as Microsoft Anti-Spyware Beta, Spybot Search & Destroy, Lavasoft Ad-Aware, or Spyblaster. (Note: only run one of these programs at a time. Do not install several and leave them all running auto-protect programs because they may conflict with each other and slow down your computer.)
  - Service Pack 2 (SP2) for Windows XP with the built-in firewall and automatic updates enabled
  - The latest security patches for all your software (Go to the manufacturer’s website and check for updates regularly.)

Do not install these things on your work computer without consulting your network administrator. You may create conflicts with other software on your computer or network.