

Technology Tips

What is Spyware/Malware?

Spyware is software that resides on a computer and sends information to its creator. That information may include surfing habits, system details or, in its most dangerous form, passwords and login information for critical applications such as online banking. Many spyware programs are more annoying than dangerous, serving up pop-up ads or gathering e-mail addresses for use in spam campaigns. Even those programs, however, can cost you valuable time and computing resources.

Often, spyware comes along with a free software application, such as a game or a supposed productivity booster. Once it's downloaded to your computer, the functional element of the software works exactly as promised, while the information-gathering system sets up shop behind the scenes and begins feeding your personal data back to headquarters.

Malware, short for *malicious software*, is programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior.



How to Avoid Spyware/Malware:

- Don't click on any pop-up or advertisement for free anti-spyware software. These are almost always fake, even if they carry the name and logo of a well-known publisher. Ironically, this is a very popular method used to distribute spyware and other malware. If you're looking for anti-virus software, go directly to the company's Web site and be sure you're where you think you are.
- Avoid questionable Web sites. If you visit a site that seems strange, there's a good chance you shouldn't be there.
- If a virus alert appears on your screen as you visit a Web site, don't click on it, even to close it. Instead, type control-alt-delete to launch the Task Manager and use the "End Task" command to close the window.
- Never open an e-mail attachment if you're uncertain of its source.
- Stay away from online Internet games, or downloading free screen savers.
- Be wary of Google searches (or other search engines: Yahoo, MSN, BING). Google makes it easy to find web sites on the content you're looking for, but you have no idea where the suggested web sites are from and who created them.
- Avoid using add-on toolbars in your web browser.
- Be wary of security warnings that ask to download software while you browse the web.