



SPYWARE

Just when you thought you were Web savvy, one more privacy, security, and functionality issue crops up—spyware. Installed on your computer without your consent, spyware software monitors or controls your computer use. It may be used to send you pop-up ads, redirect your computer to websites, monitor your Internet surfing, or record your keystrokes, which, in turn, could lead to identity theft.

Many experienced Web users have learned how to recognize spyware, avoid it, and delete it. According to OnGuard Online, all computer users should get wise to the signs that spyware has been installed on their machines, and then take the appropriate steps to delete it.

The clues that spyware is on a computer include:

- Barrage of pop-up ads
- Hijacked browser—that is, a browser that takes you to sites other than those you type into the address box
- A sudden or repeated change in your computer's Internet home page new and unexpected toolbars
- New and unexpected icons on the system tray at the bottom of your computer screen
- Keys that don't work (for example, the "Tab" key that might not work when you try to move to the next field in a Web form)
- Random error messages
- Sluggish or downright slow performance when opening programs or saving files

The good news is that consumers can take steps to lower their risk of spyware infections. Indeed, OnGuard Online suggests that you:

Update your operating system and Web browser software. Your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that spyware could exploit.

Download free software only from sites you know and trust. It can be appealing to download free software like games, peer-to-peer file-sharing programs, customized toolbars, or other programs that may change or customize the functioning of your computer. Be aware, however, that some of these free software applications bundle other software, including spyware.



SPYWARE

Don't install any software without knowing exactly what it is. Take the time to read the end-user license agreement (EULA) before downloading any software. If the EULA is hard to find—or difficult to understand—think twice about installing the software.

Minimize “drive-by” downloads. Make sure your browser security setting is high enough to detect unauthorized downloads, for example, at least the “Medium” setting for Internet Explorer. Keep your browser updated.

Don't click on any links within pop-up windows. If you do, you may install spyware on your computer. Instead, close pop-up windows by clicking on the “X” icon in the title bar.

Don't click on links in spam that claim to offer anti-spyware software. Some software offered in spam actually installs spyware.

Install a personal firewall to stop uninvited users from accessing your computer. A firewall blocks unauthorized access to your computer and will alert you if spyware already on your computer is sending information out.

If you think your computer might have spyware on it, experts advise that you take three steps: Get an anti-spyware program from a vendor you know and trust. Set it to scan on a regular basis—at least once a week—and every time you start your computer, if possible. And, delete any software programs the anti-spyware program detects that you don't want on your computer.

OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

September 2005