



People Fall into the Spyware Trap by the Thousands

You might think you are immune to spyware, but people fall into the spyware trap by the thousands every day. The following scenario should be enlightening.

It's Wednesday and your friend's birthday is Saturday. You decide to buy her a CD. An Internet search takes you to some online stores that seem legitimate, so you place an order with one. After you create an online account, agree to the store's policies, and select "check out," you enter your credit-card number and personal information. You pay for overnight shipment so you know you'll have the gift in time for the party.

What you don't know is that while you were shopping some programs were installed on your computer without your knowledge. These programs are called **spyware**. They transmit personal information to a third party without your knowledge and explicit consent.

Often spyware has been added to your computer legally because you actually consented to have it installed. You might not be aware that you agreed because some end-user-license agreements (EULAs) are very long-winded and subtle. Many shoppers will breeze over the verbiage and grant permission to spyware without being truly aware of it. According to the Ponemon Institute 2005 Spyware Study:

- More than 84 percent of respondents believe that they are victims of spyware
- Of these individuals, 97 percent do not recall seeing an EULA

Some spyware is quite nasty. It may slow down your system, steal confidential information, or compromise the security of your PC.

[Back to top](#)

How Spyware Works

Traditional viruses come in a single package (such as an .EXE file). But in the spyware world, things multiply quickly. Once suspicious software is executed, it usually deploys many (dozens or hundreds) of other files onto your system. Some of these files are so well hidden that they are difficult to find and remove. Some start their dirty work immediately, finding and sending out personal or sensitive data. Others download yet more components onto your system. This eats

up network bandwidth and makes removal a challenge.

Spyware works in stealth mode. Sometimes it jumps into action when you connect your infected laptop to your company's network. One type of spyware searches through your files and sends your usernames and passwords to a third party. Another type records and sends out your keystrokes as you log into Internet sites or sensitive internal areas of your company's information systems.

The less damaging kind just might pop up web sites that distract you from your work. The result is that your system becomes so unreliable and slow that you will need intensive technical support to fix the problems.

[Back to top](#)

Types of Spyware

Adware is software whose primary function is to make revenue through advertising that is targeted at the person using the computer on which the adware is installed. This revenue can be made by the vendor or partners of the vendor. This does not imply that any personal information is captured or transmitted as part of the software's functioning, though that is often the case.

A **dialer** is a piece of code that redirects Internet connections to a party other than the user's Internet Service Provider for the purpose of incurring connection charges for a content provider, vendor, or other third party.

A **remote administration tool** is designed to allow remote control of a system by a knowledgeable administrator. When controlled by a party other than the legitimate owner or administrator, remote administration tools are a large security threat.

Password crackers are code designed to allow a legitimate user or administrator to recover lost or forgotten passwords from accounts or data files. When in the hands of an attacker, these same tools allow access to confidential information and represent a security and privacy threat.

A **key-logger** is a software program that captures keystrokes entered on the computer for the purpose of stealing information, like IDs and passwords. Often, this information is stored in a file that is later retrieved by or transmitted to a hacker to compromise a system or gain access to private company information.

A **joke** is a piece of software that has no malicious payload or use, and does not impact security or privacy states, but that may alarm or annoy someone.

[Back to top](#)

Many Computer Users Are Unaware

Industry analysts at IDC estimate that 67 percent of all computers have some form of spyware. In many cases, there are multiple on a single computer.* Many, if not most, computer users are

unaware that they have these programs on their computers and they generally don't know what to do about it.

Financial gain is the top motivator that is driving the accelerated growth of spyware. Random outbreaks have given way to organized, targeted attacks that harvest valuable information and control of the computer resources. The cost to homes and businesses is in the millions of dollars.

[Back to top](#)

Tips for Avoiding Spyware

1. Keep your operating system and browser updated.
2. Use a hardware firewall or [software firewall](#) like McAfee® VirusScan® Plus.
3. Use and regularly update a quality [anti-virus program](#) like McAfee VirusScan Plus.
4. Use and regularly update a quality [anti-spyware program](#) like McAfee VirusScan Plus.
5. Read all EULAs and privacy policies carefully. If you see terms that seem questionable, don't install the software.
6. Use a web browser that is less targeted (like Mozilla Firefox).
7. Be wary of "free" software, which is often offered without requiring payment in exchange for accepting other (spyware) software.
8. Don't normally run as administrator; set up a regular user account for day-to-day work, and log on as administrator only to install updates, etc.
9. Think about what software you actually need on your computer. Can you do without that screensaver or those smileys (emoticons)?
10. Never click on links in email unless you can verify that a person known to you sent it intentionally.
11. Beware of pornography, online gambling, get-rich-quick, and other high-risk web sites.

[McAfee SiteAdvisor™](#) provides web-site ratings to help you avoid these types of sites.

*Rose Ryan, J.D. and Brian E. Burke, IDC, *Spyware: Trademark Infringement or Legitimate*