

Spyware is a general term used to describe software that performs certain behaviors, generally without appropriately obtaining your consent first, such as:

- **Deceptive functionality.** Spyware often uses a classic "trojan horse" tactic--like a virus. It offers to synchronize your PC's clock or keep track of forms, but it is also doing other hidden things while you browse.
- **Home page hijacking.** Did you ever find that your home page was changed, or discover new sites in Favorites that you didn't add? It might be spyware.
- **Loss of privacy.** Some spyware keeps track of the web sites you visit and sends that information back to the spyware vendor. Do you want to tell everyone?
- **More advertising.** Did you install a popup stopper but you are still getting popups? The ads you are getting may not be from the web site you are on, but from spyware.
- **Stolen advertising.** Instead of showing the ads that should appear on a web site, some spyware substitutes its own ads which can rob a web site of revenue.
- **Broken web sites.** Spyware sometimes changes the actual content on a web page, and in the process it "breaks" the page. The page may not look correct, or you may get Javascript errors.
- **Reduced performance.** Spyware uses up system resources, CPU time, memory, disk space, and Internet bandwidth, making your system slower.
- **System instability.** Most spyware isn't very well tested or debugged, and there is no way to report bugs or obtain tech support. The result can be system crashes, hangs, or other strange behavior.
- **Security risks.** Some spyware has a built-in update feature that lets the spyware maker download and install new code to your system without your knowledge or approval.

Spyware is often associated with software that displays advertisements (called adware) or software that tracks personal or sensitive information.

Trading tracking for services

That does not mean all software that provides ads or tracks your online activities is bad. For example, you might sign up for a free music service, but you "pay" for the service by agreeing to receive targeted ads. If you understand the terms and agree to them, you may have decided that it is a fair tradeoff. You might also agree to let the company track your online activities to determine which ads to show you.

What spyware does

Other kinds of spyware make changes to your computer that can be annoying and can cause your computer slow down or crash.

These programs can change your Web browser's home page or search page, or add additional components to your browser you don't need or want. They also make it very difficult for you to change your settings back to the way you had them.

Know what you're installing

The key in all cases is whether or not you (or someone who uses your computer) understand what the software will do and have agreed to install the software on your computer.

A common trick is to covertly install the software during the installation of other software you want such as a music or video file sharing program.

Whenever you install something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes the inclusion of unwanted software in a given software installation is documented, but it might appear at the end of a license agreement or privacy statement.

There are a number of ways spyware or other unwanted software can get on your computer. To learn more about spyware,

Here are several ways you can help protect your computer against spyware and other unwanted software.

Step 1: Use a firewall

While most spyware and other unwanted software come bundled with other programs or originate from unscrupulous Web sites, a small amount of spyware can actually be placed on your computer remotely by hackers. Installing a firewall or using the firewall that's built into Windows Vista and Windows XP provides a helpful defense against these hackers.

Step 2: Update your software

Visit [Microsoft Update](#) to confirm that you have automatic updating turned on and that you've downloaded and installed all the latest critical and security updates.

Step 3: Adjust Internet Explorer security settings

You can adjust your Internet Explorer Web browser's security settings to determine how much-or how little-information you want to accept from a Web site.

Microsoft recommends that you set the security settings for the **Internet zone** to **Medium** or higher. (If you use Windows 7, Windows Vista or Windows XP Service Pack 2 (SP2) and you use Internet Explorer to browse the Web, your browser security settings for the Internet zone are set to Medium by default.)

To view your current Internet Explorer security settings:

1. In Internet Explorer, click **Tools** and then click **Internet Options**.
2. Select the **Security** tab.

For more information about security in Internet Explorer, see [Change Internet Explorer Security Settings](#).

[Internet Explorer](#) also includes a number of features to help protect against spyware and many other kinds of deceptive or unwanted software.

Step 4: Download and install antispware protection

An excellent application for Spyware & Malware removal is [SPYBOT Search & Destroy](#). [Microsoft Security Essentials](#) helps protect your computer from spyware and other unwanted software. It's available as a no-cost download for Windows XP SP2 and higher, Windows Vista, and Windows 7.

Step 5: Surf and download more safely

The best defense against spyware and other unwanted software is not to download it in the first place. Here are a few helpful tips that can protect you from downloading software you don't want:

- Only download programs from Web sites you trust. If you're not sure whether to trust a program you are considering downloading, enter the name of the program into your favorite search engine to see if anyone else has reported that it contains spyware.
- Read all security warnings, license agreements, and privacy statements associated with any software you download.
- Never click "Agree" or "OK" to close a window. Instead, click the red "x" in the corner of the window or press **Alt + F4** on your keyboard to close a window.
- Be wary of popular "free" music and movie file-sharing programs, and be sure you understand all of the software packaged with those programs.
- Use a standard user account instead of an administrator account. For more information, see [Why use a standard account instead of an administrator account](#).