Microsoft

Security At Home > Fight Spyware

What you should know about spyware

Published: April 16, 2004

We've all heard the cliche, "There's no such thing as a free lunch." This is as true on the Internet as anywhere else. Whether it's through advertising, or through the use of your personal information, you're going to have to pay somehow. The key is to understand what you're agreeing to and what you're willing to pay for something that claims to be free.

There's a new type of software out there that you may have heard about. It's called spyware and the most common way it gets on your computer is when you are downloading something else that claims to be free.

What is spyware?

Spyware is software that collects personal information from you without first letting you know what it's doing and without letting you decide whether this is OK or not. The information spyware collects can range from all the Web sites you visit to more sensitive information like usernames and passwords. You might be the target of spyware if you download music from file-sharing programs, free games from sites you don't trust, or other software programs from an unknown source.

Spyware is often associated with software that displays advertisements, called adware. Some advertisers may covertly install adware on your system and generate a stream of unsolicited advertisements that can clutter your desktop and affect your productivity. The advertisements may also contain pornographic or other material that you might find inappropriate. The extra processing required to track you or to display advertisements can tax your computer and hurt your system performance.

This is not to say that all software which provides ads or tracks your online activities is bad. If you sign up for a free music service and in return for that free service the company offers you targeted advertisements, it might be a fair tradeoff. Likewise, tracking online activities can be useful when displaying customized search content or personalized preferences at an online retailer.

The key is whether or not you (or another user of your computer) have been properly notified of what the software will do and that you have provided consent to have that software installed on your computer. In other words, is the software being deceptive in what it does or how it gets onto your computer?

⇡ Top of page

What is deceptive software?

Spyware and unauthorized adware are two examples of "deceptive" software. Deceptive software includes programs which take over your home page or

Related Links

- Cleaning Out Your PC Part I
- Cleaning Out Your PC Part II
- Working With Internet Explorer 6 Security Settings

What If I Agree To View Ads?
It's important to point out that are some situations in which the display of advertisements may benefit you. For example, you may be able to get a valuable service for free, such as internet access, if you agree to the display of advertisements during the use of that service.

Whether this is a fair deal is something you need to decide. What's important is that you are easily able to discover and understand the terms of that agreement and that you have the final say whether they are acceptable. You should be able to control what software runs on your computer.

Spyware vs. Cookies
Legitimate Web sites don't infect computers with spyware, but they do sometimes add tiny files to your computer called cookies. Cookies will remember information about you so that when you return to a Web site you won't have to enter everything again.

The website that created the

search page without first getting your permission. There are a number of ways deceptive software can get on your system. 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 are installing something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes the inclusion of adware in a given software installation is documented, but it may appear at the end of a license agreement or privacy statement.

Sometimes deceptive software gets silently installed on your system without any warning at all. If you use Internet Explorer as your Web browser, this can happen if your Internet Explorer security setting is set to its lowest value. Make sure to keep this setting at the medium level or higher. Doing so will help you control what is being installed on your computer. (We'll discuss this more in a moment.)

Have you ever had an experience where you were repeatedly asked to accept a download even after you said "no"? Creators of deceptive software often use such tricks to get you to load their software. If this happens to you, do not click "yes". Instead, try to close the Web page that first asked you to accept the download by hitting the "X" in the corner of the window. Alternatively, quit Internet Explorer and restart it to begin browsing the Internet again. If you visit a Web page that continually displays these tricky pop-up windows, that Web site may not be worthy of your trust.

Read on to learn how to help avoid infecting your computer with deceptive software and to find out what to do if you are already infected.

Top of page

Step 1: Adjust your Internet Explorer 6 (Web browser) security settings

You can adjust your Web browser's security settings to determine how much—or how little—information you are willing to accept from a Web site. The higher the security level, the lower the risk. The downside: using the highest security levels may make Web sites less usable.

By default, Internet Explorer 6 strikes a balance. When you first install Internet Explorer, it classifies all Web sites into a single zone (the Internet zone) and assigns everything medium level security. When you are using this level of security, Internet Explorer should ask you to confirm that you want to download a file, unless you have previously indicated that the Web site or publisher is trusted. If you change the security level to "low," Web sites will be able to download software to your computer without telling you, so be careful when using this setting. If you need to change the security level to low for some reason, change it back to medium or higher as soon as possible.

Tip: Working With Internet Explorer 6 Security Settings includes step-by-step instructions for adjusting your Internet Explorer 6 security settings.

Top of page

Step 2: Don't take downloads from strangers

The best defense against deceptive software is not to download it in the first place. Here are a few helpful tips that may help guard against deceptive software.

- **Install software only from Web sites you trust.** Before you download anything from a Web site, ask yourself if you would feel comfortable doing business with that Web site. If the answer is no, then don't

cookie is responsible for disclosing to you what is in the cookie and what the cookie is for. This is usually done in a privacy statement posted on the website. You should be suspicious of sites that do not disclose this information.

Can an Internet Firewall or Antivirus Software Program Help?
Although it is important to turn on your firewall, run an antivirus program, and keep your software up to date, none of these measures are guaranteed to keep you from downloading deceptive software. Special detection and removal software is available to help you find and remove unwanted software on your computer.

Some Well Known Tools That May Help Detect and Remove Unwanted Software

- Lavasoft Ad Aware
- Spybot Search & Destroy (S&D)

Please note that Microsoft is not responsible for the quality, performance, or reliability of these third party tools.

download the software. If you aren't sure, do some research, such as asking friends or checking other resources you trust.

- **Read the fine print.** When you install any program make sure you read the message on each window before you click "Agree" or "OK." You should also carefully read any license agreements or privacy statements associated with the software. You may discover behaviors you find objectionable. If the window will not let you click "No" or "I do not accept", close the window by clicking on the "X" in the corner. Never click "Yes" or "I accept" just to get rid of the window.
- **Be wary of popular "free" music and movie file-sharing programs.** Statistics show that many people get deceptive software on their system from these programs. To use the analogy of your house, when you install file-sharing programs you are literally leaving your front door open. Besides the obvious risks of having someone steal something from you, they can also leave things behind that you may not want around.

Top of page

Step 3: Look for signs of deceptive software on your computer

Deceptive software is intended to run without your knowledge, but there are a few ways you can tell if your system is infected.

- **When you start your Internet browser, does it open to a page you've never seen before?** When you select "search", are you taken to a page you do not recognize? Some deceptive software will alter these settings without your knowledge.
- **Do you see a sudden increase in advertisements on pages where you've never seen them before?** Deceptive software sometimes bombards you with pop-up ads no matter what page you visit. These ads are often for adult or other Web sites you may find objectionable.
- **Does your computer seem sluggish?** Deceptive software is not necessarily designed to be efficient. The resources it uses to track your activities and deliver advertisements can slow down your computer and bugs in the software can make your computer crash.

Top of page

Step 4: Use a tool to help detect and remove unwanted software

Several companies offer free software that will check your computer for unwanted software. These tools may help you determine if you have installed unwanted software and may help you remove it.

If your Internet provider doesn't offer a spyware removal (or similar) tool, ask people you trust for a tool they recommend. Keep in mind that removing unwanted software with these tools may mean you will no longer be able to use a free program that may have come with it.

Tip: Keep your detection and removal tool up to date. Many manufacturers offer an option to check for updates automatically when you go online. If this feature isn't available, check the manufacturer's Web site regularly for downloads. Either way, be sure to update frequently.

Top of page

Step 5: Keep Windows up to date

The last step in helping keep yourself safe from deceptive software is making sure your Windows software is always current. You can do this by visiting Windows Update and by enabling Automatic Updates. For detailed instructions, see our story about updating your Microsoft software.

Top of page

Take time to protect your personal information

Keeping your computer off of the Internet will help you avoid deceptive software—but that wouldn't be practical. You can still enjoy all that the Internet has to offer. Just be cautious about who you do business with online, especially if something appears to be free. The hidden cost might be uninvited spyware or adware. A good question to ask yourself is "Would I let this stranger into my house?"

⇧ Top of page

Manage Your Profile