



IT Alley

4742 42nd Ave SW #272
Seattle, WA 98116-4553
www.italleypllc.com
sales@italleypllc.com

WHAT'S THE DIFFERENCE BETWEEN SPYWARE AND VIRUSES

Published: February 17, 2007

Source: www.microsoft.com

Please note this article was written in 2007 when installing recommended software download the newest versions.

Spyware and viruses are both forms of unwanted or malicious software, sometimes called "malware." You need to protect yourself from both.

What's the difference?

- **Spyware** (sometimes called adware) collects information about you without appropriate notice and consent.
- A computer **virus** spreads software, usually malicious in nature, from computer to computer.

Spyware can get installed on your computer in a number of ways. One way is through a virus. Another way is for it to be secretly downloaded and installed with other software you've chosen to install.

In short, spyware is a specific type of unwanted software that secretly collects your information.

A virus is a specific way software can be secretly distributed, often by e-mail or instant messaging.

Both spyware and viruses can cause damage to your computer or cause you to lose important data.

To help protect against spyware, try [Windows Defender](#). (Windows Defender is [built into Windows Vista](#).)

What is Spyware?

Spyware is a general term used to describe software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent first.

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

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.

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. These programs also make it very difficult for you to change your settings back to the way you originally had them.

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.

There are a number of ways spyware or other unwanted software can get on your computer. To learn more about spyware, read [How to help prevent spyware](#). 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.

[Sings of Spyware: Are you being watched?](#)

If your computer starts to behave strangely or displays any of the symptoms listed below, you may have spyware or other unwanted software installed on your computer.

- **I see pop-up advertisements all the time.** Some unwanted software will bombard you with pop-up ads that aren't related to a particular Web site you're visiting. These ads are often for adult or other Web sites you may find objectionable. If you see pop-up ads as soon as you turn on your computer or when you're not even browsing the Web, you may have spyware or other unwanted software on your computer.
- **My settings have changed and I can't change them back to the way they were.** Some unwanted software has the ability to change your home page or search page settings. This means that the page that opens first when you start your Internet browser or the page that appears when you select "search" may be pages that you do not recognize. Even if you know how to adjust these settings, you may find that they revert back every time you restart your computer.
- **My Web browser contains additional components that I don't remember downloading.** Spyware and other unwanted software can add additional toolbars to your Web browser that you don't want or need. Even if you know how to remove these toolbars, they may return each time you restart your computer.
- **My computer seems sluggish.** Spyware and other unwanted software are not necessarily designed to be efficient. The resources these programs use to track your activities and deliver advertisements can slow down your computer and errors in the software can make your computer crash.

If you notice a sudden increase in the number of times a certain program crashes, or if your computer is slower than normal at performing routine tasks, you may have spyware or other unwanted software on your machine.

If you think your computer is infected with spyware, find out [how to get rid of spyware](#) and how you can [prevent spyware](#) from getting on your computer.

How to help prevent spyware

[Spyware](#) and other unwanted software can invade your privacy, bombard you with pop-up windows, slow down your computer, and even make your computer crash. 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 XP provides a helpful defense against these hackers.

To learn more about firewalls, read [Why you should use a computer firewall](#) and get answers to your [Frequently asked questions about firewalls](#).

STEP 2: UPDATE YOUR SOFTWARE

If you use Windows XP, one way to help prevent spyware and other unwanted software is to make sure all your software is updated. Visit [Microsoft Update](#) to confirm that you have Automatic Updates turned on and that you've downloaded 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 are willing to accept from a Web site. Microsoft recommends that you set the security settings for the **Internet zone** to **Medium** or higher.

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 a step-by-step guide to adjusting your settings without blocking content from sites that you trust, see [Working with Internet Explorer 6 Security Settings](#).

If you're running Windows XP Service Pack 2 (SP2) and you use Internet Explorer to browse the Web, your browser security settings for the Internet zone are already set to Medium by default. Internet Explorer in Windows XP SP2 also includes a number of

features to help protect against spyware and many other kinds of deceptive or unwanted software.



Tip: Don't know which version of Windows your computer is running? [Find out.](#)

STEP 4: DOWNLOAD AND INSTALL ANTISPYWARE PROTECTION

Windows Defender protects your computer from spyware and other unwanted software. Windows Defender comes with [Windows Vista](#) and you can [download it](#) for no charge for Windows XP SP2. For more information, see [Windows Vista: Windows Defender](#).

Additional security tools to help block, detect, and remove unwanted software from your computer are available on our [Security Downloads](#) resources page.

Note: Microsoft is not responsible for the quality, performance, or reliability of third-party tools.

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, ask a knowledgeable friend or 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 the **Alt + F4** buttons on your keyboard to close a window.
- Be wary of popular "free" music and movie file-sharing programs, and be sure you clearly understand all of the software packaged with those programs.

[Signs of viruses: Are you infected?](#)

After you open and run an infected program or attachment on your computer, you might not realize that you've introduced a virus until you notice something isn't quite right.

Here are a few primary indicators that your computer *might* be infected:

- Your computer runs more slowly than normal
- Your computer stops responding or locks up often
- Your computer crashes and restarts every few minutes
- Your computer restarts on its own and then fails to run normally
- Applications on your computer don't work correctly
- Disks or disk drives are inaccessible
- You can't print correctly
- You see unusual error messages
- You see distorted menus and dialog boxes

These are common signs of infection—but they might also indicate hardware or software problems that have nothing to do with a virus. Unless you run the [Microsoft Malicious Software Removal Tool](#) and install industry-standard, up-to-date [antivirus software](#) on your computer, there is no way to be certain if your computer is infected with a virus or not. If you don't have current antivirus software installed or if you're interested in installing a different brand, you can try [Windows Live OneCare free for 90 days](#) or visit our [Security software downloads page](#) for software from other companies.



Tip: Beware of messages warning you that you sent e-mail that contained a virus.

This can indicate that the virus has listed your e-mail address as the sender of tainted e-mail. This does not necessarily mean you have a virus. Some viruses have the ability to forge e-mail addresses.

Help avoid computer viruses that spread through e-mail attachments

Many of the most common [computer viruses and other malicious software](#) are spread through e-mail attachments—the files that are sent along with an e-mail message. If a

file attached to an e-mail message contains a virus, it's often launched when you open the file attachment (usually by double-clicking the attachment icon). No matter what e-mail program you use or what version of Windows you're running, you can help avoid some viruses by following a few basic rules. If you use the latest version of Outlook or Outlook Express and if you use the latest version of Windows, there are a few unique enhancements and default settings to help keep you from accidentally infecting your computer with a virus. Read on to learn more.

5 TIPS FOR DEALING WITH E-MAIL ATTACHMENTS

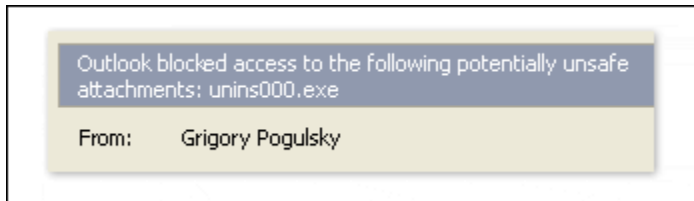
Follow these basic guidelines when dealing with attachments in an e-mail message, no matter what e-mail program you're using:

1. Don't open any attachment unless you know whom it's from *and* you were expecting it.
2. If you receive an e-mail message with an attachment from someone you don't know, delete it immediately.
3. Use antivirus software and keep it updated.
4. If you need to send an e-mail attachment to someone, let them know you'll be sending it so they don't think it's a virus.
5. [Use spam filters](#) to help block unwanted e-mail, much of which contains dangerous attachments. For information on how to do this with Outlook, see [Update junk e-mail filters for Outlook](#).

Important: Microsoft and other reputable companies will never send you unsolicited e-mails that contain attachments. If you receive an e-mail attachment that appears to come from Microsoft, it may contain a virus, [spyware](#), or another [e-mail scam designed to steal your identity](#). Delete the e-mail immediately.

DEALING WITH E-MAIL ATTACHMENTS IN MICROSOFT OUTLOOK

Microsoft Outlook can block potentially unsafe attachments before they get to you. For example, if you're using Outlook 2003 and you receive an e-mail with an attachment that could contain a virus, you'll see the warning below.



An example of an e-mail attachment blocked by Outlook 2003.

If you know that an attachment is safe and need to know how to unblock it, see [About unblocking attachments](#). If you'd like to learn more about why Outlook blocks certain attachments and not others, see [Blocked attachments: The Outlook feature you love to hate](#).

DEALING WITH E-MAIL ATTACHMENTS IN OUTLOOK EXPRESS

If you use Outlook Express, you can greatly increase your chances of avoiding viruses, worms, and Trojans by upgrading to [Windows XP Service Pack 2 \(SP2\)](#). With SP2, Outlook Express will block potentially harmful attachments by default and has numerous other features that help prevent viruses and other malware. If you use Outlook Express, but you're not sure what operating system you're running, visit [Find out which operating system your computer is using](#). If you're not using Windows XP SP2, you can check your virus protection settings manually.

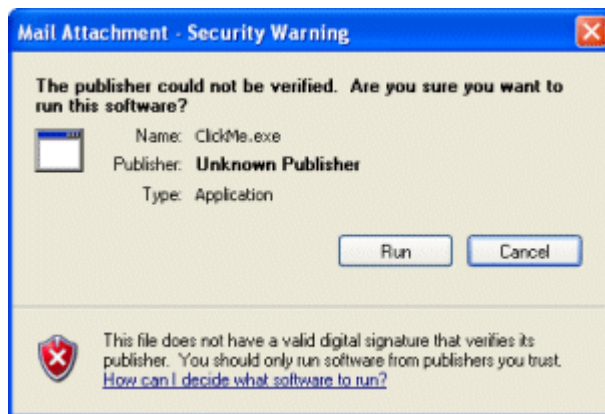
To ensure your e-mail virus protection is turned on in Outlook Express

1. On the **Tools** menu, click **Options**.
2. Click the **Security** tab.
3. Select the **Do not allow attachments to be saved or opened that could potentially be a virus** check box.
4. Click **OK**.

To open an attachment that you know to be safe

1. On the **Tools** menu, click **Options**.
2. Click the **Security** tab.
3. Clear the **Do not allow attachments to be saved or opened that could potentially be a virus** check box.
4. Click **OK**.
5. Close and reopen the message with the attachment that you know to be safe.
6. Open the attachment.
7. Repeat Steps 1 and 2. Then select the **Do not allow attachments to be saved or opened that could potentially be a virus** check box.

If you're running Windows XP SP2 you may be given one more warning, such as the one you see below.



Security warning

Always use caution before clicking **Run**, as that could install a virus or other potentially dangerous program.