What are spyware and adware?

Although they may sometimes be confused with one another, spyware and adware are different. Spyware is a program or technology that aids in gathering information about a person or organization, often without their knowledge, and includes programs like hijackers and keyloggers. Adware is typically a program that displays advertising through pop-up or pop-under windows while you are surfing the Web.

You may have unknowingly installed spyware or adware when you downloaded programs from the Internet or installed software from disks. Spyware is easy to install but often difficult to remove without downloading specialized anti-spyware programs.

Many applications may display a window or interrupt your activities while you are using your computer. For example, Yahoo! Messenger may display an alert or a chat window from time to time, either of which may contain an advertisement. Most people do not classify these kinds of communications as adware because they were initiated for a purpose other than advertising.

How Spyware Gets Installed

Here are a few potential ways spyware and adware may find their way onto your computer. Please keep in mind, this is not a comprehensive list:

Unintentional Download

You may intentionally download and install spyware or adware without realizing it has an unrelated, secondary purpose that isn't always clearly disclosed. For example, you may be told a program will keep your computer clock synchronized with the atomic clock. If it is spyware or adware, the program may also send information about your browsing habits or display advertising pop-ups whenever you are online.

Software Bundle

Spyware and adware may be included (bundled) with programs you download and install. For example, many file-sharing programs require you install additional, unrelated programs that may be considered spyware or adware.

Involuntary Download

You may voluntarily but unintentionally install spyware or adware while surfing the Web. Often times, spyware or adware appears to be corrective software or a special plug-in that will help you view a site. If you don't know the source of the download or aren't sure what a program does, you can generally learn more by searching on the name of that program in Yahoo! Search.

Other Users

Someone else who uses your computer may also install spyware or adware on your computer. They may do so unintentionally in any of the ways mentioned above, or they may maliciously install a program with keystroke logging, to capture passwords or other personal information.
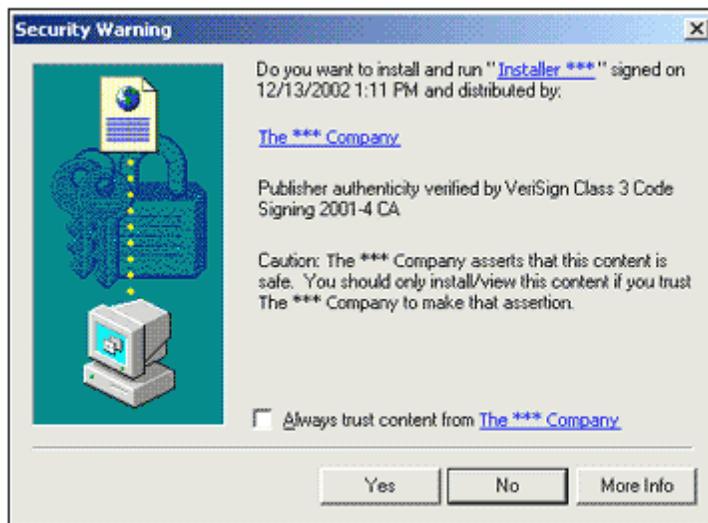
Computer Virus or Worm

A computer virus or worm can also install spyware that could allow someone remote access to your computer, turn your computer into a pornography or spam server, log keystrokes to steal

passwords or credit cards, or perform other malicious acts.

Automatic Installation

Some unscrupulous companies use advertisements to automatically begin the installation process for their programs. By default, most browsers will prompt you with a security warning to either continue or stop the installation process. Typically, these warnings don't offer a description of the program or tell you what it will do.

Browsers that allow programs to install without a prompt are security threats and make your computer more susceptible to computer viruses and hacking attempts. Please review documentation for your browser to learn more about how to protect your security. Remember to **carefully read pop-up warnings**. If you don't expect to install a program or if you aren't sure what the program does, cancel the installation process. Here is an example of one such warning, given in Microsoft Internet Explorer:

In this example, the company name and the program name have been modified. There is no information about what the program does.

Note: The browser provides the security warning, and the same message is shown during the installation of many different programs.

It is Yahoo!'s policy not to accept advertising that deceives consumers into installing software. If an advertisement on Yahoo! appears to start installing software without your consent, write down the details from the Security Warning, click "No," and then scan your computer for spyware and adware. If no spyware or adware is found, please contact us and include the details from the Security Warning.

Avoiding Spyware

Here are some steps you can take to avoid spyware:

Regularly use anti-spyware software in conjunction with anti-virus software to give your computer maximum protection against spyware and other malicious computer programs. Yahoo! offers an anti-spyware solution as part of the Yahoo! Toolbar Beta. Simply download the Yahoo! Toolbar and run the Yahoo! Anti-Spy program to find and remove spyware and adware. Anti-spyware software may also be available from your ISP or elsewhere online.

Verify the security settings on your browser do not allow programs to be installed without your permission. By default, most browsers will prompt you with a security warning to continue or stop the installation process.

Carefully read pop-up warnings. If you don't expect to install a program or if you aren't sure what the program does, cancel the installation process.

Before downloading and installing programs, investigate them and their publisher. You can generally find more information by searching for the name of the program in Yahoo! Search.

--Excerpt from "PCPitstop.com"--

Dirty Spyware Tricks

If you had a complete knowledge of what most spyware was doing to your system, you would never agree to install it. So how does it end up installed on so many PCs? Here are some of the dirty tricks that spyware uses to worm its way onto your system and stay there. (Not all spyware uses every technique.)

1) Hide inside another program's installer.

You will often see this technique in peer-to-peer programs like Kazaa. Hundreds of "freeware" programs install some form of spyware along with the main application. In some cases the spyware is relatively innocuous, but in others it can crash your system or invade your privacy. The only hint you may see is a short sentence or two in the end user license agreement (EULA) to the effect of "third party software may be installed along with the application."

2) Use confusing legalese.

The license agreements don't just come out and say "we're going to collect information and screw up your browsing" since that wouldn't get them a lot of customers. Instead, the licenses are full of vague and confusing prose.

3) Keep asking until you say *Yes*.

This is particularly common with drive-by downloads. Some spyware is delivered by an ActiveX control that tries to load each time you visit a web page where the spyware is present. As a security measure, the browser will ask if you want to install. If you say *No* it's only good until the next web page you load, where you'll again be asked the question. After a few pages of this, some people will give up and say *Yes*. (A better move would be to give up and leave that site.)

4) Create a false pretense for needing the software.

You get this email message from a friend: "I've just sent you a greeting card, go to this web site to read it!" When you get to the web site it asks you to install a "greeting card viewer" that turns out to be spyware, and it sends a similar card to everyone in your address book. In the license agreement you didn't read but agreed to, you gave it permission to do that!

5) Look essential, or be invisible.

Some spyware will use an official-sounding name like "winstartup" so that you'll be less likely to disable it if you see it running. Others maintain a low profile by using dozens of different file names and locations, or even generating a random file name to escape detection. To further mask its existence and reduce your awareness of it, many spyware packages will even install software updates without your knowledge.

6) Don't uninstall, even when asked.

Whether by design or mistake, a lot of spyware does not remove itself when you uninstall the application that originally installed the spyware. In many cases the only way to completely remove spyware is with a utility like Pest Patrol.

Some useful tools to help control and remove Spyware & Adware.

- www.javacoolsoftware.com (spywareblaster) *FREE
- www.spybot.info (Spybot) *FREE
- www.lavasoft.de (Ad Aware) *FREE
- www.pestpatrol.com (Pest Patrol) *Not FREE
- www.webroot.com (Spy Sweeper) *Trial for 30 days

Top 25 Spware

This Week	Last Week	Prevalence	File Name	Description
1	1	2.171	mwsoemon.exe	MyWebSearch toolbar
2	2	1.721	webrebates1.exe	TopRebates hijacker/adware
3	5	1.717	wsup.exe	HuntBar spyware
4	4	1.706	wtoolsa.exe	HuntBar spyware
5	3	1.692	webrebates0.exe	TopRebates hijacker/adware
6	6	1.529	gmt.exe	Gator adware
7	7	1.483	cmesys.exe	Gator adware
8	8	1.332	wtoolss.exe	HuntBar spyware
9	9	1.05	optimize.exe	MoneyTree Dialer
10	10	0.966	bargains.exe	Bargain Buddy
11	11	0.655	save.exe	WhenU SaveNow adware
12	12	0.583	msbb.exe	180Solutions adware
13	17	0.55	precisiontime.exe	Gator adware
14	13	0.544	actalert.exe	MoneyTree Dialer
15	14	0.533	istsvc.exe	IST adware/hijacker
16	15	0.521	asm.exe	Brilliant Digital Spyware
17	21	0.439	dmserver.exe	Comet Download Manager
18	19	0.404	nls.exe	Navisearch / TopRebates
19	18	0.395	autoupdate.exe	Apropos Media adware
20	22	0.389	updmgr.exe	KeenValue spyware
21	20	0.381	vvsn.exe	WhenU ClockSync
22	25	0.36	sync.exe	WhenU Adware
23	27	0.353	gamechannel.exe	WildTangent/Game Channel
24	26	0.307	points manager.exe	TopSearch Points Manager
25	24	0.28	hbinst.exe	Hotbar adware/spyware