

Hello Friend,

Thank you taking the time to download, read this manual, and secure your computer(s)

Topics covered in this manual

- Getting Started.
- What is Spyware – the definition.
- What is a computer virus – the definition.
- How did my computer get infected?
- Other methods of infection.
- How can I prevent infections?
- Tools for spyware removal, virus removal, and protection.
- Keeping your machine clean.
- Bonus Links.

Getting Started

I'm glad to see you have decided to prevent the spreading of spyware by cleaning and preventing spyware infections on your computer(s).

Thank you for being a responsible Internet user. Your fellow netizens are smiling. Let's get started by learning a bit about these pesky bugs.

What is Spyware?

Spyware as a category overlaps with adware. The more unethical forms of adware tend to coalesce with spyware. Malware uses spyware for explicitly illegal purposes. Exceptionally, many web browser toolbars may count as spyware.

Data collecting programs installed with the user's knowledge do not, technically speaking, constitute spyware, provided the user fully understands what data they collect and with whom they share it. However, a growing number of legitimate software titles install secondary programs to collect data or distribute advertisement content without properly informing the user about the real nature of those programs. These barnacles can drastically impair system performance, and frequently abuse network resources. In addition to slowing down throughput, they are often have design features making them difficult or impossible to remove from the system.

What is a Computer Virus?

Spyware can closely resemble computer viruses, but with some important differences. Many spyware programs install without the user's knowledge or consent. In both cases, system instability commonly results.

A virus, however, replicates itself: it spreads copies of itself to other computers if it can. Spyware generally does not self-replicate. Whereas a virus relies on users with poor security habits in order to spread, and spreads so far as possible in an unobtrusive way (in order to avoid detection and removal), spyware usually relies on persuading ignorant or credulous users to download and install it by offering some kind of bait. One typical spyware program targeted at children, for example, claims that:

“He will explore the Internet with you as your very own friend and sidekick! He can talk, walk, joke, browse, search, e-mail, and download like no other friend you've ever had! He even has the ability to compare prices on the products you love and help you save money! Best of all, he's FREE!” (also known as Bonzia Buddy)

A typical piece of spyware installs itself in such a way that it starts up every time the computer starts up (using CPU cycles and RAM, and reducing stability), and runs at all times, monitoring Internet usage and delivering targeted advertising to the affected system. It does not, however, attempt to replicate onto other computers it functions as a parasite but not as an infection.

A virus generally aims to carry a payload of some kind. This may do some damage to the user's system (such as, for example, deleting certain files), may make the machine vulnerable to further attacks by opening up a "back door", or may put the machine under the control of malicious third parties for the purposes of spamming or denial of service attacks. The virus will in almost every case also seek to replicate itself onto other computers. In other words, it functions not only as a parasite, but as an infection as well.

The damage caused by spyware, in contrast, usually occurs incidentally to the primary function of the program. Spyware generally does not damage the user's data files; indeed (apart from the intentional privacy invasion and bandwidth theft), the overwhelming majority of the harm inflicted by spyware comes about simply as an unintended by-product of the data-gathering or other primary purpose.

A virus does deliberate damage (to system software, or data, or both); spyware does accidental damage (usually only to the system software). In general, neither one can damage the computer hardware itself (but see CIH virus). Certain special circumstances aside, in the worst case the user will need to reformat the hard drive, reinstall the operating system and restore from backups. This can prove expensive in terms of repair costs, lost time and productivity. Instances have occurred of owners of badly spyware-infected systems purchasing entire new computers in the belief that an existing system "has become too slow."

How did my computer get infected?

Spyware normally installs itself through one of three methods:

- 1) The spyware component comes bundled with an otherwise apparently useful program. The makers of such packages usually make them available for download free of charge, so as to encourage wide uptake of the spyware component. This applies especially with file-sharing clients such as Kazaa and earlier versions of Bearshare. (To address this concern and to discourage the U.S. Congress from regulating the P2P "industry", P2P United formed to promise informed consent and easy removal. Kazaa does not form part of P2P United. -- Note furthermore that anti-spyware removers generally do not remove spyware applications from their databases because of such changes. (Lavasoft has come under criticism from some on their support forums for reaching agreements with former vendors of spyware to be removed from their database. Lavasoft representatives say they remove spyware if it no longer meets their inclusion criteria.)
- 2) The spyware takes advantage of security flaws in Internet Explorer.
- 3) Internet Explorer can also install spyware on your computer either via a drive-by download (with or without any prompt. A drive-by download takes advantage of easy installation via an ActiveX control (or several ActiveX components) with or without a prompt, depending on security settings within Internet Explorer.

Other Methods of Infection

Spyware can also install itself on a computer via a virus or an e-mail Trojan program, but this does not commonly occur.

An HTTP cookie, a well-known mechanism for storing information about Internet users on their own computers, often stores an individual identification number for subsequent recognition of a website visitor. However, the existence of cookies and their use generally does not hide from users, who can also disallow access to cookie information. Nevertheless, to the extent that a Web site uses a cookie identifier (ID) to build a profile about the user, who does not know what information accumulates in this profile, the cookie mechanism could count as a form of spyware. For example, a search engine website could assign an individual ID code to a user the first time he or she visits and store all search terms in a database with this ID as a key on all subsequent visits (until the expiry or deletion of the cookie). The search engine could use this data to select advertisements to display to that user, or could legally or illegally transmit derived information to third parties.

Granting permission for web-based applications to integrate into one's system can also load spyware. These browser helper objects known as Browser Hijackers embed themselves as part of a web browser.

Spyware usually installs itself by some stealthy means. User agreements for software may make references (sometimes vague) to allowing the issuing company of the software to record users' Internet usage and website surfing. Some software vendors allow the option of buying the same product without this overhead.

How can I prevent Infection?

Use of automatic updates (on Windows systems), anti-virus, and other software upgrades will help to protect systems. Software bugs and exploits remaining in older software leave one vulnerable, because the public rapidly learns over time how to exploit unpatched systems.

A number of software applications exist to help computer users search for and remove spyware programs. (See sections Spyware Removal Programs) Some programs purge a system of spyware, only to install their own.

As some spyware takes advantages of Internet Explorer vulnerabilities, using a less vulnerable browser, such as Mozilla Firefox or Opera, may also help.

Disabling ActiveX in Internet Explorer also prevents some infections, however websites using ActiveX will not work in this case.

Currently-known spyware does not target non-Windows systems, such as those running Mac OS or Linux. However, browser cookies can attack such systems.

Tools for Spyware Removal and Virus Removal and Protection.

Windows XP, Windows 2000, Windows ME, Windows 98

I suggest you purchase [Panda Antivirus 2007 - \\$5 Discount Coupon](#). It is a complete protection suite, a great value for your money.

It is also PC Worlds "Best Buy" here is their recommendation

"we recommend Panda Software's Platinum Internet Security Our pick as Best Buy among the suites, Panda scored the highest of the three in total spyware removal..."

Take a minute and read about the benefits on [Pandas Product page](#)

Comes with the following protection

- 1) Antivirus
- 2) AntiSpyware
- 3) Protection from online fraud (banking and shopping)
- 4) AntiSpam
- 5) Automatic Updates
- 6) 24hour 365 day support
- 7) Firewall
- 8) Secure wireless connections
- 9) Privacy control
- 10) Web content filtering (if you have kids this is definitely needed)

While there are free programs available to help keep your system clean and they do offer some level of protection, I personally prefer using a Security Suite like [Panda Internet Security 2007](#) it is a much better solution. The components of the [Panda Internet Security 2007](#) are designed to compliment each other and work together to offer the best possible coverage.

Keeping your machine clean

Here are some things you can do to make your computer safer:

Don't use any file sharing (P2P) applications. This includes KaZaa, morpheus, iMesh, Limewire or grokster. You are not doing anything legal with it, and you are contributing to the spyware and trojan problem because many trojans propagate through the P2P networks. Plus, you might get sued by the RIAA or MPAA. It's not worth it, just buy the CD..

Don't use Internet Explorer as your browser. There are many alternatives, and in some cases the alternatives are better browsers. Of course, it's a matter of opinion, but it is fact that IE is the most easily exploitable and vulnerable browser. If you don't use IE, you will not experience ActiveX exploits or BHO infections any longer. I highly recommend Mozilla for novice users or Firebird for advanced users, since they have integrated popup blocking and tabbed browsing, which is an amazingly helpful feature. I would recommend against IE just because it is a common source of spyware infections.

Do not open any email attachments. I can't stress this enough. If you would stop opening email attachments that had "funny jokes" or "cute screensavers" or "hot babes", then the virus problem would be seriously reduced. Just don't bother. And never, ever believe the sender of the email. If your Aunt Sally's computer is infected with a virus, it will send you email, and it will look as if it is coming from her. "Oh, Aunt Sally would never send me a virus" you think, and so you open the cute screensaver that she sent you. Now you are infected, and you are a part of the problem. DON'T DO IT. I truly believe that the ability to attach files should be eliminated from email. There are better ways to transfer files. If you MUST open attachments, make SURE they don't have the following file extensions: .EXE, .SCR, .BAT, .PIF, .ZIP, .COM .. Also, watch out for "fake" file extensions, such as .JPG.EXE or .GIF.PIF .. The first three letters are designed to trick you. It's only the last three letters that count. If they are executable, you've just infected yourself.

Do not install any activeX controls. With the exception of a notable few such as WindowsUpdate control, Macromedia Flash, Macromedia Shockwave, or from your computer's manufacturer (Dell, Compaq, etc.) there are no safe ActiveX controls. If you don't use Internet Explorer, of course this won't be a problem. But if you are married to Internet Explorer as your browser, please observe diligence and safe browsing habits so that you aren't (say it with me now) part of the problem.

Don't visit questionable websites. There is nothing free on the internet, Spyware is distributed about the Internet by sites offering porn, casino gambling, free games, free screensavers, free desktop backgrounds, free tools, free organizers, you name it. There is nothing free. Don't believe it. If it's free, then that means they want you to agree to giving up your privacy in order to partake. And generally, that means installing spyware. If you install a "free" game, you are generally installing spyware on your computer. If you visit porn sites, don't be surprised when your computer starts getting porno pop ups all the time.

Use a good anti-virus product. You need it. If you can't afford a good antivirus program, there are acceptable free alternatives. They don't have all of the features I recommend, but some protection is better than no protection.

Check for updates daily. If you have a bad spyware infestation, you probably have a high-speed network connection such as cable or DSL. If you do, there is no excuse. You must update your anti-virus definitions daily. It takes seconds. Just do it. Also, check for windows updates at windowsupdate.microsoft.com while you're at it. Come on, you're not that busy. If you're stuck with dial-up, you have my condolences, but you still need to do it. Update virus definitions daily at the very least. Please.

Educate yourself. If you plan on spending a lot of time on the computer, you owe it to yourself and to the rest of the community to learn a bit more about the tools you are using, since computers can become a liability. You wouldn't want to get into a car and start driving around if you've never done it before and are unlicensed. A computer can cause a lot of damage in today's networked economy. Keep yours from becoming "part of the problem".

If you follow this guide, use the available tools, and practice safe surfing you can be spyware free.

Bonus Link:

On occasion I have utilized a free online scan and had good success in finding some bugs that other tools have missed (different tools utilize different scanning techniques). These online scans need ActiveX in order to work, so you will need to visit the online scan sites with MS Internet explorer. These online scans will not work with Mozilla browsers as Mozilla doesn't utilize ActiveX. Here are the links:

Panda Software <http://www.pandasoftware.com/activescan>

References:

Definitions are taken from Wikipedia, the free encyclopedia.
<http://en.wikipedia.org/wiki/Spyware>

<http://spyware-remover-help.com/>