

The Spyware Secrets Report



This Report is Copyright 2006 KN Dataservice, All Rights Reserved.

KN Dataservice grants all readers the rights to give away unlimited copies of this report. It may be given away by itself, bundled, in membership sites or on media as cd/dvd.

The report can not be sold by itself.

**[Get your own branded copy
of this report to give away here!](#)**

Disclaimer : Every effort has been made to accurately represent our product and it's potential. Each individual's results depends on his or her background, knowledge, computer, operatingsystem and other variables outside of our control. As with any software usage there is an inherent risk of loss of information or problems with your operating system or installed software. KN Dataservice can not be held responsible for any problems that may arise from using software or information included in this report. The reader must take the needed steps to secure their computer and its content before making changes or using any kind of software. The reader must also read and follow each manufacturers rules, guidelines and directions when using their software. The information found in this report may not be correct when read due to changes made to software by third parties.



<i>The Spyware Secrets Report</i> _____	1
<i>Spyware - Know Your Enemy</i> _____	3
How does spyware infect? _____	4
<i>How Common are Spyware</i> _____	6
<i>Spyware - Eradicate It Now</i> _____	7
<i>How to Remove Spyware</i> _____	9
Anti-spyware Programs _____	9
Protection and removal _____	10
<i>You need a spyware remover!</i> _____	11
What can Spyware do? _____	11
<i>Tools to Use</i> _____	12
Our number 1 choice _____	12



Spyware - Know Your Enemy

Spyware is a term that has become quite common to hear.

The term spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the “known” consent of that machine's owner or user. Spyware is as a term is being used quite loosely and includes a number of different programs. The thing they all have in common as spyware, is that they monitor the computer and/or user and share information with a third party. With or without the consent of the computer’s owner.

Semi spyware has become widely used and they manifest themselves as software, plugins or help files to other programs you want or need, and if you accept their policies and term of usage, you also accept the fact that these semi spyware programs will be installed and used.

They are normally not directly malicious as the secret spyware, but they do send out information from your computer to a third party. Most commonly some kind of habit tracing or statistics of surfing or similar. In most cases the information is completely anonymous and do not pose any kind of threat to you as an individual.

Spyware – a virus or not?

Spyware differs from viruses and worms in that it does not usually self-replicate. Like many recent viruses, however, spyware – by design – exploits infected computers for commercial gain.

Typical tactics furthering this goal include delivery of unsolicited pop-up advertisements; theft of personal information (including financial information such as credit card numbers); monitoring of Web-browsing activity for marketing purposes; or routing of HTTP requests to advertising sites.

These things are very hard to keep track of and know if a spyware is alive in your computer or if pop ups and other changes in your surfing programs behavior should occur.

The only reliable way to know if an evil spyware is living and thriving inside your computer, is to install and use a good spyware removal program.



How does spyware infect?

Spyware does not spread like a computer virus or worm. Instead, spyware installs on your computer through deception or exploitation of software vulnerabilities.

Spyware Trojan horse!

A Trojan horse, by definition, smuggles in something dangerous in the guise of something desirable. So spyware often hide, as an add on to some other program you really want.

Bundled Spyware

Spyware can also come bundled with shareware or other downloadable software, as well as music CDs. The user downloads a program (for instance, a music program or a file-trading utility) and installs it, and the installer additionally installs the spyware. Although the desirable software itself may do no harm, the bundled spyware does.

Manipulating Security Features

Another way of distributing spyware involves tricking users by manipulating security features designed to prevent unwanted installations. Internet browsers like Internet Explorer for example are easy targets t this method. Everybody has them and use them online almost daily. The way you protect yourself against this, is to always keep your operating system up to date when it comes to security updates.

Use Microsoft Update regularly (and often).

Examples of Spyware

As with computer viruses, researchers give names to spyware programs which frequently do not relate to any names that the spyware-writers use. Researchers may group programs into "families" based not on shared program code, but on common behaviors, or by "following the money" or apparent financial or business connections.

For instance, a number of the spyware programs distributed by Claria are collectively known as "Gator". Likewise, programs which are frequently installed together may be described as parts of the same spyware package, even if they function separately.

It is also important to know that different anti spyware program creators and big antivirus software creators may have different names for the save spyware. This can cause you to believe that you have 2 or more spyware products installed when you actually only have one, but mentioned with different names.

* CoolWebSearch, a group of programs, installs through the exploitation of Internet



Explorer vulnerabilities. The programs direct traffic to advertisements on Web sites including coolwebsearch. To make this happen, they display pop-up ads, rewrite search engine results, and alter the infected computer's hosts file to direct DNS lookups to these sites.

* Internet Optimizer, also known as DyFuCa, redirects Internet Explorer error pages to advertising. When users follow a broken link or enter an erroneous URL, they see a page of advertisements. However, because password-protected Web sites (HTTP Basic authentication) use the same mechanism as HTTP errors, Internet Optimizer makes it impossible for the user to access password-protected sites.

* 180 Solutions transmits extensive information to advertisers about the Web sites which users visit. It also alters HTTP requests for affiliate advertisements linked from a Web site, so that the advertisements make unearned profit for the 180 Solutions company. It opens pop-up ads that cover over the Web sites of competing companies.

Toolbars from any other than the big players like Google, Yahoo, Msn and similar very often contains spyware to some degree today.

And even the big guns have started to incorporate “spyware like” statistics gather from their toolbars. They do tell you about them, and ask for your permission to install or active these routines. But they often do it in such a convoluted way, no one actually understand it.

So start out the day by cleaning your computer and then working. Make sure you have a restful safe day, download, scan and clean your computer from any spyware today ...



How Common are Spyware

If you use the internet, “There is over 90% chance your computer is infected with spyware” - Source CNN.

Just think about it. You probably have at least one, if not more computers in your home. Most computers today have internet access. And if you receive email from others and surf to a couple of sites can you be almost completely sure you have some kind of spyware installed in your computer.

How Dangerous are Spyware?

Let me give you a short list of things spyware can do,

- Spyware can run completely hidden on your computer
- It can slow down your computer a lot
- It can spy on you and send everything you type to someone else
- It can record everything you do, allowing someone to see it later
- It can spy on you and send account information, passwords, credit card numbers and similar to a third party
- It can “steal” files, pictures, videos and more from your computer

Some spyware will do just a few things and others everything from the list above, and more.

You must keep your computer clean from spyware or risk losing personal information, financial information and even your private photos or family videos.

Run a spyware scanner regularly to clean out any spyware that may have sneaked their way into your computer. Do note that antivirus software (even the most expensive ones) have problems to keep spyware out. So get a good anti spyware software and use it!

No matter what the spyware's purpose really is, the bottom line is that at the very least it will cause you countless hours of problem solving and slow downs on your computer.

Scan your PC now to make sure it is clean. If you find anything, avoid using any credit cards or visit your online bank until the PC is cleaned with a top anti spyware software.

There are many different types of software that can harm, cripple or just reside quietly inside your computer. Beside virus, the most common types are Spyware, Adware, Malware, Trojans, Backdoors, Bots and Dialers. They all have different agendas but



will to a degree change the way your computer function and how well it works. This beside the obvious threat the program itself imposes.

Spyware - Eradicate It Now

Spyware removal has become a tedious work. As the spyware threat has worsened, a number of techniques have emerged to counteract it. Among these are

- programs designed to remove or to block spyware
- educating the users in such a way that spyware removal no longer is needed
- user practices which reduce the chance of getting spyware on a system.

Spyware remains a costly problem even with all new technology used to combat them. If a large number of spyware programs have infected a Windows computer, the only way to save the computer may be to back up user data, and fully reinstalling the operating system.

Anti-spyware programs

One of the markets most popular anti-spyware programs, Adwarealert will help you find and ultimately rid your computer of unwanted spyware software.

Many programmers and some commercial firms have released products designed to remove or block spyware. Steve Gibson's OptOut, , practically invented a growing category. Programs such as,

- [Adwarealert](#)
- **Lavasoft's Ad-Aware SE**
- **Patrick Kolla's Spybot - Search & Destroy**

rapidly gained popularity as effective tools to remove, and in some cases intercept, spyware programs.

Recently Microsoft bought the GIANT Anti-Spyware software, renaming it as Windows AntiSpyware beta and releasing it as a free download for Windows XP, Windows 2000, and Windows 2003 users. The renamed software for now exists as a time-limited beta test product that will expire at the end of July 2006. Microsoft is continuously developing and updating this product.

Antispyware protection, removal and antivirus

Major anti-virus firms such as Symantec, McAfee and Sophos have come later to the table, adding anti-spyware features to their existing anti-virus products.



In the beginning, anti-virus firms did not want to add anti-spyware functions, citing lawsuits brought by spyware authors against the authors of web sites and programs which described their products as "spyware".

However, recent versions of these major firm's home and business anti-virus products do include anti-spyware functions. The spyware is treated differently from viruses though.

Symantec Anti-Virus, for instance, categorizes spyware programs as "extended threats" and now offers real-time protection from them (as it does for viruses). The drawback with these programs is that they are very complex and in many cases produce more hurdles to jump over than you as a user really need.

Like most anti-virus software, anti-spyware software requires a frequently-updated database of threats. As new spyware programs are released, anti-spyware developers discover and evaluate them, making "signatures" or "definitions" which allow the software to detect and remove the spyware.

If a spyware program is not blocked and manages to get it installed, it may resist attempts to terminate or uninstall it. Some programs work together: when an anti-spyware scanner (or the user) terminates one running process, the other one starts up the killed program again, making it virtually impossible to clean the computer.

Some spyware will detect attempts to remove registry keys during the spyware removal and immediately add them again. Usually, booting the infected computer in safe mode allows an anti-spyware program a better chance of removing persistent spyware.

The most extreme way of cleaning is to move the hard drive to another computer, boot on the normal boot disk that computer has, and then clean the infected disk. You can also mount the infected disk over the local network and scan & clean it to remove as much spyware as possible.

It doesn't matter what way you choose to clean your computer, but using a good spyware removal program will make your life much easier ...



How to Remove Spyware

Spyware removal has become a tedious work. As the spyware threat has worsened, a number of techniques have emerged to counteract it. Among these are

- * Programs designed to remove or to block unwanted programs
- * Educating the users in such a way that they can keep bad programs from infecting their computer
- * User practices which reduce the chance of any software sneaking their way into your computer.

Information gather software remains a costly problem even with all new technology used to combat them. If a large number of spyware programs have infected a Windows computer, the only way to save the computer may be to back up user data, and fully reinstalling the operating system.

Anti-spyware Programs

One of the markets most popular programs, Adwarealert will help you find and ultimately rid your computer of unwanted software.

Many programmers and some commercial firms have released products designed to remove or block spyware. Steve Gibson's OptOut, , practically invented a growing category. Programs such as,

- * [Adwarealert](#)
- * Lavasoft's Ad-Aware SE
- * Patrick Kolla's Spybot - Search & Destroy

Rapidly gained popularity as effective tools to remove, and in some cases intercept, badly behaved programs.

Recently Microsoft bought the GIANT Anti-Spyware software, renaming it as Windows AntiSpyware beta and releasing it as a free download for Windows XP, Windows 2000, and Windows 2003 users. The renamed software for now exists as a time-limited beta test product that will expire at the end of July 2006. Microsoft is continuously developing and updating this product.



Protection and removal

Major anti-virus firms such as Symantec, McAfee and Sophos have come later to the table, adding anti-spyware features to their existing anti-virus products.

In the beginning, anti-virus firms did not want to add functions that were connected to other forms of threats than virus, citing lawsuits brought by software authors against the authors of web sites and programs which described their products as "spyware".

However, recent versions of these major firm's home and business anti-virus products do include anti-spyware functions. The malware, adware type of software is treated differently from viruses though.

Symantec Anti-Virus, for instance, categorizes all kinds of malware as "extended threats" and now offers real-time protection from them (as it does for viruses). The drawback with these programs is that they are very complex and in many cases produce more hurdles to jump over than you as a user really need.

All protection software requires a frequently-updated database of threats. As new threats are released, the protection software developers discover and evaluate them, making "signatures" or "definitions" which allow the software to detect and remove the offending software.

If a threatening program is not blocked and manages to get it installed, it may resist attempts to terminate or uninstall it. Some programs work together: when a threat scanner (or the user) terminates one running process, the other one starts up the killed program again, making it virtually impossible to clean the computer.

Some malware will detect attempts to remove registry keys during the spyware removal and immediately add them again. Usually, booting the infected computer in safe mode allows an anti-spyware program a better chance of removing persistent programs.

The most extreme way of cleaning is to move the hard drive to another computer, boot on the normal boot disk that computer has, and then clean the infected disk. You can also mount the infected disk over the local network and scan & clean it to remove as much spyware as possible.

It doesn't matter what way you choose to clean your computer, but using a good malware removal program will make your life much easier ...



You need a spyware remover!

If you use the internet, **"There is over 90% chance your computer is infected with spyware"** - Source CNN.

Just think about it. You probably have at least one, if not more computers in your home. Most computers today have internet access. And if you receive email from others and surf to a couple of sites can you be almost completely sure you have some kind of spyware installed in your computer.

What can Spyware do?

Let me give you a short list of things spyware can do,

- Spyware can run completely hidden on your computer
- It can slow down your computer a lot
- It can spy on you and send everything you type to someone else
- It can record everything you do, allowing someone to see it later
- It can spy on you and send account information, passwords, credit card numbers and similar to a third party
- It can "steal" files, pictures, videos and more from your computer

Some spyware will do just a few things and others everything from the list above, and more.

You must keep your computer clean from spyware or risk losing personal information, financial information or even your private photos or family videos.

Run a spyware scanner regularly to clean out any spyware that may have sneaked their way into your computer. Do note that antivirus software (even the most expensive ones) have problems to keep spyware out. So get a good anti spyware software and use it!

No matter what the spyware's purpose really is, the bottom line is that at the very least it will cause you countless hours of problem solving and slow downs on your computer.

Scan your PC now to make sure it is clean. If you find anything, avoid using any credit cards or visit your bank until the PC is cleaned with a top anti spyware software.



Tools to Use

There are many tools to combat Spyware, Adware and Malware.

The truth is that due to the large amount of software infecting your computer on different levels, you must use several tools to even have a fighting chance of keeping your computer clean.

Our number 1 choice is [Adwarealert!](#) Go there and use the free download & Scan to see if you have any spyware that should be removed.

To get more information about Spyware and Malware in general and a see our "Top 3 list" over spyware removal software with free downloads, please visit our site at

[Free Spyware Remover Reviews](#)

Good Luck with your Spyware Hunting!

**[Get your own branded copy
of this report to give away here!](#)**