

What is Spyware?

An Article by

Genesys Micro

In simple terms, Spyware is software that is installed on your computer, without your knowledge, that is intended to collect and track confidential information. The concept of Spyware has morphed in to more than data collection, and has become a way to control a computer and attack other systems for the purpose of spreading infections and committing crimes.

A Short History

Before Spyware, there was "Adware", or advertising supported software. Rather than sell their software, software companies would provide free access to anyone prepared to tolerate built-in advertising. Sometimes there was an option to remove these ads and banners, but only if you paid a fee.

Some Adware then began to include tracking software designed to provide internet statistics on web surfing habits. It became more insidious when information on the users computer was "data mined" to include personal or confidential information such as e-mail addresses and software serial numbers. As long as data collection was disclosed to the user, it was considered Adware.

Then, some Adware programs were modified to collect information and secretly send it back over the internet to a server. There was never any disclosure. It then became known as "Spyware".

In simple terms, "spying" on everything you do and collecting all kinds of information on your computer! This can include every keystroke you type (known as [keystroke loggers](#)), which may include credit card and bank account numbers.

Spyware has now morphed in to a general form of software called Malware. These have nothing to do with Adware at all and they go beyond what Spyware does because they are entire programs that are secretly installed on your computer that do data collection, but also includes more serious functions such as remote control and computer warfare ([Denial of Service Attacks, etc.](#))

Today, hackers develop and use Malware to steal your personal information and use your computer to commit serious crimes.

To differentiate itself from Malware, Spyware and Adware are sometimes referred to as "Grayware". Not as bad as Malware but in that "gray" area between "good" and "bad".

Even though Malware is the more correct term used to define what users face today, Spyware appears to be the jargon that "stuck". Most removal tools define themselves as "anti-spyware" and not "anti-malware" so for now we will refer to "Spyware" and "Malware" interchangeably.

Are all Adware products "Spyware"?

No, but some are. True [Adware](#) software programs display advertising but don't install any tracking software. Some Adware will install tracking software but discloses this during

installation and prompts for your permission. [Weatherbug](#) is a good example of legitimate, advertising supported software. Adware software that installs tracking software [without your permission](#) are then, by definition, re-classified as "Spyware"

Is Spyware illegal?

Even though the name may indicate so, Spyware has not yet been declared illegal. In a global internet, this would prove be difficult to achieve. In the absence of laws, internet users need to be aware of certain privacy issues that involves the tracking and sending of confidential data and statistics via a server installed on the user's PC and the use of your Internet connection in the background.

Is Malware illegal?

In many cases, Yes. Any software used for any malicious purpose which includes committing a crime is considered illegal in the USA.

What are the privacy issues?

While legitimate Adware software that includes tracking software will disclose the nature of data that is collected and transmitted in their privacy statement, there is almost no way for the user to actually control what data is being sent. Spyware software will not disclose that tracking software is even installed. The fact is that the technology in theory is capable of sending much more than just internet statistics - and this is why many people feel uncomfortable with the idea of tracking software in general.

Will it harm my computer?

Many internet users are using advertising supported Spyware and Adware products and are totally unconcerned about the privacy issues. [However, the real problem with these programs is the fact that is can cause computer failures](#) - system slow-downs, lock-ups, and internet connection failures. This costs users and companies millions of dollars each year to remove and repair these problems. Also, most cannot be easily removed. Just imagine 10 or 20 different Spyware or Malware programs on your computer system, all working at the same time, collecting data and transmitting this back to a remote web site. Just one code related bug or incompatibility can send your system into failure, or make it work so slow you think your system is un-responding. You might even think you need an upgrade! It is quickly becoming the most reported computer related problem so far, even more serious than viruses.

Real "Spyware"...

There are also many PC surveillance tools that allow a user to monitor all kinds of activity on a computer, from keystroke capture, snapshots, email logging, chat logging and just about everything else. These "spy" tools are often designed for parents, businesses, and similar environments, but can be easily abused if they are installed on your computer without your knowledge. [Spector Pro](#) by SpectorSoft™ is an example of legitimate spying software.

These tools are perfectly legal for businesses, but for private use may violate the laws of some states.

How do computers get infected?

There are several ways computers become infected with malware. [The most common way to become infected is by clicking on links that take you to web sites with built-in content that is intentionally programmed with code that infects your computer](#) (i.e. active scripting. See the section below). You cannot know when a web site has this code, so don't blame yourself for using the internet as it was intended. Second, your computer can become infected by installing software on your computer that also has this code. For example, you may see a download link for a "free" utility that you might find useful, only to discover that this was just a fake program (aka "[Trojan horse](#)") designed to infect your system with Malware.

There are some basic ways to help prevent your system from getting infected.

Disclaimer: The following information is provided for informational purposes only and does not come with any warranty, implied or otherwise. Although we list many ways to protect your computer, it is the sole discretion of the reader to take full responsibility for any changes that you decide to implement.

- 1) [Turn off active scripting](#) in Internet Explorer (or use Firefox, a browser that does not use active scripting). To turn off active scripting in Internet Explorer, see the section on active scripting below.
- 2) [Add a blocked list](#) of known web sites with malware content to your restricted sites in your browser preferences. Some anti-virus and anti-spyware software can do this for you.
- 3) [Install sandboxing software](#) to "virtualizes" your browser (see the sandboxing section below).
- 4) [Do not install untrusted software](#) downloaded from the internet. Businesses should have blocking software and a restrictive policy about installing software on company computers.
- 5) [Install all critical Windows updates](#), but check with your IT department first - some updates have been known to cause problems. Also don't forget to install applications updates too (Adobe Acrobat Reader™, Microsoft Office™, etc.)
- 6) [Turn on the built-in Windows Firewall](#), but check with your IT department first - this may interfere with printer sharing and other legitimate functions. Some anti-virus programs come with their own firewall too.

What is Scripting?

Active Scripting is "Microsoft's® technology that allows different software components to interact with one another in a networked environment" such as the internet. ActiveX controls (also a Microsoft® technology) are downloadable software controls that enhances your Internet Explorer web browser by providing content such as buttons and pop-up menus. Together these are known as "Active Content". Microsoft's™ newer [.net framework](#) (pronounced "dot net") has replaced Active Scripting technology in favor of a more secure programming platform. However, support for Active Scripting will continue for years to come.

The simple fact is that not all internet content is "friendly" - some web sites contain carefully crafted scripting code that can harm your computer by silently installing malware or by modifying your operating system. [The problem is that you have no way of knowing which web sites are infected with malware code](#). Hackers and malware developers are constantly finding new ways to infect legitimate, well known web sites, using newly discovered flaws in the browser technology by injecting code in to their web pages.

Until the industry solves this problem, you can protect yourself by using a browser ([Firefox](#)) that does not use either. Also there is a free add-on called "[No Script](#)" that goes even further in locking-down the Firefox browser controls.

If you must use Internet Explorer (IE), [version 9](#) is, by far, safer than previous versions. Keep in mind that you cannot completely un-install IE from your Windows computer because many built-in applications require it such as Windows Updates. However, there are ways to "hide it" and make it safer. Also, if you are on a corporate network, check with your IT department before upgrading IE to version 8 as there may be compatibility issues with legacy software.

Because the exact method of disabling scripting is different in each version of IE, you may want to read Microsoft's® article on "[How to disable active content in Internet Explorer](#)". As stated before, IE and active scripting are required to receive Microsoft's Windows and Office updates. If you use Microsoft's Outlook Express, read the article "[How to Disable Active Scripting in Outlook Express](#)".

Another popular, more secure language is [Java™](#). Java code requires an "interpreter" to execute, and is known as the Java™ Virtual Machine (JVM). Most web browsers can execute Java™ applets because the JVM is built-in to the browser. However, some Java™ exploits have been discovered, so it is recommended that you install the most recent JVM. For more information go to www.java.com.

How do I know I have Spyware on my computer?

Most people start to notice problems with their computer such as a sudden change in their web browser's home page, or lots of pop-up ads. You may start to get porn-related ads, or be re-directed to web sites that you have never visited or would ever visit. You may notice that your computer is slower than usual. Or you might not notice anything at all. Here is a short list of some things to look for:

- ▶ An abundance of pop-up ads
- ▶ Porn related advertising (including sudden change in e-mails)
- ▶ Sudden change in your browser's home page
- ▶ Web redirection (also known as hijacking) to unusual web sites
- ▶ Over-all slowness
- ▶ Inability to surf the web or dial-up your internet provider
- ▶ Sudden lock-ups
- ▶ Changes to Windows Background Wall Paper
- ▶ Search Engine has been changed to one you have never seen before

How do I detect and remove Malware from my computer?

There are many programs available that can be used to detect and remove Malware from your computer. No single solution is perfect, so often two or more different programs are required to completely remove all Malware from your computer.

Many programs now detect all types of Malware, including Spyware and Viruses. However, you may need both an anti-spyware and an anti-virus program to have complete protection. Don't be surprised that you may need expert help in removing some spyware from your computer. There are variants of some very nasty spyware that will do everything it can to prevent removal from your system. Aside from backing up your files and re-installing your operating system from scratch, [the best way to keep your system clean is prevention.](#)

Should I use any Anti-Spyware removal software?

No! There are hundreds of fake or rogue "anti-spyware" programs that are in fact Malware! This is a new way to get unsuspecting users to actually infect their systems - by pretending to be an anti-spyware program. Be very careful when selecting your anti-spyware software. At this time, we recommend only the software programs list above, but there are many more legitimate programs available.

My computer has a pop-up that says I'm infected with spyware. What should I do?

Unless this message is from your anti-virus or anti-spyware program, **DO NOT TRUST IT!** Malware programmers are reaching new lows by actually generating totally fake "scare messages" to get unsuspecting users to install software that supposedly cures the computer of any detected spyware or malware. These pop-up boxes may look like real Windows error messages, but are in fact fake - they attempt to scare you in to believing that your computer is infected with malware, and then attempts to get you to install and later purchase the "cure". If you see any message like these, you are already infected with some kind of malware - time to call your computer professional for help.

How do I stop Pop-up Ads?

If you have Windows 2000 or XP, stop the Windows "messenger service". [Click here](#) for instructions.

If you have Windows XP, Service Pack 2 and Service Pack 3 includes a built-in pop-up manager. If you have Windows Vista, install SP1 (to avoid incompatibilities, always check with your IT department before installing any service packs).

Protect Yourself by "Sandboxing"

One of the best ways to protect yourself from malware is to use a form of software virtualization called browser sandboxing. Basically it's a software program designed to act as a gateway between the internet and your computer that prevents scripting code from infecting your system with spyware or viruses (or any kind of malware). Once your internet session is terminated by closing your browser any scripts that remain in memory are also terminated. As a result, your computer stays clean. Although not perfect, it currently one of the best ways to prevent malware infection. You could also take sandboxing to the next level, by completely virtualizing the entire computer, not just your browser. This is often done by software developers that want to test programs or operating systems for stability and errors. See out technical article "[What is Sandboxing?](#)".

 A popular, and free to home-users (non-commercial installations), browser sandboxing solution is "[Sandboxie](#)". It is very effective in malware prevention.

 For total computer solution see Microsoft's™ "[Virtual PC](#)" and [Parallels™ Workstation](#).

The latest thing..

Now that malware has been targeted as a threat to both security and system stability, malware designers have found a new and potentially dangerous way of circumventing detection - [Rootkit Technology](#). Basically, this is a way for a program to bypass normal API programming rules and hook directly into the Windows operating system. This will have the effect of making malicious code totally hidden and possibly un-removable! Currently, many anti-malware tools cannot detect Rootkit Technology and cannot remove them from your system. Even if they could, your system may not run properly again without at least re-installing Windows. You *can* detect *some* Rootkits on your computer by downloading and running Microsoft's free [RootKitRevealer](#) program, but this method of detection is no longer considered 100% reliable when executed from an infected system.

If you suspect that your system is infected, please contact Genesys Micro for more information on our services.