

# Avoid Spyware & Adware Infestations

Is your computer running slow, does it lock up or reboot itself without warning? Are you getting blue screens and other error messages? Are strange icons appearing on your desktop and/or in your taskbar? Are pop-up ads and junk mail driving you crazy? If you answered yes, chances are your computer is infected with advertising supported software known as spyware.

Our experience has shown that spyware problems are rampant. In fact, about 90 percent of all computers we service are infected with spyware ... and operate poorly because of it.

Advertising spyware, or adware, is software embedded in seemingly useful or entertaining programs which include a hidden mechanism to watch your browsing habits. Spyware is often installed without your knowledge, or without full disclosure that it will be used for gathering personal information and/or showing you ads.

The threat is serious. Advertising spyware can log information about you, including your name, age and sex. It may also capture your passwords, email addresses and other personal information. It can record and report your web browsing history and online buying habits. It can also determine your computer's hardware and software configuration and set itself up to use your computer to achieve its goals. Hackers could read your emails to family and friends and even see your instant messages. Technically, the truly dangerous spyware programs in the wrong hands can even steal your credit card numbers.

The media has drawn attention to the many virus attacks over the past few years, but the growing spyware problem has sneaked under the radar and gotten little attention until very recently. The fact is, spyware causes tremendous problems ... even more troublesome for the average user than viruses. And virus scanners are virtually useless in battling these problems. Spyware doesn't self-replicate or destroy data, so virus scanners typically ignore it. Because of this threat, surfing the Web gets more dangerous by the day. While many users notice the operational problems caused by spyware,



most have no idea their privacy is being threatened.

## What is it, what does it do & why?

Internet marketing companies scramble for an audience for their advertising, and pay top dollar for any demographic information they can get. As a result, less-than-ethical companies have emerged to provide less-than-ethical software to gather this demographic information. In a word, spyware monitors your browsing history and reports this information back to someone you don't know so advertisements can be targeted toward you ... with little regard for your privacy. These advertisements are actually based on your search interests and the websites you regularly visit and are generally presented as annoying pop-up windows. Some versions of spyware attack by bombarding you with unsolicited email, including those pornographic and "health" related advertisements you've become accustomed to seeing in your mailbox.

In addition to the privacy and security issues, spyware also takes over your computer's resources for its own use. Spyware uses valuable RAM, CPU cycles, and hard disk reads to do its dirty work. This surreptitious use of your hardware and operating system can make your computer unstable, and even unusable, for varying periods of time. General sluggishness, lock ups, blue screens, error messages and crashes are not uncommon. Network and Internet bandwidth are also used by spyware, resulting in slower access to the internet and slower legitimate network communications.

In the virus world, this hidden activity classifies spyware as a Trojan because of the obvious allusion to the

mythical Trojan horse -- it looks friendly enough until it infests your system. Unfortunately, spyware is not legally considered a virus. Why? Because you actually invite attacks when you install these types of free programs. When you install software containing spyware, you agree to be spied upon by clicking through the End User License Agreement. Have you ever actually read one of them? It would take a lawyer to figure it all out ... and who would hire a lawyer before installing a nifty piece of free software? By skipping this important step, you give these companies permission to spy on you and use your computer for their own clandestine purposes.

It is not uncommon for otherwise "friendly" programs to include spyware in their install routines. One of the most identifiable types of spyware is from a company called Gator Advertising. Their spyware is installed alongside free programs such as MyWebSearch Toolbar, TopRebates, Precision Time, Date Manager, and Offer Companion. You may have seen one or more of these programs after they magically appear in your Taskbar Tray (where your computer clock is displayed). Hotbar, WeatherBug, Webshots, Bonzi Buddy, Comet Cursor, Lop.com, Scratch and Win, Pass This On, and music and file sharing applications such as KaZaA and Grokster either are, or include, spyware. These are just a few of the common spyware programs ... there are many more lurking on the Internet and new ones emerge every month.

## What you get free costs too much

Most of us have gotten into the habit of accepting downloads whenever presented without thinking of the consequences. This seemingly innocent

practice opens the door for spyware providers to install their tools on your computer, creating problems and risks you shouldn't be willing to take.

Companies such as Lop.com, for example, have exploited this as a vehicle to install the most annoying software ever written — it pops up advertisements whether you are surfing the Web or not, changes Internet Explorer's start page, won't let you change it back, and like most other spyware, heavily resists removal.

One common method for spyware deployment is via an ActiveX control in Internet Explorer. Have you ever been alerted while browsing the web to install some software you weren't expecting you would need? This ActiveX installation ability was a good idea when it was first implemented. It gave the computer user a simple way to install Macromedia Shockwave or Flash, or a codec for Media Player so an embedded movie file could be played without a large download, and in a lot of cases, without even needing to close and reopen the browser window. ActiveX controls also allow such useful innovations as installation of security patches for Windows, and system virus scans using your browser. If you see an alert pop up asking if you would like to install some software, even if the alert claims the software has been digitally signed, you're safer assuming the software is something you don't want.

Do a little research before you download anything free. Go to the Internet and search on the word "spyware." Learn all you can. But, as a general rule, to protect yourself against spyware and adware attacks, avoid free software, even that offered by apparently respectable companies. Think about it. How can those companies afford their snazzy web development? How do they make money for their owners? Who's financing their paychecks? Why do they want to give you something for nothing? As a well-known French playwright once said, "What you get free costs too much."

#### "FEATURES" OF SPYWARE

Some spyware may only use one or two of these tactics, while others do quite a bit more.

**Deceptive functionality:** Spyware often uses a classic "Trojan horse" tactic—like a virus. It offers to synchronize your PC's clock or keep track of forms, but it is also doing other hidden things while you browse.

**Home page hijacking.** Did you ever find that your home page was changed, or discover new sites in Favorites that you didn't add? It might be spyware.

**Loss of privacy.** Some spyware keeps track of the web sites you visit and sends that information back to the spyware vendor. Do you want to tell everyone?

**More advertising:** Did you install a popup stopper but you are still getting popups? The ads you are getting may not be from the web site you are on, but from spyware.

**Stolen advertising:** Instead of showing ads that should appear on a web site, some spyware substitutes its own ads which can rob a web site of revenue.

**Broken web sites:** Spyware sometimes changes the actual content on a web page, and in the process it "breaks" the page. The page may not look correct, or you may get Javascript errors.

**Reduced performance:** Spyware uses up system resources, CPU time, memory, disk space, and Internet bandwidth, making your system slower.

**System instability:** Most spyware isn't very well tested or debugged, and there is no way to report bugs or obtain tech support. The result can be system crashes, hangs, or other strange behavior.

**Security risks:** Some spyware has a built-in update feature that lets the spyware maker download and install new code to your system without your knowledge or approval.

#### How do I get rid of spyware?

If you feel comfortable uninstalling software from your computer, go to Control Panel and double-click on Add / Remove Programs. In Add / Remove Programs, uninstall any program you don't use, never heard of, or suspect to

be spyware. Entries that say "Hotfix" or a Q (plus some number) are safe to leave alone unless you have reason to suspect otherwise. Those are examples of rather ambiguously named patches for Windows from Microsoft. Be careful and if you are unsure about what to uninstall, seek help from a computer store with a service center. If you are a skilled user, you can even edit your Windows registry file to remove spyware instructions. But in our experience, this practice should be left to professional technicians.

Remember ... most spyware aggressively resists removal. Once you uninstall the spyware, the Trojan applications are deleted, but the spying programs and processes remain active. Fortunately, there are some programs that can scan your system for spyware and remove it, similar to the way virus scanners remove viruses in a full system scan. The most popular of these are two free programs, SpyBot Search & Destroy and Ad-Aware.

You can find these programs free on the internet. However, our experience has shown that simple removal of spyware and adware does not eliminate all problems. You should consult a computer repair center for assistance. In many cases, our technicians are required to edit registry files, deleting the secret entries, before your problem can be completely solved. In the worst cases, we have to format your hard drive and reinstall your operating system. We also sell and install a more robust version of AdAware.

In general, it's best to remember that wise man's saying. "What you get free costs too much." Avoid accepting the nifty little free utilities you are always offered, be wary of messages which look like they come from Microsoft, stay away from the free music sites and, ironically, avoid the pop-ups that advise you are being watched by spyware and offer a solution. The spyware companies have learned to hide themselves in software offering to remove other spyware from your computer.

# computerone™

Fairway Square, 2825 Washington Rd., Augusta, Ga. - 706-667-9009 - [www.computerone.us](http://www.computerone.us)