

This free informational report is compliments of Computer Troubleshooters.

Computer Troubleshooters, a worldwide network of computer service franchises, works to meet the technical needs of small business and residential computer users. **We're the computer experts**...the people to call when your computer breaks down, when your machine or software needs upgrading, when viruses attack and even for service plans that guarantee no downtime.

Computer Troubleshooters technicians offer **unique, economical computer solutions and services** geared toward your needs—focusing on products and solutions most beneficial to small business clients and residential computer users. Our technicians combine friendly, personal service from a locally-owned and operated Troubleshooter with the knowledge, support and reliability of the world's largest computer service franchise.

Computer Troubleshooters
Black Division
Stone Mountain, Georgia
770.279.2677
www.itsolved.us

What is Spyware

And how to protect yourself

According to Wikipedia, “Spyware is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.”

“Spyware” has also come to refer more broadly to any software that is installed on a user's computer, and subverts that computer's operation for the benefit of a third party. Many freeware and adware programs fall in this category.

Spyware and Legalities

At the time of this writing, there are two bills in the House of Representatives related to spyware and protection against cyber trespassing. Neither of these bills has yet become a law. The bills prohibit the following acts, and much more: Taking control of a computer to send unsolicited information, diverting the internet browser or computer, user the computer as part of a group activity to cause harm to another computer, modifying computer settings without the operator's consent, collecting personally identifiable information through keystroke or without user consent, inducing users to install or disable software, misrepresentation to induce users to provide passwords or removing or disabling security, anti-spyware, or anti-virus technology from the computer.

The statuses of these bills are below:

<http://www.opencongress.org/bill/110-h964/show>

<http://www.opencongress.org/bill/110-h1525/show>

Anti-spyware and anti-virus programs

Trusted programs

There are many reputed, legitimate anti-spyware and anti-virus programs available for you to choose from. Many high-quality programs are available for free, trial basis or paid. When choosing a program, you should only consider programs with a proven track record, and a strong reputation. Always be aware of anti-spyware programs that are heavily and aggressively advertised online – these are often suspect programs that come bundled with their own adware or malware.

ZEDO recommends these quality products:

- [ESET](#)
- [Spybot Search and Destroy](#)
- [AVG Anti Virus Guard](#)
- [Ad-Aware Free](#)
- [Windows Defender](#)
- [Bit Defender](#)

Suspect Programs

If there are several choices of high-quality, well-known anti-spyware products for you to choose from, there are

thousands of unknown, poor-quality adware packages that look and act like anti-spyware software.

Suspicious antispyware programs are known to use inadequate detection techniques, false positives to coerce users to pay for upgrades, provide insufficient information about the company, contain unacceptable End User License Agreement (EULA) terms. These suspicious programs are also often distributed maliciously through aggressive, confusing advertising, spam emails, and sometimes installed directly in free software, adware, often without user knowledge or consent.

COMPUTER TROUBLESHOOTERS is not a software review company and does not conduct major software reviews of any sort. The following products are known to be suspicious and are rampantly reported to cause user problems:

- PSGuard
- RazeSpy
- WinSpyControl
- SpySheriff
- Internet Browsing

How to protect your computer against spyware

The best defense for your computer against spyware and other malicious software is your own vigilance.

Install and Run Security Software

- Install and run the appropriate security for your computer, including antispyware and antivirus software, and a personal firewall. If you have children in your household, use parental control software to block inappropriate downloads.
- Set your antispyware and antivirus software to automatically update so that the software recognizes new threats.
- Before purchasing security software, check to see if your computer manufacturer has already provided this software. If not, check with your Internet service provider to determine if these programs are provided with your Internet service.

Maintain Your Computer

- Regularly check for security updates for your operating system and other software; download and install patches immediately. Set your software to automatically install updates.
- Run a full spyware and virus scan of your computer whenever you suspect that you might be infected with spyware and never less than once per week. Symptoms of spyware infections include: unexpected popups, a home page change, random error messages, and slower computer performance.
- Adjust the security and privacy settings on your Internet browser and operating system to control what software is installed on your computer.

Be Cautious When You Are Online

- When surfing the Internet, only visit web sites that you are familiar with and trust.
- Carefully read any operating system or Internet browser warnings. To close a window or dialog box, consider the options provided by your operating system or Web browser, such as closing the window with the “x” mark in the upper corner.
- Be wary of “free” software; it could include extra software you may not want. Be especially cautious with free file sharing programs, screensavers, wallpaper, and smiles because these almost always come with extra software. If you’re not sure about a program, enter the name of the software into a search engine to see what others say about it.
- Always read the licensing agreements and privacy statements for any software. Many of the potentially unwanted behaviors are only revealed in the “fine print.”
- Pay close attention to the information that appears on your screen when you are installing software. The installation program may use vague or confusing language to trick you into saying “yes” when you want to say “no.”

