

HUDSON

330.342.4728 - 50 W. Streetsboro St.

MEDINA

330.725.7287 - 3725 Medina Rd.



What is Spyware?

Spyware is a general term used to describe software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent first.

Spyware and adware are extremely difficult to prevent. Most people install spyware inadvertently when they are tricked into clicking on a link that installs it; for example, by clicking a cancel button to close a dialog box. Spyware or adware may also get installed when other software is installed. That is why it is important to read all disclosures, including the privacy statement and license agreement, before installing any software. Spyware can also be installed with music and video downloads.

Other kinds of spyware make changes to your computer that can be annoying and can cause your computer to slow down or crash.

These programs can change your Web browser's home page or search page, or add additional components to your browser you don't need or want. These programs also make it very difficult for you to change your settings back to the way you originally had them.

The key in all cases is whether or not you (or someone who uses your computer) understand what the software will do and have agreed to install the software on your computer.

There are a number of ways spyware or other unwanted software can get on your computer. A common trick is to covertly install the software during the installation of other software you want such as a music or video file sharing program.

Whenever you install something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes the inclusion of unwanted software in a given software installation is documented, but it might appear at the end of a license agreement or privacy statement.

You may have spyware IF...

- **You see pop-up advertisements all the time.** Some unwanted software will bombard you with pop-up ads that aren't related to a particular Web site you're visiting. These ads are often for adult or other Web sites you may find objectionable. If you see pop-up ads as soon as you turn on your computer or when you're not even browsing the Web, you may have spyware or other unwanted software on your computer.
- **My settings have changed and I can't change them back to the way they were.** Some unwanted software has the ability to change your home page or search page settings. This means that the page that opens first when you start your Internet browser or the page that appears when you select "search" may be pages that you do not recognize. Even if you know how to adjust these settings, you may find that they revert back every time you restart your computer.
- **My Web browser contains additional components that I don't remember downloading.** Spyware and other unwanted software can add additional toolbars to your Web browser that you don't want or need. Even if you know how to remove these toolbars, they may return each time you restart your

computer.

- **My computer seems sluggish.** Spyware and other unwanted software are not necessarily designed to be efficient. The resources these programs use to track your activities and deliver advertisements can slow down your computer and errors in the software can make your computer crash.

If you notice a sudden increase in the number of times a certain program crashes, or if your computer is slower than normal at performing routine tasks, you may have spyware or other unwanted software on your machine.

How to help prevent spyware

Surf and download more safely

The best defense against spyware and other unwanted software is not to download it in the first place. Here are a few helpful tips that can protect you from downloading software you don't want:

- Only download programs from Web sites you trust. If you're not sure whether to trust a program you are considering downloading, ask a knowledgeable friend or enter the name of the program into your favorite search engine to see if anyone else has reported that it contains spyware.
- Read all security warnings, license agreements, and privacy statements associated with any software you download.
- Never click "agree" or "OK" to close a window. Instead, click the red "x" in the corner of the window or press the Alt + F4 buttons on your keyboard to close a window.
- Be wary of popular "free" music and movie file-sharing programs, and be sure you clearly understand all of the software packaged with those

programs.

- Use Firefox as your main web browser.
- Avoid installing peer-to-peer programs, like a music swapping software.
- Investigate the credibility of a program and its publisher before downloading them.

Fake anti-spyware programs

Malicious programmers have released a large number of fake anti-spyware programs. These web banners usually warn users that their computers have been infected with spyware, directing them to purchase programs which do not actually remove spyware — or worse, may add more spyware of their own.

A lot of these fake programs often bill themselves as antispyware, antivirus, or registry cleaners, and sometimes feature popups prompting users to install them. They are called rogue software.

Known offenders include:

- AntiVirus Gold
- AV System Care
- ContraVirus
- Disk Knight (spreads through USB
- Spyware Quake
- Spydawn
- Spylocked
- SpyShredder

- storage devices)
- errorsafe (AKA system doctor)
 - MalwareAlarm
 - MagicAntiSpy
 - PAL Spyware Remover
 - PCSecuresystem
 - Pest Trap
 - PSGuard
 - SecurePCcleaner
 - SpyAxe
 - SpywareStrike
 - SysProtect
 - Spy Ranger
 - Spy Sheriff
 - Spy Wiper
 - Registrycleanerxp.com
 - UltimateCleaner
 - Virus Protect Pro (3.1 and other number.number)
 - WinAntiVirus Pro 2006
 - WinFixer
 - WorldAntiSpy
 - Your Privacy Guard

Notable programs distributed with spyware

- Bonzi Buddy
- Dope Wars
- ErrorGuard
- Grokster
- Kazaa
- Morpheus
- RadLight
- WeatherBug
- EDonkey2000
- LimeWire