

What is Spyware?

If you are reading this, Spyware may have already been introduced to you, although you may not have been properly introduced to Spyware.

This is Spyware:

In keeping with emergent industry standards, iS3 uses the word, “Spyware” to refer to potentially unwanted software that is non-viral in nature.

Spyware includes the following behavior that is illegal under existing law—Section 5 of the FTC Act, 15 U.S.C.§45—as an unfair or deceptive act or practice.

- **Gathers information from a user’s computer without knowledge OR consent;**
- **Reports the information to the creator of the software or to one or more third parties;**
- **Is installed on a user’s computer without having given adequate notice to the user;**
- **Provides the user with little or no control over removing the software.**

This is what Spyware is NOT:

Spyware is not a virus, although both are malicious, both capture or destroy information and both can ruin the performance of your computer system. The difference is; Viruses attempt to spread; Spyware attempts to embed. A virus attempts to infect your computer, replicate itself and spread to as many other computers as possible, at lightening speed. Spyware attempts to infect your computer and disguise itself, embedding itself deeply in your computer’s operating system so as to evade detection and removal as long as possible.

Spyware’s purpose is to monitor your activities and transmit data back to a third party. The longer it stays, the more effective it is.

Lastly, viruses are created to show off the technical abilities of their creators by wreaking as much havoc as possible. Spyware is created purely for financial gain.

This is what Spyware does:

- **Changes system settings:** Spyware can “hijack” your browser, redirecting your Web searches to a disreputable search engine that delivers unwanted, potentially offensive search results. It can change your homepage settings, and even make surfing impossible.
- **Installs unauthorized dialers:** Spyware can install programs that alter your dial-up settings and then dial numbers without your knowledge. Often, these numbers connect to potentially offensive sources. Once dialer software is downloaded, you will be disconnected from your Internet service provider. Dialers automatically dial “900 numbers” and you will be billed for the time used. Dialers are malicious in nature and can rack up expensive and unwanted bills
- **Installs Keyloggers:** Spyware can install programs that monitor and record every key stroke you type. Keyloggers are a grave threat to both your privacy and your security. They can monitor your e-mail and chat, capture account numbers, user names, passwords, Social Security numbers and other identifiers that you type when making purchases or doing banking.
- **Collects and reports user’s personal information to the developer of the software or to one or more unauthorized third parties:** Once Spyware has captured your personal information, it relays this information back to its creators, who use it for targeted advertising, or worse; fraud, identity theft or other illegal activities. The longer the Spyware remains on your computer undetected, the more information it collects and transmits.
- **Uses computer processing capacity without permission:** If your computer processing has suddenly slowed to a crawl, you are probably infected with Spyware. At the very least, Spyware runs as a background application, as soon as you boot up. Unlike the makers of legitimate software, the makers of Spyware do not care how inefficient their programs are with your resources. They tend to hog your computer’s RAM and processing power. Sometimes, buried in the End User License Agreement (that long document in legal language under which you clicked I Accept when you installed some application), is a clause authorizing the software makers to use your computer without your permission, even to turn your computer into a “bot” that launches additional Spyware.

- **Delivers spam or ads without user's notice and consent:** If Spyware is monitoring your surfing habits, it can deliver ads that seem relevant to your search. For example, you could be searching the Web for mortgage rates when a pop-up ad for a bank or realtor is displayed on your screen. Ads relevant to your searching are much more effective than random ads. Although the ad itself may be merely a nuisance, it has been delivered at that time because your search was being monitored, and you should be concerned for your privacy.

This is how you become infected with Spyware:

Spyware is often transmitted by downloading freeware and shareware or swapping files. Music files, free toolbars, pictures, screen savers and other "cool" applications can infect you with Spyware. Spyware is also delivered via spam, when you open a malicious message or attachment.

Phishing sites often download Spyware onto unsuspecting users who believe they are replying to requests for information by their banks, credit unions or merchants with whom they do business.

This is how to prevent infection by Spyware:

- **Do not click on pop-up advertisements.**
- **Download only those software programs that come from reputable sources.**
- **Install a good anti-virus product, and make sure you are running the latest updates at all times.**
- **Install STOPzilla. It provides True Real-Time® protection from Spyware, blocks Phishing attacks and kills pop-up ads. To make sure you are running the latest updates to STOPzilla, set it to download and install definition updates automatically.**