



Spyware

Spyware, a kind of malicious software, can monitor and control your computer without your permission. It may be used to monitor your internet surfing, record your keystrokes and could potentially lead to identity theft.

Because spyware is mostly focused on information collection or “spying”, the clues that spyware is on a computer can be difficult to spot. Spyware-like services are also sometimes installed ‘legally’ through the wording of EULA agreements on social media and legitimate software.

The good news is that consumers can minimize how much of their information is collected by following some simple recommendations.

Recommendations

- **Keep your operating system and web browsers updated.** Your operating system (like Windows or Linux) may offer free software “patches” to close holes in the system that spyware could exploit.
- **Download free software only from sites you know and trust.** It can be appealing to download free software like games, peer-to-peer file-sharing programs, customized toolbars, or other programs that may change or customize the functioning of your computer. Be aware, however, that some of these free software applications bundle or hide other programs in the software, including spyware.
- **Don’t install any software without knowing exactly what it is.** Take the time to read the end-user license agreement (EULA) before downloading any software. If the EULA is hard to find — or difficult to understand — think twice about installing the software.
- **Minimize “drive-by” downloads.** Make sure your browser security setting is high enough to detect unauthorized downloads, for example, at least the “Medium” setting for Internet Explorer. Keep your browser updated.
- **Don’t click on any links within pop-up windows.** If you do, you may install spyware on your computer. Instead, close pop-up windows by clicking on the “X” icon in the title bar.
- **Don’t click on links in spam that claim to offer anti-spyware software.** Some software offered in spam actually installs spyware.
- **Install a personal firewall to stop uninvited users from accessing your computer.** A firewall blocks unauthorized access to your computer and will alert you if spyware already on your computer is sending information out.





What to do if you suspect Spyware

If you think your computer might have spyware on it, you should take three steps:

1. **Get an anti-malware program from a vendor you know and trust.**
2. **Set it to scan on a regular basis** — at least once a week — and every time you start your computer, if possible.
3. **Uninstall unused software from your computer.** Review and uninstall what you don't use.

Resources

Canadian Anti-Fraud Call Centre

www.antifraudcentre.ca

Stay Safe Online

<http://www.staysafeonline.info/>

