

Who's Spying On You?

In the past, most of us worried about viruses, trojans, and worms, but in recent years, a new form of attack has appeared that has been added to the list of malicious software or malware.

With the growing threat of spyware and the impact it can have on your computer, it's more important than ever that you take the time to educate yourself about what spyware is, its sources, and good security and Internet surfing habits that can help you avoid possible infection.

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

Spyware is typically created to monitor your internet usage, gather information that you type, or force adverts upon your desktop either by pop-ups or by hijacking your web browser to point to various websites.

Spyware is generally classified as software that installs itself without a user's permission and doesn't clearly or honestly tell users what personal information it is gathering and how it is using it and can affect your computer with results that vary from minor annoyances to causing your computer to slow down or crash. Spyware isn't the best-written software in the world and commonly causes system instability and the dreaded blue screen of death.

Software vendors offer anti-spyware tools to permit users to scan their computers for recognised spyware and remove it. Some advertising software can be identified as malicious by trying to re-install itself after you have removed it

Spyware should not be taken lightly, your personal information could be recorded with a variety of techniques; one particularly nasty breed of software is the key-logger which can essentially capture every keystroke you type, your web browsing history and in some cases even email a screen shot of what you are doing on your computer at various times throughout the day without you even knowing. Spyware infringes on your privacy, because you are usually unaware what information is being released and what happens to it. Finally, you may be inconvenienced as a result of what is subsequently done with the information.

{mospagebreak title=Infected}

Infected

Spyware installs itself on your computer in different ways. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Spyware is also delivered via spam, when you open a malicious message or attachment.

Malicious web sites may install hijackers; these are browser plug-ins or helpers that monitor web pages as you view them and then replace banner ads or generate new pop-ups from advertisers that offer similar products who are paying royalties to the party responsible for the hijackers.

Identifying the source of spyware is especially difficult when it has been installed by "drive-by methods", given that users probably were not even aware that the spyware was being installed.

A plug-in is a software program that extends the capabilities of your Internet browser in a specific way. Not all browser plug-ins are harmful and some may be helpful. Browser hijackers commonly do one or more of the following

- Change your search page and pass all searches to a pay-per-search site
- Redirect your web searches to a disreputable search engine that delivers unwanted, often offensive search results
- Change your default home page to the advertiser's page

Some spyware authors infect a system through security holes in the web browser or in other software. Most spyware is designed for Microsoft Windows and Internet Explorer because the vast majority of computers use these technologies.

Since most spyware is built to take advantage of Explorer's weaknesses, using an alternative browser, such as Firefox, can help to keep the spyware out.

Fortunately, there are many ways you can tell if spyware is on your computer. Spyware does not usually set out to harm or damage the computer; however, spyware will normally cause the computer to slow down or crash because of all the spyware programs running.

The following symptoms may indicate that spyware is installed on your computer:

- Endless pop-up windows
- You are redirected to web sites other than the one you typed into your browser
- Unexpected toolbars appear in your web browser
- Unexpected icons appear on your desktop or in the task tray at the bottom of your screen
- Your browser's home page suddenly changes
- The search engine your browser opens when you click search has been changed
- Security programs, such as firewalls or anti-virus programs have been disabled

{mospagebreak title=Anti-spyware}

Anti-spyware

While most spyware requires you to download or click something before it can be installed, some programs take advantage of security holes in the software on your computer. If you're a regular user of the Internet then spyware detection software is vital.

As new spyware programs are released, anti-spyware developers discover and evaluate them, making "signatures" or "definitions" which allow the software to detect and remove new threats. Just like computer viruses and spam, spyware will continue to change and evolve, so you need to check regularly for updates to your protection software.

Anti-spyware programs can combat spyware in

two ways:

- Real-time monitoring, which helps to prevent the installation of spyware
- Detection and removal, to remove spyware from an infected computer

Real-time protection from spyware works identically to real-time anti-virus protection: the software scans incoming files on access and blocks the activity of components known to represent spyware

Anti-virus programs do not detect most spyware because the programs do not have the characteristics of a virus; also, anti-virus software, firewalls and Internet pop-up blockers generally do not provide adequate protection from spyware once it's on your machine.

It is no longer safe to assume that because you have installed anti-virus software you are safe from network attacks and prying eyes.

{mospagebreak title=Spyware or Virus?}

Spyware or Virus?

Spyware is not a virus, although both are malicious, both capture or destroy information and both can ruin the performance of your computer.

Worms and viruses are self-replicating programs that travel from computer to computer by various means. A virus seeks to infect a computer, replicate and infect as many computers as possible, as quickly as possible. It usually relies on email for propagation, but tries other avenues of attack such as file sharing, telnet, FTP, Instant Messaging, or any services and programs on your computer that communicate with other computers.

A worm is a virus-like program that spreads automatically to other computers by distributing itself via email or other means. For example, an email-delivered virus (a worm) may search your computer's file system for your address book and send infected email messages to all of your contacts.

Both worms and viruses have, as their first objective, merely propagation.

Spyware is more interested in having the host remain healthy: a non-functional computer has neither advertising value nor revenue potential to spyware. So whereas virus activities are overt and generally attract attention quickly, spyware activities are typically covert and their infection is often long lasting.

The difference is: Viruses attempt to spread. Spyware attempts to embed.

{mospagebreak title=Removal}

Removal

Spyware attempts to infect your computer and disguise itself, hiding itself deeply in the operating system to avoid detection and removal as long as possible and many spyware packages are resistant to removal: you may uninstall them only to find that they reappear immediately or when you reboot your computer. Others modify many critical components of the operating system and removal often results in the computer becoming inoperable.

Protection

There are many precautions you can take to avoid spyware:

- Update your operating system and web browser software by downloading the latest patches available in order to close security holes
- Do not follow email links offering security updates; visit the vendor's web site directly
- Do not follow email links offering anti-spyware software
- Do not download software unless you explicitly trust the source

- Do not click banner ads that offer free games consoles, Instant Messaging Smilies or games

{mospagebreak title=Business Effects}

Effects On Your Business

Since many of us use our computers for work as well as entertainment, spyware can quickly go from being an annoyance to being a productivity killer for your business. The opportunities that spyware creates for fraud, identity theft, and personal or business-targeted extortion should be taken very seriously.

Small and medium business must understand what spyware is and the threat that spyware poses; if your business operates in a regulated environment, place the threat level between High and Severe.

The shocking truth is that industry experts estimate that around 90% of computers are infected with spyware. Unfortunately, once your system is infected with one type of spyware, there's a good chance you'll find others as well. Add in fake anti-spyware programs and web banner ads that warn users that their computer has been infected, claiming that they need to purchase programs which do not actually remove spyware, or worse still, add more spyware of their own and it's easy to see why spyware is fast becoming the single biggest threat to privacy and productivity on the Internet.

The first step to controlling spyware is to prevent it from installing in the first place. The safest way to remain free from spyware is to use one or more anti-spyware programs that actively scan your system for intrusion and help inoculate your system from penetration.

You should be using both a high quality commercial anti-virus program and one or more good quality programs for handling the spyware threat.

Even with anti-spyware programs active, do not develop a false sense of security, be alert for any uninvited programs suddenly offering to help;

If you would like more information on protecting your computers or think that you have a spyware infection then call 01424 858185 for prompt and professional advice.