



Series 5 – How Do I Access the Internet, Securely?

Welcome back to a series of computer related articles brought to you by VistaSol Computer Solutions. Over the coming weeks we are going to be featuring articles based on the theme of 'How do I . . .?'

This week we're continuing our series of articles on the subject of 'How Do I Access the Internet' by offering more advice on how to keep yourself secure on-line.

Part 5 – Spyware & Adware

Following on from last week's article about Viruses, Worms and Trojans, this week we're going to be looking at spyware and adware.

Spyware and adware don't technically fit into either the virus or spam category, but they should be treated in the same way! At times these programs may invade your privacy, contain malicious code, and at the very least they can be a nuisance when using a computer connected to the Internet.

What is Spyware?

Spyware is defined as being any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of some freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about email addresses and even passwords and credit card numbers.

Spyware is similar to a Trojan horse in that you may unwittingly install the product when installing something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Because spyware exists as independent executable programs, they have the ability to monitor keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, consistently relaying this information back to the spyware author who will either use it for advertising / marketing purposes or sell the information to another party.

Licensing agreements that accompany software downloads sometimes warn the user that a spyware program will be installed along with the requested software, but the licensing agreements may not always be read completely because the notice of a spyware installation is often couched in obtuse, hard-to-read legal disclaimers.

What is Adware?

Adware is considered to be a legitimate alternative offered to consumers who do not wish to pay for software. Programs, games or utilities can be designed and distributed as 'freeware'. Sometimes freeware blocks features and functions of the software until you pay to register it. Today we have a growing number of software developers who offer their goods as "sponsored" freeware until you pay to register. Generally most or all features of the freeware are enabled but you will be viewing sponsored advertisements while the software is being used. The advertisements usually run in a small section of the software interface or as a pop-up ad box on your desktop. When you stop running the software, the ads should disappear. This allows consumers to try the software before they buy and you always have the option of disabling the ads by purchasing a registration key.

In many cases, adware is a legitimate revenue source for companies who offer their software free to users. A perfect example of this would be the email program, Eudora. You can choose to purchase Eudora or run the software in sponsored mode. In sponsored mode Eudora will display an ad window in the program and up to three sponsored toolbar links. Eudora adware is not malicious; it reportedly doesn't track your habits or provide information about you to a third party. This type of adware is simply serving up random paid ads within the program. When you quit the program the ads will stop running on your system.

How do I know if I've been infected?

Although you may not realise that you have installed spyware, there will often be some signs that it exists on your computer. Check to see if there are any changes to your Web browser that you did not make e.g. extra toolbars or different homepage settings, as well as changes to your security settings and favourites list – if so, you may have spyware running on your system. Other signs of a spyware infection include pop-up ads which aren't related to a Web site you're viewing; usually these spyware advertisements are adult content in nature, and are not displayed in the same fashion as legitimate ads you would normally see on your favourite Web sites. You may also see advertisements when you're not browsing the Web. Clicking hyperlinks which do not work (or take you somewhere you didn't expect), a sluggish system, or your system taking longer to load the Windows desktop are all signs that your computer may be infected with spyware.

How do I remove / prevent Spyware?

Anti-spyware software works by identifying any spyware installed on your system and removing it. Since spyware is installed like any other application on your system it will leave traces of itself in the system registry and in other places on your computer. Anti-spyware software will look for evidence of these files and delete them if found.

We particularly like 'MalwareBytes', and as always recommend this program as your first port of call if you have any doubts about whether or not you may be infected with any form of 'Malware'. You can find a link for this software on our web site.

We also recommend using caution and being vigilant at all times when installing software – especially if it is free. The suppliers of this software are not charities, and will often install 'additional' software with their program, in order to generate some form of revenue for them. In most cases you will be offered the option of not including this 'additional' software, which may take the form of a 'search engine' or 'browser toolbar'. In all cases we recommend NOT installing this additional software, unless you have specifically requested these additions.

Enjoy your on-line surfing experience, but be safe and think about your security at all times.