

Spyware – What Is It and How Do I Deal With It?

Compiled by Hugh McClean
Managing Director, PropertyPro (Suppliers of **PropertyPro**[®]) 12 April 2005



What are Spyware, Adware and Malware?

These are all forms of programs, plug-ins and cookies that provide extra functionality to your systems. For the rest of this document, I will group these together and refer to them as a general term of Spyware.

They are only installed with the agreement (implicit or otherwise) of the end user. Typically, these are available when visiting websites or opening emails. The installation of these would normally be preceded by a question like:

"Would you like to download the following program?"

"Do you wish to enable this ActiveX control?"

"Do you wish to allow this pop up?"

or similar. The largest number of these types of products, are installed from Porn sites, Gaming sites and Music and Video download sites. It is rare for any of these products to be installed by visiting a business related website.

Why is this such a problem now?

We have all been familiar with the problem of viruses for some time and over the years, anti-virus software has become effective in minimising the impacts of virus attack. Provided that your virus definitions are always up to date, the risk of virus infection is now relatively small. Unfortunately, the same types of people who spend time writing and distributing viruses have now identified a new means of causing problems to business and private users of PCs. Because these products are "invited" into your machines, they are not considered as viruses and bypass this form of protection. With the advent of broadband connections to the internet and their spread to large numbers of private users and businesses, the speed of spread of such attacks has massively increased.

What do they do and why should I worry?

Spyware allows access to your computers from the internet. In itself, this is not necessarily dangerous. However, once the addresses of machines on your networks are made public, there is an increased risk of external attack. On individual PCs, additional software will be running in the background using system resources and adversely affecting performance. In addition, annoying pop-ups and potentially embarrassing advertising may appear whilst using the internet. The home page on Internet Explorer may be changed to an inappropriate site for a work computer. By the very nature of Spyware, there is increased internet activity and if you have a shared internet connection then increased network activity and degraded network performance.

Why doesn't my antivirus protect me?

Modern antivirus software is extremely effective at preventing direct virus attacks on computers and networks. However, it is not designed to prevent you from making your own decisions as to what you consider suitable to install on your own PCs.

Why does Spyware affect my network?

Because Spyware opens an additional communication channel to the internet, this results in increased traffic. In most businesses, these days, there is a shared internet connection via broadband, which is connected to your local area network. All traffic, internal and external, is routed via this network and there is a finite capacity. Many Spyware products result in massive internet activity and use increasingly greater amounts of your available internet capacity. Put simply, by one user on a network installing Spyware on their machine, your entire network can grind to a halt.

Page 1 of 2

Spyware – What Is It and How Do I Deal With It?



Compiled by Hugh McClean
Managing Director, PropertyPro (Suppliers of **PropertyPro**[®]) 12 April 2005

Is it only porn sites that I should worry about?

Porn sites are obviously a concern and offer a high risk of virus and Spyware infection. These should always be avoided on a works PC. Spyware, however, can originate from many other sources, the most prevalent of these being gaming, music and video sites. It is important that you are aware that most sites that allow music and video to be downloaded free of charge are breaking copyright and effectively downloading from these sites is illegal. Many of these sites source their material from down loaders. So, when you log on to download music, you are also sharing music stored locally on your PC, thus allowing external access to your network.

How do I protect against these threats?

Firstly, it is essential to always keep antivirus definitions up to date on every PC on your network. With Windows operating systems, many loopholes and vulnerabilities are fixed in automatic updates which are available from Microsoft. All PCs should be set to download these upgrades and it is important to check that these are installed. If PCs are set to automatically update at night, then ensure that the PCs are left on. Where automated updates have not been configured, then check daily on the Windows update sites and install all critical updates.

For Microsoft Windows XP and 2000 operating systems, free anti-Spyware software is available to download from Microsoft's website www.microsoft.com under the heading "Popular Downloads", click on Windows AntiSpyware (Beta). This will lead you through a wizard, enabling you to download and install the software. Once installed, you should allow the software to make regular scans and automatically update.

For users still running Windows 98 operating system, unfortunately, the Microsoft AntiSpyware product is not available. There are third party products, such as Spybot, which provide similar protection. Windows 98 is no longer fully supported by Microsoft, so threats are dealt with less effectively. Now is the time to consider upgrading Windows 98 machines to XP Professional, which provides a greater level of security and stability. It is recommended that users should migrate from Windows 98 as soon as is practical.

There is no guarantee that by following these steps you will never get infected by Spyware or viruses, but you will minimise the risk of this happening.

Why do I need an internet policy?

Without an internet policy, all members of staff are able to use the internet for whatever purpose they see fit. If no policy is in place, then it is extremely difficult to bring any sort of disciplinary action against an employee who may be placing your network at risk. Employees also have a great deal of uncertainty as to what they are and are not allowed to do whilst using the internet at work. The simple solution to this is to document clearly acceptable and unacceptable use. This need not be incredibly detailed and does not need to be draconian. In simple terms, employees should be able to use the internet for any purpose relating to their job, including acquiring background information. A good rule of thumb would be that should a customer see which sites have been visited, they would not cause offence or show the company in an unprofessional light.

It is possible to listen to the radio via the internet using sites provided by major broadcasters. It is unlikely that these sites offer any significant threat and you may decide to allow employees to use these sites, provided there is no adverse impact on network performance.

Gaming and music download sites offer more serious threats to companies. The impact on network performance is potentially massive and there are legal issues relating to copyright which may impact your company. I would recommend that employees are specifically informed that downloading music, video and games from the internet is not allowed.