

Spyware & Adware



- Do you share files online?
- Do you download free programmes (e.g. / toolbars)?
- Do you click on adverts or pop-ups?
- Do you open unsolicited email?
- Do you open email attachments without scanning them first?
- Do you allow users to insert discs or flash drives into your computer?
- Does your computer ever act erratically without reason (e.g. lights flash / fan starts up)?
- Do adverts seem to appear on screen from nowhere?

If you answered yes to any of the above questions then your computer equipment may be at risk or may already be infected.

Description

"23% of businesses are infected by spyware"

– The Invisible Crime: A Business Crime Survey –
British Chambers of Commerce 2008

Spyware refers to hidden programmes running on your computer without your knowledge or consent. The programmes track and communicate all your on-line activity to a third party. The more malicious ones are able to log everything you type on your keyboard including credit card details, important client data, online banking passwords and other sensitive information before sending it back to the creator.

Whilst spyware itself will be unlikely to cause damage to your computer and files, it may be carrying other malicious codes such as viruses and Trojans.

Spyware finds its way onto a computer often piggybacking on the back of a free programme aimed at enhancing your computer, such as a screen-saver or tool bar.

Cyber criminals infect legitimate websites that when clicked execute the spyware script on the computer, this is known as a drive-by install. Specially designed emails are also used to tempt naïve users to open them before installing the malware.

Trying to differentiate between adware and spyware is a difficult task and causes much confusion. Adware is a piece of software that sits on your computer undetected bringing up adverts, often opening in new windows.

Adware is generally installed in the same way as spyware, unwittingly on the back of another programme; however some file sharing sites require users to install adware as a way of subsidising costs.

Whilst Adware is annoying and it can take up valuable processing power, it is not malicious and that's what differentiates it from Spyware. It will monitor your internet surfing and then tailor new adverts based on that activity but it won't steal private data.

CASE STUDY

Engineering Company, Nottingham

The business specialises in shaping and grinding component parts for machinery. They do not rely heavily on computers but do have one which is used for administration including online banking.

The administrator used the computer for surfing the internet and as she was the only person using the computer in the business, liked to personalise it with screen savers, tool and search bars. During breaks, she often played freeware games. Unfortunately hidden in the software, was spyware.

The company had no idea of a problem until there was a large transaction from their bank to an unrecognised account. Their initial fear was internal theft. On contacting their bank they found out that the transfer occurred online.

A specialist technical adviser was employed to investigate the computer and discovered an array of different malware and spyware applications running behind the scenes. Incorporated in the spyware was a key-logger, designed to log all of the key strokes of the computer user. This was identified as the way the cyber criminals had managed to gain access to the accounts.

The computer did have an internet security package installed which included anti-virus and anti-spyware, however, automatic updates were not switched on and scans not regularly undertaken. With new forms of malware appearing daily, the anti-virus updates must also be installed daily. In addition, the administrator and all other computer users needed to be educated as to the dangers of spyware, how it can infect a machine and prevention.

Solutions

- + Install anti-spyware, anti-virus and anti-adware
- + Exercise caution about who or what you allow access to your computer
- + Viruses could also be present so ensure you have a backup system in place and that backups are carried out regularly and stored offsite – see 'Disaster Recovery' flyer. Ensure clients, colleagues and employees are aware of infected emails and attachments and do not open any unsolicited mail
- + Run an anti-virus scan prior to backing up data as you will also backup viruses if present
- + Do not install anything from a website including free software when asked to unless it can be verified
- + Install a personal firewall to block attacks
- + If sharing files, exercise extreme caution about what is shared and ensure up to date anti-spyware is in operation
- + If using Microsoft Windows, ensure you have the updates set to automatic. Updates and patches should also be set to automatic for all software
- + If you discover a spyware infection, remove it and then change all of your passwords
- + Regularly check your bank accounts for suspicious activity
- + Consider a firewall for your server to ensure that attacks are stopped before accessing the network
- + Share examples and experiences of spyware with other users in the network
- + If spyware is detected, remove with anti-spyware, restart the computer and change all of your passwords. Consider warning your clients of the infection

Business Type	Method of Attack	Negative Consequences	Solution	Cost
BASIC + Not linked to the internet + Administration only	+ Via media storage device (flash drive / optical disk)	+ Whilst you may be infected by spyware, until you are linked to the internet no theft of data can occur.	+ Limit all access to your computer + Ensure backups are carried out – see 'Disaster Recovery' flyer	+ No cost + No cost
ONLINE COMPUTER USER + Single machine linked to the internet + Receive email/transact online + (includes laptops, smartphones, blackberrys, PDA's)	Risks the same as above but also: + Via email + Via infected website + Via file sharing + Via pop-up advert	+ Theft of sensitive data + Theft of money + Infection from viruses + Annoyance and loss of time due to continual pop-up adverts	Solutions the same as above but also: + Ensure clients, colleagues & employees are aware of email risks + Don't install anything from websites + Ensure your personal firewall is switched on + Exercise extreme caution if file sharing + Ensure all updates are set to automatic + Regularly change all passwords + Install latest web browser + Limit access to websites except for business use	+ No cost + No cost + No cost + No cost + No cost + No cost
NETWORKED + Same as above, but a collection of computers form a network (The risk increases as there are potentially more staff, increased computer business activity, therefore increased exposure to the risks)	Risks the same as above but also: + Via networked computer. One computer infecting other computers on the network	As above	Solutions the same as the above but also: + Install a hardware firewall for your server + Share examples and experiences of spyware	+ Medium-High cost + No cost
ONLINE TRADER + Uses an e-commerce strategy to sell products to a global audience	Risks the same as above	As above but also: + Loss of clients sensitive information + Damage to company reputation and loss of business	Solutions the same as above but also: + If infected, change all of your passwords and warn your clients of the infection	+ No cost

Useful Websites

- <http://www.ktn.qinetiq-tim.net/>
- <http://www.berr.gov.uk/whatwedo/sectors/infosec>
- <http://www.bcrc-uk.org>
- <http://www.businesslink.gov.uk>
- <http://www.getsafeonline.org/>
- <http://www.sophos.com/security>
- <http://zdnet.co.uk/toolkits/securitythreats>
- <http://www.sophos.com/security/spyware>
- <http://www.safer-networking.org/en/index.html>

Internet Security Packages

- Includes: anti-virus, anti-spyware, a firewall and anti-spam
- <http://www.symantec.com/en/uk/norton/>
 - <http://www.mcafee-online.com/uk/store/>
 - <http://www.kaspersky.co.uk/store>
 - <http://uk.trendmicro.com/uk/home/>