

# FACTSHEET

## Spyware Explained



### Background

The increased sophistication of malicious software programming has given rise to a new breed of threats known collectively as 'spyware'. Like 'spies', these are very small software applications that silently infect unprotected users, controlling their computers and collecting information about their behaviour before sending it back to cybercriminals.

Protecting against spyware has become a key element of best-practice information security, although many organisations still remain unaware of the threat and how to combat it.

### The Potential Risks

A single unsecured PC infected by spyware can result in enormous damage, and this effect is multiplied when spyware infects businesses. Spyware risks can include the following:

- Illegal spammers can obtain information about a user's Internet usage patterns in order to inundate them with targeted, unsolicited spam content.
- Cybercriminals, using 'keylogging' programmes, can intercept passwords entered into a user's computer; potentially enabling them to commit identity theft and gain 'authorised' access to a company network, financial databases, online banking, personal social networking profiles etc.
- Individual PCs' connections to the Internet can be controlled by 'diallers' to operate via long distance or premium rate phone numbers in order to create revenue for cybercriminals.
- Spyware known as 'hijackers' can manipulate users' web browsers or other settings to change favourite or bookmarked sites, start pages, or menu options. Some hijackers have the ability to turn a PC into a 'zombie' so that it will attack big business IT systems when commanded remotely by the cybercriminal.
- So-called 'ghost downloaders' can disable desktop anti-virus programs, leaving the user immediately prone to infection – often by duping the user into unwittingly switching off their virus protection.
- Users infected with spyware can inadvertently infect other users on the same company network or via email to the outside world

### Example

One of the most troubling aspects of spyware is its capacity to remain undetected, even once it has been used remotely to successfully commit a crime. One of the most high-profile UK examples of spyware is the failed

Sumitomo Mitsui Bank Heist of 2005, when an attempted robbery of £220m was thwarted by police. Here, keylogging programmes had been silently deployed over a sustained period and used to acquire password and other information of material use to the robbers.

### Detection

The most threatening impacts of spyware, such as usage pattern tracking, invasion of privacy and information theft, typically remain unseen and are all possible without the user having to consciously open, download or execute any applications. Just visiting an infected website is enough to become a victim.

Despite the secretive nature of spyware threats, the following offer some indicators that a spyware infection has taken place:



- Your computer is slower, indicating that spyware programmes are consuming a noticeable proportion of its resources.
- The send/receive lights on your broadband modem/router are flashing, even though you believe you are 'offline'.
- There have been changes to your web browser settings that you did not make, and changing them back may not solve the problem.
- Your anti-virus or other desktop security settings have been disabled without your intervention.

## Steps to Protection

To avoid the risk of spyware infection, consider the following steps:

1. Educate and encourage employees to understand and take seriously the risks of spyware and the measures required to mitigate the possibility of infection.
2. Avoid clicking web links to websites you are not acquainted with, or whose recommendation comes from a dubious source (i.e. a spam email or loosely connected contact met in an online business forum).
3. Ensure that users do not connect their PCs, laptops etc. to any 'untrusted' devices such as USB sticks or load CDs that arrive in the post from apparently legitimate sources. The same is true for unauthorised wireless Internet access – all of which should be covered by an agreed acceptable ICT usage policy signed by all employees.
4. Consider deploying a specialist anti-spyware solution either onto your company network, or on each employee's PC desktop.
5. Be wary of any 'free' anti-spyware programmes you are offered. While some are bona fide, there are numerous examples of fake products that are actually spyware designed to cause the very damage that unsuspecting users download it in order to avoid.
6. Consult a qualified ICT advisor with expertise in information/network security. They will be able to advise on a solution appropriate to your needs and budget, and how a strategy for combating spyware should fit alongside a broader security strategy for your entire ICT system.