



A White Paper from

 **Techcare**™

## What is Spyware?

Authored by:

John Avelis

Techcare, Managed Services Practice Area Leader

### ABOUT THE AUTHOR

John Avelis is responsible for the development and delivery of Techcare's remote services and managed services offerings. During his 10+ years with Techcare, John has been responsible for implementing and supporting network infrastructure, servers and end users in all the markets Techcare serves.



## What is Spyware?

*"If enough spyware programs infect a system, the user is likely to encounter slowdowns, crashes, software conflicts or other odd behavior"*

### What is Spyware?

Spyware is hidden software that collects information from a computer system without the user or owner's consent and sends the stolen information over the Internet to an attacker.

Information stolen can include any data stored or displayed on the system or network: Keystrokes (the actual words you type), Usernames or passwords, email information, address books, financial information, documents and screen captures are just some examples of information that attackers can use spyware to collect.

The term Spyware is often used interchangeably with the term *Adware*, which refers to freely distributed software that contains advertising. Adware often contains an invisible component that collects information and returns it to the software vendor to use in crafting their marketing.

Spyware is just one type of malicious software (also called *malware*) that threatens computer users, from individuals to the largest businesses. Spyware can share some characteristics with other malware such as viruses, Trojan horses, or worms, but the distinguishing features of spyware are the *collection* and *transmission* of information (often personal or valuable information) from the infected system to another party.

These other forms of malware (viruses, Trojans, worms) are usually installed without user interaction (as part of a web or email script) and for some purpose other than data gathering, such as destroying information on the local network, launching a distributed denial of service (DDoS) on Internet services, or simply spreading itself to as many computers as possible.

In contrast, a spyware writer will not intentionally damage the computer or network – the longer a program remains running, the more likely it is to gather and transmit useful information to the malware distributor. However, if enough spyware programs infect a system, the user is likely to encounter slowdowns, crashes, software conflicts or other odd behavior.



## What is Spyware?

While it is common for Spyware or Adware hidden in a piece of software to reveal its information gathering in the fine print of the End-User Licensing Agreement (EULA), it is also common for users to click "Agree" to a EULA without reading it, giving legal coverage to the writers of the software.

*"Clearly, spyware isn't a problem that can be avoided through obscurity, because any system is a target"*

## Am I At Risk?

A common question from small business owners is "I'm not a high-profile operation with cutthroat competitors or business 'enemies.' **Who would attack my business?"**

Many attacks on Internet-connected computers have no particular target. The attacker may be looking for unprotected systems to use for a more directed attack; they might be trying to compromise a system as a base for sending spam; or they might be staging a truly random attack, aimed at causing mayhem against any unprotected system.

In 2004, 53% of respondents to the Online Safety Study by AOL and the National Cyber Security Alliance reported having spyware or adware on their computers. However, an actual malware scan of respondents' computers found that 80% of the systems actually had spyware/adware installed.

Clearly, spyware isn't a problem that can be avoided through obscurity, because any system is a target. A competent attacker will compromise as many systems as possible in hopes of finding some valuable information.



## What is Spyware?

*“Once spyware is active on your network, you and your users have no way of controlling, or even finding out, what information is collected and sent”*

### The Impacts of Spyware

Unfortunately for small businesses, they often have more to lose from spyware than a large enterprise. A small business is often the majority of the owner’s personal wealth – a single attack that would pass unnoticed in a global enterprise can mean absolute ruin to a small, closely held business. Plus, the smaller the business, the fewer human and technology resources that business has available to counter the threat.

The negative impact of spyware on your business can be divided into three areas: The threat of lost or compromised sensitive data, the cost of lost time and productivity, and the cost of implementing effective countermeasures.

### The Security Threat to Sensitive Data

As the Internet has become indispensable in business and personal life, there is no limit to the sensitive information users store on their home and work computers. In a work environment, this might include trade secrets, the company’s financial data and confidential information about company personnel and customers. It’s this trove of data that motivates spyware authors and attackers.

Once spyware is active on your network, you and your users have no way of controlling, or even finding out, what information is collected and sent. Once it’s off your network, you can’t even know who has the information or what they will do with it.

At companies that produce digital, rather than tangible property, the value of the digital assets stored on computer systems might greatly exceed the value of the computers themselves. A vendor can replace or rebuild ruined network hardware in a matter of hours or days after a fire; not so with the years of creativity stored on that hardware.



## What is Spyware?

*“Because spyware is not written and tested for compatibility with other programs, infected computers often have reliability problems”*

If your employees do any non-business web browsing on their company-owned computers, they might also have personal information such as bank account numbers, credit card numbers and social security numbers stored on your systems.

Spyware often collects usernames and passwords that may be used for future access to the infected system. Because users often use the same username and password for many different systems, stolen credentials may be used to access other systems, which can be compromised and used to extend the attacker’s reach.

## The Cost of Time and Productivity

Companies that charge their customers an hourly rate for the intellectual rather than physical labor of employees (e.g. architects, graphic artists, attorneys) are often extremely dependent on networked computer systems. When a computer is unavailable, or running at less than top efficiency, the profitability of that employee and of the entire company suffers.

Like any other network-aware software program, spyware consumes local resources as well as network bandwidth – Even more so if it’s a form of spyware that is constantly watching and reporting user behavior. Depending on the amount of spyware loaded on a computer or network, users can face a huge performance hit.

Because spyware is not written and tested for compatibility with other programs, infected computers often have reliability problems. Applications may crash frequently or the whole system may become unstable, resulting in productivity and data losses.



## What is Spyware?

*“Educating users about common methods of spyware infection can reduce, but not eliminate, your network’s exposure”*

### The Costs of Countermeasures

According to a report by IDC, home users and businesses are expected to spend over \$300 million on technical solutions to stop spyware. This doesn’t seem like a lot of money when spread over every consumer and business consumer user – however, it only covers the cost of software, not the time and expense of removing spyware or rebuilding systems rendered unusable in spyware attacks.

It also doesn’t include the cost of outsourced labor -- any small business owner who has had to pay for hours of labor to rebuild systems knows that it can be a huge unplanned expense.

### Preventing Spyware

Educating users about common methods of spyware infection can reduce, but not eliminate, your network’s exposure. Users should be taught the basic rules of avoiding spyware infection:

- don’t install software unless you are certain of the vendor and source (it is a good idea to create network policies preventing end users from installing any software without expert approval and administrator privileges)
- don’t click anywhere in pop-up ads - including clicking the boxes in these windows labeled “No” or “Click here to close.” These are links to application installers disguised as Windows messages. Users need to learn the difference and know how to close the browser window directly rather than clicking in the window
- don’t open spam or click on links in emails that aren’t from a known legitimate source
- don’t use peer-to-peer file sharing programs
- use network policies to ensure that web browser settings do not allow script execution or installation without prompting the user



## What is Spyware?

Unfortunately, even with detailed behavioral training, spyware is still likely to infect your network. Spyware attackers are always coming up with new workarounds for anti-spyware defenses. User education is a necessary first step, but even small businesses need a spyware defense strategy.

*“Spyware attackers are always coming up with new workarounds for anti-spyware defenses. User education is a necessary first step, but even small businesses need a spyware defense strategy.”*

## Defusing Anti-Spyware Myths

The exponential growth of the Internet has led to many different security risks on Internet-connected networks and there is no “silver bullet” solution that stops every threat. Here are some facts every small business owner should know about common network security tools and spyware.

### Firewalls are not Spyware Protection

While no network should be without a firewall, and firewalls can prevent Internet-based attacks that are a result of virus or spyware infections, a firewall alone will not prevent the vast majority of spyware infections, which usually result from user interaction with malicious emails, websites or application installers.

While there are multi-purpose appliances and combination hardware/software solutions that can help prevent spyware infection restricting web browsing, do not make the mistake of thinking that any firewall you buy will prevent spyware infections or the negative effects of spyware infections mentioned earlier.



## What is Spyware?

*“Don’t assume your anti-virus is also anti-spyware; get answers from your vendor as to exactly what anti-spyware-specific features, functionality and signature updates are included in the package you buy”*

### **Anti-Virus Software**

Because of all the confusion over different types of malware, many small businesses believe their virus protection must also provide protection from adware, spyware and network-based attacks. This is not necessarily the case.

With the disparate markets served by the major anti-malware companies, it’s not always easy to know whether the features in their “personal” or “small business” editions match the functionality they advertise in their marketing materials.

Just as much as anti-virus solutions, effective anti-spyware protection requires frequent updates to detect new signatures and methods of infection. Don’t assume your anti-virus is also anti-spyware; get answers from your vendor as to exactly what anti-spyware-specific features, functionality and signature updates are included in the package you buy.



## What is Spyware?

*“The most important step a responsible owner or manager can take is asking questions of a prospective IT manager, security vendor or service provider”*

## Conclusion and Recommendation

Most network security threats can make computers and network resources unavailable. Spyware carries this threat, but is unique in that it also threatens to compromise sensitive personal and business information.

Like any network threat, spyware countermeasures require a multi-layered defense: Awareness of the threat; knowledge of the signs of spyware infections; end-user behavior modification; “Safe” web browsing practices; and technical defenses to prevent spyware installations and effectively remove spyware are all necessary parts of a defense plan.

Effective education resources for end users are available from your network support organization, or online from industry and government organizations such as the Federal Trade Commission (<http://www.ftc.gov/>), US-CERT (<http://www.us-cert.gov/>) and the National Cyber Security Alliance (<http://www.staysafeonline.org>).

It can be difficult for small business to know the effectiveness of their computer security defenses. A manager or owner usually wears too many hats to become a computer security expert on top of every other responsibility.

The most important step a responsible owner or manager can take is asking questions of a prospective IT manager, security vendor or service provider. For example,

- 1) How does this product (service) catch and prevent spyware?
- 2) When is your product updated to catch new forms of spyware?
- 3) If there is a subscription fee, does it entitle me to signature updates, new versions of the software or both?
- 4) How will this solution grow with my business?
- 5) What reporting is available to tell me how much spyware is being caught?



## What is Spyware?

### **About the Sponsor**

Techcare, through a particular focus in continuing care, ensures our customers gain the maximum value from their IT investments through a progressive set of IT outsourcing services.

Techcare assumes accountability for the management of a variety of Information Technology services including server management, security and availability of the infrastructure, end user support and help desk, hardware repair, and responsibility for helping link technology investments to your business plan.

For more information on how Techcare can deliver the results expected from IT, please contact us at [info@techcare.com](mailto:info@techcare.com) or by calling 847.374.1600.

