

What's the Fuss about Spyware?

Spyware and other threats are responsible for a range of ills from slow PCs and clogged networks to annoying ads and identity theft.

Spyware is bad stuff. Just ask Julie Amero, a seventh-grade teacher in Connecticut, who was convicted in January 2007 of risking injury to a minor and impairing the morals of a child, according to the newspaper [The Norwich Bulletin](#).

Amero's defence could be summed up as "The spyware did it." And it's very possible it did. Pornographic spyware is known to take control of one's computer and automatically serve up pornographic images. This jives with Ms. Amero's testimony that she could not control the pornographic images that were popping up on her computer in the classroom.

Businesses and other organizations need to protect themselves against the growing threats from spyware and other malicious software. At a minimum, this type of malware causes computers to run slowly or crash. Spyware and other pests clog the network, wasting bandwidth and slowing real business applications. The time and expense of cleaning up pests drain both user and IT productivity.

But the greatest danger of spyware lies in its ability to collect information, such as passwords, surfing history, Internet search strings and other personal information. Stolen personally identifiable information puts your employees and customers at risk for identity theft and it may put your company at risk of violating privacy laws and regulatory compliance mandates if a breach involves the loss of customers' personally identifiable information. If criminals use spyware and other malicious software to orchestrate the theft of intellectual property, your company can lose money or even go out of business.

Many Types of Spyware, All Bad

Spyware, quite simply, is software that gathers and transmits information about a user or their behaviour without his or her knowledge, according to the [CA Security Advisor Glossary](#). Spyware and other harmful pests like adware, keyloggers and backdoors are getting more sophisticated and daring.

Adware is by far the most prevalent type of spyware. It accounted for 45 percent of spyware threats seen in 2006 according to the CA 2007 Security Outlook Report. [Adware](#) is used to target advertising to people based on watching what Websites they've visited.

[Keyloggers](#) may record your keystrokes, capturing passwords, account numbers and other personally identifiable information as it is entered or transmitted. Criminals use these programs for identity theft and fraud. In 2006, password capture programs and keyloggers accounted for 3 percent of threats, according to CA's 2007 Security Outlook Report.

Less common but more damaging are backdoors. [Backdoors](#) are malware that exploits a software vulnerability and opens it to future access by an attacker. Backdoors are often used to control a computer as part of a botnet. Once under control of a botnet, criminals can remotely command a compromised PC to pump out volumes of spam, perform denial-of-service attacks or conduct other nefarious activities.

Spyware can be installed on a computer without the user knowing it. Spyware can be installed simply by visiting a Website. This distribution method is known as a "drive-by download." Peer-to-peer file sharing networks are a major source of spyware, as spyware is often bundled with a free program, which are shared in great numbers within the peer-to-

peer communities. Spyware and adware also come bundled into software that you intentionally download, such as a free screen saver.

Spyware can be extremely difficult to remove manually, so the best defense is a good offense. Corporations can closely govern the use of free software through the use of policy and technology. Microsoft Group Policy in Windows Server 2003, asset inventory systems and host intrusion protection systems can all be used to proactively protect against the dangers of unauthorized software installations.

Yet regardless of how secure your systems are, the threat of a spyware installation still exists. So make anti-spyware software part of your suite of security protections, including anti-virus and desktop firewall software. Be sure to choose an anti-spyware solution that both detects and removes spyware, adware and other non-viral malicious code to protect your confidential data and the performance of your PCs.