

White Paper

Online Security: A Medical Necessity

03/23/06

Index

Section	Page
Overview	3
Threat of Keyloggers	4
Medical Providers Need More Than Anti-virus Protection	5
Mitigating Online Threats	6
Resources	6
Conclusion	6
About XoftSpySE	7
Free Spyware Awareness Tool (SWAT)	7
About ParetoLogic, Inc.	8

Overview

Health care providers are bound by strict security laws, regulations, policies, procedures, standards and guidelines around client confidentiality. One of the biggest concerns is the risk involved in using the internet where patient confidentiality could be compromised due to inadequate security measures. In today's world, anti-virus software alone does not protect Internet users.

According to the Anti-spyware Coalition,

“spyware has quickly evolved from an online nuisance to one of the most dire threats facing the Internet. As users struggle to maintain control over their computers, many find themselves trapped in a cyclical battle against programs that install themselves without warning, open dangerous security holes and reinstall themselves after they've been deleted. The worst of these programs allow online criminals to hijack users' sensitive personal information at will. As the threat has grown, so has the need to mount a coordinated defense against these unwanted programs and their adverse effects.”¹

While many health care professionals have some familiarity with the Internet and its inherent risks and may be using some sort of anti-virus software, far fewer are familiar with the importance of anti-spyware applications. Spyware is now widely recognized as a bigger threat than computer viruses. According to the Computer Security Institute (CSI) and the FBI's Computer Crime and Security Survey, 99% of companies use antivirus software, but 82% of them were still hit by viruses and worms.² A recent study by Forrester Research, an independent research firm, states that “a clear majority of North American computer users (60%) fail to scan for spyware at least once a month. Furthermore, 45% of users don't even know what spyware is, much less how to protect against it.”

The potential for thieves to steal hundreds of thousands of records from a single source is now possible as documented by thefts reported by credit bureaus and other corporate entities in 2005 alone. This is in large measure due to the concentration of information and data about millions of people that is stored in relatively few places. To date there has been very little liability for companies that do not adequately protect this information, nor means of redress for the victims of such crimes, as Congress has been very slow and loathe to address the issue. Outright theft however is not the only problem, spyware can also cripple productivity.

Health service facilities lose revenue due to lost claims and computer system errors and crashes. Spyware is one of the leading causes of computer system failure and according to a June 2005 study by the Radicati Group, the cost to deal with a spyware-infected computer costs roughly \$265.00 per user for each time that a spy-ware infection is identified.³

¹ Anti-Spyware Coalition Definitions and Supporting Documents, www.antispywarecoalition.org/documents/definitions.htm

² Computer Security Institute & Federal Bureau of Investigation. (2003). Computer crime and security survey.

³ Radicati Group Report. *Corporate Anti-Spyware Market, 2005-2009*

In a spyware article in the Magazine for Senior Financial Executives, an IT support staff member at Miami Children's Hospital stated she noticed something just wasn't right with the desktop machines used by the hospital's 650 physicians and 2,400 employees. "We had machines that experienced freak reactions" says Alex Naveira, the hospital's information security officer. They were running too slow or they reacted oddly to Websites and pop-ups. After a battery of tests, the diagnosis was clear: an acute case of spyware."⁴

The Threat of Keyloggers

In medical applications, a big concern is the ability for spyware to infiltrate a system and monitor the user's actions through keystroke loggers or screen captures, placing confidential patient information and identity at high risk. Spyware programs vary in their sophistication and capabilities to monitor and record some or all of the following: keystrokes, screen captures, e-mails, chat room conversations, instant messages, Web sites visited, programs run, time spent on Web sites or using programs, usernames, passwords or other types of data in transit. This sensitive, medical and personal information is typically either stored for later remote retrieval or transmitted to the remote process or person employing the monitor.⁵

Unfortunately, spyware is usually installed surreptitiously, without the user's knowledge, capturing keystrokes, personal information, and marketing data and then sending that information to a third party. Spyware is therefore far more likely than a computer virus to intercept information that could be used to steal personal identity. While viruses and other malware caught by anti-virus software are usually intended to replicate and "take over" computers for use by the virus writer, spyware and keystroke loggers (typically called "keyloggers") operate silently in the background, reporting the information to a third party. If they go undetected by a doctor or medical center that is known to have access to patient records and that information is lost, the liability under HIPAA will rest on the providers, since the third party who monitored their computers to steal the information is long gone or not easily traced.

Keyloggers have existed in some form for many years. The growth of spyware in this decade has resulted in a mass propagation of the technology. In an article on the spread of spyware infections via the Internet, the respected Internet research firm Gartner Group reported, "At mid-2004, Gartner customers are seeing a surge in manifestations of 'spyware,' invasive methods to steal user privacy that disrupt users and their workstations at home and at work. Customers report that the cleanup effort may take a few hours, but that in no time at all, the same systems are infected again."⁶

Keyloggers present one of the major risks for the medical industry especially for those people that use computer practice management (CPM) or electronic health records (EHR) software or interacting with Internet sites. They will typically generate a log file or even screen shots of what is on the user's desktop, and email or download this

⁴"Somebody's watching you: spyware has come in from the cold to become corporate America's top security threat", [CFO: Magazine for Senior Financial Executives, Summer, 2005](#) by [John McPartlin](#)

⁵ Anti-Spyware Coalition Definitions and Supporting Documents, www.antispywarecoalition.org/documents/definitions.htm

⁶ Gartner, "A Field Guide to Spyware Variations," John Girard, July 2004

information to a server somewhere on the Internet. These user logs or screen shots can then be used to harvest personal information including details of patient claims or medical records from the unsuspecting user causing violations of HIPAA laws and putting practices at risk.

Medical Providers Need More Than Anti-virus Protection

Anti-virus software alone (such as programs available from well-known antivirus suppliers) does not adequately safeguard against spyware or help make computer systems HIPAA-compliant. The financial implications of having a security breach explain why the Radicati Group reports that the number of anti-spyware programs installed on business computer systems will increase from 16 million in 2005 to 540 million in 2009, and the anti-spyware industry is projected to reach 1.2 billion in revenue by 2010. Realizing that highly confidential information, including banking and patient information, is at risk, the IT and office managers of leading health facilities will be employing anti-spyware tools.⁷

In order to ensure that patient information and identity is not jeopardized, an anti-spyware program that will help eliminate security threats is critical. According to a recent article by Arthur Gasch, MSP Industry Alert, "MSP has found that not all programs are the same in terms of scan speed or the number of security threats detected and removed. Ideally, an anti-spyware detector should not drag down machine performance, should run quickly and still catch all the risks. That is the ideal combination. But it doesn't matter how fast a spyware detector runs if its false-negative performance misses actual spyware programs installed on your system."⁸

Mitigating Online Threats

1. Install, run, and regularly update anti-spyware software

There are many security programs available for download and trial on the Internet. If you are using a Microsoft Windows operating system on your computer, ParetoLogic Inc. publishes and sells a leading-edge anti-spyware solution, XoftSpySE (available at <http://www.paretologic.com/industry/health.aspx>) which includes state-of-the-art detection and removal of known keyloggers and spyware aimed at identity theft. A free Spyware Awareness Tool (SWAT) is available to determine if a user's computer has any threats or infections. In the event spyware is detected the user can purchase an annual license for the fully functional program including removal tools and customer support.

XoftSpySE is designed to scan the user's complete computer system to detect spyware parasites and quarantine the infected files for immediate protection. The scanner should be installed on every network server and workstation. In addition to scheduling XoftSpySE to automatically run once in the morning and later in the day, we recommend that you run it manually after every Internet browsing excursion. For those workstations or servers that are directly connected to the Internet, a scan should be scheduled at least 3 times a day. XoftSpySE will help meet health professionals' need for high-performance, comprehensive, scalable, and customizable tools that detect online threats faster and

⁷ Radicati Group Report. *Corporate Anti-Spyware Market, 2005-2009*

⁸ MSP Industry Alert, *Electronic Health Records & Online Security: Medical Necessity*, April 2006, pg.26

more completely than other anti-spyware companies. Regular use of XoftSpySE will provide ongoing protection against spyware, keyloggers and other forms of malware helping medical providers stay HIPAA-complaint.

2. Ensure that your operating system is up-to-date

Due to security challenges faced by the most popular operating systems, the major software companies that create and license them offer continual patches and updates to ensure the integrity of your operating system remains intact. Updates are typically automatically downloaded to your computer, but you are responsible for installing them. If you run Microsoft Windows, you can visit Windows Update at www.windowsupdate.com.

3. Increase your knowledge of prevention techniques

The following resources are available to assist you in determining if you are at risk, and to respond to threats if you believe your personal and/or client information has been obtained by an unauthorized source:

<http://www.spywaredaily.com/>

Internet blog about Spyware, Adware and other Internet threats

<http://www.paretologic.com/industry/health.aspx>

Free Spyware Awareness Tool (SWAT) available by download

<http://www.ic3.gov/>

Internet Crime Complaint Center provided in the U.S. by the FBI

<http://www.usdoj.gov/criminal/fraud/idtheft.html>

Identity Theft and Fraud web site of the U.S. Department of Justice

<http://www.consumer.gov/idtheft/>

U.S. Federal Trade Commission web site on identity theft

<http://www.fraud.org/>

National Fraud Information Center

<http://www.justice.gc.ca/en/ps/ec/index.html>

Department of Justice, Government of Canada

Conclusion

As health care providers are bound by strict security laws, regulations, policies, procedures, standards and guidelines around client confidentiality, the risks posed by online threats to breach of confidentiality are high. In today's world, anti-virus software alone does not protect Internet users from spyware, identity theft or other electronic threats. Taking the three simple steps outlined in this white paper will decrease your likelihood of suffering identity theft or the loss of personal and/or client confidential information.

There are many anti-spyware programs available for download and trial on the Internet, however not all programs are the same. There are several important differences in anti-spyware programs such as scan speed, and number of security threats detected and removed. Faster detection scanning is preferable, but, it doesn't matter how fast a spyware detector is if it misses actual spyware programs installed on your system.

Medical Strategic Planning highly recommends ParetoLogic's XoftSpySE and calls it the best protection for computers running Microsoft Operating Systems. In an article in the MSP Industry Alert, author Arthur Gasch of MSP states, *"we have found XoftSpySE to be the fastest of the programs we tested that didn't miss spyware threats and did not drag down computer performance to a crawl while it was scanning. Perhaps it is so effective because Paretologic already has compiled one of the largest detection and removal databases in the industry."*

About [XoftSpySE](http://www.paretologic.com/industry/health.aspx)
(available at <http://www.paretologic.com/industry/health.aspx>)

XoftSpySE is an industry leader in advanced spyware detection and removal. XoftSpySE features a leading-edge anti-spyware solution that includes state-of-the-art detection and removal of known keyloggers and spyware aimed at identity theft. XoftSpySE is fast and has one of the largest detection and removal databases in the industry, providing powerful protection to secure your privacy and your PC.

Key Benefits:

- Provides complete PC scanning, checking processes currently running, registry entries, files and folders
- Detects and removes: adware, spyware, pop-up generators, keyloggers, trojans, hijackers, and malware from your system
- Protects against more spyware threats using one of the largest spyware definition databases in the industry
- Automatically keeps its code and threat database current, transparently to the use, so you always have the most up-to-date protection (during each 1-year license period)
- Operates quickly on your computer, not dragging down the performance of other programs that are concurrently executing
- Helps assure the privacy of your patients' confidential information, to help keep your electronic medical office HIPAA-compliant
- Provides you with no-charge customer support
- 60-day money back satisfaction guarantee

Free Spyware Awareness Tool

As spyware generally installs on your system without your knowledge or consent you may be surprised to find spyware detected on your system. We encourage you to give your computer, like your patients, a physical "check up" to determine the presence of spyware. Download and use our **FREE Spyware Awareness Tool (SWAT)** to ensure the security of your personal and business computers located at <http://www.paretologic.com/industry/health.aspx>. An annual license for the fully functional program including removal tools and customer support may be purchased for the program to remove any identified threats.



**About [ParetoLogic Inc.](http://www.paretologic.com)
(www.paretologic.com)**

ParetoLogic is an international software development company headquartered in Victoria, British Columbia, Canada. A member of the Software Industry and Information Association (SIIA), we specialize in providing advanced security applications for enterprise, business and personal computer users. These include custom software solutions for business and government.