



Why should small and medium-sized businesses be concerned about spyware?

An article on spyware risks contributed by a leading independent researcher



Ask typical consumers about spyware, and these days they'll say it's a big problem. They're right. Spyware programs often show annoying popups, while creating extra risks to security and privacy. But serious as these problems are for typical computer users, they're even worse for businesses. Let me explain.

Privacy

The "spy" in spyware correctly suggests risks to privacy. Many spyware programs primarily track what web sites users visit and what searches they conduct. This might seem innocuous, but it can paint a surprisingly detailed picture of your company's operations. Considering an acquisition? Bugged by a competitor? Developing a new product? Your employees' web browsing gives away many of the details. Even so-called "adware" programs (which largely focus on advertising rather than outright spying) typically track, transmit, and store this information.

The most outrageous spyware programs take privacy invasion to the extreme – installing malicious tracking to record passwords, PIN numbers, or even all keystrokes in any Windows program. With this information, a hacker could access your network – even download customer lists, whether for spam or for competitors. These problems are more than speculative: In 2003, hackers stole the source code for a popular video game just before release. More recently, even law enforcement officers have been targeted. Although these targeted attacks remain relatively infrequent, their potential cost is staggering. Losing product designs or customer lists to a competitor or to the public at large could mean the end of some companies – not to mention potential legal liability for customers' privacy and investors' losses.

Performance, Reliability, and Productivity

Beyond effects on privacy and data security, spyware is also often detrimental to computer performance and reliability. Spyware-infected PCs often take extra time to boot up, load programs, and retrieve web pages. These delays occur because spyware programs typically run all the time, without users affirmatively requesting them. So an infected PC could be running a dozen hidden tasks in addition to the programs users actually want. These extra programs add substantial additional complexity, with resulting risks: If even a single spyware program crashes, it could take Internet Explorer or Windows down with it.

In a business setting, it's also important to consider the effects of spyware on productivity. Even a web browser toolbar takes screen space that could be used for more useful purposes – so handy toolbars like Google's are usually OK, but second-tier toolbars are less likely to earn their keep. Other spyware programs come bundled with trinkets like screensavers or games – which generally aren't appropriate on office PCs. Remove this junk from users' computers, and they'll have fewer distractions wasting their time. Plus, you'll free up disk space and memory, and even reduce the size of PC backups.

Why should small and medium-sized businesses be concerned about spyware?

An article on spyware risks for SMB contributed by a leading independent researcher



Special Problems for Business Networks

These days, it's a rare business that isn't networked. But LAN file-sharing offers an additional way for spyware to spread. I've recently observed spyware that propagates through Windows file sharing. Frighteningly, if one machine on your network gets infected, it can spread to all the rest. Finally, repairing the damage from spyware is particularly costly in a business setting. When computers are slower or less reliable due to spyware infections, that's real money down the drain – time wasted and data lost. Even the process of cleaning a PC costly: A computer's primary user has no computer while a technician repairs the infected PC, so the infection wastes both the user's time and the technician's. If a computer can only be repaired by restoring a fresh Windows installation, the process is that much more tedious: Data files and program settings must then be copied, lengthening the procedure and risking further losses.

What To Do

What to do in the face of increasingly sophisticated attacks? If you observe specific symptoms – extra popups, unusual crashes, or just a slow PC – then get an anti-spyware scanner and run a test. And with the high costs of after-the-fact removal, consider a spyware protection system that will try to block unwanted software before it gets installed.

The Internet isn't the safe place many of us remember fondly. But with a bit of planning and the right tools, your network can be far better protected.



About Benjamin Edelman

Benjamin Edelman is a researcher studying spyware, especially installation methods, privacy effects, and revenue sources. Ben has also served as an expert or consultant in a multiple cases against purveyors of spyware, including the successful Washington Post / New York Times suit against Gator. Ben's spyware research is posted on www.benedelman.org.

Trend Micro Security Resource Center

Helping you protect your business.

The Trend Micro Security Resource Center helps you protect your business from viruses and other Internet threats by providing timely threat information, expert advice, and simple, effective tools.

www.trendmicro.com/smb/security



Trend Micro Inc.

10101 N. De Anza Blvd.
Cupertino, CA 95014, USA
toll free: 1+800-228-5651
phone: 1+408-257-1500
fax: 1+408-257-2003
www.trendmicro.com

Trend Micro, and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.