



100 Superior Plaza Way, Suite 200  
Superior, CO 80027

O 303.381.3800  
F 303.381.3881

## Is Your PC Secure? Unlikely, Study Finds; More Vigilance Needed; Research finds wide use of malicious code, which can be hard to outsmart

BY DONNA HOWELL

*Originally published in the Investor's Business Daily, April 6, 2006*



Applying patches and updating anti-virus programs are good starts. But they're not enough to ensure the safety of your personal computer.

That's the finding of researchers at **StillSecure**, a network security firm. In a test, the company protected computers in different ways and watched to see which ones got infected when attacked. Their results suggest that users need to take a few extra steps to successfully secure their systems.

The computers in the study encountered a wide range of malicious code -- so-called malware -- says Mitchell Ashley, **StillSecure's** chief technology officer.

"Malware is used more than just to compromise your computer and steal your data," he said. "It can also be used for other malicious intent, as spyware or to present ads."

Attack programs often look to see what security products are in place and work around them, Ashley says. They also deposit programming code that's hard to remove and can reinfect the machine later.

Some attack security software directly. "It's very possible (security software) could be disabled and the end user would never know it," Ashley said.

Spyware, which snoops on a user's activities, is on the rise. So is adware, which delivers unwanted ads to PCs. Unlike traditional viruses and worms -- written mainly just to make trouble -- such programs can generate money for hackers.

Malicious code writers earn anywhere from 5 to 20 cents each time they are able to download adware to people's PCs, says Dave Cole, director of security response at the software firm Symantec. That's driven them toward more sophisticated attacks, he says.

Consumers have to be very smart to avoid becoming victims, Cole says. "The level of consumer knowledge that's required and how much they're in the cross hairs of attack has increased," he said. "The bar has raised."

To test what worked in security, **StillSecure** researchers outfitted computers with the Microsoft Windows XP operating system. They then set up each with one of four security schemes.

The first was lax security: no firewall, no software patches, no anti-virus or anti-spyware software, and low Web browser security settings. The second added anti-virus software but didn't update it, and applied software patches with a five-day lag after their issuance.



The third updated the anti-virus software and kept patches current. Browser security settings were ratcheted up a notch to medium-low. The fourth had the works: a firewall, up-to-date patches, anti-virus and anti-spyware software, and browser security settings on high. "We take a series of computers and load them up with the software an end user would have on their computer and secure them in a less and more secure fashion," Ashley said. "And then they go out and surf the Web."

In the experiment, each computer was sent automatically to the same bunch of Web sites -- some that weren't known to harbor attack code and some that were.

Not surprisingly, the system with the lax security scheme had many virus and spyware infections.

The second computer's minimal security greatly reduced the incidence of infection -- especially with viruses. And the third and fourth schemes provided progressively better protection. But even the systems with the highest security settings had some problems.

Still, the results show that every little bit of security helps, Ashley says.

"One of the key factors in this is the security of the device," Ashley said. That means it's key to have the right safety settings in the browser software and other programs.

"A second factor is the behavior of the end user," he said.

Applying patches as soon as possible and keeping anti-virus programs up to date proved vital to warding off attacks.

\* \* \*