Computer spies

How to protect your business from spyware **Interviewed by Chelan David**

Spyware is a general term used for software that gathers information about Internet users without their knowledge or consent. Symptoms of an afflicted computer can range from intrusive pop-up ads to frequent crashes.

But a stealth spyware program can be the most dangerous. Quietly embedded, a user might not even be aware that a hidden program is recording passwords and other confidential and private information.

Like viruses, spyware programs mutate at a swift pace. Fortunately, protection for computers has evolved as well.

"Spyware is now recognized as a threat, and protection is available through enterprise level software," says Hormazd Dalal, president of Castellan Inc.

Smart Business spoke with Dalal about the importance of protecting yourself from spyware and the transformational nature of viruses.

Hormazd Dalal
President
Castellan Inc.

What is spyware, and how does it differ from viruses?

Spyware is a malicious code designed to monitor activity on a computer. Examples of this include basic monitoring and the more malicious key loggers, which means that the perpetrators write a program that sits on the computer and then logs your keystrokes. This means they could log passwords that you are typing in or your credit card/Social Security numbers, etc.

Basic monitoring spyware is more annoying than malicious. They record what you do, how long you spend at each site, and then they force pop-up ads on you. Generally, it's used by marketers, but it can plague a computer because it spies on the way you're working.

Viruses, on the other hand, are in a different category, and they are written to do damage on your computer. Spyware is different from viruses but equally malicious.

How have computer threats changed over the years?

Spyware is relatively new. Computers have started to get infected by it over the last 18 months to two years. Just like viruses, new ones are written every single day by somebody out there with different objectives, from making sure that you go to a certain homepage to tracking where you've been, to sending pop-up ads to you.

How can a business protect its network from spyware?

Just like with viruses when they first came out, there were standalone tools to help with protection. Now most businesses are well-protected from viruses because they have enterprise-level monitoring and management services.

These services check viruses before they come into a network and monitor the virus definitions on the work stations centrally, so you can look at one computer and do a sweep of the entire network.

Likewise, there are some manufacturers making very good enterprise-level spyware protection. This software sits on the server and deploys the latest definitions through every workstation in the network and implements levels of spyware protection — from making sure that your homepage isn't hijacked to making sure that something isn't added to your start-up programs.

How important is it for a business to protect itself against spyware?

As important as protecting yourself against viruses. In fact, possibly more, because without it, you risk having identity theft and your computers can slow down and freeze. And, of course, pop-up ads can become an annoyance and reduce productivity.

How does a business know if its computers are infected with spyware?

Invariably, you will go to your homepage and you will find that it has been hijacked and you'll be getting pop-up ads. But in some cases, you don't know because it's just logging everywhere you're going on the Internet and it's not taking up (many) resources.

With a slow PC, you can tell. Fast PCs just manage to let that process run.

With a serious infection, the user will know about it but might not notice a minor infection.

What steps should a business take if it is infected by spyware?

There are several removal tools available.

Typically, you need a professional or an IT person to come in who knows how to run these tools. Sometimes systems need to be brought down into safe mode before they can be cleaned up.

In some very, very extreme cases, the computer needs to be rebuilt with the software being reinstalled. This is a last resort, which is both expensive and time-consuming, which is why the protection is so important.

HORMAZD DALAL is president of Castellan Inc. Reach him at (818) 789-0088, ext. 202, or hormazd@castellan.net.

Insights Technology is brought to you by Castellan Inc.