

Assessing The Spyware Plague

When one rep complained about how slowly his computer was operating, two of his breakfast partners simultaneously hissed the word “Spyware.” When he passed on his questions about spyware to *Agency Sales* magazine, we went to an expert.

Three years ago, if a computer user ventured online minus the proper protection, it might take him 15 minutes to get infected with some form of spyware. Today, give him in the neighborhood of 15 seconds before he falls victim to the same fate.

That’s what David A. Milman, founder and CEO of RESCUECOM, a Syracuse, New York-based franchisor in the computer services industry, offers in partial response to *Agency Sales’* questions on the subject of spyware. Milman, whose company delivers business and sales resources from computer technicians and consultants on a one-hour on-site response basis, maintains that the question is very timely given the insidious nature and continued proliferation of spyware on the Internet.

One definition of spyware is “any software which employs a user’s Internet connection in the background (the so-called “back-channel”) without their knowledge or explicit permission.”

According to Milman, there are three danger levels that can

be associated with various forms of spyware:

- **Low** — “This type emanates from people who write spyware just so they can say they’ve done it. It will result in a performance hit on your computer. Your processing cycles will take longer and overall it will create large speed reductions. Chances are when you hear someone complain about speed decreases on their computer, they’ve got spyware.”

- **Medium** — “This level is achieved by a combination of spyware and adware (those annoying popups that appear on your computer, such as when you’re surfing the web and an ad comes up behind a browser.)”

In an effort to explain the persistence of adware, Milman says, “We did a study on the effectiveness of these ads and learned that people only fall for them one percent of the time. These ‘advertisers’ don’t care, however, because there’s no cost for advertising in that manner. The result is they clog computers. All the same, however, the danger of identification theft begins to present itself. Software has been loaded on your computer and it captures your keystrokes. Your personal information may be captured and stolen.”

- **High** — “This is the identity theft level. This is where spyware acts just as a ‘spy’ would. Typically



you receive what appears to be a genuine e-mail. You open it and nothing is there. This can open the door to all your private Internet activities including purchases and online banking.”

Getting Rid of What You’ve Got

If it’s determined that spyware has wormed its way onto your computer, it’s imperative to have it removed, according to Milman. “In getting that done, you’ve got to be careful,” he cautions. “There are a number of people that call themselves consultants. They may have come from a factory job, and now think they know something about computers. I’ve even heard of occasions where the ‘consultant’ hired is, in

fact, the carrier of the virus.” Milman urges computer users to be careful whom they contact to fix their problems “because, chances are, you can’t get rid of it yourself.”

For more information on RESCUECOM and the services they offer, visit the company’s web site at www.rescuecom.com.

In addition to this company, readers should keep in mind the advice that appeared in this column last month regarding the need to get professional assistance when it comes to tech concerns. Seek out someone competent, someone who has experience and someone who has your best interests at heart.

Help on the Net

The following tip comes to us courtesy of the The NonProfit Times Weekly (www.nptimes.com):

**Technology ...
PC Problems? Use the Web.**

Oh-oh, your PC seems to be sick. It’s acting funny, and you don’t know what to do. Assuming that you’re not a repair technician in your spare time, and

If there are any subjects that you feel should be explored in Tech for Repls, or if you have any comments about this subject, please contact the Tech Talk editor at: alaplante@MANAonline.org.

don’t have a toolbox full of diagnostic applications and hardware test cards, your first impulse is probably to run for help.

Before you panic and pack up the system for a trip to the computer store repair shop, there are some things that you can use to try to determine your PC’s state of health (or lack of the same). All you’ll need is a good quality connection to the Internet. High-speed broadband is best, but you can even get by with 56K dial-up if necessary.

The Internet connection lets you find helpful sites that can lead you through troubleshooting and identifying problems that might exist on your PC. Also available are lots of software tools, many free for the downloading, which let you test the components and peripherals that comprise your computer system.

A good place to start is www.pcpitstop.com. This site sells a variety of reasonably-priced

utilities. It also has a diagnostic test that you can run directly from the site by downloading a small software utility. This utility and the test do not change anything on your PC, and is safe to run. At the end of the test, you are presented with the results, and if any problems are found, the utility offers to fix them for you.

For troubleshooting guidance, take a look at www.pcguide.com. This site features an expert system that queries you on what symptoms your PC is showing, then suggests possible causes and solutions. It’s completely free and a good resource. Another great site for help with troubleshooting your PC is www.arstechnica.com.

One thing to keep in mind before you start fiddling with your PC’s innards is: It’s always a good idea to back up the data and applications residing on your hard disk. That way, even if your PC is inadvertently nuked, you’ll be able to restore critical data. □