Holzsager Technology Services, LLC
P.O. Box 535, Fair Lawn, NJ 07410-0535
(201) 797-5050 info@tech4now.com
Visit us on the Web at http://www.tech4now.com

Bogged down with Spyware

by Fred W. Holzsager

Many of my clients call and complain that their computer systems are running slowly or hang or have a gazillion pop-ups. It doesn't matter whether you have cable in Fair Lawn or DSL in Bergenfield, the neighborhood is infected. Is the problem local? To an extent it is. Can the scourge be stopped? To some degree, yes. If you move to the Hackensack, will it stop? Not necessarily. Many of your neighbors have been hit by spyware.

Spyware is the executable software that is downloaded onto a host computer by an unknowing participant. Typically, a user will install the software at the same time that a desired program is loaded. At times, the software will be mentioned in the License Agreement of the "good" software; at times, it won't. What spyware does is track your information (shopping habits, sites visited, usernames and passwords and payment info) surreptitiously to report back to its developer. In other words, it spies on you as you surf the Internet.

Spyware is a form of MalWare (malicious software) which will often "attack" a system, causing it to perform poorly or hang. Some spyware programs will only work as AdWare and reroute your personal information to sponsors or hijack your browser to visit an "alternate" site of comparable interest. Such programs might detect that you want to buy flowers by entering in a URL (*sic* web address) to visit one florist, detect that you are about to visit a non-sponsor, reroute you to the URL's competitor. You weren't paying much attention to the name on the site, got redirected, saw flowers on the screen and proceeded to patronize the sponsored florist—it's that simple!

I mentioned above that the problem was local. Even though the Internet is a worldwide resource, your access point to it **IS** local. Some people connect through broadband, others use dial-up. Either way, it is a connection to the Internet at a single computer. The question then emerges: Is the computer protected?

Most end users are savvy enough to have computers running antivirus software. They recognize that it can protect them against viruses, but not all end users recognize that spyware and adware are not necessarily considered viruses. As mentioned above, many are installed by the end users, thus they are considered "welcome" by definition. Viruses are not invited and attack a system, but who would intentionally install a program on their machine that was undesirable?

Earlier versions on Symantec's and McAfee's products worked under this premise. Nowadays, however, spyware has become so prevalent and such a

nuisance that their "viral signatures" are now being traced. Score one for the good guys! The "gotcha" is that many users are still under the impression that they are protected because they are using an antivirus program. The bad news is that even if you have the latest virus definitions downloaded onto your PC, you may still be susceptible to spyware because the program does not look for it. IT IS CRITICAL TO NOT ONLY UPDATE YOUR VIRUS DEFINITIONS, BUT TO OCCASIONALLY UPGRADE THE PROGRAM, AS WELL! Sorry for yelling, but it is too important to overlook.

Joe from Plaza Road has purchased an upgrade because he realized something was wrong with his system. He installs the program, runs the update and performs a full scan of his system. Alert! A virus has been detected. Joe follows the easy to understand instructions in the program—Delete or quarantine the files. Quarantine fails, delete fails. Now what?! Well, if Joe is comfortable with his computer, he may try some of the built-in utilities that come with the Windows program. Many times, an end user's comfort level might not go that high. So, you call in a computer consultant to remove it. You consider the time and expense and become annoyed with the situation. What could you have done to avoid this situation? Consider these three points to computer security: Virus protection, system updates and firewalls.

Is it difficult to perform those three items? No. As a matter of fact, most of them are set and forget (but not for too long):

Windows Updates: If you are running any version of Windows 98 or later with Internet Explorer, select Tools, Windows Update. Have the system scanned for updates and install. If you are on Windows 2000 Professional, go to the Control Panel, click on Automatic Updates or with Windows XP, right click on My Computer, Properties, on the Automatic Updates tab, click on download and let me install, check off the Keep my computer up to date box and you're set. Just make sure that you perform the installs in a timely manner once the updates icon  appears in the lower right corner (system tray). It's also a good idea to run the Office Updates to maintain security on your application suite. (My humble apologies for the Microsoft assumption.)

Antivirus Updates: The two most visible antivirus software vendors are McAfee and Symantec (Norton). Both providers, as well as others, make the updates a mindless task: Set the program's configuration to perform automatic updates without interrupting you and you're set. Whenever you are online, the program detects the connection and downloads/installs the updates in the background—no mess, no fuss! Keep in mind, however, that updates are not the same as upgrades. Occasionally, it is well worth it to buy the upgrades. (The newer versions can detect spyware and adware in addition to viruses.) In fact, the competition is so stiff that consumers are often rewarded with mail-in rebates for upgrades, even after deep discounts have been made by vendors on

the software. To qualify for the rebates please read the instructions BEFORE installing the upgrade.

Firewalls: Firewalls come in two implementations: hardware and software.

A software firewall is a program which helps your computers filter out which programs may communicate across the network/Internet. Software firewalls have one significant drawback, at their onset, they must identify which programs you will allow to pass through to the local network or Internet. As a result, they will often prompt you with dialog boxes to verify which programs are allowed and which should be blocked. If you have children on a computer with a firewall, you may wish to have them ask for your assistance if the prompts appear, otherwise, they may grant permission to malware for access to the Internet.

The hardware version is a physical device that is modestly involved to install. Most vendors provide a self-install CD with decent documentation to perform the installation on your own. The hardware firewall will create a private network for your computer(s) to access the Internet using a single broadband connection in addition to its filtering capabilities.

Both firewalls may work together to afford you an even higher degree of protection. Be aware, however, that new threats are developed everyday, thus even a combination of firewalls can be breached. A nice complement to the software firewall is a pop-up stopper and/or a content filter. The "stopper" helps to reduce the incidence of annoying windows popping up when you browse; whereas, the content filter can help you control (censor) where your children may visit on the Internet.

I cannot stress enough that an ounce of prevention is worth a pound of cure. Whenever you are on the Internet and see an offer which appears too good to be true, it probably is—*caveat emptor* (let the buyer beware!). Trusting your intuition is one of the most reliable weapons against attack: take your time before clicking on the OK button, read some of the text boxes and be selective about the sites that you visit. Mind you, with some worms, it won't matter, but if you maintain your systems regularly, you will have installed many of the needed features necessary to ward off the scourge of malware.

If you are interested in learning more about the items discussed above, feel free to contact Holzsager Technology Services, LLC at (201) 797-5050 or by e-mail at support@tech4now.com. For general information about other services for your home or office, kindly visit www.tech4now.com, there you may retrieve additional information bulletins and articles to help you use technology to your fullest advantage.

