



Spyware, Trojans and Keyloggers. Oh My!!

Bits & Bytes

Bits & Bytes is a monthly newsletter for home users who want to stay up to date on the newest technology, tips, tricks and trends.

So you thought you were safe?

What would you say if I told you to unlock the windows and doors in your house, and after doing that to open them wide? This would seem like a strange request leaving all of your important possessions inside something that was not protected. You would probably think this was a crazy idea.

Now what would you say if I told you that your computer was very much like this house in that the Windows operating system allows programs called spyware to enter and install themselves without asking. These programs have access to your browsing habits and, in some cases, banking and credit card information.

So how do you protect your computers when Microsoft will not?

This issue of *Bits and Bytes* will explain what spyware is, how it gets onto your computer, and, most importantly what steps to take to fight and prevent it.

What is Spyware?

Malware, trackware and adware are all forms of spyware. You may also hear keylogger, trojan, system monitor, browser hijacker, and dialer used; these are also forms of spyware. The definition of spyware from dictionary.com is "Any software that covertly gathers information about a user while he/she navigates the Internet and transmits the information to an individual or company that uses it for marketing or other purposes."

Usually this is done without your knowledge or consent. Anyone who uses a computer attached to the Internet is susceptible to a spyware infection. Whether you are surfing the Internet or checking emails you can attract spyware files, applications or programs.

These programs do not always ask to be installed. They will install themselves in the registry, startup menu, files and folders. The varied ways spyware can get onto your computer are what makes it so dangerous.

Spyware can be installed by a

hacker, someone else who uses your computer, through a pop-up window, an ad, via an instant messenger service, through spam email or through attachments on an email. Other common places to receive spyware are file-sharing programs such as Kazaa and Limewire.

Sometimes spyware is bundled with a desired program, and it is disclosed as part of the EULA, or end-user-license agreement (the thing you have to say "I agree" to before a program will install) however it is buried way down in the EULA where most people will not read it. In some cases it is as easy a visiting the wrong website and spyware will just hop onto your system.

There is spyware that is mostly benign, such as adware tracking cookies, which allow online companies to track your activities on a website and tailor pop-up advertising messages based on your choices. Then there are the malicious types of spyware like trojans, keyloggers and system monitors, which are capable of

capturing keystrokes, online screenshots, and personally identifiable information like your social security number, bank account numbers, logins and passwords, or credit card numbers.

Aside from the personal information that spyware steals from you, many spyware programs will tax your computer, making it extremely slow, and will steal your internet bandwidth as it "talks" to the spyware's home base using your internet connection.

In summary, all forms of spyware are bad. The worst forms of spyware will capture all of your keystrokes and then send them to a hacker. This means everything that you type, every username, password, credit card number, address, social security number, etc.

On the backside of this newsletter we will look at what can be done to stop spyware from gaining entry to your PC, as well as removing and detecting spyware already present on your PC.



Protect, Check and Clean

Protect

Update, update, update. This cannot be stressed enough. Microsoft releases updates to Windows on a regular basis. These are very important to your computer. Windows allows you to set automatic updates when it connects to the Internet:

* On a Windows XP machine right-click on the "My Computer" icon (either on the desktop or in the Start Menu) and select "Properties" click on the "Automatic Updates" tab and put a dot next to "Automatic" to have the updates automatically managed by windows.

* On a Windows 2000 or 98 machine, click on "Start", "Settings", then "Control Panel" and look for the "Automatic Update" icon. Double-click on it and select the "Automatic" option.

When you update Windows, you patch up holes that allow spyware to enter your PC. You also need to make sure that there is a firewall protecting your PC. Some routers have a built-in firewall, and there are software firewalls that can be bought if you need. Some good software firewalls are: Zone Alarm (www.zonelabs.com) and Sygate (www.sygate.com). If you have Windows XP you have a firewall built right into Windows and can enable it by clicking on "Start", "Control Panel", "Windows Firewall" and then putting a dot next to the "on" option.

Check and Clean

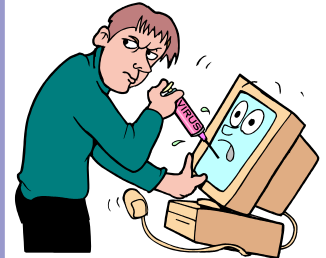
There are a few programs that will check for and rid your computer of spyware. We recommend using at

least two of the programs together to increase effectiveness. The programs are:

- * Microsoft AntiSpyware Beta (www.microsoft.com/downloads) - 6.3MB -free;
- * Adaware SE Personal (www.lavasoft.com) - 2.5MB - free;
- * Spybot Search and Destroy (www.microsoft.com/download) - 4.15MB - free;
- * SpySweeper 3.5 (www.spysweeper.com) - 3.7MB - free to try, \$29.95 to buy.

If you own Windows 2000 or Windows XP, the best free choice for you is Microsoft AntiSpyware Beta because of its ability to protect you in real-time, stopping the spyware before it gets onto your computer. As a pay version of a real-time spyware stopper, SpySweeper 3.5 is the best choice. No matter which, if either of the above programs are used, we recommend using both adaware and Spybot Search and Destroy along with them, which are both free. Using these free programs also increases your chance of catching anything that another program may not. We recommend scanning once or twice a month, depending on how often you are downloading files and browsing the Internet.

Similar to antivirus programs, the above-mentioned programs will not be effective unless they are updated before being used. All of the programs listed either automatically update or have a button to update them. Always update before scanning. After the scan has completed it will list anything found that is suspicious; we recommend removing all found threats.



Indications of Spyware

When you start your computer, or when your computer has been idle for several minutes, your Internet browser opens and displays advertisements.

*

When using your browser to view web sites, advertisements pop-up.

*

Your web browser's home page changes without you changing it.

*

Web pages are being added to your Favorites folder.

*

New toolbars are added to your Web browser.

*

Your Web browser suddenly closes or stops responding.

*

It starts taking a much longer time to start/resume your PC.



**Working for you
when your computer is not.**

REALM 249, LLC

Phone: (847) 738-0249
Email: support@realm249.com

Watch Out!!

There seems to be a myth that antivirus software such as Norton Antivirus, or McAfee VirusScan will protect you from spyware. This is incorrect.

Most antivirus products are built for one purpose: viruses. Do not feel safe if all you have done to protect your PC is to install antivirus software.

Also beware of other spyware removers. Many trick you into downloading them when in fact they are actually spyware in disguise. This is not to say that there are not other legitimate companies that offer spyware detectors and removers, but please be safe, and use a reputable company. If there is ever any doubt in a program's legitimacy call us, and we will look into it for you.