THE DAYS OF CARELESSLY SURFING THE INTERNET ARE GONE!!!!

The Internet used to be a place that you could carelessly surf for whatever information you wanted. While the Internet continues to grow everyday so does the potential threats. There are over 78,000 pieces of SPYWARE/MALWARE roaming around the internet just looking for a host machine to infect.

What is SPYWARE?

SPYWARE are applications, programs, or files that hide on your PC's hard drive without your direct knowledge. These programs allow hackers and advertising companies to track your every move whether you're online or not. They track the sites you visit, the items you buy, the emails your send and receive, and your Instant Message dialogs.

What is MALWARE?

MALWARE is malicious forms of SPYWARE that causes more harm than the traditional forms of SPYWARE. Most forms of SPYWARE are used for advertising. MALWARE on the other hand can record your credit card numbers, personal identification numbers, and all of your passwords. If you use a dial-up connection to the Internet MALWARE can be used to bill 900 numbers to your phone bill. The 900 numbers are often billed at extremely high rates. MALWARE can place icons on your desktop that you never asked for and even change your existing icons. MALWARE can change your home page from the one you set to one it wants you to visit, which most likely will be a site that will further infect you with more SPYWARE and MALWARE. MALWARE can set up programs that go out onto the Internet and invite more instances of MALWARE, SPYWARE, and even viruses to infect a PC. In very extreme cases MALWARE can cause so much damage that you will have to buy a new computer altogether. MALWARE is the form of SPYWARE that you should be most concerned about since it is the most harmful.

How can SPYWARE and MALWARE infect you computer?

You can be infected if you download music, games, screensavers, video clips, and pictures from the Internet. A good majority of these downloadable files contain SPYWARE and MALWARE. Clicking on random pop-up ads can also infect your computer. In general while you surf the Internet you are bombarded by many instances of SPYWARE and MALWARE trying to infect your PC.

The following are some of the warning signs that your PC might be infected:

- When you open your browser the home page has mysteriously changed. You can manually change it back to your desired page and before long you find that it has been hijacked once again to some other page.
- You constantly get pop-up advertisements when your browser is not running or when your system is not even connected to the Internet, or the pop-ups address you by name.

- Your phone bill lists expensive calls to 900 numbers that you know you never made, most likely at an outrageous price per minute.
- New items appear in your Favorites list without you even book marking them. You may delete them but they will reappear.
- You attempt a search in Internet Explorer's address bar and when you press Enter to complete the search some unusual site handles your search instead of your usual search site.
- Your PC runs considerably slower than it did previously.
- You launch the "Task Manager" and under the "Process Tab" you see an unfamiliar process is using nearly 100% of your available CPU cycles.
- When you're doing anything online, the send or receive lights on your modem blink wildly as if you were downloading a file or surfing the Internet. Or the network/modem icon in your system tray flashes rapidly even though you're not using your connection.
- A search toolbar or other browser toolbar appears even though you didn't request or install it. Your attempts to remove it fail, or it comes back after removal.

So what can you do about infections?

Well to start off if you have an infection you need to run "msconfig" and check the processes running under the "Startup Tab." If there are any suspicious processes running they should be unchecked so that they are no longer running. Some of the SPYWARE/MALWARE can not be removed until they have been stopped from running. Next you should check to see what is running under the "Services Tab." Start by checking the box that says "Hide All Microsoft Services." Once all these services are hidden make sure that all the rest of the services are legitimate, and if they are not then they should once again be unchecked. If you're unsure about a process's legitimacy can be researched on the Internet by doing a "Google" search on the process. Keep in mind though that some processes are very important to the operation of the machine. You don't want to accidentally disable a process that is needed for proper operation. So you have to make sure you know what you're doing. Then click the "OK" button and reboot the PC.

Once rebooted run "regedit" and check the registry keys under:

HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run,
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/RunOnce

Some times SPYWARE/MALWARE will install registry keys. You must keep in mind that registry keys are absolutely critical to the proper operation of you PC. I stress that if you going to edit your registry you must absolutely know what you are doing, if you delete the wrong key you may lose the operation of a program or the whole PC itself. At the very least you will have to reinstall the program or in an extreme case you may have to reformat your hard drive and do a complete reinstallation of your operating system and your programs. However, if you are comfortable editing the registry you need to delete any keys that have been installed by the infection. Once again the keys can be researched by doing a "Google" search on them.

After you have completed these two tasks the next recommendation is to run SPYWARE removal programs. Two of the best are Ad-Aware SE and Spybot Search and Destroy. There are two versions of Ad-Aware SE a personal addition that can be downloaded for free at http://www.lavasoft.com/ and a professional version that can be purchased for somewhere around $40.00 dollars. Spybot Search and Destroy is freeware and can be downloaded at http://www.majorgeeks.com/download2471.html.

Ad-Aware should be installed, updated, and ran first. Once a scan is ran by the program you get a list of the SPYWARE/MALWARE infections and the opportunity to remove them. Occasionally the program will ask if it can run a scan on boot-up, you should allow it to do so and restart your machine. Some infections can only be removed if they are not running in the background. Keep in mind that you should always check for updated definitions before you use the program to scan your computer.

The difference between Ad-Aware SE personal and Ad-Aware SE professional is that the professional version comes with a tool called Ad-Watch. Ad-Watch can be configured to run on start-up and in the background. Ad-Watch is a preventative tool that stops the infections before they happen. Mind you not all these programs are perfect; it is a constant race between the people that create the SPYWARE and the people that write the software packages to remove them. A never ending battle if you will.

Spybot Search and Destroy should be installed, updated, and ran after Ad-Aware. Once again this program will pull of a list of the infections on your machine and allow you to remove them. This program as well sometimes will ask if it may run a scan on start-up. If it asks you to let it do that you should allow it and restart your machine. Again you should always check for definition updates before running a scan.

Chances are you should be able to remove all infections if you follow the above recommendations. If these recommendations don't remove all of your infections then you can count on having to reformat your hard drive and doing a complete reinstallation of the operating system and all your programs.

Other forms of prevention!

You can help prevent infection from SPYWARE and MALWARE as well as block most pop-ups by installing either the MSN toolbar or the Yahoo toolbar for your web browser. The MSN toolbar can be downloaded by going to http://toolbar.msn.com/. The Yahoo toolbar can be downloaded by going to http://toolbar.yahoo.com/. Both the MSN toolbar and the Yahoo toolbar install into Internet Explorer.

I would not recommend the installation of the EarthLink toolbar because this toolbar automatically updates itself and will block trusted sites like the Microsoft Windows Update site.

You can also use prevent some infections by using a browser other than Internet Explore. The recommended browser to use is Mozilla Firefox. The browser works in pretty much the same manor as Internet Explore but it has built in SPYWARE/MALWARE blockers. If you choose to

use this browser all of your book marked pages can be imported into the browser from Internet Explore. Firefox can be downloaded at http://www.mozilla.org/. If you are interested in more protection other than just using the Mozilla Firefox browser you can install a version of the Yahoo toolbar designed for the Firefox browser; however, this is a new release. The toolbar has some bugs and is not full implemented.

One last tip, when you get those pop-ups while surfing the web you should always close them using the "red X" in the corner of the window. However, before you hit the "X" you should put your mouse cursor over the "X" and make sure that the word "Close" comes up. Sometimes the "red X" is actually a website address to a site where you will get SPYWARE, MALWARE, and viruses. If you click any of the buttons on the pop-up you will run the risk of an infection. If the "red X" is a website address then you can use "ALT" and "F4" together to close the window.

Brian Colston
Solutions Engineer
www.needteksupport.com
help@needteksupport.com