Spyware and Viruses

Spyware and viruses are getting to be the largest problem in the battle of keeping your computer running smoothly and being able to use your computer with any kind of efficiency.

There is a distinct difference between spyware and viruses.

Viruses can and do cause damage to your computer, your files, and the software programs you use. Viruses attack your computer at the base level of programming. As some of you know, computers use a "binary" language as where we as humans, use a base 10 language. Computers do tasks and perform calculations based on the binary or base 2 programming. This basically means that a computer uses ones and zeros as a communication tool to do it's job. When a virus infects the code inside of your computer it changes the "meaning" of certain commands that cause your computer to "freeze" or "lock up" or just cause errors. An example of this would be something like this:

11100100011101001 may mean something like.. launch Microsoft word... as to where...
11 00 00011 010 1 may mean, let's go to McDonalds for lunch!

Its a matter of how and where the ones and zeros are placed. Viruses "eat" or destroy bits of data like the missing ones and zeros that you see above that cause malfunctions or miscommunications with your computer.

A lot of times, the only way to fix this kind of damage is to first get rid of the virus and then reinstall the affected software.

Spyware and Malware on the other hand is just purely annoying and generally slows your computer down to a crawl if it is even usable. Spyware usually doesn't harm your computer when it's infected it just makes it impossible to work with.

The purpose of spyware is to trick you into buying a product to fix a problem with your computer that you really don't have! Sound confusing? This is why it's called SPY-ware or sometimes it's also known as malware.

Usually spyware is brought into your computer by "pop-ups" that show up when you are browsing the internet with internet explorer. They will usually appear to be a message from your computer telling you that there is a problem with your computers performance or your system has detected a virus then it prompts you to click on a button to fix the problem. This NEVER fixes the problem, it only makes it worse.

Here’s how to deal with them:

Even with new browsers and security technology aimed at reducing or eliminating annoying pop-up ads, it seems that a few still manage to slip by on occasion. Many users simply close the pop-up box and continue with what they were doing. But, "closing" the pop-up box may just be an invitation to download some sort of virus or other malware onto your system.

Pop-up ads often appear to be standard message boxes which users of Microsoft Windows operating systems are used to seeing. They typically contain a short message or alert of some sort and have a button or buttons at the bottom. Perhaps it asks if you would like to scan your system for spyware, and includes "Yes" and "No" buttons for you to enter your selection. Or, maybe it is just an alert of some sort with a button at the bottom to "Close" the window.

Don't Trust Pop-Ups

At first glance, it seems innocent enough. The pop-up ad is slightly annoying, but at least whoever made it and sent it to your computer was nice enough to give you a simple way to get rid of it, right? Well, sometimes that is true, but not always. Obviously, if the creator of the pop-up ad truly had high moral and ethical standards, you wouldn't be getting the pop-up ad in the first place.

In many cases, the box or button that seems to be the obvious choice for quickly getting rid of the pop-up is actually a link to download some sort of virus, spyware or other malware onto your system. By clicking "No" or "Close" you may actually be inadvertently downloading malware onto your computer.

Safely Closing Pop-Up Ads

To avoid accidentally infecting your computer, some security experts recommend that you click on the "X" in the upper right hand corner of the pop-up window rather than using the buttons within the pop-up. However, some of the more malicious pop-ups may even have disguised a malware download to mimic that "X", and again you might actually be initiating a download rather than closing the pop-up ad.

To really play it safe, you should right-click the pop-up ad in your taskbar and select "Close" from the menu. If you have a pop-up ad which is not listed on your taskbar, you may need to dive into the Task Manager to shut down the application or process behind the pop-up ad. To access Task Manager, you can right-click on the taskbar at the bottom of the screen and select Task Manager from the menu.

These programs are designed to do only one thing, sell you products you don't need. You'll notice that if you click on one of those warnings, it brings you to a web page that wants to sell you some program that will supposedly fix your problem (the problem that was created by them) and they want your money!

Again, the only way to fix this problem is to remove the spyware with honest spyware removal tools and be educated as what not to do on the internet.

We at I.C.U. Computer Repair specialize in virus and spyware removal and cleaning up the mess left behind by them. We strive not only to fix your computer problems but to further educate our customers to help them to avoid these kind of problems in the future.

Malware, What is it?

Along with viruses, one of the biggest threats to computer users on the Internet today is malware. It can hijack your browser, redirect your search attempts, serve up nasty pop-up ads, track what web sites you visit, and generally screw things up. Malware programs are usually poorly-programmed and can cause your computer to become unbearably slow and unstable in addition to all the other havoc they wreak.

Many of them will reinstall themselves even after you think you have removed them, or hide themselves deep within Windows, making them very difficult to clean. This article will detail the different varieties of malware along with basic preventive measures.

You can get infected by malware in several ways. Malware often comes bundled with other programs (Kazaa, iMesh, and other file sharing programs seem to be the biggest bundlers). These malware programs usually pop-up ads, sending revenue from the ads to the program's authors. Others are installed from websites, pretending to be software needed to view the website. Still others, most notably some of the CoolWebSearch variants, install themselves through holes in Internet Explorer like a virus would, requiring you to do nothing but visit the wrong web page to get infected.

The vast majority, however, must be installed by the user. Unfortunately, getting infected with malware is usually much easier than getting rid of it, and once you get malware on your computer it tends to multiply.

Types of Malware

Although there is no official breakdown, we can divide malware into several broad categories of malware: adware, spyware, hijackers, toolbars, and dialers. Many, if not most malware programs will fit into more than one category.

It is very common for people to use the words adware, spyware, and malware interchangeably. Most products that call themselves spyware or adware removers will actually remove all types of malware.

Adware

Adware is the class of programs that place advertisements on your screen. These may be in the form of pop-ups, pop-unders, advertisements embedded in programs, advertisements placed on top of ads in web sites, or any other way the authors can think of showing you an ad. The pop-ups generally will not be stopped by pop-up stoppers, and often are not dependent on your having Internet Explorer open. They may show up when you are playing a game, writing a document, listening to music, or anything else. Should you be surfing, the advertisements will often be related to the web page you are viewing.

Spyware

Programs classified as spyware send information about you and your computer to somebody else. Some spyware simply relays the addresses of sites you visit or terms you search for to a server somewhere. Others may send back information you type into forms in Internet Explorer or the names of files you download. Still others search your hard drive and report back what programs you have installed, contents of your e-mail client's address book (usually to be sold to spammers), or any other information about or on your computer – things such as your name, browser history, login names and passwords, credit card numbers, and your phone number and address.

Spyware often works in conjunction with toolbars. It may also use a program that is always running in the background to collect data, or it may integrate itself into Internet Explorer, allowing it to run undetected whenever Internet Explorer is open.

Hijackers

Hijackers take control of various parts of your web browser, including your home page, search pages, and search bar. They may also redirect you to certain sites should you mistype an address or prevent you from going to a website they would rather you not, such as sites that combat malware. Some will even redirect you to their own search engine when you attempt a search. NB: hijackers almost exclusively target Internet Explorer.

Toolbars

Toolbars plug into Internet Explorer and provide additional functionality such as search forms or pop-up blockers. The Google and Yahoo! toolbars are probably the most common legitimate examples, and malware toolbars often attempt to emulate their functionality and look. Malware toolbars almost always include characteristics of the other malware categories, which is usually what gets it classified as malware. Any toolbar that is installed through underhanded means falls into the category of malware.

Dialers

Dialers are programs that set up your modem connection to connect to a 1-900 number. This provides the number's owner with revenue while leaving you with a large phone bill. There are some legitimate uses for dialers, such as for people who do not have access to credit cards. Most dialers, however, are installed quietly and attempt to do their dirty work without being detected.

Again, when in doubt, stop using your computer and seek the advice of a professional or use the proper software tools to take care of the problem.
At ICU we are here for you. Call us if you have any questions or any further needs with your computer.