

A Quick Tutorial on Spyware
Justin Bishop
Computer Experts, Inc.
April 15, 2004

Maybe it came from the cool new *free* fish tank screensaver you just downloaded, or the cute little golf cart icon that now takes the place of your mouse pointer. Maybe it started when all you wanted to do was make somebody's day a little brighter by giving them a smiley face icon you downloaded that now you put in your all of your e-mails. But all you know is that now you're getting a lot of ad pop-ups whenever you surf the web. Maybe you're getting them even when you're *not* surfing the web...you're just trying to type up a document for tomorrow's meeting. No matter what, you just can't stop them.

Congratulations, you're now infected with *Spyware* and it's only going to get worse unless you take action now. Hopefully after reading this article, you will be armed with the knowledge and tools to prevent such hideous crimes or to disinfect your PC right now.

But first, what is Spyware or Adware. In a nutshell, many revenue driven websites need a new source of income because they are not making enough money with you simply looking at their site and then leaving. So in return, some websites will place a wonderful little program on your PC (some with your "permission" and some without you even knowing) that just sits back and watches your web activity. Then, that program will send information back to a particular company who will sell your information to a "marketing" firm(s) who, in return, sends you ad pop-ups, hoping that you will be gullible enough to click on their ad to get more information. Visit enough websites like these, and you've got enough pop-ups to keep you busy all day long.

Before we talk about prevention, let's talk about symptoms. The obvious of course is the ever-elusive ad pop-up. But there are many other symptoms. If you look closely in your web browser, you may have a new search toolbar labeled "My Search Bar" or "Hotbar". If you're really lucky you'll have a great big search bar at the bottom of your screen that helps you find the best porno and gambling sites that money can buy. When you start your PC, you may get a program that wants to "help" you rid your PC of porn called "PowerScan" or "PurityScan". Basically, if you see new toolbars in your web browser or new programs on your desktop or in your "Start" bar, and you know you haven't downloaded or installed any new programs, then you probably have Spyware.

Now let's talk about prevention...or can we. Many of these programs are downloaded onto your PC without you even knowing. Some are malicious enough to install on your PC even after you tell them no. However, more than likely you have agreed to their "Acceptance Terms" without reading the fine print. Many sites may give you a pop-up that says "To view this page properly, you will need to install...". And because you just have to see what's on that page, you say yes. Still, some websites will give you a pop-up that says "Accept" or "No Thanks" and then as soon as you click "No Thanks" or you simply click the "X" at the top of the window to make it disappear the program gets installed to your PC anyway.

The best prevention is to simply stop surfing the web. Now, since that's not going to happen, let's try a few simple things:

1. Install the Google toolbar, which has a built-in pop-up blocker (or other similar products). This will stop the pop-ups that are generated from the website itself which will help deter you from having to answer any questions that you may be unfamiliar with. However, it will not stop Spyware pop-ups once your PC is infested.
2. Avoid websites that offer nothing more than free products for you to download and share with others.
3. Install a software based Firewall program such as ZoneAlarm, which will warn you when your PC is being attacked from the "outside". It also acts as a Spyware catcher once your PC is infected because it will catch any program trying to access the internet.

Now let's talk about removal. The first thing to do is to go to *Start, Control Panel*, then click on *Add/Remove Programs*. Then proceed to remove any programs that you are CONFIDENT that you have not installed. NEVER manually remove any of these programs by simply deleting its folder from your hard drive. More often than none, we have found that by doing so, you will find yourself unable to browse the internet because these programs attach themselves to Internet Explorers settings.

Also, there are two great programs on the market today that will remove most, if not all of the Spyware from your PC. Our company uses both because we find that what one program doesn't find, the other will. The first one is called *Spybot – Seek and Destroy*. This is a "free" program that can be downloaded from www.safer-networking.org. Once installed, make sure you check for webupdates and install if necessary. Many Spyware programs are running concurrently with Spybot and cannot be removed until you reboot your PC and let Spybot run again before any other programs can be loaded. If this is the case, Spybot will prompt you to do so. The second one is a retail product called Ad-Aware that can be purchased at most software stores and online. Again, always run the "Check for updates" tool to find new updates from the web before scanning your PC.

Spyware is absolutely an epidemic. It's just as bad as viruses and there is no way to regulate or halt the use of these programs. The best prevention is common sense. If it sounds too good to be true...it probably is. If it seems too easy to just say yes...DON'T.