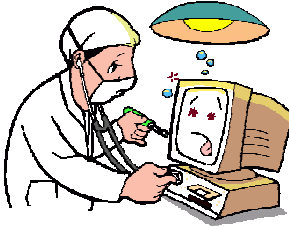


Spyware Information (Portions Courtesy of GetNetWise.org)

Robert Osorio - IT Consultant, (352) 750-0845, Email: IhateSpyware@RobertOsorio.com



Symptoms of spyware

Below are just a few symptoms that may reveal that you have spyware operating on your computer.

- **Sluggish computer**
- **Strange icons on your desktop**
- **Fishy pop-up ads:** Pop-up ads from spyware software are designed to look like they've been served up by the legitimate Web site you're visiting. As a result, you may not recognize them as a symptom of infection. There's no way to be sure, but if the contents of the ads seem strange -- or if you're getting pop-up ads when you're not even surfing the Internet -- it's very likely that they are being served up by spyware software installed on your computer.
- **Change of your default home page:** One of the oldest spyware tricks is to automatically change your Web browser's default or start-up home page. This is the Web page that appears when you start your browser or click the "home" button.
- **Scary security warnings:** A popup window designed to look similar to your security software with frightening warnings about someone trying to attack your computer or spying on you and offering a free security scan.



Examples of Devious Spyware

How does spyware get on my computer in the first place?

- **Fool me once:** A computer user sees an Internet advertisement for SomeProgram. She clicks on the ad and is sent to a page that pops up a window asking if she wants to download SomeProgram. The user clicks "no," but SomeProgram is surreptitiously downloaded and installed anyway because the "no" button is actually a "yes" button.
- **I'm not touching you:** In this case, a computer user sees an ad for AnotherProgram, and clicks on it. She is sent to a page that immediately pops up a window asking if she wants to download AnotherProgram. The user clicks "no." An identical window pops up as soon as she declines, however, and repeats until the user gets frustrated and clicks "yes".
- **Homepage hijack:** In this common case, a computer user goes to a Web page, www.acompany.com. The page has a malicious script on it. Any time the user attempts to reset his home page, the script changes it back.
- **Bait and Switch:** Here, a computer user downloads a software package for a free screensaver (as an example). Among with the program it also installs a toolbar called GreatBargains. The toolbar may flash annoying advertisements at you and make your web browser unstable (these programs are often poorly written). If you uninstall the screensaver, the toolbar remains and there is no uninstaller for the toolbar.
- **No such thing as a free lunch:** In this case a computer user installs a peer-to-peer (P2P) file sharing program that will allow her to download free music from the Internet. What she doesn't realize is that the program also shares all her private files on the internet. If she installed this on her work computer this could be a serious security breach for her employer.

Why can't I get rid of the spyware once I've found it?

- **No way out:** In this example, a computer user has downloaded "New Game: Return to Hades" from the Internet, but now wants to remove the game program from the computer because he fears it might be spyware. "New Game" does not have an uninstall program or instructions, and does not show up in the "Add and Remove Programs" section of the Windows Control Panel.
- **It will not die:** Here, a computer user has downloaded Program 2.0. He thought it would be a helpful program, but it has turned out to be spyware. Now he wants to remove Program 2.0 from the computer. Program 2.0 appears in "Add and Remove Programs" section of the Windows Control Panel, but when he utilizes the "remove" option, it doesn't work.
- **Extortion racket:** In this example a computer user visits a website with malicious code on it that causes a popup to appear, designed to look similar to a real security warning. Assuming it's a valid warning, she clicks "yes" for the offer of a free security scan which reports all kinds of horrible things are installed on the computer that can only be removed by the "Pro" version which costs \$50. The fake security warning keeps nagging her to pay \$50 for the full version. There is no way to uninstall this program and she finds the computer is unusable unless she pays. Feeling she has no choice she clicks okay and gives them her credit card. The "Pro" version does nothing, and the people behind this scam have double charged her credit card and then sold her credit card number on the black market.



Spyware Prevention

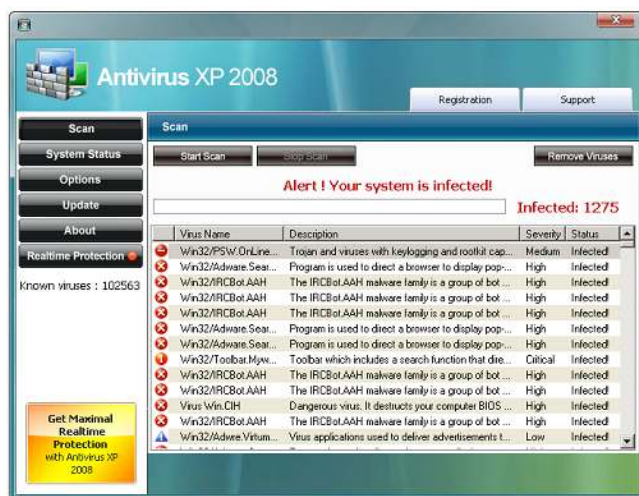
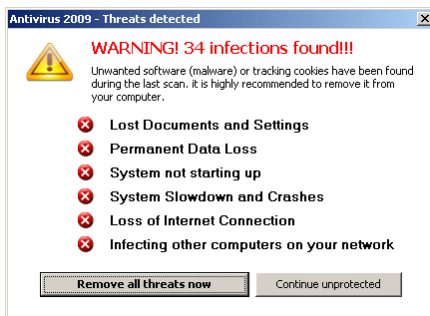
Prevention is the key to protecting yourself from spyware. While these tips will help you prevent spyware, they are also examples of good habits that will help protect your privacy and security while online.

Keep in mind that most spyware **MUST** be installed by **YOU**. You must give explicit permission. Thus the people behind these scams use social engineering to try to trick you into installing their malicious software. They may tantalize you with photos of celebrities, prey on your desire to give to charities, lure you with offers of free programs, or scare you with bogus security threats.

- **Read any popup window VERY carefully, and close it properly if it looks suspicious.** If a suspicious window or advertisement pops up on your screen that you suspect could be an attempt to fool you into installing a spyware program, click the “X” in the upper right corner of the window to close it instead of clicking on the “No” or “Decline” button (often these buttons will only open another window in an attempt to annoy you into accepting the product, or the “Decline” button may actually be the “Accept” button in disguise). If you still can’t close the window, or others pop up to replace it, then shut down the computer and restart it.
- **Be skeptical about installing strange or “free” software:** Make sure you know **EXACTLY** what is being installed onto your computer when you download applications off the Internet. Spyware is often bundled with many free software downloads. Make sure you know what’s in a package of software before you install it. Many of the file sharing or peer-to-peer music sharing programs include spyware in the installation package. Before installing a program, do a search on Google for the name of the program and the word “spyware” (eg: “Daisies Screensaver Spyware?”). If there’s something nasty in it, people will be reporting on it somewhere.
- **Pay attention to security warnings:** Windows security warning screens alert users to new software being installed from Web pages they visit in Internet Explorer. You should not blindly accept such software installations. Be sure you trust the company installing the software. Make sure you are dealing with a reputable company and that you are actually on their website and not a fake website with a misspelled address (jcpenny.com instead of jcpenny.com for instance).

- Beware of fake security messages.** Just because a security warning appears on your screen, it does not mean it's a legitimate message from your anti-virus program or Windows. It could just as easily be a fake pop-up made to look like a legitimate security warning. Be especially skeptical of messages designed to frightening you into immediate action (eg: "Someone is spying on you!" or "Your system is seriously compromised!" or "Someone is trying to access your credit card information!") and then asks you to "Click her for a free security scan". Your real anti-virus program will **never** try to scare you like this. Read the message **CAREFULLY**. Make sure the message is actually from your anti-virus program (for instance your real anti-virus may be called "Norton 360" but a fake security popup may identify itself as "Security 360" with a similar log to try and fool you). If it's not the same name as your anti-virus, then it's probably a fake. If in doubt click the "X" in the upper right corner. **NEVER** click on "No" or "Cancel".

Examples of fake security messages:





Dangerous Attachments

Do not open attachments or click on links in emails. There really are NO safe attachments you can open in an email. Let me repeat that:

THERE IS NO SUCH THING AS A SAFE EMAIL ATTACHMENT!

For example, Power Point slide shows are commonly used to carry malicious software. While you're watching the pretty slide show, a script may be running that installs spyware. These slide shows will be innocently emailed to you by friends and family who have no idea they are helping criminals infect other computers.

Another example: Fake emails from retailers may contain a PDF file attachment that the email asks you to open to see your invoice and the PDF contains a script that infects your PC.

DO NOT OPEN ATTACHMENTS! PERIOD! Unless you are expecting one. For example if your accountant calls and says he's emailing you a PDF of a document, then when that email arrives addressed from him in the next few minutes, you can be fairly sure it's really from your accountant.

SOCIAL NETWORKS:

The above rule on attachments and links also applies to social networks like Facebook and Twitter. Never open links or attachments sent to you by friends on social networks. It's very common for criminals to hack into Facebook accounts and then send spyware to all of that person's friends in the hopes of infecting them. This is particularly used in targeted attacks on employees of companies.

While we're talking about Facebook, think twice about posting anything that can be used against you by criminals. Assume EVERYTHING you post on Facebook is public. All it takes is one friend's account being compromised and the world will know everything about you.

I would recommend not filling out social network questionnaires. The questionnaire is made public so people can find you via common interests, but it also exposes you to great risk. Common questions include the name of your high school, date of birth, and where you were born. **THESE ARE ALL COMMONLY USED AS SECURITY QUESTIONS BY YOUR BANK** or other institutions in order to reset your password if you should forget it. Knowing these things, and your email address, is all a criminal needs to access your bank account or steal your identity.

Practice basic computer security hygiene:

- **Always use anti-virus software:** And keep the software up to date. Over 500 new viruses are discovered each month. You are not just protecting yourself when using anti virus software, but also others you communicate with.
- **Always use a firewall:** A firewall is an "internal lock" for information on your computer. Windows XP, Vista and Windows 7 already have firewalls installed and these are adequate, you just have to make sure they're turned on.
- **Keep your Windows operating system up to date:** You should always make sure that the Windows operating system on your computer is up to date with the latest security patches from Microsoft. Make sure Windows Automatic Updates is enabled.
- **Keep Java and Adobe Reader updated.** These are necessary programs used by your computer to browse the web. They are updated monthly to fix security flaws. When they require updates, allow them.
- **Beware of "free" programs:** While not all free programs are malicious, many are, and many "free" programs are not actually free. The price is sometimes allowing some advertising spyware to be installed on your computer that nags you with advertisements, or tracks your browsing habits on the Internet, or (as in the case of rogue security software) extorts you for money.
- **Beware of additional payloads:** When installing legitimate programs and updates, there will often be a free toolbar included (for instance Java updates try to install a toolbar). The toolbar may not be malicious (Google, Yahoo, MSN toolbars for instance) but it might be annoying or may slow down your computer and is certainly not required. Legitimate software will usually give you the option to "opt out" of installing the toolbar by un-checking a box during the install process, so read each screen carefully.
- **Do not overly rely on your anti-virus program:** Anti-virus programs are not perfect. New threats are being discovered all the time and there is often a delay between the time a new threat is discovered, and your anti-virus program is updated to recognize it. Also many spyware programs exist in a legal "gray area" and your anti-virus may not be able to legally block it if you gave your approval to install it. **Safe browsing habits are your first line of defense!** Your anti-virus program should only be a last line of defense.
- **Use Firefox instead of Internet Explorer:** Firefox is a free web browser available from Firefox.com. It works just like Internet Explorer but is MUCH safer. It does not replace Internet Explorer, and you can run either one if you have both installed. Be sure to keep Firefox up to date whenever it notifies you that a new update is available.

Why Do People Write Spyware And Viruses?



MONEY. Pure and simple. This is not for fun anymore, it's for profit. Malicious software is a multi-BILLION dollar industry, run by organized crime.

How does it work? Well let's assume someone can make just ONE DOLLAR by infecting a single computer with a virus or spyware. Then assume he can infect 10,000 computers a month. That's \$10,000 a month!

What's worth so much on your computer? Sure passwords, social security and credit card numbers, are used for identity theft, but this is small change in the criminal world. Sorry to say, but your credit card number is only worth a couple of dollars on the black market.

Selling you something you may THINK you need, which you don't really need is also profitable: fake security software, fake registry cleaners, programs that claim to "speed up" your computer.

Even more valuable is INFORMATION. Personal information about your browsing habits is extremely valuable to marketers both legitimate and shady.

Your computer is also valuable all by itself. Trojan horse (trojan) programs are designed to take over your computer without giving themselves away. Usually the only way you can tell if there is a professional trojan on your computer at all is if it's running slow or using a lot of your internet traffic. While you are typing a letter or browsing the Internet, the trojan may be using your computer (along with hundreds of thousands of other infected PCs) to send SPAM, attack corporate or government websites, or store illegal files like child pornography.

Targeted attacks are becoming more common as well. They may not be interested in YOU specifically, but they may want to take over your computer to see if it contains information about the company you work for, people you know, or just to fake your identity to take advantage of someone else.