

SECTION 13

SPYWARE

13. SPYWARE

13.1 WHAT IS SPYWARE?

Spyware refers to the software that performs tasks on your computer without your consent, for example: Advertising, Collecting personal information, or Changing the configuration of your computer.

13.2 SIGNS OF SPYWARE

If your computer starts to behave strangely or displays any of the symptoms listed below, you may have spyware or other unwanted software installed on your computer.

I see pop-up advertisements all the time

Some unwanted software will bombard you with pop-up ads that aren't related to a particular website you're visiting. These ads are often for adult or other websites you may find objectionable. If you see pop-up ads as soon as you turn on your computer or when you're not even browsing the web, you may have spyware or other unwanted software on your computer.

My settings have changed and I can't change them back to the way they were

Some unwanted software has the ability to change your home page or search page settings. This means that the page that opens first when you start your Internet browser or the page that appears when you select "search" may be pages that you do not recognise. Even if you know how to adjust these settings, you may find that they revert back every time you restart your computer.

My web browser contains additional components that I don't remember downloading

Spyware and other unwanted software can add additional toolbars to your web browser that you don't want or need. Even if you know how to remove these toolbars, they may return each time you restart your computer.

My computer seems sluggish

Spyware and other unwanted software are not necessarily designed to be efficient. The resources these programs use to track your activities and deliver advertisements can slow down your computer and errors in the software can make your computer crash.

If you notice a sudden increase in the number of times a certain program crashes, or if your computer is slower than normal at performing routine tasks, you may have spyware or other unwanted software on your machine.

13.3 WHAT IS THE DIFFERENCE BETWEEN SPYWARE AND ADWARE?

Spyware is often associated with software that displays advertisements (called adware) or software that tracks personal or sensitive information. This type of software is not necessarily bad. For example, you might sign up for a free service, but "pay" for the service by agreeing to receive targeted ads. If you understand the terms and agree to them, you may have decided that it is a fair trade-off. You might also agree to let the company track your online activities to determine which ads to show you.

Spyware includes other types of unwanted software. This software will make changes to your computer that can be both annoying, and can cause your computer to slow down or crash. These programs may change your Web browser's home page or search page, or add additional components to your browser that you did not request. They may also make it very difficult for you to revert back to your computer's original settings.

13.4 HOW TO PREVENT SPAM?

STEP 1: USE A FIREWALL

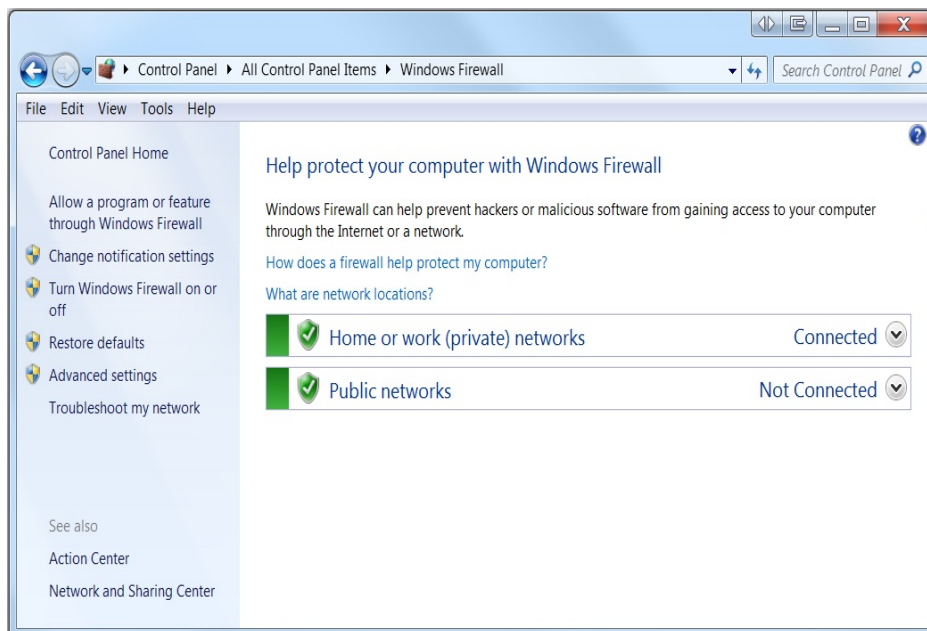
While most spyware and other unwanted software come bundled with other programs or originate from unscrupulous Web sites, a small amount of spyware can actually be placed on your computer remotely by hackers. Installing a firewall or using the firewall that's built into Windows XP/7/VISTA provides a helpful defence against these hackers.

To enable Windows Firewall in Windows XP, follow these steps:

Click Start, click Settings, click Control Panel.
Click Windows Firewall.
On the General tab, click On (recommended).
Click OK.

To enable Windows Firewall in Windows 7, follow these steps:

Click **Start**, click **Settings**, click **Control Panel**. (all items view)
Click on the **Windows Firewall** icon.
Click on the Turn **Windows Firewall** on or off link in the left blue pane. (See screenshot below)



STEP 2: UPDATE YOUR SOFTWARE

If you use Windows XP/7/VISTA, one way to help prevent spyware and other unwanted software is to make sure all your software is updated. Visit Microsoft Update at <http://www.update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en-us> to confirm that you have Automatic Updates turned on and that you have downloaded all the latest critical and security updates.

STEP 3: ADJUST INTERNET EXPLORER SECURITY SETTINGS

You can adjust your Internet Explorer Web browser's security settings to determine how much—or how little—information you are willing to accept from a Web site. Microsoft recommends that you set the security settings for the **Internet zone** to **Medium** or higher.

To view/adjust your current Internet Explorer security settings:
In Internet Explorer, click **Tools** and then click **Internet Options**
Select the **Security** tab.
Click Medium-high.

STEP 4: DOWNLOAD AND INSTALL ANTISPYWARE PROTECTION

Windows Defender protects your computer from spyware and other unwanted software, it can quickly and easily find spyware and other unwanted programs that can slow down your computer, display annoying pop-up ads, change Internet settings, or use your private information without your consent. It eliminates any detected spyware easily and allows you to schedule your scanning and removal times when it's convenient for you, whether it's on-demand or on a schedule that you set.

Windows Defender comes with Windows and you can download it for no charge for Windows XP SP2/7/Vista at: <http://www.microsoft.com/windows/products/winfamily/defender/default.mspx>

1. Keep your operating system software updated with the latest critical and security updates. For Microsoft Windows, go to <http://update.microsoft.com> to obtain updates.

STEP 5: SURF AND DOWNLOAD MORE SAFELY

The best defence against spyware and other unwanted software is not to download it in the first place. Here are a few helpful tips that can protect you from downloading software you don't want:

- Only download programs from Web sites you trust. If you're not sure whether to trust a program you are considering downloading, ask a knowledgeable friend or enter the name of the program into your favourite search engine to see if anyone else has reported that it contains spyware.
- Read all security warnings, license agreements, and privacy statements associated with any software you download.
- Never click "Agree" or "OK" to close a window. Instead, click the red "X" in the corner of the window or press the **Alt + F4** buttons on your keyboard to close a window.
- Beware of popular "free" music and movie file-sharing programs, and be sure you clearly understand all of the software packaged with those programs.

13.5 HOW TO REMOVE SPYWARE

Many kinds of unwanted software, including spyware, are designed to be difficult to remove. If you attempt to uninstall or delete this software, you might find that the program reappears as soon as you restart your computer. If you are experiencing difficulty with uninstalling the unwanted software, you may need to download a tool to do the job for you.

Several companies offer free and low-cost software that will scan your computer for spyware and other unwanted software and help you remove it.

To remove spyware:

1. Download and install a spyware removal tool. They can be easily found by using an Internet search engine. For example you may install Microsoft Windows AntiSpyware.
2. Run the tool to scan your computer for spyware.
3. Review the files discovered by the tool for spyware.
4. Select suspicious files for removal by following the tool's instructions.

13.6 FURTHER INFORMATION

Search the Internet for more information on spyware and adware.