

What's the difference between spyware and a virus? What is Scareware?



Spyware and viruses are both forms of unwanted or malicious software, sometimes called "malware." You can use Microsoft Security Essentials to protect yourself from both. Other programs work well also. You must use protection if you are connected to the Internet!

What's the difference between these items?

Spyware (sometimes called adware) collects information about you without appropriate notice and consent.

A computer virus spreads software, usually malicious in nature, from computer to computer. It may also and often does disable your computer.

Spyware can get installed on your computer in a number of ways. One way is through a virus. Another way is for it to be secretly downloaded and installed with other software you've chosen to install.

In short, spyware is a specific type of unwanted software that secretly collects your information.

Spyware is a general term used to describe software that performs certain behaviors, generally without appropriately obtaining your consent first, such as:

- **Advertising**
- **Collecting personal information**
- **Changing the configuration of your computer**
- **Spyware is often associated with software that displays advertisements (called adware) or software that tracks personal or sensitive information.**

What spyware does

Other kinds of spyware make changes to your computer that can be annoying and can cause your computer slow down or crash.

These programs can change your Web browser's home page or search page, or add additional components to your browser you don't need or want. They also make it very difficult for you to change your settings back to the way you had them.

Know what you're installing

The key in all cases is whether or not you (or someone who uses your computer) understand what the software will do and have agreed to install the software on your computer.

A common trick is to covertly install the software during the installation of other software you want such as a music or video file sharing program.

A virus is a specific way software can be secretly distributed, often by e-mail or instant messaging.

Both spyware and viruses can cause damage to your computer or cause you to lose important data, or share it unknowingly.

What is Scareware?

Scareware is a type of malware designed to trick victims into purchasing and downloading useless and potentially dangerous software.



Scareware, which generates pop-ups that resemble Windows system messages, usually purports to be antivirus or antispyware software, a firewall application or a registry cleaner.

The messages typically say that a large number of problems -- such as infected files -- have been found on the computer and the user is prompted to purchase software to fix the problems. In reality, no problems were detected and the suggested software purchase may

actually contain real malware. It is virtually impossible to scan a computer within an Internet browser.

If the user falls for the scam, they will lose the money they paid for the useless software and he may also make his computer unusable. Frequently, the message window has a clickjacking feature that takes the user to the attacker's Web site or initiates a malware download if the user clicks "Cancel" or the "X" to close the window.

Do I need both Microsoft Security Essentials and another antivirus software program?

The short answer? No.

The long answer? Microsoft Security Essentials is free software that helps protect against viruses, spyware, worms, and other malicious or unwanted software. Microsoft Security Essentials has already won awards and gotten great reviews from security experts.



If you use Microsoft Security Essentials you don't need to install any other antivirus or antispyware software. If you use other products you generally need both types of software. They may be built in as a complete package.

In fact, if you run more than one antivirus or antispyware program at once it might affect your computer's performance. If you already have antivirus software and you want to install Microsoft Security Essentials, You need to uninstall other types of software. Don't just disable them, uninstall them

Note: Windows 7 and Windows Vista both come with antispware software called Windows Defender. If you install Microsoft Security Essentials it will automatically disable (but not uninstall) Windows Defender. It does this so that you don't have two programs on your computer that are doing the same thing. Windows Defender is built into Windows Vista and Windows 7 and it's available as a free download for Windows XP. Windows Defender helps protect your computer from spyware and some other potentially unwanted software, but it will not protect against viruses.

In other words, Windows Defender only protects against a subset of known malicious software but Microsoft Security Essentials protects against ALL known malicious software.

If you want to install another antivirus program, uninstall Microsoft Security Essentials first.

Trading tracking for services

That does not mean all software that provides ads or tracks your online activities is bad. For example, you might sign up for a free music service, but you "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 tradeoff. You might also agree to let the company track your online activities to determine which ads to show you. Cookies are also a form to tracking, but are generally safe.

What's the latest threat?

A new type of cookie is being used, new generation of 'Super-Cookie', which silently conquered the internet. This new cookie generation offers unlimited user tracking to industry and market research. If you use Firefox browser there is an addon developed to make users aware of those hidden, never expiring objects and to offer an easy way to get rid of them - since browsers are unable to do that for you.

Flash-cookies (Local Shared Objects, LSO) are pieces of information placed on your computer by a Flash plugin. Those Super-Cookies are placed in central system folders and so protected from deletion. They are frequently used like standard browser cookies. Although their threat potential is much higher than conventional cookies, only a few users began to take notice of them. They are being used so frequently that -after a time- hundreds of those Flash-cookies reside in special folders. And they won't be deleted as they never expire.

The Last Words:

Whenever you install something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes the inclusion of unwanted software in a given software installation is documented, but it might appear at the end of a license agreement or privacy statement. If you have any doubt, do some research, suing Google. simply type in the name, such as Antivirus 2010.



Antivirus 2010 will not protect you from malware. In fact, it *is* malware. It's a *rogue* program, pretending to protect you from infections while infecting your computer.

If you get a pop-up warning you of danger and suggesting you install this wonderful program, don't click Yes and don't click No, either. Close the window. The safest way to do this is with a right-click on the toolbar, then select Close.