

HOW TO CHECK YOUR SECURITY STATUS ON YOUR PC

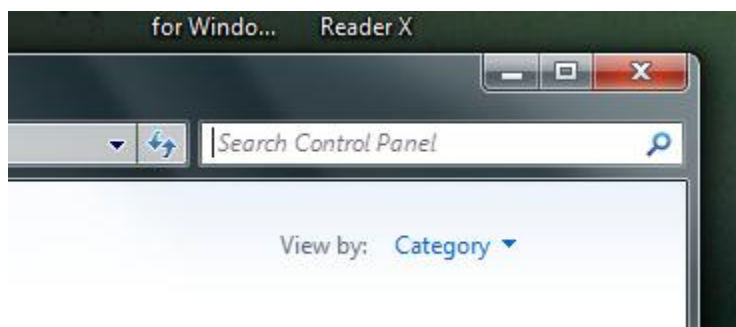
BY : MIKE



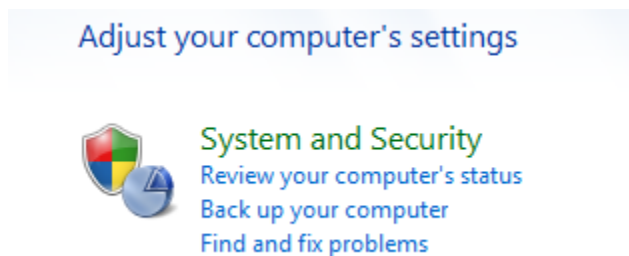
1. Click on the start menu located to the left and at the bottom of the desktop screen.



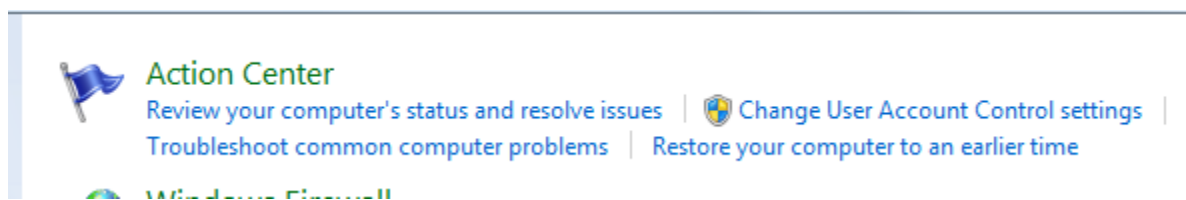
2. In the right side of the menu that pops up click on Control Panel.



3. In the next box that pops up you want to change the View by: to **Category**(if not already selected you can click on the down arrow located next to that choice), Located in the top right under the search control panel box.



4. Now in that same dialog box click on the **System and Security**.



5. In the top of the screen click on **Action Center**.

Security



6. Click on the down arrow to the right of the word security to verify all your security settings.

This screen will pop up:

Review recent messages and resolve problems

Action Center has detected one or more issues for you to review.

Security



Network firewall	On
Windows Firewall is actively protecting your computer.	
Windows Update	On
Windows will automatically install updates as they become available.	
Virus protection	On
AVG Anti-Virus Free Edition 2011 reports that it is up to date and virus scanning is on.	
Spyware and unwanted software protection	On
AVG Anti-Virus Free Edition 2011 reports that it is turned on. View installed antispyware programs	
Internet security settings	OK
All Internet security settings are set to their recommended levels.	
User Account Control	On
UAC will notify when programs try to make changes to the computer. Change settings	
Network Access Protection	Off
Network Access Protection Agent service is not running What is Network Access Protection?	

[How do I know what security settings are right for my computer?](#)

7. You can choose your settings or learn what the right ones are and why they are helpful.

Understanding security and safer computing

If you connect to the Internet, allow other people to use your computer, or share files with others, you should take steps to protect your computer from harm. Why? Because there are computer criminals (sometimes called hackers) who attack other people's computers. These people can attack directly, by breaking into your computer through the Internet and stealing your personal information, or indirectly, by creating malicious software to harm your computer.

Fortunately, you can help protect yourself by taking a few simple precautions. This article describes the threats and what you can do to defend against them.

Protect your computer

These are ways to help protect your computer against potential security threats:

- Firewall. A firewall can help protect your computer by preventing hackers or malicious software from gaining access to it.
- Virus protection. Antivirus software can help protect your computer against viruses, worms, and other security threats.
- Spyware and other malware protection. Antispyware software can help protect your computer from spyware and other potentially unwanted software.
- Windows Update. Windows can routinely check for updates for your computer and install them automatically.

[Top of page](#)

<

>

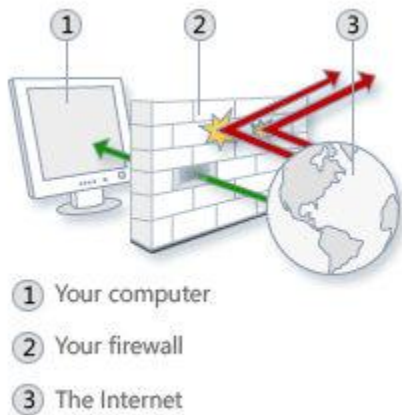
> [Manage security settings with Action Center](#)

Action Center is a central location for monitoring and managing firewall settings, Windows Update, anti-malware software settings, Internet security, and User Account Control settings. Action Center also monitors computer maintenance settings and provides links to troubleshooters and other tools that can help fix problems. For more information about Action Center, see [How does Action Center check for problems?](#)

Use a firewall

A firewall is software or hardware that checks information coming from the Internet or a network and then either turns it away or allows it to pass through to your computer, depending on your firewall settings. In this way, a firewall can help prevent hackers and malicious software from gaining access to your computer.

Windows Firewall is built into Windows and is turned on automatically.



How a firewall works

If you run a program such as an instant messaging program or a multiplayer network game that needs to receive information from the Internet or a network, the firewall asks if you want to block or unblock (allow) the connection. If you choose to unblock the connection, Windows Firewall creates an exception so that the firewall won't bother you when that program needs to receive information in the future.

For more information, see [Firewall: frequently asked questions](#).

[Top of page](#)

Use virus protection

Viruses, worms, and Trojan horses are programs created by hackers that use the Internet to infect vulnerable computers. Viruses and worms can replicate themselves from computer to computer, while Trojan horses enter a computer by hiding inside an apparently legitimate program, such as a screen saver. Destructive viruses, worms, and Trojan horses can erase information from your hard disk or completely disable your computer. Others don't cause direct damage, but worsen your computer's performance and stability.

Antivirus programs scan e-mail and other files on your computer for viruses, worms, and Trojan horses. If one is found, the antivirus program either quarantines (isolates) it or deletes it entirely before it damages your computer and files.

Windows does not have a built-in antivirus program, but your computer manufacturer might have installed one. If not, there are many antivirus programs available. Microsoft offers Microsoft Security Essentials, a free antivirus program you can download from the [Microsoft Security Essentials](#) website. You can also go to the [Windows 7 security software providers](#) website to find a third-party antivirus program.

Because new viruses are identified every day, it's important to use an antivirus program with an automatic update capability. When the program is updated, it adds new viruses to its list of viruses to check for, helping to protect your computer from new attacks. If the list of viruses is

out of date, your computer is vulnerable to new threats. Updates usually require an annual subscription fee. Keep the subscription current to receive regular updates.



Warning

If you don't use antivirus software, you expose your computer to damage from malicious software. You also run the risk of spreading viruses to other computers.

[Top of page](#)

Use spyware protection

Spyware is software that can display advertisements, collect information about you, or change settings on your computer, generally without appropriately obtaining your consent. For example, spyware can install unwanted toolbars, links, or favorites in your web browser, change your default home page, or display pop-up ads frequently. Some spyware displays no symptoms that you can detect, but it secretly collects sensitive information, such as the websites you visit or the text you type. Most spyware is installed through free software that you download, but in some cases simply visiting a website results in a spyware infection.

To help protect your computer from spyware, use an antispyware program. This version of Windows has a built-in antispyware program called Windows Defender, which is turned on by default. Windows Defender alerts you when spyware tries to install itself on your computer. It also can scan your computer for existing spyware and then remove it.

Because new spyware appears every day, Windows Defender must be regularly updated to detect and guard against the latest spyware threats. Windows Defender is updated as needed whenever you update Windows. For the highest level of protection, set Windows to install updates automatically (see below).

For more information, see [Using Windows Defender](#).

[Top of page](#)

Update Windows automatically

Microsoft regularly offers important updates to Windows that can help protect your computer against new viruses and other security threats. To ensure that you receive these updates as quickly as possible, turn on automatic updating. That way, you don't have to worry that critical fixes for Windows might be missing from your computer.

Updates are downloaded behind the scenes when you're connected to the Internet. The updates are installed at 3:00 A.M. unless you specify a different time. If you turn off your computer before then, you can install updates before shutting down. Otherwise, Windows will install them the next time you start your computer.

This article is written by the good folks over at Microsoft.com, visit if you like very helpful information on any windows question.