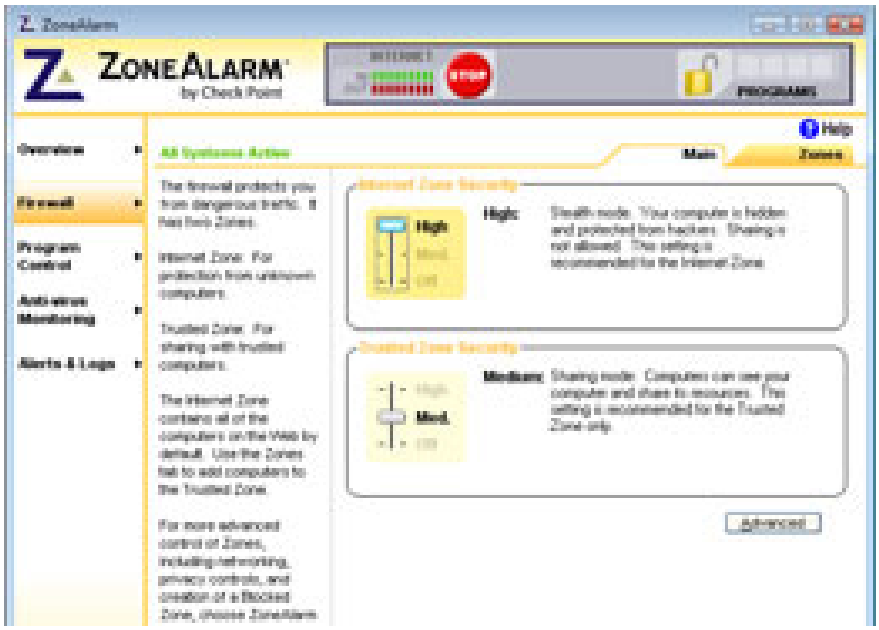
Great way to be safe when using Wi-Fi

Using Wi-Fi at wireless hotspots will help you work more comfortably than having to sit in the office.

Using Wi-Fi at wireless hotspots will help you work more comfortably than having to sit in the office. However, there are many dangers here because hackers can attack your computer when you don't know it.

Here are the tips to help you 'wear armor' for laptops at Wi-Fi wireless access points.

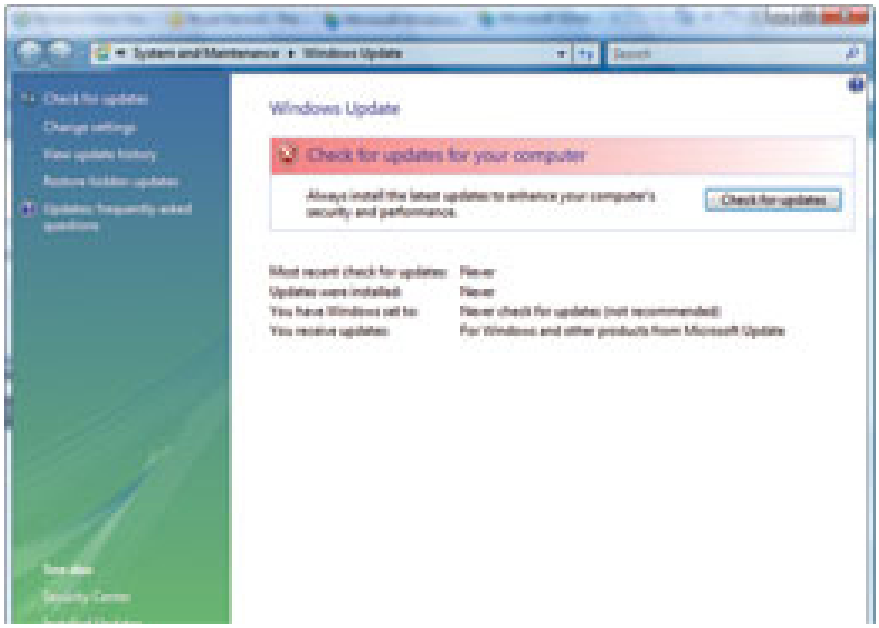
1. Install ZoneAlarm free firewall



Most hotspot hotspots do not have a firewall, but if it is, it is difficult to protect you from skilled hackers who are sharing Wi-Fi.

Therefore, you should turn on the personal firewall before logging in to the Wi-Fi network at the airport or hotel lobby. ZoneAlarm is a free firewall that is highly rated. ZoneAlarm will help you "invisible" your computer to avoid "curious eyes" that want to access your computer via Wi-Fi.

2. Upgrading the operating system (OS)



If you feel shy or don't have much time to upgrade your operating system, you may have to change your habits. The easiest way to upgrade the OS is to access Microsoft's Windows Update system to set up download mode and automatically install important security patches to protect your computer.

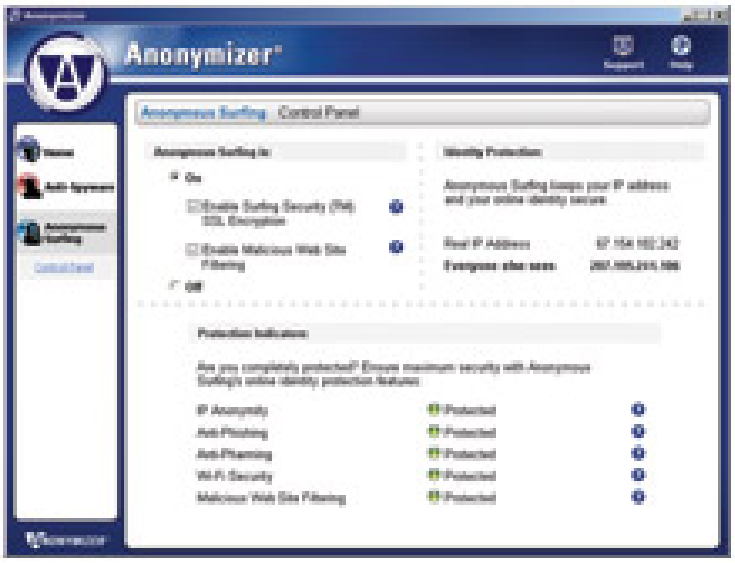
3. Turn off hard drive access and network detection

Although hard drive sharing is convenient for you at work, it's best to turn it off to prevent others from automatically accessing your hard drive. You can do this: Control Panel - Security Center - Windows Firewall - open the Exceptions tab and uncheck File and Print Sharing.

The 'Network Discovery' function in Windows Vista displays the status of the computer so others can see and find ways to illegally connect to your laptop. Therefore, when using a public network, you should turn this off. Open ControlPanel - View network status and tasks - Sharing and Discover - select the Network Discovery

button and click on the 'Turn off network discovery' section - Apply.

4. Don't arbitrarily disclose personal information



Even if a reputable independent website, like VeriSign has confirmed that the site you are trying to access is safe, you should think carefully before declaring personal information when online banking or buy and sell online at hotspot points.

Professional hackers may "catch up" this information by spoofing websites to steal personal information. Our tricks create websites with domain names that are similar to reputable websites, like Citybank instead of citibank, to deceive users off guard.

In addition, you should also install Anonymizer Nyms software for laptops in case you have to perform online transactions at hotspots, it will be more secure. The software will create hidden e-mail addresses to help users make purchases without being detected. Thus, you will protect personal information. Anonymizer Nyms software is priced at $ 19.95 / year.

5. Protect e-mail and password

Sending an e-mail at a public connection the hotspot means that the e-mail is not encrypted and anyone can read its contents. Currently there are many e-mail software, allowing encryption of all sent messages and attachments. In Outlook 2003 software, select Options in the Tools menu and select the Security tab. Click on the option of 'Encrypt contents and attachments for outgoing messages' - OK.

Or you can use password management software, like RoboForm to encrypt accounts and e-mail passwords.

The free RoboForm software will remember your password and account name so it will automatically log in when you need it instead of typing on the keyboard. Therefore, you will avoid plotting to steal passwords of keylogger keyboard scanners. RoboForm can backup passwords and copy between computers.