Protect yourself from wireless access points

Today, you can freely access the Internet anywhere through Wi-Fi hot spots (hotspots) such as airports, restaurants, cafes and even in economic zones. joint. The connection to a cough

Today, you can freely access the Internet anywhere through Wi-Fi hot spots (hotspots) such as airports, restaurants, cafes and even in economic zones. joint. Unfortunately, the more hot spots are used, the higher the security risk.

Connecting to a hot spot can open a danger. Hot spots are often used together, which paves the way for those who like to attack or snoop on other people's problems. They use unsecured and unencrypted connections, but most people treat them as secure private networks.

This can allow anyone to get your personal data and steal passwords and personal information when you are online. In addition, it can also allow a thief to infiltrate your computer without your permission.

However there are many ways to help you solve this problem, we will introduce you in the article. If you follow these instructions, you can completely establish secure connections at any hot spot.

Disable special mode

Few people know : You don't use a hot spot or a wireless router to create or connect to a wireless network through special mode. With this mode, you connect wirelessly directly to another nearby computer. If your computer is set up in special mode, anyone nearby can create a special connection to your computer without your knowledge. They can take actions that damage your system and take away files and personal information.

Solving this problem is simple : Turn off this special mode and you're done. Normally this mode is set to off, but you may turn it on for some time but don't understand them. To turn them off in Windows XP follow these steps:

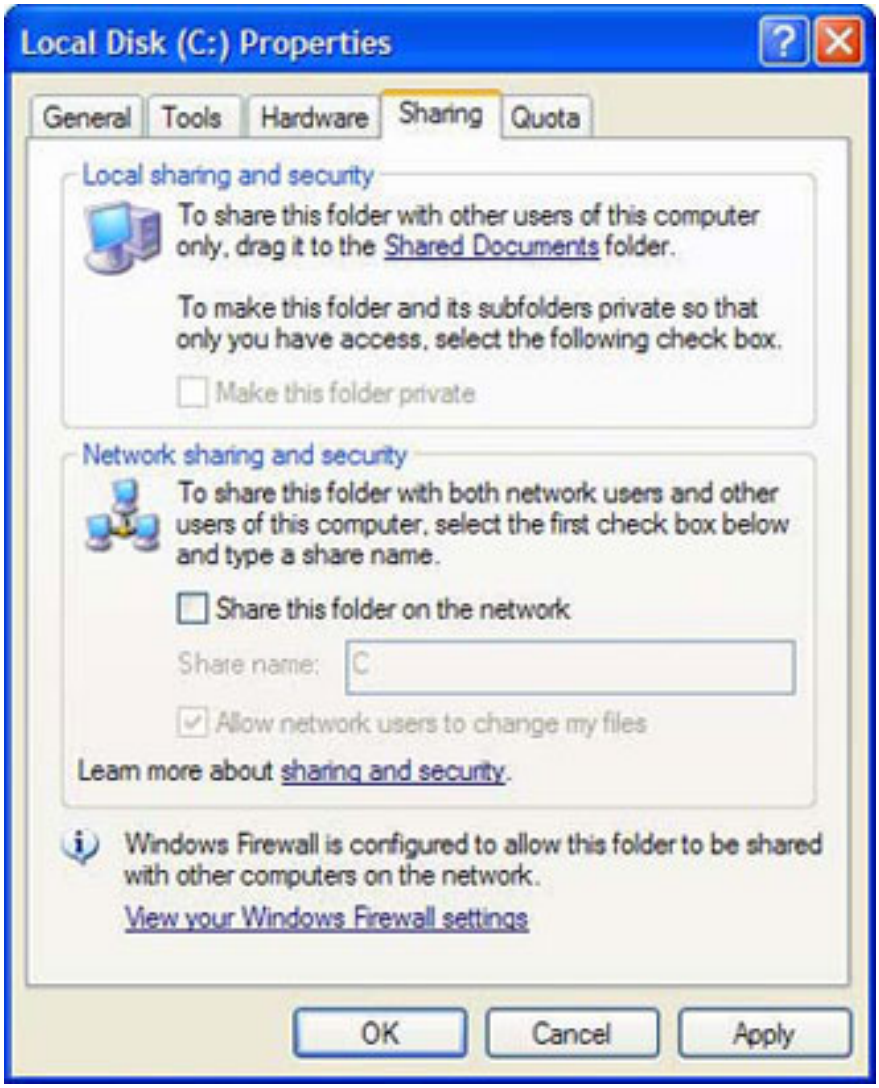
1. Right-click the wireless icon in the System Tray.
2. Select ***Status*** .
3. Click ***Properties*** .
4. Select ***Wireless Networks*** tab
5. Select your current network connection
6. Click ***Properties*** then the ***Association*** tab
7. Uncheck " ***This is a computer-to-computer (ad hoc) network*** ."
8. Click ***OK*** until the dialog boxes do not appear.

In Windows Vista, this step is not necessary because you must perform manual steps to connect to a particular network; and no settings left to make it turned on by default.

Turn off file sharing

Depending on the network used at home or at work, you can share files so the work is done easily and that's great when the network is absolutely secure. But when using a hot spot, this is a completely different matter. It's like you're hanging a line with the text: ' *Go in and get whatever you want* .'

So make sure you turn this off before connecting to a hot spot. To disable this function in Windows XP, go to ***Windows Explorer*** , right-click on the shared drive or folder, select ***Sharing and Security*** **.** and uncheck the box near " ***Share this folder on the network*** ."



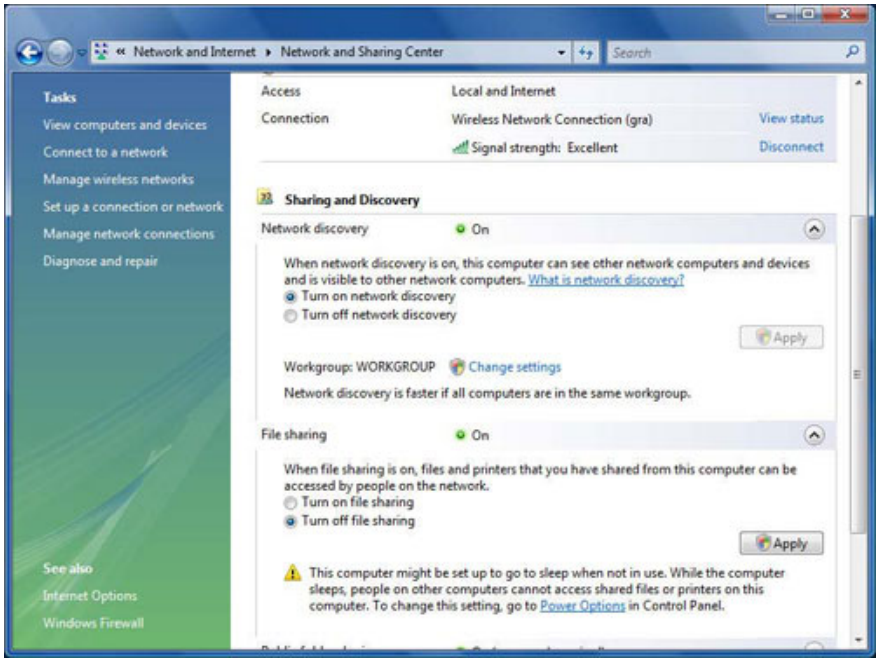
Turn off file sharing mode

If you use Windows Vista, it's easy to turn it off. When you connect to a hot spot, specify the network in *Public* mode. Meanwhile, Windows Vista will automatically turn off file sharing. You can also turn them off manually by selecting ***Control Panel*** -> ***Set up file sharing*** , click ***File sharing and*** choose " ***Turn off file sharing*** " and click ***Apply*** . Then click ***Password protected sharing and*** select " ***Turn off password protected file sharing*** " and click ***Apply*** .

Turn off Network Discovery

If you use Windows Vista, a feature called Network Discovery will make your computer appear on the network so others can see and connect to it. This is useful on an individual network, but if you are on a hot spot, it will cause you more security risks. When you connect to a hot spot and specify the network as Public, Network Discovery will be turned off.

However, you can be sure that Network Discovery is turned off in your hot spot connection. When you connect, select ***ControlPanel*** -> ***View network status and tasks*** . Then in the ***Sharing and Discover section,*** click and click the ***Network Discovery*** button, select " ***Turn off network discovery*** " and click ***Apply*** .



Vista users should turn off Network Discovery to get the highest security

Encrypt e-mail

When you send an e-mail in the hot spot, it is completely exposed so anyone can read it. There are many e-mail software that allow you to encrypt your mail and attachments. Check how you can use it and then use it in this case. In Outlook 2003, select ***Option*** from the ***Tools*** menu, click ***Security*** tab, then check the close box " ***Encrypt contents and attachments for outgoing messages*** ." Finally click ***OK*** .

Encrypt e-mail in Outlook 2003

Use an encrypted USB flash drive

Currently many people use USB flash drives, it is easy to use and convenient, but the price is getting cheaper. With a USB device with a capacity of about 2GB, there is enough space for Windows, the applications you use and the data you need. Make sure that the drive you purchase can use encryption for security. Then install your Windows, applications and data on it.

With laptops, you should not store important data on your hard drive. When connecting to a hot spot, you should start from the USB drive. This way, even if someone somehow gets into the computer, they can't read or change your data because the data is securely encrypted on the USB drive.

Protect yourself with a virtual private network

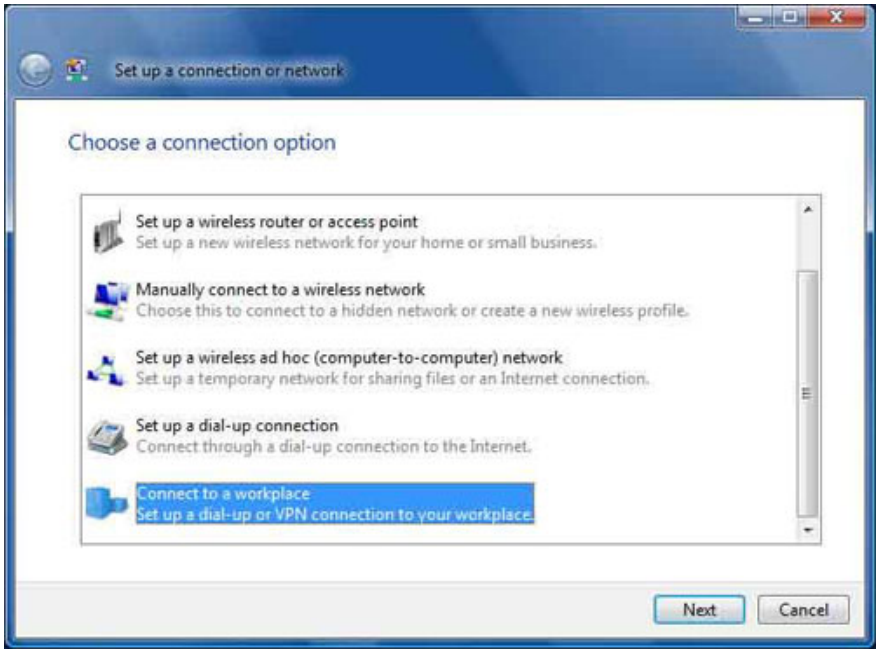
Most hot spots are not safe and do not use encryption. This means that anyone with appropriate software can observe all the packets you send and receive.

But there is a way that does not need to depend on the encryption of the hot spot. With a certain amount of money, you can use a wireless virtual private network encrypted connection. There are now a few services, but we still use one of our favorite services for years, hotspotVPN.

No special VPN software is required, you can use these features in XP and Vista. This service costs about $ 8.88 / month or may cost a bit more to get better services around $ 10.88 - $ 13.88 / month.

When registering a member (subscriber), you will have a username, password and IP address of a wireless VPN server. You run a Windows network connection, fill in the username, password and IP address information and all jobs are done in order. In Windows XP, select ***Control Panel*** -> ***Network and Internet Connections*** -> ***Create a connection to the network at your workplace*** . From the screen that appears, select the virtual private network connection.

If in Vista, select ***ControlPanel*** -> ***View network status and tasks*** . Click " ***Set up a connection or network*** " and select " ***Connect to a workplace*** " then " ***Use my Internet connection (VPN)*** "



Set up wireless VPN using Windows Vista

Disable wireless network card

You can occasionally stay in the hot spot without connecting to the Internet, be absolutely secure by disabling the wireless network card so you can't connect to the network.

If you have a wireless PC card, simply remove them. If you have an adapter that comes with your computer, you can disable it by right-clicking on the wireless network icon and selecting ***Disable*** . If you are using Adapter software to manage computer connections, check out more details to find out how to disable them.

If using Windows Vista, select ***ControlPanel*** -> ***Network and Sharing Center*** . In the ***Connection*** area, click " ***View status*** ," then click ***Disable*** .

Disable a wireless adapter in Windows XP

Watch out for those who "steal behind your back"

If you think that all attacks are good programmers, you should think again. "Thieves behind" don't need to write a single line of code to steal your password, all they do is look over your shoulder from behind when you type a password. So pay attention when entering a password.

Add to that the stolen laptop. If you just need a bit of an opening, for example, you are sitting in a coffee shop and just for a moment you go to the toilet, your computer will most likely be stolen by bad guys. To counteract this phenomenon, in some countries in cafes people have used the port to allow you to lock your laptop.

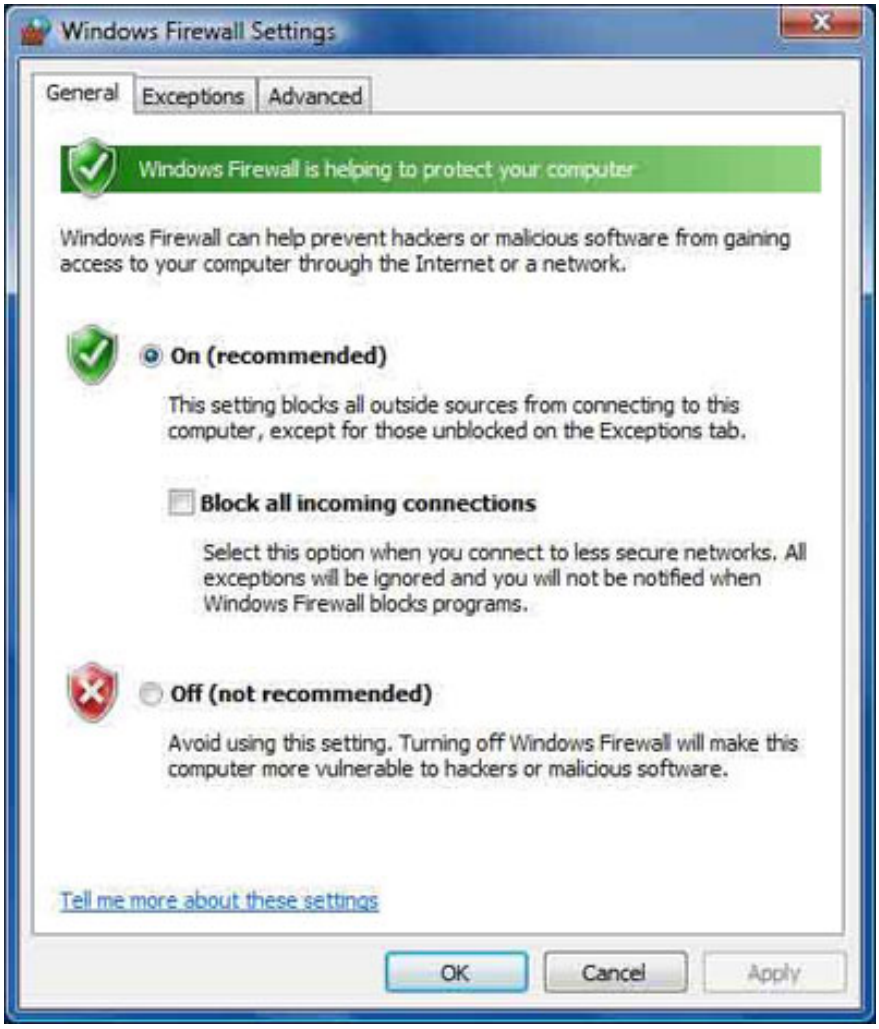
Be careful with fake hot spots

Be careful with this issue! Someone deliberately set up a hot spot near a cafe and created for the purpose of stealing personal information. You are asked to enter personal login information, taking advantage of this, crooks will get important information. To avoid this, you should ask the staff at the café whether there is a hot spot there and what its name is. If you find that there are two hot spots of the same name, you should not connect to both because this can be called "evil twin" set up by someone to trick you into connecting to that fake hot spot.

Turn on the firewall

Both Windows XP and Windows Vista have built-in firewalls, so turn them on. In Windows XP, select ***ControlPanel*** -> ***Security Center*** , click the ***Windows Firewall*** icon at the bottom of the screen. Select ***On*** and click ***OK*** .

If you use Windows Vista, select ***ControlPanel*** -> ***Security*** -> ***Windows Firewall*** . The screen that appears will inform you whether the firewall is enabled. If not, click ***Change Settings*** , select ***On*** and then click ***OK*** .



Turn on the firewall in Windows Vista

Windows XP's personal firewall is not very secure because it protects only the incoming information, not the information (Vista protects both). If you use Windows XP, use a third-party software (possibly ZoneAlarm) to make your computer safer.