Protect your computer against threats

With the popularity of broadband Internet connections, more and more users are connecting to the Internet for the duration of their computers being turned on. Even if you do not have access to the Internet, the computer will still be connected. Such users often worry about more dangerous issues than those who access the Internet through the dia connection

Gabriel Torres

Trojan Horses

With the popularity of broadband Internet connections, more and more users are connecting to the Internet for the duration of their computers being turned on. Even if you do not have access to the Internet, the computer will still be connected. Such users are more worried about malicious issues than those accessing the Internet through dial-up connections or users without Internet access.

To begin with, you must understand that a hacker can only invade your computer if you allow him to do so. For example, a hacker can only invade a computer with a spyware such as Netbus and Back Orifice if you have that type of program installed on your computer. That type of program transforms your computer into a server, making it possible for anyone in the world to invade your computer and read files (with the right tools). But is anyone crazy about installing that file on his computer? Obviously no one. They are usually "Trojan Horses", this is a type of program hidden in screen savers. Fortunately, however, all antivirus programs now recognize and remove that type of program, so upgrading an antivirus program is an important issue.

It should be noted that today Trojans Horses can fake emails sent from investment banks and brokers. For example, while checking your Citibank account, you receive a fake email saying that you should update your data and provide a direct link to help you do that, maybe you will click on it. That link or maybe even install the software attached to this fake email. Not so! This link or this software will steal your passwords and bank data! This technique is also known as phishing attacks, which are increasingly popular.

The best advice in this case is that you should not click on any links or install any software from people you don't know. Because many people today know about phising, they will send emails saying that your relatives send you an e-card or something like that, asking you to click on the link already in it to read the notice. Don't be fooled, in such cases, you should not click on these links! It is Trojan Horse!

However, besides Trojan Horse, is there any other type of procedure that users can unknowingly perform a behavior that causes their computer to be exposed to threats? That is the file sharing.

File sharing

If your home or office computer is not connected to a network, file sharing should be disabled or any hacker can

read (change or delete) all files. in the component you allow to share. To check and disable this feature, go to **Control Panel** , and click the **Network and Internet Connections** icon (or **Network Connections** , depending on how your Windows is configured), select your network connection. you and right-click it, select **Properties** . When the Properties window appears, uncheck ' **File and Printer Sharing For Microsoft Networks** '. This procedure will disable file sharing and protect your computer.

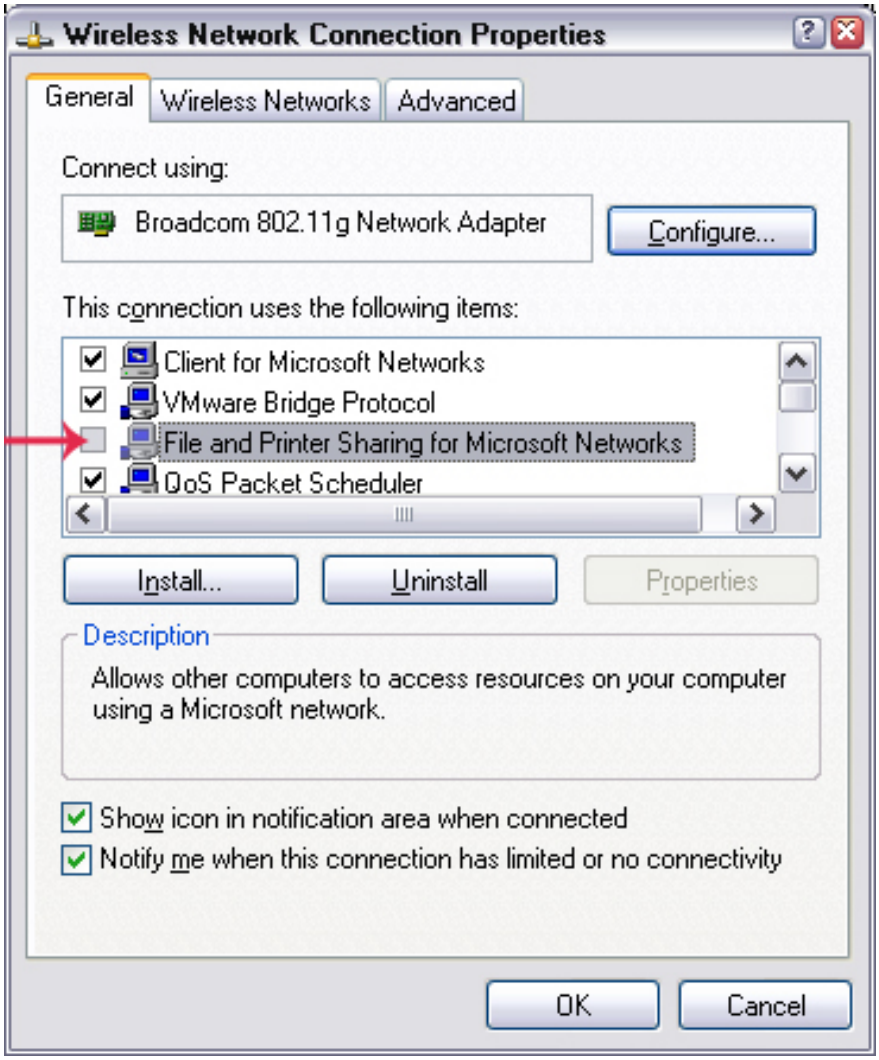

Figure 1: Disable file sharing issues

If you have multiple computers at home or in the office and they are connected to a network, it may be necessary to share files with colleagues - that's why we set up a network. Here you have several options to improve your network security, depending on whether your broadband Internet connection is being shared. Let's take a look at these options.

If the broadband Internet connection is being shared using a router - this is a device that you plug into your modem and computers that want to share the Internet connection. These routers work as a firewall and block incoming requests for folders and files. So you can share files in your office and home network without having to worry about being exposed by file sharing.

But if you don't use a router, you need to be very careful. Maybe an Internet-connected computer is also the

second network card that connects this computer to another computer (usually via a crossover cable) or it can be to a hub or a switch, to share the Internet connection with other computers. In this case, the Internet-connected computer has some vulnerabilities and all computers on the Internet can access its files if file sharing is enabled!

There are several solutions to this problem. The best is to spend some budget and buy a broadband router. As we said, this device also functions as a firewall, protecting your entire network. Installing this device is easy, just plug the Internet connection (cable from the xDSL modem or cable) into the WAN, Boadband or similar jack, then plug the other end into the computer on your network. If you need multiple ports - because these devices often have up to 4 ports - buy a switch with the desired port number and connect this device to one of the router's ports. The switch will work as an extension port. Some routers have wireless antennas to share Internet connectivity with laptops and desktops with wireless connectivity. In this case you need to learn more about wireless security.

However, if you don't have a lot of money, you can simply disable file sharing from an Internet-connected computer. But sometimes this computer needs to share files because it is not always disabled. In this case there are two solutions. First, put all the files you want to share into another computer and enable file sharing on this computer. Or transfer the broadband modem to a computer that doesn't need file sharing.

You may wonder why it is safe to enable file sharing on other computers that do not have a modem. What happens is, usually a modem will have a common IP address. A computer with a public IP address can be viewed by anyone on the Internet. Other computers do not have this type of IP address (computers on the network usually have the form 192.168.xx or 10.xxx,), which are IP addresses that only work on a local network. Computers with this internal IP address are not compromised by anyone from the Internet, so they are safe. At least with file sharing. Don't forget that there are many other types of attacks like phishing .

Personal firewalls are also a good idea. If you use Windows XP, install SP2 package because it has Windows firewall feature, which can prevent malicious software from attacking your computer and if you accidentally install a Trojan The horse can block its attempts to send data out of the computer.

In addition to these threats, there are many other security-related issues such as malware and spyware. Along with it, there are many software that can detect and eliminate these threats. So, install useful software to keep your computer and network safe.