How to check the firewall

You may have turned on the firewall feature of your PC or wireless router at some point, but how do you know if it really works?

The main purpose of a personal network firewall is to keep everything behind it safe from hackers and malware.

Why are firewalls so important to security?

If deployed properly, a network firewall can essentially make your PC 'invisible' to the bad guys. If they can't see your computer, then they won't be able to target network-based attacks on you.

Hackers use port scanning tools to scan computers with open ports, which may have associated vulnerabilities, and provide them with backdoors to enter the computer. For example, you may have installed an FTP port opening application on your computer. An FTP service running on that port may have a security vulnerability that has just been discovered. If a hacker can see that you are opening the port and have a vulnerable service running, then he can exploit the vulnerability and gain access to the computer.

One of the main advantages of network security is that only the ports and services that are really needed are allowed. The fewer open ports and services running on the network and / or PC, the fewer paths an attacker has to try to attack the system. Firewalls need to prevent access from the Internet unless you have specific applications that require it, such as remote administration tools.

Chances are you are using a firewall as part of your computer operating system or wireless router.

The best security approach is to enable "stealth" mode on the router's firewall. This helps keep your network and computer from being vulnerable to hackers. Check the router manufacturer's website for details on how to enable this feature.

How do you know if a firewall is actually protecting you?

You should periodically check your firewall. The best way to test the firewall is from outside the network (ie the Internet). There are many free tools out there that can help you with this. One of the easiest and most useful today is ShieldsUP from the Gibson Research website. ShieldsUP will allow you to run a number of different ports and services, scan your network's IP address (determine when you visit the website). The available scan types from the ShieldsUP site include:

Check file sharing

The file-sharing test will test the common ports associated with vulnerable file-sharing ports and services. If these ports and services are running, it means you probably have a hidden file server running on your computer, giving hackers access to your file system.

Check out common ports

The port testing process typically tests the ports used by popular (and possibly vulnerable) services including FTP, Telnet, NetBIOS, and more. The test will let you know if your router's router or 'stealth' mode is working as advertised.

Check all ports and services

This scan checks every single port from 0 to 1056 to see if they are open (indicated in red), closed (indicated in blue), or in 'invisible' mode (indicated by color. green). If any of the ports are red, you should learn more to see what is running on those ports. Check your firewall settings to see if these ports have been added for some specific purpose.

If you don't see anything in your firewall rule list regarding these ports, it might indicate that you have malware running on your computer, and possibly your PC. has become part of the botnet. If something is confusing, you

should use an anti-malware scanner to check your computer and find out for hidden malware.

Check for Messenger Spam

The Messenger Spam check attempts to send a Microsoft Windows Messenger test message to your computer, to see if the firewall is blocking a service that spammers can exploit and use to send messages to. you or not. This test is only for Microsoft Windows users. Mac / Linux users can skip this test.

Check out what the browser might reveal

Although not a firewall test, this test shows what the browser might reveal about you and your system.

The best results you can hope for on these tests is the message saying your computer is in **"True Stealth" mode** (really stealth) and the scan shows that you are not. Which open port on the system is visible / accessible from the Internet. Once you have achieved this, you can have a little more peace of mind knowing that your computer is not becoming a good prey for hackers.