

Title:

Firewall Protection Needed

Word Count:

621

Summary:

Anti-virus and/or anti-spyware cannot provide the security protection that an Internet firewall can. Enable a firewall for maximum security on you computer to protect against intruders accessing your files and data.

Keywords:

computers, firewall, protection, virus,

Article Body:

If you're using the Internet, then you must have a firewall to protect your computer. It's the only sure way to block intruders seeking to access your computer.

Why would someone want to get to your computer? There are many reasons, including stealing credit card numbers or other personal information. Without a firewall, you expose every item located on your computer to the world. Moreover, using a cable or DSL modem places you at greater risk, since you're always connected to the internet.

WHAT YOU CAN DO - It's essential to run an updated anti-virus program as well as anti-spyware software; however, this is not enough protection. You must also be sure to have at least one firewall installed and running on your computer. A firewall is an extra layer of security that blocks intruders from accessing files and data on your computer. It acts as a barrier and only allows certain types of information both coming in as well as going out of your network. It has built-in filters which permit only those with permission to enter, limiting access between two or more networks, usually between a private network and a public (untrusted) network, such as the Internet. Firewalls also log attempts of others trying to gain access to your network.

TYPES OF FIREWALLS -- A hardware firewall can be installed between your computer network and the outside connection. This is usually used in environments that have many computers networked together, sharing information. For large business environments where maximum protection is essential, it is best to have this type of firewall as well as a software one to prevent your network from

attack. A software firewall is simply a program installed and running in the background to prevent the computers from infecting one another, should a virus or other unwanted hazard make its way onto the network.

However, it should be noted that it is not a good idea to run two software firewalls simultaneously as they are likely to conflict with one another. The existing firewall should be uninstalled or disabled before adding a new firewall program. The hardware version is a bit trickier to install but once it is installed it virtually takes care of your computer with no interaction from you. It provides protection and logs information without the user even being aware of its existence; unlike firewalls of the software version which require some interaction. Software firewalls will sometimes ask permission to allow certain programs access, and you must be knowledgeable enough to know what to allow and what to block. But don't worry; an explanation is always included along with a recommendation as to what action to take.

WHERE TO GET FIREWALL PROTECTION -- If you are running Windows XP you probably have a built-in firewall as Microsoft included it in the Service Pack 2 update. Although there are more efficient and effective firewalls available, the one Microsoft provides would be better than nothing at all. There are also many fairly effective firewalls offered as freeware and many more for purchase. Whatever firewall you choose to use, you should test it after installation and make sure it is working properly. You can do this at the website listed below.

MORE INFORMATION ABOUT FIREWALLS -- Microsoft has a very good website explaining about firewalls that can answer any questions you may have about Internet firewalls. It can be found at the following address - <http://www.microsoft.com/athome/security/protect/firewall.msp>. Another good resource to learn more about firewalls is maintained by Steve Gibson, of Gibson Research Corporation. It can be found at the following address - <http://www.grc.com/x/ne.dll?rh1dkyd2>. You can also test your firewall protection at that site.