

Firewall Recommendations

Connecting to the Internet without a firewall is like leaving the keys in your car with the engine running and the doors unlocked while you run into the store. Although you may be able to get in and out before anyone notices, someone may take advantage of the opportunity. On the Internet, hackers use malicious code such as viruses, worms and Trojan horses to try to find unprotected computers. A firewall can help protect your computer against these and other security attacks.

So what can a hacker do? It depends on the nature of the attack. While some attacks are just nuisances that may play simple pranks, others are created with malicious intent. These more severe strains may attempt to delete information from your computer, crash it, or even steal personal information, such as passwords or credit card numbers. Some hackers enjoy nothing better than breaking into vulnerable computers. Viruses, worms, and Trojan horses are scary. Fortunately, you can reduce your risk of infection by using a firewall.

How do I choose a firewall?

A firewall works by examining information coming from and going to the Internet. It identifies and stops information that comes from a dangerous location or seems suspicious. If you set up your firewall properly, hackers searching for vulnerable computers will not even be able to detect your computer.

There are three basic types of firewalls available today. The first step in choosing a firewall is to determine which one is best for you.

- Software firewalls
- Hardware routers
- Wireless routers

Windows Firewall (Windows XP Service Pack 2 only)

If you are using Window XP Service Pack 2 (SP2), the most updated version of Windows XP, you have a firewall built-in and turned on by default.

If you are using Windows XP and you choose not to install Service Pack 2

You'll still have access to the Internet Connection Firewall (ICF) that's built into Windows XP, but you'll need to turn it on.

Software firewalls

Software firewalls are a good choice for single computers, and they work well with Windows 98, Windows ME, and Windows 2000. (Windows Vista and Windows XP have a built-in firewall, so an additional firewall is not necessary.) Software firewalls are available from many different software companies.

Hardware firewalls

Hardware firewalls are a good choice for multiple computers on a network for central management or for network access control. They should all be compatible with Windows Vista, Windows XP, Windows 95, Windows 98, and Windows NT 4.0. Some networking hardware, such as wireless access points and broadband routers, come with built-in hardware firewalls. These types of equipment can help protect smaller networks. If there is a need for a higher level of security, there are many business and enterprise class firewalls that can protect your network.

Start using a firewall today

Connecting to the Internet can create dangers for the unaware computer user. Using a firewall can help reduce your risk. Installing a firewall is just the first step for safer surfing online. You can continue to improve your computer's security by keeping your antivirus software current. It's also very important to maintain your Operating System software by visiting Windows Update web site to confirm that you've downloaded all the latest critical and security updates for your Operation System.