Use a Firewall

Protecting your Home Computer

When anyone or anything can access your computer at any time, your computer is more susceptible to being attacked. You can restrict outside access to your computer and the information on it with a firewall.

PLEASE NOTE:

This article is intended for personally-owned machines only. UNI systems should have their firewall software managed by the appropriate support staff.

What do firewalls do?

Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary Internet traffic. Firewalls can be configured to block data from certain locations while allowing the relevant and necessary data through. They are especially important for users who rely on "always on" connections such as cable or DSL modems.

What type of firewall is best?

Firewalls are offered in two forms: hardware (external) and software (internal). While both have their advantages and disadvantages, the decision to use a firewall is far more important than deciding which type you use.

- **Hardware** - Typically called network firewalls, these external devices are positioned between your computer or network and your cable or DSL modem. Many vendors and some Internet Service Providers (ISPs) offer devices called "routers" that also include firewall features. Hardware-based firewalls are particularly useful for protecting multiple computers but also offer a high degree of protection for a single computer. If you only have one computer behind the firewall, or if you are certain that all of the other computers on the network are up to date on patches are free from viruses, worms, or other malicious code, you may not need the extra protection of a software firewall. Hardware-based firewalls have the advantage of being separate devices running their own operating systems, so they provide an additional line of defense against attacks. Their major drawback is cost, but many products are available for less than $100 (and there are even some for less than $50).

- **Software** - Some operating systems include a built-in firewall; if yours does, consider enabling it to add another layer of protection even if you have an external firewall. If you don't have a built-in firewall, you can obtain a software firewall for relatively little or no cost from your local computer store, software vendors, or ISP. Because of the risks associated with downloading software from the Internet onto an unprotected computer, it is best to install the firewall from a CD, DVD, or floppy disk. Although relying on a software firewall alone does provide some protection, realize that having the firewall on the same computer as the information you're trying to protect may hinder the firewall's ability to catch malicious traffic before it enters your system.

How do you know what configuration settings to apply?

Most commercially available firewall products, both hardware- and software-based, come configured in a manner that is acceptably secure for most users. Since each firewall is different, you'll need to read and understand the documentation that comes with it in order to determine whether or not the default settings on your firewall are sufficient for your needs. Additional assistance may be available from your firewall vendor or your ISP (either from tech support or a web site). Also, alerts about current viruses or worms sometimes include information about restrictions you can implement through your firewall.

Unfortunately, while properly configured firewalls may be effective at blocking some attacks, don't be lulled into a false sense of security. Although they do offer a certain amount of protection, firewalls do not guarantee that your computer will not be attacked. In particular, a firewall offers little to no protection against viruses that work by having you run the infected program on your computer, as many email-borne viruses do. However, using a firewall in conjunction with other protective measures (such as anti-virus software and "safe" computing practices) will strengthen your resistance to attacks.

Firewall Links

This section will focus on the free software firewalls available to home users that have demonstrated adequate protection. Many of these programs may not be used on institutional computers and are only licensed for non-commercial home use.

Windows Users

Windows machines have a built-in firewall, but many criticize it for not providing full security. The built-in firewall is usually on by default unless a program or user has disabled it.

Comodo Firewall [1]	Free firewall program from a company selling other security solutions.
Windows XP Firewall [2]	Information about the Firewall in Windows XP.
Windows Vista Firewall [3]	Information about the Firewall in Windows Vista.
Windows 7 Firewall [4]	Information about the Firewall in Windows 7.

Mac Users

Recent Mac OS X releases have a built-in firewall. Commercial firewalls are also available.

Leopard (10.5) Firewall [5]	Instructions for the Leopard Firewall.
Snow Leopard (10.6) Firewall [6]	Instructions for the Snow Leopard Firewall.
Lion (10.7) Firewall [7]	Instructions for the Lion Firewall.

Linux Users

Most Linux distributions come with a software firewall or the easy ability to install one. Check your Linux distribution's instructions for more information.

Gnome Lokkit [8]	Instructions for a common, easy-to-use firewall configuration tool for Linux.

Source URL: http://www.uni.edu/its/support/article/717

Links:
[1] http://www.personalfirewall.comodo.com/download_firewall.html
[2] http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx
[3] http://www.microsoft.com/windows/windows-vista/features/firewall.aspx
[4] http://windows.microsoft.com/en-US/windows7/Understanding-Windows-Firewall-settings
[5] http://www.macworld.com/article/131116/2007/12/firewall.html
[6] http://www.macobserver.com/tmo/article/snow_leopard_enabling_the_built-in_firewall/
[7] http://techmix.net/blog/2011/05/24/firewall-on-mac-osx-lion/
[8] http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/custom-guide/s1-basic-firewall-gnomelokkit.html