Enabling Personal Firewalls

Q: Enabling Personal Firewalls

On this page:

Overview
What is a Firewall?
What Does it Protect Against?
Enabling Personal Firewalls

Overview

IS&T recommends using a software-based firewall when using Windows, Macintosh and Linux operating systems. As with any computer safety measure, always check with your local IT support provider prior to enabling a personal firewall.

What is a Firewall?

A personal or host-based firewall is software installed on a computer that controls communication to and from that computer when connected to a network or the internet. It provides a line of defense against someone who might try to access your computer remotely without your permission.

What Does it Protect Against?

A personal firewall can help prevent unauthorized access to your computer by blocking unsolicited communications. Using a defined set of rules, the firewall determines whether to allow or block connections to your computer.

Enabling Personal Firewalls

For any questions about enabling or configuring personal firewalls, contact the IS&T Service Desk or your local IT support provider.

Windows

Windows has built-in firewall that are turned on by default. You only need to configure Windows Firewall if you are having a problem connecting to the Internet. These web pages provide further information about Windows Firewall:

Windows 10: Windows Defender Security Center
Windows 7, Windows Server 2008 R2 : Windows Firewall with Advanced Protection

Macintosh

Mac OS X systems have built-in firewalls that are not turned on by default. The firewall configurations can be found in System Preferences > Security & Privacy.

Linux

Linux has a built-in firewall. See Red Hat Enterprise Linux 3: Chapter 20. Basic Firewall Configuration.