

Home Network Security Guide

Basic Security Guidelines

- 1) Run Windows and Office Updates on your computer every week. Download and apply everything in the Critical Updates section, then reboot your system.
- 2) Update your virus definitions every week. Better yet, set your anti-virus software to update itself automatically. Make sure your subscription stays up-to-date.
- 3) Use a hardware-based router/firewall and keep your Internet connection locked down. Software-based products like Zone Alarm also work well, but may cause problems with your system. This is extremely important, especially if you have a high-speed Internet connection!
- 4) Be careful what you install on your computer. Many programs like *Webshots*, *Kazaa*, *Date Manager*, *Bonzai Buddy*, etc. install “spyware” programs on your computer that compromise your privacy and may cause your computer to crash. A good rule of thumb is, “*If you don’t absolutely need it, don’t install it*”.
- 5) Never reveal your identity to people you meet online. Don’t give any personal information to a website just because they ask for it. Use strong, hard-to-guess passwords and keep them secret!
- 6) Never send sensitive information in an email! An email message is just like a postcard...anyone who sees it can read what it contains.
- 7) Wireless networks: turn on encryption, change the default channel and rename your SSID. If you really want to lock it down, disable broadcasting and enable MAC address filtering.

Eternitek

“*Advancing Christian Ministries Through Technology*”

www.eternitek.com