



Eagle Eye on Technology

May 6, 2006, Volume I, Number I

Risks of Having an Unsecured Wireless Network:

- Your internet connection speed can be reduced due to unauthorized user access.
- Wireless hackers will be almost anonymous, so anything they do online will look as though it's coming from your address.
- Shared files or devices you have on an unsecured wireless network will be accessible to strangers.
- It's also possible that anything you do on your computer can be monitored.
- Your data and personal information can be copied, changed, deleted or misused.



What can you do to be sure you're secure?

For all existing Eagle Eye Computer customers, we are offering a free in-house evaluation of your wireless security.

New or non-wireless customers are invited to contact us for a free estimate for setting up your own secure wireless network.

call us: 503-649-1821 **email us:** help@eagleeyecomputer.com

A network in your home or business offers many conveniences. This includes having multiple computers accessing the Internet simultaneously and the ability to share files and printers. No more copying that document or picture to a removable disk and walking up a flight of stairs to print it!

Wireless networks take the convenience even further. Having a wireless connection is like giving each computer a walkie-talkie or cell phone. Wireless network use is ever increasing. With the constant rise of wireless computers, we are seeing a rise in privacy and security risks.

Much like a walkie-talkie, anyone close enough and tuned to your radio's frequency can hear everything you say. That is, unless you use a secret code to make your conversation unintelligible to anyone who doesn't have the code. This is what enabling security features of your wireless network will do for your privacy. It encrypts your computer's "conversations" to each other and to the Internet.

At the time of purchase, your wireless router typically has little, if any, of the security features enabled. These settings must be turned on during installation or your network will be open to intruders.

To demonstrate how common this problem occurs, I did a site survey of my neighborhood. In a 4x6 block grid I found 103 computers that I could identify as being on a wireless network. *64 of them were unsecured!* Many had shared data and devices that an unscrupulous person could have exploited.

The last issue in the list is the scariest, as identity theft seems to be the mainstay of criminals in today's technology-savvy crooks.

In summary, would you be comfortable with a stranger coming into your home and having complete access to your computers and all they contain?

KEY WORDS DEFINED

WIRELESS: Term describing radio communication that requires no wire between two communicating points.

NETWORK: A group of computers, connected by a telecommunications link, that share information.

REMOVABLE DISK: A computer storage device for the purpose of data transport.

WIRELESS NETWORK: The use of radio frequencies to transmit information between individual computers

ROUTER: An electronic device that connects two or more computers.

SITE SURVEY: The process whereby a wireless network installer inspects a location prior to putting in a wireless network.

ENCRYPT: To scramble information in such a way that it is unreadable to all but those individuals possessing the key to the code.

Web Pages of Popular Wireless Devices

www.linksys.com

www.belkin.com

www.dlink.com

www.netgear.com

Thank you and we look forward to helping you with any computer needs.

Sincerely,

Eagle Eye Computer, Inc.

www.eagleeyecomputer.com

help@eagleeyecomputer.com

503-649-1821