



[WWW.ROGERSONKENNY.COM.AU](http://WWW.ROGERSONKENNY.COM.AU)

## Business Update

### Keep your wireless network safe and secure

Wireless technology makes using your computer easier and more convenient than ever before. With the help of a fast Internet connection and a wireless router, it's possible to surf the Web, print documents or download a movie from any room in the house or office.

Unfortunately, without the right type of network security, anyone near your house or office can jump onto your wireless network and slow down your Internet connection. Even worse, that person could gain access to all of your personal and business documents.

### Keeping out uninvited wireless guests

Restricting access to your wireless network through encryption is easy through encoding or scrambling information that you are sending and receiving. Only those with the right password or "encryption key" can access the network.

Before setting up your own wireless router, let your laptop or desktop computer search for wireless networks within range of your house or office. If you are running Microsoft Windows XP\*, do the following:

1. Click the Start button
2. Click Connect To, which will give you a list of nearby wireless networks
3. Some may say unsecured, which means it's someone's unsecured home/office network, or it's a public hotspot – free WiFi in cafés, libraries, and more. When you're out and about on the town, these free surfing locations are the best!

Here are some ways you can get your wireless network protected:

- Wired equivalent protection (WEP). The most basic kind of encryption, WEP is the wireless equivalent of putting a door on the front of your house or office. It will slow down an intruder, but a determined person can find a way inside.
- Wi-Fi protected access (WPA). A more powerful encryption scheme, WPA was created because of the explosive growth of wireless networks. It definitely offers more security than WEP, but a determined and skillful computer user could break through in a few hours.
- WPA2. A newer and more secure encryption process, WPA2 is what you should be using to protect your network.

“ACCOUNTANTS  
YOU CAN TALK  
TO...”

ADDRESS:  
SUITE 13,  
241 BLACKBURN ROAD  
MOUNT WAVERLEY, VIC

CORRESPONDENCE:  
PO Box 323  
MOUNT WAVERLEY VIC 3149

T (03) 9802 2533  
F (03) 9802 0590

MAIL@ROGERSONKENNY.COM.AU  
WWW.ROGERSONKENNY.COM.AU

## Making a strong password

When choosing a password, people tend to select a small, easy-to-remember word or number such as a child's name or a birthday. Unfortunately, these are the easiest types of passwords for a hacker to crack, so you need to follow some basic guidelines when creating a wireless network password:

- Passwords should be a minimum of 20 characters in length. The longer the password, the longer it takes someone to figure it out.
- Use a combination of uppercase and lowercase letters.
- Insert several numbers in between letters.
- Change your password every 90 days or sooner.
- Write your password down and safeguard it like you would a credit card number.

## Cementing your firewall

If someone gets through your frontline security, make sure your computer and its data are secure from prying eyes. If you are running a Windows-based system, do the following:

1. Click Start.
2. Click on Control Panel.
3. Click on Internet Options.
4. Click on Security and set your Internet security level to at least Medium-High.

## Renaming your network

Routers come out of the box with factory settings. When hooking up your wireless network, make sure to give your router a new name. If your network says the name of the router, people will know immediately what kind of system you have which makes it easier to hack. For computers with built in hardware-based security features, look for laptop and desktop PCs with Intel Inside®.