



# Wireless Security Basics 2008

## Net Sciences, Inc.

### (505) 266-7887

Wireless security is not the oxymoron it has been portrayed to be. Whether you run 802.11 a, b, g or are already a “pre-N” bleeding edge type, improving the security of your home or office wireless network is a relatively painless three-step process. You will change the SSID of your wireless access point or router (alter), use MAC address filtering (filter) and enable WPA/2 encryption (protect) your connection. This entire process can be accomplished in 15 minutes.

#### **SSID (Alter)**

All wireless access points come with a default device name (or SSID). Nearly all manufacturers use simple, obvious SSIDs for their devices. For example, since every Linksys is shipped with “Linksys” as the default SSID it’s pretty easy to find your device in its default configuration. Change it now! Use something obscure, even if it is just something you know well spelled backwards. At the very least, you’ll keep people from guessing the name of your access point.

#### **MAC Address (Filter)**

Every device that communicates on an Ethernet network has a MAC address burned into it during manufacturing. This is a serial number that all Ethernet devices (wired or wireless) have. This MAC address is unique to every device and is very useful to you as you can use it to setup MAC filtering in your wireless device to disallow any but the few addresses you want on your network. The method varies, but it is usually found under wireless security, filtering or MAC ID settings.

#### **WPA and WPA2 (Protect)**

Wireless Protected Access (WPA) and the newer WPA2 are standards for encrypting wireless connections, and offers major improvements over the earlier standards such as WEP. WPA uses a password or phrase to encrypt your data and is not easy to crack. While there is a slight performance hit using WPA, it is well worth it. Also note that all of your connected wireless devices must support WPA. Usually found under “wireless security” options, it is easy to configure and pretty secure.

#### **A Bit More Wireless InSecurity**

As always, the weakest link is always the “nut that holds the wheel” and that will never change. In other words, use common security sense, and don’t hand out your WPA passphrase or put it on your router for all to see. And consider using something more complex than your last name. After all, if I can guess you used it as a passphrase, so can the bad guys.

Of course, even with an altered SSID, there are devices and software that can sniff out your access point and its new SSID. And MAC addresses can be “spoofed” by those in the know. WPA/WPA2 can be cracked by experts as well. But there are still very good reasons for employing these precautions; they are fast and easy to configure and they will prevent the vast majority of wireless attacks. On the horizon is a new 802.11i wireless standard that will offer much more secure wireless networks. Until then, Alter, Filter & Protect your way to secure wireless.