Wireless Security Basics

Securing your home wireless network is easier than ever before. Improving the security of your home or office wireless network is a relatively painless three-step process. You will learn to change the SSID of your wireless device (alter), use MAC address lock down (filter) and enable WPA2 encryption to (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, every Linksys is shipped with "Linksys" as the default SSID making it simple to find your device in its default configuration. Change it now! Use something obscure and be creative. At the very least, you'll keep people from guessing the name of your access point. ***The SSID is usually found in the admin area of your device.***

MAC Address (Filter)

Every networked device (wired or wireless) has its MAC address assigned during manufacturing; this is essentially a unique serial number. It is very useful, as you can setup MAC filtering in your wireless network. That way, only your devices can access your wireless network. The downside is that you must update this when you get new gear, but that is even easier. ***MAC filtering is generally found under the security portion of your wireless access point or router.***

WPA2 (Protect)

Wireless Protected Access (WPA) and WPA2 are the newest security standards for protecting your wireless connection. They use a passphrase to encrypt (scramble) your data and are not easy to crack. Using this sort of protection for your wireless connection is very important. Without it, *anyone* can do whatever they want with your connection, legal or not. These options are usually found in the wireless security area of your device. ***When possible, use "AES" and "WPA2" options.***

The Weakest Link

The weakest link is always the "nut that holds the wheel" and that is you. So use common security sense, and don't hand out your passphrase or put it on your router for all to see. Consider using more complex passphrases. And change that admin password! It is good to know that many of the latest wireless devices include wizards that will step you through the above steps, making secure setup even easier. ***Just do your part and you can have a secure wireless network.***

Net Sciences, Inc.

If you are protecting either critical personal or business assets, or a remote connection to your office, or just want a higher level of security, call on Net Sciences at (505) 266-7887. With ten years of secure wireless experience, offering a full line of wireless solutions, Net Sciences can provide you all the functionality and security you need for your wireless network.