

## Wi-Fi Network Security Basics – How Much Do You Know?

You finally got that new laptop {substitute cell phone, PDA, or tablet PC here} and noticed it has a built-in Wi-Fi antenna showing four available and unsecured wireless networks named “linksys”. You choose one, click on “Connect” and voilà – you are surfing the Internet. How great is that? But do you have any idea whose network you are connected to? Where they are physically located? Is it even legal to connect to someone else’s network without their knowledge? Welcome to the world of Wi-Fi networks; a term short for Wireless Fidelity and used generically when referring to any type of IEEE 802.11 wireless protocol network, whether 802.11b, 802.11a, 802.11g, or dual-band. This article is the first in a two part series that will cover security basics for home wi-fi networks in part one and connecting to public wi-fi networks – such as airports, coffee shops, and even downtown Greenville in part two.

Wardriving is the practice of driving around with a wireless enabled device, usually a laptop, and trying to find unsecured wireless networks. It affects mostly smaller businesses (think private practices) and homes alike, and these rogue connections could be using the majority of your bandwidth, viewing sensitive data, or potentially gathering enough information to lead to identity theft. Large enterprises with sophisticated wireless security are compromised easily by employees adding an unauthorized access point. Public hotspots, such as those at Atlanta Bread Company, have proven that even the most basic computer user can easily log into an unsecured wireless network.

When setting up a home wi-fi network, also referred to simply as a wireless network, there are several steps that can be taken to add security. This is equivalent to adding locks to a door, each layer becomes more and more secure, but not all of them are necessary, and just a few of them will keep out 90% of those up to no good. The first and most obvious step is to **change your router or access point name and password**. Every manufacturer sets a default name and password on their equipment and these are well known by techies who set up networks all the time. When attempting to access a router, trying the manufacturer defaults is about the same as turning the doorknob back and forth to see if the door is locked. If these have not been changed, it opens right up.

The next step would be to **disable “ad-hoc” mode** on any clients in the network, which allows other computers to access them directly and create a peer-to-peer network. In ad-hoc mode 802.11 enabled devices do not need to go through the access point or router to “see” each other, they just need to be within range. So anywhere you are using your laptop, in public or at home, even if you are not connected to a wireless network, you are broadcasting your identity when your antenna is enabled.

**Disable the SSID broadcast** on your access point or router. The SSID, or Service Set Identifier, is the name of your particular wireless network. It is also included in the ‘header’ of every packet of information transmitted within your network. Wardrivers can easily scan for SSID broadcasts and set their laptops the same in order in an attempt to join your network. This may or may not work depending on whether other security measures are in place such as MAC filtering or WEP encryption.

MAC filtering is a simple way to restrict access based upon the MAC address (think serial number) of particular devices. Every network device has a specific number that never changes and your router can be set to only allow specific MAC addresses. This works well if the same devices connect to your network all the time and guest devices are rare. However, it is a low level of security, and can be detected via packet interception, but it is still adding a deadbolt to the door.

There are two types of encryption available currently, **WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access)**. WEP is the older of the two, comes in 40bit, 64bit, and 128 bit formats, but adds considerable size to each packet of data making them take longer to transmit and more susceptible to being dropped. Tools are available on the Internet that can easily decode WEP keys, and in response to that WPA was developed. WPA builds upon WEP by scrambling the key and adding integrity-checking. It also allows authentication by using PKI, or Public Key Infrastructure, encryption. Again, adding more locks to the door. A new encryption standard, WPA2 will be released when 802.11i becomes available.

And finally, check for rogue clients or access points on a regular basis. This is simple to do by using your router's logging capabilities and knowing your own clients addresses. You can also use packet sniffer software to show you the traffic (and how easy it is to see your passwords, text messages and other sensitive information) on your own network. It gives you a good perspective of what other people could see if they gained access to your wireless world.

These are only a handful of the most basic security measures achievable; remember you can incorporate as many or as few as your wish, depending on your comfort level. Think about it like your front door, you can leave it wide open as you drive to the office or you can close it, lock it, and set the alarm system – it is your choice. Next month we will cover connecting to public hotspots since there is absolutely no security on these, but there are several things you can do to protect your data when using them. For more information on Wi-Fi networks, please contact Carin Slader at 864-297-8889.