



From time to time we will have a section here called the “**Glitch Corner**” to help our customers with various topics geared around computers.

This month’s topic is “**Going Wireless**”. Yes the previous month spoke about routers, and I sort of jumped the gun. Now is when this information could be most helpful, with all those wireless gifts: I pads, Ipods, Kindle, Nook and other tablet devices. It is as simple as 123.

What we want to talk about here is Securing your wireless signal. When you go to a hotel and connect, they are making it as easy as possible for you to get connected. They usually broadcast the SSID as the name of the hotel and you click on that wireless. You don’t want to be the “Holiday Inn”, you want your information more secure.

1. Picking an SSID: involves logging into the router either using the “wizard” software that came with the unit or simply typing in the IP of the router (most cases is 192.168.1.1) depending on the brand it will either have no password, admin or password to log in. Once in go to the SSID section and change it from the default settings and put something in you can remember, not your name. Remember the goal is to not be the “Holiday Inn”. You don’t put your last name in (Smith Wireless network). I have proposed not broadcasting the SSID but I have found in the real world this does not work unless you help everyone connect their equipment. If you know how to do this, I would stop broadcasting also, it creates one more level of security.

2. Security code: Normally I use an unpublished number like your cell number. It is easy to type in most devices and even easier to remember. The 10 digits work great for both WEP and WPA2 security. Currently I like to use WPA2 personal, it is more secure than WEP and more clients (equipment) will attach better. People with Windows XP machines may want to use WEP.

3. Change the Password: In the first part of this I said that the password may be password, admin or nothing. I normally change it to the customer’s last name. The reason is to simply get it away from standard settings. You can only get to the router from inside so making a super strong password is not a major factor. There are carefully crafted web sites that can change settings without your knowledge. I have seen this 2 times in our little world.

More advanced things to improve performance would be to change the default channel to something other than 6. Good chance your neighbor did not. Also updating the firmware or software for the router, this will fix many known problems. Backup the settings so in case you have a relative that likes to hit the reset button. You can put all these settings back in place.

All standard routers work on ComSouth’s system. We prefer the Linksys/Cisco brand, specifically the E2500. It has wonderful features and performance. Belkin offers an inexpensive unit with the SSID and WPA2 key preprogrammed in the device. Simply put the information on the card into each device you connect. Netgear has two features I like. First is that it looks for firmware updates when you log into them. The second some models with change the internal IP scheme should it see a conflict. They also offer some models in the distance range of the E2500.

We offer professional setup of these devices to secure them from outside intruders, at very reasonable pricing.

G²