Is Your Wireless Network Secure?

A recent national study estimated that 60 to 70 percent of all wireless networks are unsecured. CNN recently reported that out of a survey of over 3000 detected wireless networks in US metropolitan areas, over 67 percent had no encryption enabled.

Due to the convenience of mobility and no need to route network cabling between connected devices, more and more homes and businesses are turning to wireless networking. However, many may be unaware of the multitude of security risks that arise when making the choice to implement a wireless network.

The nature of wireless networking is radio broadcast oriented, whereby network communications are propagated through space with no boundaries and receivable by anybody in range with a wireless network adapter. This means that if you have an unsecured wireless network in your home or office, anyone within range can spy on your on-line activities.

They can also connect to your wireless network and access your Internet gateway, leeching away your precious bandwidth that you are paying hard earned dollars to your Internet service provider for. Even more threatening, if the offending person is conducting illegal activities through your Internet connection, these activities can be traced back to You! If you are sharing folders and files on your network, any one who gains network access can view and download their contents as well.

Sensitive personal information you may have stored on your computer could be retrieved and you could end up being a victim of fraud or identity theft.

A big contributing factor to the prevalence of unsecured wireless networks is that most wireless router or access point

manufacturers ship their devices with no security as the default setting. The average customer sets their wireless device up, connects their wireless enabled computers, and upon finding that everything is “working”, decides not to configure any further.

The lack of security on the device makes for an easy installation, however at the cost of serious risk of breach. An analogy would be to leave your car in a parking lot unlocked with the keys in the ignition, all for the sake of conveniently entering and starting it up. No one in their right mind would leave their car like this in public, so neither should they leave their wireless network in such a state.

If you have a wireless network and are unsure about whether or not it is secure, or don’t know how to properly secure it, please give me a call today and schedule an on-site network security assessment. I will secure your wireless network to the highest possible standards available for your equipment, and give you peace of mind about enjoying the benefits of wireless networking!

-Ted Eiler
Computer Service and Repair Technician
www.tecs-onsite.com
800.993.TECS (8327)
tedeiler@tecs-onsite.com