Protect Your Wireless Network

Author: Brian Lisse

Enable WPA2 Encryption To Protect Your Wireless Network

It is very convenient to be able to sit across the house from the wireless access point or router and be connected to the Internet while sitting on the couch or lounging in bed. You always need to keep in mind though that your data is being beamed through the airwaves in all directions and that if you can receive it from where you are, so can just about anyone else within that same range.

In order to protect your data from snooping or prying eyes, you should encrypt, or scramble, it so that nobody else can read it. Most recent wireless equipment comes with several encryption schemes that you can enable.

WEP was the encryption scheme included with the first generation of wireless networking equipment. It was found to contain some serious flaws which make it relatively easy to crack, or break into, so it is not the best form of security for your wireless network.

WPA was later rolled out to provide significantly stronger wireless data encryption than WEP. The current strongest standard type of commercial wireless encryption is WPA2.If you can use WPA2 you should because it is much more secure and will keep casual snoopers and novice hackers out of your wireless network. Using encryption with a longer key length provides stronger security.

Refer to the owner's manual for your wireless router or access point to determine how to enable and configure encryption for your device. Once you enable encryption on your router or access point, you will need to configure your wireless network devices with the proper information to access the network.

If you are unsure of how to enable encryption or secure your wireless network, please contact us so we can assist you. We may have to take remote control or send out a technician to do it properly, but having a secure network can give you greater peace of mind that others are not "leeching" from your network.