



MYRA'S 7 WAYS TO SECURE YOUR WIRELESS NETWORK

It is second nature for us to have locks and alarm systems installed to protect the physical area of our home or business. We protect our assets using physical locks to deter criminals. Wireless networks are common in homes and businesses because of its convenience. It allows us to move around freely with our laptop and work anywhere as long as we are within the coverage of our wireless network. Wireless networks are considered part of your basic network setup.

Unfortunately, having a wireless network means that criminals no longer need to set foot in your home or office to steal from you and your business. Please consider the following tips to help prevent cybercriminals from snooping, capturing, stealing, and analyzing your data:

- 1) The placement of your wireless access point is important. If you can, place your router in the middle of your home or office to prevent anyone from the outside to “reach” and access your wireless access point.
- 2) (Always) read the manual that came with your wireless access point and turn off broadcasting. Check your router manual and look for how to turn off SSID or Service Set Identifier. So that when connecting to your wireless network, you will not see your wireless network listed in the “wireless network available” window. Instead you will need to manually configure your computer to logon to your wireless network.
- 3) Do not use the default SSID name. Change it. Also, do not assign SSID names that are easy to guess. For example, if your business name is ACME, do not use ACME for your SSID name. You’ll be surprise on how many people actually do this. Also do not use a department name or a street name.
- 4) Your wireless access point came with a pre-configured admin account password. Change it!
- 5) Although this might be a demanding task, if you have more than 20 devices, allow Known Media Access Control Address, or MAC Address, only. Every NIC or Network Interface Card has its own unique address. It is like a social security number. Limit access to only MAC addresses that you have pre-configured.
- 6) Limit the range of the Dynamic Host Configuration Protocol or DHCP private IP addresses available for lease. If you have 10 computers and devices, allow 12 (10+additional 2) IP addresses to lease. When the set limit is reached, any wireless device requesting an internet protocol or IP address will be denied access. Set your leased IP addresses to expire at least every 3 days. Your device will auto-renew its leased IP address.
- 7) Take advantage of available authentication and security protocol that your wireless access point offers. If your wireless access point supports Wi-Fi Protected Access or WPA, use it. If not, WEP or Wireless Equivalent Privacy will work as well.

The above tips will help secure your wireless network and better protect you information. Please remember that it is very important to routinely check your wireless access point’s manufacturer’s website for firmware updates.

Please check back soon for more free tips about the importance of routers.

P.O. Box 5666
Concord
California 94524
925.779.0929 **F**

MYRA SANTOS
415-286-3421 **T**
msantos@e5hex.com
MICHAEL C. ESVER
925-575-4382 **T**
mesver@e5hex.com