Quick Facts About Wireless Network Security

- *It takes on average 5 minutes to break a WEP security key. The more personal wireless devices on that network, the quicker the hack.*
- *49% of the households in the world that use WiFi are using it unsecured.*
- *80% of households use the default admin password.*
- *89% of Public WiFi (Fast Food Joints, Coffee Shops, etc.) use unsecured hotspots.*
- *77% of people who have used FREE WiFi have experience Cyber Crime.*

Prepared by
Jim Guckin
For
www.JimGuckin.com

Jim has worked in the technology field 2005, in that time He's worked in the Law, Retail, Project Management and Government fields. He has worked on many major projects, but his main interests are in computer security and disaster recovery.

WIRELESS NETWORK SECURITY

What everyone <u>NEEDS</u> to know about securing a personal
Wi-Fi network.

WIRELESS NETWORK SECURITY

WIRELESS NETWORKS

The use of laptops, tablets and smart phones continues to grow as devices become more affordable and easier to use. As a result wireless networks (Wi-Fi networks) have become more popular. Wi-Fi networks work by using radio waves to talk back to the Wi-Fi router and get you out on the internet.

Two components comprise a Wi-Fi network: a Wireless Access Point (WAP), also known as a wireless router; and a computer with a wireless network adaptor.

The wireless router is the building block of a wireless network. It has a small radio transmitter and receiver. The wireless card in your device also transmits and receives from the wireless router. Most modern devices come with a built in wireless card that will work with Wi-Fi networks.

PROBLEMS WITH Wi-Fi NETWORKS

The convenience of Wi-Fi networks also brings security liabilities. With modern Wi-Fi networks, the wireless signal may be visible to people outside of your home. This is very common, with the pursuit of strong signals. For example, anytime you search for a Wi-Fi signal on your devices and your see several other networks in the area.

Thankfully there are easy steps to make sure your home wireless network is secure. But before we get there. Here are the reasons for securing it.

Wi-Fi makes it so an attacker doesn't need physical access to your network to attack it, they only need to be in signal range. Attackers usually use a method called War Driving to scout out networks to attack. This involves searching around for the most vulnerable networks. Once your wireless network is discovered, attackers can access your network and data from outside your residence. Since physical access to the network is not required, the likelihood of being detected is decreased, therefore providing more time to hack into and use your network.

What are these attackers looking for? Well it depends on what they want to do. Some concerns are:

- Stealing your personal information (identity theft)
- Gaining access to your banking or credit cards
- Sending spam through your network
- Illegally downloading software or music
- Using your computer(s) or device(s) to attack another target
- Infecting your computer to distribute viruses of malware.

Even if they only want free internet, that can have an impact on your network. Most internet connections have a maximum speed at which you can download information, If an attacker starts to use your connection it can slow things down for you. Plus if they have any malware or viruses infecting their computer, it could easily spread to your network.

HOW TO SECURE YOUR WIRELESS NETWORK

There is no way to make your network 100% safe, but there are easy ways to make it an unappetizing target for an attacker.

Change the default information from your Wi-Fi router. This is the default admin password and the passphrase to connect to the network. Vendors default administrator passwords to the routers are usually very well-known and easy to look up. The default passphrase is sometimes easy to guess as well, as its mathematically assigned.

Turn off the SSID broadcast. Most wireless networks want you to know their name, and they broadcast this information out. You have the option of turning that announcement off and still being able to connect to your network.

Make sure you are using WPA2 encryption on your wireless connection. WEP is a popular encryption protocol. The problem with WEP is it's code has been broken and hackers can listen to your wireless traffic and use math to get your wireless passphrase. WPA2 prevents this by not using a known algorithm.

Use MAC filtering. If you know that there will be no other devices using your network, then MAC filtering will only let those computers connect. This works well if it's an controlled environment without new devices logging on.

Cut down the transmitter strength. Some Wi-Fi routers will give you this ability. While this will cause the signal to lose strength, it may keep people from accessing.

Turn off remote management. Most Wi-Fi routers give you the ability to make changes to your network remotely, but most people don't, so leaving it on is a security vulnerability, giving an attacker access.

Turn off WPS (Wi-Fi Protected Setup). This is an convenience tool many wireless networks come with, but once again with it on, hackers can attack the router and get the passphrase.

Use Firewalls. Almost all routers come with a firewall. Make sure it's turned on as well as turning on your computers firewall. This will help block some traffic if an attacker get in.

Install anti-malware software, on your computers and keep them up to date. These will help prevent your network from being easily infected.