

## Home Wireless Network Security Issues

Running a business from home has its advantages, including no commute, a more accommodating work schedule, fresh coffee and home-cooked meals at any time you want.

But running a business from home using a home wireless local area network (WLAN) with your computer may lead to thievery of confidential information and hacker or virus penetration unless proper actions are taken. As WLANs send information back and forth over radio waves, someone with the right type of receiver in your immediate area could be picking up the transmission, thus acquiring access to your computer.

Here is a list of things that you should consider as a result of implementing a home wireless network setup used your business:

Viruses could be loaded onto your laptop which could be transferred to the company's network when you go back to work.

Up to 75 per cent of home wireless network WLAN users do not have standard security features installed, and 20 per cent are left completely open as default configurations and are not secured, but are made for the users to have their network up and running ASAP.

It is recommended that home wireless network router/access point system setups be always done through a wired client.

Always change the default administrative password on your home wireless network router/access points to a secured password.

Enable at least 128-bit WEP encryption on both card and access point. Change your WEP keys periodically. If equipment does not support at least 128-bit WEP encryption, consider replacing it. Although there are security issues with WEP, it represents minimum level of security, and it should be enabled.

Change the default SSID on your router/access point to a hard to guess name. Setup your computer device to connect to this SSID by default.

Setup router/access points so as to not broadcast the SSID. The same SSID needs to be setup on the client side manually. This feature may not be available on all equipment.

Setup your home wireless network router to block anonymous internet requests or pings.

On each computer having a wireless network card, network connection properties should be configured to allow connection to Access Point Networks Only. Computer to computer (peer to peer) connections should not be allowed.

Enable MAC filtering. Deny connection to wireless network for unspecified MAC addresses. MAC or physical addresses are accessible through your computer device wireless network connection setup and they are physically written on network cards. When adding new wireless cards / computer to the network, their MAC addresses should be registered with the router /access point.

Your home wireless network router should have firewall features enabled and demilitarized zone (DMZ) feature disabled. Periodically test your hardware and personal firewalls using Shields Up test available at Gibson Research Corp. web site. All computers should have a properly configured personal firewall in addition to a hardware firewall.

Update router/access point firmware when new versions become available.

Locate router/access points away from strangers so they cannot reset the router/access point to default settings. Also, locate router/access points in the middle of the building rather than near windows to limit signal coverage outside the building.

You should know that nothing is 100%. While none of the actions suggested above will provide full 100% protection, countermeasures do exist that will help. The good collection of suggested preventative actions contained herein can help you deter an intruder trying to access your home wireless network. This deterrent then makes other insecure networks easier targets for the intruder to pursue.

Source: <http://www.articlecircle.com>

## About the Author

Greg Lietz is a freelance writer and internet businessman. His main website is <http://www.theonlinebizplace.com> where he provides content about internet business opportunities. He owns the website <http://www.theonlinearticleplace.com> which is a new article directory.