

What You NEED To Know About Wireless Network Security

**By Chris McVey, Special Projects Manager
United General Title**

Over the past few years, wireless networks have increased in popularity and are now common in most cities and homes. Wireless networks provide many advantages over traditional wired networks, but they do add an extra level of concern regarding security over their wired counterparts. Studies have shown that 60 to 80 percent of home wireless networks are insecure. Running a home wireless network with no security is similar to unlocking your front door and hanging a sign that invites thieves inside to steal. This article is intended to inform the reader as to why wireless network security is important and what are some of the basic security options available.

I'm Just Browsing the Internet – Why Do I Need 'Extra' Security?

Many individuals think that they do not need to worry about complicated extra security measures because they are just browsing the Internet or sending e-mails to friends and family via Hotmail or Yahoo. The first thing to consider is that wireless networks turn on very few security measures in their default configurations. Meaning if you set up your wireless router based on the basic instructions, your network is wide-open and insecure.

If you have an unsecured wireless network in your home, anyone in close proximity, a car parked across the street or a neighbor, can spy on your online activities. One way to think of a wireless network is that it is very much like running a cable from your home network out to the street curb and inviting any passerby to plug in. Indeed, every file on your computer's hard drive could also be available to others depending on how your network is configured. Similarly, an intruder could spread viruses or other "malware" to your computer(s) since they are in essence masquerading as a trusted member of your home network. If your wireless network is unsecured your neighbors could be using your wireless network for Internet access; using the bandwidth you are paying for. If your neighbor downloads music illegally or conducts another illegal activity while using your connection, that activity could be traced back to your network.

OK, I Know I Need to Secure My Wireless Network – What Do I Do?

Now that we have established why a secured wireless network is important, we can review some of the security options we do have. One of the most basic things you can do is to change the default username and password to your router when first configuring your network. The options listed below are just some of the basic security options available. Implementing these options will greatly improve the security of your wireless network, although no solution will make a wireless network 100% secure.

- **Run a Firewall:** A firewall can be a program or hardware device that protects your computer from malicious users and websites. By default most software firewalls block all incoming traffic and prompt you for permission to allow specific traffic through. A wireless intruder cannot access your files or easily spread viruses on your network since the firewall will block such activity. A software firewall is a great choice because it will also keep you protected if you ever use a public wireless network (HotSpot). Windows XP has a built in software firewall and some links to other software firewalls are listed below.
- **WEP / WPA Security:** WEP and WPA are schemes to help protect wireless networks. Both require that the user provide a secret key, not unlike a password, when first connecting to a wireless network. WPA is the more secure method, although older hardware may only support WEP. If your current hardware does not support WPA it may be time to consider upgrading the hardware. Both protocols provide a level of security that can deter casual snooping, but WPA corrects a lot of the security problems that can be found in WEP schemes.

- **MAC Address Filtering:** This method does not use a secret key to authenticate users; it uses a computer's hardware to limit access to the network. Each computer has a unique MAC address. MAC address filtering allows only computers with specific MAC addresses to access the wireless network. You must manually specify which addresses are allowed access to the network when configuring your router. This method is fairly secure except when dealing with experienced hackers, although any new computer that needs access must be added in the router's configuration. This method basically allows you to designate what computers may access the network; any devices not on your list will be denied access.

Conclusion

In addition to the methods above there are many other security options to help secure your wireless network. We recommend implementing multiple security measures to help keep your network secure. Below are some links to additional resources on the internet that pertain to wireless security. The one thing to remember is that unless you take some simple security precautions, your wireless network is very vulnerable to intrusion.

Wireless Security Links

[Top 9 Tips for Wireless Security from About.com](#)

[Complete Guide to Wi-Fi Security by Jiwire \(home networks & public hotspots\)](#)

[Improve the Security of Your Wireless Home Network with Windows XP](#)