

How to Secure Your Wireless Network

If you use a wireless network, chances are good it is not secure. If you don't make some important configuration changes on your wireless router after installing it, your wireless network is wide open to hackers, curious neighbors and people who would rather use your broadband internet service instead of buying their own.

Several of my neighbors have a wireless network set up in their home, and from my living room I can connect to three different networks in addition to my own. I do this easily, using no special skills, software or equipment. All I do is click on my wireless networking icon and select "view available wireless networks". I choose one, click "connect", and in an instant I am using my neighbor's internet connection instead of my own. Kind of creepy, isn't it?

Following are 6 things you can do to make your wireless network invisible and impenetrable to the majority of intruders.

- Change the default password of your wireless router. This makes it harder for a would-be intruder to access the router administration controls.
- Change the name of your SSID. The SSID (service set identifier) is the name of your wireless network, and by default is usually the brand name of your wireless router (like Linksys). Change this to a unique name of your choice. A good rule of thumb to follow when setting up any type of network is to always change the default settings to something else, which makes it harder for an intruder to get in.
- Use an encryption key. Most wireless routers have WEP encryption capability (Wireless Equivalent Protocol), and the newer ones also have WPA (Wi-Fi Protected Access). WEP is an older standard and less secure than WPA, so if you have both, choose WPA. Even WEP is probably good enough, and if this is all you have choose the highest bit encryption possible (usually 128 bit). Once you set up encryption on your wireless router, write down the method you are using as well as the key (a long string of cryptic-looking characters), because you will need this to set up encryption on each of your computers that will use the wireless network.
- Disable broadcasting of your SSID. By default, the SSID (your wireless network's name) is broadcast to anyone with a wireless network card. Although this makes it easy to configure your computers to access your network, it also makes it easy for outsiders to know about your network. By disabling SSID broadcast, no one will ever see your network.
- Limit the number of IP addresses your wireless router allows on the network. By default, your wireless router will assign an IP address to as many computers that request one. If you limit the number of addresses that the router's DHCP server assigns to just the number that you need, you will "block" all other computers that try to connect to your network.
- Use MAC address filtering. You can configure your wireless router to only allow certain computers on the wireless network by including each computer's MAC address in the list of "allowed" users. A MAC address is a unique physical address that is hard coded onto each network interface card. It is much like a serial number, as every MAC address is unique. Find your network card's MAC address by opening up a command prompt and typing in `ipconfig /all`. Look for something that says "physical address", and the series of letters and numbers following this is your MAC address. It will look something like this: 00-06-5B-CE-DA-B5. Key this information into the wireless router's MAC address filtering setup under MAC address 1. Repeat this process for every computer on your network, using MAC address 2, 3, and so on.

In addition to securing your wireless network, there is one more thing you need to do to make sure your wireless network is safe:

- Install a personal firewall on each of the computers on your wireless network. If an intruder does happen to get into your network, a personal firewall (also known as a software firewall) will keep him out of your computer. With a personal firewall running, the most an intruder can do is use your internet connection and your bandwidth; he will not be able to access your data.

To learn more about computer security, visit:

Antivirus, Firewall and Spyware Resources

Personal Firewalls - Software Firewalls

Free Report - Internet Crime - How to Protect Yourself Online

Article Source: http://EzineArticles.com/?expert=Debbie_Jacobsen