# How to Secure Your Wireless Network Connection

By: Gail Seymour

Your wireless network connection may be designed to be easy for ordinary users to connect to, but that also makes it easy for hackers to access. An unsecured network is open to every passing device. That means your neighbors, kids on the street with smartphones and hand-held gaming devices, and criminals in a van intent on stealing your identity or watching you stop your newspaper online to learn when you will be away on vacation all have an open invitation to your network. Even a secure network can be easily hacked with the right tools and enough time.

Take the time to make your wireless network as secure as possible. Start by connecting to the router by entering its IP address in your Internet browser where you would normally type a Web address. This is usually 192.168.1.1, and it should be identified in your router's instruction manual. If not, you can find it by running the ipconfig utility on your computer. On a Windows PC, type "cmd" in the search bar on the start menu and "ipconfig /all" at the command line, and hit enter. On a Mac, you need to open "Terminal" in Applications / Utilities, and type "ipconfig -- a." Look for a line labelled as "Gateway," and make a note of the number.

One of the first things you should do when securing a wireless network is change the administrator password from the default, which is often as obvious as

"password," or "admin." Use an alphanumeric, random password. Write it down, and store it somewhere safe, because you won't use it often. Even if you think you will remember it, chances are you won't. This single step alone won't secure your network, though; it will only make it harder for hackers to hijack your Internet connection and make changes to lock you out.

Change the Service Set Identifier (SSID), which your router uses to identify itself. Many default names include the manufacturer or Internet service provider or some other details that make hacking the network easier. Don't include your address or name details either in the new SSID. Whether you decide to broadcast the SSID is really up to you. If you don't broadcast the SSID, it won't show up in the list of available networks on your devices -- so most of your neighbors won't know it's there. However, it will still be visible to serious hackers with packet sniffers. If you do decide to turn broadcasting off, do it after you've set up your own devices on the network.

Add encryption to your wireless network to prevent unauthorized traffic monitoring and access.

If possible, set authentication to WPA/WPA2. This will use the newer WPA2 when available but revert to the older WPA on devices that don't support it. Avoid using the less secure WEP if possible, but remember that even that is better than a totally unsecured connection.

By default, your router will be set up to accept connections from any wireless-enabled device. You can use the security settings on most routers to change this by either blocking certain IPs or MAC addresses. For even greater security, you can also change the settings to allow connection only from IPs and MACs on a list you provide. It's generally better to control connections with MAC addresses (found under ipconfig, listed as a physical address and consisting of six pairs of alphanumeric digits) rather than IP numbers. MAC addresses are specific to the piece of hardware, whereas IP numbers may be dynamically assigned. Although hackers can "spoof" Mac addresses, these precautions will deter the casual "piggyback" use of your Internet connection.

Source:

http://www.life123.com/technology/computer-networking/wireless-network/how-to-secure-your-wireless-network-connection.shtml