

# How to Make a Wireless Network Secure



In this short paper, we're going to go through 5 steps to secure a home wireless network.

## 1. Login to your wireless router

- a) If you've never logged into your wireless router, look up the make and model of the router, and find the default IP Address, username, and password, then login.
- b) For example, if your wireless router has a default IP Address of 192.168.1.1, default username of admin, and default password of blank. Login by doing the following:
  1. Open Internet Explorer and type in the address <http://192.168.1.1>
  2. When prompted, the username would be admin, and the password would be blank.
- c) If the router's password is still set to the default password, it is important to change this password to something else to keep an intruder from effectively kicking you off of your own network.

## 2. Enable MAC Filtering

This is probably the easiest way to keep intruders off of your wireless network although the least secure. You can enable a White-list of MAC Addresses and then only the MAC Addresses that you specifically put into this list will be able to use your Wireless. You'll have to remember this if a friend comes over and tries to use your wireless network.

## 3. Enable Encryption

It's important to use encryption on your wireless network. Not only does it keep intruders off of the network, it also keeps eavesdroppers from listening in on your network traffic. The two major types of wireless encryption are listed below. Please also note that any encryption enabled on the wireless router must also be enabled on each Wireless Device that needs to connect to the internet.

- a) **WEP** – This is still the most common type of encryption enabled on most wireless routers. Please note that this can be broken by serious hackers in about 2 minutes, but will keep out most neighbors and passerby's.
- b) **WPA2** – This is becoming the most common type of encryption and is enabled on most new wireless routers. WPA2 is much more secure than WEP and has not been compromised yet, but is not available on some older types of Wireless Devices.

### Deciding between WPA2, WEP, or MAC Filtering

WPA2 Encryption is the most secure method for keeping intruders off your network. If you have older devices that will not support WPA2, WEP is encouraged. If you are unsure how to setup encryption, MAC filtering is least secure, but easiest to setup.

#### **4. Disable SSID Broadcasting**

This option decides whether people can or can not see your wireless signal. This is not necessarily recommended because although this will keep your network invisible to the common nosy neighbor, it will not protect your network from any serious hackers. It can also make setting up your own devices on your wireless network more difficult. So, it's good to know how this works, but always use encryption and don't rely on just disabling SSID broadcasts to keep your network secure.

#### **5. Install Who's On My Wifi**

Download and Install Who Is On My Wifi Software onto a desktop computer that is always on at your home or office. Who's On My Wifi acts as a detection engine by scanning your network every few minutes to see if anyone has gotten onto your network. People could get in by breaking WEP encryption, faking through a MAC Filter, somehow breaking WPA2, or by good old fashioned hard line plugging into your router directly instead of connecting through the wireless. Monitoring for intruders is the final step in securing a Wireless Network.

Who Is On My Wifi is available for download at <http://www.whoisonmywifi.com>

The original article can be found at  
[http://www.whoisonmywifi.com/How\\_To\\_Make\\_A\\_Wireless\\_Network\\_Secure.pdf](http://www.whoisonmywifi.com/How_To_Make_A_Wireless_Network_Secure.pdf)