



# Wireless Security Tips

1. **Change the default password.** Default passwords for wireless equipment are usually set by the manufacturer. Once a hacker figures out what kind of access point you are using, they can easily figure out the default password.

2. **Turn on Encryption.** Use WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) to encrypt information on your wireless network. Encrypting the data will prevent unauthorized users from viewing it.

3. **Change the default SSID.** When changing the SSID, remember to use something that is nondescript. Never use anything that can be easily identified... i.e. your name or address.

4. **Disable SSID broadcast.** Access points ship with SSID broadcast enabled. With broadcast enabled, you announce to the world that you have a wireless network. By disabling the SSID broadcast, you make your wireless network harder to find. (If they don't know it's there, they won't spend time trying to get in.)

5. **Enable MAC address filtering.** By using MAC address filtering, you can limit connections to your wireless access point. If someone tries to connect to your AP and their MAC address isn't in the table, they will be denied access.

6. **Limit your wireless signal.** Many access points let you adjust the signal strength. Ideally you should place your AP in the center of the area you want covered and then adjust the signal to cover the smallest possible range.

7. **Limit the number of user addresses or disable DHCP completely.** If you disable DHCP, unauthorized users would have to figure out what your IP addressing scheme is to be able to access your network. If disabling DHCP is not an option, at least limit the number of addresses that can be assigned.

8. **Turn off your wireless network during extended periods of non-use.**