

# Tips for Wireless Security

If you have more than one computer or mobile device in your home, chances are you have or are going to set up a wireless network. Just as you secure your home by locking your doors, there are steps you can take to protect your wireless network. The tips below will help to ensure that your network is not the neighborhood hotspot.

## 1. Change SSID Name

Change the default Service Set Identifier (SSID) name, which is the name of your wireless LAN. Hackers know the default names of the different brands of equipment and using the default name suggests that the network has not been secured. You may wish to use a name that will not be associated with you to avoid being specifically targeted.

## 2. Disable SSID Broadcast

Disabling the SSID Broadcast prevents others in your neighborhood from finding your wireless LAN and gaining unauthorized access.

## 3. Control Access Point Coverage

Radio signals used to broadcast your wireless network are visible to others who may be trying to use your network. Any wireless signal that spills outside of the desired area could provide an opportunity for a hacker to access the network without entering the premises. Directional antennas should be used, if possible, at the perimeter directing their broadcasting inward.

## 4. Turn On Encryption

The signal from your wireless network is broadcast throughout your surrounding area. By encrypting the data, only the intended recipient device is able to access it.

## 5. Change the Default Password

Change the default password needed to access your wireless device. By changing the password you can prevent hackers from accessing and changing your network settings.

## 6. Enable MAC Filtering

Enabling MAC Filtering allows you to prevent or permit specific PCs to access your wireless network.

## 7. Disable File and Print Sharing on Your PC

Disable File and Print Sharing if you don't need it. This can limit a hacker's ability to steal data or commandeer resources in the event that they get past the encryption.

*Following these suggestions should reduce the likelihood of security problems but does not guarantee that you will never experience such problems*