# Protecting Your Wireless Network

## Benefits and Risks of a Wireless Network

Many consumers and small businesses use wireless (Wi-Fi) networks to enable their laptops and other wireless devices to access the Internet. Wi-Fi networks generally include a wireless "router" connected to a broadband Internet service via a modem that is attached to the cable or telephone network. Sometimes the wireless router and the modem are integrated into one device.

While Wi-Fi networks provide many benefits, an unprotected network can result in unauthorized use and potential harm unless certain steps are taken. In some cases, unauthorized users may be able to access your private information, view the content of transmissions, download unlawful content using your network or infect computers with viruses or spyware. Unauthorized users may also cause harm beyond your computer or network, such as sending spam, spyware or viruses to others, and the activity can be traced back to your network.

## How to Secure a Wireless Network

The following tips can help secure a Wi-Fi network against unauthorized access. Consult the owner's manual that came with your wireless router for specific instructions on performing the following steps. Manuals are often available on the manufacturer's website. At the bottom of this page you will find links to product manuals from some of the most popular manufacturers, and links to how-to videos produced by the Federal Trade Commission.

### 1. Turn Encryption On

Turning on your wireless router's encryption setting can go a long way toward securing your network. Wireless routers often come out of the box with the encryption feature disabled, so be sure to check that encryption is turned on shortly after you or your broadband provider installs the router. Note that there are different types of encryption. "WPA2" currently is the most effective standard. Another common standard, "WEP", is less secure, and therefore is not recommended. To turn on encryption, you will need to pick a wireless network password. Longer passwords that utilize a combination of letters, numbers and symbols are more secure.

### 2. Turn the Firewall On

A "firewall" is designed to protect computers from harmful intrusions and can be hardware-based or software-based. Wireless routers generally contain built-in firewalls, but are sometimes shipped with the firewall turned off. Be sure to check that the wireless router's firewall is turned on.

### 3. Change Default Passwords

Most wireless routers come with preset passwords for administering the devices settings (this is different from the password used to access the wireless network itself). Unauthorized users may be familiar with the default passwords, so it is important to change the router device's password as soon as it is installed. Again, longer passwords made up of a combination of letters, numbers and symbols are more secure.

### 4. Change the Default Name of the Network

A network's name is known as its "SSID" (service set identifier). When a computer with a wireless connection searches for and displays the wireless networks nearby, it lists each network that publicly broadcasts its SSID. Manufacturers usually give all of their wireless routers a default SSID, which is often the company's name. It is a good practice to change your network's SSID, but to protect your privacy do not use personal information such as the names of family members.

### 5. Turn Network Name Broadcasting Off

Wireless routers may broadcast the name of the network (the "SSID") to the general public. This feature is often useful for businesses, libraries, hotels and restaurants that want to offer wireless Internet access to customers, but it is usually unnecessary for a private wireless network. It is recommended that owners of home Wi-Fi networks turn this feature off.

### 6. Use the MAC Address Filter

Every device that can connect to a Wi-Fi network has a unique ID called the "physical address" or "MAC" (Media Access Control) address. Wireless routers can screen the MAC addresses of all devices that connect to them, and users can set their wireless network to accept connections only from devices with MAC addresses that the router is set to recognize. In order to create another obstacle to unauthorized access, change your router's settings to activate its MAC address filter to include only your devices.

### Additional Wi-Fi Safety Tips

- Turn off your Wi-Fi network when it will not be in use for extended periods of time;
- Use anti-virus and anti-spyware software on the computers that access your wireless network;
- Don't assume that public wireless networks are secure.

## Links to Additional Wi-Fi Security Resources

The FCC and Federal Trade Commission have collaborated on an instructional video[1] narrated by FCC staffer Yul Kwon that highlights the tips above. Feel free to screen this video to others.

The Federal Trade Commission's OnGuard Online website has detailed video tutorials[2] on how to adjust the security settings of wireless routers from particular manufacturers.

Operation manuals for many wireless routers may be found at the manufacturers' websites. Here are links for several manufacturers:

| | |
|---|---|
| Apple Airport: | support.apple.com/manuals/#airport |
| Belkin: | en-us-support.belkin.com/app/product/list/q/routers/ |
| Buffalo Inc.: | www.buffalotech.com/support/ |
| D-Link: | www.dlink.com/support/ |
| Linksys: | homesupport.cisco.com/en-us/wireless/linksys |
| Motorola: | broadband.motorola.com/consumers/support/ |
| NETGEAR: | kb.netgear.com/app/ |

For more information and online safety tips, please visit www.fcc.gov/consumers.

[1] www.onguardonline.gov/videos/wireless-secuirty-yul-kwon.aspx
[2] www.onguardonline.gov/tools/watch-tutorial.aspx#WS