ONLINE

ftc.gov
For The Consumer

Federal Trade Commission
1-877-FTC-HELP

FTC FACTS for Consumers

Securing Your Wireless Network

Increasingly, computer users interested in convenience and mobility are accessing the Internet wirelessly. Today, business travelers use wireless laptops to stay in touch with the home office; vacationers beam snapshots to friends while still on holiday; and shoppers place orders from the comfort of their couches. A wireless network can connect computers in different parts of your home or business without a tangle of cords and enable you to work on a laptop anywhere within the network's range.

Going wireless generally requires a broadband Internet connection into your home, called an "access point," like a cable or DSL line that runs into a modem. To set up the wireless network, you connect the access point to a wireless router that broadcasts a signal through the air, sometimes as far as several hundred feet. Any computer within range that's equipped with a wireless client card can pull the signal from the air and gain access to the Internet.

The downside of a wireless network is that, unless you take certain precautions, anyone with a wireless-ready computer can use your network. That means your neighbors, or even hackers lurking nearby, could "piggyback" on your network, or even access the information on your computer. And if an unauthorized person uses your network to commit a crime or send spam, the activity can be traced back to your account.

Fortunately, there are steps you can take to protect your wireless network and the computers on it.

Precautionary Steps

1. **Use encryption.** The most effective way to secure your wireless network from intruders is to encrypt, or scramble, communications over the network. Most wireless routers, access points, and base stations have a built-in encryption mechanism. If your wireless router doesn't have an encryption feature, consider getting one that does.

   Manufacturers often deliver wireless routers with the encryption feature turned off. You must turn it on. The directions that come with your wireless router should explain how to do that. If they don't, check the router manufacturer's website.

   Two main types of encryption are available: Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). Your computer, router, and other equipment must use the same encryption. WPA is stronger; use it if you have a choice. It should protect you against most hackers.

   Some older routers use only WEP encryption, which is better than no encryption. It should protect your wireless network against accidental intrusions by neighbors or attacks by less-sophisticated hackers. If you use WEP encryption, set it to the highest security level available.

2. **Use anti-virus and anti-spyware software, and a firewall.** Computers on a wireless network need the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the "off" mode, turn it on.

3. **Turn off identifier broadcasting.** Most wireless routers have a mechanism called identifier broadcasting. It sends out a signal to any device in the vicinity announcing its presence. You don't need to broadcast this information if the person using the network already knows it is there. Hackers can use identifier broadcasting to home in on vulnerable wireless networks. Disable the identifier broadcasting mechanism if your wireless router allows it.

4. **Change the identifier on your router from the default.** The identifier for your router is likely to be a standard, default ID assigned by the manufacturer to all hardware of that model. Even if your router is not broadcasting its identifier to the world, hackers know the default IDs and can use them to try to access your network. Change your identifier to something only you know, and remember to configure the same unique ID into your wireless router and your computer so they can communicate. Use a password that's at least 10 characters long: The longer your password, the harder it is for hackers to break.

5. **Change your router's pre-set password for administration.** The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router. Hackers know these default passwords, so change it to something only you know. The longer the password, the tougher it is to crack.

6. **Allow only specific computers to access your wireless network.** Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses access to the network. Some hackers have mimicked MAC addresses, so don't rely on this step alone.

7. **Turn off your wireless network when you know you won't use it.** Hackers cannot access a wireless router when it is shut down. If you turn the router off when you're not using it, you limit the amount of time that it is susceptible to a hack.

8. **Don't assume that public "hot spots" are secure.** Many cafés, hotels, airports, and other public establishments offer wireless networks for their customers' use. These "hot spots" are convenient, but they may not be secure. Ask the proprietor what security measures are in place.

   Be careful about the information you access or send from a public wireless network. To be on the safe side, you may want to assume that other people can access any information you see or send over a public wireless network. Unless you can verify that a hot spot has effective security measures in place, it may be best to avoid sending or receiving sensitive information over that network.

GLOSSARY

Encryption: The scrambling of data into a secret code that can be read only by software set to decode the information.

Extended Service Set Identifier (ESSID): The name a manufacturer assigns to a router. It may be a standard, default name assigned by the manufacturer to all hardware of that model. Users can improve security by changing to a unique name. Similar to a Service Set Identifier (SSID).

Firewall: Hardware or software designed to keep hackers from using your computer to send personal information without your permission. Firewalls watch for outside attempts to access your system and block communications to and from sources you don't permit.

Media Access Control (MAC) Address: A unique number that the manufacturer assigns to each computer or other device in a network.

Router: A device that connects two or more networks. A router finds the best path for forwarding information across the networks.

Wired Equivalent Privacy (WEP): A security protocol that encrypts data sent to and from wireless devices within a network. Not as strong as WPA encryption.

Wi-Fi Protected Access (WPA): A security protocol developed to fix flaws in WEP. Encrypts data sent to and from wireless devices within a network.

Wireless Network: A method of connecting a computer to other computers or to the Internet without linking them by cables.

Facts for Consumers

The Federal Trade Commission (FTC) works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER

Federal Trade Commission
Bureau of Consumer Protection
Office of Consumer and Business Education

March 2006