Use Encryption on Your Wireless Network

Once you go wireless, you should encrypt the information you send over your wireless network, so that nearby attackers can't eavesdrop on these communications. Encryption scrambles the information you send into a code so that it's not accessible to others. Using encryption is the most effective way to secure your network from intruders.

Two main types of encryption are available for this purpose: Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). Your computer, router, and other equipment must use the same encryption. WPA2 is strongest; use it if you have a choice. It should protect you against most hackers. Some older routers use only WEP encryption, which likely won't protect you from some common hacking programs. Consider buying a new router with WPA2 capability.

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

Understanding How a Wireless Network Works

Going wireless generally requires connecting an internet "access point" – like a cable or DSL modem – to a wireless router, which sends a signal through the air, sometimes as far as several hundred feet. Any device within range can pull the signal from the air and access the internet.

Unless you take certain precautions, anyone nearby can use your network. That means your neighbors – or any hacker nearby – could "piggyback" on your network or access information on your device. If an unauthorized person uses your network to commit crime or send spam, the activity could be traced back to your account.

Limit Access to Your Network

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

SECURING YOUR WIRELESS NETWORK

* Source: Federal Trade Commission

Secure Your Router

It's also important to protect your network from attacks over the internet by keeping your router secure. Your router directs traffic between your local network and the internet. So, it's your first line of defense for guarding against such attacks. If you don't take steps to secure your router, strangers could gain access to sensitive personal or financial information on your device. Strangers also could seize control of your router, to direct you to fraudulent websites.

Change the name of your router from the default. The name of your router (often called the service set identifier or SSID) is likely to be a standard, default ID assigned by the manufacturer. Change the name to something unique that only you know.

Change your router's pre-set password(s). The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router, as its "administrator." Hackers know these default passwords, so change it to something only you know. The same goes for any default "user" passwords. Use long and complex passwords – think at least 12 characters, with a mix of numbers, symbols, and upper and lower case letters. Visit the company's website to learn how to change the password.

Turn off any "Remote Management" features. Some routers offer an option to allow remote access to your router's controls, such as to enable the manufacturer to provide technical support. Never leave this feature enabled. Hackers can use them to get into your home network.

Log out as Administrator: Once you've set up your router, log out as administrator, to lessen the risk that someone can piggyback on your session to gain control of your device.

Keep your router up-to-date: To be secure and effective, the software that comes with your router needs occasional updates. Before you set up a new router and periodically thereafter, visit the manufacturer's website to see if there's a new version of the software available for download. To make sure you hear about the latest version, register your router with the manufacturer and sign up to get updates.

And when you secure your router, don't forget to secure your computer too. Use the same basic computer security practices that you would for any computer connected to the internet. For example, use protections like antivirus, antispyware, and a firewall -- and keep these protections up-to-date.

Protect Your Network during Mobile Access

Apps now allow you to access your home network from a mobile device. Before you do, be sure that some security features are in place.

Use a strong password on any app that accesses your network. Log out of the app when you're not using it. That way, no one else can access the app if your phone is lost or stolen.

Password protect your phone or other mobile device. Even if your app has a strong password, it's best to protect your device with one, too.