

Securing Your Wireless Network

If you don't secure your wireless network, strangers could use it and gain access to your computer – including the personal and financial information you've stored on it. Protect your computer by using WPA encryption.

Understand 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 computer within range with a wireless card can pull the signal from the air and access the internet.

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

Use Encryption

Encryption scrambles the information you send over the internet 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: 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 may not 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.

Tutorials for Turning Your Router's Encryption On:

- [Linksys \(/media/video-video-0016-linksyst-wireless-network-set-wpa-password\)](/media/video-video-0016-linksyst-wireless-network-set-wpa-password)
- [NETGEAR \(/media/video-video-0017-netgear-wireless-network-set-wpa-password\)](/media/video-video-0017-netgear-wireless-network-set-wpa-password)
- [Apple Airport \(/media/video-video-0018-apple-airport-wireless-network-set-wpa-password\)](/media/video-video-0018-apple-airport-wireless-network-set-wpa-password)

Secure Your Computer and Router

Use anti-virus and anti-spyware software, and a firewall. Use the same [basic computer security practices \(/articles/0009-computer-security\)](/articles/0009-computer-security) that you would for any computer connected to the internet.

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. 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. Use passwords that are at least 10 characters long: the longer the password, the tougher it is to crack.

Visit the company's website to learn how to change the password.

Tutorials for Changing the Default Password for Your Router:

- [Linksys \(/media/video-video-0013-linksys-router-change-default-admin-password\)](#)
- [NETGEAR \(/media/video-video-0014-netgear-router-change-default-admin-password\)](#)
- [Apple Airport \(/media/video-video-0015-apple-airport-change-default-admin-password\)](#)

Limit Access to Your Network

Allow only specific computers to access your wireless network. Every computer 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.

Tutorials for Limiting Access to Your Wireless Network:

- [Linksys \(/media/video-video-0019-linksys-wireless-network-restrict-access-mac-address\)](#)
- [NETGEAR \(/media/video-video-0020-netgear-wireless-network-restrict-access-mac-address\)](#)
- [Apple Airport \(/media/video-video-0021-apple-airport-wireless-network-restrict-access-mac-address\)](#)

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.

Don't Assume That Public Wi-Fi Networks Are Secure

Be cautious about the information you access or send from a public wireless network. Many cafés, hotels, airports, and other public places offer wireless networks for their customers to use. These "hot spots" are convenient, but they may not be secure. To learn more, check out these [tips for using public Wi-Fi \(/articles/0014-tips-using-public-wi-fi-networks\)](#).

September 2011

You Might Also Like

- [Laptop Security \(http://onguardonline.gov/articles/0015-laptop-security\)](http://onguardonline.gov/articles/0015-laptop-security)
- [Understanding Mobile Apps \(http://onguardonline.gov/articles/0018-understanding-mobile-apps\)](http://onguardonline.gov/articles/0018-understanding-mobile-apps)

