# Securing Wireless Networks

**How do wireless networks work?** As the name suggests, wireless networks, sometimes called Wi-Fi, allow you to connect to the internet without relying on wires. If your home, office, airport, or even local coffee shop has a wireless connection, you can access the network from anywhere that is within that wireless area.

Wireless networks rely on radio waves rather than wires to connect computers to the internet. A transmitter, known as a wireless access point or gateway, is wired into an internet connection. This provides a "hotspot" that transmits the connectivity over radio waves. Hotspots have identifying information, including an item called an SSID (service set identifier), that allow computers to locate them. Computers that have a wireless card and have permission to access the wireless frequency can take advantage of the network connection. Some computers may automatically identify open wireless networks in a given area, while others may require that you locate and manually enter information such as the SSID.

**What security threats are associated with wireless networks?** Because wireless networks do not require a wire between a computer and the internet connection, it is possible for attackers who are within range to hijack or intercept an unprotected connection. A practice known as war-driving involves individuals equipped with a computer, a wireless card, and a GPS device driving through areas in search of wireless networks and identifying the specific coordinates of a network location. This information is then usually posted online. Some individuals who participate in or take advantage of war-driving have malicious intent and could use this information to hijack your home wireless network or intercept the connection between your computer and a particular hotspot.

**What can you do to minimize the risks to your wireless network?**

- **Change default passwords** - Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily found online, so they don't provide any protection. Changing default passwords makes it harder for attackers to take control of the.

- **Restrict access** - Only allow authorized users to access your network. Each piece of hardware connected to a network has a MAC (media access control) address. You can restrict or allow access to your network by filtering MAC addresses. Consult your user documentation to get specific information about enabling these features. There are also several technologies available that require wireless users to authenticate before accessing the network.

- **Encrypt the data on your network** - WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) both encrypt information on wireless devices. However, WEP has a number of security issues that make it less effective than WPA, so you should specifically look for gear that supports encryption via WPA. Encrypting the data would prevent anyone who might be able to access your network from viewing your data.

- **Protect your SSID** - To avoid outsiders easily accessing your network, avoid publicizing your SSID. Consult your user documentation to see if you can change the default SSID to make it more difficult to guess.

- **Install a firewall** - While it is a good security practice to install a firewall on your network, you should also install a firewall directly on your wireless devices (a host-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your.

- **Maintain anti-virus software** - You can reduce the damage attackers may be able to inflict on your network and wireless computer by installing anti-virus software and keeping your virus definitions up to date. Many of these programs also have additional features that may protect against or detect spyware and Trojan horses.