WiFi Hotspots

Wireless or "WiFi" Internet hotspots provide convenience and flexibility for Internet users. As WiFi hotspots and notebook computers have become prevalent, it's easy to work where you want, when you want. As with all technologies, WiFi hotspots come with risks. If you follow the appropriate precautions, you can take advantage of all the benefits of WiFi, while limiting your exposure to danger.

Public Wireless Hot Spots

The most convenient wireless services -- free hotspots offered by coffee shops, schools, libraries, etc. -- carry the greatest risks. Many hotspots are completely open, or protected by a common password that you get for the price of a cup of coffee. Clever scammers using the network can intercept messages as you send and receive information. If you're connecting to email or e-commerce sites, you may be transmitting passwords that can be snatched out of the ether by a nearby crook.

If you're going to use a public WiFi hotspot, make sure your security tools (anti-virus, anti-spyware and particularly firewall are up-to-date and active. Most firewalls can be used to secure your wireless connections, but you have to check the settings. You may want to avoid conducting sensitive transactions over public wireless networks.

Setting Up Your Own Wireless Network

One of the best ways to take advantage of wireless access, while maintaining strong security is to set up your own WiFi hot spot using your high-speed Internet connection. Many ISPs offer wireless routers as an add-on, and you can buy wireless routers that are easy to set up. Once you set up your network, you can restrict access by requiring a password key and increase your protection level further by:

- Change your default passwords. Many wireless devices come pre-configured with simple administrator passwords to help in setup. Change your password to something unique and hard-to-guess.
- Encrypt the data on your network. US-CERT has more information on how to encrypt your data.
- Make sure your firewall is running. Your firewall is your first line of defense against wireless and wired intrusions. Check the firewall section and make sure your software and settings are up-to-date.