FOR MORE INFORMATION

Multi-State Information Sharing and Analysis Center Cyber Security Tips Newsletter
http://www.msisac.org/awareness/news/2008-02.cfm

US-CERT:
http://www.us-cert.gov/cas/tips/ST05-003.html

Digital Inspiration Blog:
http://www.labnol.org/internet/secure-your-wireless-wifi-network/10549/

PCWorld:
http://www.pcworld.com/article/130330/how_to_secure_your_wireless_network.html

CYBER SECURITY IS OUR SHARED RESPONSIBILITY

State of Alabama
Information Services Division
www.cybersecurity.alabama.gov

Multi-State Information Sharing and Analysis Center
www.msisac.org
info@msisac.org

Securing A Wireless Network

State of Alabama
Office of the Chief Information Security Officer
www.cybersecurity.alabama.gov

Brought to you in partnership with the Multi-State Information Sharing and Analysis Center

Securing a Wireless Network

WIRELESS NETWORKS

The use of notebook computers and wireless mobile devices continues to grow as these devices become more affordable and incorporate enhanced functionality. As a result, wireless networks, also known as WiFi networks, use radio waves instead of cables to connect to the Internet . Because they are not hooked to the network by a cable, notebook computers can be used anywhere. WiFi networks comprise two components to a WiFi network: a Wireless Access Point (WAP), also known as a wireless router; and a computer with a wireless network adaptor.

The WAP is the foundation for building a wireless network. It is a small radio transmitter and receiver.

A wireless network adaptor is required for each computer you intend to connect to a WiFi network. When purchasing WiFi networking hardware from vendors, be sure to obtain guarantees that the hardware conforms to defined wireless standards and will work with your existing WiFi equipment. The wireless network adaptor is usually built into notebook computers and other mobile devices, while it is an add-on component inserted into a USB port on desktop computers.

PROBLEMS WITH WIRELESS NETWORKS

The convenience of WiFi networks is also its greatest security liability. People can wander around with a laptop looking for nearby wireless networks. This is called wardriving. Once your wireless network is discovered, predators can access your network and data from outside your residence. Since physical access to the network is not required, the likelihood of being detected is decreased, therefore providing more time to hack into and use your network.

Some hackers get into home wireless networks looking for personal information so they can steal your identity and gain access to your bank accounts, credit cards, and other financial assets or worse, to conduct illegal activity such as accessing child pornography. Others look to gain control of your computers to use them for malicious purposes, such as sending SPAM, spreading malware or attacking other computers.

Even if these hackers only want to use your network to connect to the Internet, it can have a detrimental effect. They may use large amounts of your connection bandwidth, slowing down your network, or, if their computers are infected by malware, spreading it to your computers.

STEPS TO SECURE YOUR WIRELESS NETWORKS

There are several steps you can take to help secure your WiFi network. Most wireless access points (WAPs) default to an unprotected state. By following these steps you can prevent all but the most determined hackers from getting in.

- Change the default password on your WAP. The default password for each vendor is generally well known and readily available. Replace it with a strong password using a combination of upper and lower case letters, numbers and special characters. Choose a password or passphrase that is easy for you to remember but hard for someone else to guess.

- Consider turning off SSID broadcasting. Your SSID is the name of your wireless network. Hackers need to know this, in addition to the password, in order to get onto your network. By default, wireless networks advertise their presence by sending out a signal with the SSID to all nearby wireless network adaptors. By turning off SSID broadcasting, it makes it harder for people to know there is a wireless network nearby.

- Activate built-in encryption. Encryption scrambles the data being transmitted over the network. This reduces the risk of someone successfully eavesdropping or monitoring your communications. Use the strongest technique available to all of the computers on the network and the WAP. WPA2 is the strongest encryption method available. The next strongest would be WPA. The oldest method is WEP. Both WPA and WEP have known weaknesses, however using one of these methods is far better than not encrypting your network. If your devices only support WEP or WPA, check for firmware updates to add WPA2 support. Many vendors offer them.

- Use MAC filtering on your network. A MAC address is a hard-coded address that is unique to every network adaptor. By specifying which MAC addresses are allowed on the network, you can exclude other device. Turn the broadcast power down. Some WAPs allow the user to turn the power down on the transmitter. This will cut the range of the wireless network and make it harder to detect the network from outside the house. Turn off the remote administration function on your WAP. Remote administration is not necessary for home networks. By shutting this function off, physical access is required.

- Enable a firewall on all computers as well as on the WAP. This is a good practice on any network, not just wireless networks.

- Install anti-malware software, on your computers and keep them up to date. These will help prevent your network from being easily infected.