How to Secure Your Home Wireless Network

Since your neighbors, or anyone else within range, can potentially connect to your wireless access points, you should take extra security precautions when setting up your home wireless network.

The methods listed below vary in their overall effectiveness, but remember that a hacker will probably try to find the path of least resistance with regard to breaking in to your network. The more of these measures that you take, the greater the chance that someone will simply move on and attempt to locate a less secure network.

Choose a strong administrator password

Most routers require an administrator password to access the setup and configuration settings. However, the default passwords for these routers are generally weak, and some have none to all.

Disable remote administration

Unless you require remote administration and are familiar with WLAN administration and security, disable this feature. Otherwise, anyone connected to the Internet could conceivably gain administrative access to your router and your network.

Encryption

Enable or set an encryption password. All Wi-Fi equipment supports a form of encryption; you should choose the most secure type that works across all the devices that you need to connect.

If possible, use WPA2/WPA (Wi-Fi Protection Access) rather than WEP (Wired Equivalency Privacy).

Change you default SSID

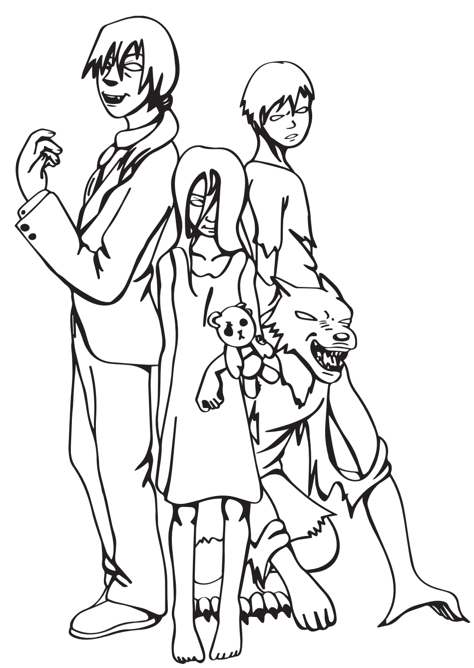
Your SSID (Service Set Identifier) is the name of your network. Most commercial products have a default name (e.g., Linksys routers are usually set to "linksys"). Change this default name, and choose a unique, robust name, prefereably a longer one with letters and numbers. Your new SSID should not contain personal or sensitive information such as your name or address.

Also don't broadcast your SSID. This requires that you manually add a wireless network on your computer, but it prevents people from finding your network easily.

MAC address filtering

MAC addresses are unique to each network adapter, whether wired or wireless Most wireless routers offer some sort of MAC address filtering, which limits access to your wireless network to specifically allowed devices.

Use MAC address filtering if possible. A knowledgeable hacker can easily spoof or fake a MAC address, so you should not rely on filtering alone. Even so, MAC filtering does add a valuable layer of protection against unauthorized access to your network.



National Cyber Security Awareness Month

http://keepitsafe.auburn.edu