

Wireless Internet Security:

With an increase in the use of wireless Internet technology, security professionals recommend that you take a moment to review your home's wireless security. When you have an insecure wireless network, people many houses away from your home might be able to connect to your system and the Internet. Anyone connecting to your system could have access to your computers and access any passwords, financial or other personal information you have stored. While connected to your system, a person could also commit a crime and because you own the Internet connection, it could lead police back to you. For all these reasons, it is important to keep your wireless network secure.

Below are some tips for keeping your wireless network as secure as possible.

Wireless Network Security Tips

- **Install a firewall.** A firewall can help protect your computer in two ways. First, it can prevent unauthorized users from accessing your computer through the Internet or another network. It can also act as a barrier that checks data coming from outside your network and then blocks the data or allows it to pass through to your computer.
- **Change the administrative password on your wireless routers.** Wireless devices are shipped with default passwords for easy setup and access, but these passwords are easy to find on the vendor support sites and should be replaced with a strong secure password when you complete your installation.
- **Change the default SSID name and turn off SSID broadcasting.** The SSID is the public name of your wireless network. You should turn the SSID broadcasting feature off. This feature is set up to make it easier for any casual user whose is configured to connect to any available SSID broadcast it finds. Entering the SSID manually takes only a moment and will make it more difficult for any nearby user to log onto your network. You should also change the SSID name from the default name that is set up by the vendor, as these are just as easy to discover as the default passwords.
- **Disable DHCP.** For a small network with only a few nodes, consider disabling DHCP (Dynamic Host Configuration Protocol) on your router and assigning IP addresses to your computers manually. On newer wireless routers, you can even restrict access to the router to specified MAC addresses.
- **Replace WEP with WPA.** WPA is a stronger encryption standard than WEP and will provide stronger protections for your network.
- **Position the wireless access point safely.** Wireless signals normally reach to the exterior of a home. A small amount of "leakage" outside of the premises is not a major problem, but the further this signal reaches, the easier it is for others to detect and exploit. Wireless signals can often reach across streets and through neighboring homes. When installing a wireless home network, the position of the

access point determines its reach. Try to position these devices near the center of the home rather than near windows to minimize this leakage.

- **Turn Off the Network During Extended Periods of Non-Use.** The ultimate in security measures, shutting down the network will certainly prevent outside hackers from breaking in! While impractical to turn the devices off and on frequently, at least consider doing so during travel or extended periods offline.
- **Keep your operating system patched and updated with the latest releases.**