WIRELESS SECURITY TIPS

This information is provided by Cascade Networks Inc. as a recommendation for our customers' protection of their personal networks. Any further advice should be sought from an Information Technology Consultant, or Computer Technician. Please remember that Cascade Networks Inc. only provides a static IP address for your wireless device (if needed) and does not provide tech support for them. Most routers function normally in DHCP. We recommend you do not run the set up disk that came with the device. Please connect your router to one of the ports on our equipment, and at least set the Admin Password and WPA encryption by logging in through the default gateway (consult owner's manual for this). Cascade Networks Inc. is only your High Speed Internet provider; all other equipment is considered part of your personal network.

1. **Change Default Administrator Passwords**

At the core of most Wi-Fi home networks is an access point or router. To set up these pieces of equipment, manufacturers provide Web pages that allow owners to enter their network address and account information. These Web tools are protected with a login screen (username and password) so that only the rightful owner can do this. However, for any given piece of equipment, the logins provided are simple and very well-known to hackers on the Internet. Change these settings immediately. Remember to use a good password naming convention such as using a variety of upper case and lower case letters, symbols, and numbers. You are welcome to share your password with us, so that we can keep it in our database for you in case you lose it.

2. **Turn on (Compatible) WPA / WEP Encryption**

All Wi-Fi equipment supports some form of "encryption." Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by humans. Several encryption technologies exist for Wi-Fi today. Naturally you will want to pick the strongest form of encryption that works with your wireless network. To function, though, all Wi-Fi devices on your LAN must share the identical encryption settings. Therefore you may need to find a "lowest common denominator" setting. Some Windows XP users may need to do an update for WPA to work.

3. **Change the Default SSID**

Access points and routers all use a network name called the SSID. Manufacturers normally ship their products with the same SSID set. For example, the SSID for Linksys devices is normally "linksys." While it is true that the SSID does not by itself allow anyone to break into your network, changing the default makes it more secure. Change the default SSID when configuring your LAN.

4. **Position the Router or Access Point Safely**

Wi-Fi signals normally spread throughout the interior of a home. A small amount of "leakage" outdoors is not a problem, but the further this signal reaches, the easier it is for others to detect and exploit your system. When installing a wireless home network, the position of the access point or router determines its reach. Try to position these devices near the center of the home rather than near windows to minimize leakage.

If you have further questions, please contact the manufacturer of your router.