

Special Report:

## Computer Security

### Wireless Security at a Glance:



#### 1. Wireless Security Issues

Many of us over look the security risk when setting up our wireless internet connection, we just want to get connected. Configuring the security features can also be a slow and non-intuitive process. Below are several steps you may perform to achieve greater security.

##### ***a) Change default Administrator Password and Username***

At the heart of most wireless networks is an “access point” or “router”. Typically to configure these devices the manufacture supplies a web interface (a webpage to setup network addresses and other tools). This menu is protected by a login screen so that only the rightful owner can gain access. However, right out of the box the default logins provided are simple and are well-known to the hacker. **CHANGE these settings IMMEDIATELY !!**

##### ***b) Turn on WPA - WEP Encryption***

All wireless equipment offers some form of “encryption”. Encryption technology applied, simply scrambles messages sent over the wireless network so they cannot easily be read. Naturally you want to pick the strongest form of encryption to work with your wireless network. To successfully apply the encryption you must share the identical encryption setting across all your wireless devices on your network.

##### ***c) Disable SSID Broadcast***

The Wi-Fi “access point” or “router” will typically broadcast the network name (SSID) over the air at regular cycles. This feature was designed for so called “Hot Spots “and businesses. In the home this is not needed and it would be in a sense advertising and possibly inviting an unwelcome neighbor or hacker into your Wi-Fi network. I believe most current equipment will allow you to turn the SSID broadcast feature off.

##### ***d) Enable MAC Address Filtering***

Each Wi-Fi device has a unique identifier called the “ MAC address or physical address”. Routers and Access Points keep track of all the devices that are attached to them thru these addresses. Many of these Routers and Access Points offer the owner the ability to configure the MAC addresses of their own network equipment in to these Routers thus allowing only their equipment to function across network. However, be aware some equipment also offer the option to fake the MAC address easily.

**Protective Countermeasures & Consulting:**

[www.ProtectiveCountermeasures.com](http://www.ProtectiveCountermeasures.com)

308 Main Street New Rochelle, NY 914-576-8706

page 2 of 2

*Special Report:*

## **Computer Security**

### **Wireless Security at a Glance:**



#### ***e) Assign Static IP Addresses to Devices***

It is my experience that most home networks use dynamic IP addressing. DHCP technology is an easy way to setup IP addressing across your network. Unfortunately, this convenience also can work to the advantage of an unauthorized person connecting into your network by easily obtaining a valid IP address from the DHCP address pool. Turn off DHCP on the "Router" or "Access Point", set a fixed or static IP into each networked device. Be sure to use a valid private IP address as to not inadvertently be able to be reached directly from the Internet.

#### ***f) Change the default SSID***

Wi-Fi Routers and Access Points all use a network name (SSID). Equipment manufactures typically sell their product with the same network name. An example would be Linksys would normally use "linksys" as the network name(SSID) on the device. Someone wanting to gain access, sees the default SSID could assume that the network is poorly configured.