Home Wireless Safety Checklist

Consumer Task Force

The following six steps are recommended for owners of wireless networks in order to provide protection from hackers and malicious programs such as viruses and spyware. Consult the owner's manual that came with your wireless router or the manufacturer's website for specific instructions on performing the following steps. More information on this and other online safety topics is available at **www.fcc.gov/encyclopedia/consumer-publications-library.**

1. Turn On Encryption ☐

WPA2 is currently the strongest home encryption available. Because it is less secure, WEP is not recommended.

2. Turn On the Router's Firewall ☐

Wireless routers are sometimes shipped with the firewall turned off. Ensure that yours is turned on.

3. Change the Router's Preset Password ☐

To be most secure, your password should include letters, numbers and/or symbols and should be at least 12 characters long.

4. Customize the Network's Name ("SSID") ☐

You should give your network a unique name; however, you should not use personal information, such as family members' names.

5. Turn Off Network Identifier Broadcasting ☐

Broadcasting the network's name ("SSID") is unnecessary with a home network and may invite attempts at unauthorized access.

6. Set Up a MAC Address Filter ☐

This allows you to pre-approve the devices that can access your network.

The OnGuard Online website, www.onguardonline.gov, has video tutorials[1] on adjusting the security settings of wireless routers from several manufacturers.

[1] http://www.onguardonline.gov/tools/watch-tutorial.aspx#WS