Secure your home wireless network

Properly securing your home wireless network is critical to securing your information and your reputation. Don’t be an easy victim. Here are some ideas that help keep your information and home network safe.

1. **Change the default password and logon name for your router.** Most wireless routers come with a default password and logon ID. Since these are well known, it is a common vector of attack. Reference your wireless router manual to change the default password and logon name.
2. **Enable the strongest encryption that your equipment will support.** Wireless traffic which is not appropriately encrypted may be intercepted and disclosed. Configure WPA (Wi-Fi Protected Access) WPA2 or at a minimum WEP.
3. **Disable SSID broadcasting and change the SSID.** The SSID (Service Set Identifier) is effectively the name of the network and usually set to a default value. The default values for the various network routers are easily available on the internet. Change the SSID to a name that is difficult to guess. The wireless router will broadcast the SSID by default. Anyone within range of the access point will be able to detect your access point. Reference your wireless router manual to disable this feature.
4. **Restrict the devices that can connect to your wireless network.** You can do this by using the MAC (Media Access Control) address filtering capabilities of your wireless router. Every wireless network card has a MAC address. Configure your network to only allow specific MAC addresses to access your network.
5. **Turn off you wireless router when you know you won’t be using it.** If you will not be using your wireless network for an extended period of time than turn it off.