Do's and Don’ts for Wireless networks

1) By default wireless routers have no security enabled at all.

2) Always use WPA (Wi-Fi Protected Access) and not the older WEP (Wired Equivalent privacy).

3) Every computer is uniquely identified by a MAC address or machine address or Media Access Control address. Turn on Access Control by means of which only those machines (desktops or laptops) that have known MAC addresses have access to your wireless network.

4) You configure your router using web pages that come with a user name which you cannot change and a password like admin or password or blank. Change this default password immediately or all your settings will come to naught.

5) Your wireless router has a name which is broadcast to all and sundry at regular intervals. This router name is also called the SSID or Secure Set identifier. Change the default name to something else.

6) Disable the SSID broadcast so that the attacker finds it difficult to locate your wireless router.

7) Every router has a reset switch which is depressed for some time will remove all the settings and set the router back to its insecure state. Protect your router physically so that no one is allowed to reset it.

8) Turn off File and printer sharing so that no one can remotely use your computer or printer.

9) Change the IP address of the client side of the router from the default value.

10) Always use the latest software and hardware. Use 802.11g and not 802.11b.
