Wi-Fi Security and SOPs

Wi-Fi Security -
Internet users are widely using Wi-Fi devices to access Internet. Every year millions of Wi-Fi devices are sold in the market. Out of these most of the wireless devices are vulnerable in their default configuration mode. Since end users are not fully aware of security levels to be set on these devices, these get rendered vulnerable. By taking advantage of these unsecured Wi-Fi devices terrorists and hackers fulfil their needs.

The most common types of Attacks on wireless environment-
Denial of Service Attack.
Man-In-The-Middle Attack in Wi-Fi devices.
Wardriving

Some SOPs (Standard Operating Procedures) for the safe use of WiFi devices-

- Never auto-connect to open Wi-Fi networks in public places.
- All Wi-Fi equipment support some form of encryption. So, enable them.
- Enable MAC address filtering on Wi-Fi devices.
- Avoid dynamic IP address for home Wi-Fi rather use static IP addresses.
- Use encryption technology for sensitive data in wireless networks.
- Always use strong password for encryption.
- Always use the maximum key size supported by access point for encryption.
- Isolate the wireless network from wired network with a firewall and a antivirus supported gateway.
- Restrict access to the Access Point based on MAC address.
- Shutdown the Access Point when not in use.
- Change the default username and Password of the Access Point.
- Do not broadcast your network name.
- Always maintain a updated firmware.
- Use VPN or IPSEC for protecting communication.
- Do not make the SSID information public.
- Disable DHCP service.