



Security Best Practices for Home Wireless Routers (APs)

DOs

Turn off your wireless router (AP) when not in use.

This minimizes the risk of unauthorized users stealing and misusing your Internet connection.

Use WPA or WPA2 security on your wireless router

Use WiFi Protected Access (WPA) or WPA2 to secure WiFi communication between your laptop and home WiFi router. Select WPA-PSK or WPA2-PSK (also often termed as WPA-Personal and WPA2-Personal). Use a strong passphrase that is at least eight characters long and is a mix of alphanumeric and special characters.

Restrict access to your wireless router

- **Use a strong password**

Change the default password of your WiFi router with a stronger password (at least eight characters and a mix of alphanumeric characters). This will prevent unauthorized users from logging into your WiFi router and manipulating its settings.

- **Disable remote administration**

Disabling remote administration ensures that no one can change the settings on your wireless router from the Internet.

- **Disable administration from wireless**

If your router supports this option, disable it. This ensures that the router's internal settings are accessible only if you are connected to it via an Ethernet cable.

Turn on logging on your wireless router

Logging will record activities of your wireless router including WiFi activities of the clients that connect to it. This record can serve as an audit trail in case of a security breach and can be useful for troubleshooting.

DON'Ts

Do not use OPEN security

If you configure your router's security setting to "Open" then wireless communication between your computer and the wireless router is unencrypted. Anyone in the vicinity can sniff your data over the air and steal confidential information such as passwords, credit card numbers, etc. Further, without any authentication and encryption, your wireless router can accept connections from any other computer leaving your network and Internet connection vulnerable to misuse.

Do not use WEP security

Wired Equivalent Privacy (WEP) is an obsolete encryption technique that is flawed. WEP encryption can be broken in minutes using free software available on the Internet. WEP does not provide real security. Use WPA or WPA2 instead.

Do not share passwords

Do not share either the administrator's password or the wireless security key/passphrase with anyone.

MYTHS

MYTH: Disabling SSID broadcast hides your WiFi network from unauthorized users.

Disabling SSID broadcast does not hide your WiFi network. Your SSID can be discovered in minutes by sniffing certain control WiFi packets over the air. Disabling SSID broadcast only gives a false sense of security.

MYTH: Using MAC address based access control list (also known as MAC filtering) prevents unauthorized users from connecting your WiFi router.

Most wireless routers will allow you to specify which computers can connect to it based on the MAC address of the wireless card in the computer. By sniffing the over-the-air packets, a hacker can discover an authorized MAC address, then spoof the MAC address (using free software available on the Internet) and bypass MAC filtering.

MYTH: Reduce the transmit power on your WiFi router or place it so as to reduce signal spillage outside premises.

How far the signal from your WiFi router can be detected does not depend on the transmission power alone. A hacker using a high gain antenna can detect and communicate with your WiFi router from far distances. Reducing transmission power of your WiFi router could in fact cause coverage holes in parts of your home.

MYTH: Turning off DHCP or using static IP addresses is a way to prevent unauthorized connections.

Just like your SSID, a hacker can quickly determine valid IP address range for your network. Turning off the DHCP server in your wireless router or using static IP addresses for your computers provide no security benefit. If you have several machines using WiFi, then it will be cumbersome for you to configure all your machines with appropriate IP addresses.

MYTH: Using cryptic SSID or changing SSID frequently adds to the security of your WiFi network.

SSID is simply the name of your WiFi network. Use an SSID that is simple to remember, but that does not reveal private information about you such as your name, address, employer, occupation, etc. You do not need to change your SSID frequently.