



Security DOs, DON'Ts and MYTHs for Home Wireless Routers (APs)

DOs

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

This ensures that no one can use your internet connection when you are not around. Save power, protect the environment and yourself.

2 Use WPA or WPA2 security on your wireless router

Using WPA (or better – WPA2 if your wireless router supports it) on your wireless link ensures that no one can access your internet connection or snoop into your wireless communication.

3 Restrict access to your wireless router

3.1 Change the administrator's password

Once you change the administrator's password no one can change the settings that you have made to your wireless router.

3.2 Disable remote administration

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

3.3 Disable administration from wireless (if your wireless router supports it)

This ensures that you need to be connected to your wireless router using a network cable for changing the settings.

4 Turn on logging on your wireless router

Turning on logging will record the activities of your wireless router and this information can be very handy if something untoward does happen.

DON'Ts

1 Do not use OPEN security

Open security means that the communication between your computer and the wireless router is not encrypted. With this setting, your wireless router will accept connections from anyone; leaving your network and internet connection vulnerable to misuse. In addition, communication between your computer and the wireless router is open to view by anyone who cares to snoop.

2 Do not use WEP security

WEP is a security mode available on your wireless router (along with WPA and WPA2). This is an obsolete encryption standard which can be cracked by hackers within minutes

3 Do not share passwords

Do not share either the administrator's password or the wireless security key/passphrase with anyone. This includes your internet service provider, neighbors, etc. If you must share it for any purpose; change it immediately afterwards.



MYTHs

1 MYTH: Disable SSID broadcast

Disabling SSID broadcast does not add anything to your security. A hacker can determine your SSID within minutes even if the broadcast is disabled.

FACT: If your computer is setup to connect to you broadcasting disabled AP; you could be at risk when you use it away from your home. More on this in a companion article.

2 MYTH: Use MAC address access control list

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. A hacker can easily determine your valid MAC and use that instead of his own.

FACT: If a hacker uses your MAC instead of his own, it will be very difficult to prove that it was someone else that used your wireless router without your knowledge. More on this in a companion article.

3 MYTH: Trying to prevent signal from leaking outside

While you can take steps to prevent your signal from leaving your home; this can be easily defeated by a hacker by using a high gain antenna.

FACT: Trying to prevent spillage of your signal can cause connectivity problems within your own home.

4 MYTH: Turning off DHCP or using static IP addresses

Just like SSIDs, a hacker can determine valid IP address range for your connection within seconds. Turning off the DHCP server in your wireless router or using static IP addresses for your computers provide no security benefit.

FACT: Turning off DHCP or using static IP addresses will be an annoyance when you try to configure your own computers.

5 MYTH: Using cryptic SSIDs

Using cryptic SSIDs will not even slow down a hacker. This does not add to your security in anyway at all.

FACT: Having a cryptic SSID can be an annoyance when you try to configure your own computers.

For further information please go to:

<http://www.airtightnetworks.com/home/resources/prevent-wifi-attacks.html>

For information related to AirTight Network's solutions for preventing WiFi attacks go to:

<http://www.airtightnetworks.com/home/resources/prevent-wifi-attacks-solutions.html>