

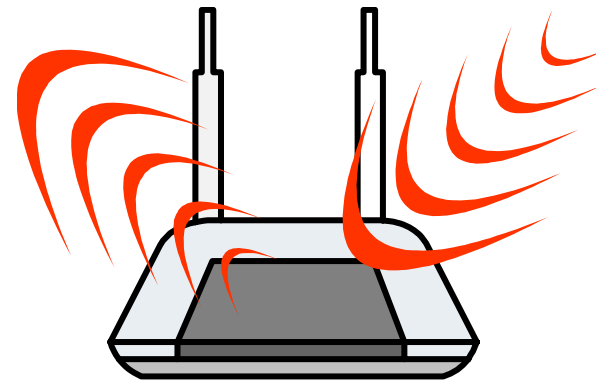


Preventing Wi-Fi Cyber Crimes

Security DOs, DON'Ts and MYTHS

for

Home Wireless Routers (APs)



DOs

DOs - Turn off your wireless router when not in use

This simple step will ensure that your wireless router and the internet connection cannot be misused when you are not around

As a bonus you save electricity and the environment



DOs - Use WPA or WPA2 security



Encrypt your wireless communication by turning on WPA security. If your wireless router supports the better standard – WPA2, use that instead.

You will have to specify a key or a pass phrase. To use the wireless router, the same key / pass phrase has to be setup on your computer

The key / pass phrase should be at least 8 characters long with numbers and special characters

DOs - Restrict access to your wireless router



Change the administrator's password

Once you change the administrator's password no one can change the settings on your wireless router.

Disable remote administration

This ensures that no one can change the settings on your wireless router from the internet.

Disable administration from wireless

You must be connected to your wireless router using a network cable for changing the settings.

DOs - 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.

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

DON'Ts

DON'Ts - 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.

DON'Ts - 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



DON'Ts - Do not share passwords

Do not share either the administrator's password or the wireless security key / pass phrase with anyone. This includes your internet service provider, neighbors, etc.

If you must share it for any purpose; change it immediately afterwards.



MYTHS

MYTHS - Disabling 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.

MYTHS - Using MAC address access control list



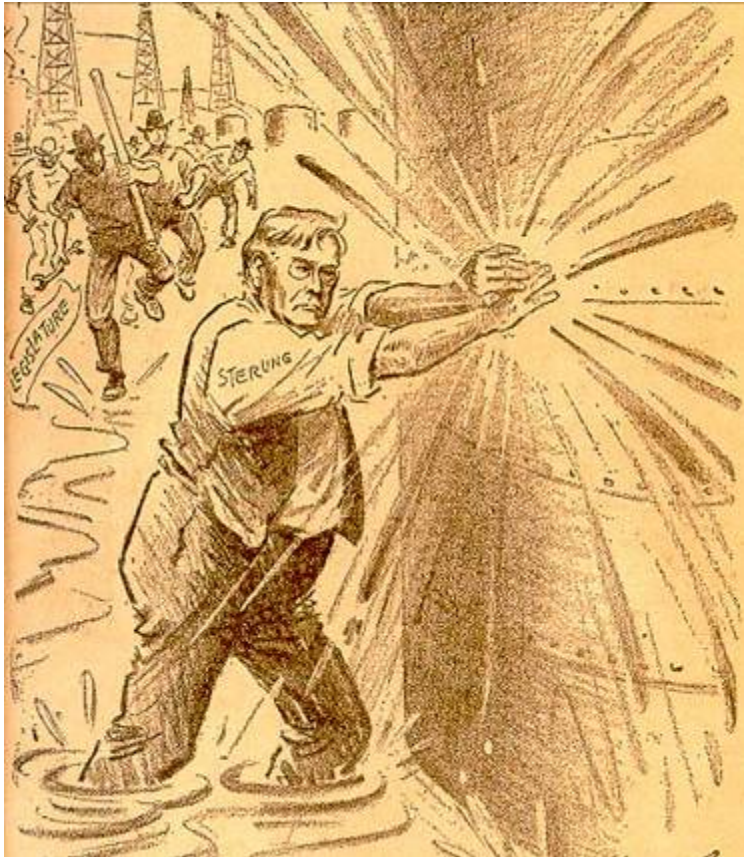
Most wireless routers will allow you to specify which computers can connect to it based on the MAC address of the wireless card in the computer.

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.

MYTHS - 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.

MYTHS - Turning off DHCP or using static IP addresses

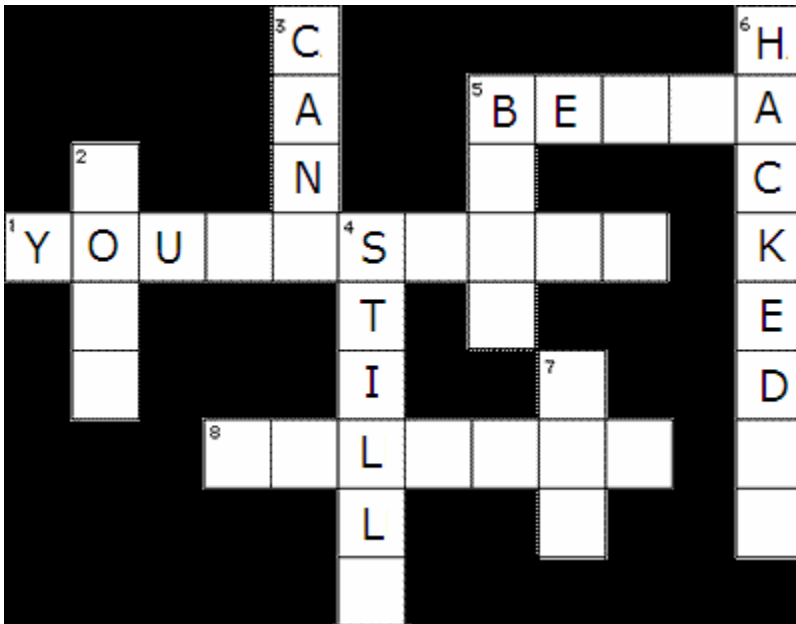


Just like SSIDs, a hacker can determine valid IP address range for your connection within seconds. Turning off the DHCP server in your wireless router or using static IP addresses for your computers provide no security benefit.

FACT

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

MYTHS - 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.

About AirTight Networks

AirTight: We Make Wireless Secure

SpectraGuard Enterprise



- On site appliance and sensors
- CapEx one time investment
- 24x7 WiFi scanning
- Detect and Prevent Attacks

SpectraGuard Online



- Security as a Service
- No upfront investment
- 27x7 WiFi scanning
- Detect & Prevent Attacks

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

About AirTight Networks



We Make Wireless Secure

www.airtightnetworks.com

To learn more about WiFi security risks and best practices for preventing WiFi attacks, please visit

www.airtightnetworks.com/home/resources/prevent-wifi-attacks.html

www.airtightnetworks.com/home/resources/prevent-wifi-attacks-solutions.html

To learn how AirTight can help secure your wireless network, send mail to:

contact@airtightnetworks.com

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