

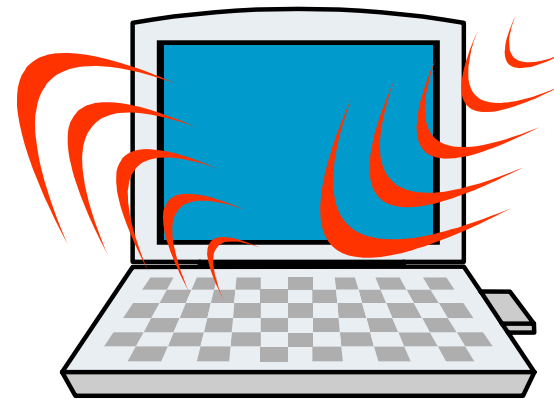


## Preventing Wi-Fi Cyber Crimes

Security DOs, DON'Ts and MYTHS

for

Wireless Enabled Computers



# DOs

## DOs - Switch off your wireless card when not in use



This ensures that your wireless card will not connect to any wireless router, AP or a peer-to-peer network without your knowledge.

Turning off the card also protects you from attacks like Café Latte targeted towards computers with switched on wireless cards while they are disconnected.

## DOs - Turn off “Automatically connect to non-preferred networks”



Windows wireless connection settings is set to connect to any available wireless network. You **MUST** turn off this setting.

Leaving this on will cause your computer to connect to any available network without your knowledge. Such networks can be viral or malicious.

## DOs - Select “Access Point (infrastructure) networks only”



Selecting “Any available network (access point preferred)” or “Computer-to-computer (ad hoc) networks only” enables your computer to use ad-hoc networks. Ad-hoc networks (also called Peer-to-peer networks) are formed when two computers start a network between themselves without a wireless router or an AP.

When ad-hoc connectivity is enabled, your computer will advertise this whenever your wireless card is on. Hackers can read this advertisement and lure you to connect to their computers using this peer-to-peer network.

## DOs - Ensure that you use WPA2 or WPA security

Ensure that you setup your wireless router or AP to operate on WPA2 or WPA security.

Using OPEN or WEP leaves your computer vulnerable to connection hijack and your communication open to snooping.



# DON'Ts

## DON'Ts - Do not connect to (unknown) 'free' SSIDs



Unknown or unexpected 'free' connections are usually malicious and sometimes viral as well. These connections force you to use OPEN security and this exposes you to snooping and other threats.

Once you connect to these SSIDs, these get added to your list of preferred SSIDs and your computer automatically connects to them the next time they are in range; even without your knowledge.

## DON'Ts - Do not access confidential sites when using Hotspots



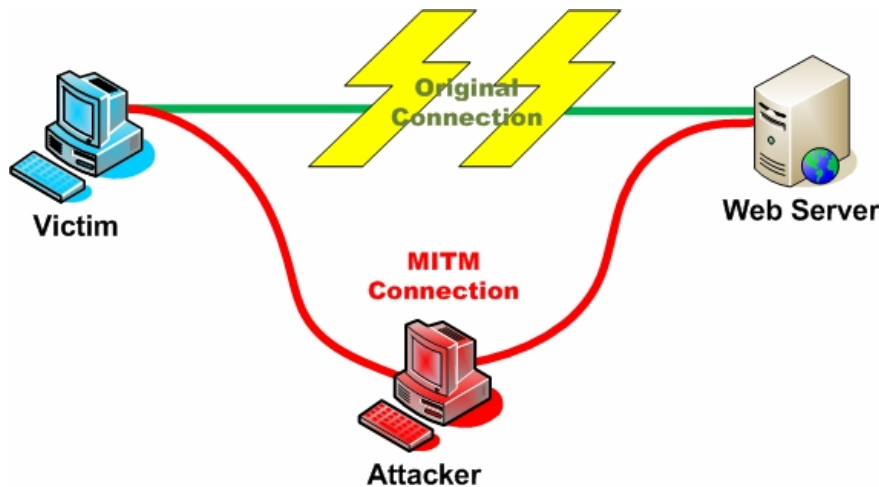
When you use hotspots, do not connect to confidential sites like e-banking. Your connection can be hijacked and your passwords stolen.

If you must connect to such sites from a hotspot, ensure that you are connecting to a secure (<https://>) site. When accessing a secure site, please disconnect immediately if your browser displays any certificate error.

Security DOs, DON'Ts and MYTHs for Wireless Enabled Computers

# MYTHS

# MYTHS – It is always safe to connect to secure (HTTPS) sites



Using HTTPS ensures that the communication between your computer and the site that you are visiting is encrypted and snoopers cannot read this traffic. You **MUST** use HTTPS whenever you access confidential site or data over the net; irrespective of how you are connected to the internet.

## FACT

Man-in-the-middle attacks are designed to trick you into thinking that you are connected securely to your target site, while you are actually connected to a intermediate computer that the hacker uses to snoop into your data before it is sent to the actual site. The only indication that this is happening is a 'certificate error' that your browser will display. If you see such an error please disconnect immediately.

Security DOs, DON'Ts and MYTHs for Wireless Enabled Computers

## MYTHS – My firewall and antivirus will protect me



Firewall, antivirus and anti-malware are very important components for ensuring that you are safe from the dangers of cyberspace. Firewall ensures that no one from the internet can connect to your computer, while allowing your computer to connect to the internet. Antivirus and anti-malware ensures that no 'bad' program can be installed on your computer.

### FACT

Firewall, antivirus and anti-malware will not protect you from threats that attempt to either trick you into connecting to a hacker's network or a man-in-the-middle attack. You must follow these DOs and DON'Ts to protect yourselves from these threats.

# 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 Wireless Enabled Computers

# About AirTight Networks



**We Make Wireless Secure**

[www.airtightnetworks.com](http://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](http://www.airtightnetworks.com/home/resources/prevent-wifi-attacks.html)

[www.airtightnetworks.com/home/resources/prevent-wifi-attacks-solutions.html](http://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](mailto:contact@airtightnetworks.com)

---

Security DOs, DON'Ts and MYTHs for Wireless Enabled Computers