

# PUBLIC WI-FI



## Where is it...

Wi-Fi Hotspots in coffee shops, airports, hotels, shopping centres and libraries are a fantastically convenient way to connect your device to a Wi-Fi network and browse the web quicker or get more out of your apps. However Public Wi-Fi is insecure and opens your device up to numerous threats.



## What are the dangers...

Public Wi-Fi gives hackers a great opportunity to steal your personal data and login credentials. The openness of the signal sent from your device to the Wi-Fi Hotspot means that criminals can view the information you are sending as well as hijacking your communications. This is known as a Man-in-the-Middle attack. Cyber criminals can set up their own public hotspots in an attempt to get you to connect to them, they will capture any data you are sending. Public Wi-Fi with a password is not secure either, everyone has the password!



## How do I stay safe...

- Don't do anything on Public Wi-Fi you wouldn't be happy with strangers seeing. Avoid logging on to any service where your username or password is needed.
- Use a Virtual Private Network (VPN) this will encrypt the traffic from your device and ensure the hacker can't read it.
- If you are unsure as to whether a Wi-Fi Hotspot connection is secure do not use it. Use your 3G or 4G data connection to access the internet instead. Data passed over 3G and 4G is encrypted.



 @PoliceDSC

 @Police Digital Security Centre

  
POLICE DIGITAL SECURITY CENTRE

[www.policedsc.com](http://www.policedsc.com)