Wi-Fi

Many retail outlets including cafes, pubs, restaurants and shopping malls offer customers free Wi-Fi. Whilst these are very convenient for keeping your email up-to-date and surfing the web over coffee, they do offer an easy way for criminals to steal your data.

Public Wi-Fi - Staying Safe: for the ultimate in security when using a public Wi-Fi we recommend the use of a Virtual Private Network (VPN) which encrypts all of your outgoing traffic. If you are not too comfortable using a VPN then only use websites that display 'https' in the address bar (this indicates that traffic is encrypted by your browser although it does not indicate that the website in question is trusted). Apps provided by organisations such as banks are generally safe to use anywhere.

Mobile data, whether 4G or 5G, is intrinsically safe and can be used to send and receive confidential data.

If you are using a laptop over a public Wi-Fi connection it is most important that your anti-virus software is up-to-date and the device firewall (Windows' Defender or macOS Firewall) is active.

Private Wi-Fi Risks: unless switched off in the Router Control Panel, all Wi-Fi systems broadcast their SSID (the name you see when connecting); you can hide your Wi-Fi from public gaze and let trusted users connect by asking them to search for the name of your Wi-Fi or by providing a QR code for them to scan (which also keeps the Wi-Fi access password secret).

For ultimate Wi-Fi protection, you can restrict access to designated MAC addresses (A MAC address is a unique code used to identify individual devices on a network.)

*For more Police advice on Wi-Fi security, tap **here**.*

Surrey and Sussex Cyber Crime Unit
Prepared by Jeff Maynard (20919)
jeff.maynard@surrey.police.uk

In an emergency always dial 999