Wi-Fi Hotspots

How to surf safely

A Wi-Fi hotspot is a location that provides internet access through a wireless network. These can be found almost anywhere – from airports to coffee shops and even on public transport. By signing into the wireless network, you can access the internet in the same way as you would using your own personal Wi-Fi at home.

How secure is public Wi-Fi?

Wi-Fi signals can easily be intercepted and anyone with access to the network can 'see' all the activity taking place on the network. Wi-Fi that is installed in your own home, is usually securely protected when set up, requiring a key or password to enter the network. This means that all traffic on the network is encrypted and only those with the key can access it. Anyone can access a public Wi-Fi network, meaning it is a lot less secure.

VPNs – extra security

The safest way to use public Wi-Fi is to invest in a Virtual Private Network or VPN. A VPN encrypts all your network traffic independent of the network itself, meaning that eavesdroppers can't see the data you are transmitting or receiving. Many organisations use VPNs to ensure the security of their information, but this can come at a cost. VPN providers often charge for the service and the quality of connections often depends on the provider.

Why is public Wi-Fi targeted by criminals?

Criminals can easily spoof a Wi-Fi hotspot, giving them information about connected devices and the ability to monitor network traffic. If passwords, banking information or other private information are sent across a public Wi-Fi network insecurely, it can be intercepted and used later. Fake Wi-Fi hotspots can also direct you to bogus web pages, which encourage you to enter credentials or personal information that can be stolen.

How can I surf safely?

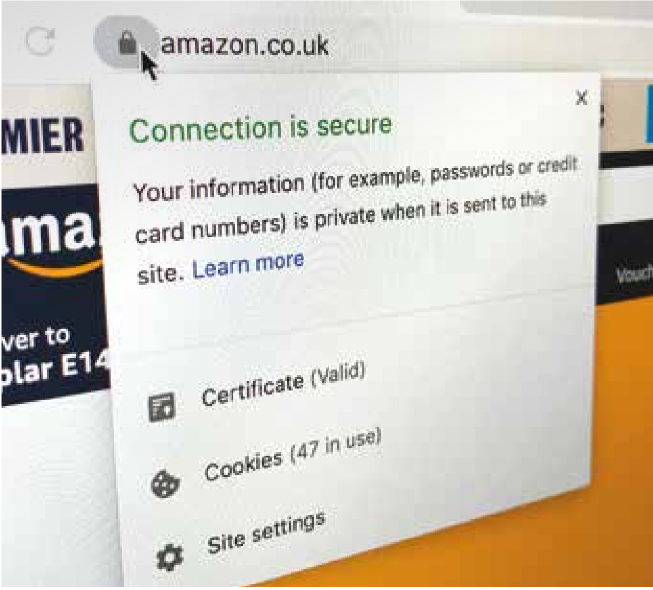
Many websites use Hypertext Transfer Protocol over SSL (or https) to secure connections to them. This means that traffic to and from the website is encrypted, so eavesdroppers will be unable to de-code intercepted communications. Using these sites can protect you from criminals attempting to target users of public hotspots.

Remember that anyone can create a website using 'https', so it is vital you use the correct URL when visiting a website. For example, a criminal could try and direct you to a fake secure website called 'https://www.natvvest.com' – rather than the real 'https://www.natwest.com'.

To avoid these traps, use hyperlinks from your bookmarks toolbar or type them in manually rather than following a link.

'You should be cautious when using Wi-Fi connections that are public and think about your online activity.'

Sites employing https can often be identified by a green padlock or a closed padlock in the URL bar. This is how it looks in Firefox:



Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Most browsers allow you to see details of the certificate used to secure the website from the same place. Just click to see the information.

What else can I do?

You should be cautious when using Wi-Fi connections that are public and think about your online activity. Be careful about entering personal information or undertaking financial transactions, which is the kind of data criminals will target when accessing these networks. If you use your mobile devices, remember that apps will be constantly trying to automatically access the network and you rarely know how secure this connection is.

If in doubt, use your mobile connection rather than public Wi-Fi – or wait until you get home.

You can access advice and information on a range of cyber security topics at the following sites:

www.ncsc.gov.uk

www.cyberaware.gov.uk

www.takefive-stopfraud.org.uk

www.actionfraud.police.uk

www.serocu.police.uk/individuals

Report online at **www.sussex.police.uk** or **www.surrey.police.uk** or **call 101**. In an emergency always **call 999**.

Find us on social media

Produced by Sussex Police Corporate Communications 2019