Safe Wi-Fi Hotspots

Wireless networks have revolutionised the way we use computers and mobile devices in our homes, offices and out in public. Free public Wi-Fi is available at some businesses, at airports, restaurants, coffee shops and even in some parks in the Pacific Islands. These networks are used by hundreds of people every day.

However, what most people don't realise is that free public Wi-Fi isn't always secure, even if it requires a password to login. You might love public Wi-Fi, but so do hackers! So, if you use public Wi-Fi without adequate protection, you could be risking becoming a victim of fraud or identity theft, or both.

The Risks of Public Wi-Fi

The security risk associated with using public Wi-Fi is that unauthorised people can intercept your confidential personal or financial activity in the following ways:

- **Capturing your passwords, snooping on your financial transactions and reading your private emails:** This can happen if the hotspot you're using isn't secured.
- **Fake hotspot:** This can fool you into thinking that it is the legitimate hotspot when in fact it's an authentic-sounding hotspot name set up by a cybercriminal.
- **Spreading malware over unsecured Wi-Fi:** Hackers can also use an unsecured Wi-Fi connection to infect your device with malware. Having infected software on your computers and mobile devices can damage both your business and personal finances.

Sometimes, you may simply be prompted to log in to gain internet access. This tells the provider that you are online in their café, hotel or company. But there may be no encryption and so it's unsecure.

How to Protect Yourself

- Avoid financial transactions that might reveal valuable passwords or personal information such as credit card numbers.
- Wherever possible use well-known, commercial hotspot providers.
- Ensure you have effective and updated antivirus/antispyware software running before you use public Wi-Fi.
- As an alternative, you could use your own Wi-Fi device (mobile broadband 'dongle'), which should provide you with a more secure connection.
- Businesspeople wishing to access their corporate network should use a secure, encrypted , reputable Virtual Private Network (VPN).
- If you don't have access to a VPN, use your data if it's urgent, or wait until you get home or back to the office where you can use your secure Wi-Fi.
- Don't leave your computer, smartphone or tablet unattended in public places.
- Be aware of who is around you and may be watching what you are doing over your shoulder.

GET SAFE ONLINE

Funded by COMMONWEALTH UNITED KINGDOM CHAIR-IN-OFFICE