

REVERSE THE THREAT

STAYSMARTONLINE

WEEK 8-14 OCTOBER 2018

Using Public Wi-Fi Safely

Public Wi-Fi isn't always safe. Without the right protection, your personal information could become public. Reverse the threat of cybercrime and get smart about using public Wi-Fi.

What is a public Wi-Fi hotspot?

A public Wi-Fi hotspot is a location — such as a café, airport, hotel or library — offering a Wi-Fi internet connection to people for their digital devices, such as smartphones, tablets or laptops.

87%

of people have taken risks
ON PUBLIC WI-FI*

* Symantec, Norton Wi-Fi Risk Report (2017)

Is a public Wi-Fi hotspot secure?

Public Wi-Fi hotspots are convenient but can be risky. It's easy for the information being sent between your device and the public Wi-Fi network to be intercepted. Cybercriminals have also been known to set up rogue Wi-Fi hotspots with names that look like a legitimate network. Cybercriminals use these networks to get their hands on your banking credentials, account passwords and other valuable information.

How to stay safe when using public Wi-Fi

Be careful about what you do online when you're using a public Wi-Fi hotspot. Here are some tips to help keep your information safe:

- Confirm the 'official' hotspot name from venue staff and manually connect your device to it. Don't let your device automatically connect to the first hotspot in its list.
- Check the privacy and security details before agreeing to the network's terms of use. Check to see what data will be collected about you and how it will be used.
- Don't do your online banking or shopping, send confidential emails or enter your passwords or credit card details on public Wi-Fi. Wait until you're using a secure home, office or mobile connection.
- Consider using the mobile data on your phone instead. If you're using a laptop or tablet without mobile data, try setting up your phone as a personal hotspot with a strong password.
- Use secure websites. Always look for a https ('s' stands for secure) in the website address and a padlock on the web browser.
- Turn off file sharing. If you have file sharing turned on and you connect to a public Wi-Fi hotspot, your files may be accessed by others using the same hotspot.
- Install a reputable Virtual Private Network (VPN) on your device. When enabled, this boosts security by creating an encrypted 'tunnel' for your information to pass securely through public Wi-Fi networks.
- Turn on your firewall and virus scanner. Firewalls are designed to prevent unauthorised access. Be sure to check your device and turn on its firewall (if applicable).
- Always remember to disconnect from the hotspot after you've finished using it.

For more information
on how to reverse the
threat of cybercrime and
Stay Smart Online, please visit:
**[staysmartonline.gov.au/
reversethethreat](https://staysmartonline.gov.au/reversethethreat)**



Follow us on
Facebook
fb.com/staysmartonline



Sign up to our free alerts
**[staysmartonline.gov.au/
alert-service](https://staysmartonline.gov.au/alert-service)**