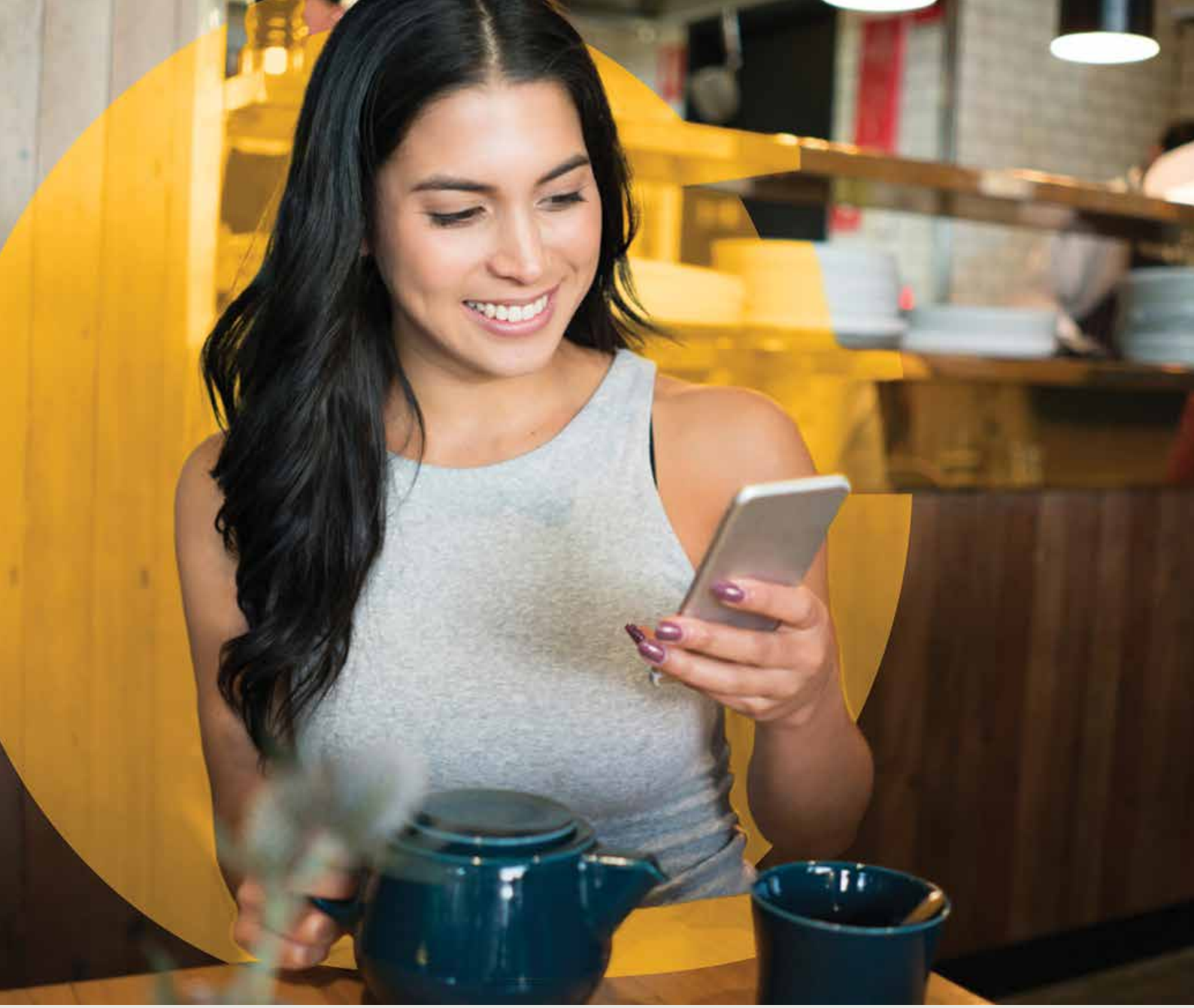


NORTON WI-FI RISK REPORT

Australia

Norton by Symantec

CONTENTS

PUBLIC WI-FI RISK SNAPSHOT

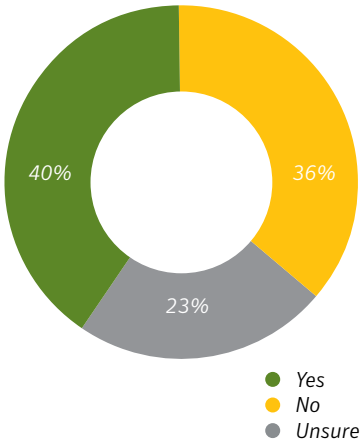
NORTON RISK REPORT

This report presents the summary findings of Norton's Wi-Fi Risk Survey, which aimed to obtain an understanding of public Wi-Fi perceptions and practices amongst the general public in Australia. The survey findings have been released to help raise awareness about the security risks many Australians are exposed to, and provide insights and measures Australians can take to help mitigate those risks to improve the security of their personal information.

The survey found that three in five (60 percent) Australians feel safe using public Wi-Fi. 40 percent of Australians can tell the difference between a secure or unsecure public Wi-Fi network, while 36 percent cannot and 23 percent are unsure.

81 percent of Australians cannot tell if apps are transmitting data securely over public Wi-Fi or not.

AUSTRALIANS WHO CAN TELL THE DIFFERENCE BETWEEN A SECURE AND UNSECURE PUBLIC WI-FI NETWORK



EVALUATING THE RISKS

Despite the risks of public Wi-Fi, Australians are willing to trade security for convenience

While Virtual Private Networks (VPN) are an option to keep safe on public Wi-Fi, a total of 51 percent of Australians do not use a VPN every time they use Wi-Fi, while 30 percent hadn't heard of the term VPN.

Most Australians (83 percent) have admitted to taking risks while connected to a public Wi-Fi network on their mobile phone, tablet or laptop. All actions that require you to send or receive information is considered risky. This includes logging into personal email accounts (58 percent), logging into social media accounts (54 percent), checking bank or financial information (30 percent). There are only 17 percent who've not taken any risks while online.

83%

of Australians have admitted to taking risks while on public Wi-Fi

THE CHOICE BETWEEN FREE OR SAFE WI-FI

Is a free Wi-Fi connection more important to Australians than a safe Wi-Fi connection?

The survey finds Australians value a strong and free Wi-Fi connection. 57 percent wouldn't do, share or exchange anything for free Wi-Fi. Of the 43 percent that is willing to do something, one third would be willing to watch a 3 minute ad.

On the other hand, 51 percent of Australians would be horrified if a hacker managed to steal personal information from their mobile phone, tablet, or laptop and posted it publicly online. 33 percent would be horrified if their photo library (intimate, personal and family photos) was stolen and posted publicly.

43%

of Australians would watch a 3 minute ad in exchange for free Wi-Fi

Travel decisions based on Wi-Fi availability

Australians place value on access to a strong Wi-Fi signal. 59 percent of Australians require a strong Wi-Fi signal when choosing a hotel, hostel or holiday rental. 29 percent of Australians require a strong Wi-Fi signal when choosing an airline, similarly to 28 percent say the deciding factor for a transport hub for travelling and/or commuting is their deciding factor. 26 percent of Australians select a place to eat or drink (cafe, bar, restaurant etc) by their strong Wi-Fi signal.

PUBLIC WI-FI SECURITY: TIPS AND TRICKS

The best way to keep your information safe while using public Wi-Fi is to use a virtual private network (VPN) like Norton WiFi Privacy while on your PC, Mac, smartphone or tablet.

If you have to use public Wi-Fi, Norton recommends the following best practices to help protect your information:

1. **Be vigilant**
Review the network you're joining, and check with staff for the correct network name. Cyber criminals often set up rogue hotspots that may sound close to the name of the legitimate network you may be trying to connect to.

2. **Avoid networks with no passwords**
Ensure you only join password protected public Wi-Fi hotspots, even if you need to buy a cup of coffee to obtain the password at a café.

3. **Login securely**
Don't access sensitive information or online accounts via an app. Go directly to the website and verify they are using HTTPS before logging in. Enable two-factor authentication to increase your security coverage.

4. **Manage your connections**
Ensure to turn off any auto-connect settings for Wi-Fi or Bluetooth on your devices. Disable file sharing as well to ensure you aren't unknowingly sharing files with nearby devices.

5. **Manage your accounts**
Always log out of accounts when you're finished using them.

ABOUT THE SURVEY

Norton's Wi-Fi Risk survey researched Australians' perceptions of Wi-Fi security issues. This report presents the summary findings of the global survey comprising of over 15,500 mobile device users who had connected to Wi-Fi, with at minimum national sample of 1,000 Australian mobile device users, conducted during May - June, 2017.

This research report was prepared by Reputation Leaders through the international online panel of Research Now. It has a standard error margin of +/- 3 percent.

ABOUT SYMANTEC

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organisations, governments and people secure their most important data wherever it lives. Organisations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

For additional information, please visit **www.symantec.com** or connect with us on **Facebook, Twitter,** and **LinkedIn.**