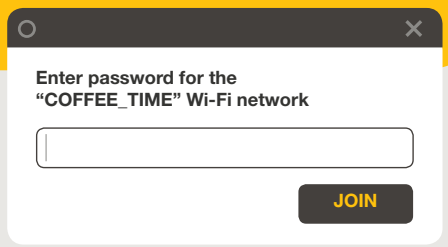
SECURITY ON PUBLIC WI-FI

Australia

A guide to help you stay safe online while using public Wi-Fi

Norton by Symantec

“WHAT’S YOUR WI-FI PASSWORD?”



An all too common question asked in our constantly connected digital age.

Public Wi-Fi is readily available at airports, hotels, cafes and even shopping centres amongst many other places. Whether you need to send a quick email, catch up on your friend’s overseas travels on social media, or check your bank balance, you can do it at the touch of your mobile device easily. However, have you ever thought to ask yourself, “is public Wi-Fi even risky?”

The recent Australian Norton Wi-Fi Risk Report found that 60% of Australians feel safe using public Wi-Fi, however only 40% can confidently tell the difference between a secure or unsecure public Wi-Fi network.

While you may be a regular public Wi-Fi user, have you thought about the consequences of the sites you’re visiting or content you’re accessing while you’re using it?

58% of Australians have logged into personal email accounts, and 54% have logged into social media accounts on their mobile phones, tablets or laptops while connected to a public Wi-Fi network[1]

Everything you access whilst on public Wi-Fi puts your private information at risk. Hackers, cyber criminals or even just nosy neighbours can easily view everything you’re accessing, just by being on the same network as you.

Norton by Symantec

1. The Norton WiFi Risk Report - Australia, June 2017

PUBLIC WI-FI MAY NOT BE AS SAFE AS YOU THINK

The 5 most common ways hackers can access your information on public Wi-Fi:

⚠ Man in the Middle attack

One of the most common threats on Wi-Fi networks. A Man in the Middle attack (MitM) is a form of eavesdropping. When a computer makes a connection to the Internet, data is sent from point A (computer) to point B (service/website), and vulnerabilities can allow an attacker to get in between these transmissions and "read" them. So what you thought was private, no longer is.

⚠ Malware distribution

Thanks to software vulnerabilities, there are also ways that attackers can slip malware onto your computer without you even knowing. A software vulnerability is a security hole or weakness found in an operating system or software program. Hackers can exploit this weakness by writing code to target a specific vulnerability, and then inject the malware onto your device.

⚠ Unencrypted networks

Encryption means that the messages that are sent between your computer and the wireless router are in the form of a "secret code," so that they cannot be read by anyone who doesn't have the key to decipher the code. Most routers are shipped from the factory with encryption turned off by default, and it must be turned on when the network is set up. If an IT professional sets up the network, then chances are good that encryption has been enabled. However, there is no surefire way to tell if this has happened.

⚠ Malicious hotspots

These "rogue access points" trick victims into connecting to what they think is a legitimate network because the name sounds reputable. Say you're staying at the Goodnyght Inn and want to connect to the hotel's Wi-Fi. You may think you're selecting the correct one when you click on "GoodNyte Inn," but you haven't. Instead, you've just connected to a rogue hotspot set up by cybercriminals who can now view your sensitive information.

⚠ Snooping and sniffing

Cybercriminals can buy special software kits and even devices to help assist them with eavesdropping on Wi-Fi signals. This technique can allow the attackers to access everything that you are doing online — from viewing whole webpages you have visited (including any information you may have filled out while visiting that webpage) to being able to capture your login credentials, and even being able to hijack your accounts.

Norton™ by Symantec

2. https://au.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html

THE REALITY OF AUSTRALIANS AND PUBLIC WI-FI

Only

19%

of Australians can tell if their apps are transmitting information securely over Wi-Fi

83%

of Australians have taken risks online using public Wi-Fi

51%

of Australians would be horrified if a hacker stole details of their bank accounts and financial information

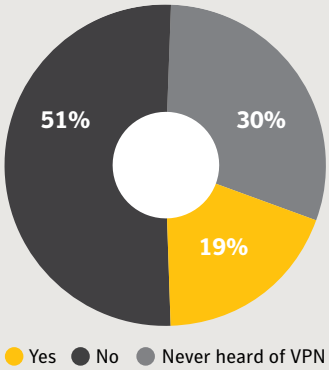
57%

of Australians won't do or swap anything in exchange for a free Wi-Fi connection with a strong signal

59%

of Australians make a choice on hotel/hostel/ holiday rental based on a strong Wi-Fi signal

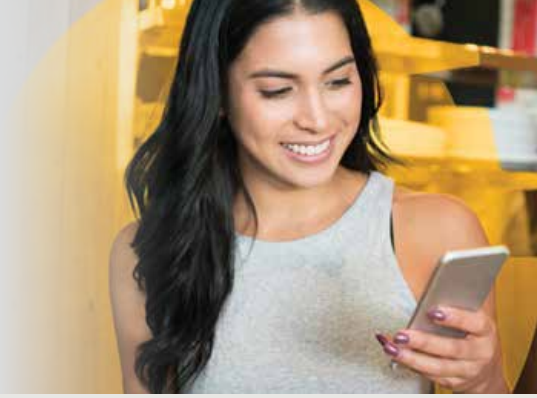
Do you use a VPN every time you use Wi-Fi?



1. The Norton WiFi Risk Report – Australia, June, 2017

Norton by Symantec

TOP TIPS TO HELP STAY SAFE ON PUBLIC WI-FI



If you have to connect to public Wi-Fi,
then be aware of the risks involved!

Here are our top tips to help you stay stafe:

Pay attention to the network you're joining. Cyber criminals set up rogue hotspots with names that are close to that of the legitimate network you may be trying to connect to.

Select password-protected public Wi-Fi hotspots, even if it means buying a cup of coffee to get the password at a café.

Don't access sensitive information or online accounts that contain such data if you're on public Wi-Fi.

Turn off any auto-connect settings for Wi-Fi or Bluetooth on your devices. Also remember to disable file sharing.

Always log out of accounts when you are done using them.

Use a VPN to ensure all data transmitted during your online sessions is encrypted. **Norton WiFi Privacy** is a VPN app that automatically turns on when it detects a public Wi-Fi network.

Norton™ by Symantec

4. https://au.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html

WHAT IS A VPN?

A virtual private network (VPN) gives you online privacy and anonymity by creating a private network from a public Internet connection.

HOW DOES A VPN WORK?

VPNs mask your Internet protocol (IP) address so your online actions are virtually untraceable. Most importantly, VPN services help you establish secure and encrypted connections, providing greater privacy.

Norton by Symantec

5. https://au.norton.com/internetsecurity-privacy-what-is-a-vpn.html

HOW TO CHOOSE A VPN?

The best way to stay secure when using public Wi-Fi is to use a VPN solution, like Norton WiFi Privacy, which is compatible with Android and iOS smartphones and tablets, as well as with Windows PCs and Apple Macs.

Here are some questions to ask when you're choosing a VPN provider:

Do they respect your privacy? The point of using a VPN is to protect your privacy, so it's crucial that your VPN provider respects your privacy, too. They should have a no-log policy, which means that they never track or log your online activities.

Do they run the most current protocol? OpenVPN provides stronger security than other protocols, such as PPTP.

Do they set data limits? Depending on your Internet usage, bandwidth may be a large deciding factor for you. Make sure their services match your needs by checking to see if you'll get full, unmetered bandwidth without data limits. Remember, some packages may not cost you money, but you'll be subjected to frequent advertisements instead.

Where are the servers located? Decide which server locations are important to you. If you want to appear as if you're accessing the Web from a certain locale, make sure there's a server in that country.

Will you be able to set up VPN access on multiple devices? If you are like the average consumer, you use between three and five devices. Ideally, you'd be able to use the VPN on all of them at the same time.

What happens if the VPN goes down? Be sure that your provider implements a kill switch system in the event of failure. This means that your connection would automatically be locked down and would not default to an unsecured Internet connection if something goes wrong.

There are many factors to consider when choosing a VPN provider, so do your research to make sure you're getting the best suited for your needs. Regardless of the provider you choose, any good VPN will provide more security, privacy and anonymity online than any public Wi-Fi network ever could.

Norton™ by Symantec

6. https://au.norton.com/internetsecurity-privacy-what-is-a-vpn.html

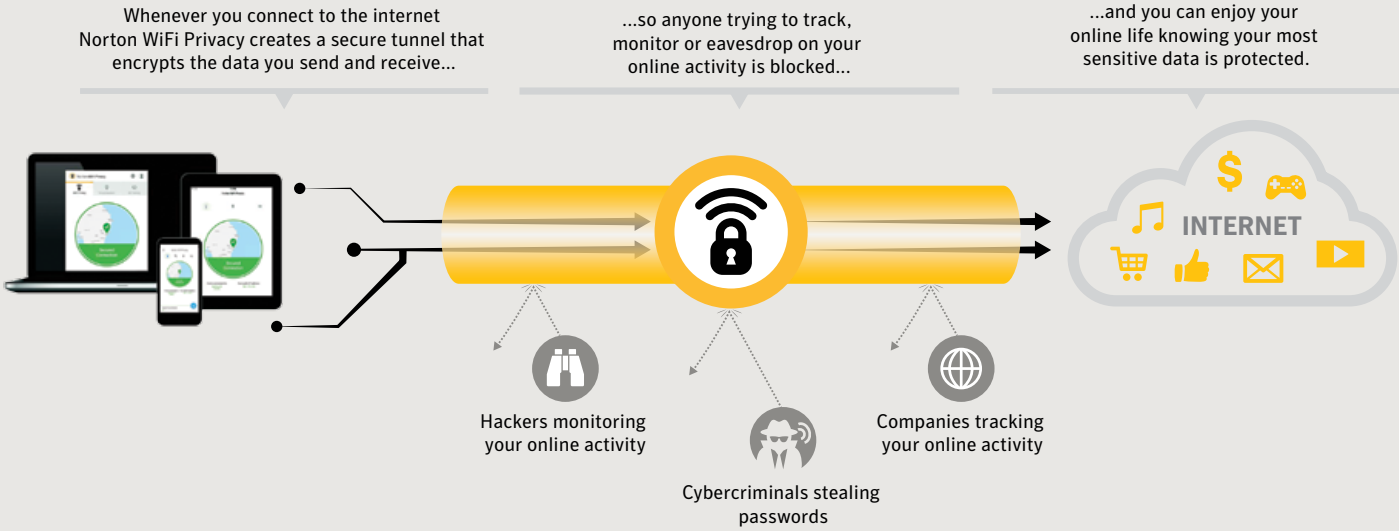
NORTON WIFI PRIVACY

iOS

Norton WiFi Privacy helps keep your personal information protected

The security you've always trusted from Norton now helps protects your most sensitive information like passwords and credit card numbers while using public Wi-Fi hotspots.

Norton WiFi Privacy is a VPN app that helps protects your information when you're on public Wi-Fi. Norton WiFi Privacy is designed to help you connect safely and privately with Windows PCs, Macs, iOS and Android devices.



Norton by Symantec

NORTON WIFI PRIVACY

iOS

Bank-grade encryption to protect your private information on public Wi-Fi.

Unlimited data and bandwidth – high performance surfing and streaming.

Compatible across all devices and operating systems. Secure the information you send and receive across Windows, Mac, Android and iOS.

No-log VPN that encrypts your information, and doesn't track or store your online activity or location.

World-class 24x7 customer support included – by phone or chat.

Protection promise. We offer a money-back guarantee with your subscription.

SECURE YOUR PUBLIC WI-FI CONNECTION NOW »

Also available at leading electronics retailers now.

Norton by Symantec

Check system requirements: https://au.norton.com/wifi-privacy


Norton™
by Symantec