The ESET Cyberawareness Index Australia 2019

Survey of more than **1000 individuals in Australia** reveals cybersecurity knowledge and best-practice behaviour leaves room for improvement

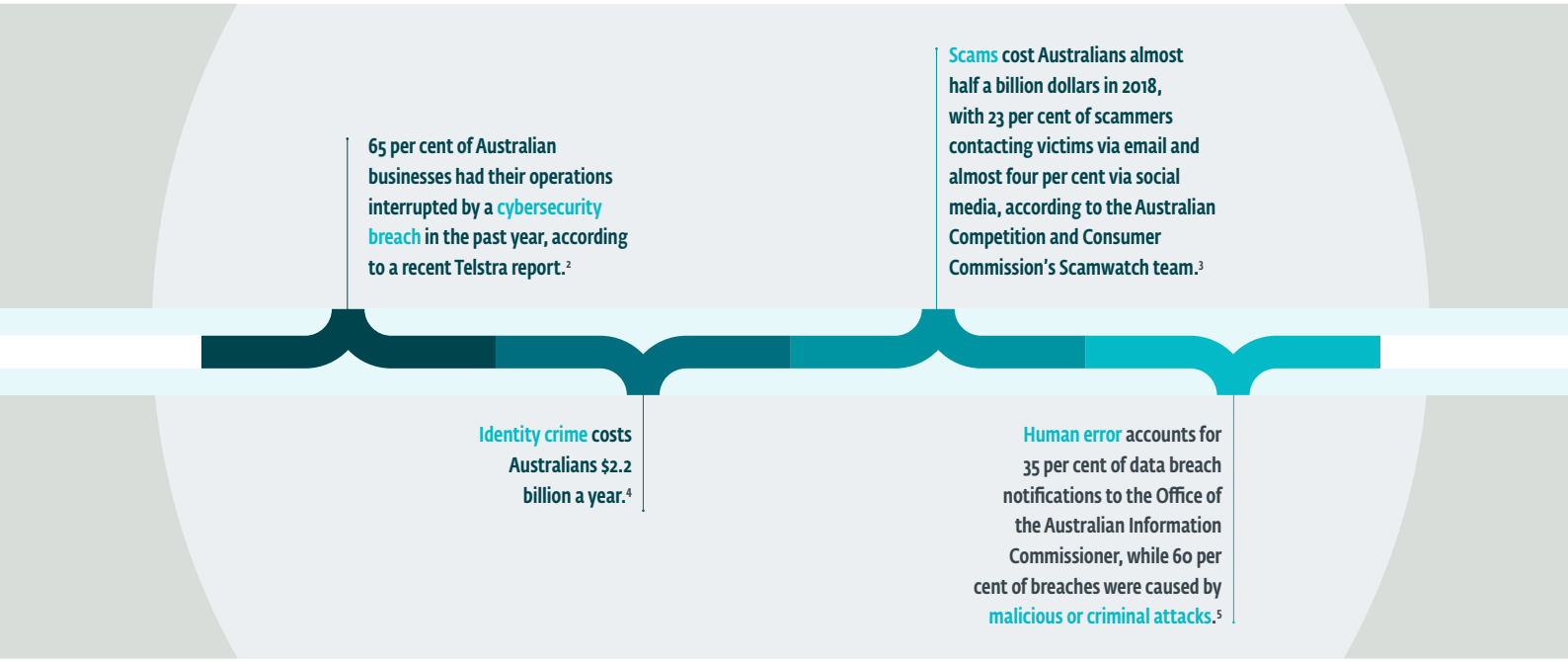
ENJOY SAFER TECHNOLOGY™

Introduction

As of January 2019, **87 per cent of the Australian population were internet users** (21.7 million people), and **93 per cent of these people used the internet every day** to consume a wide variety of online information and services.[1]

As internet usage reaches saturation point, it might seem reasonable to assume that attitudes and behaviour around securing personal and business data assets would have matured in recent times.

This is particularly so in light of staggering statistics such as:



To understand the current status of Australia's cyberawareness, ESET conducted a survey of 1,062 Australian online users in August 2019. This yielded a statistically-valid result that is representative of the Australian population as a whole.

This white paper outlines the findings of that survey, including:

- the current state of technology adoption
- what users are doing online and what they're doing (or not doing) to protect themselves
- tips on cybersecurity best practices.

1 https://www.roi.com.au/blog/australian-internet-social-media-statistics-2019

2 https://www.telstra.com.au/content/dam/shared-component-assets/tecom/campaigns/security-report/Summary-Report-2019-LR.pdf

3 https://www.scamwatch.gov.au/news/scams-cost-australians-half-a-billion-dollars

4 https://apo.org.au/sites/default/files/resource-files/2016/11/apo-nid71709-1189581.pdf

5 https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report/

Australian consumers have embraced mobile technology

Mobile technology is ubiquitous in Australia and is being used in people's personal lives as well as at work.

Almost all Australians (92 per cent) use a smartphone while 72 per cent use a laptop and 53 per cent use a tablet or iPad. Moreover, 48 per cent use a desktop computer and only 37 per cent have adopted smart home devices such as a smart TV or smart speakers. However, the wearables market is still nascent with just 27 per cent using wearable technology such as a fitness tracker or smart watch.

Android commands the market on smartphones

Android has a firm grasp on the smartphone operating system environment with 59 per cent of consumers choosing an Android device versus 38 per cent choosing an Apple iOS device. Windows has just two per cent of the market.

When it comes to tablets, however, 57 per cent of consumers are using iPads while 35 per cent are using Android devices and seven per cent are using a Windows tablet.

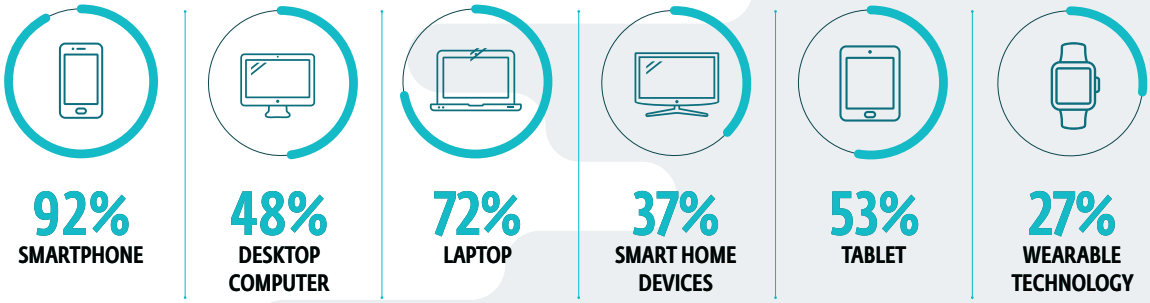
Nick FitzGerald, senior research fellow, ESET, said, "Android devices can be less secure than Apple iOS devices due to slow and inconsistent updates, which delays important security patches and increases vulnerability to hacks. Users can also download apps from third-party app stores, which aren't always secure or updated, which can also make devices less secure.

"ESET is a founding member of the App Defense Alliance, protecting the Google Play Store. This will help make the Google Play Store safer for users. This is a full-fledged and proactive campaign to protect billions of consumers and businesses at the source.

"Apple is prompt with security updates and only allows users to download apps from its App Store, where they are heavily vetted by Apple. Tight oversight and additional security features such as encrypted messaging and privacy protection makes iOS the more secure of these operating systems.

"However, this doesn't mean that users need to be either paranoid or complacent. Regardless of the platform being used, it's still essential to download and install all security updates and patches, only choose apps that have strong user reviews, and protect the device with all password or biometric options available."

Device use in Australia



Windows wins with laptops and desktops while Apple wins with wearables

While Windows may not have a serious stake in the mobile technology market according to this survey, it still holds the majority of market share when it comes to laptops with 77 per cent of the market versus macOS, which has 21 per cent.

Desktop computers are even more Windows-centric at 85 per cent versus macOS with 13 per cent.

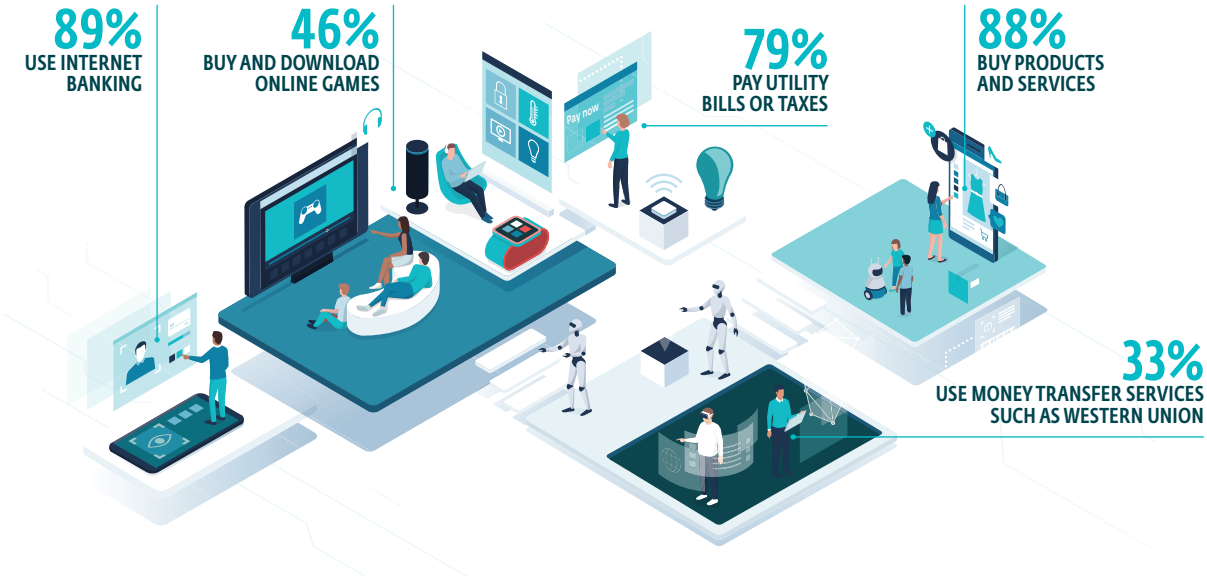
The operating systems underpinning smart home devices are more varied, with respondents to this survey claiming 44 per cent of their smart home devices are powered by Android, 28 per cent by iOS, and 10 per cent by Windows. However, it should be assumed that many respondents provided the OS of the device they use to control their smart home devices, rather than the OS of the devices themselves. Furthermore, 14 per cent of respondents said they didn't know what operating system their smart home devices used.

Apple wins again when it comes to wearable technology with 43 per cent of respondents with such devices versus Android's 37 per cent. Windows has six per cent while other operating systems account for seven per cent. Six per cent of respondents didn't know what operating system their wearable device used.

Nick FitzGerald said, "Wearable devices are as susceptible to malicious activity as any other connected device so it's important to install the regular updates from the manufacturer and ensure strong protection is in place when using these devices for sensitive purposes."

Whether they're aware of the risks or not, Australians conduct financial transactions online

Nearly all (94 per cent) of the survey respondents indicated that they conduct financial transactions online including online banking, paying bills, or online shopping. Breaking those numbers down:



Of these, 51 per cent of respondents said internet banking was the platform they used most, while 18 per cent said online shopping was the financial transaction they conducted the most.

Of those who shop for products and services online, 41 per cent did it a few times a month, 31 per cent did it a few times a week, 15 per cent did it a few times a year, and 11 per cent said they did it at least once a day.

When it came to paying bills online, 57 per cent did it a few times a month, 18 per cent did it a few times a week, and 17 per cent did it a few times a year.

Purchasing games online happened a few times a month for 30 per cent of respondents, a few times a year for 27 per cent, a few times a week for 24 per cent, and at least once a day for 10 per cent. Just nine per cent said they did it rarely.

Online money transfer services were used a few times a month by 28 per cent of respondents, a few times a week by 26 per cent, a few times a year for 21 per cent, and at least once a day for 14 per cent.

46 per cent of people said they logged into internet banking a few times a week, 26 per cent said they did it a few times a month, and 24 per cent said they did it at least once a day. Three per cent said they did it a few times a year and one per cent said they did it rarely.

Nick FitzGerald said, "When performing any kind of transaction online, it's essential for people to use the strongest protection possible. This means using strong, unique passwords and leveraging multifactor authentication and biometrics as much as possible. For devices without biometric capabilities and services without multifactor authentication options, users need to be especially vigilant about their passwords."

Online financial transactions are happening while people are on the move

People are overwhelmingly doing financial transactions from their smartphones (56 per cent) and laptops (21 per cent). Just 14 per cent use a desktop and nine per cent use a tablet.

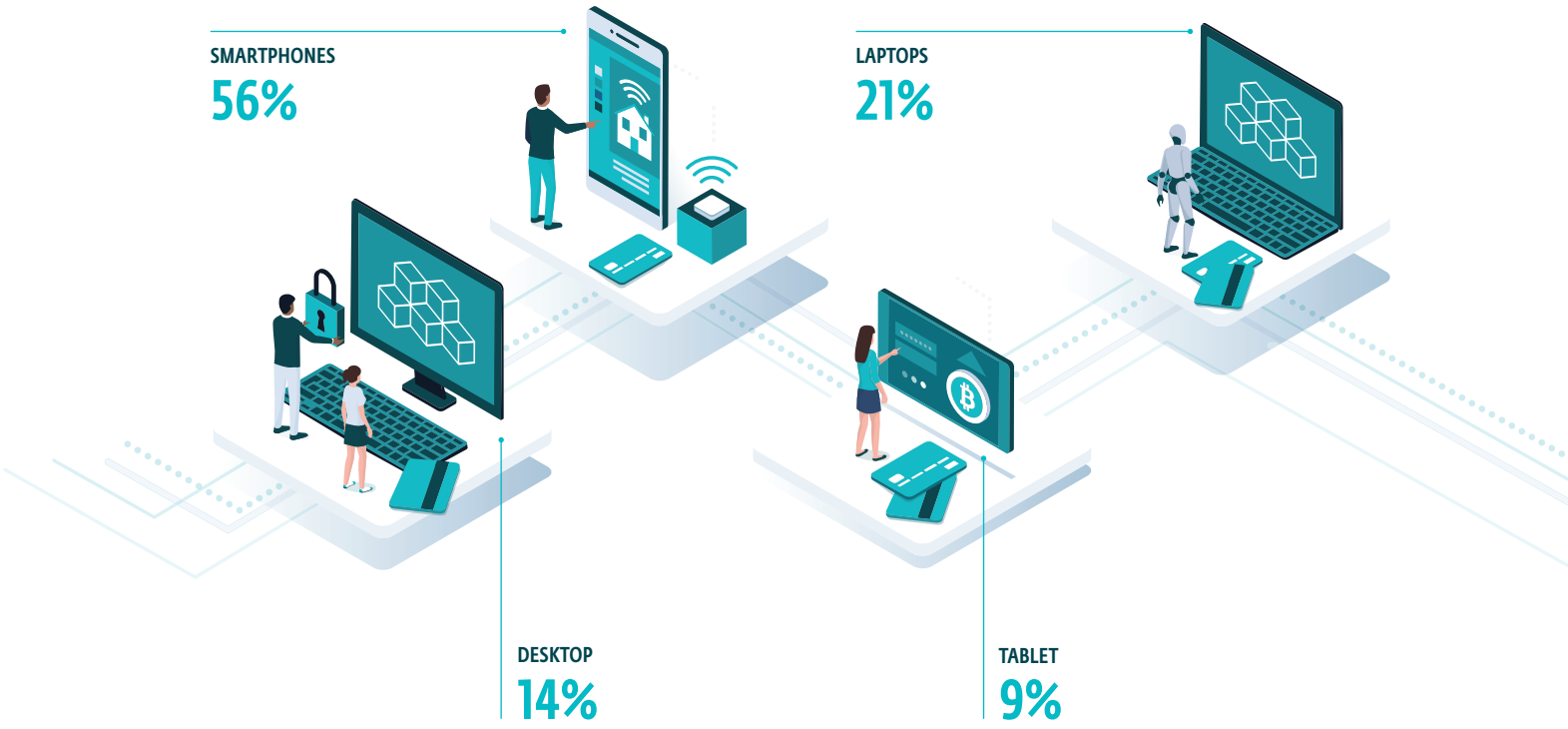
36 per cent use public Wi-Fi for online financial transactions often or occasionally. 26 per cent do it rarely and just 38 per cent said they never do it.

Nick FitzGerald said, "Public Wi-Fi is a security quagmire. It is very easy for bad actors to steal data, including account credentials, and to spy on users using public Wi-Fi. Often, they create a malicious Wi-Fi network that unsuspecting users connect to.

"For users that must connect to the internet while in public, it's much safer to use cellular data rather than public Wi-Fi. And, with unlimited data plans, this doesn't have to be prohibitively expensive. If travelling often, a mobile hotspot might be the economical solution for providing secure connectivity, especially for those carrying multiple Wi-Fi devices.

"Using public Wi-Fi for financial transactions is a recipe for disaster and should be avoided wherever possible. The risks are simply too high."

Financial transactions



People tend to stick to the platforms they know and trust

PayPal is the most common platform for financial transactions. 90 per cent of respondents said they used PayPal and only one per cent said they'd never heard of it. Meanwhile, 82 per cent said they used the official banking platform or app of their bank.

The next most popular payment platform was BPAY with 66 per cent of respondents saying they used it.

Apple Pay, Google Pay, and Android Pay are gaining in popularity with 43 per cent of people saying they used one of these platforms. 50 per cent of people said they'd heard of them but not used them. Seven per cent said they'd never heard of them.

Micro-investing apps (which round purchases up to the dollar and invest the extra funds in stocks), mobile payment apps, and WeChat Pay/Alipay had low awareness and weren't used by many people. Cryptocurrencies were relatively well known but unused by most respondents. And buy-now-pay-later platforms were used by 38 per cent of respondents and heard of by 56 per cent.

Nick FitzGerald said, "When using a payment app or platform, it's important for users to set unique, strong passwords. More complex passwords are better, within reason, and enabling multifactor authentication is better still. For users with numerous accounts, a password manager makes it easy to have strong, unique passwords while only having to remember a single password."

Apple Pay, Google Pay, and Android Pay users

43%
OF PEOPLE SAYING THEY USED ONE OF THESE PLATFORMS

50%
OF PEOPLE SAID THEY'D HEARD OF IT BUT NOT USED IT

7%
SAID THEY HAVE NEVER HEARD OF IT

People are aware of the risks they're taking but take them anyway

77 per cent of respondents worried about the security of their data either often or occasionally. A further 20 per cent worried rarely while only four per cent said they never worried. This is concerning, especially given the significant risks that people face when undertaking financial transactions online and using insecure connections through public Wi-Fi.

Fittingly, people are most worried about security when doing online banking (37 per cent) and online shopping (33 per cent). These numbers are on par with the results seen in the 2016 version of this survey. They're much less worried when paying bills or downloading games (just six per cent each).

Unfortunately, people are falling victim to security breaches. 20 per cent have had a virus, ransomware, or malware affect their devices, 18 per cent had a social media account compromised or hacked, and 15 per cent had their email compromised. More concerning was that 15 per cent of respondents had lost money to an online banking fraud or scam and 14 per cent had fallen victim to a fraud or scam received via their mobile phone.

Nick FitzGerald said, "There's a difference between a scam and a hack or malware. It's possible to put security tools in place that can limit the risks of a hack or malware taking hold. However, scams rely on social engineering or user naiveté to work and hence are not especially amenable to technical solutions, so it's essential for anyone who uses the internet to be aware of potential scams and know how to deal with them.

"Recognising a scam when it arises, such as through a phone call, text message or email, is the first step. Users should avoid clicking on links in emails or text messages, especially if those links require the user to enter their login details. If they receive a communication apparently from their bank or other organisation asking them to re-enter or confirm their login details, they should contact that organisation directly, not respond to the message itself, to confirm whether such a request is legitimate. And, users should always only type the website URL directly into their browser or use a bookmark they have already saved rather than click on links in messages. This avoids situations where they can be redirected to spoof sites designed to steal their details."

When it comes to a cybersecurity breach, 78 per cent of people are worried about losing money while 72 per cent are worried about identity or credential theft. 56 per cent are also worried about losing personal data and 37 per cent are worried about being locked out of online accounts. Just 17 per cent were concerned with losing sentimental data.

Victims of security breaches

20%
HAVE HAD A VIRUS, RANSOMWARE, OR MALWARE INFECTING THEIR DEVICES

18%
HAD THEIR SOCIAL MEDIA ACCOUNT COMPROMISED OR HACKED

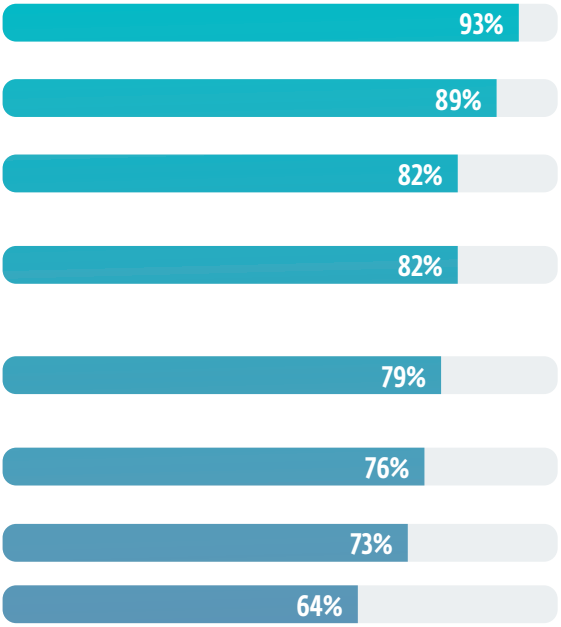
15%
HAD THEIR EMAIL COMPROMISED

15%
HAD LOST MONEY TO AN ONLINE BANKING FRAUD OR SCAM

14%
HAD FALLEN VICTIM TO A FRAUD OR SCAM RECEIVED VIA THEIR MOBILE PHONE

People are taking the risk seriously and trying to protect themselves

The vast majority of respondents were aware of the cybersecurity actions they could take:



93 per cent said they knew how to create **strong passwords** such as using pass phrases, not using publicly available information as passwords, etc.

89 per cent said they only **download software** and apps from official sources, which is down from 91 per cent in 2016.

82 per cent said they **disconnect all devices** from the internet immediately if they think there is a breach or virus infection

82 per cent said they have **different passwords** for different online accounts, which is a significant drop from the 2016 results, in which 94 per cent of respondents said they used different passwords for different accounts

79 per cent said they install **anti-virus and cybersecurity software** on their devices, a drop from 2016 when 86 per cent said they installed anti-virus and cybersecurity software on their devices

76 per cent said they **regularly updated the anti-virus** and other cybersecurity software on their devices

73 per cent said they use **two-factor authentication** whenever the option is available, compared with 89 per cent in the 2016 report

64 per cent said they **back up** their data regularly

More than half (54 per cent) of people say they know what they need to do to protect themselves online, and they make a conscious effort to improve their awareness. Others say they know what they need to do but they don't do it as it's too time-consuming or inconvenient (19 per cent), or they're just not that worried about the risks (14 per cent). Just 13 per cent of respondents claimed they didn't know what cybersecurity steps they needed to take to protect themselves online.

Nick FitzGerald said, "It's great to see that most people claim to be aware of what they need to do to protect themselves. However, it's worrying to see that these numbers have dropped compared with the survey results in 2016, which suggests that people may be becoming complacent.

"For those who know what to do but don't do it because it's time-consuming or inconvenient, the message is to invest a little bit of time upfront to save themselves a lot of hassle down the road. Taking a few moments to make all their passwords strong and unique (or set up a password manager) or to back-up their data, can mean that hackers fail to access their accounts, or that a ransomware attack is less devastating because the data is safe.

"For users that don't know what cybersecurity steps to take, it's important to proactively seek education and information to avoid becoming a victim."

People are taking responsibility for their own cybersecurity education

31 per cent of respondents said they hadn't received any cybersecurity education but they were interested in learning more because they believed it was very important. 35 per cent said they continuously educate themselves on what they need to do to stay safe online. 26 per cent said they received formal education from school or another educational institution and 17 per cent have a regular education and awareness campaign running at their workplace. Just 13 per cent have no interest in learning about cybersecurity.

Top tips for staying safe online

The risks of becoming a victim of a scam or cyberattack are growing all the time. Attackers are becoming more sophisticated and their methods are becoming harder to detect. That's why users must take all possible steps to protect themselves through security tools and safe behaviour based on awareness of the risks.

ESET's top tips for staying safe online are:

1. AVOID USING PUBLIC WI-FI

Users should avoid public Wi-Fi and use their mobile phone as a hotspot instead. However, if there is no alternative, users can connect to public Wi-Fi and use the following precautions:

- ensure the network is legitimate and not a spoof one designed to steal personal details
- use a laptop rather than a smartphone
- avoid conducting financial transactions including shopping online.

2. PROTECT DEVICES AND ACCOUNTS

Users should install appropriate security solutions on their home and work devices. They should:

- install updates and patches as soon as they're available
- use two-factor authentication and biometric protection
- always use strong and unique passwords.

3. BE AWARE OF SCAMS

Scams, including phishing, cost Australians money and can compromise their identity. People should:

- be on the lookout for potential scams and treat unsolicited emails and text messages with suspicion
- never click on links in emails or text messages or provide login details in response to such messages
- type the URL directly into the browser or use an existing bookmark to ensure they're accessing a legitimate site rather than a spoof site.

4. BEWARE OF CONDUCTING FINANCIAL TRANSACTIONS ONLINE

Online shopping and accessing banking and other financial details are risky when done in public or using an unsecured device. People need to:

- only use a secure connection (not public Wi-Fi) to access bank accounts or shop online
- shop only from official stores which have higher security settings
- use trusted payment platforms to avoid using bank accounts, but ensure those accounts are just as well-protected as bank accounts.

To learn more

Overall, Australian internet users are generally aware of the risks of online activities and are at least taking some steps to protect themselves. However, most users could potentially be more secure either through better password management or a clearer understanding of the risks, which would result in more cyber aware behaviour.

To report a cyberattack, go to:

www.cyber.gov.au/report

To learn more about how to stay safe online, go to:

www.eset.com.au

www.welivesecurity.com

ENJOY SAFER TECHNOLOGY™