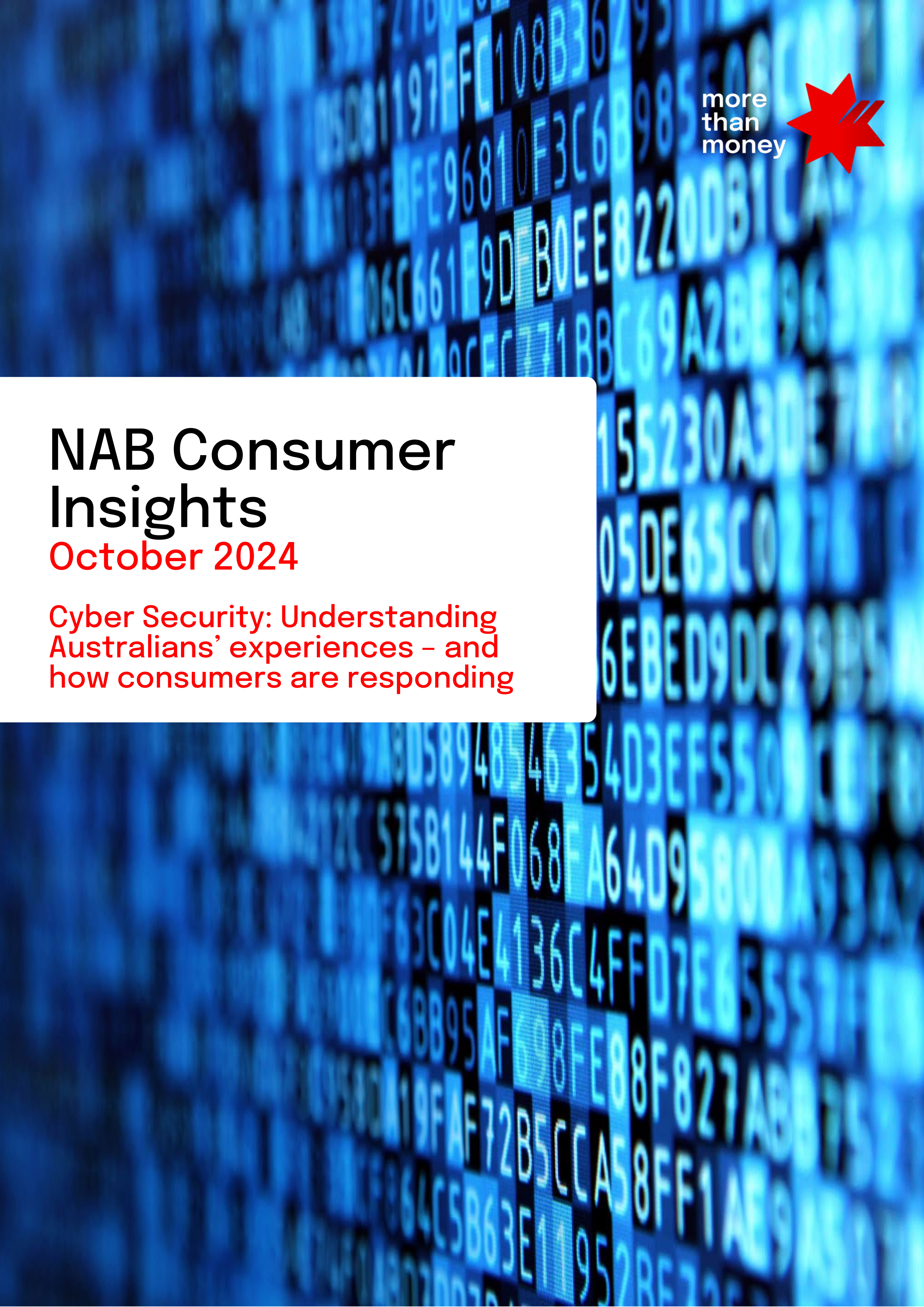


more
than
money

NAB Consumer Insights

October 2024

Cyber Security: Understanding Australians' experiences – and how consumers are responding

Key Findings

NAB research shows that cyber security is a critical, widespread issue for Australian consumers. Overall, the survey results show that almost two-thirds of consumers have experienced some sort of cyber security incident, with consumers of all ages and incomes affected. Consumers have a high level of concern about their cyber security, and while many are familiar with basic cyber security practices, many still don't know about or follow good practices all the time.

Phishing, breaches and hacks: consumer experiences

The survey examines the overall prevalence of cyber security incidents, who is most likely to be affected, and the different kinds of incidents that can occur. Key findings include:

- Almost two-thirds (63%) of consumers have experienced some kind of cyber security incident, with nearly half (44%) reporting they had experienced more than one event.
- Cyber security incidents are common across society, with a majority having experienced an incident across every age group and income group as well as both males and females.
- Being a victim of a data breach by an external company was the most common type of incident, affecting 38% of consumers, followed by being a victim of a phishing scam, affecting 34%.

Consumer cyber security habits and behaviours

The survey also examines consumers' levels of concern around cyber security, their familiarity with basic practices, and how they use these practices in the daily life to keep themselves safe. Key findings include:

- Almost all consumers are at least somewhat concerned about their personal cyber security, with 62% reporting they are 'concerned' or 'very concerned' and a further 31% 'slightly concerned'.
- Most consumers (85%) say they are 'quite familiar' or 'very familiar' with basic cyber security practices, but only a few (16%) say they follow good practices all the time.
- Nearly one in five consumers (18%) are still using simple passwords for some or all their online accounts, and only around a third of consumers (36%) use a password manager or browser to store and manage their passwords.
- More than a quarter of consumers (27%) rarely or never back up their important data such as photos and documents, and around one in five (21%) do not always update software and apps straight away.
- A quarter of consumers sometimes access online banking through public Wi-Fi networks, with most of these consumers not regularly using a VPN when doing so.

Survey background

These results are based on a survey of 1,038 Australian consumers conducted over the course of August and September 2024.

Scams, breaches and hacks: consumer experiences

In simple terms, cyber security involves the protection of computer systems connected to the Internet. Entities such as government, business and organisations, as well as millions of consumers in Australia rely on these connections every day. As the threat of cyber-crime continues to escalate in Australia, greater awareness and preventative measures are crucial.

According to the latest Australian Annual Cyber Security (ACSC) Threat Report 2023, Australia saw an increase in the number and sophistication of cyber threats. A range of malicious cyber actors showed the intent and capability needed to compromise vital systems, and Australian networks were regularly targeted by both opportunistic and more deliberate malicious cyber activity. The ACSC received nearly 94,000 cybercrime reports, up 23% on the previous year. This equates to one report every six minutes on average, an increase from one report every seven minutes in 2021-22.

In the first part of this report, we explore the prevalence of cyber security incidents including scams, data breaches, hacking and computer viruses in the community. The results show that these events are widespread, with a majority of consumers reporting they or a member of their household have been a victim. Moreover, cyber security incidents do not discriminate with consumers of all ages and income levels affected.

Prevalence of cyber security incidents

To get a picture of the prevalence of cyber security incidents in the community, we asked consumers if they or a member of their household had ever experienced an incident – such as being a victim of a scam, having personal data stolen due to a data breach at an external company, having a computer or online software hacked or accessed by an unauthorised person, or had a computer virus or malware attack.

Overall, almost two thirds (63%) of consumers reported they had experienced an incident of some kind, with 44% reporting they had experienced more than one cyber security event (either multiple events of the same type, or events of different types) (**Chart 1**).

The rates at which consumers have experienced cyber security incidents are strikingly similar across different groups (**Chart 2**). For example, 64% of males and 61% of females reported experiencing at least one incident. Likewise, the prevalence of incidents ranged from 55%-72% across different age groups, with 18-24 year olds reporting the lowest frequency and 25-34 years olds reporting the highest.

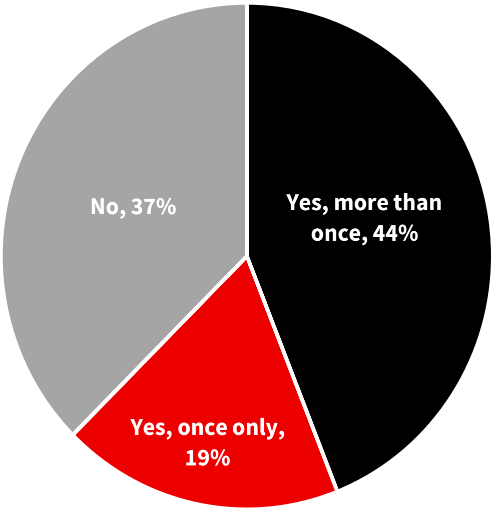
We also compared results across households of different incomes, again finding similar prevalence of cyber security incidents regardless of income. Overall, 64% of households with income over $100k reported experiencing some at least one incident, only marginally higher than households with incomes of $50k-$100k (62%) and those under $50k (61%).

In terms of the types of cyber security event experienced, the most common was being affected by a data breach of an external company, with 38% of consumers reporting this had happened to them including 18% who reported being affected more than once (**Chart 3**).

Data breaches were most commonly reported by those aged 25-34 (50%) and 35-44 (47%), and least common among those aged 65+ (21%). Data breaches were also reported relatively more by consumers in higher income households (45% for those with household income over $100k).

The next most common type of incident was being a victim of a scam, with 34% of consumers reporting this had happened to them including 13% who reporting being affected more than once.

Chart 1: Overall – have you or someone in your household ever experienced a cybersecurity incident?



Being a victim of a scam was most commonly reported by those aged 25-34 (43%) and was less commonly reported by those aged 55-64 (25%) and 65+ (28%).

Some 30% of consumers reported they had had a virus or malware attack their computer, with 14% saying this had happened more than once. This issue was again most commonly reported by the 25-34 age group. Less frequent, but still common was having a computer or online software hack or accessed by an unauthorised person, which was reported by 17% of consumers. Younger and lower income groups were again somewhat more likely to be affected by this kind of incident. **Table 3**, below, provides more details on the prevalence of each type of incident across different groups.

Chart 2: By demographic – have you or someone in your household ever experienced a cyber security incident?

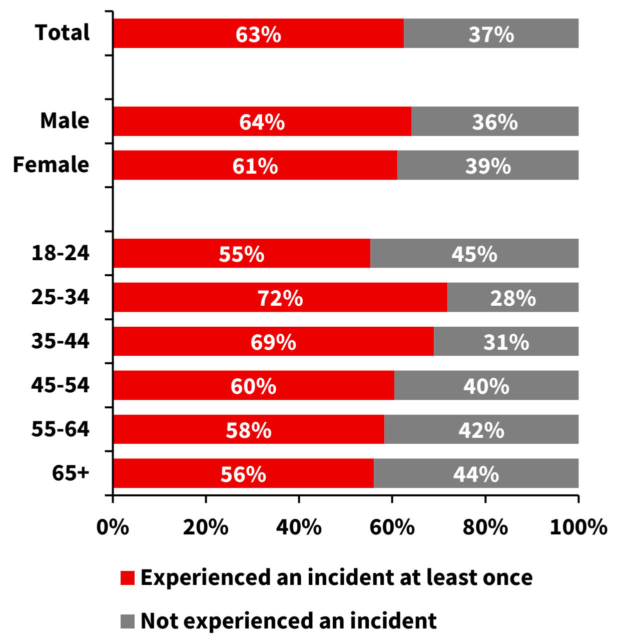


Chart 3: By type of incident – have you or someone in your household ever experienced a cyber security incident?

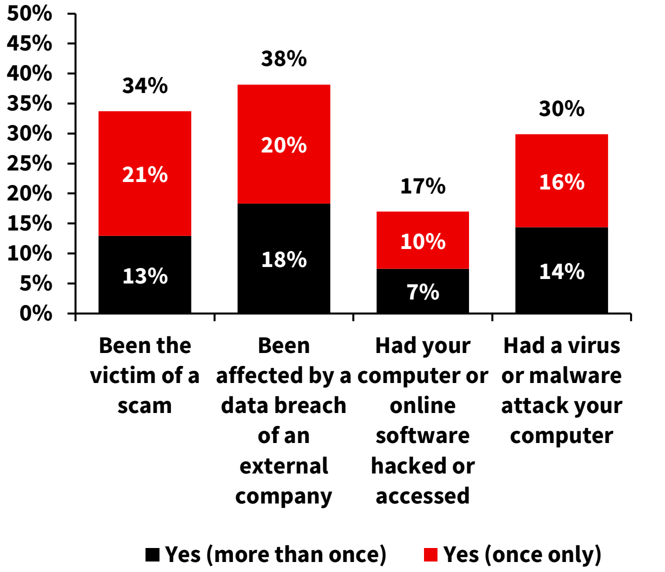


Table 1: Detailed results – have you or someone in your household ever experienced a cyber security incident?

	Total	Male	Female	By Age						Houshold Income		
				18-24	25-34	35-44	45-54	55-64	65+	<$50k	$50k-100k	>$100k
Been the victim of a scam	34%	35%	33%	33%	43%	35%	34%	25%	28%	38%	35%	31%
Been affected by a data breach of an external company	38%	37%	39%	31%	50%	47%	42%	34%	21%	32%	36%	45%
Had your computer or online software hacked or accessed	17%	18%	16%	24%	29%	16%	10%	8%	14%	24%	17%	14%
Had a virus or malware attack your computer	30%	33%	26%	27%	44%	29%	23%	25%	27%	33%	35%	25%
Total, any incident	63%	64%	61%	55%	72%	69%	60%	58%	56%	61%	62%	64%

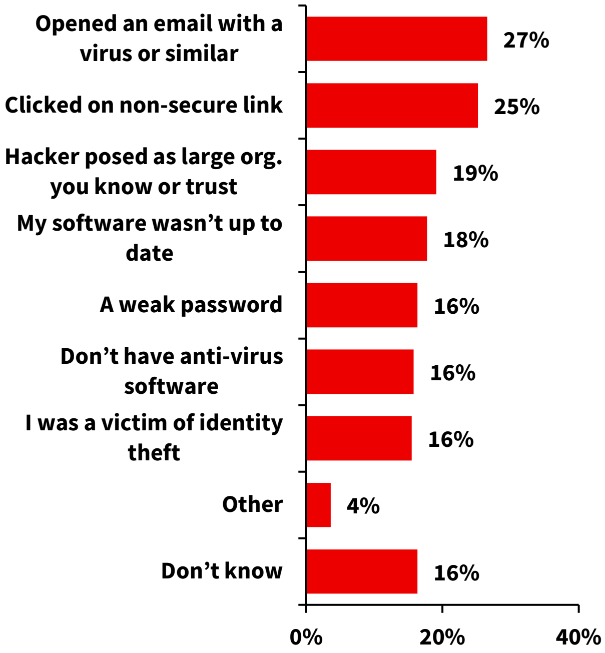
Causes of hacking and virus incidents

Where consumers reported they had been the victim of a hacking event or a virus, we asked what caused the issue to occur (**Chart 4**). Top of the list were opening an email with a virus (27%) and clicking on a non-secure link (25%), while many also reported that a hacker had posed as being from a large organisation that the respondent knew or trusted (19%). Out of date software, weak passwords or a lack of anti-virus software were also common issues.

In many respects, these answers highlight that there are many simple habits and behaviours that, if followed, can help consumers to protect themselves from cyber security incidents. In part two of this report, we explore these habits and behaviours in more detail.

16% of consumers said they didn't know what had caused the incident to occur – and while there were few significant differences across groups overall in terms of causes, there was a clear trend that older groups were more likely to respond that they didn't know the cause including 29% of those aged 65+ and 26% of those aged 55-64.

Chart 4: If you were a victim of a hacking or virus, what caused the cyber security incident?



Consumer cyber security habits and behaviours

In simple terms, cyber security involves the protection of computer systems connected to the Internet. Entities such as government, business and organisations, as well as millions of consumers in Australia rely on these connections every day.

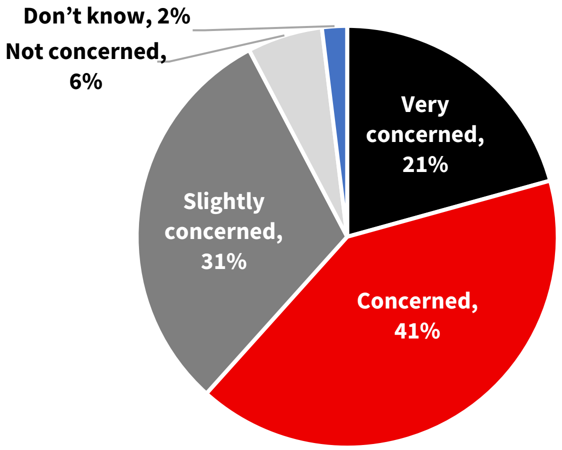
In the second part of this report, we look at the habits and behaviours of consumers as they relate to cyber security. The results show that most consumers are concerned about their personal cyber security, and many are trying to maintain good cyber security practices. However, there are still many consumers who are not following best practices everywhere that they can, which suggests there is more to do to educate consumers on this critical issue.

Overall personal cyber security concerns

Unsurprisingly given the widespread prevalence of cyber security incidents highlighted above, there is a high level of concern about cyber security among consumers. In the survey, a total of 62% of respondents said they were either 'concerned' or 'very concerned' about their personal cyber security, while a further 31% were at least 'slightly concerned' (**Chart 6**).

The data suggests that experiencing a cyber security incident increases consumers' level of concern. Overall, 68% of consumers who reported they had experienced an incident said they were 'concerned' or 'very concerned', compared to 50% among those who had not experienced an incident.

Chart 6: How concerned are you about your personal cyber security?



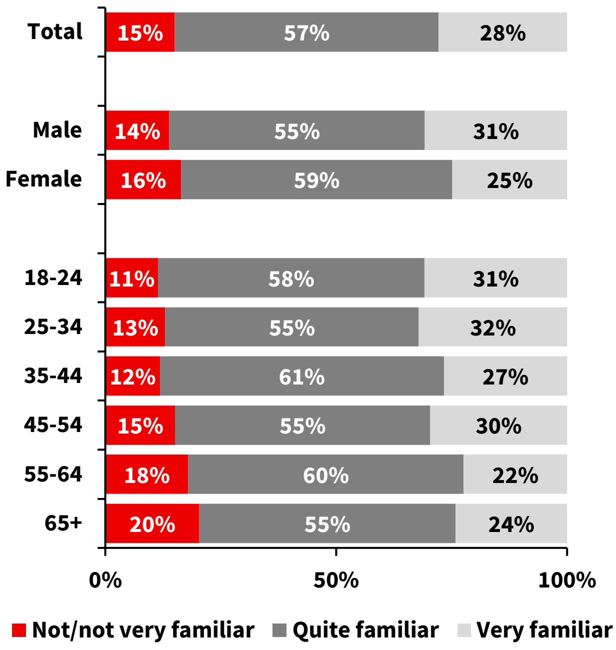
Familiarity & use of basic cyber security practices

As highlighted above, many cyber security incidents can be the result of simple things such as clicking on a non-secure link – so using basic practices such as using unique and complex passwords, installing anti-virus software and backing up data are important to stay safe. But do consumers know about these practices, and if they do, are they using them?

When asked about their familiarity with basic cyber security practices, 28% said they were 'very familiar' and a further 57% said they were 'quite familiar', leaving just 15% who said they were 'not at all' or 'not very' familiar (**Chart 7**).

Familiarity with basic cyber security practices was similar across males and females, but there was a clear trend across age groups. The share of respondents not familiar with basic practices was as low as 11% for those aged 18-24, rising across older age groups to as high as 18% for those aged 55-64 and 20% for those aged over 65.

Chart 7: How familiar are you with basic cyber security practices?



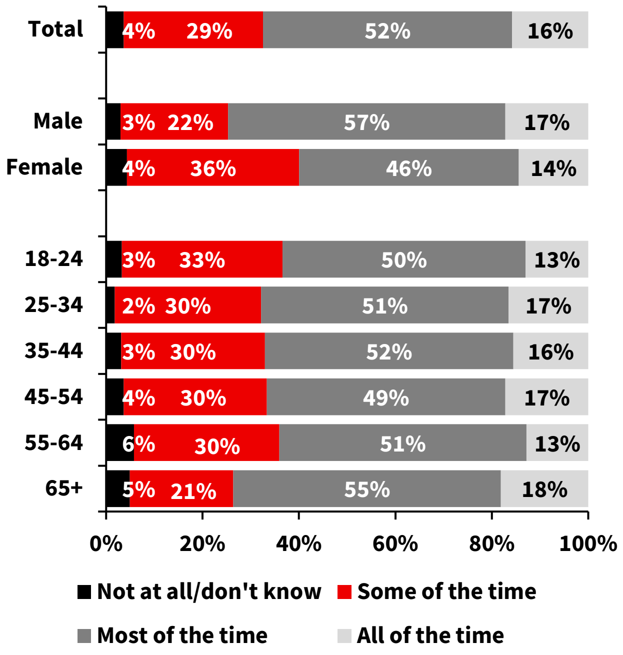
Of course, sometimes we might know we should do something, but that doesn't mean we do it all of the time. Despite most respondents saying they were at least 'quite' familiar with basic cyber security practices, only a small number – just 16% – say they follow good practices 'all the time' (**Chart 8**).

Around half (52%) say they follow good practices 'most of the time', leaving around a third of consumers who only do so 'some of the time' (29%) or even 'not at all' (3%), while 1% say they simply 'don't know'.

Interestingly there is a bit of a difference in this area across males and females, with only 60% of females saying they follow good practices 'most' or 'all of the time', compared to 75% of males.

There were also some differences across age groups. Despite the youngest group having the best familiarity with basic practices, they were the least likely to follow them with only 63% saying they followed good practices 'most' or 'all of the time'. At the other end of the spectrum, despite having the lowest familiarity, some 74% of those aged over 65 claimed they used good practices 'most' or 'all of the time'.

Chart 8: How often do you believe you follow good cyber security practices?



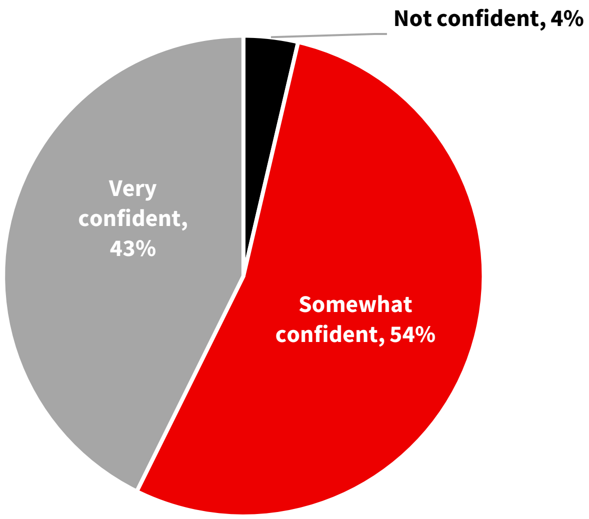
Identifying phishing emails and scam messages

Phishing scams involve criminals contacting people through phone calls, text or email, pretending to be from trusted businesses, government departments, and sometimes family and friends. Their goal is to trick unsuspecting people into handing over their personal information and stealing their money or identity. Phishing is one of the most common ways that cyber security incidents can occur. The first defence against phishing is knowing how to recognise the red flags. For example, checking the sender's address for unusual or misspelled formatting and taking time to stop and check the legitimacy of communications when it creates a sense of urgency (example – an email that encourages you to click a link or download an attachment to avoid a problem).

The good news is that the vast majority of consumers surveyed reported they had at least some degree of confidence in identifying phishing emails and scam messages. However, only 43% – less than half – said they were 'very confident'. A further 54% said they were 'somewhat confident', while 4% said they were 'not confident'.

Confidence identifying phishing was very similar across groups including across males and females and age groups. However, the share of those 'not confident' was a little higher among those aged over 65, at 8%.

Chart 9: How confident are you in identifying phishing scams (emails, text, phone call, etc.)?



Logging in: authentication and password security

From banking and email to social media, online accounts are a ubiquitous part of everyday life, which makes logging in securely a key part of cyber security. But how are consumers managing the login process?

One of the most secure ways to log in to an account is to use multi-factor authentication (MFA). Among surveyed consumers, 31% said they do so for all accounts where it is enabled, while a further 62% said they use it for at least some accounts (**Chart 10**).

In terms of passwords, more than half of consumers said they use unique, complex passwords or passphrases for either everything (27%) or at least important accounts (31%) (**Chart 11**). Another quarter (25%) use a complex password but rely on the same one for most or all accounts.

Overall, this suggests more than 80% of consumers use complex passwords or passphrases – up from 40% who said they used complex passwords in the 2023 survey.

Of more concern, 8% use unique but simple passwords for everything and a further 5% use unique, simple passwords only for important accounts. Finally, 5% of consumers say they use the same simple password for most or all accounts.

How we manage and remember passwords is also important (**Chart 12**). Surprisingly, around half of consumers say they 'just remember them' – which likely makes it harder to use unique and complex passwords in most cases. This approach was much less common among those over 65.

Many say they write them down, either on a piece of paper (30%) or a digital note (15%) – which can be more of a security risk. Only a reasonably small share of respondents use software to help, such as storing passwords in a browser (17%) or using a password manager (19%).

Chart 10: Do you use multi-factor authentication for any of your online accounts where it's enabled?

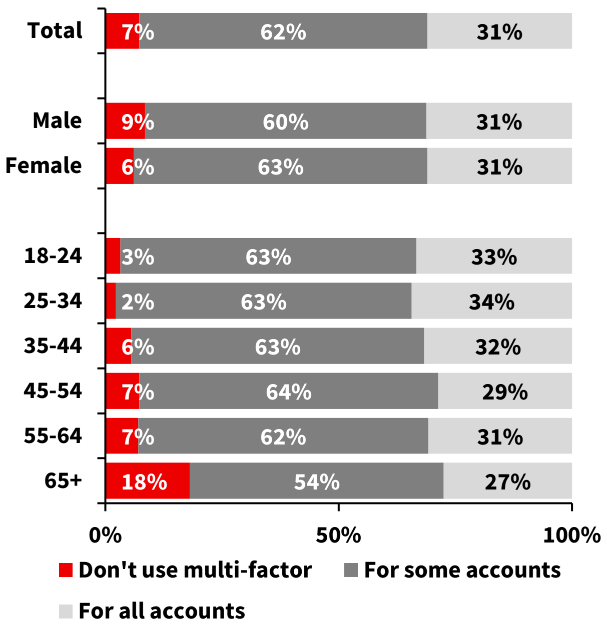


Chart 11: Which of the following best describes how you use passwords?

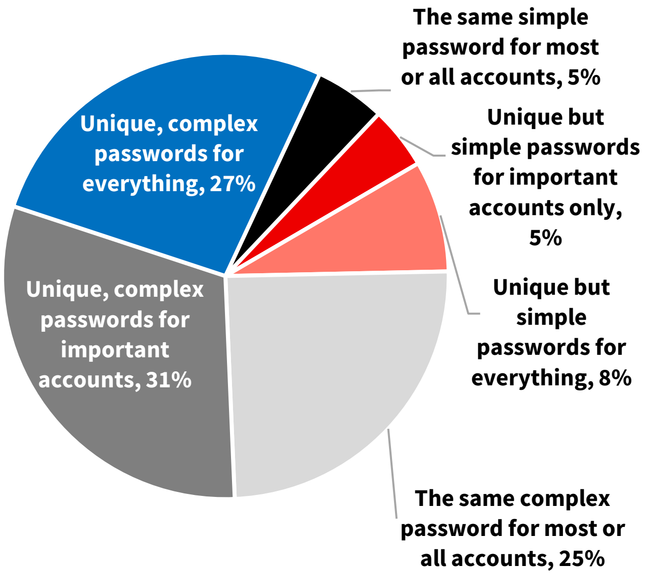
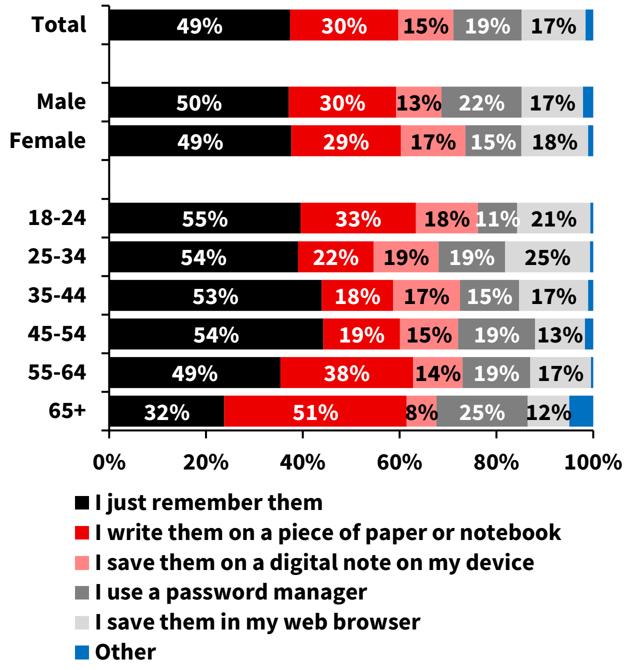


Chart 12: How do you remember your passwords?



Data backups and software updates

Another key form of defence against cyber security is how we manage our software and data storage. For example, backing up important data regularly can help ensure photos and documents are safe in the event of a cyber security incident such as a hacking or virus.

When asked, 30% of surveyed consumers said they regularly (weekly or monthly) back up their important data and a further 43% said they did so occasionally (every few months) (**Chart 13**). This suggests data backups may have become more common practice since our 2023 survey, when only 31% of consumers said they had backed up data to the cloud in the past 12 months.

Still, not everyone is backing up their data that often. In total, more than a quarter said they did so rarely (21%) or never (6%), leaving these consumers at risk.

Frequency of backing up data was slightly higher among males, with 34% backing up data 'regularly' compared to 25% for females. By age group, backing up 'regularly' was most common among the oldest cohort (40%) and least common amongst the youngest (21%). At the same time, older groups were also slightly more likely to say they never back up important data.

Regularly updating software and apps to the latest versions – including updating anti-virus software – is another key strategy for managing cybersecurity risks.

In our 2023 survey, 56% of consumers said they 'keep mobile devices and apps updated' but in this survey we dug deeper into how consumers actually manage their software updates.

The results find only half (49%) of consumers surveyed said they have automatic updates turned on, ensuring software is always up to date (**Chart 14**). A further 24% said they update their software and apps themselves as updates become available.

A smaller number of consumers said they update apps manually, but usually wait for a period of time to make sure they don't have errors (11%), while 10% said they only update their apps and software 'sometimes'.

Males were slightly more likely to report that they have automatic updates turned on or update straight away, at a combined 78% compared to 67% for females.

There were even clearer differences across age groups. Younger groups were significantly less likely to rely on automatic updates – around 40% for 18-24 and 25-34 year olds, compared to around 60% for 55-64 year olds and those over 65.

Younger groups were the most likely to wait to install updates to avoid errors, with 21% of 18-24 year olds and 15% of 25-34 year olds taking this approach compared to 11% or less among older age groups. Still, the share that reported they 'only update sometimes' was similar across groups at around 10%.

Chart 13: How often do you back up your important data (e.g., photos, documents)?

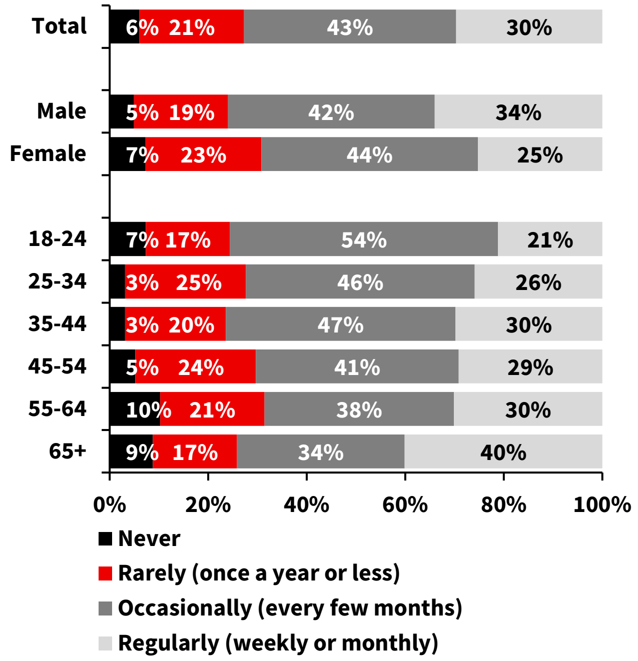
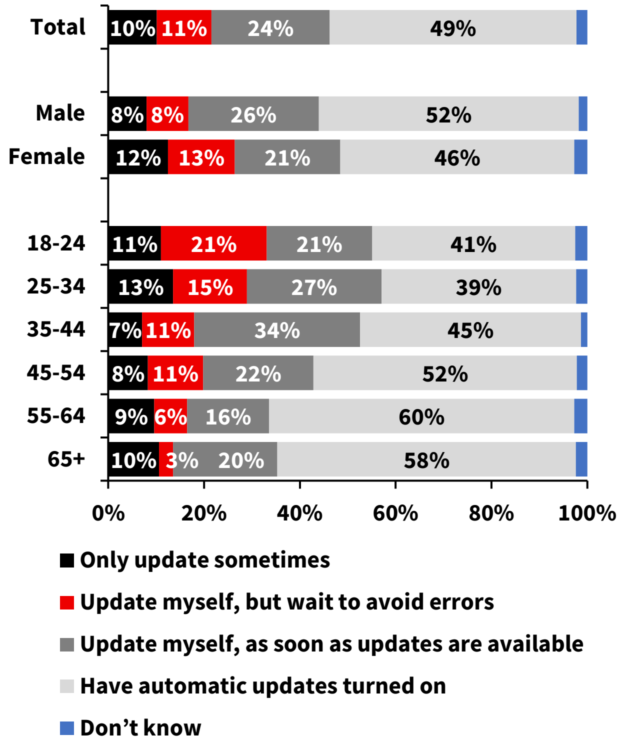


Chart 14: Do you regularly update the software and apps on your devices to the latest versions?



Using public Wi-Fi networks

Public Wi-Fi networks can pose a risk as data can be intercepted by criminals on unsecured networks. In the survey, 70% of respondents said they avoid using public Wi-Fi to access their online banking, but a quarter said they did so 'occasionally' or even 'frequently' (Chart 15).

Using a public Wi-Fi network for online banking was most common among younger groups, including those aged 25-34 (42% either 'occasionally' or 'frequently') and those aged 18-24 (38%). By contrast, just 7% of those over 65 reported that they do so, with the vast majority of older consumers saying they avoid doing so.

For those consumers who do use public Wi-Fi to access online banking, a key tool can be to use a Virtual Private Network (VPN), available through a VPN provider. A VPN hides your real location by masking your IP address and encrypts your internet traffic, making it much harder for anyone to see what you're doing or to steal your data. It's like sending your information through a secure tunnel that no one else can look into. In the survey, 27% said they use a VPN frequently when doing so (**Chart 16**) – up from 18% in the 2023 survey. However, this still leaves some 29% who said they don't use a VPN when using public Wi-Fi to access online banking, while 37% said they only do so 'occasionally'.

Chart 15: Do you use public Wi-Fi networks to access your online banking?

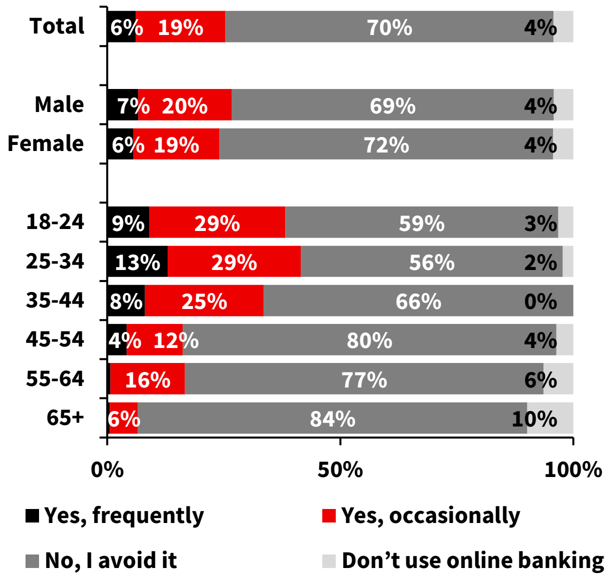
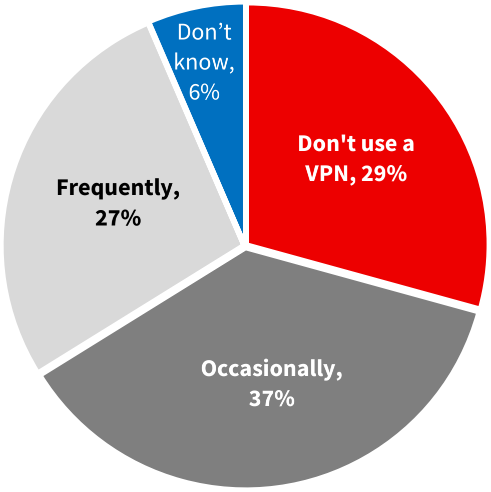


Chart 16: When using a public Wi-Fi network to access your online banking, do you use a VPN?



Important Notice

This document has been prepared by National Australia Bank Limited ABN 12 004 044 937 AFSL 230686 ("NAB"). Any advice contained in this document has been prepared without taking into account your objectives, financial situation or needs. Before acting on any advice in this document, NAB recommends that you consider whether the advice is appropriate for your circumstances.

NAB recommends that you obtain and consider the relevant Product Disclosure Statement or other disclosure document, before making any decision about a product including whether to acquire or to continue to hold it.

Please click **here** to view our disclaimer and terms of use.

Media contact

NAB Media
nab.media@nab.com.au
+61 (0) 3 7035 5015