NAB Consumer & Business Insights

September 2023

Scams: Education, training & slower payment processing to minimise scams and cybersecurity risks

Key Findings

NAB research shows consumers and businesses are increasingly prepared to make trade-offs for greater protection from scams. Over 4 in 10 Australian consumers would be "extremely prepared" to experience slower payments processing if they were better protected from scammers, and 1 in 2 SMEs are "completely prepared" to sacrifice the time it takes to process a payment if it's safer. And, while over 4 in 10 Australians are being very proactive in getting educated about scams, just 15% of Australian SMEs conduct extensive training around scams and other cybersecurity risks.

Australian Consumer Viewpoints

What actions do Australians think are most effective in stopping them from being scammed? Around 3 in 4 believe not opening suspicious texts, pop-up windows or clicking on links or attachments in emails and keeping their personal details secure are most effective. 2 in 3 also believe keeping mobile devices and computers secure, never sending money, credit card and online account details or copies of personal documents to anyone they don't know, not responding to phone calls about their computer asking for remote access, being careful when shopping online, being more alert to the fact scams exist, being wary of unusual payment requests, and choosing passwords difficult for others to guess and updating them regularly are also most effective. Only 1 in 2 think reviewing privacy and security settings on social media would keep them safe.

Are Australian consumers proactively getting educated about scams? They are being "quite" proactive, scoring a solid 6.9 pts. Encouragingly, over 4 in 10 were "very" proactive, with fewer than 1 in 10 "not very" active. The extent Australians were being proactive increased with age irrespective of gender (rising from 5.9 pts for men 18-29 to 7.7 pts for men over 65, and 5.9 pts for women 18-29 to 7.6 pts for women over 65). Women and men in the same age groups scored proactiveness broadly the same. The number who scored "high" levels of proactiveness increased sharply with age - it doubled from 29% for men 18-29 to 59% for men over 65, and from 30% for women 18-29 to 57% for women over 65.

Are Australian consumers prepared to experience slower payments processing if they were better protected from scammers? They are "quite" prepared to, scoring 6.9 pts out of 10. Over 4 in 10 Australians are also "extremely" prepared to do so, and fewer than 1 in 10 "not very" prepared to. Women scored higher than men in all age groups except the 50-64 group. The number of people who scored "high" increased significantly with age - from around 1 in 4 in 18-29 age groups to around 2 in 3 in over 65 age groups. Willingness to sacrifice convenience for security rated a little higher in rural areas (7.0 pts) than in capital and regional cities (6.9 pts), with more consumers in rural areas (47%) "extremely" prepared to experience slower payment processing times than in regional and capital cities (43%).

Australian SME Viewpoints

To what extent does business conduct training around scams & other cybersecurity risks? Not very extensively, scoring on average just 3.6 pts out of 10. Only 15% of SMEs overall said they conduct extensive training around scams and other cybersecurity risks, and 4 in 10 not much training at all. Training rated quite low in most states, ranging from 3.8 pts in WA to 3.3 pts in SA. TAS was the outlier (5.6 pts) but from a smaller sample size. Over 4 in 10 SMEs in SA, NSW and VIC did not do much training at all. By industry, training was highest in the Finance & Insurance sector (6.6 pts), with over 4 in 10 firms conducting extensive training. Accommodation & Hospitality firms were least likely to have conducted scams training (2.0 pts), with only 1 in 20 firms conducting extensive training. At the other extreme, over 1 in 2 firms in Construction and Transport & Storage did not conduct much training at all.

Where are SMEs sourcing their information & training about scams and cybersecurity risks? The 3 most widely used sources are industry associations (57%), bank websites and messaging (53%) and external consultants or experts (51%). Around 1 in 3 rely on government websites, 1 in 4 social media and internal IT consultants and experts, and 1 in 5 their telecommunications provider. Around 1 in 20 don't get any information or training at all. Around 8% of SMEs in QLD did not get any information on training - double the number in NSW and VIC (4%). Key disparities by industry included a much higher number in Accommodation & Hospitality (81%) and Finance & Insurance (77%) sourcing information from industry associations, significantly more in Construction and Transport & Storage (64%) from bank websites and messaging, and in Finance & Insurance (79%), Health (74%) and Business Services (67%) external IT consultants and experts. Sourcing information from social media was much more common in Construction (36%), Transport & Storage (36%) and Retail (33%), particularly when compared to Finance & Insurance (9%). Interestingly, we noted a much higher number of Finance & Insurance firms who don't get any information or training (14%) than any other sector.

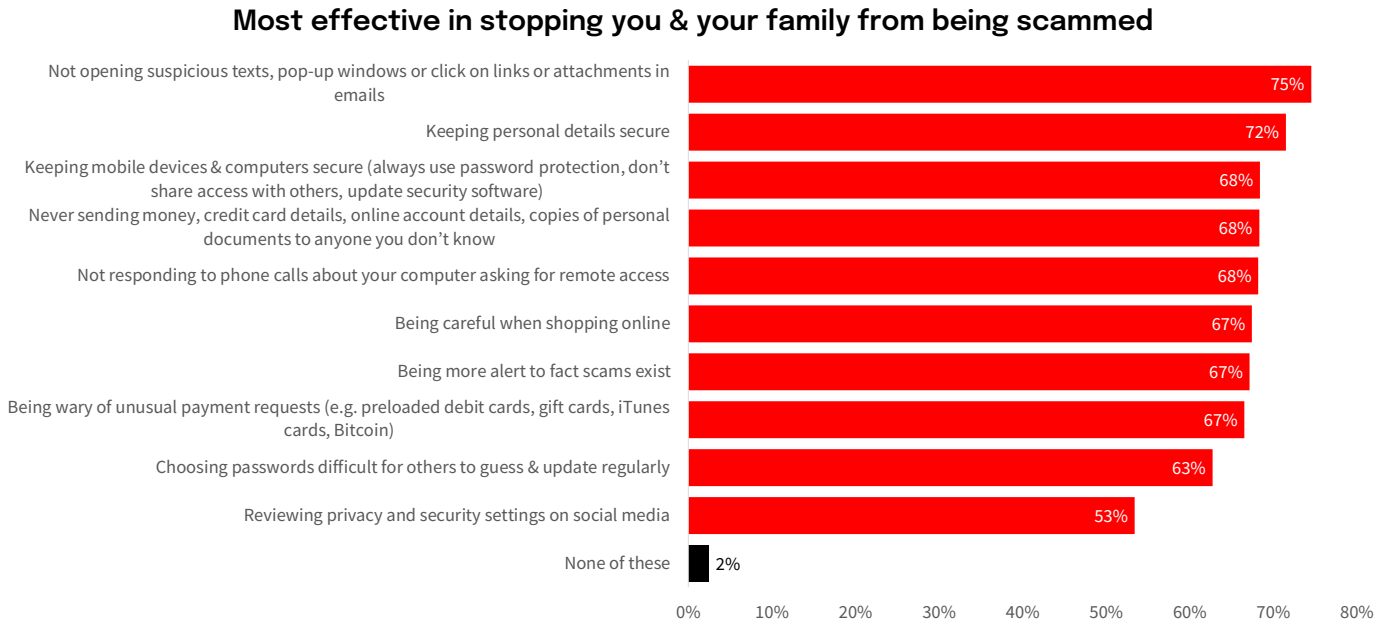
To what extent are SMEs prepared to sacrifice the time it takes to process a payment if it was ultimately safer? Support for more checks and balances is quite solid, with SMEs on average scoring 6.7 pts (only marginally lower than support for slower payments processing times by Australian consumers - 6.9 pts). Support was relatively strong across key states (ranging from 6.9 pts in SA to 6.4 pts in QLD) but fluctuated widely by industry (ranging from 7.9 pts in the Finance & Insurance sector to just 3.7 pts in Accommodation & Hospitality). The survey also found that 1 in 2 SMEs "very highly" prepared to sacrifice the time it takes to process a payment if it was ultimately safer, with this number ranging from 56% in SA to 50% in QLD and TAS, and nearly 7 in 10 in the Finance & Insurance sector to around 3 in 10 in Accommodation & Hospitality.

Scams: The view from consumers

A scam is a fraudulent invitation, request, notification or offer designed to obtain personal information or money or obtain a financial benefit by deceptive means. Due to the deceptive nature of scams, people may not always be aware they have been exposed to or responded to a scam. According to Personal Fraud data released by the Australian Bureau of Statistics (ABS) in February 2023, around two-thirds (65%) of Australians over the age of 15 (13.2 million people) were exposed to a scam in the 2021-22 financial year, up from 55% in the previous financial year. As the threat of being scammed continues to escalate, greater awareness and preventative measures are crucial.

In this section, NAB explores what Australian consumers believe would be most effective in stopping them and their family from being scammed. We also explore the extent Australians are being proactive in getting educated about scams, and if they are prepared to experience slower payments processing if they were better protected from scammers. The findings are based on survey responses from over 2,000 Australian consumers over the period 15 May to 6 June 2023.

In section 2, NAB explores the extent Australian SMEs conduct training around scams and other cybersecurity risks, where they currently source their information about these risks, and the extent they are prepared to sacrifice the time it takes to process a payment if it was ultimately safer. The findings are based on survey responses from around 760 SMEs over the period 22 May to 8 June 2023.



Most effective in stopping you and your family from being scammed…

There a numerous actions Australians can take to avoid being scammed. When Australian consumers were asked what actions, they thought would be most effective to protect them from being scammed, the survey revealed very strong consensus about what would help most people.

Overall, around 3 in 4 Australians overall believe not opening suspicious texts, pop-up windows or clicking on links or attachments in emails (75%) and keeping their personal details secure (72%) are the most effective actions they could take from being scammed.

Around 2 in 3 also believe keeping mobile devices and computers secure (68%), never sending money, credit card details, online account details or copies of personal documents to anyone they don't know (68%), not responding to phone calls about their computer asking for remote access (68%), being careful when shopping online (67%), being more alert to the fact scams exist (67%), being wary of unusual payment requests (67%), and choosing passwords that are difficult for others to guess and updating them regularly (63%) are also effective. A somewhat lower 1 in 2 (53%) Australians thought that reviewing privacy and security settings on social media would keep them safe (53%).

Only 1 in 50 Australians believe that none of these actions would be effective (2%).

But what was considered most effective varied widely by region and by age & gender. By region, we noted a higher number of consumers living in rural areas who believe all these actions would be effective in helping them from being scammed, with responses lowest in capital cities for all actions. The gap was widest in relation to not responding to phone calls about their computers asking for remote access (rural area 78%; capital city 66%), reviewing privacy and security settings on social media (62% vs. 51%), changing passwords regularly (71% vs. 61%) and never sending money, credit card or online account details etc. to people they don't know (76% vs. 66%).

The survey also found a higher number of women who believed all these actions would be effective than men in all age groups with only two exceptions - being more careful when shopping online and being more alert to the fact that scams exist, where slightly men than women in the 50-64 age group said they would be most effective.

By age group, some key differences included the much higher number of women in the 18-29 group who said not opening suspicious texts, pop-up windows etc. would be most effective (79% women; 64% men), in the 30-49 age group more women not opening suspicious texts, pop-up windows etc. (70% women; 56% men), keeping mobile devices and computers secure (64% women; 52% men) and never sending money, credit card details etc. to people they don't know (60% women; 49% men), and in the 50-64 age group significantly more women who also said not opening suspicious texts, pop-up windows etc. (87% women; 75% men). Responses were more closely aligned in the 65 age group, with positive response rates for both men and women higher than their peers in all other corresponding age groups - see table below.

Most effective in stopping you and your family from being scammed

	All Australians	Capital City	Regional City	Rural Area	Men 18-29	Women 18-29	Men 30-49	Women 30-49	Men 50-64	Women 50-64	Men 65+	Women 65+
Not opening suspicious texts, pop-up windows or click on links or attachments in emails	**75%**	72%	78%	80%	64%	79%	56%	70%	75%	87%	86%	92%
Keeping your personal details secure	**72%**	70%	74%	76%	70%	72%	55%	64%	75%	79%	86%	87%
Keeping your mobile devices and computers secure	**68%**	67%	69%	74%	63%	69%	52%	64%	72%	76%	81%	84%
Not sending money, credit card, online account details, copies of personal docs to people you don't know	**68%**	66%	73%	76%	66%	72%	49%	60%	74%	76%	83%	87%
Not responding to phone calls about your computer asking for remote access	**68%**	66%	69%	78%	61%	63%	54%	57%	75%	80%	84%	90%
Being careful when shopping online	**67%**	65%	71%	74%	60%	69%	53%	60%	74%	72%	80%	86%
Being more alert to the fact that scams exist	**67%**	65%	71%	74%	62%	66%	50%	60%	74%	73%	82%	88%
Being wary of unusual payment requests (e.g. preloaded debit cards, gift cards, iTunes cards, Bitcoin etc.)	**67%**	65%	69%	71%	60%	69%	52%	58%	70%	72%	80%	86%
Choosing passwords that would be difficult for others to guess and update them regularly	**63%**	61%	65%	71%	56%	59%	50%	56%	66%	72%	76%	83%
Reviewing privacy and security settings on social media	**53%**	51%	57%	62%	51%	56%	42%	52%	56%	60%	56%	63%
Other	2%	3%	2%	1%	3%	1%	6%	2%	1%	1%	3%	1%

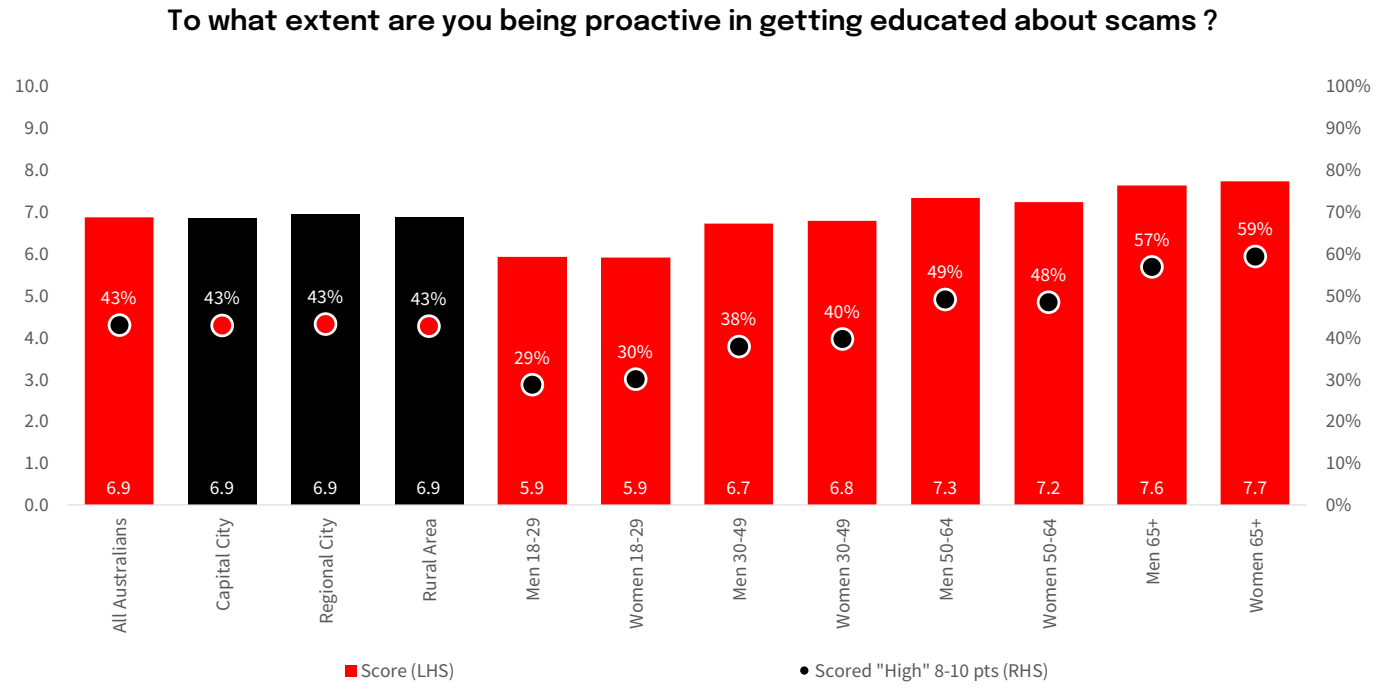
Proactively getting educated about scams

Anyone can fall victim to scams but being educated about the latest frauds and scams can help consumers become better equipped with tools to recognise potential red flags. When Australians were asked to score the extent they were being proactive in getting educated about scams, an average, they scored a relatively solid 6.9 pts out of 10. Encouragingly over 4 in 10 (43%) said they were being very proactive (i.e. scored 8 pts or higher), with less than 1 in 10 (9%) "not very" active (i.e. scored 3 pts or lower).

The extent Australians were being proactive about getting educated did not vary by region, with Australians in all areas scoring 6.9 pts and 43% scoring "high". The number that scored proactiveness "very low" was also broadly similar, ranging from just 8% in regional cities to 10% in rural areas.

The extent Australians were being proactive in getting educated about scams increased with age irrespective of gender - ranging from 5.9 pts for men 18-29 to 7.7 pts for men over 65, and from 5.9 pts for women 18-29 to 7.6 pts for women over 65. Women and men in the same age groups scored their proactiveness basically the same.

A much bigger gap was noted in the number of Australians who scored "high" levels of proactiveness. This also rose with age and doubled from 29% among men 18-29 rising to 59% of men over 65, and nearly doubled from 30% of women 18-29 to 57% of women over 65 - see chart below.

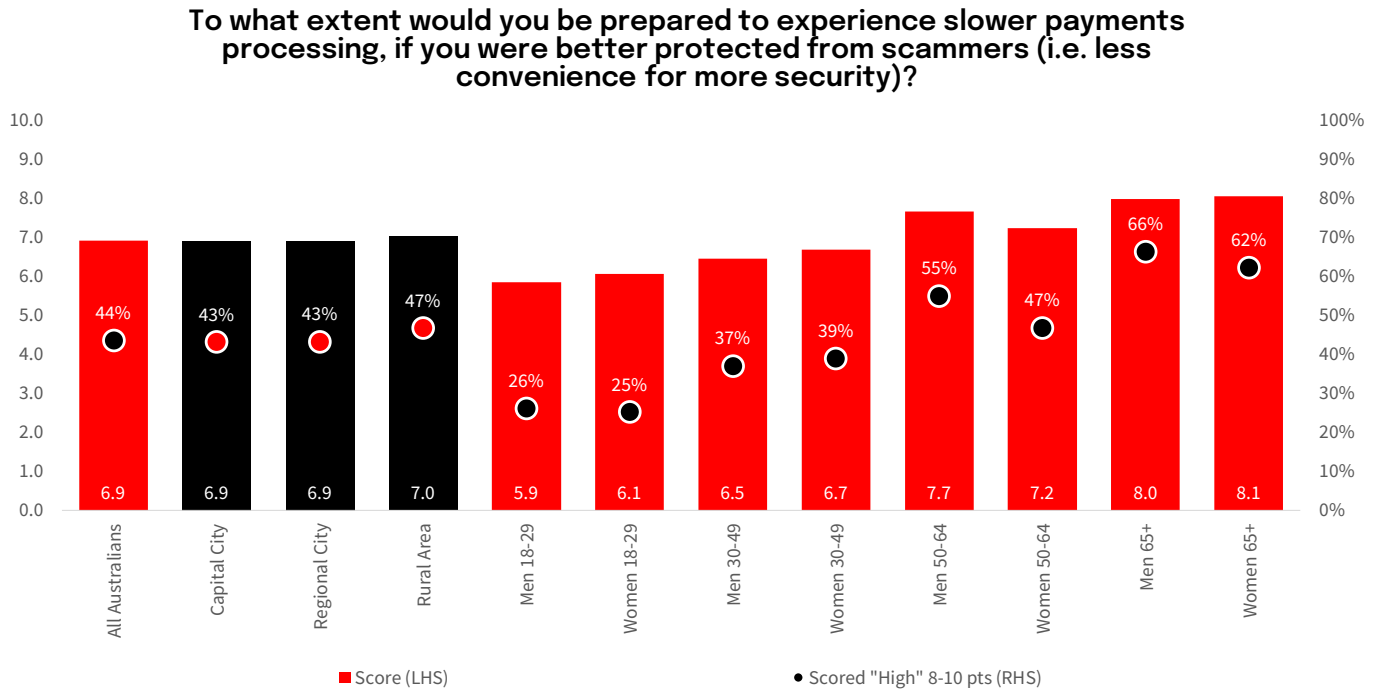


Less convenience for more security

Major Australian banks want to slow down the speed of some banking activity (including online payments) to ensure customers are kept safe from rising criminal activity targeting them. In this survey, we asked Australians to score the extent they would be prepared to experience slower payments processing if they were better protected from scammers - i.e. less convenience for more security. They indicated they were "quite" prepared to do so, scoring on average 6.9 pts out of 10, with over 4 in 10 "extremely" willing to do so (i.e. scored 8 pts or higher) and only 8% "not very" willing (i.e. scored 3 pts or lower).

Willingness to sacrifice convenience for security rated a little higher in rural areas (7.0 pts) than in capital and regional cities (6.9%), with more consumers in rural areas (47%) "extremely" prepared to experience slower payment processing times than in regional and capital cities (43%).

Less convenience for more security against scammers increased with age for both genders. Women scored higher in all age groups except the 50-64 group where the gap was also widest (men 7.7 pts; women 7.2 pts). The number of people who scored "high" increased significantly with age from around 1 in 4 in 18-29 age groups to around 2 in 3 in over 65 age groups.



Scams: The view from SMEs

Extent business conducts training around scams & other cybersecurity risks

Cybersecurity and scams training can help educate employees about the cybersecurity landscape. It can raise awareness of cybersecurity threats, reduce risks associated with cyberattacks and scams and help embed a culture of security compliance in their business.

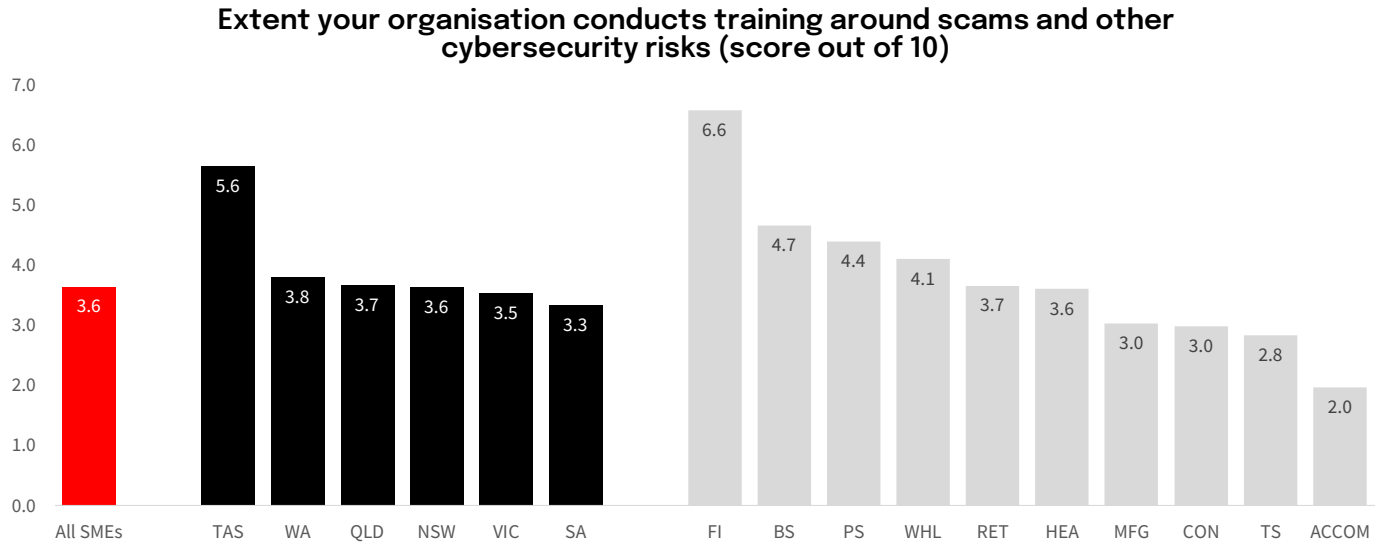
Clearly there is work to be done in this area. NAB's Cyber Security Attacks & Scams report released in April 2023 found that on average, Australian SMEs felt only "moderately to quite" comfortable about the extent they were minimising the risk of a cyberattack on their business. Only 4 in 10 SMEs also believed they were being very vigilant regarding their cybersecurity, and around 15% felt were doing this very "poorly".

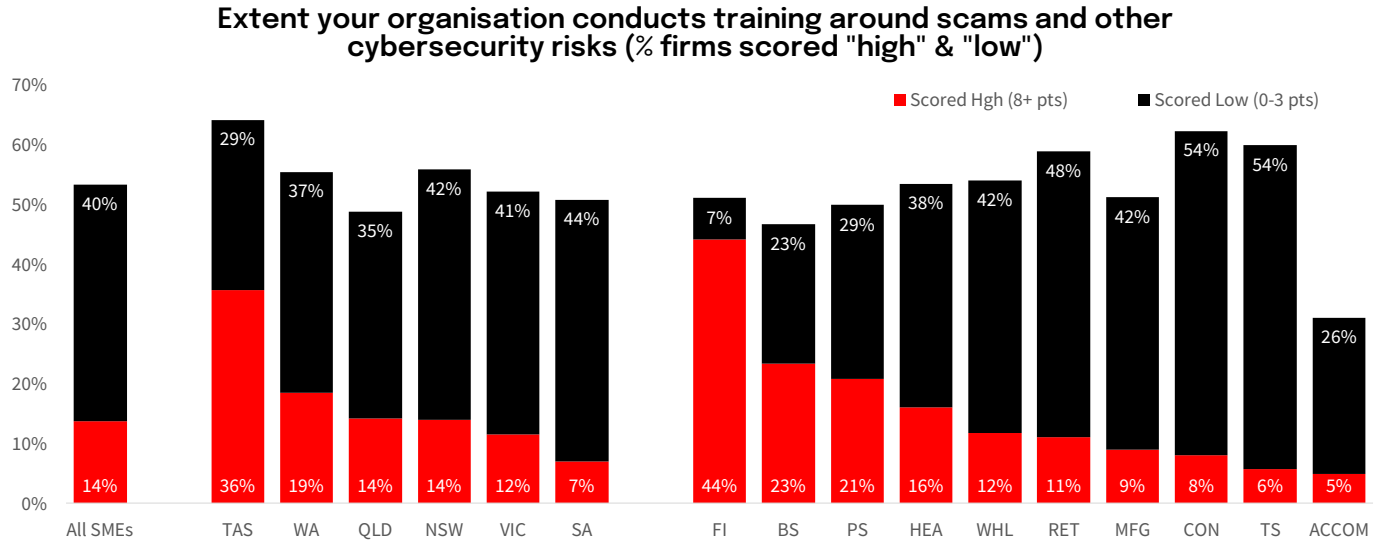
In this survey, we asked Australian SMEs to rate the extent their organisation conducts training around scams and other cybersecurity risks. On average, they scored 3.6 pts out of 10 (10 = extensively). Only 15% of SMEs overall said they conducted "extensive" training (i.e. scored 8 pts or more), and 4 in 10 (40%) "not much" training" at all (i.e. scored 3 pts or less).

The extent SMEs conducted training was quite low in most states, ranging from 3.8 pts in WA to 3.3 pts in SA. TAS was the outlier (5.6 pts) but from a smaller sample size. Outside TAS (36%), the number of SMEs who conducted extensive training ranged from 19% in WA to 6% in SA. Over 4 in 10 SMEs in SA, NSW and VIC did not do much training at all.

By industry, the extent training was conducted was highest in the Finance & Insurance sector (6.6 pts), with 44% also doing so "extensively". SMEs in Business Services (4.7 pts), Personal Services (4.4 pts) and Wholesale Trade (4.1 pts) were next most likely to conduct training, but much less so than in Finance & Insurance firms. Accommodation & Hospitality firms were least likely to have conducted scams training (2.0 pts), with only 1 in 20 (5%) firms in this sector doing so "extensively".

At the other extreme, over 1 in 2 firms in Construction and Transport & Storage (54%) did not conduct much training at all.



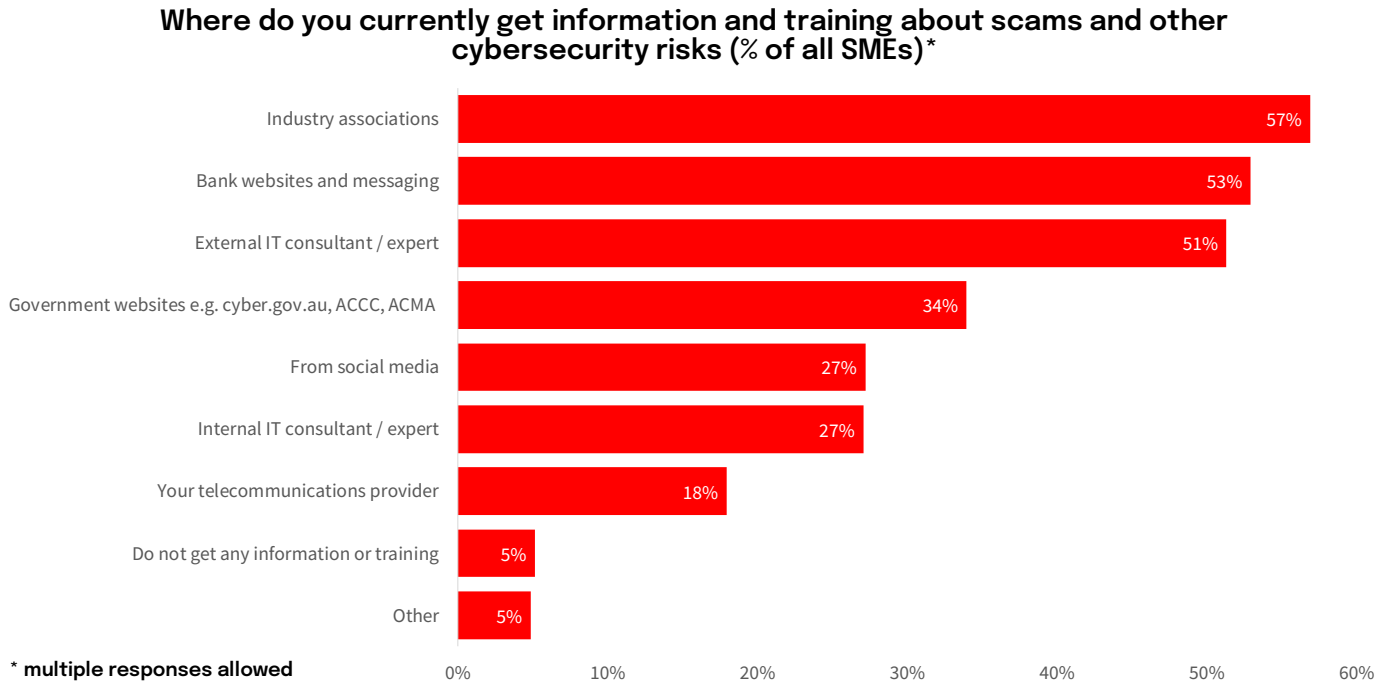


Where is information & training about scams and cybersecurity risks sourced

There are 3 key areas where SMEs currently source their information and training about scams and other cybersecurity risks - industry associations (57%), bank websites and messaging (53%) and from external IT consultants or experts (51%).

Around 1 in 3 SMEs also rely on government websites, around 1 in 4 from social media and internal IT consultants and experts (27%), and 1 in 5 from their telecommunications provider (18%).

Around 1 in 20 SMEs rely on other methods (5%), but 1 in 20 (5%) SMEs also said they don't get any information or training at all – see chart on following page.



Where do you currently get information & training about scams and other cybersecurity risks

	Industry associations	Bank websites and messaging	External IT consultant / expert	Government websites	From social media	Internal IT consultant / expert	Telecoms provider	Do not get any information or training	Other
All SMEs	**57%**	**53%**	**51%**	**34%**	**27%**	**27%**	**18%**	**5%**	**5%**
NSW	55%	52%	**55%**	35%	29%	**32%**	19%	4%	3%
QLD	55%	51%	**56%**	33%	26%	22%	19%	**8%**	3%
SA	**60%**	**60%**	52%	37%	**33%**	13%	12%	6%	4%
TAS	**71%**	**86%**	43%	**21%**	29%	14%	**36%**	0%	0%
VIC	**61%**	51%	46%	34%	25%	**28%**	15%	4%	7%
WA	51%	51%	46%	33%	24%	**29%**	**21%**	6%	**11%**
MFG	48%	45%	48%	30%	20%	26%	14%	6%	5%
CON	60%	**64%**	50%	35%	**36%**	23%	21%	8%	5%
RET	56%	52%	37%	36%	**33%**	16%	13%	3%	7%
WHL	43%	57%	46%	27%	22%	29%	19%	2%	5%
TS	52%	**64%**	42%	33%	**36%**	21%	**30%**	3%	**9%**
FI	**77%**	42%	**79%**	40%	**9%**	35%	16%	**14%**	0%
BS	60%	48%	**67%**	43%	25%	**46%**	16%	6%	1%
PS	60%	47%	49%	26%	21%	30%	19%	4%	6%
ACCOM	**81%**	48%	39%	42%	29%	16%	13%	3%	6%
HEA	51%	45%	**74%**	30%	21%	38%	21%	0%	2%

Where SMEs sourced their information and training about scams and other cybersecurity risks varied by state. Somewhat more firms in TAS (71%), VIC (61%) and SA (60%) turned to industry associations for information, while bank websites and messaging was used by significantly more firms in TAS (86%) and SA (60%). A somewhat higher number in QLD (56%) and NSW (55%) relied on external IT consultants or experts. Around 1 in 3 firms in all states (apart from TAS) relied on government websites, while SMEs in SA relied noticeably more on social media (33%) than in any other state. Usage of internal IT consultants was somewhat higher in NSW (32%), WA (29%) and VIC (28%), and telecommunication providers in TAS (36%) and WA (21%), where significantly more firms also got information from other sources (11%). Around 8% of SMEs in QLD did not get any information on training - double the number in NSW and VIC (4%).

Differences by industry were more pronounced. Key disparities we noted included a much higher number of SMEs in the Accommodation & Hospitality (81%) and Finance & Insurance (77%) sectors who sourced information from industry associations. Significantly more in Construction and Transport & Storage relied on bank websites and messaging (64%) and in Finance & Insurance (79%), Health (74%) and Business Services (67%) external IT consultants and experts. Reliance on government websites (such as cyber.gov.au, ACCC, ACMA) ranged from 43% in Business Services to 26% in Personal Services. Getting information from social media was much more common in Construction (36%), Transport & Storage (36%) and Retail (33%) firms, particularly when compared to the Finance & Insurance sector (9%). Noticeably more firms in Business Services sourced information from internal IT consultants and experts (43%), and in Transport & Storage from telecommunication providers (30%) or other means (14%). Interestingly, we noted a much higher number of SMEs in the Finance & insurance sector who said they don't get any information or training (14%) than in all other sectors.

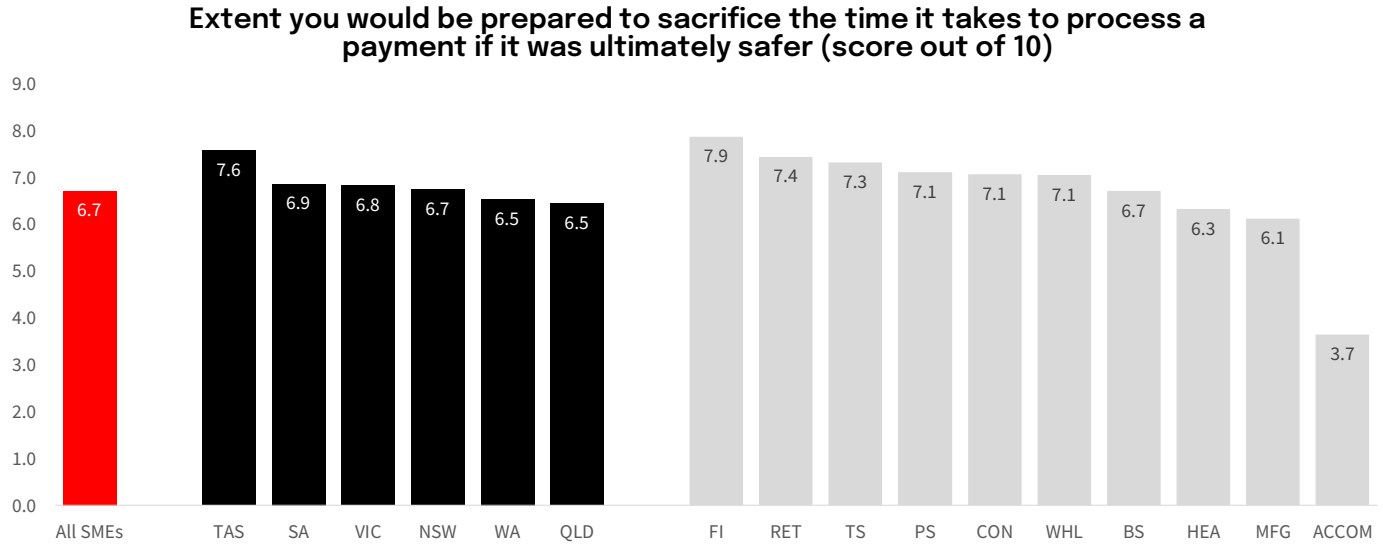
More checks & balances from financial institutions

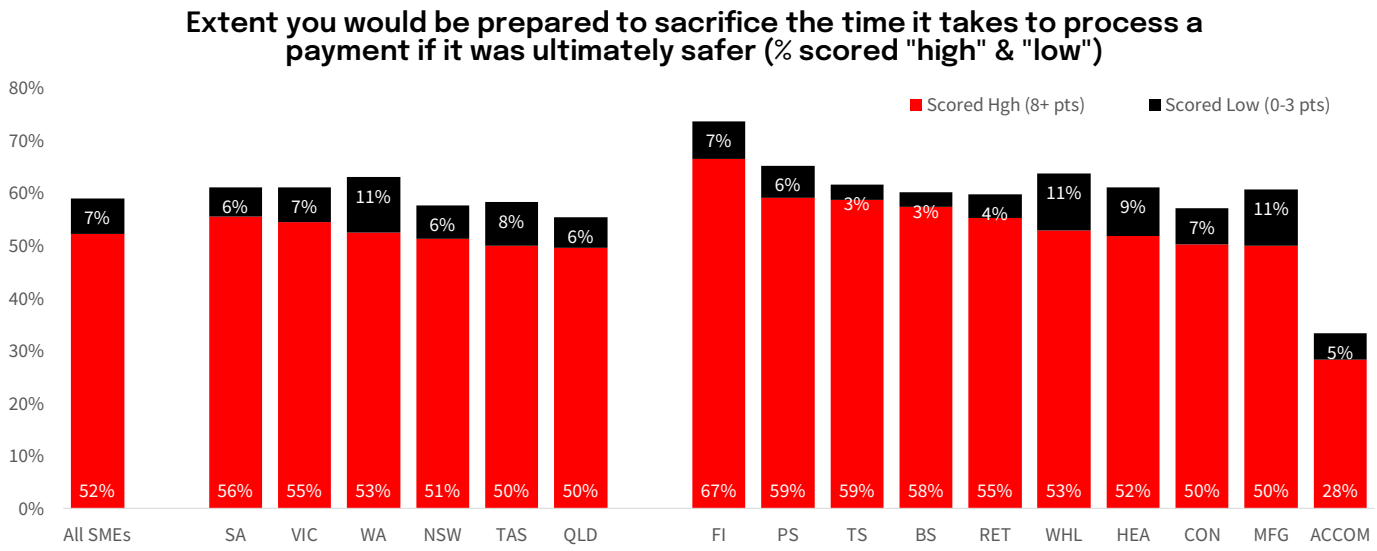
Real time payments growth is accelerating globally with many businesses (both big and small) wanting access to funds more quickly. Faster receipts can help their businesses manage cash flows in real time and avoid expensive short-term financing. But instant payments also pose some unique challenges due their speed and irrevocability

When surveyed Australian SMEs were also asked to rate the extent they would be prepared to sacrifice the time it takes to process a payment if it was ultimately safer (i.e. more checks and balances from financial institutions), they indicated they would support it "quite" strongly scoring a solid 6.7 pts out of 10 (10 = completely support).

Support was highest in TAS at 7.6 pts (but from a smaller sample size). In other states it ranged from 6.9 pts in SA to 6.4 pts in QLD. Support ranged more widely by industry. It was highest in the Finance & Insurance sector (7.9 pts), followed by Retail (7.4 pts) and Transport & Storage (7.3 pts). Support was lowest in in Accommodation & Hospitality by a significant margin (3.7 pts).

The survey found that 1 in 2 SMEs overall (52%) also scored their support "very high" (i.e. scored 8 pts or more), with this number ranging from 56% in SA to 50% in QLD and TAS. Around 2 in 3 SMEs in the Finance & Insurance sector (67%) scored support "very high", followed by 6 in 10 in Personal Services and Transport & Storage firms (59%). Only 3 in 10 (28%) SMEs in the Accommodation & Hospitality sector score support "very high".




Extent you would be prepared to sacrifice the time it takes to process a payment if it was ultimately safer (% scored "high" & "low")
Scored Hgh (8+ pts)
Scored Low (0-3 pts)
80%
70%
60%
50%
40%
30%
20%
10%
0%
All SMEs 7% 52%
SA 6% 56%
VIC 7% 55%
WA 11% 53%
NSW 6% 51%
TAS 8% 50%
QLD 6% 50%
FI 7% 67%
PS 6% 59%
TS 3% 59%
BS 3% 58%
RET 4% 55%
WHL 11% 53%
HEA 9% 52%
CON 7% 50%
MFG 11% 50%
ACCOM 5% 28%

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.

Contact the authors

Dean Pearson
Head of Behavioural and Industry Economics
Dean.Pearson@nab.com.au
+61 3 8634 2331

Robert De Iure
Associate Director Economics
Robert.De.Iure@nab.com.au
+61 3 8634 4611