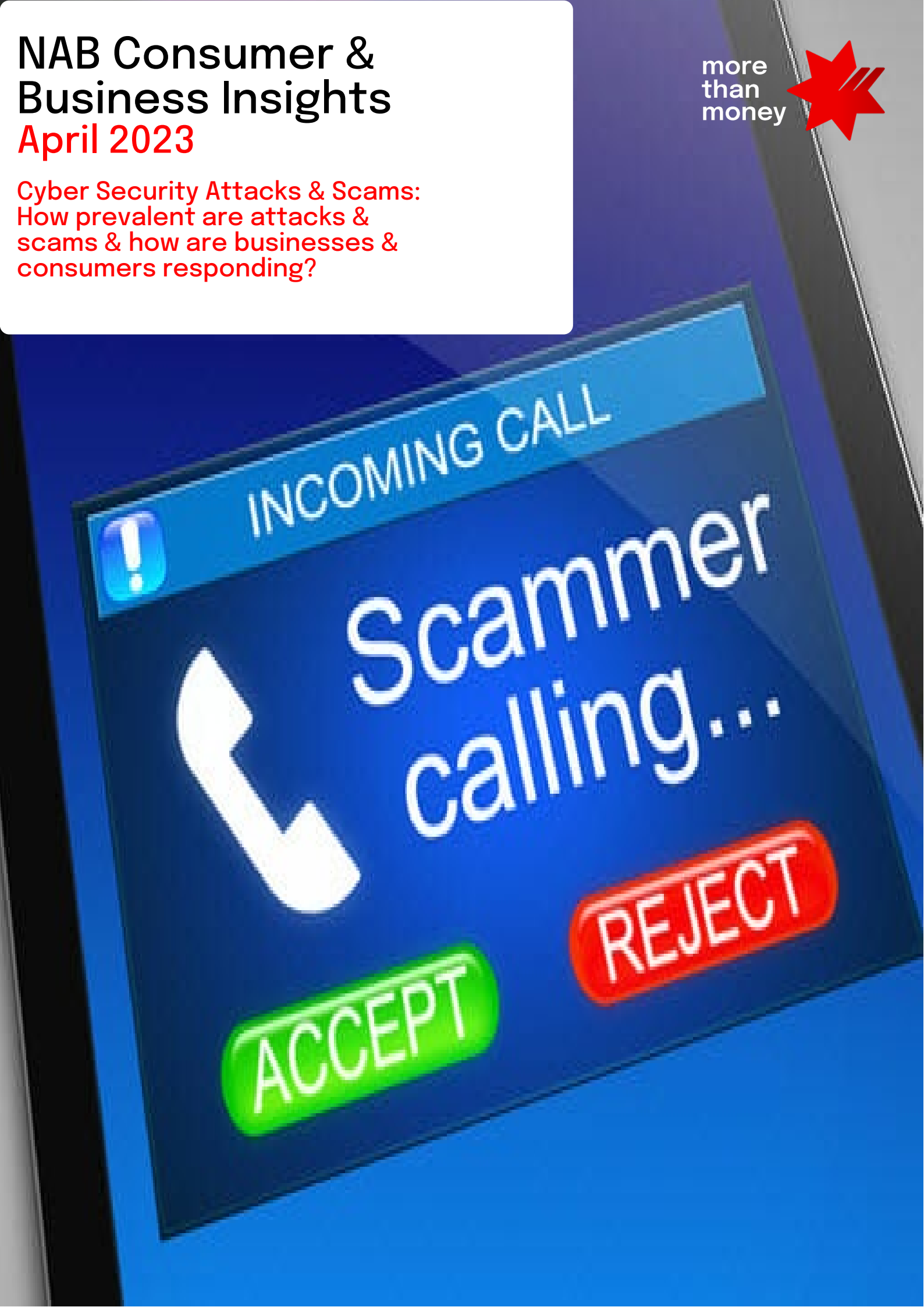
NAB Consumer & Business Insights

April 2023

Cyber Security Attacks & Scams: How prevalent are attacks & scams & how are businesses & consumers responding?

more than money



Key Findings

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. Cyberspace, as it's often known, is the vehicle criminals use in a digital world. The results are many and varied, but included crimes such as scams, fraud, extortion and espionage.

NAB research shows over 1 in 5 Australians and just over 1 in 10 businesses (SMEs) have been victims of a cyber-attack, scam or data breach in the past 12 months alone. On average, Australians have lost $569, while the average losses for SMEs was $19,400. Around 1 in 3 Australians are finding it difficult to trust or are feeling powerless and vulnerable.

Consumer Impacts & Responses

NAB research shows over 1 in 5 Australians have been the victim of a cyber-attack, scam or data breach in the past 12 months alone, losing on average $569. Interestingly, women ($921) have lost significantly more than men ($375).

With incidence of cyber-crime on the rise, around 3 in 10 Australians identify as "extremely concerned" about their cyber security. And a significant number are potentially vulnerable to future cyber-attacks, with only 1 in 10 Australians believing they have "very good" knowledge of good cyber security practices. Cyber security awareness is highest among younger people and falls in each successive age group. This relationship also holds true for men and women, though men believe they have a greater understanding than women in all age groups.

Overwhelmingly, the most common type of cyber security issue (experienced by around 6 in 10 victims), is third party exposure (i.e., a personal data leak from another organisation). The next most common form of attack (for 1 in 10 impacted Australians) was a phishing attack (i.e. a fake email or website tricked them into giving away personal information), a data breach (i.e. personal data stolen from their computer), or malware attack (i.e. their computer system was disrupted/data stolen due to a virus, trojan or malicious software).

While the impact of cyber-attacks or being the victim of a scam is usually measured in time and money lost, it can also impact mental and emotional wellbeing. This can manifest is several ways, such as emotional stress from stolen data and concern about how the data may be used, feelings of shame and guilt for not being cautious enough, sense of helplessness, and loss of trust, autonomy, and control.

When asked to identify the biggest impact from a cyber-attack or scam outside of money, almost 4 in 10 Australians overall pointed to feelings of anxiety, fear, stress, or frustration (particularly amongst women). Around 1 in 3 were finding it difficult to trust or felt powerless and vulnerable. Around 3 in 10 had feelings of intense outrage and anger and 1 in 4 feelings of helplessness and feeling that they are likely to be the victim of future cybercrime. Around 1 in 10 were experiencing feelings of shame and guilt, decreased energy levels, disturbed sleep, trouble concentrating and becoming more isolated. Only 1 in 5 people did not experience any of these feelings.

The most common measure employed by Australians to protect themselves against a cyber-crime (identified by over 2 in 3 of the adult population) is regularly checking bank statements. The next most common measures (used by around 1 in 2 people) include: keeping mobile devices & apps updated; clearing browser histories; using multi-factor authentication to log into their digital accounts; and only shopping on known or secure websites.

Around 4 in 10 people regularly change or use complex passwords or use cyber security software such as malware protection/antivirus software packages, while 1 in 3 use a pop-up blocker or back up data in the cloud. Almost 1 in 4 use a password protection app and 1 in 5 a VPN when using a public Wi-Fi. Fewer than 1 in 10 Australians had enabled parental controls on their children's devices.

Behaviours are quite different by gender and age. For example, over 8 in 10 people over 65 regularly check their account balances, compared to just 55% of men and 63% of women aged 18-29. A much higher number of young people (aged 18-29) use a VPN when using public Wi-Fi, while young women are much more likely to use multi-factor authentication to login into their digital accounts. Women over 65 are more inclined to only shop on known or secure websites, while men over 65 are much more likely to use cyber security software.

Australians on average have spent $620 on cyber-attack prevention and recovery (e.g., buying hardware/software, IT repair, insurance, etc.). Men have spent more than women across most age groups. Around 6 in 10 Australians overall however had spent no money on cyber-attack prevention and recovery.

Business Impacts & Responses

Around 3 in 10 Australian SMEs have experienced a cyber-attack or data breach during the life of their business and just over 1 in 10 in the last 12 months alone. Attacks were most common in QLD (14% of SMEs) and least common in TAS (8%) and NSW (9%) over the past year.

On average, SMEs estimate they have lost around $19,400 because of cyber-attacks in the past year.

The number of businesses impacted by a cyber-attack or data breach range considerably by industry. Over the past 12 months, cyber-attacks or data breaches impacted most in Construction (16%), Retail (15%) and Business Services (14%). Attacks were least common in the Health Services (3%), Accommodation & Hospitality (4%), and Wholesale Trade (5%) sectors.

The most common forms of cyber security breaches are malware attacks, ransomware, phishing, and business email compromise, including invoice scams. Around 1 in 3 SMEs (36%) experienced a malware attack, just over 1 in 4 (27%) ransomware, and 1 in 5 a phishing attack (22%) or business email compromise including invoice scams (20%). The least common attacks experienced by SMEs were identity-based attacks (3%), distributed denial of service (7%), and other or man-in-the-middle (8%) attacks.

Malware and ransomware attacks were typically the most common types of cyber-attacks across all industries, but particularly in Transport & Storage, Construction and Accommodation & Hospitality firms. A higher number of SMEs in the Manufacturing sector have also been impacted by business email compromise, including invoice scams (33%), in Construction malware (40%) and identity based attacks (9%), in Transport & Storage malware (40%), ransomware (60%), phishing (40%) and business email compromise, including invoice scams (40%), in Finance & Insurance Services phishing attacks (43%), Business Services impersonation scams (35%), man-in-the-middle attack (17%) and distributed denial of service (13%), in Accommodation & Hospitality ransomware (50%), and in Health Services data breach (25%).

Only 4 in 10 SMEs believe they are being very vigilant regarding their cyber security. On average, Australian SMEs feel "moderate to quite" comfortable about the extent they are minimising the risk of a cyber-attack on their business. When asked to rate how they felt, on average they scored 6.8 pts out of 10 (0 = not at all; 10 = significantly). Though 4 in 10 (43%) businesses overall believe they are being very vigilant (scoring 8 pts or higher), around 15% feel they are doing this "poorly" (scoring between 0-4 pts).

By industry, SMEs in the Health Services (7.5 pts) and Manufacturing (7.4 pts) sectors scored themselves highest, and Accommodation & Hospitality (5.9 pts), Wholesale Trade (6.5 pts), Retail Trade (6.5 pts), Construction (6.6 pts) and Transport & Storage 6.7 pts) firms lowest.

The number SMEs who think they are being very vigilant trying to minimise risks (scoring 8+ pts) was highest in the Business Services (57%) sector and lowest in Wholesale Trade (38%).

On average, SMEs have spent $6,350 on cyber insurance prevention in the past 12 months. By industry, spending was highest by some margin in Health Services ($17,018), and almost 10 times more than in Accommodation & Hospitality Services were spend was lowest overall ($2,453).

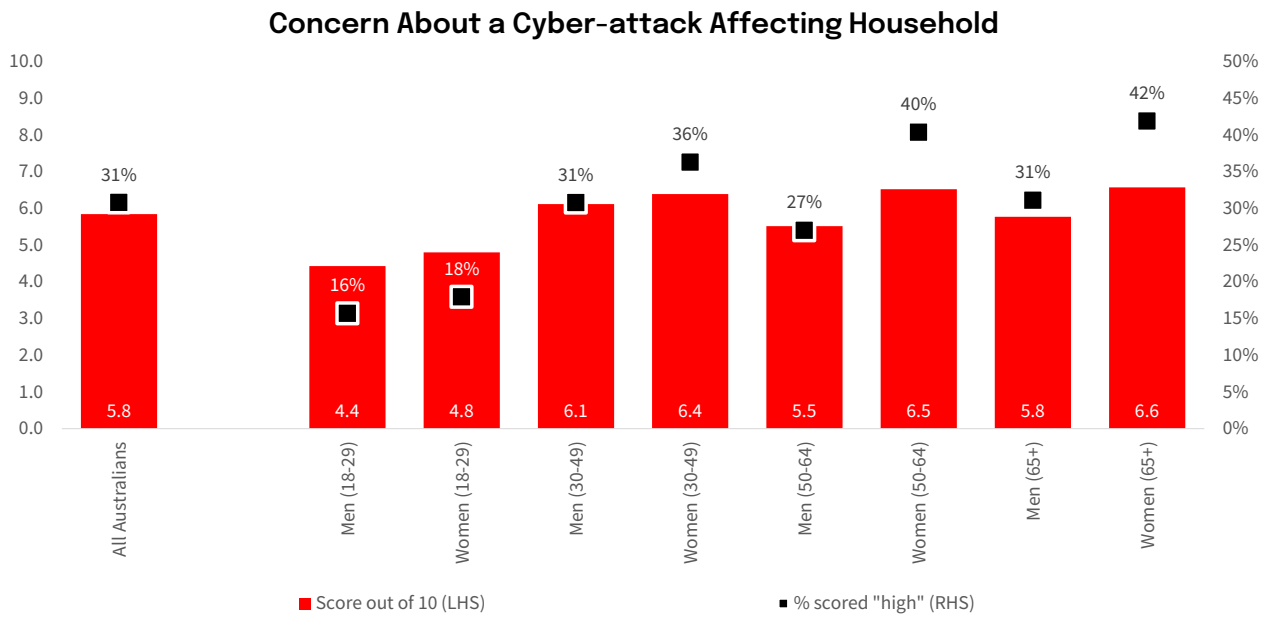
Cyber security - The view from consumers

In simple terms, cyber security involves the protection of computer systems or devices connected to the Internet and/or a telecommunications network. 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 cybercrime continues to escalate in Australia, greater awareness and preventative measures are crucial.

According to the latest Australian Annual Cyber Security (ACSC) Threat Report 2021-22 Australia saw an increase in the number and sophistication of cyber threats, making crimes like extortion, espionage, and fraud easier to replicate at a greater scale. The ACSC received over 76,000 cybercrime reports, an increase of nearly 13% from the previous financial year. This equates to one report every 7 minutes, compared to every 8 minutes in the previous financial year. Australians lost $3.1 billion to scams in 2022, according to the ACCC's Scamwatch. Scams are often under reported so the true figure is probably higher. This type of crime often also has an emotional impact.

In the first part of this report, we explore how concerned Australian consumers are about a cyber-attack or scam, their level of cyber security knowledge, if they have taken actions to prevent a scam or cyber-crime, if someone in their household has ever been the victim of a cyber-attack, scam or data breach, the type of attack they experienced, how much money they lost, and what type of emotional impact the attack had.

The results are based on survey responses from around 2,000 Australian consumers conducted over the period 17 February to 8 March 2023.



Level of concern about scam or cyber-attack impacting consumer households…

Despite the rapid escalation of cybercrime in Australia, consumers remain on average only "moderately concerned about a cyber-attack (e.g. viruses, fake emails, cyber bullying etc.) affecting them or their household. When asked to rate their level of concern, they scored on average just 5.8 pts out of 10 (where 0 = not at all concerned and 10 = extremely concerned).

The level of concern did however vary somewhat by age and gender. Men were less concerned about a cyber-attack than women in all age groups, with the gap biggest in the 50-64 (men 5.5 pts; women 6.5 pts) and over 65 (men 5.8 pts; women 6.6 pts) age groups. Concern was lowest in the 18-29 group for both men (4.4 pts) and women (4.8 pts). It was highest for men in the 30-49 age group (6.1 pts), and for women in the over 65 group (6.6 pts).

The average score does however hide a large number of Australians who are "very" concerned about a cyber-attack, with around 3 in 10 (29%) signalling extreme levels of concern (i.e. scored 8+ pts). Again, this ranged significantly from around 4 in 10 women in the over 65 (42%) and 50-64 (40%) age groups, to less than 1 in 5 men (16%) and women (18%) in the 18-29 age groups. Far fewer men in the 50-64 (27%) and over 65 age groups (31%) were extremely concerned about a cyber-attack than women in these age groups.

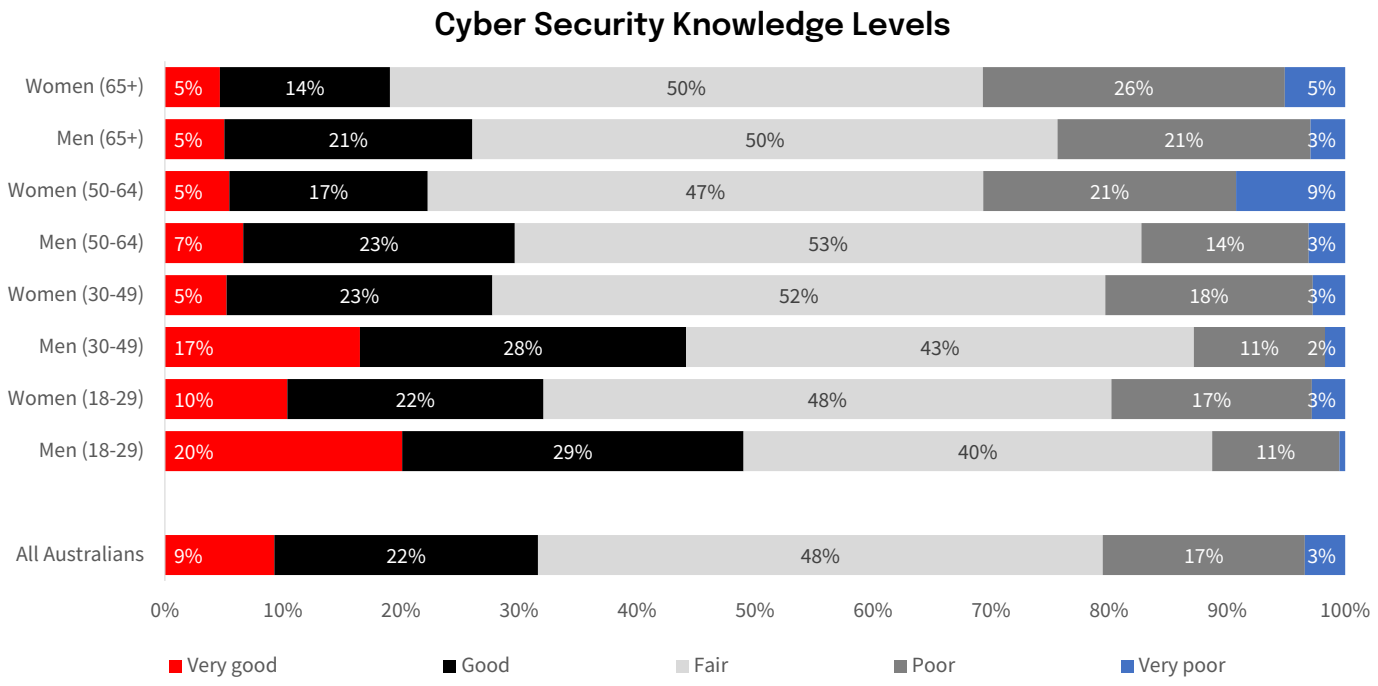
Cyber security knowledge levels…

Around 1 in 10 (9%) Australians believe they have "very good" knowledge levels around cyber security, and a further 2 in 10 (22%) "good levels" of knowledge. Around 1 in 2 (48%) rated their knowledge "fair". However, 1 in 5 rated their knowledge "poor" (17%) or "very poor" (3%), suggesting a significant number of Australians do not understand how to reduce the risk of being impacted by cyber-crime.

The survey found a direct correlation between "very good" and "good" levels of cyber security knowledge and age - it is highest in the 18-29 age group and falls in each successive age group. This relationship also holds true for men and women - though more men report higher knowledge levels than women in all age groups. These results may help explain why younger people are also less concerned about a cyber-attack impacting their household.

Around 1 in 2 men in the 18-29 age group have "very good" (20%) or "good" (29%) knowledge levels. This compares to just 1 in 4 men over 65 (5% very good; 21% good). In contrast 1 in 3 women in the 18-29 group had "very good" (10%) or "good" knowledge (22%), with this falling to just 1 in 5 in the over 65 age group (5% very good; 14% good).

Women over the age of 50 appear most vulnerable to a cyber-attack, with 3 in 10 women in the 50-64 and over 65 age groups reporting "poor" or "very poor" knowledge levels around cyber security. Around 1 in 4 men over 65 are also at risk (21% "poor" knowledge; 3% "very poor" knowledge).

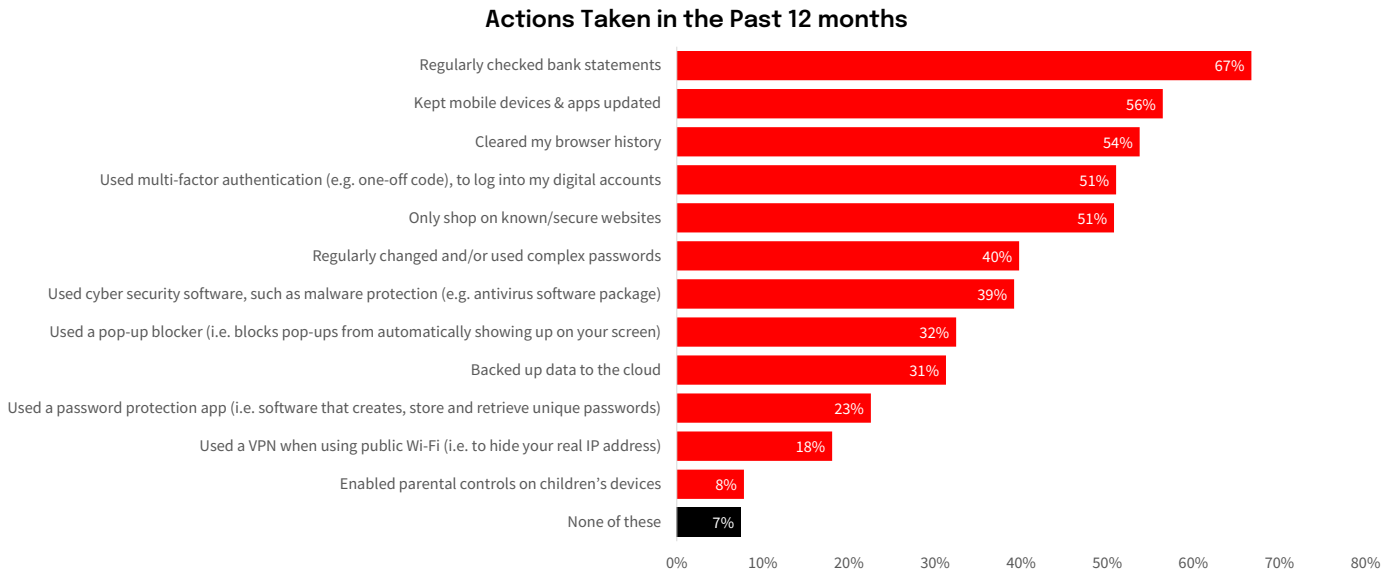


Actions taken to avoid a scam or cyber-attack in the past 12 months…

What actions have Australian consumers taken to avoid cyber-attacks in the past year? The most common measure employed by 2 in 3 (67%) people overall was regularly checking bank statements. The next most common measures were keeping mobile devices & apps updated (56%) and clearing their browser history (54%), while 1 in 2 used multi-factor authentication to log into their digital accounts (51%), or only shopped on known or secure websites (51%).

Around 4 in 10 said they regularly changed or used complex passwords (40%), or used cyber security software such as malware protection/antivirus software packages (39%), and 1 in 3 a pop-up blocker (32%), or backed up data in the cloud (31%). Almost 1 in 4 people used a password protection app (23%), and 1 in 5 a VPN when using a public Wi-Fi (18%). Fewer than 1 in 10 Australians enabled parental controls on their children's devices (8%), and 8% none of these things - see chart below.

Actions taken by consumers to avoid cyber-attacks does however vary quite widely by gender and age. For example, over 8 in 10 people over 65 regularly check their account balances, compared to 55% of men and 63% of women aged 18-29. Among some other key differences were the much higher number of men in the 18-29 age group using a VPN when using public Wi-Fi (29%), women 18-29 using multi-factor authentication to login into their digital accounts (63%), women over 65 only shopping on known or secure websites (61%), and men over 65 using cyber security software (61%) - see table below.



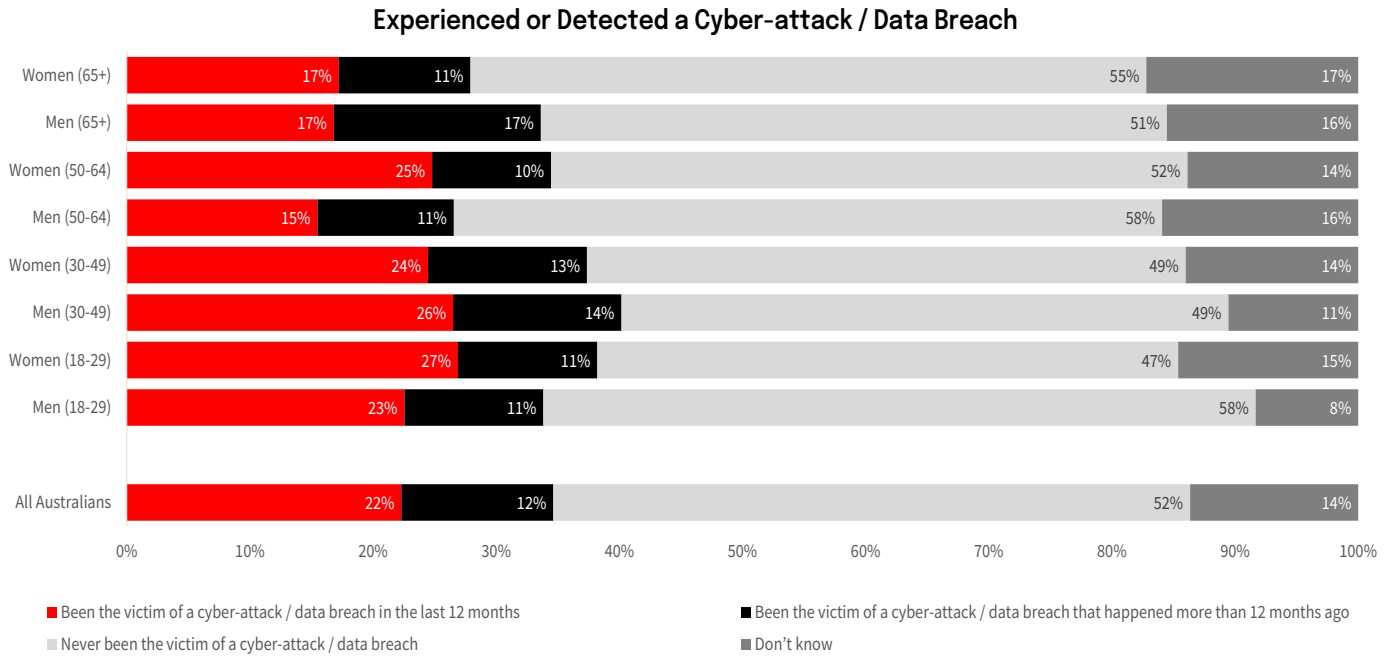
Actions Taken in Past 12 Months

	All Australians	Men (18-29)	Women (18-29)	Men (30-49)	Women (30-49)	Men (50-64)	Women (50-64)	Men (65+)	Women (65+)
Regularly checked bank statements	67%	54%	63%	53%	60%	76%	72%	83%	82%
Kept mobile devices & apps updated	56%	55%	64%	42%	53%	67%	61%	61%	60%
Cleared my browser history	54%	49%	52%	46%	46%	63%	62%	67%	53%
Used multi-factor authentication (e.g. one-off code), to log into my digital accounts	51%	53%	63%	43%	46%	53%	55%	55%	49%
Only shop on known/secure websites	51%	50%	57%	40%	48%	54%	51%	53%	61%
Regularly changed and/or used complex passwords	40%	42%	36%	35%	35%	41%	50%	42%	43%
Used cyber security software, such as malware protection (e.g. antivirus software package)	39%	31%	27%	28%	33%	51%	40%	61%	49%
Used a pop-up blocker (i.e. blocks pop-ups from automatically showing up on your screen)	32%	38%	35%	30%	27%	42%	29%	39%	24%
Backed up data to the cloud	31%	40%	42%	30%	29%	24%	31%	29%	30%
Used a password protection app (i.e. software that creates, store and retrieve unique passwords)	23%	29%	25%	21%	20%	24%	19%	24%	21%
Used a VPN when using public Wi-Fi (i.e. to hide your real IP address)	18%	29%	14%	22%	16%	20%	16%	14%	12%
Enabled parental controls on children's devices	8%	9%	8%	12%	16%	4%	5%	1%	0%
None of these	7%	5%	6%	11%	8%	9%	8%	6%	5%

How common are cyber-attacks/scams/data breaches…

The incidence of cyber-attacks has grown rapidly over the past year. NAB's survey data found that over 1 in 5 (22%) Australians had been the victim of a cyber-attack of data breach in the past 12 months, compared to and just over 1 in 10 (12%) more than 12 months ago. Around 1 in 2 (52%) people however indicated they had never been the victim of an attack or breach, while 14% were unsure.

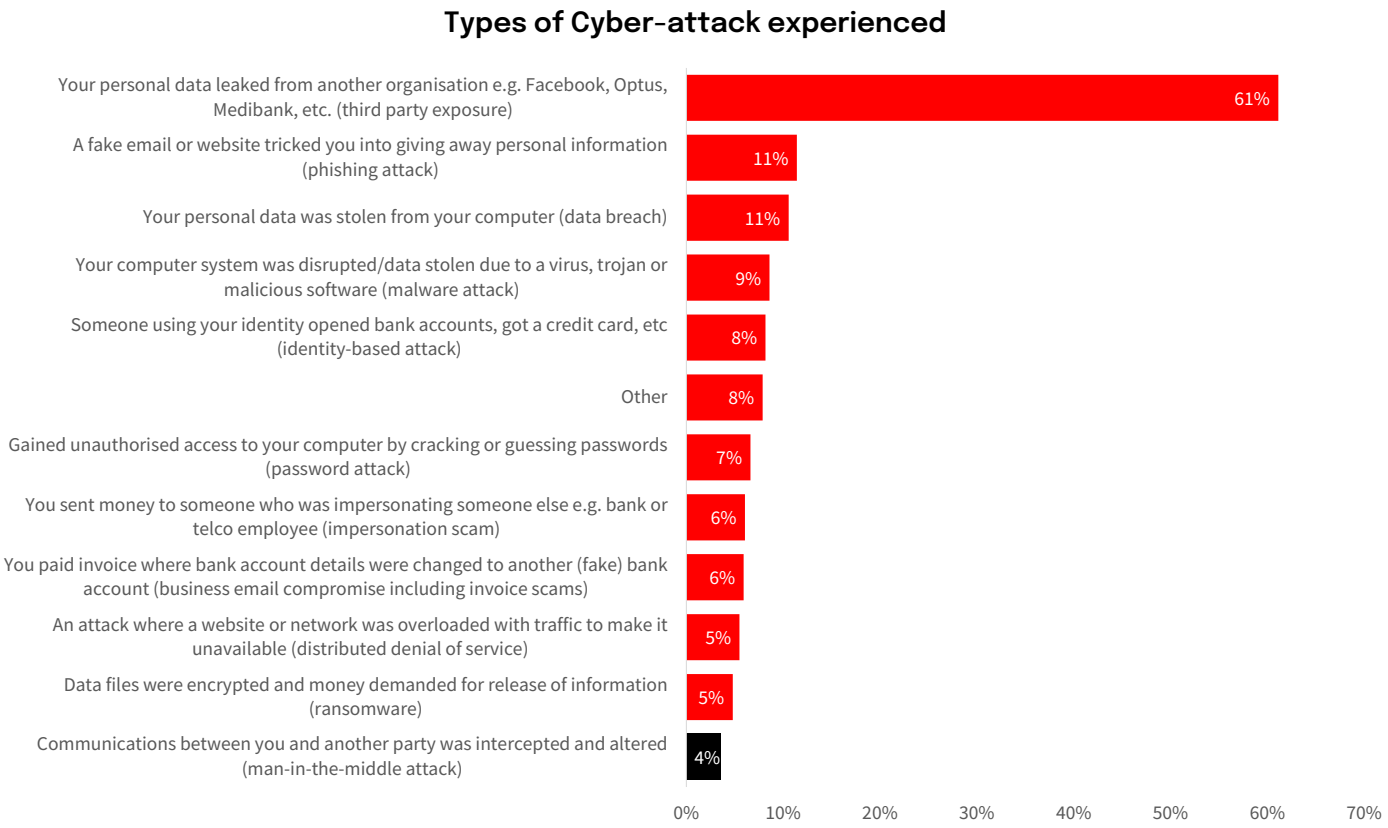
Interestingly, around 1 in 4 people under 50 (both men and women), and women in the 50-64 group had been victim of an attack in the past 12 months, compared to just 17% of men and women over 65. Men over the age of 65 had however been somewhat more vulnerable more than 12 months ago (17%), and women 50-64 least impacted (10%). Almost 6 in 10 (58%) men in the 18-29 age group indicated they had never been a victim of a cyber-attack, compared to 47% of women in the 18-29 age group.



Types of scams and cyber-attacks experienced

Australians who experienced or detected a cyber-attack were asked to describe the type of attack. Around 6 in 10 (61%) said it was third party exposure i.e. a personal data leak from another organisation, such as Facebook, Optus, Medicare etc. This was also by far the most common type of cyber-attack experienced. The next most common attacks according to 1 in 10 Australians were a phishing attack i.e. a fake email or website that tricked them into giving away personal information (11%), data breach i.e. personal data stolen from their computer (11%), or malware attack i.e. their computer system was disrupted/data stolen due to a virus, trojan or malicious software (9%).

The least common types of attack were man-in-the-middle i.e. having communications to another party intercepted and altered (4%), ransomware i.e. having data files encrypted and money demanded for release of information (5%), or distributed denial of service i.e. where website or network was overloaded with traffic to make it unavailable (5%).

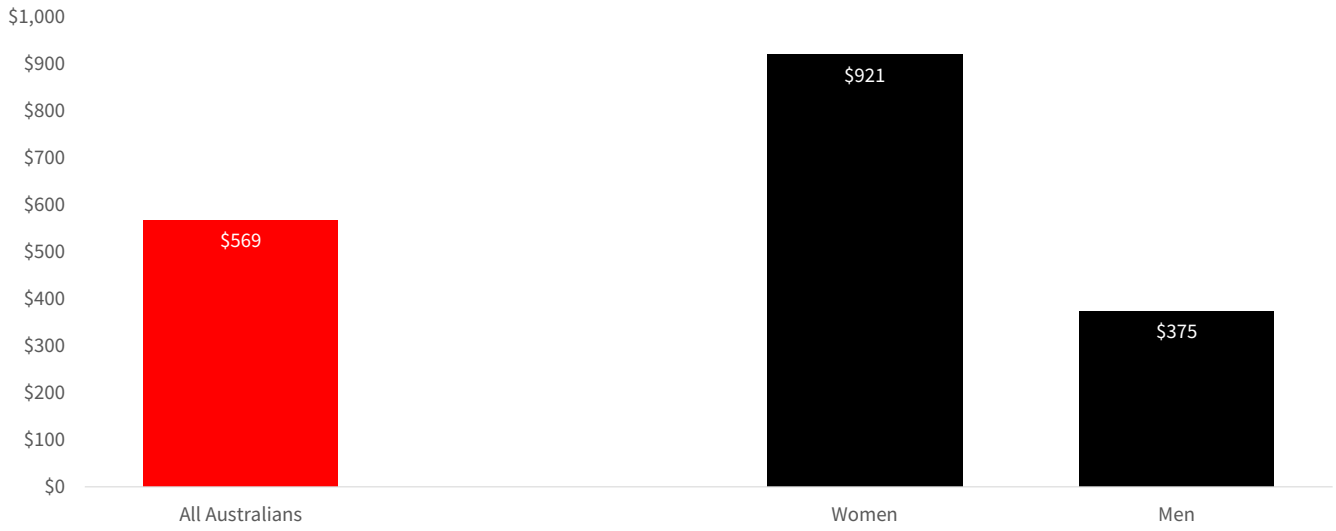


Types of Cyber-attack and scam experienced

	All Australians	Men (18-29)	Women (18-29)	Men (30-49)	Women (30-49)	Men (50-64)	Women (50-64)	Men (65+)	Women (65+)
Third party exposure	61%	62%	65%	60%	64%	68%	61%	48%	62%
Phishing attack	11%	6%	11%	11%	13%	10%	10%	16%	15%
Data breach	11%	12%	11%	18%	12%	7%	1%	9%	7%
Malware attack	9%	6%	5%	10%	9%	10%	5%	15%	8%
Identity-based attack	8%	6%	5%	12%	10%	7%	7%	8%	7%
Password attack	7%	6%	5%	14%	9%	5%	1%	4%	0%
Impersonation scam	6%	4%	7%	9%	10%	2%	1%	3%	5%
Business email compromise	6%	9%	7%	7%	9%	3%	4%	4%	0%
Distributed denial of service	5%	6%	4%	12%	7%	3%	1%	1%	3%
Ransomware	5%	7%	1%	12%	2%	3%	2%	5%	0%
Man-in-the-middle attack	4%	6%	1%	6%	4%	5%	0%	1%	5%

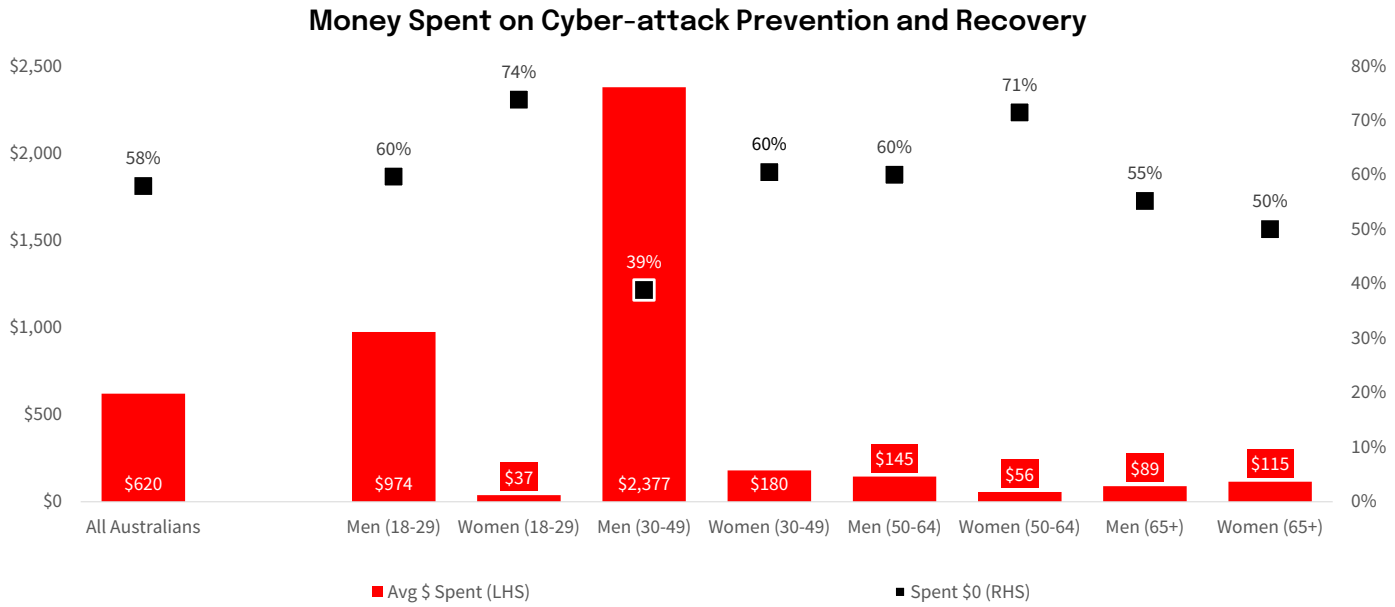
Significantly more men and women in all age groups experienced third party exposure than any other type of attack, though the number that did so ranged from 68% among men in 50-64 age group to 48% for men over 65. We also noted a somewhat higher number of men in the 30-49 age group that experienced a data breach (18%), password attack (14%), distributed denial of service (12%) and ransomware (12%) attack than in other groups, men over 65 a malware attack (15%), and men and women over 65 a phishing attack.

Amount Lost from Cyber-attacks in the Past 12 months



How much money have people lost…?

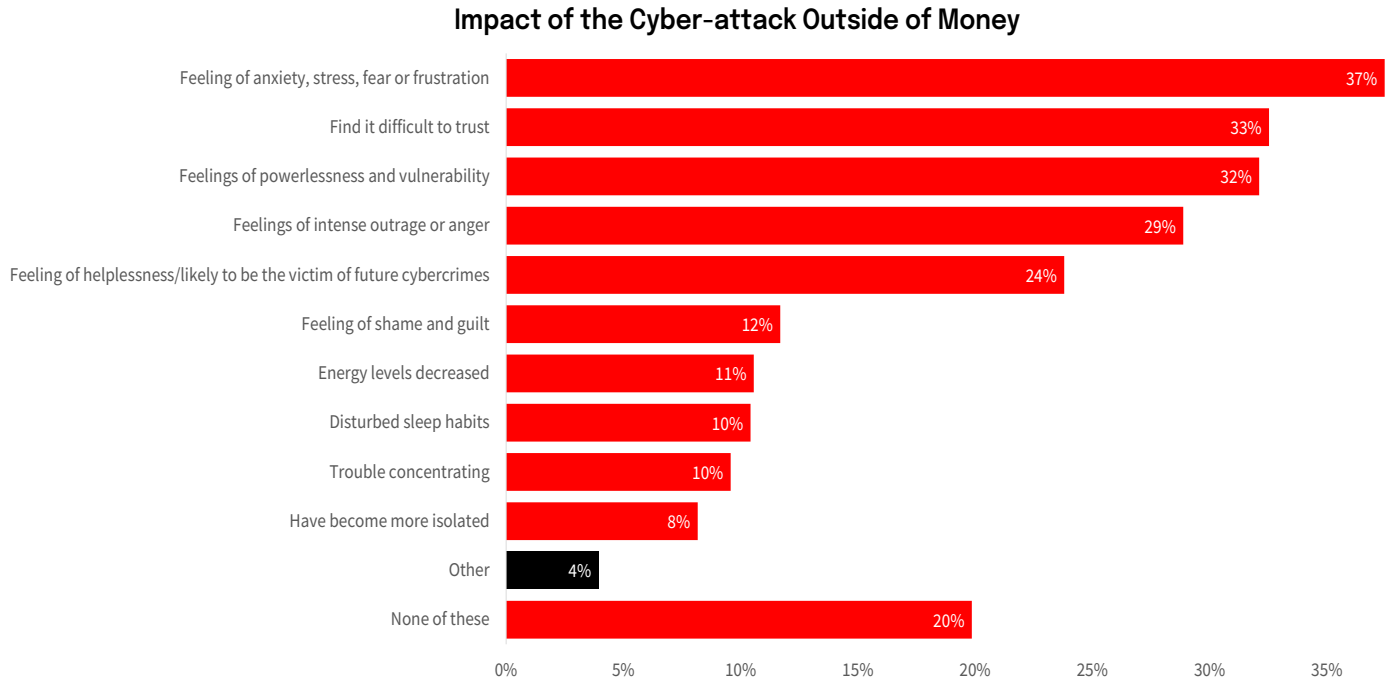
People who were victim of a cyber-attack, scam or data breach in the last 12 months lost on average $569. But this ranged from $921 for women to $375 for men.



Amount spent on cyber security & recovery…

Australians were asked to estimate how much money (if any) did they spend on cyber-attack prevention and recovery (e.g. buying hardware/software, IT repair, insurance, etc.). On average, they spent $620. Men spent more than women in all age groups, except in the over 65 group, where women spent somewhat more ($115 women; $89 men). The gulf was greatest in the 30-49 age group where men spend much more than women ($2,377 men; $180 women) and in the 18-29 age group ($974 men; $37 women). Men in the 50-64 age group also spent around 3 times more than women ($145 men; $56 women).

Around 6 in 10 Australians overall however said they spent no money on cyber-attack prevention and recovery. However this ranged from 3 in 4 (74%) women in the 18-29 age group to just 4 in 10 (39%) men in the 30-49 age group.



Impacts of cyber security issues outside of money

While the impact of cyber-attacks is usually measured in time and money lost, research also shows it can profoundly impact mental and emotional wellbeing. This can manifest is several ways, such as emotional stress from stolen data and concern about how the data may be used, feelings of shame and guilt for not being cautious enough, sense of helplessness, and loss of trust, autonomy and control.

When asked to identify the biggest impact from a cyber-attack outside of money, almost 4 in 10 (37%) Australians overall pointed to feelings of anxiety, fear, stress, or frustration. Around 1 in 3 were finding it difficult to trust (33%) or felt powerless and vulnerable. Around 3 in 10 had feelings of intense outrage and anger (29%), and 1 in 4 feelings of helplessness and feeling that they are likely to be the victim of future cybercrime (24%). Around 1 in 10 intimated feelings of shame and guilt (12%), decreased energy levels (11%), disturbed sleep (10%), trouble concentrating (10%), and becoming more isolated (8%). Only 1 in 5 people did not experience any of these feelings (20%).

Impact of the cyber-attack outside of money

	All Australians	Men (18-29)	Women (18-29)	Men (30-49)	Women (30-49)	Men (50-64)	Women (50-64)	Men (65+)	Women (65+)
Feeling of anxiety, stress, fear or frustration	37%	29%	49%	30%	46%	38%	44%	28%	32%
Find it difficult to trust	33%	22%	38%	29%	34%	33%	44%	31%	28%
Feelings of powerlessness and vulnerability	32%	25%	28%	31%	32%	32%	37%	36%	38%
Feelings of intense outrage or anger	29%	19%	26%	23%	29%	40%	32%	38%	33%
Feeling of helplessness/likely to be victim of future cybercrimes	24%	25%	23%	23%	23%	20%	23%	20%	37%
Feeling of shame and guilt	12%	13%	15%	13%	17%	7%	5%	11%	7%
Energy levels decreased	11%	9%	12%	18%	14%	7%	6%	3%	5%
Disturbed sleep habits	10%	6%	9%	17%	14%	8%	12%	4%	3%
Trouble concentrating	10%	9%	10%	16%	10%	10%	7%	6%	3%
Have become more isolated	8%	6%	9%	13%	13%	5%	2%	8%	2%
Other	4%	3%	0%	3%	4%	7%	4%	9%	5%
None of these	20%	26%	19%	17%	15%	32%	20%	25%	13%

Feelings of anxiety , stress, fear or frustration were somewhat more common among women 18-29 (49%), women 30-49 (46%) and women 50-64 (44%) than among men in the same age groups. Noticeably more women 18-29 also found it difficult to trust (38%), and intense outrage and anger (28%). A lot more women 50-64 also found it difficult to trust (44%), and women over 65 helpless and feeling they will to be the victim of future cybercrimes (37%). Men in the 50-64 age group felt the biggest sense of outrage and anger (40%).

Around 1 in 3 men 50-64 experienced none of these feelings (32%), as did 1 in 4 men aged 18-29 (26%) and over 65 (25%). This was significantly higher than for similarly aged women.

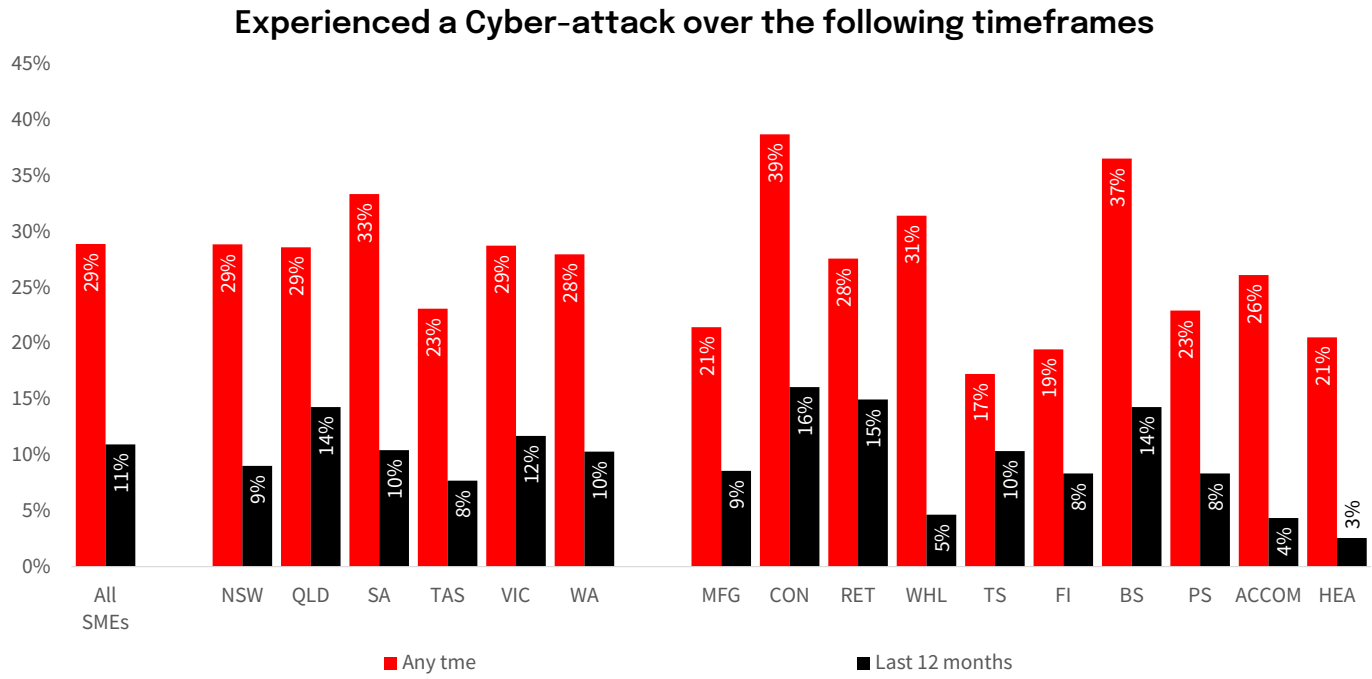
Cyber security - The view from SMEs

Cybercrime can have a significant impact on business of all sizes. ACSC data for 2021-22 estimated the average cost per cybercrime at over $39,000 for small business, $88,000 for medium business, and over $62,000 for large business - an average increase of 14%.

The ACSC also noted that many small and medium-sized business are often less security conscious, less likely to implement cyber security measures, and spend less on cyber security measures than large organisations, leaving them more exposed to attacks.

In the second part of this report we establish how many Australian SMEs have experienced a cyber-attack or data breach, the nature of the attack, how much money was involved, and what percentage of their organisation's capital expenditure budget will be spent on cyber prevention recovery, insurance, education, training etc. in the current financial year.

The results are based on survey responses from around 800 Australian SMEs conducted over the period 14 February to 9 March 2023.



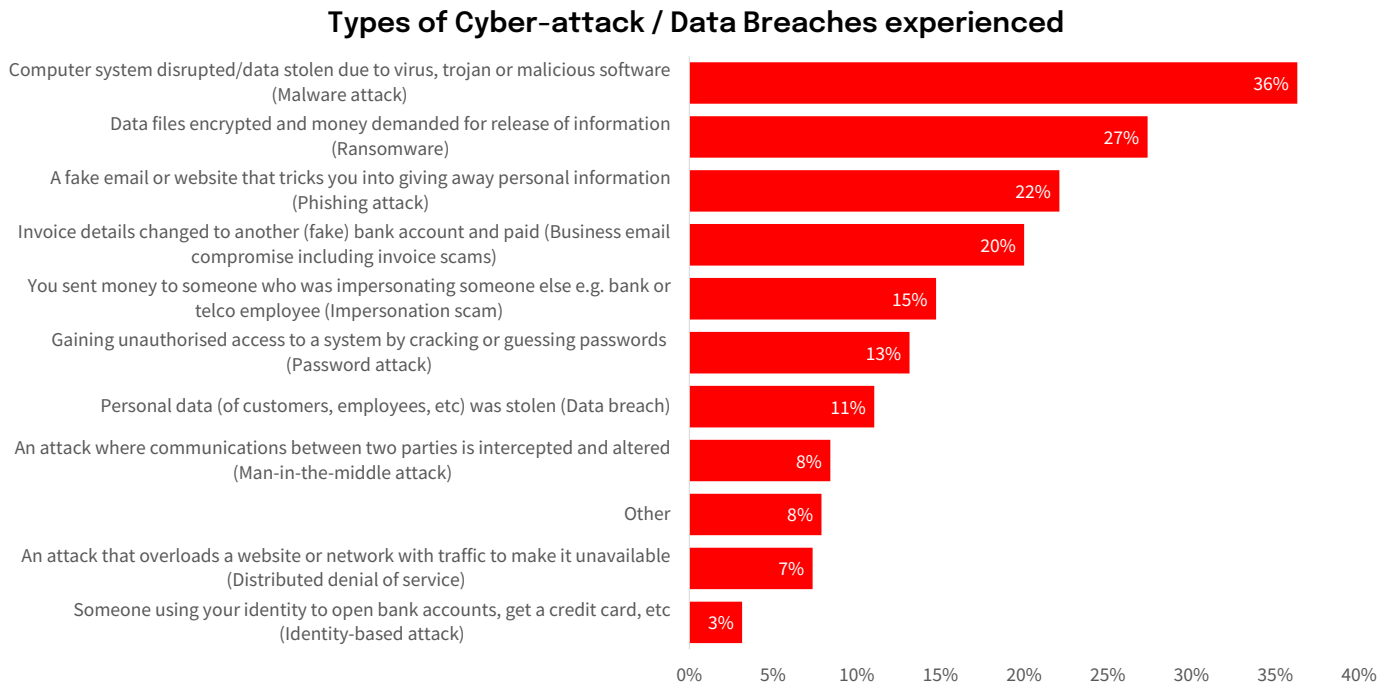
How many SMEs have experienced a cyber-attack or data breach…?

Around 3 in 10 (29%) SMEs overall have experienced a cyber-attack or data breach during the life of their business. Just over 1 in 10 (11%) have experienced an attack in the last 12 months. **On average, SMEs also estimate they lost around $19,400 as a result of cyber-attacks in the last 12 months.**

By state, the number of SMEs that experienced a cyber-attack or data breach during the life of their business was highest in SA (33%) and lowest in TAS (23%). Over the last 12 months however, attacks were most common in QLD (14%) and least common in TAS (8%) and NSW (9%).

The number of businesses impacted by a cyber-attack or data breach ranged considerably by industry. The number of attacks during the life of their business was highest in Construction (39%) and Business Services (37%). It was lowest in the Transport & Storage (17%) and Finance & Insurance Services (17%) sectors.

Over the past 12 months, cyber-attacks or data breaches impacted most SMEs operating in Construction (16%), Retail (15%) and Business Services (14%). Attacks were least common in the Health Services (3%), Accommodation & Hospitality (4%), and Wholesale Trade (5%) sectors.



Type of cyber-attack/scam/data breach experienced.

Around 1 in 3 SMEs (36%) experienced a malware attack, just over 1 in 4 (27%) ransomware, and 1 in 5 a phishing attack (22%) or business email compromise, including invoice scams (20%). The least common attacks experienced by SMEs were identity based attacks (3%), distributed denial of service (7%), and other or man-in-the-middle (8%) attacks.

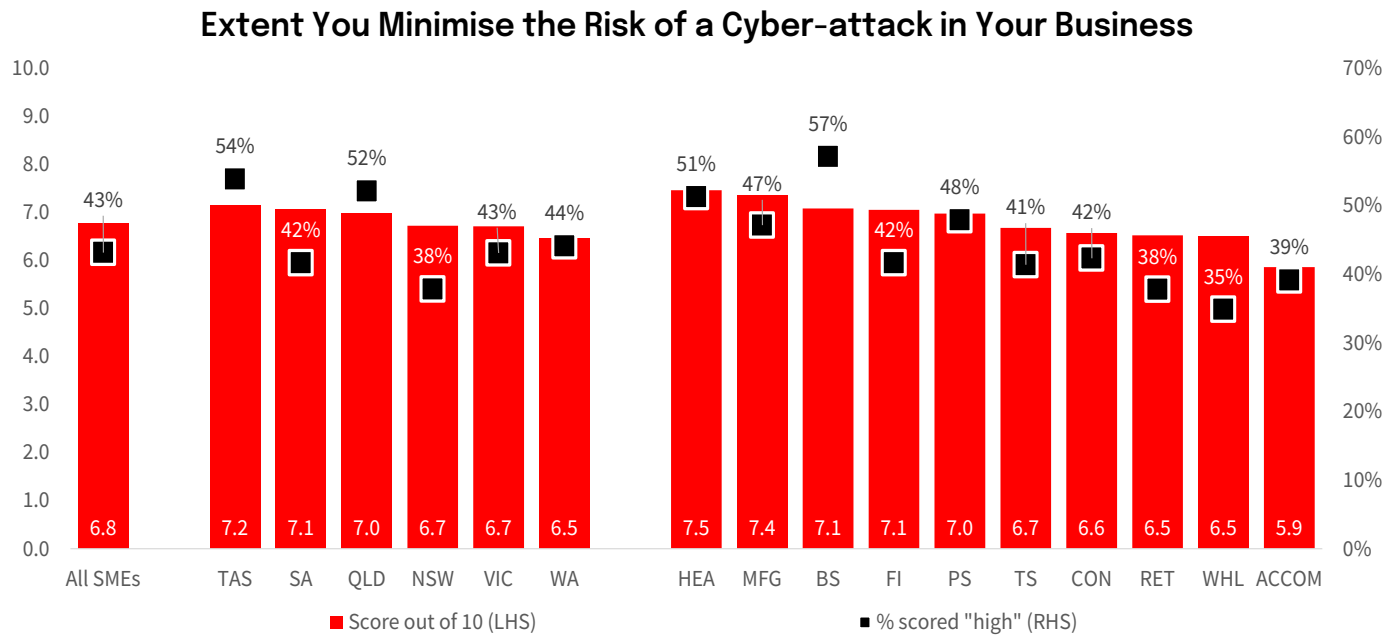
Type of cyber-attack/data breach experienced

	Malware attack	Ransomware	Phishing attack	Business email compromise	Impersonation scam	Password attack	Data breach	Man-in-the-middle attack	Other	Distributed denial of service	Identity-based attack
All SMEs	36%	27%	22%	20%	15%	13%	11%	8%	8%	7%	3%
NSW	41%	23%	19%	23%	13%	13%	11%	14%	8%	6%	2%
QLD	32%	26%	26%	26%	24%	26%	6%	12%	6%	6%	9%
SA	44%	38%	19%	19%	19%	0%	13%	0%	13%	0%	0%
TAS	67%	67%	33%	0%	0%	0%	0%	0%	33%	0%	0%
VIC	31%	22%	24%	17%	13%	13%	13%	4%	7%	11%	4%
WA	32%	42%	21%	11%	11%	5%	16%	5%	5%	11%	0%
MFG	33%	20%	13%	33%	7%	20%	7%	7%	20%	7%	0%
CON	40%	30%	23%	26%	9%	9%	9%	8%	9%	8%	9%
RET	34%	17%	20%	26%	9%	17%	14%	6%	14%	9%	3%
WHL	37%	41%	11%	11%	19%	19%	7%	15%	4%	7%	0%
TS	40%	60%	40%	40%	20%	0%	20%	0%	0%	0%	0%
FI	29%	0%	43%	29%	0%	14%	14%	0%	0%	0%	0%
BS	35%	26%	35%	13%	35%	4%	4%	17%	4%	13%	0%
PS	36%	9%	27%	0%	27%	27%	18%	9%	0%	9%	0%
ACCOM	33%	50%	17%	0%	17%	0%	17%	0%	0%	0%	0%
HEA	38%	38%	13%	0%	13%	13%	25%	0%	0%	0%	0%

Malware and ransomware attacks were typically the most common types of cyber-attacks experienced by business in all states (particularly TAS & WA) and in most industries (particularly Transport & Storage, Construction and Accommodation & Hospitality firms).

The table above also shows a much higher number of SMEs in NSW (23%) and QLD (26%) impacted by business email compromise including invoice scams, and man-in the-middle attacks (14% & 12% respectively). Noticeably more firms in QLD were also impacted by impersonation scams (24%), password attack (26% and identity-based attack (9%). Phishing attacks were somewhat more common in TAS (33%), data breach in WA (16%), and distributed denial of service in VIC and WA (11%).

By industry, we also discovered a higher number of SMEs in the Manufacturing sector impacted by business email compromise, including invoice scams (33%), in Construction malware (40%) and identity based attacks (9%), in Transport & Storage malware (40%), ransomware (60%), phishing (40%) and business email compromise, invoice scams (40%), in Finance & Insurance Services phishing attacks (43%), Business Services impersonation scams (35%), man-in-the-middle attack (17%) and distributed denial of service (13%), in Accommodation & Hospitality ransomware (50%), and in Health Services data breach (25%).



Extent you feel you minimise the risk of a cyber-attack on your business…

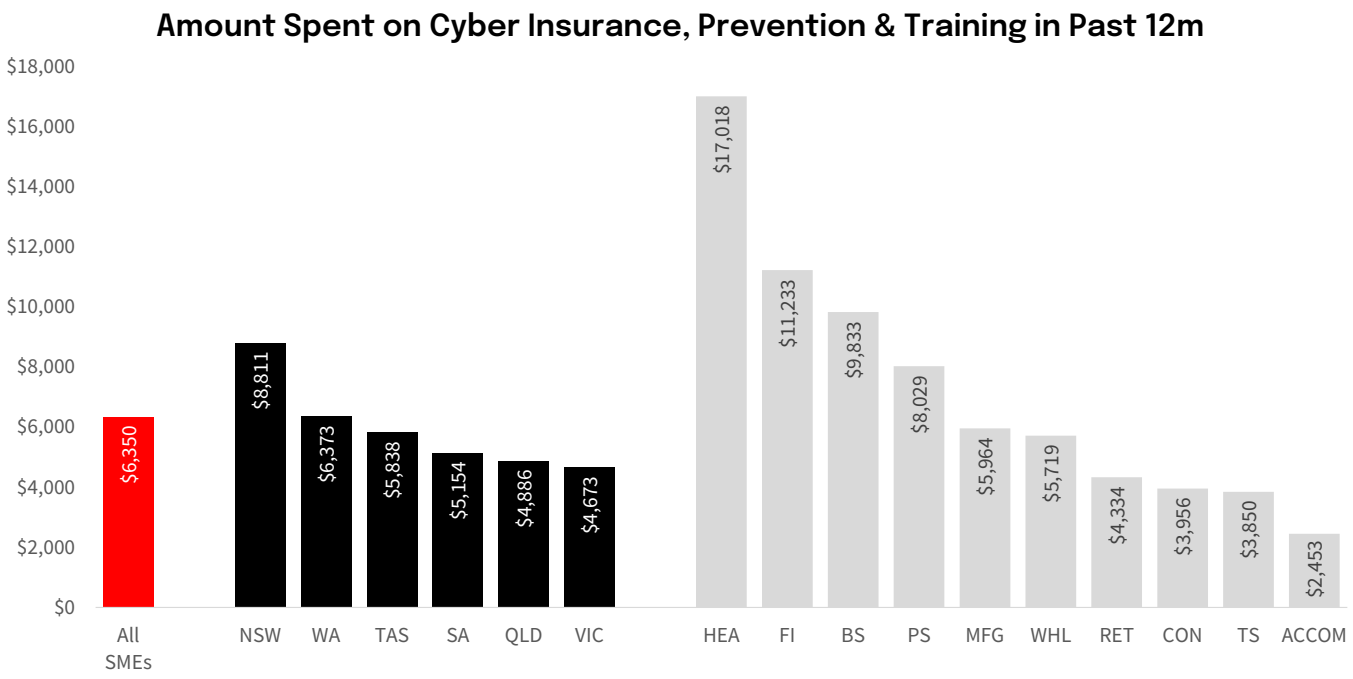
On average, Australian SMEs feel “moderate to quite” comfortable about the extent they are minimising the risk of a cyber-attack on their business. When asked to rate how they felt, on average they scored 6.8 pts out of 10 (0 = not at all; 10 = significantly). Though 4 in 10 (43%) businesses overall believe they are being very vigilant (scoring 8 pts or higher), around 15% feel they are doing this “poorly” (scoring between 0-4 pts).

By state, scores were highest in TAS (7.2 pts), SA (7.1 pts) and QLD (7.0 pts), and lowest in WA (6.5 pts), VIC and NSW (6.7 pts). Over 1 in 2 SMEs in TAS (54%) and QLD (52%) said they were being very vigilant trying to minimise the risks to their business, compared to only 38% in NSW.

By industry, SMEs in the Health Services (7.5 pts) and Manufacturing (7.4 pts) sectors scored highest, and Accommodation & Hospitality (5.9 pts), Wholesale Trade (6.5 pts), Retail Trade (6.5 pts), Construction (6.6 pts) and Transport & Storage 6.7 pts) firms lowest. The number SMEs who think they are being very vigilant trying to minimise risks was highest in the Business Services (57%) sector and lowest in Wholesale Trade (38%).

How much have SMEs spent on cyber insurance, prevention & training?

On average, SMEs have spent $6,350 on cyber insurance prevention in the past 12 months. By state, spend was highest in NSW ($8,811), and lowest in VIC ($4,673). By industry, spending was highest by some margin in Health Services ($17,018), and almost 10 times more than in Accommodation & Hospitality Services were spend was lowest overall ($2,453).



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 0 457 517 342

Robert De Iure
Associate Director Economics
Robert.De.Iure@nab.com.au
+61 0 477 723 769