

A large, dark blue stylized letter 'W' dominates the right side of the page. Inside the 'W', there is a glowing, intricate network pattern resembling a fiber-optic or neural network, with bright white and yellow nodes connected by thin lines.

Cyber Security Research Report

Prepared for Australian Signals
Directorate

September 2020





Contents

<u>Background, objectives and methodology</u>	<u>3</u>
<u>Executive summary</u>	<u>8</u>
<u>Detailed findings</u>	<u>13</u>
<u>Context</u>	<u>14</u>
<u>Understanding of cyber security</u>	<u>23</u>
<u>Actions undertaken</u>	<u>36</u>
<u>Segment analysis</u>	<u>48</u>
<u>Trusted organisations</u>	<u>56</u>
<u>Australian Cyber Security Centre (ACSC) and 2020 Strategy</u>	<u>62</u>
<u>Information needs</u>	<u>67</u>
<u>Appendix: Demographics</u>	<u>74</u>

A large, dark blue letter 'W' dominates the right side of the slide. It is filled with a complex, glowing pattern of white and yellow lines and dots, resembling a cosmic web or a neural network. The background is white.

Background, objectives and methodology

Background

The Australian Cyber Security Centre (ACSC) runs the Stay Smart Online (SSO) Program to provide relevant and timely information on how home internet users and small businesses can protect themselves from cyber security threats such as software vulnerabilities, online scams, malicious activities and risky online behaviours. This includes an annual campaign: *Stay Smart Online Week*, which aims to raise awareness and drive behaviour change to improve cyber security.

The ACSC identified a need to conduct exploratory research to better understand audience awareness of cyber security practices, as well as the ACSC and SSO brand recognition. Identification of audience segments, specifically, which groups are most likely to change their behaviour or be resistant to change, is also required.

This research will be used to inform next steps in branding and communications.



Australian Government

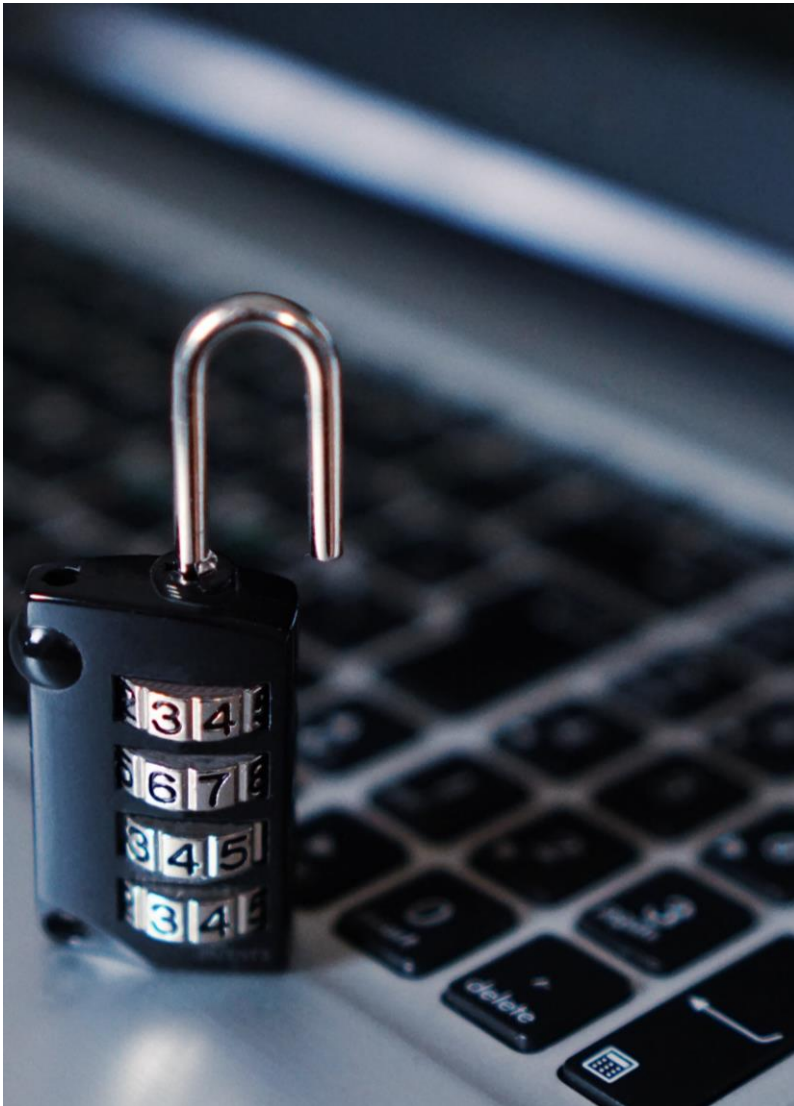
Australian Signals Directorate

ACSC

Australian
Cyber Security
Centre



Research objectives



The overarching objective of the research program is to understand levels of community awareness, understanding and behaviours in relation to the current cyber security threat in Australia.

The research will also establish the need and requirement (or otherwise) for communications to various audiences within the Australian community and inform communication imperatives.

Specifically, the research was designed to establish:

- Awareness of the ASCS and knowledge of the services and information it provides.
- Knowledge of where to go for information.
- Types of information desired by the Australian public.
- Levels of trust in various organisations and entities.
- The importance of online security to various subgroups within the community.
- Levels of confusion with other services and information sources, both government and non-government sponsored.
- Changes that people are willing or unwilling to make around cyber security.



Research methodology

Nationally representative quantitative survey

Sample size

- A representative sample of n=2,000 Australians, aged 18 years and over.

Representation

- Survey quotas applied for age, gender and location.
- Weighting applied at the analysis stage to age / gender / location proportions based on ABS census data.

Margin of error and confidence level

- The maximum margin of error on a sample of n=2,000 is +/-2.2 at the 95% confidence level.
- Differences of +/-1% for net scores are due to rounding.

Timing

- 15 minutes in length (full survey).
- Conducted from the 25th August to the 1st September 2020.



Reporting notes: segment definitions

The table below shows the definitions of sub-sample segments described throughout the report:

Label	Description
SME	Owner, financial partner or main decision maker in an Australian business turning over more than \$75,000 per annum
SME contracts cyber	SME which hires or contracts a company/provider to manage IT and cyber security
ATSI	Aboriginal or Torres Strait Islander origin
CALD	Culturally and/or linguistically diverse
Kids in hhold	Dependent children aged 18 years or under living in household
Kids 0-9 yrs	Dependent children aged 9 years or under living in household
Kids 10-18 yrs	Dependent children aged between 10 to 18 years living in household
Heavy internet user	Average of 6 hours or more spent on the internet each day, either personally or at workplace
Medium internet user	Average of 2 to 6 hours spent on the internet each day, either personally or at workplace
Light internet user	Average of up to 2 hours or less spent on the internet each day, either personally or at workplace
‘Savvy’ segment	Those with an expert or good understanding of cyber security who have implemented cyber security measures in their household to a great or moderate extent
‘Moderate’ segment	Those with an average understanding of cyber security who have implemented cyber security measures in their household to some extent or better
‘At risk’ segment	Those with a low or no understanding of cyber security and/or have implemented cyber security measures in their household to a small extent or not at all



Executive summary



Key insights summary and recommendations

Cyber security information is relevant to everyone

Use of multiple devices and programs leaves Australians exposed to cyber attack in a multitude of ways. Almost universal internet connection also means that almost everyone is vulnerable, with older and lower income people the most out of their depth and least likely to be able to detect threats and protect themselves.

Poor understanding and competency make some groups more vulnerable

Many more people are aware of the risks and concerned about cyber security than are actually capable and prepared against attacks. For example, older people, regional residents, lower income earners and light internet users all report lower levels of understanding or competency and should be a key target for information.

An obvious need for better education and information

Very few people know clearly what to do or where to go to be cyber secure, even though they are generally aware of and concerned about a wide range of potential threats across a variety of platforms and activities. The need for improved education and information could not be clearer.

Complacency compounds potential exposure to cyber attack

There is some complacency towards cyber security, with feelings of security exceeding measures actually implemented. Many people admit to the implementation of little or no security measures. Improved implementation of basic cyber security protocols is required across the population.

Lack of a known cyber security agency hampers reporting of attacks

Government websites are considered a key information source on cyber security, yet for the many people experiencing cyber breaches, only about 1 in 2 typically reports, with a key reason being not knowing where to report. Lack of awareness of a dedicated Government cyber security agency is part of the problem.



Key insights summary and recommendations (cont'd)

The ACSC is trusted by those who know it, and naturally trusted by others

There is low existing awareness of the ACSC, but very high trust among this aware group, comparable to trust of the Australian Federal Police. Importantly, the ACSC is intuitively thought of as the best source of cyber security information and for assistance on cyber crimes.

The ACSC name automatically gives it credibility

The Australian Cyber Security Agency, by its very name, is naturally seen to have credibility on cyber security issues. The ACSC engenders confidence. It is a well-kept secret that needs to be shared and potentially positioned as the single source for Government information and assistance on cyber security.

The ACSC fills a gap in the market for a trusted source on cyber security

Australians are generally interested in knowing or hearing more about the Australian Cyber Security Strategy, especially a 24/7 hotline. Most people would go to the ACSC website for information or assistance on cyber crime, so it appears to fill a gap in the market for a trusted Government source on cyber security.

Most want more cyber security info from a single Government site

It is a particularly compelling result that half the population wants to hear more about cyber security. Identity theft, internet fraud, ransomware and email compromise are the key areas of interest, but interest extends to all threats. A single dedicated Government website is the main preferred source of information.



Key opportunities for the ACSC

1. Raise profile of ACSC as the trusted Government source on cyber security




The name says it all – brand it consistently across all communications and advice and make the ACSC the automatic go-to for all cyber security matters.

2. Define the core offerings

Clearly define the role of the ACSC – the site for prevention, reporting and response on cyber security.

3. Tailor content to meet the needs of the different cyber segments

Tailor content for different cyber segments:

-  **At risk** need basic easy-to-follow information and advice to reduce their confusion.
-  **Moderates** need more detailed information to match their capacity to their exposure.
-  **Savvy** need detailed, sophisticated and up-to-date information to help keep them informed and responsive to emerging threats.



What is the ACSC's role for each of the cyber segments?



Savvy segment: High level understanding of cyber security and implementation of cyber security measures.

'Savvy' segment is proactively looking for information and advice to make them even more cyber secure

- Highly connected, internet dependent and both aware and concerned about cyber security threats – they are actively interested in knowing more.
- ACSC can play a vital role, as a ready reference for information and recommended actions on new and emerging cyber threats.
- Prime segment candidate to subscribe to or follow the ACSC for alerts.



Moderate segment: Average level understanding of cyber security and implementation of cyber security measures.

'Moderate' segment is apathetic towards risks and need ACSC as an easy go-to single source of trusted information

- Underestimate risks and their level of unpreparedness for cyber attacks. A mistaken sense of security means they can be apathetic towards information.
- Role for the ACSC is to provide information and advice on the range of threats via simple, easy to follow guides on how to become more cyber secure.
- Raise profile of ACSC as trusted go-to source on cyber security.



At risk segment: Poor understanding of cyber security and implementation of cyber security measures.

'At risk' segment has poor comprehension on cyber security and ACSC needs to reach out to them to provide basic protection

- Poor comprehension and capacity on cyber security makes them particularly vulnerable to attack and loss.
- Imperative is to raise profile of ACSC as a trusted source on cyber security.
- ACSC should provide step-by-step explanations, actions and advice on basic protocols and behaviours to implement at least minimum protection.



Detailed findings



Context



Section summary – context

Internet usage is extensive across a range of devices

The advent of connectivity of a wide range of household and portable devices, particularly smart phones, laptops and tablets, are a key reason for extensive internet usage. Approximately one in three (36%) adult Australians uses the internet for six hours a day or more, and three out of four (74%) spend more than two hours per day connected to the internet.

Social media is no longer just the domain of young people

It is a truism that social media is synonymous with youth, and indeed most under 35s report using five or more sites, but it is not exclusively their domain. The number of social media sites used does decrease with age, but most 35-59 year olds use three or more sites and most over 60s use two or more sites. In order, Facebook, Messenger, YouTube, Instagram and WhatsApp are the main sites.

Google dominates search engines and browsers

Google Chrome (56%) and Google (54%) dominate search engines used, with one out of every two people using at least one of these Google products. These products are useable on both a Windows and Apple platforms, in contrast to Safari (22%), the third-most commonly used browser, exclusive to Apple devices. On average, Australians use two search engines or browsers.

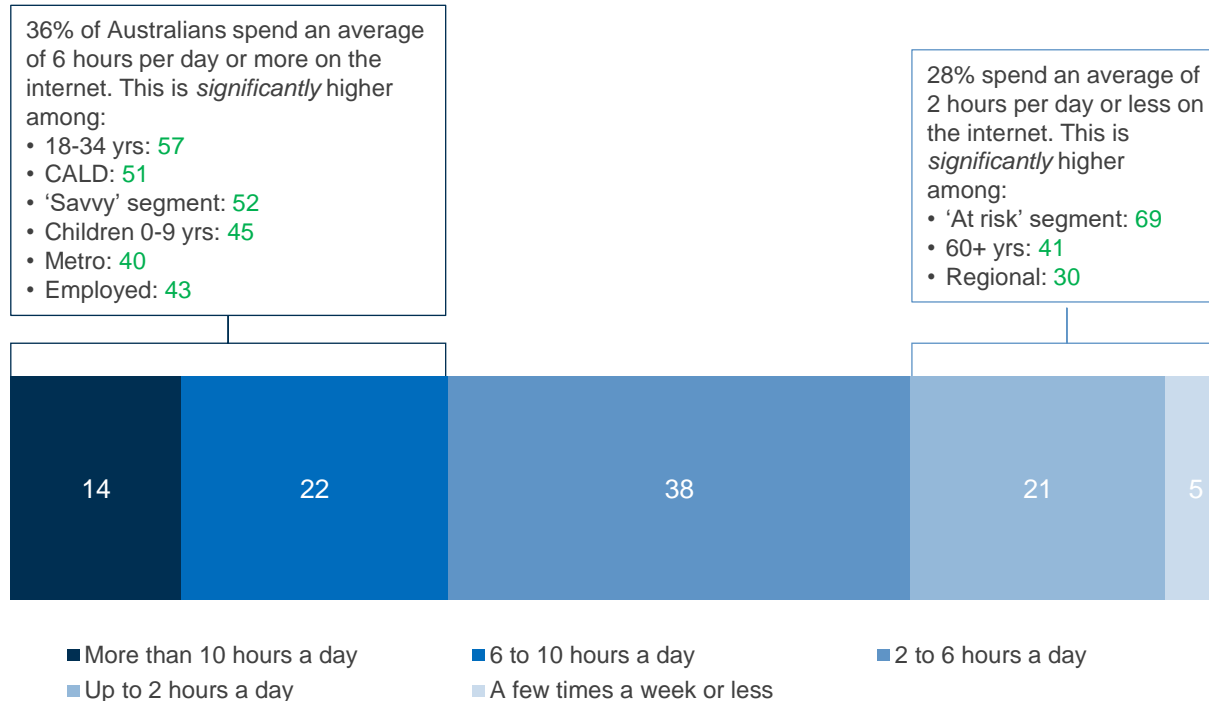
Email usage is universal, with a preference for a single provider

Email usage is universal, with 99% of Australian adults having an account. People do not use as many different providers as they do with browsers and social media. On average, people use 1.5 email providers, with potentially different providers used between work and home, although people may have multiple accounts with the same provider. Gmail (41%), Hotmail (39%) and Outlook (34%) are the key email providers used.

On average, younger and metro Australians are heavy internet users, older and regional Australians lighter users



Average time spent on internet (%)



Significantly *higher* than the total at the 95% confidence interval.

S4. On average, how much of each day do you spend on the internet, either personally or at your workplace?

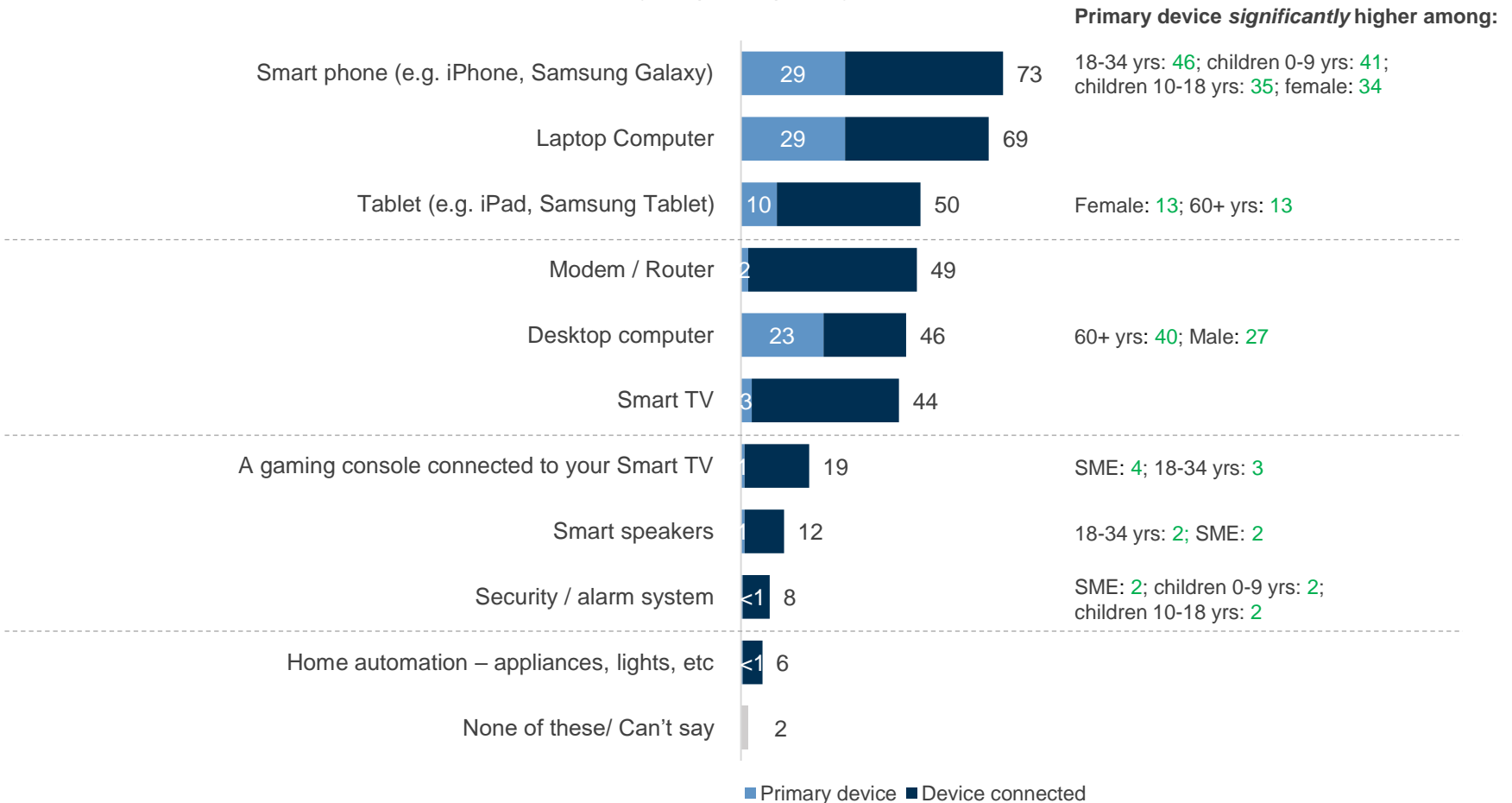
This includes accessing the internet on any device such as smartphones, iPads / tablets, laptop or desktop computers and includes any manner of internet activities such as checking email, online gaming, browsing social media, streaming video, online shopping, etcetera.

Base: All respondents (n=2,000).

Primary devices for internet connection are typically smart phones, laptops, desk top computers, or tablets



Devices connected to the internet (%)
(Multiple response)



Significantly *higher* than the total at the 95% confidence interval.

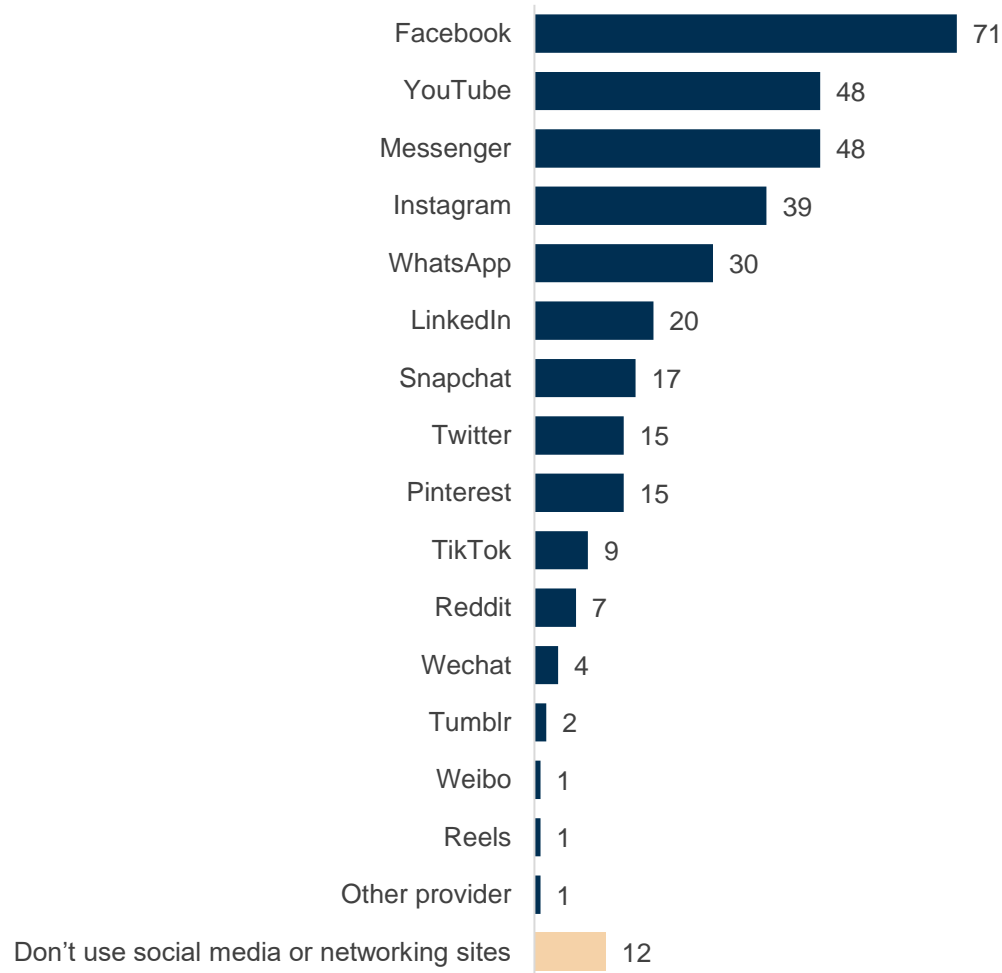
Q5. Which of the following devices do you have connected to the internet? / Q6. Thinking about all your online activities, which internet connected device would you say is your primary device: which do you spend most of your time on?

Base: All respondents (n=2,000).

Seven in ten Australians use Facebook, almost half use YouTube or Messenger



Social media and networking sites used (%)
(Multiple response)



There is high usage of social media across all demographics and segments



Social media and networking sites used (%) (cont'd)
(Multiple response)

	Total	Male	Female	18-34 yrs	35-59 yrs	60+ yrs	Metro	Regional	SME	SME contracts cyber	Kids in hhold	Internet Use			Segment		
												Heavy	Med.	Light	Savvy	Moderate	At risk
Facebook	71	69	74	76	73	63	72	71	69	70	77	78	72	61	74	74	70
Messenger	48	42	54	63	46	35	49	46	45	50	52	57	48	35	51	49	48
YouTube	48	50	46	64	45	33	48	47	50	61	50	59	48	31	61	49	43
Instagram	39	36	42	66	35	15	42	34	44	56	46	53	35	24	53	40	33
WhatsApp	30	32	29	38	34	16	36	19	35	42	43	37	29	22	42	31	27
LinkedIn	20	23	17	25	22	11	24	13	25	25	23	31	17	10	33	19	18
Snapchat	17	15	19	41	10	2	18	17	22	32	19	25	16	8	25	17	16
Pinterest	15	8	22	20	14	13	14	18	17	21	16	20	15	10	17	18	14
Twitter	15	18	12	23	15	7	16	12	20	25	18	24	12	6	25	15	12
TikTok	9	8	9	20	5	1	10	6	16	22	12	15	6	3	18	7	6
Reddit	7	8	6	17	4	1	8	5	9	12	5	14	5	1	14	6	5
Wechat	4	4	4	7	4	1	5	2	6	11	6	6	3	3	8	4	2
Tumblr	2	3	2	5	2	1	2	3	4	4	2	5	2	1	6	2	2
Reels	1	1	1	3	<1	0	1	1	3	3	2	2	1	<1	3	<1	1
Other provider	1	1	1	<1	1	1	1	1	0	0	1	1	1	<1	2	1	<1
Weibo	1	1	1	2	<1	0	1	1	3	4	1	2	0	0	2	1	<1
Don't use social media or networking sites	12	12	12	4	10	24	11	14	8	2	4	5	12	23	6	10	14

Significantly **higher** than the total at the 95% confidence interval.

Q9. Which **social media and networking** sites do you use?

Base: All respondents (n=2,000).

Most Australians use multiple social media platforms, with most younger Australians using five or more sites



Social media and networking sites used (%) (cont'd)
(Multiple response)

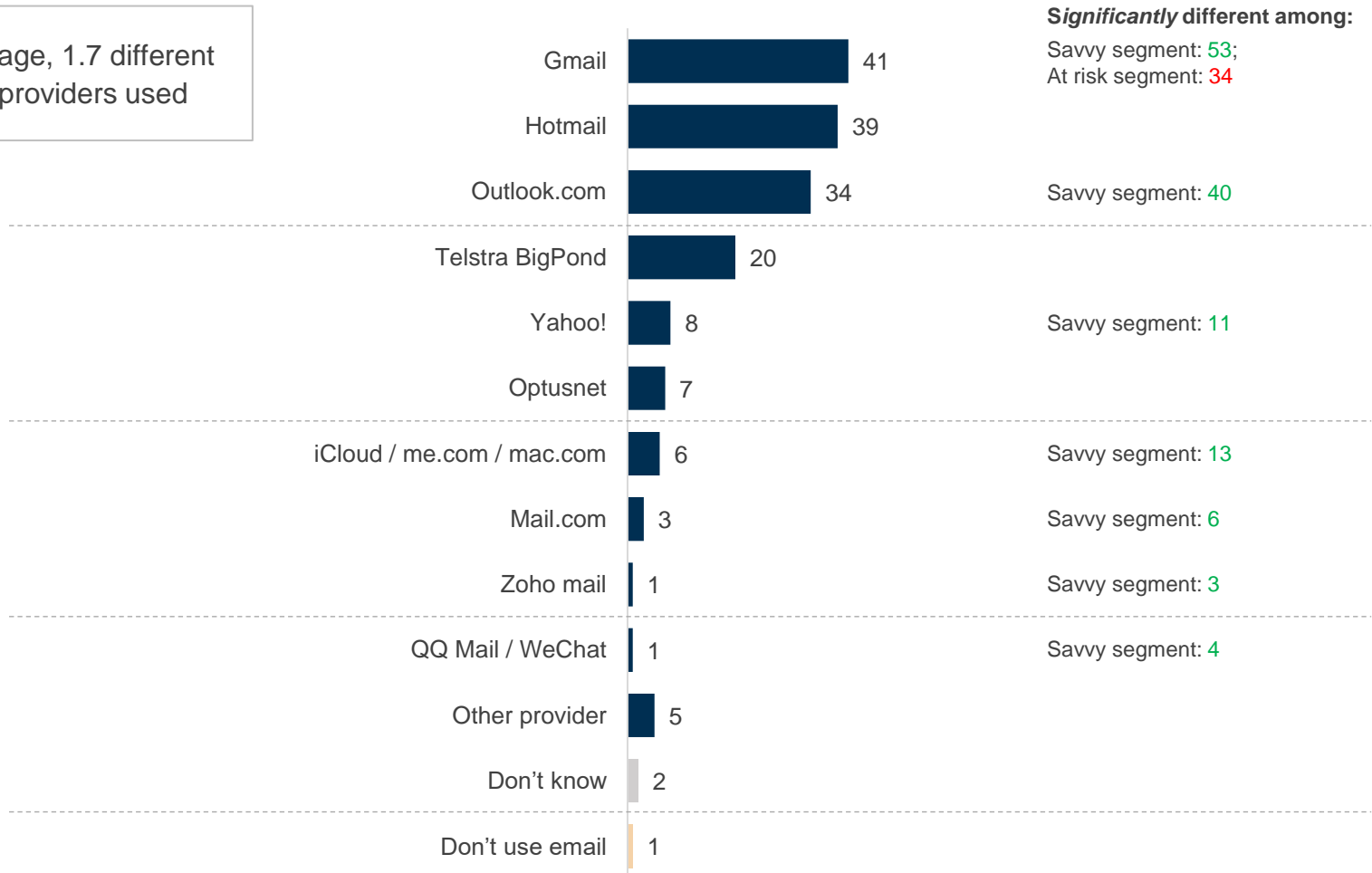
	Total	Male	Female	18-34 yrs	35-59 yrs	60+ yrs	Metro	Regional	SME	SME contracts cyber	Kids in hhold	Internet Use			Segment		
												Heavy	Med.	Light	Savvy	Moderate	At risk
Total 1 only	18	19	17	12	18	24	17	19	18	13	18	13	18	23	12	17	20
Total 2+	70	69	71	84	72	52	72	67	74	84	78	82	70	54	82	72	66
Total 3+	55	53	57	76	54	33	57	50	58	70	64	68	54	36	69	56	51
Total 4+	41	38	44	65	38	20	44	35	45	56	48	56	38	23	56	43	37
Total 5+	30	27	32	53	25	12	33	25	34	40	35	45	27	13	43	31	26

There is universal usage of email, with Gmail, Hotmail, Outlook and Telstra BigPond the dominant providers



On average, 1.7 different email providers used

Email providers used (%)
(Multiple response)



Significantly **higher** / **lower** than the total at the 95% confidence interval.

Q10. Which email providers do you use?

Base: All respondents (n=2,000).

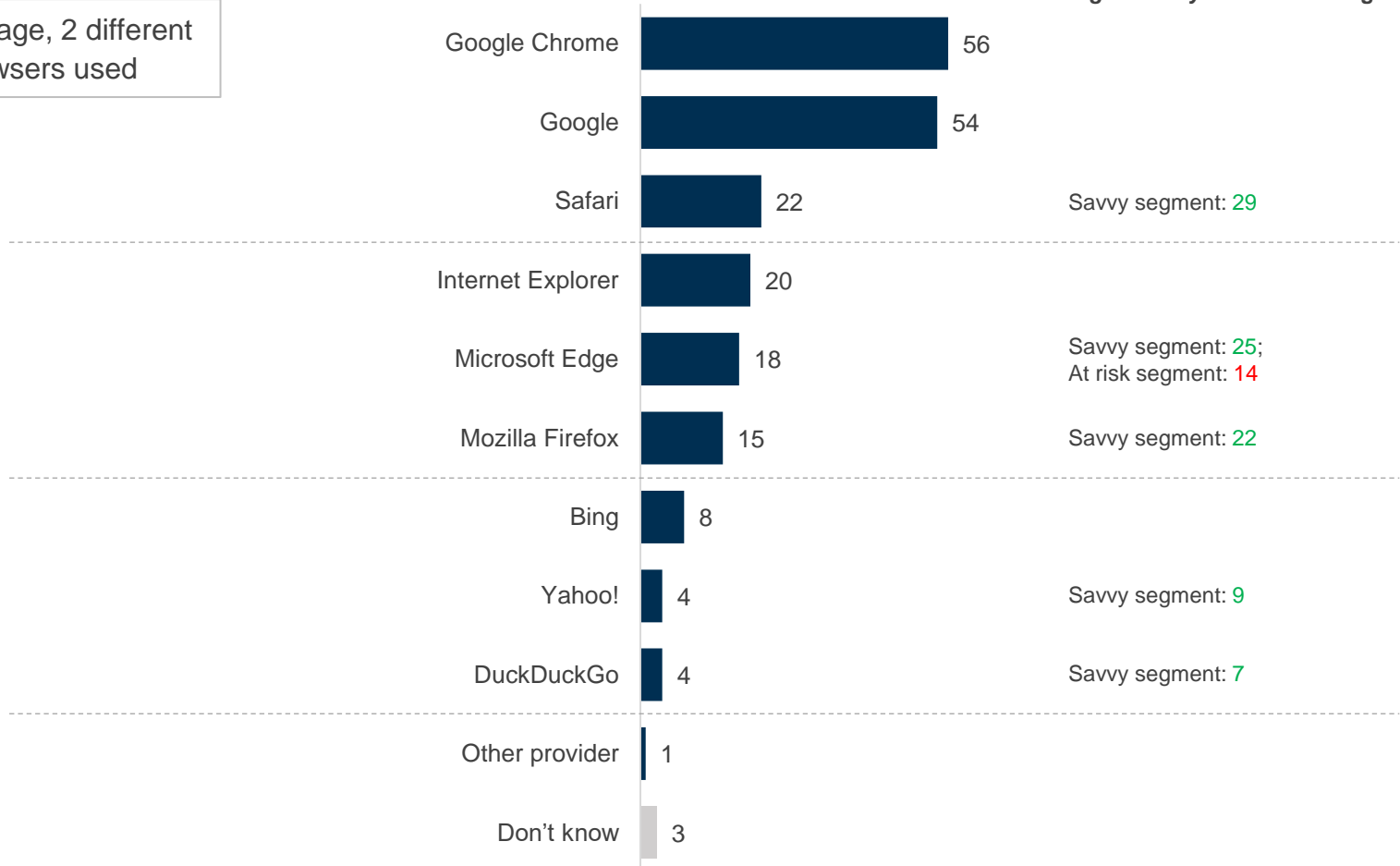
Google and Google Chrome dominate search engine usage, with significant usage of Safari, Explorer, Edge and Firefox



Search engines and browsers used (%)
(Multiple response)

Significantly different among:

On average, 2 different browsers used



A large, dark blue, stylized letter 'W' that serves as a background graphic. It is filled with a glowing, intricate network pattern of white and light blue lines and nodes, resembling a complex web or a neural network. The 'W' is positioned on the right side of the slide, extending from the top to the bottom.

Understanding of cyber security



Section summary – understanding of cyber security

High levels of concern about cyber security

Levels of concern about cyber security are high, with approximately one in two Australians indicating they are 'extremely' or 'very concerned' about it. They are most concerned about cyber security for Government (54%) and business (46%), more so than for themselves (43%).

Cyber security concerns are exacerbated by varying degrees of understanding

Cyber concerns are possibly exacerbated by the varying levels of understanding of cyber security. The majority understands cyber security, but only one in four (28%) considers themselves to have an 'expert' or 'good understanding'. Many are cognisant of the vulnerabilities every time they are online, as most agree anyone can be the victim of cyber crime, with potentially very serious consequences.

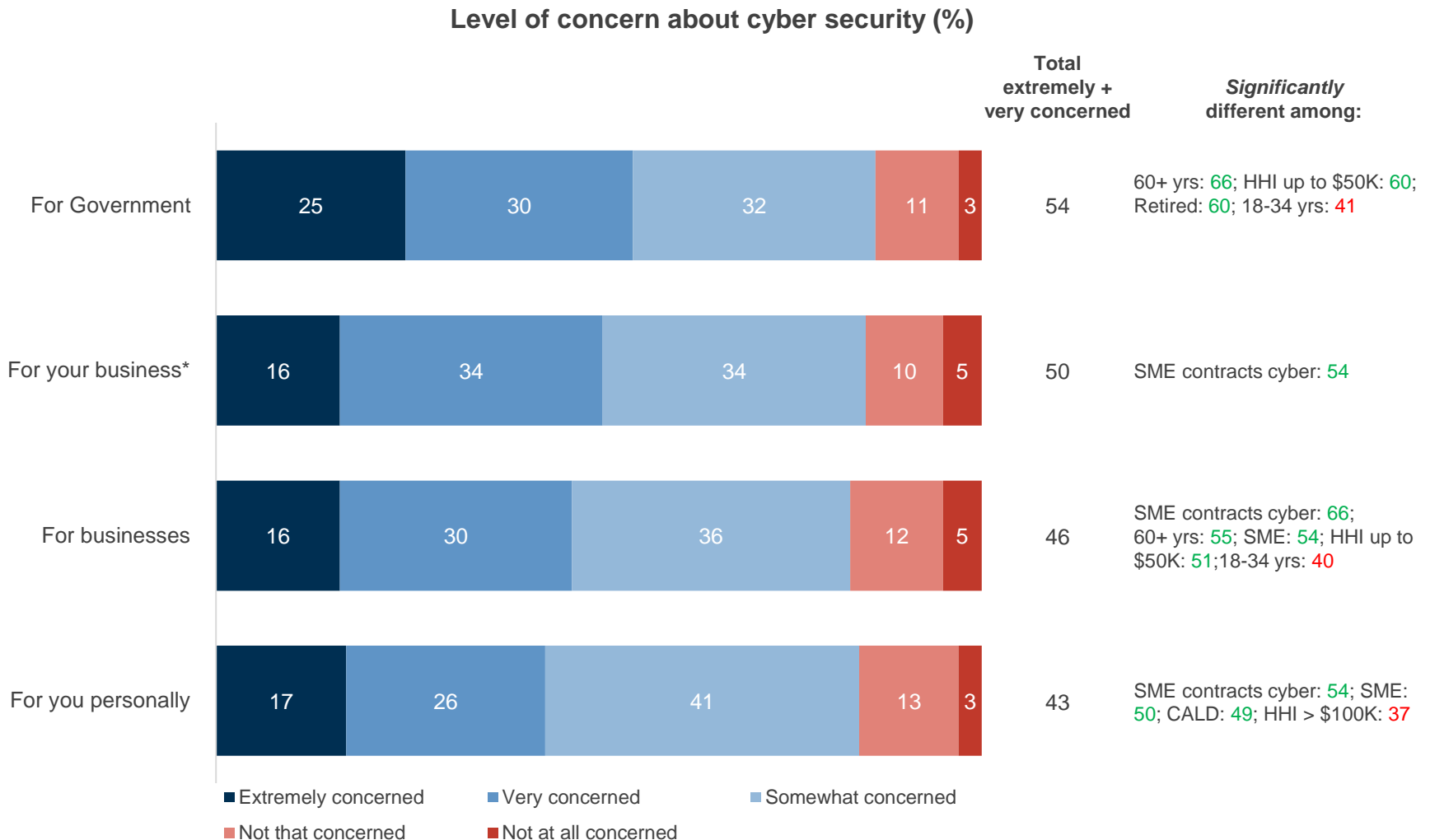
High levels of threat awareness but limited understanding

Awareness of cyber security threats is quite high, with between 63% and 77% having heard of the range of threats. However, understanding is far lower, with most only knowing 'a bit' about each threat. This lack of knowledge can contribute to higher levels of anxiety and increase the potential of becoming a victim. The greatest cyber security concerns relate to identity theft (76%) and fraud (72%).

Perception of risk does not necessarily reflect the reality

Perception of the risk of experiencing a cyber breach does not reflect levels of concern. Using social media is seen as attracting the highest level of vulnerability, with three out of five (60%) believing a breach is likely, yet only a third (34%) believe gaming and e-sports carry a risk. Some Australians' self-assessment of their understanding may not reflect reality.

Many people are concerned about cyber security, but more so for Government and business than for themselves



Significantly higher / lower than the total at the 95% confidence interval.

Q1. Cyber security means protecting data, information, devices and networks from malicious actors. It also involves protecting against harmful content and behaviours such as cyber bullying, image-based abuse and illegal and harmful online content. Please rate your level of concern about cyber security...

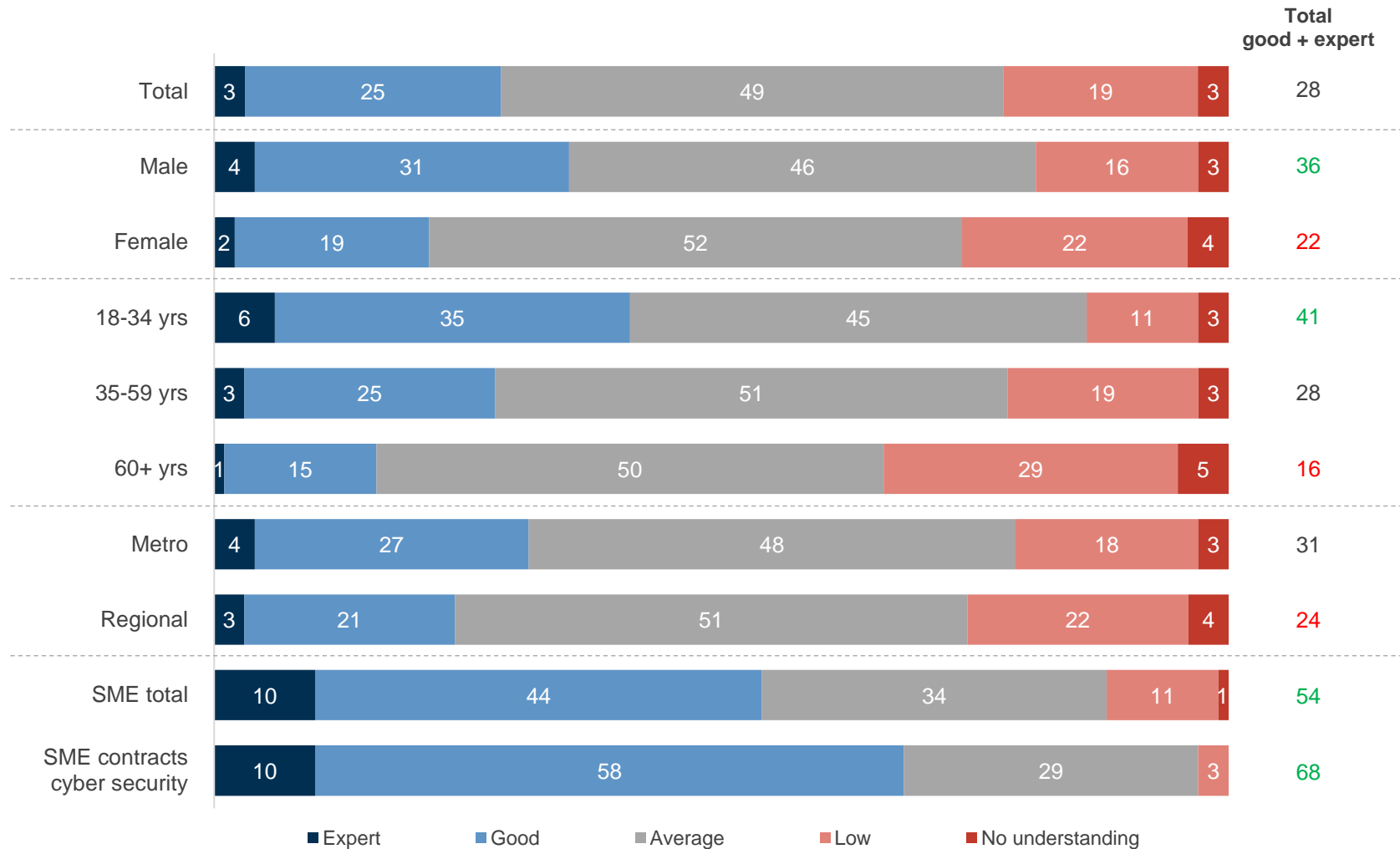
Base: All respondents (n=2,000); SMEs (n=340).

*Asked only among business owners.

Women, older and regional people have the poorest understanding of cyber security



Level of understanding about cyber security (%)

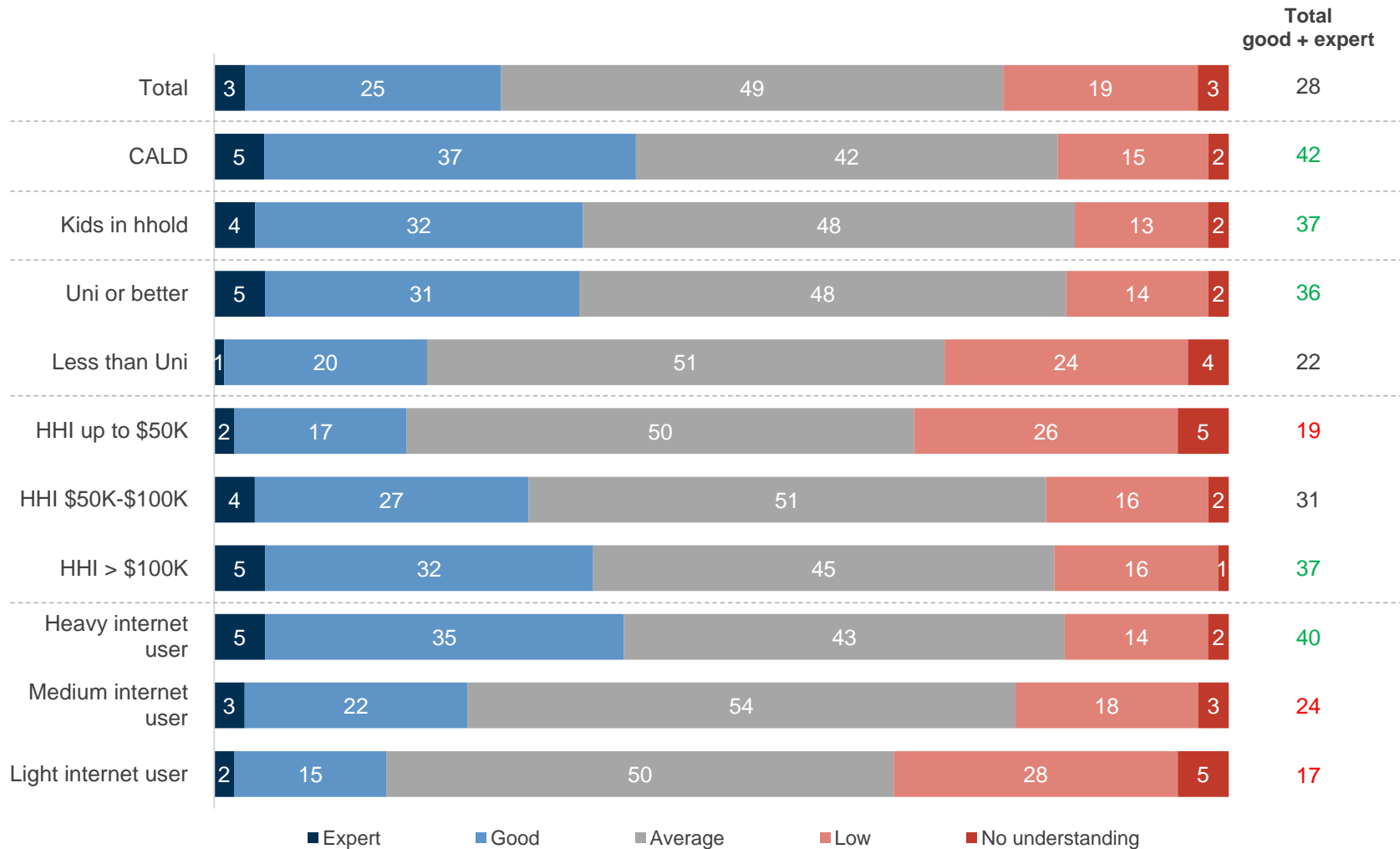


Significantly *higher* / *lower* than the total at the 95% confidence interval.
 Q3. Please rate your **personal level of understanding about cyber security**.
 Base: All respondents (n=2,000).

Lower income households and light to medium internet users also have poorer cyber understanding



Level of understanding about cyber security (%) (cont'd)

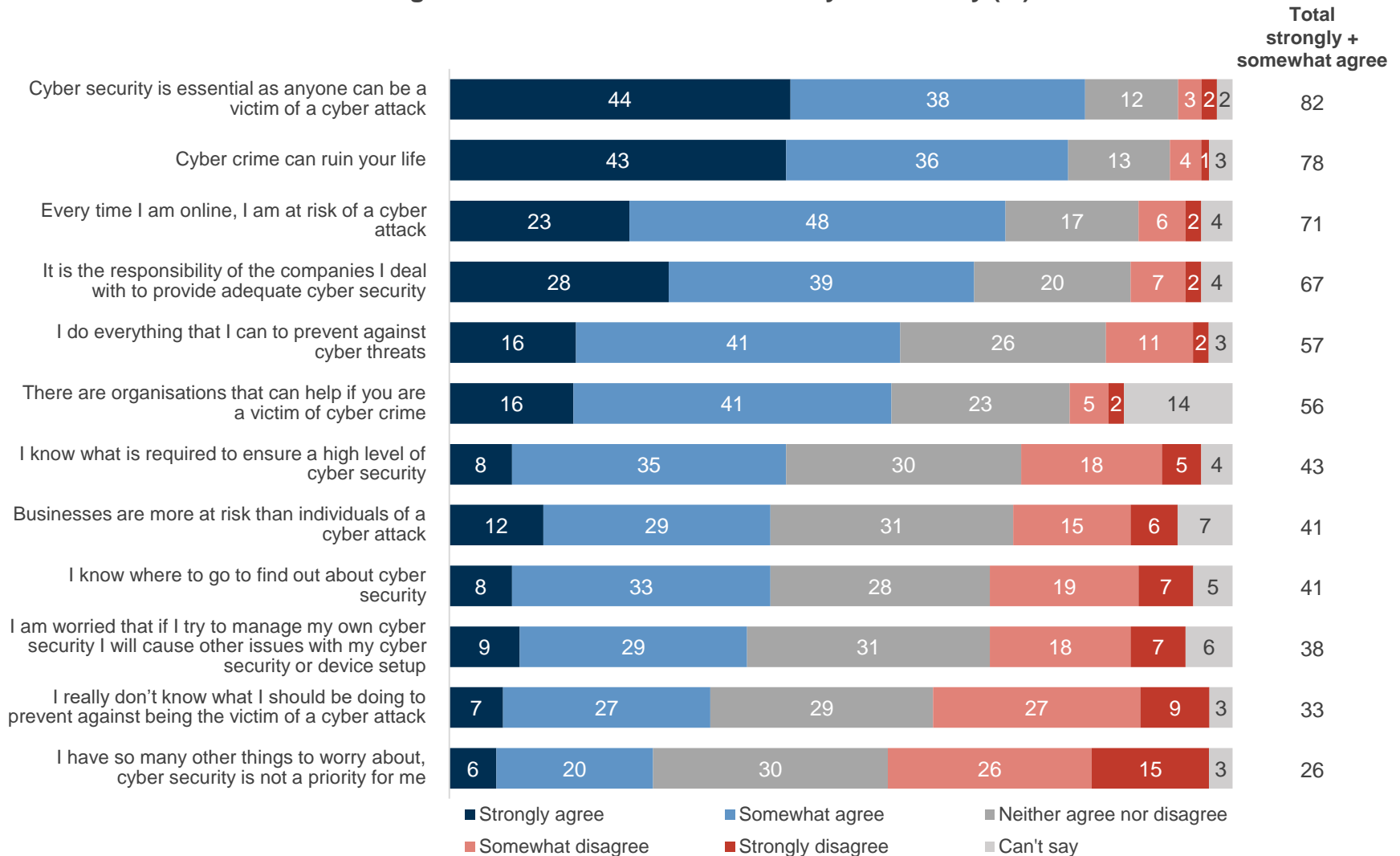


Significantly *higher* / *lower* than the total at the 95% confidence interval.
 Q3. Please rate your **personal level of understanding about cyber security**.
 Base: All respondents (n=2,000).

Most Australians appreciate cyber attacks are a real threat and that they have the potential to ruin your life



Agreement with statements about cyber security (%)



An admittedly poor understanding of cyber security does not lead older Australians into delusion about the risks



Agreement with statements about cyber security (%) (cont'd) (Total strongly + somewhat agree)

	Total	Male	Female	18-34 yrs	35-59 yrs	60+ yrs	Metro	Regional	SME	SME contracts cyber	Internet Use			Segment		
											Heavy	Med.	Light	Savvy	Moderate	At risk
Cyber security is essential as anyone can be a victim of a cyber attack	82	78	85	71	84	90	81	83	71	69	81	83	80	85	84	80
Cyber crime can ruin your life	78	74	83	69	82	84	78	80	67	58	79	79	78	87	79	76
Every time I am online, I am at risk of a cyber attack	71	69	73	60	75	76	70	71	67	67	71	70	71	76	74	68
It is the responsibility of the companies I deal with to provide adequate cyber security	67	65	69	62	67	72	65	70	60	60	67	67	66	76	68	65
I do everything that I can to prevent against cyber threats	57	56	58	46	57	70	57	58	59	69	58	58	56	84	66	37
There are organisations that can help if you are a victim of cyber crime	56	57	55	52	54	64	55	58	59	62	56	58	53	75	59	49
I know what is required to ensure a high level of cyber security	43	48	38	43	45	40	43	43	54	61	48	43	36	82	50	22
Businesses are more at risk than individuals of a cyber attack	41	43	38	44	36	44	41	39	47	50	43	39	40	50	40	42
I know where to go to find out about cyber security	41	46	37	43	42	39	42	41	51	60	47	40	36	78	48	22
I am worried that if I try to manage my own cyber security I will cause other issues with my cyber security or device setup	38	37	39	35	37	43	38	38	47	52	39	37	39	40	37	43
I really don't know what I should be doing to prevent against being the victim of a cyber attack	33	29	38	34	30	38	34	31	36	32	30	33	39	25	25	47
I have so many other things to worry about, cyber security is not a priority for me	26	27	25	34	24	20	27	23	36	35	29	25	24	31	20	33

Significantly higher / lower than the total at the 95% confidence interval.

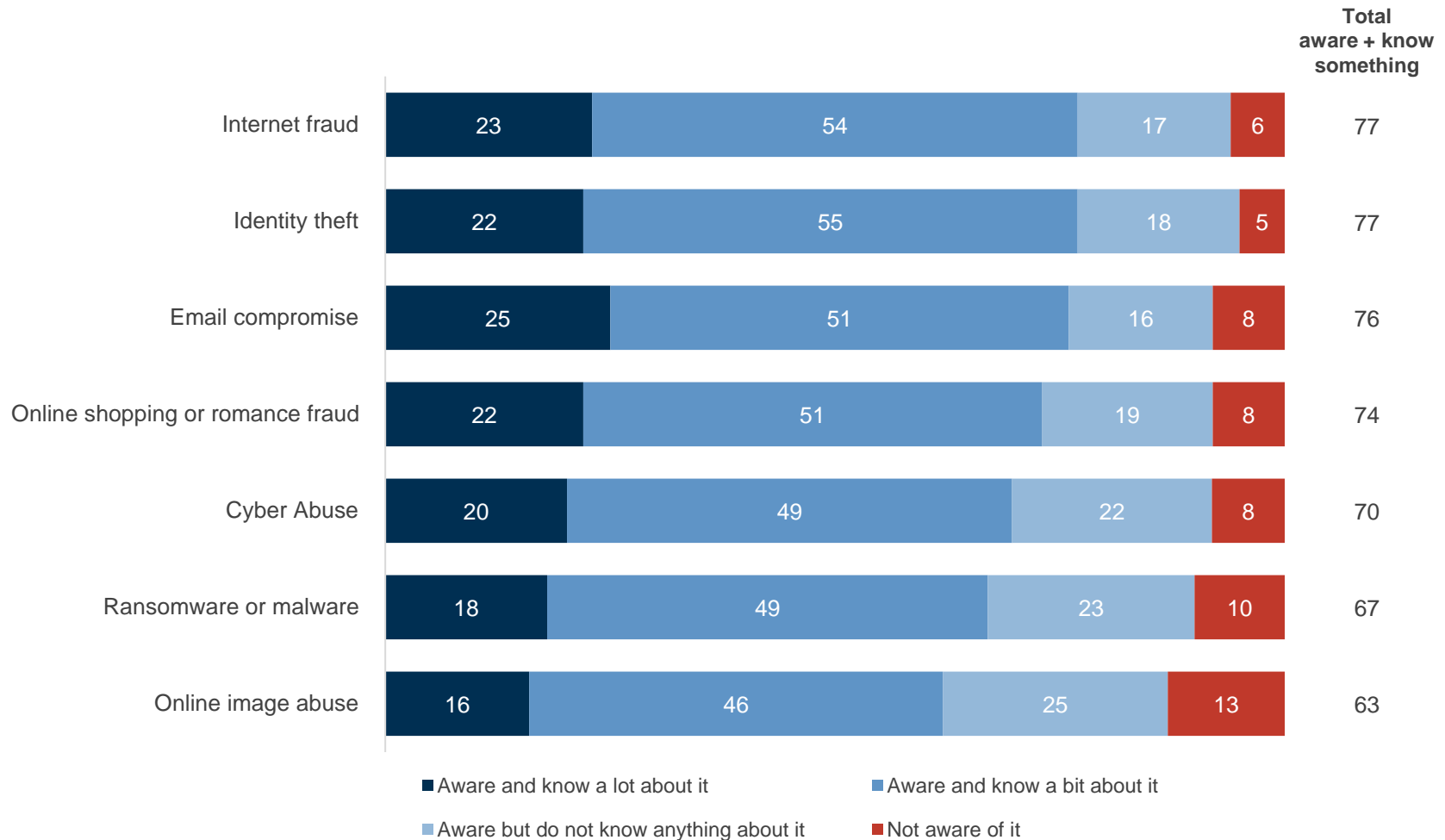
Q4. How much do you agree or disagree with each of the following statements about cyber security?

Base: All respondents (n=2,000).

Majority of Australians aware and have at least some knowledge of a great range of cyber threats



Knowledge of cyber security threats (%)



Older Australians have lower than average awareness and knowledge of many cyber security threats



Knowledge of cyber security threats (%) (cont'd) (Total aware + know something)

	Total	Male	Female	18-34 yrs	35-59 yrs	60+ yrs	Metro	Regional	SME	SME contracts cyber	Kids in hhold	Internet Use			Segment		
												Heavy	Med.	Light	Savvy	Moderate	At risk
Internet fraud	77	78	76	78	78	74	77	79	82	87	79	80	79	72	93	86	66
Identity theft	77	76	78	77	80	73	76	79	75	76	80	79	78	72	90	85	67
Email compromise	76	76	77	76	78	75	76	77	79	81	77	79	76	73	90	84	67
Online shopping or romance fraud	74	72	76	76	75	68	73	75	75	78	77	76	74	69	89	81	63
Cyber Abuse	70	68	71	75	73	59	70	69	70	71	73	76	68	63	86	77	59
Ransomware or malware	67	70	65	69	69	63	67	69	71	76	71	74	65	60	88	76	53
Online image abuse	63	63	62	74	64	48	63	62	70	74	71	70	63	52	84	69	51

Significantly higher / lower than the total at the 95% confidence interval.

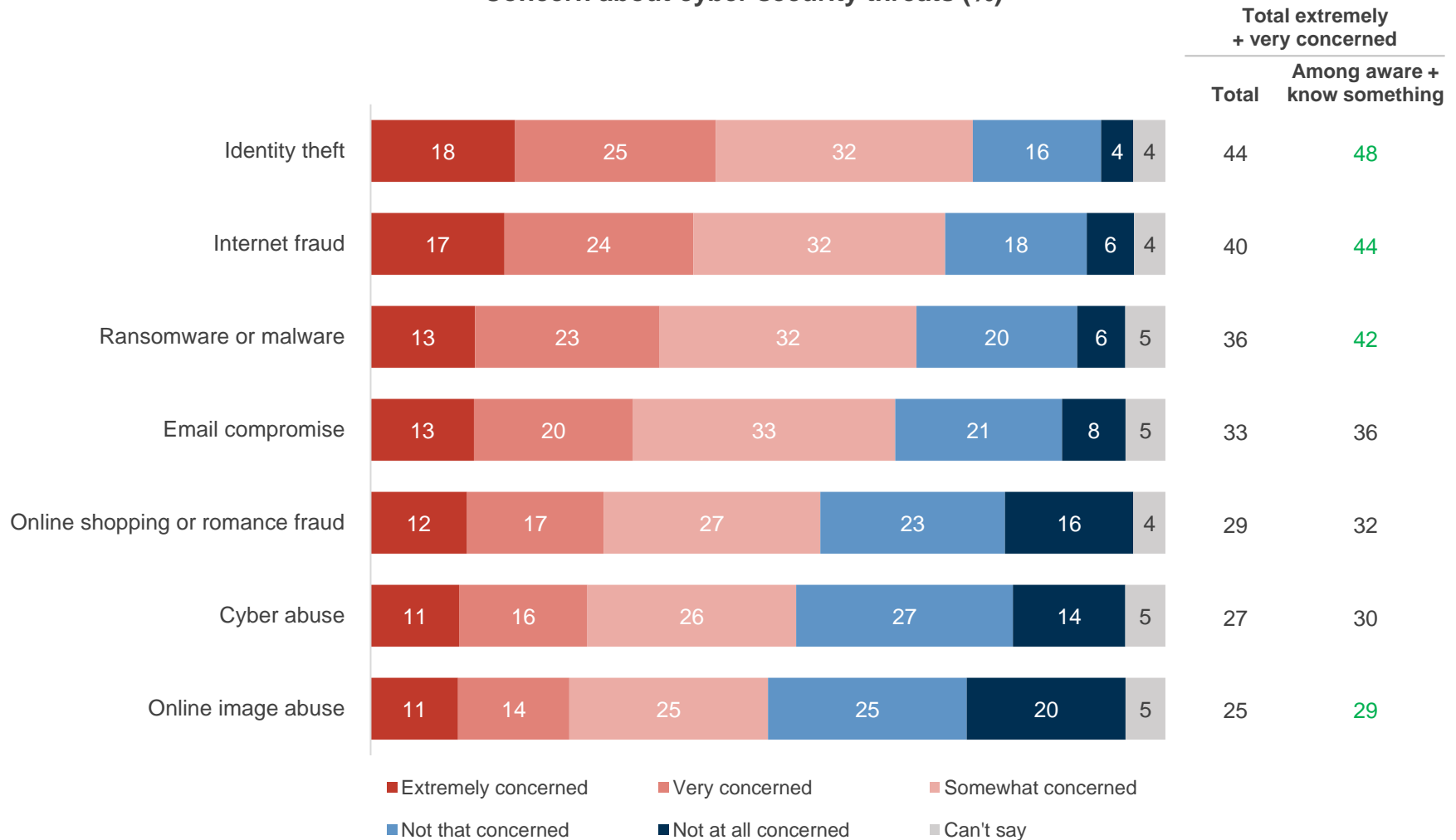
Q17. Which of the following cyber threats have you heard of before today and how much would you say you knew and understood about each of these?

Base: All respondents (n=2,000).

Most have at least some concern for every cyber threat, but identity theft and fraud are the key concerns



Concern about cyber security threats (%)



Significantly **higher** than the total at the 95% confidence interval.

Q18. How much of a concern are these cyber threats for you and your household?

Base: All respondents (n=2,000); those aware + know something about individual CS threats (n=499-887).

Concern about cyber security threats, by key analysis cohorts



Concern about cyber security threats (%) (cont'd) (Total extremely + very concerned)

44% of Australians are extremely or very concerned about **identity theft**, this is *significantly* different among:

- SME contracts cyber: **59**
- Savvy segment: **55**
- SME: **51**
- 60+ yrs: **49**
- At risk segment: **37**
- 18-34 yrs: **36**

33% of Australians are extremely or very concerned about **email compromise**, this is *significantly* different among:

- SME contracts cyber: **54**
- Savvy segment: **47**
- ATSI: **46**
- SME: **42**
- CALD: **39**
- At risk segment: **26**

27% of Australians are extremely or very concerned about **cyber abuse**, this is *significantly* different among:

- SME contracts cyber: **48**
- Savvy segment: **42**
- SME: **36**
- CALD: **32**
- HHI up to \$50K: **32**
- Kids in hhold: **32**
- Heavy internet user: **31**
- At risk segment: **22**

40% of Australians are extremely or very concerned about **internet fraud**, this is *significantly* different among:

- SME contracts cyber: **62**
- Savvy segment: **56**
- ATSI: **53**
- SME: **50**
- CALD: **49**
- Kids 10-18: **47**
- At risk segment: **35**

36% of Australians are extremely or very concerned about **ransomware or malware**, this is *significantly* different among:

- SME contracts cyber: **54**
- Savvy segment: **52**
- ATSI: **49**
- SME: **48**
- At risk segment: **29**

27% of Australians are extremely or very concerned about **online image abuse**, this is *significantly* different among:

- ATSI: **44**
- Savvy segment: **42**
- SME contracts cyber: **41**
- SME: **37**
- Kids 10-18: **36**
- CALD: **32**
- Kids in hhold: **31**
- Heavy internet user: **29**
- At risk segment: **20**

29% of Australians are extremely or very concerned about **online shopping or romance fraud**, this is *significantly* different among:

- SME contracts cyber: **50**
- Savvy segment: **45**
- ATSI: **44**
- SME: **39**
- At risk segment: **22**

Significantly **higher** / **lower** than the total at the 95% confidence interval.

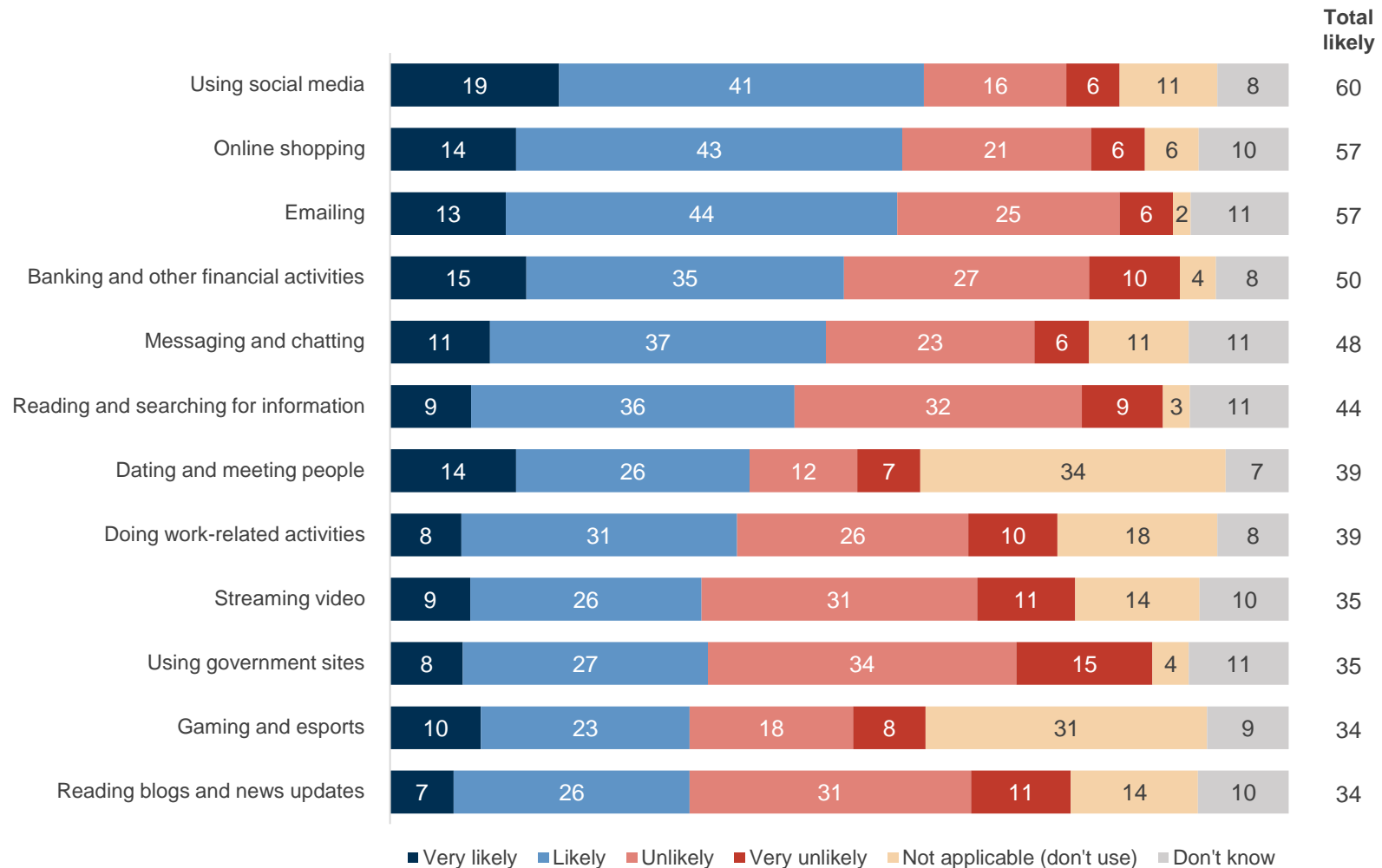
Q18. How much of a concern are these cyber threats for you and your household?

Base: All respondents (n=2,000).

Social media, online shopping, email and banking seen as most likely sources of cyber attacks



Likelihood to experience a cyber security breach, attack or hacking of personal information (%)



Q8. Thinking about all the programs, apps and activities you use on the internet, how likely do you think you are personally to experience a cyber security breach, attack or hacking of your information when you are?
 Base: All respondents (n=2,000).

Likelihood to experience a cyber security breach, attack or hack, by key analysis cohorts



Likelihood to experience a cyber security breach, attack or hacking of personal information (%) (cont'd)

(Total likely)

60% of Australians think they are likely to experience a CS breach, attack or hacking while **using social media**, this is significantly different among:

- SME contracts cyber: **71**
- Kids in hhold: **70**
- Savvy segment: **69**
- HHI > \$100K: **67**
- CALD: **66**
- Heavy internet user: **65**
- HHI up to \$50K: **55**
- Light internet user: **53**
- 60+ yrs: **52**

57% think they are likely to experience a CS breach, attack or hacking while **online shopping**, this is significantly different among:

- Kids in hhold: **64**
- Female: **61**
- Male: **52**
- 60+ yrs: **51**

57% think they are likely to experience a CS breach, attack or hacking while **emailing**, this is significantly higher among:

- Kids in hhold: **64**

50% think they are likely to experience a CS breach, attack or hacking while **banking and other financial activities**, this is significantly different among:

- Savvy segment: **57**
- Kids in hhold: **56**
- Female: **54**
- Male: **46**

48% think they are likely to experience a CS breach, attack or hacking while **messaging and chatting**, this is significantly higher among:

- Savvy segment: **60**
- Kids in hhold: **58**
- CALD: **57**
- SME: **56**

44% think they are likely to experience a CS breach, attack or hacking while **reading and searching for information**, this is significantly different among:

- SME contracts cyber: **56**
- SME: **53**
- 60+ yrs: **51**
- Savvy segment: **51**
- Kids in hhold: **50**
- 18-34 yrs: **38**

39% think they are likely to experience a CS breach, attack or hacking while **dating and meeting people**, this is significantly different among:

- Savvy segment: **48**
- SME: **47**
- Kids in hhold: **46**
- 35-59 yrs: **44**
- 60+ yrs: **30**

39% think they are likely to experience a CS breach, attack or hacking while **doing work-related activities**, this is significantly different among:

- SME contracts cyber: **62**
- SME: **52**
- Savvy segment: **52**
- ATSI: **51**
- Kids in hhold: **49**
- Heavy internet user: **44**
- At risk segment: **33**
- 60+ yrs: **31**

35% think they are likely to experience a CS breach, attack or hacking while **using government sites**, this is significantly higher among:

- SME contracts cyber: **45**
- Kids in hhold: **42**
- Savvy segment: **42**

35% think they are likely to experience a CS breach, attack or hacking while **streaming video**, this is significantly different among:

- ATSI: **55**
- SME contracts cyber: **54**
- SME: **46**
- Kids in hhold: **45**
- Savvy segment: **44**
- CALD: **41**
- Heavy internet user: **39**
- At risk segment: **30**
- Light internet user: **29**
- 60+ yrs: **27**

34% think they are likely to experience a CS breach, attack or hacking while **reading blogs and news updates**, this is significantly different among:

- SME contracts cyber: **54**
- SME: **49**
- ATSI: **48**
- Kids in hhold: **43**
- Savvy segment: **42**
- CALD: **40**
- Regional: **28**

34% think they are likely to experience a CS breach, attack or hacking while **gaming and esports**, this is significantly different among:

- SME contracts cyber: **56**
- Kids in hhold: **45**
- SME: **44**
- Savvy segment: **43**
- 35-59 yrs: **38**
- Regional: **29**
- Light internet user: **28**
- 60+ yrs: **25**

Significantly **higher** / **lower** than the total at the 95% confidence interval.

Q8. Thinking about all the programs, apps and activities you use on the internet, how likely **do you think you are personally** to experience a cyber security breach, attack or hacking of your information when you are?

Base: All respondents (n=2,000).

A large, dark blue letter 'W' that serves as a background element. It is filled with a complex, glowing pattern of white and light blue lines and dots, resembling a cosmic web or a network of stars and galaxies.

Actions undertaken



Section summary – actions undertaken

Levels of concern do not translate into implementation of preventative measures

The level of cyber security is not necessarily reflected in the implementation of preventative cyber security measures. Nearly half (47%) of Australians feel secure based on the measures they have implemented, yet just 34% have put in place extensive security measures (great / moderate). SMEs are slightly more realistic, with one in two (52%) implementing extensive measures and 56% feeling secure.

Varying cyber practices leave Australians vulnerable to attack

Cyber security behaviour reflects the variation in levels of awareness, understanding and concern. For example 59% of people never share their passwords and 57% say they are always wary of phishing and online scams, leaving the remaining two out of five Australians potentially vulnerable. Despite high usage, 14% of people never review their social media privacy settings.

Online searching and Government websites are top of the information consideration set

To improve cyber security, Australians use a variety of approaches to find out information. Online searching is the most popular (40%), followed closely by Federal Government websites (38%), cyber security companies (32%), internet service providers (30%) and specialist IT companies (28%). The list is long, however, and 10% admit to not knowing where to look.

Cyber complacency is compounded by not knowing where to report attacks

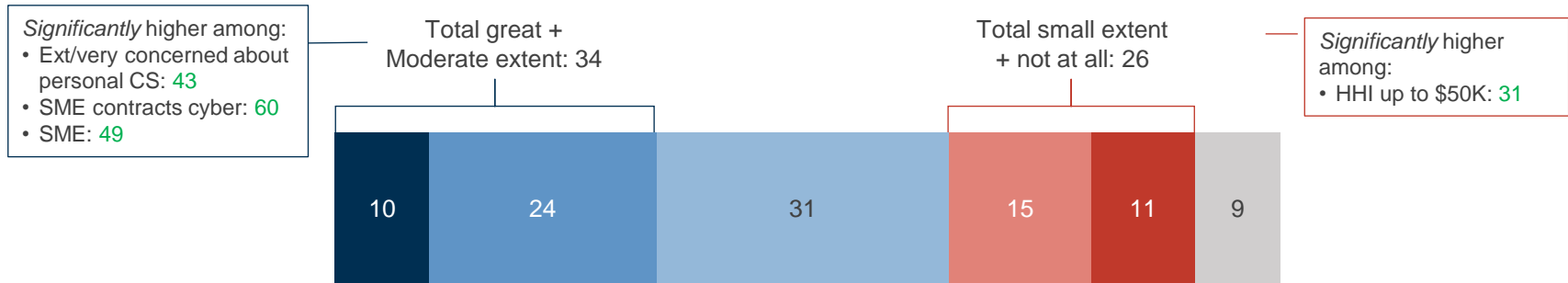
Two out of five Australians (42%) have received a phishing email in recent years, but more serious attacks such as unauthorised access to financial accounts is much lower at 15% (of which 71% reported it, the highest for all the attacks experienced). Overall, about half report any kind of attack, reasons for not reporting include: it was not considered serious enough; they didn't know where to report it; or, they thought nothing would come of it. Just 15% say they would report to ACSC's ReportCyber.

Business more likely to have implemented cyber security measures than households, but many have little protection

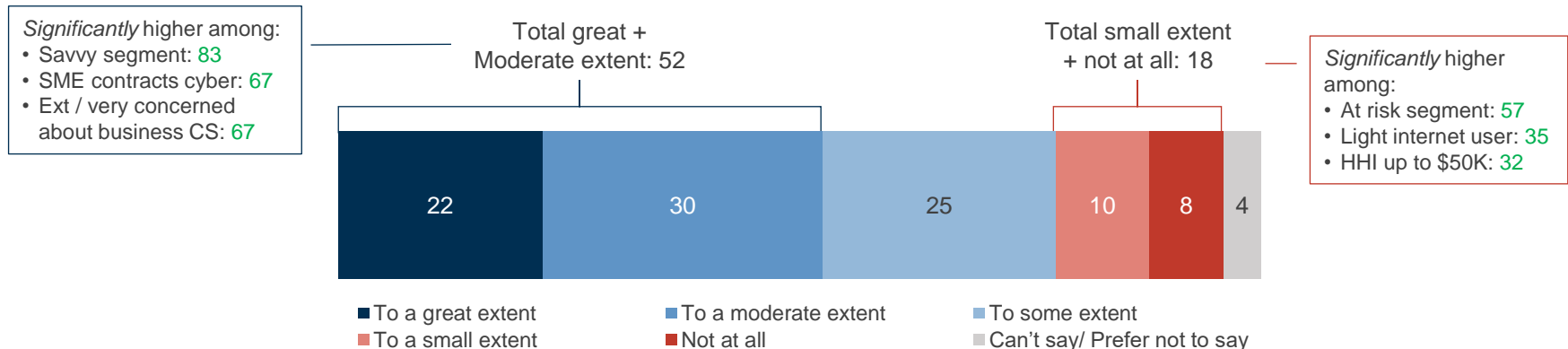


Extent of cyber security measures implemented (%)

In your household



In your business*



Significantly **higher** than the total at the 95% confidence interval.

Q12. To what extent have you implemented any cyber security measures for you personally or for your household?

Q13. To what extent have you implemented any cyber security measures for your business?

Base: All respondents (n=2,000); SMEs (n=340).

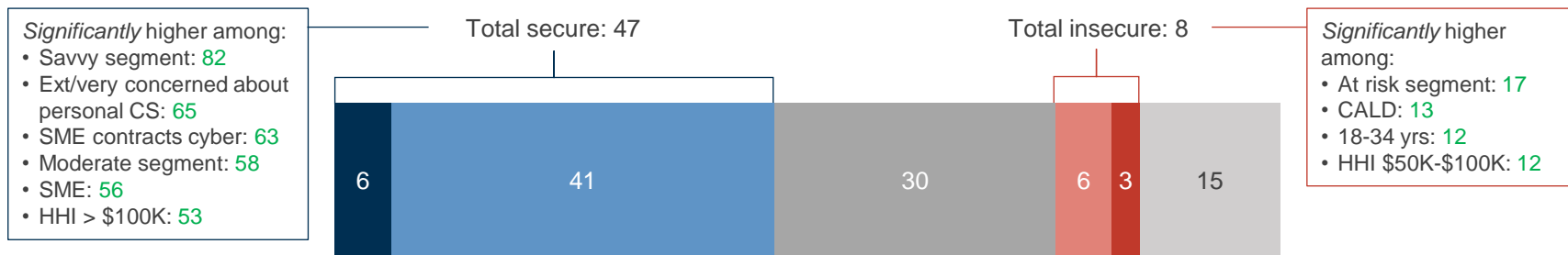
*Asked only among business owners.

At both a household and business level, many feel less than secure

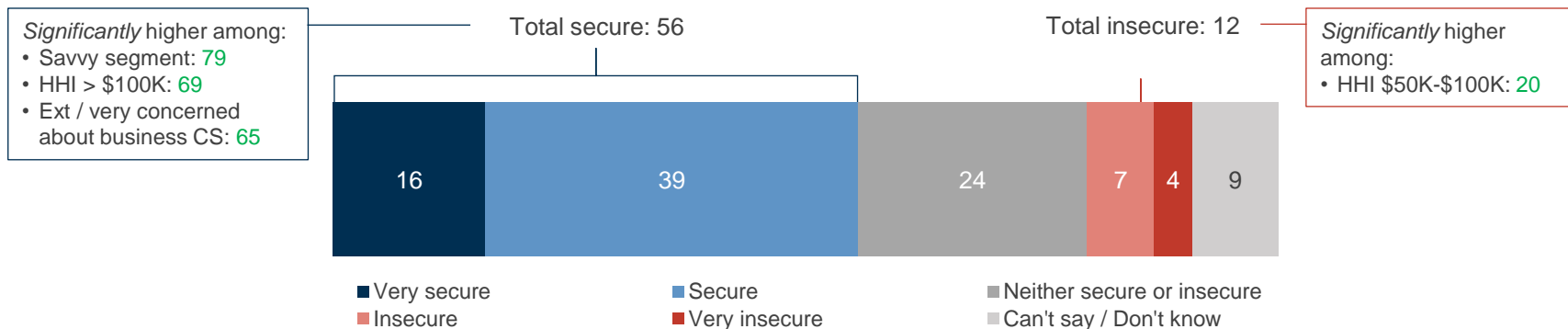


Perceived security from cyber security measures implemented (%)

In your household



In your business*



Significantly *higher* than the total at the 95% confidence interval.

Q14. Thinking about **cyber security measures you have personally implemented**, how secure do you think that you are?

Q15. Thinking about **cyber security measures you have implemented in your business**, how secure do you think the business is?

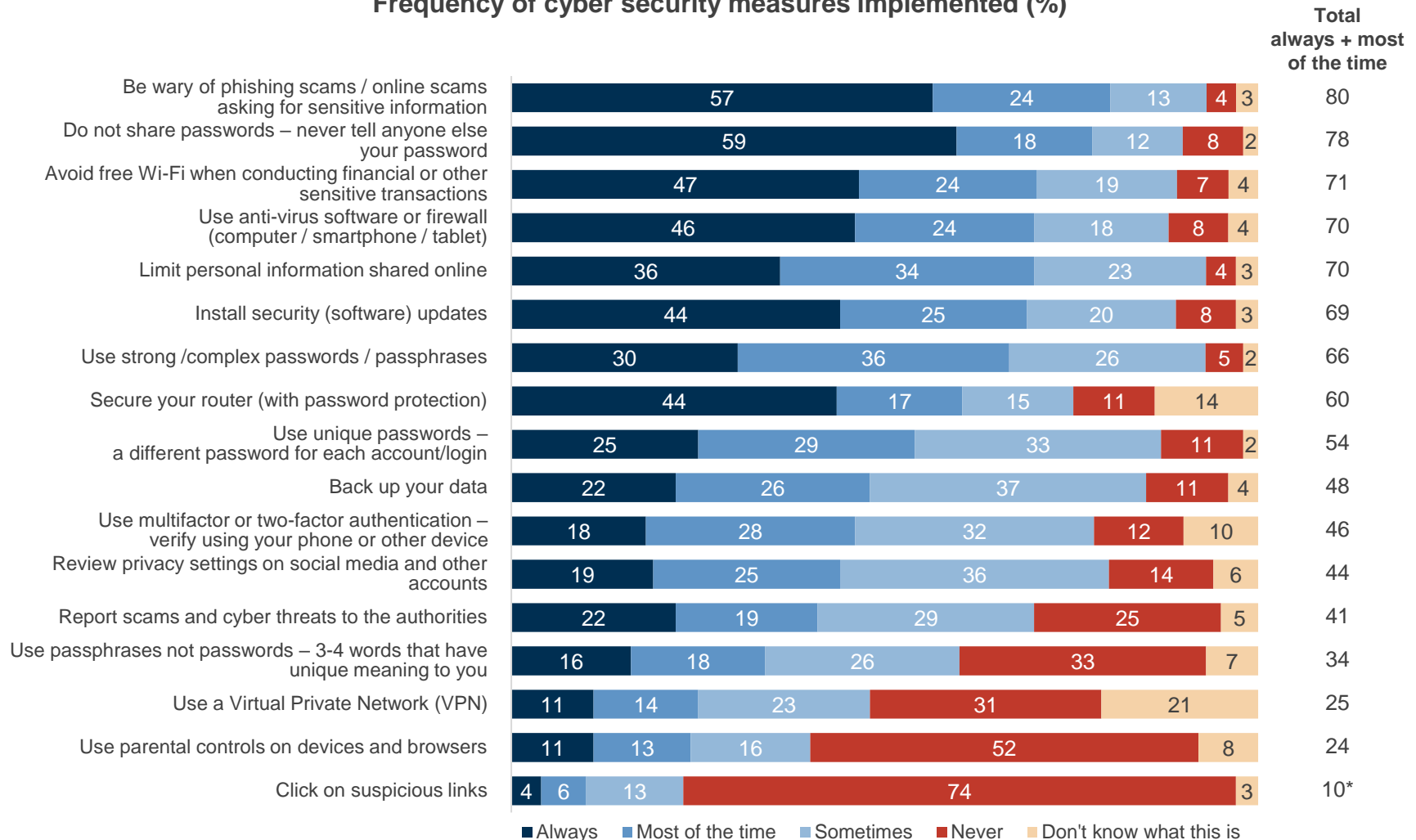
Base: All respondents (n=2,000); SMEs (n=340).

*Asked only among business owners.

There is a widely varying degree of implementation of specific cyber security measures



Frequency of cyber security measures implemented (%)



* Note: There appears to be an anomaly in this percentage as the Savvy segment is overrepresented in this 10% result. As this is the most cyber security conscious segment, it is likely that they have misinterpreted this as 'do not click on suspicious links'. On this basis, this 10% is likely to be a much smaller percentage.

Q16. Thinking about various cyber security measures that you could implement,, how often do you do the following?
Base: All respondents (n=2,000).

Australians could do more when it comes to implementing cyber security measures



Frequency of cyber security measures implemented (%) (cont'd) (Total always + most of the time)

	Total	18-34 yrs	35-59 yrs	60+ yrs	SME total	SME contracts cyber	CALD	Kids 0-9 yrs	Kids 10-18 yrs	Segment		
										Savvy	Moderate	At risk
Be wary of phishing scams / online scams asking for sensitive information	80	73	82	86	74	68	75	72	77	86	85	74
Do not share passwords – never tell anyone else your password	78	69	81	82	70	68	78	76	77	82	81	74
Avoid free Wi-Fi when conducting financial or other sensitive transactions	71	62	72	78	64	66	71	67	72	79	76	63
Use anti-virus software or firewall (computer / smartphone / tablet)	70	54	73	83	68	65	66	64	70	84	77	58
Limit personal information shared online	70	60	70	82	65	69	67	66	69	81	75	61
Install security (software) updates	69	54	72	79	67	65	64	65	66	83	76	56
Use strong /complex passwords / passphrases	66	61	70	66	64	66	65	62	70	82	73	52
Secure your router (with password protection)	60	61	63	55	63	65	62	62	65	81	66	46
Use unique passwords – a different password for each account/login	54	47	55	59	57	61	55	51	57	72	58	39
Back up your data	48	43	50	51	59	55	48	49	47	66	55	35
Use multifactor or two-factor authentication – verify using your phone or other device	46	53	49	34	57	64	53	54	57	70	51	32
Review privacy settings on social media and other accounts	44	46	45	40	53	57	47	42	48	66	49	28
Report scams and cyber threats to the authorities	41	38	40	45	50	58	40	45	42	58	46	29
Use passphrases not passwords – 3-4 words that have unique meaning to you	34	40	35	26	49	52	42	39	39	51	38	24
Use a Virtual Private Network (VPN)	25	27	26	20	42	48	28	34	31	46	27	13
Use parental controls on devices and browsers	24	25	28	16	44	55	29	41	43	43	26	14
Click on suspicious links	10*	17	9	4	28	36	16	17	14	22	11	4

* Note: There appears to be an anomaly in this percentage as the Savvy segment is overrepresented in this 10% result. As this is the most cyber security conscious segment, it is likely that they have misinterpreted this as 'do not click on suspicious links'. On this basis, this 10% is likely to be a much smaller percentage.

Significantly **higher** / **lower** than the total at the 95% confidence interval.

Q16. Thinking about various cyber security measures that you could implement, how often do you do the following?

Base: All respondents (n=2,000).

Online search and Australian Government websites are the main sources of cyber security information



Sources to find information on improving cyber security (%)
(Multiple response)



Significantly higher than the total at the 95% confidence interval.

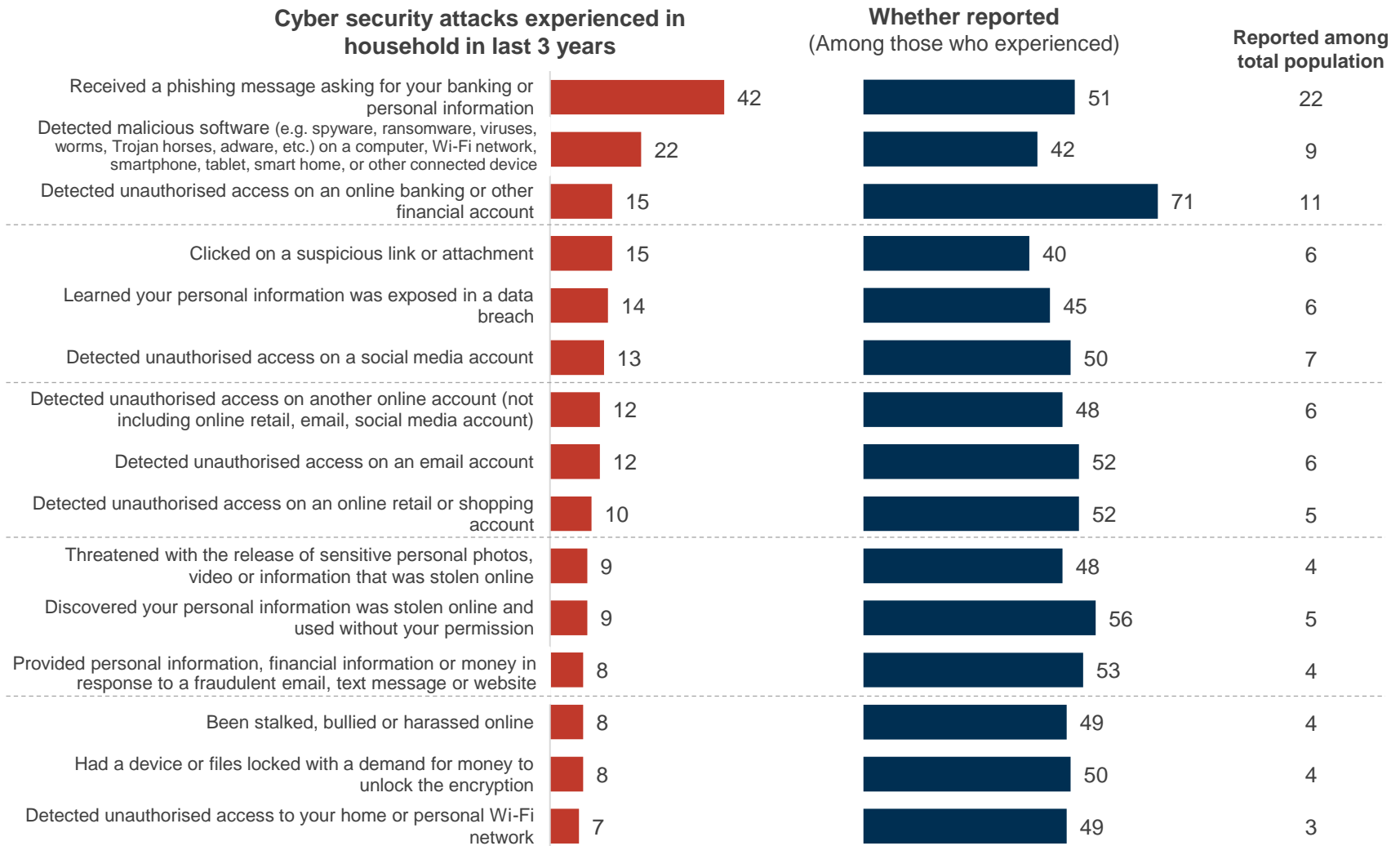
Q19. If you want to find out what you can do to improve your cyber security, where would you find this information?

Base: All respondents (n=2,000).

Unauthorised access to online banking is the incident that is most likely to be reported



Experience and reporting of cyber security attacks (%)



Q20. Thinking about a range of cyber attacks, in the last 3 years, have you or any one in your household experienced any of the following...? /

Q21. And did you report this attack?

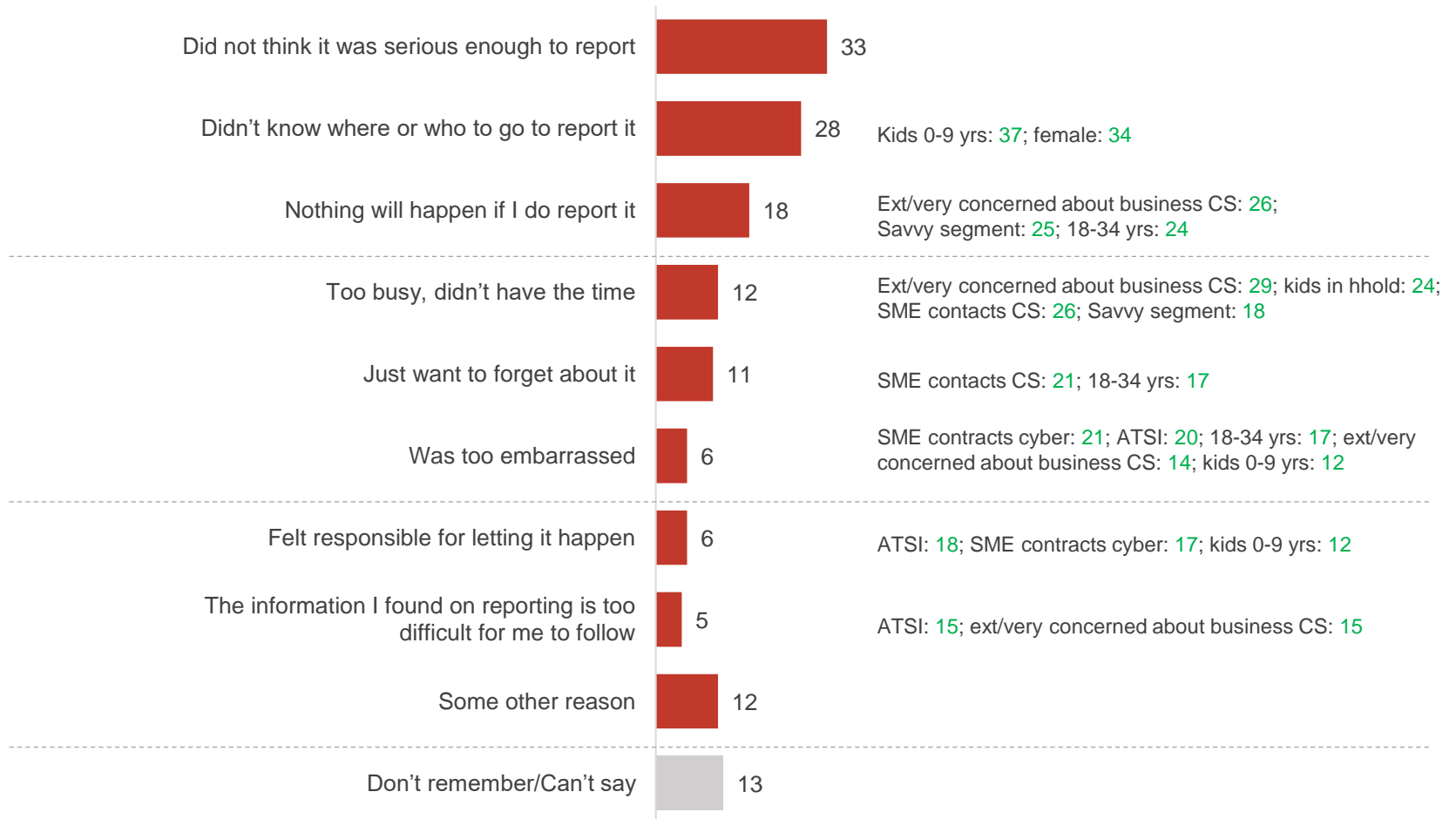
Base: All respondents (n=2,000); those who experienced cyber security attacks in household in last 3 years (n=133-859).

Key reasons for not reporting include not knowing where to report and not having faith in the response



Reasons for not reporting cyber attack/s experienced (%) (Multiple response – among those who experienced and did not report)

Significantly higher among:



Significantly higher than the total at the 95% confidence interval.

Q22. Why didn't you report the cyber attack/s?

Base: Respondents who experienced cyber security attacks in household in last 3 years and did not report (n=843).



Reasons for not reporting cyber attacks, by type of attack

Reasons for not reporting cyber attack/s experienced (%)
(Multiple response – among those who experienced and did not report)

	Total	Received phishing message	Detected malicious software	Clicked on suspicious link or attachment	Personal information exposed in data breach	Detected unauthorised access on social media account	Detected unauthorised access on another online account	Detected unauthorised access on email account	Threatened with release of sensitive personal photos, video or information stolen online
Sample size (n=)	843	379	236	151	131	109	105	100	78
Didn't think it was serious enough to report	33	38	35	37	28	36	23	27	34
Didn't know where or who to go to report it	28	32	36	29	23	28	25	32	30
Nothing will happen if I do report it	18	18	16	22	26	27	16	24	21
Too busy, didn't have the time	12	10	15	11	11	15	15	13	16
Just want to forget about it	11	8	12	14	10	18	14	11	21
Was too embarrassed	6	2	4	7	3	8	15	5	11
Felt responsible for letting it happen	6	4	7	11	2	8	4	4	9
Info. found on reporting too difficult to follow	5	4	5	6	6	8	9	6	9
Some other reason	12	15	9	2	25	6	12	8	10
Don't remember/Can't say	13	13	11	12	11	7	12	10	7

Significantly **higher** / **lower** than the total at the 95% confidence interval.

Q20. Thinking about a range of cyber attacks, in the last 3 years, have you or any one in your household experienced any of the following ...? / Q21. And did you report this attack? / Q22. Why didn't you report the cyber attack/s?

Base: Respondents who experienced cyber security attacks in household in last 3 years and did not report (n=843).

Reasons for not reporting cyber attacks, by type of attack (cont'd)



Reasons for not reporting cyber attack/s experienced (%) (cont'd) (Multiple response – among those who experienced and did not report)

	Total	Detected unauthorised access on online banking or other financial account	Detected unauthorised access on online retail or shopping account	Device or files locked with demand for money to unlock encryption	Been stalked, bullied or harassed online	Provided personal or financial information or money in response to fraudulent email, text message or website	Personal information stolen online and used without permission	Detected unauthorised access to home or personal Wi-Fi network
Sample size (n=)	843	66	65	61	64	59	57	55
Didn't think it was serious enough to report	33	25	29	16	35	25	35	26
Didn't know where or who to go to report it	28	18	30	33	28	17	37	31
Nothing will happen if I do report it	18	17	21	18	27	28	31	15
Too busy, didn't have the time	12	18	20	12	20	11	21	14
Just want to forget about it	11	18	18	26	22	30	12	20
Was too embarrassed	6	13	7	7	12	10	13	9
Felt responsible for letting it happen	6	7	16	16	10	6	8	<1
Info. found on reporting too difficult to follow	5	7	2	11	4	8	11	12
Some other reason	12	10	4	6	4	3	1	3
Don't remember/Can't say	13	7	16	4	3	8	5	7

Significantly higher / lower than the total at the 95% confidence interval.

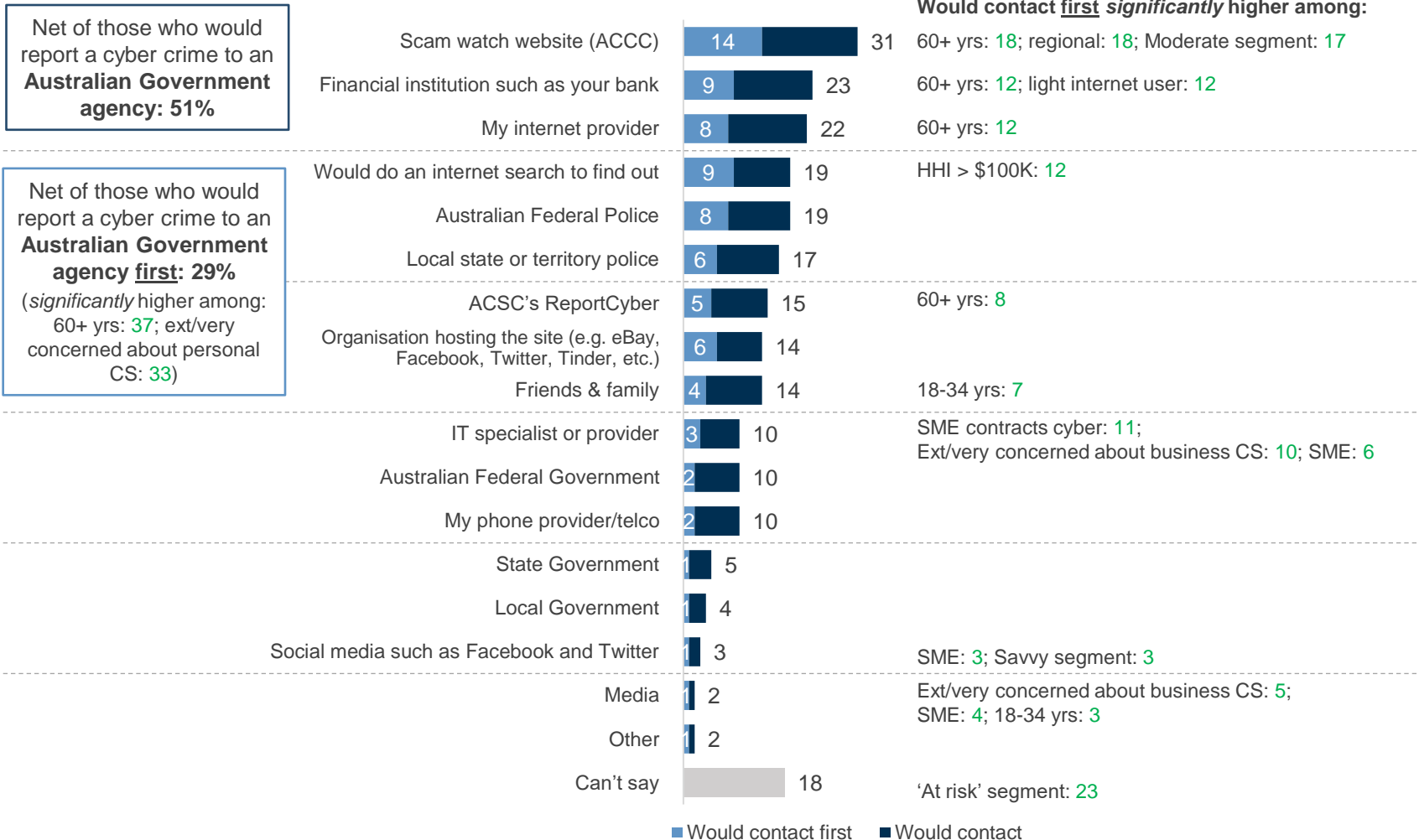
Q20. Thinking about a range of cyber attacks, in the last 3 years, have you or any one in your household experienced any of the following ...? / Q21. And did you report this attack? / Q22. Why didn't you report the cyber attack/s?

Base: Respondents who experienced cyber security attacks in household in last 3 years and did not report (n=843).

Only half would seek out an Australian Government agency to report a cyber crime, primarily ACCC Scam watch



Where to report a cybercrime or cyber attack (%) (Multiple response)



Significantly higher than the total at the 95% confidence interval.

Q23. If you wanted to report a cybercrime or cyber attack who/where would you **contact first**? / Q24. And who/where else would you contact?

Base: All respondents (n=2,000).

Segment analysis



Section summary – attitudes toward cyber security

Segmentation will be the key to the strategy

A viable segmentation has been developed on the basis of the level of understanding and the extent of cyber security measures implemented by Australians. **There is significant differentiation between the segments that will enable the ACSC to develop targeted strategies to meet the needs of a very disparate market.**

Savvy segment

The Savvy segment has a good understanding of cyber security and implements a range of protective measures. This segment tends to be educated and heavy internet users through multiple devices. They are vigilant, informed, and have an ongoing interest in keeping up with the latest developments in cyber security and threats. The ACSC can help to satisfy these needs for the Savvy segment.

Moderate segment

Moderates are aptly described as they are average in many respects. They understand and have implemented adequate levels of cyber security but not to the same degree as the Savvy segment. As a result, while they believe they have a good level of security, they are still vulnerable due to some deficits in their knowledge and security measures. They are very receptive to learning more, particularly from the ACSC, who is perceived to be a trustworthy source.

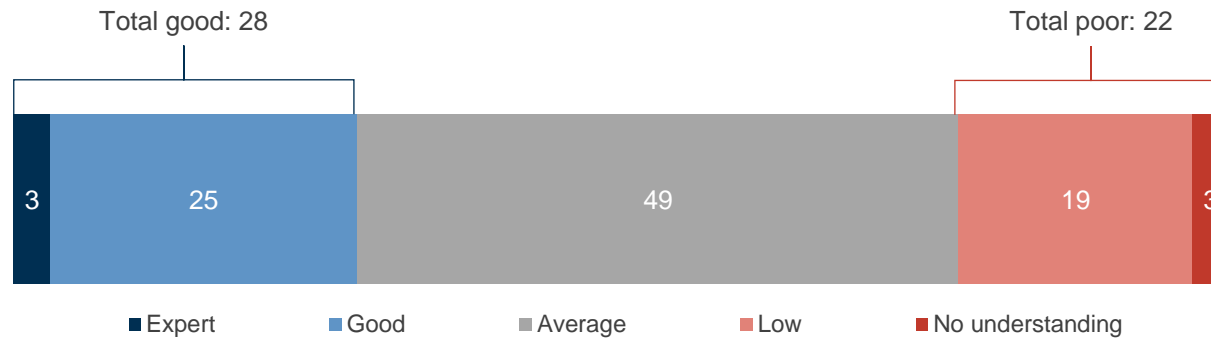
At risk segment

‘At risk’ describes this segment well, based on the implementation, or lack thereof, of cyber security measures. Their knowledge and understanding of the importance of cyber security is limited, and many of them are unconcerned about cyber security. **It is unclear if this is apathy or ignorance, but nonetheless, they are exposed to significant risks every time they are on the internet.**

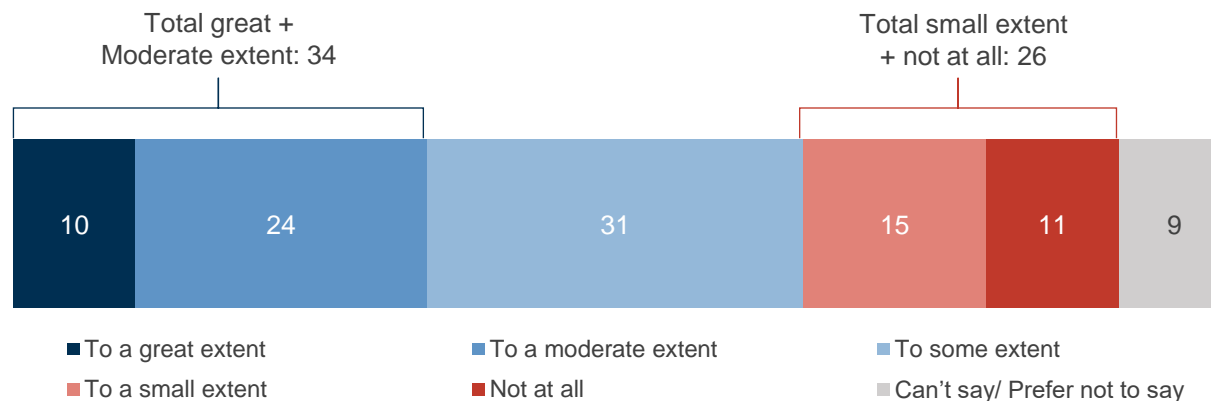
Cyber segments based on analysis of understanding (attitude) and implementation (behaviour)



Level of understanding about cyber security (%)



Extent of cyber security measures implemented in household (%)





Cyber security profile snapshot



- Expert or good understanding of cyber security and have implemented cyber security measures to a great or moderate extent

Savvy

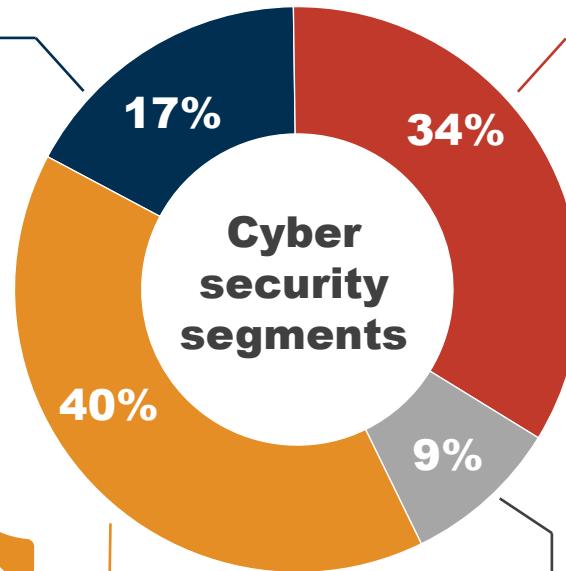
'Savvy' skews male – 61% of this cohort are men, they are more likely to be employed, have higher education levels, spend more than 6 hours per day on the internet, with household income over \$100,000, and kids. They are more likely to have a greater range of devices including alarm / security systems and home automation connected to the internet. They are also far more likely to be users of multiple social media sites (2+ sites 82% vs 70% average).



At risk

The 'At risks' skew female – 55% of this cohort are women. At risk also skews to the over 60s, households with incomes under \$50,000 and those who spend up to two hours per day on the internet. They are also less likely to use multiple social media sites, but they are still connected and vulnerable.

- Expert, good or average understanding of cyber, but security little to no implementation
- Low understanding, regardless of security implementation



Moderate

The demographic profile of the 'Moderates' cohort follows that of the Australian population. Moderates think that they are informed, but have a lower expectation than the Savvy segment of experiencing a security attack.

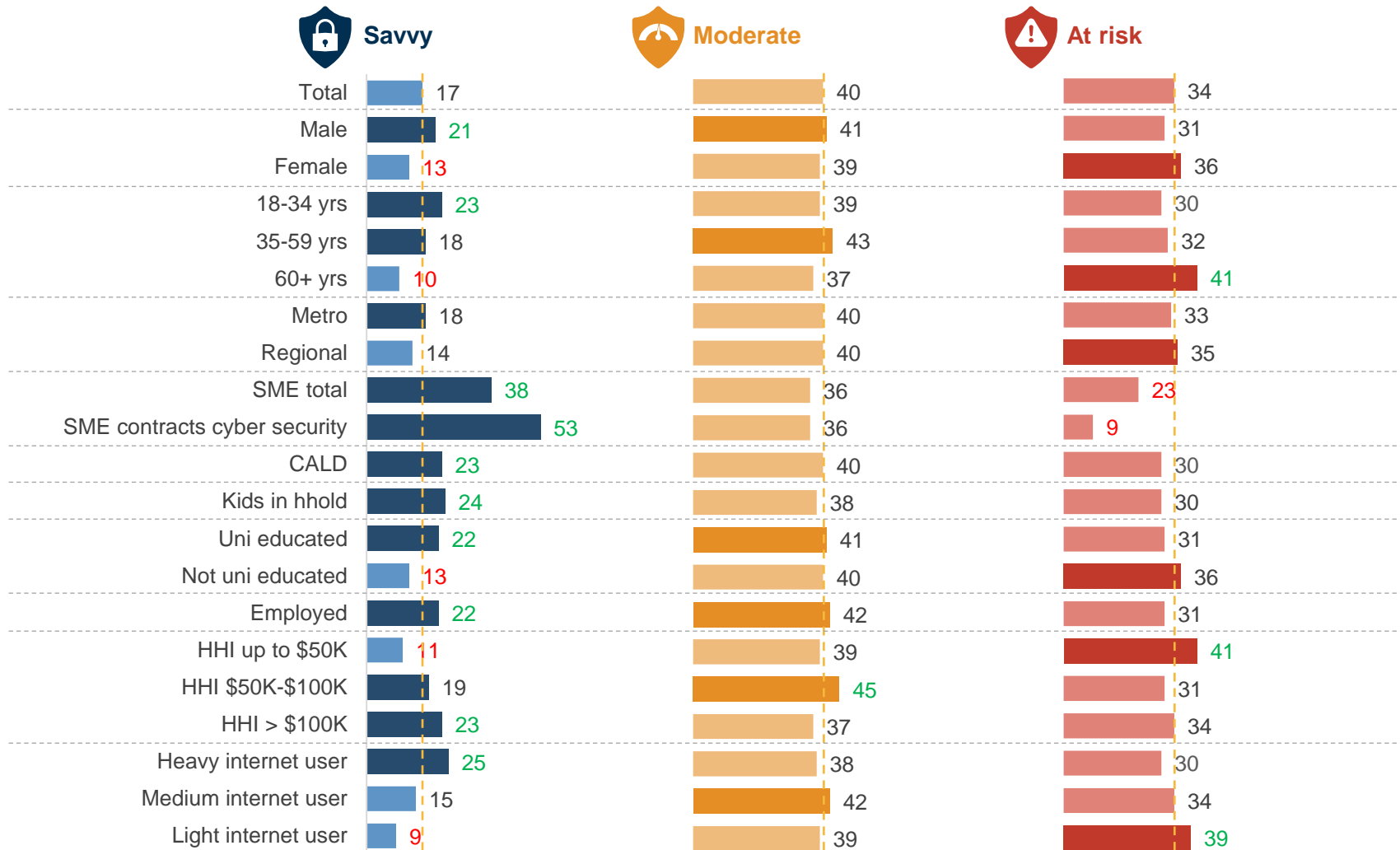
- Expert or good understanding of cyber security but only some implementation of security measures
- Average understanding and at least some implementation of security measures

Not classified



Detailed segment profiles

Profile of segments (%)



'Savvy' segment understand how critical cyber security is at every level



Savvy (17%)

Who are they?

The Savvies skew male – comprising 61% of this cohort. They are higher income and heavy internet users, spending more than 6 hours per day on the internet. They are also more likely to have a greater range of devices including alarm / security systems and home automation connected to the internet. In addition, Savvy cohort are also far more likely to be users of multiple social media sites (2+ sites 82% vs 70% average).

What underpins their views?

- **Savvies are significantly more likely to be extremely or very concerned for themselves personally about cyber security** than the other segments (56% compared to 43% among all Australians).
- Consistent with this concern, they are significantly more likely to have higher levels of concern for their business (68% vs 50% average), business in general (61% vs 46% average) and the Government (65% vs 54% average).
- More than other segments, the Savvy segment think they know what is required to ensure a high level of security (82% vs 43% average). They also know where to go for information (78% vs 41% average).

- This segment more than others believes that cyber crime can ruin lives (87% vs 78% average). This acknowledgment is vital to understanding the importance of cyber security, particularly the businesses which they are more likely to believe are at greater risk (50% vs 41% average).
- Awareness of when and how breaches can occur online is greater than for other segments: for example when messaging or chatting online (60% vs 48% average), or undertaking work activities (52% vs 39% average.)
- Savvies are confident that the measures implemented for themselves (82% vs 47% average) and, if they are SMEs, their businesses (79% vs 56% average) are secure. In fact, when reviewing the measures implemented, there is an extensive and more sophisticated range of measures used, from password-protected routers (81% vs 60% average) through to multifactor authentication (70% vs 46% average) and VPNs (46% vs 25% average).
- Consistent with their other behaviour, this segment has significantly higher levels of awareness and concern for the range of cyber threats. This raises the question of whether they have experienced a cyber attack; however, the incidence of cyber attack is in line with the other segments.
- Should they want to obtain information, Savvies trust the ACSC and are significantly more likely to go to the website (72% vs 63% average).
- Overall, Savvies are significantly more likely to want to hear more about cyber security (60% vs 50% average).

The ‘Moderate’ segment has adequate levels of awareness and knowledge but they are still vulnerable



Moderate (40%)

Who are they?

The demographic profile of the Moderate cohort follows that of the Australian population in all respects other than significantly higher middle income representation.

What underpins their views?

- **Moderates think that they are informed about cyber security.** They are more likely to know where to go to find information (48% vs 41% average). Furthermore, they are also more likely to believe that they do everything they can to prevent against cyber threats (66% vs 57% average).
- Moderates are significantly more likely to consider the measures implemented have given them a good level of personal / household security (58% vs 47% average).
- There are a number of measures they are more likely to implement, from using anti-virus software (77% vs 70% average) through to using strong passwords / phrases (73% vs 66% average). There are some differences between the Savvies and the Moderates. The Savvies have higher incidences of using more sophisticated security measures, such as VPNs and passphrases.
- Moderates are generally aware of the cyber threats and are concerned, but not to the same extent as the Savvy segment.

- In regard to the organisations that can provide assistance with cyber crimes, Moderates are significantly more likely to nominate the ACSC (52% vs 46% average). There is no apparent reason for this, other than to reinforce earlier conclusions about the power of ACSC's name association.
- **The Moderates, as with all the segments, have a high level of trust in the ACSC to provide cyber security information (77% average).** Compared to the Australian population overall, significantly more Moderates would go to the website to get this information (70% vs 63% average) and to report a cyber crime if they are a victim (76% vs 68% average).

The 'At risk' segment does not sufficiently comprehend the importance of cyber security



At risk (34%)

Who are they?

The At risk segment skews female – 55% of this cohort are female. They are lower income and lighter users, spending up to two hours a day on the internet. They are also less likely to use multiple social media sites.

What underpins their views?

- **As can be expected, the At risk cohort are more likely to be unconcerned about cyber security** on any level – personal (21% vs 16% average), for their own business (33% vs 16% average) or business in general (18% vs 22% average).
- In the attitudinal statements, it is evident that they are less concerned about cyber security, and significantly less likely to know where to go to find out about it (22% vs 41% average). Further, approximately half of the At risk segment acknowledge that they do not know what to do to prevent against an attack (47% vs 33% average).
- Of great concern is that SMEs in this segment are significantly less likely to have implemented cyber security measures for their business (57% 'not at all' or 'to a small extent' vs 18% average). At risk SMEs are also less likely to consider their business secure as result of these measures (31% vs 56% average). **This underestimation of risk, coupled with their low levels of cyber security knowledge, exposes them to cyber threats.**
- **Consistent with their other behaviours, the At risk segment are significantly less likely to have implemented any security measures**, even the most basic ones of antivirus software (58% vs 70% average) or avoiding free Wi-Fi to conduct financial or sensitive transactions (63% vs 71% average).
- This unpreparedness is further compounded by their lower awareness and levels of concern in comparison to the other segments of the various cyber threats. For example, they are significantly less likely to be concerned about online shopping or romance frauds (22% vs 29% average).
- In terms of who they trust to provide information about cyber security, seven out of ten of the At risk segment would trust the ACSC. This segment is significantly less likely to be aware of or know anything about the ACSC (9% vs 19% average), so it is interesting that there is such a high level of trust.
- Further, a majority (56%) would go to the ACSC website to seek out information about cyber security. **At the end of this research, nearly half (47%) indicate that they want to know more about cyber security.**
- **Overall, there is a vast difference in cyber security understanding and behaviour between the Savvy and At risk segments, but there is a glimmer of hope that once At risk become aware of the risks, many will want to rectify the situation and close their knowledge gaps.**



Trusted organisations



Section summary – trusted organisations

Limited awareness and knowledge of the ACSC except among specific audiences

The ACSC has a low level of awareness (31%) in comparison to organisations such as the AFP (75%) and Border Force (65%). Interestingly, there is greater awareness among those who have high levels of concern about cyber security for both personal (37%) and business (60%) as well as those who self-classify as having an 'expert' or 'good' understanding of cyber security.

ACSC – the name gives the organisation credibility

Irrespective of low awareness levels, the ACSC is nominated by approximately one out of two Australians as the organisation that can assist with cyber security information (54%), reporting a cyber crime (45%) and assisting with cyber crimes (46%). Among those aware of the ACSC, it has exceptionally high levels of trust, on par with the AFP – the only limitation is the ACSC's low awareness.

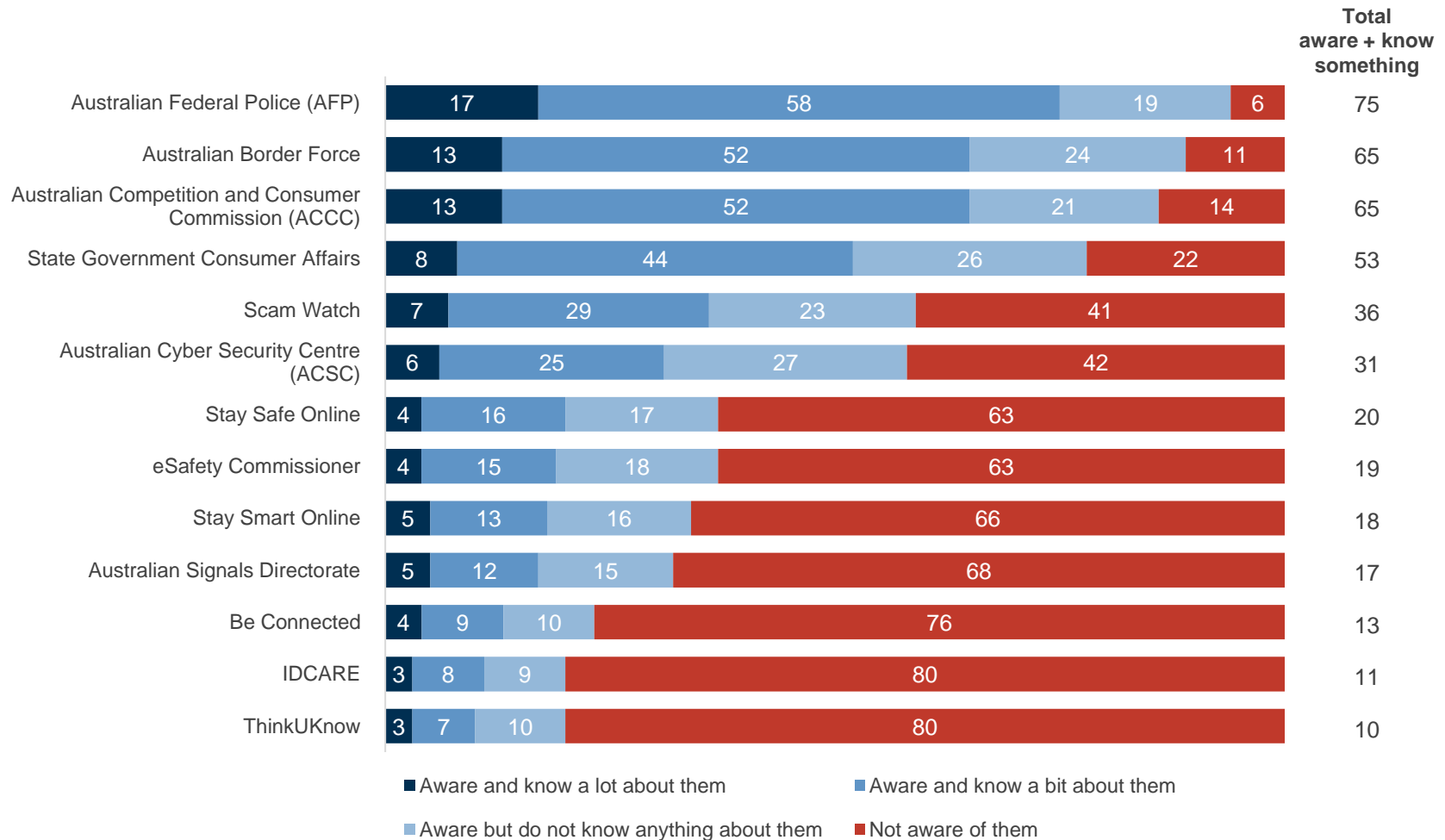
Awareness and trust of Stay Smart Online is low

Awareness of the Stay Smart Online program is low, with less than 1 in 3 (31%) aware of the program and very few knowing a lot about it. There is not a strong association that the ACSC runs the program. Overall, Stay Smart Online has a limited trust rating among those aware of it.

The ACSC has relatively low awareness, although Stay Smart Online awareness is even lower



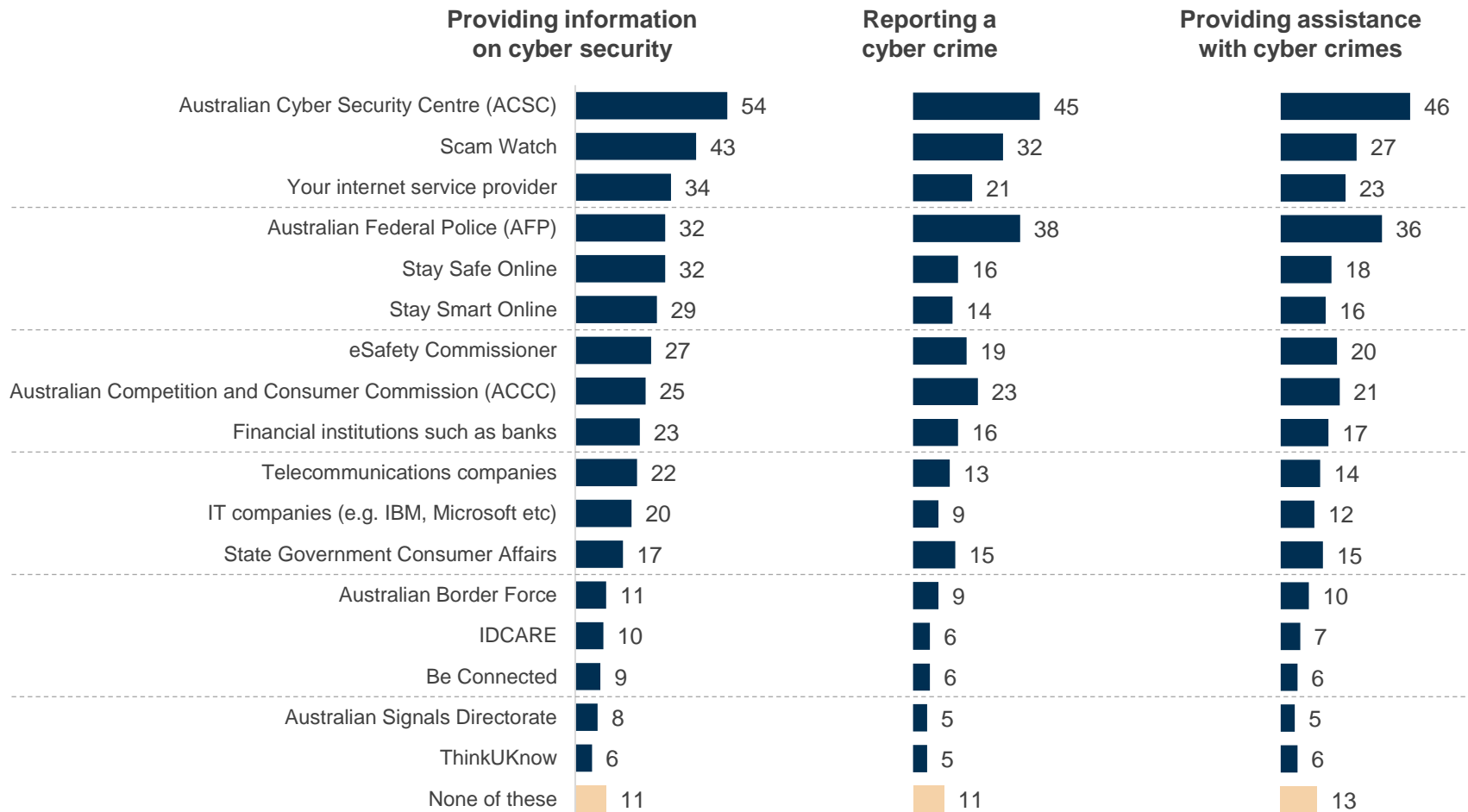
Awareness of cyber security organisations and programs (%)



The ACSC has the highest top-of-mind association for cyber security information, reporting, and assistance



Organisations and programs to assist with cyber security (%) (Multiple response)



Q26. And which of these organisations or programs do you think could assist with... A. Providing information about cyber security? /

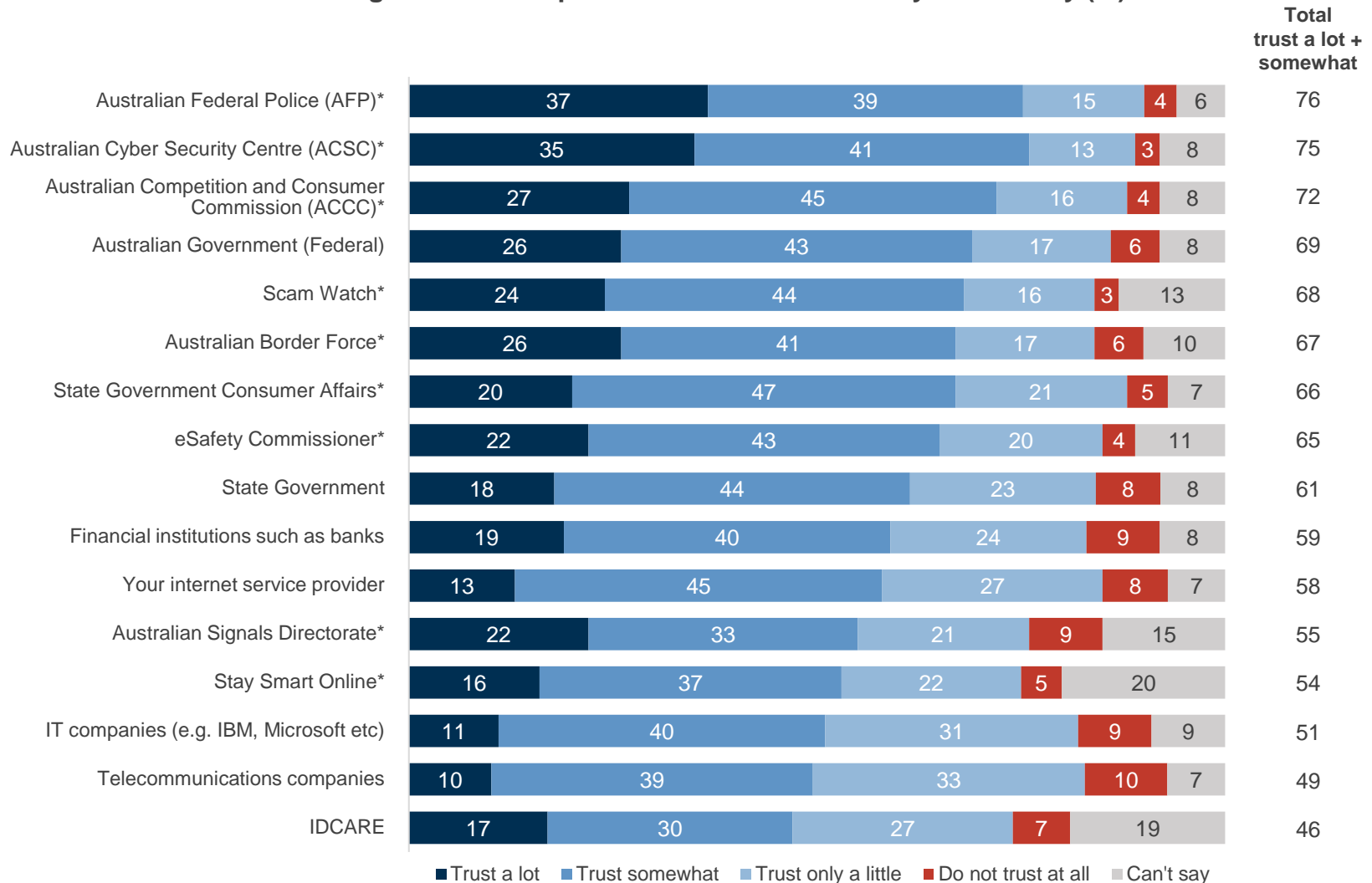
B. Reporting a cyber crime? / C. Providing assistance with cyber crimes?

Base: All respondents (n=2,000).

Among those aware of each individual organisation, the ACSC has the highest trust rating after the AFP



Trust in organisations to provide information about cyber security (%)



Q29. How much do you trust these organisations to provide you information about cyber security?

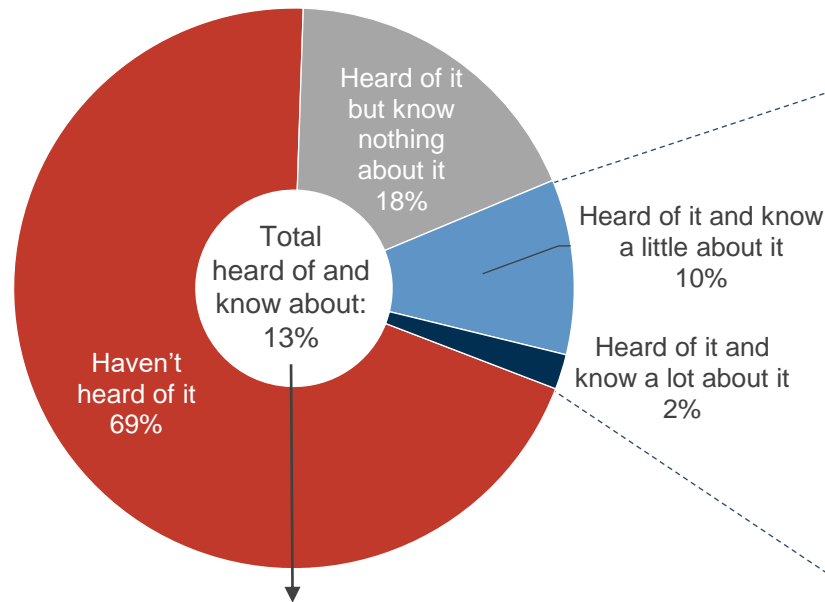
Base: All respondents (n=2,000).

*Asked only among those aware of organisation.

Almost 1 in 3 aware of the Stay Smart Online Program, but few know a lot about it or associate it with ACSC



Awareness of Stay Smart Online program

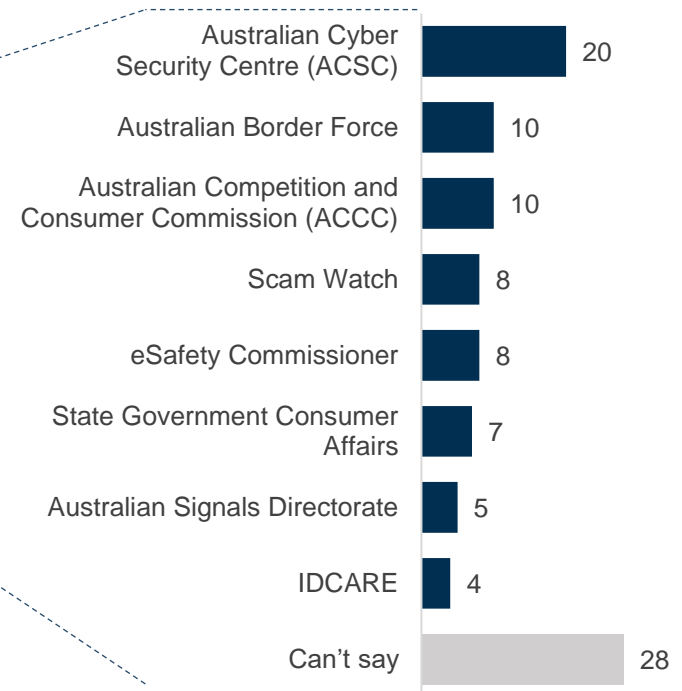


13% of Australians have **heard of and know about the Stay Smart Online program**. This is significantly higher among:

- SME contracts cyber: **47%**
- Ext/very concerned about business CS: **44%**
- SME: **37%**
- Savvy segment: **36%**
- Kids in hhold: **21%**
- HHI > \$100K: **17%**
- 18-34 yrs: **19%**
- CALD: **17%**
- Uni educated: **17%**
- Heavy internet user: **17%**
- Employed: **16%**
- Male: **16%**

Organisation thought to run Stay Smart Online (%)

(Among heard of and know about)



Significantly **higher** than the total at the 95% confidence interval.

Q27. Have you heard of the Stay Smart Online program? / Q28. Do you know what organisation runs the Stay Smart Online program?

Base: All respondents (n=2,000); heard of Stay Smart Online program (n=242).

A large, dark blue, stylized letter 'W' graphic that spans the right side of the page. Inside the 'W', there is a glowing, intricate network pattern of white and light blue lines and nodes, resembling a cyber network or data flow.

Australian Cyber Security Centre (ACSC) and 2020 Strategy

Section summary – ACSC and the 2020 Cyber Security Strategy



Appetite exists to know more about Government cyber security initiatives

Awareness of the 2020 Cyber Security Strategy is low, with only about one in ten (12%) having 'definitely' heard of it. Once prompted, there is a lot of interest in hearing about the different initiatives, particularly the 24/7 cyber security advice hotline (32%). More than a quarter (27%) want to know about all aspects of the Strategy and less than one in five (18%) are not interested in hearing anything.

The ACSC needs to define its role and raise its profile

Given an explanation of the ACSC and its mission, 47% claim some awareness, but only 19% say they have even limited knowledge of the ACSC. This contrasts with the 31% who earlier said they are aware of the ACSC and claim to know something. It can be hypothesised that, initially, Australians may have confused it with another organisation, such as the ACCC.

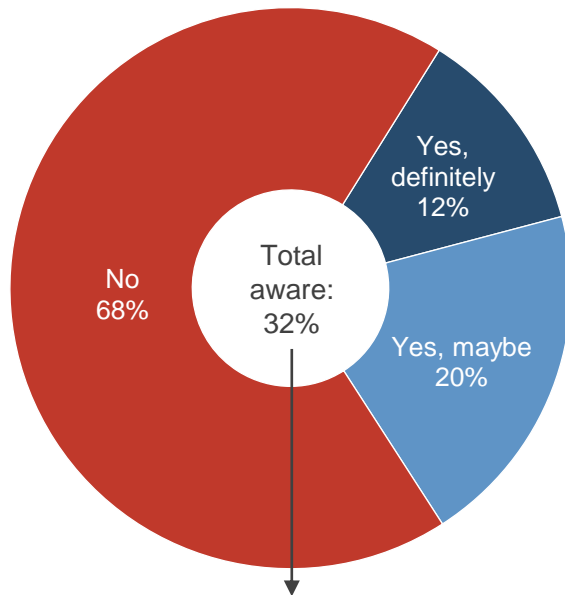
ACSC – a one-stop-shop for cyber security

The two main areas of interest in the ACSC's services are 'to get assistance if they are a victim of cyber crime' (68%) and 'going to the website to get information about security' (63%). There is less, but still considerable, appetite for following the ACSC on social media (42%) or subscribing to the ACSC alert service (39%).

Prompted awareness of the ACSC 2020 Cyber Security Strategy is low, but there is interest in a 24/7 cyber hotline



Awareness of Australian Government's 2020 Cyber Security Strategy

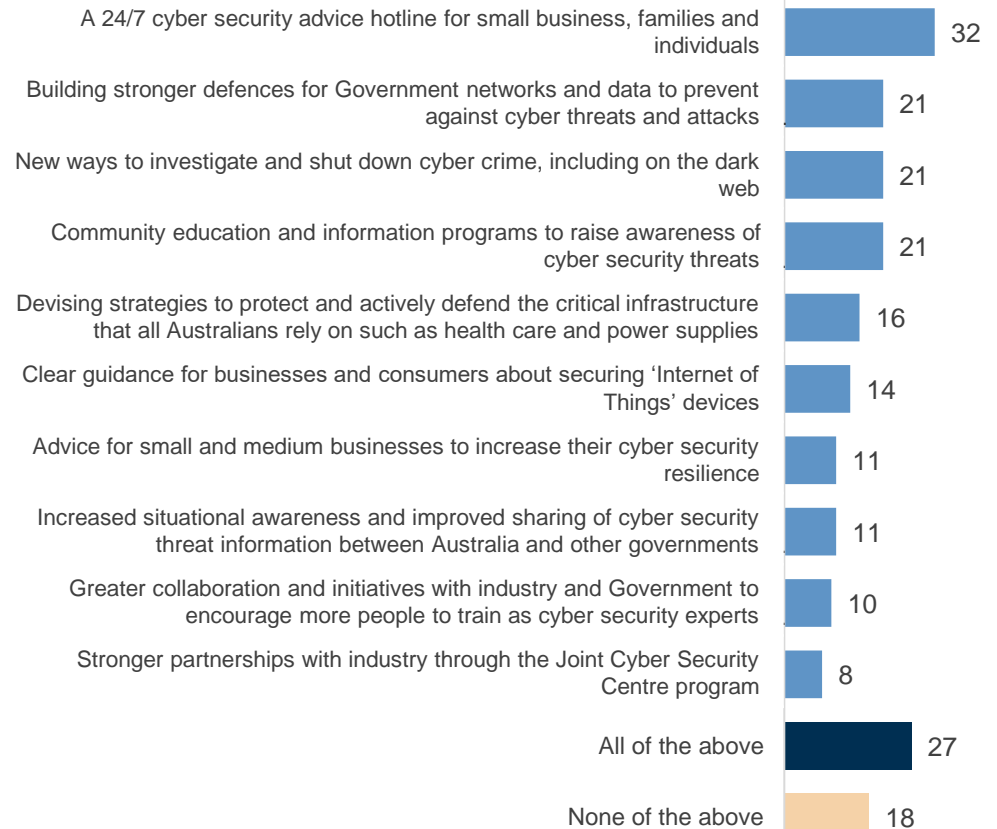


32% of Australians are **aware of the Australian Government's 2020 Cyber Security Strategy**.

This is significantly higher among:

- Ext/very concerned about business CS: **65%**
- SME: **55%**
- Savvy segment: **54%**
- Male: **39%**
- 18-34 yrs: **37%**

Areas of Strategy interested in knowing or hearing more about (%) (Multiple response)



Significantly **higher** than the total at the 95% confidence interval.

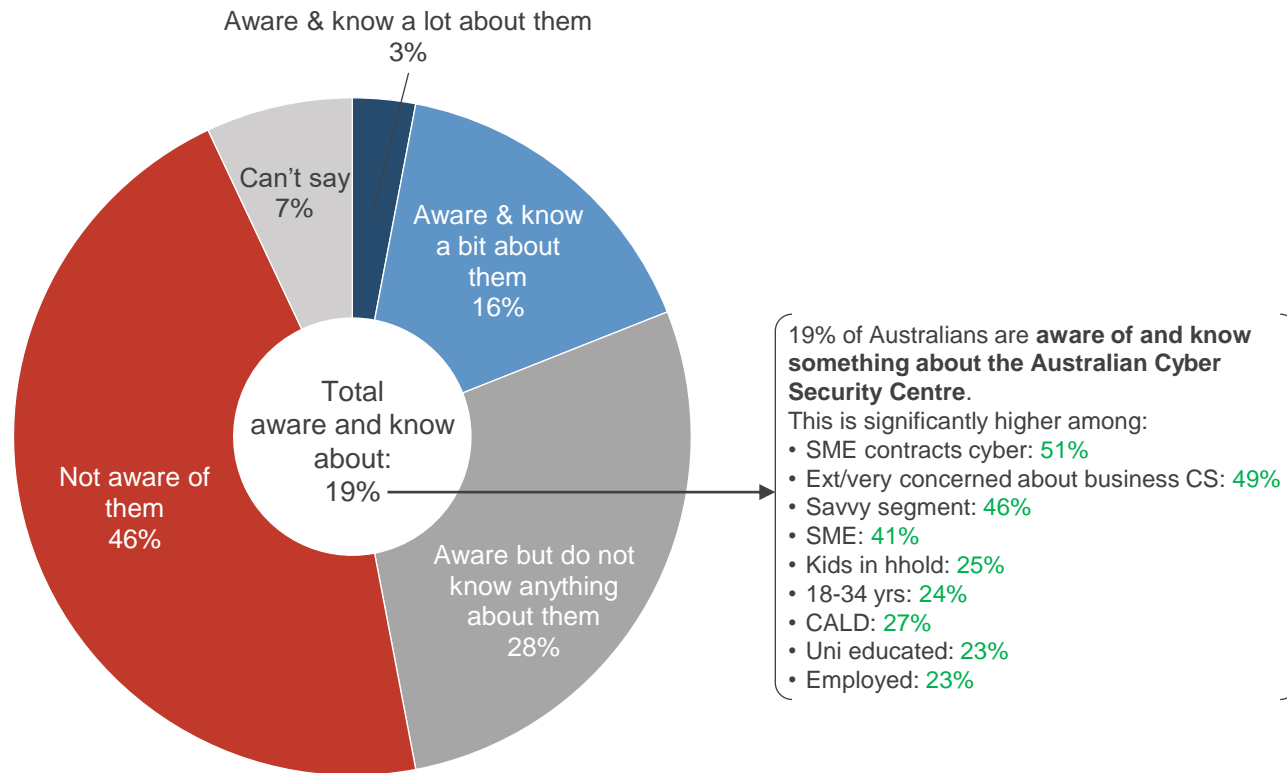
Q30. The Australian Government recently announced its 2020 Cyber Security Strategy, where \$1.67 billion will be invested over 10 years to bolster cyber security. Before now, were you aware of this announcement? / Q31. Following are some of the areas of focus of the Australian Government's Cyber Security Strategy. Which areas are you interested in knowing or hearing more about?

Base: All respondents (n=2,000).



When prompted, less than 1 in 5 Australians has knowledge of the ACSC beyond having heard of it

Prompted awareness of the Australian Cyber Security Centre



Significantly **higher** than the total at the 95% confidence interval.

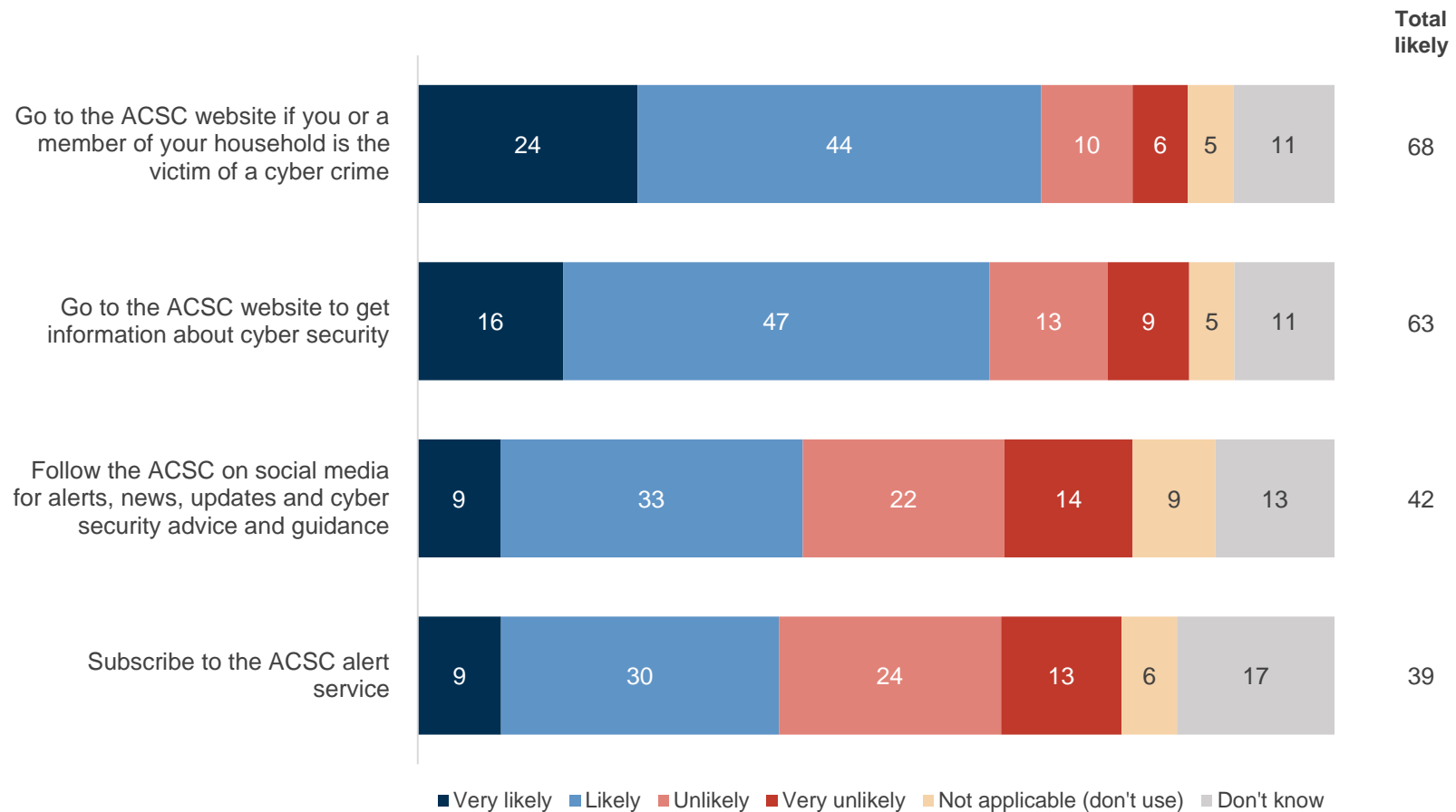
Q32. The Australian Cyber Security Centre (ACSC) provides advice and information about how to protect you, your family and your business online. ACSC leads the Australian Government's efforts to improve cyber security. Their role is to help make Australia the safest place to connect online. The ACSC is also responsible for running the Stay Smart Online program. Prior to reading the above, were you aware of the ACSC and how much do you know about them (other than what you have just read)?

Base: All respondents (n=2,000).

Providing support to victims of cyber crime or information on cyber security are most likely reasons to use ACSC



Likelihood to undertake actions (%)



A large, dark blue, stylized letter 'W' that spans the right side of the page. Inside the 'W', there is a glowing, intricate network of white and light blue lines, resembling a neural network or a complex data structure, with several bright points of light.

Information needs



Section summary – information needs

There is unmet demand for more cyber security information

There is an unmet demand for more, readily accessible information about **cyber security**. One in every two Australians (50%) wants to hear more. This figure is even higher among those who have already expressed that they are ‘extremely’ or ‘very concerned’ about cyber security. Only 6% have no interest in any information. **There is an urgency to provide this information due to the level of exposure to cyber attacks of a notable proportion of SMEs and households.**

Avoiding internet fraud and theft is of paramount concern

The types of cyber threats Australians want to know about are consistent with their greatest concerns: identify theft (36%), internet fraud (31%), ransomware (25%) and email compromise (24%). One in four Australians want to know about all potential threats. In addition to more information, Australians are also eager to learn how to be more secure online, with only 10% having no interest in more information about how to be secure online.

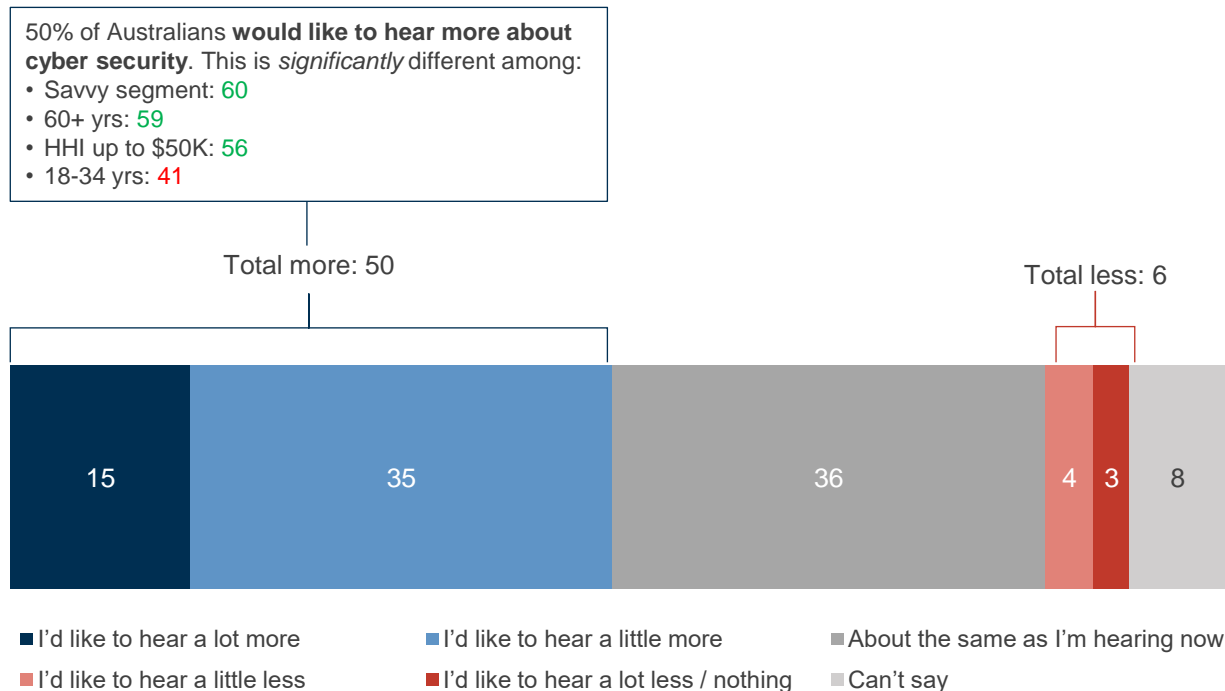
ACSC is the ideal source for disseminating cyber security information

For most Australians, the preferred source to receive cyber security information is through Government websites. A single dedicated Government website is the leading preference of two out of every five Australians (38%), coupled with other Government websites such as myGov (33%). A single site is more appropriate as it is a single touchpoint for everything cyber-related. It simplifies the search process and reduces confusion, an important consideration for people who are confused and concerned about cyber security.

Half the population wants to hear more on cyber security, more so among older and lower income Australians



Required level of information cyber security (%)

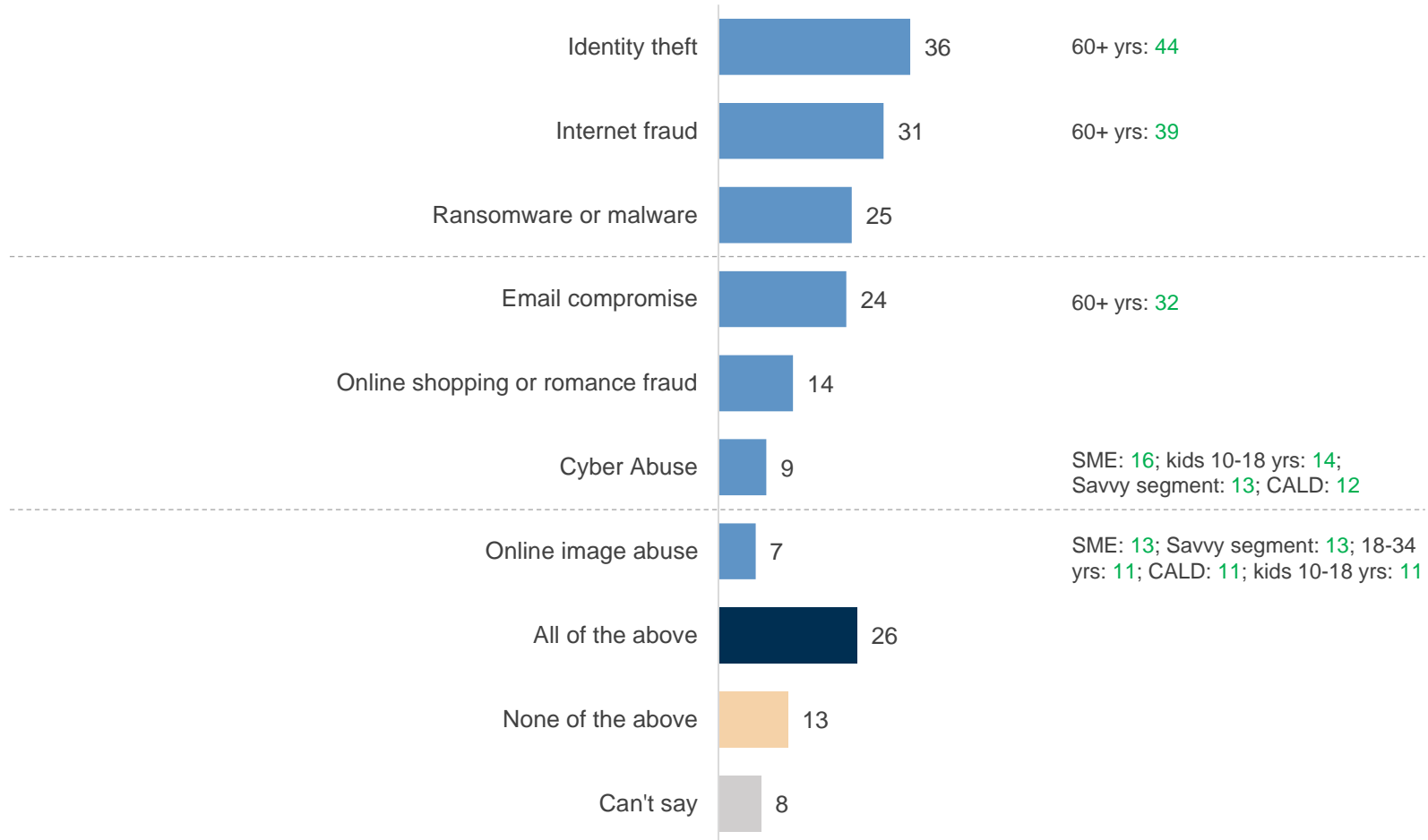


A quarter of Australians are interested in hearing about all cyber threats, but identity theft and fraud top the list



Cyber threats interested in hearing more about (%)
(Multiple response)

Significantly higher among:



Significantly higher than the total at the 95% confidence interval.

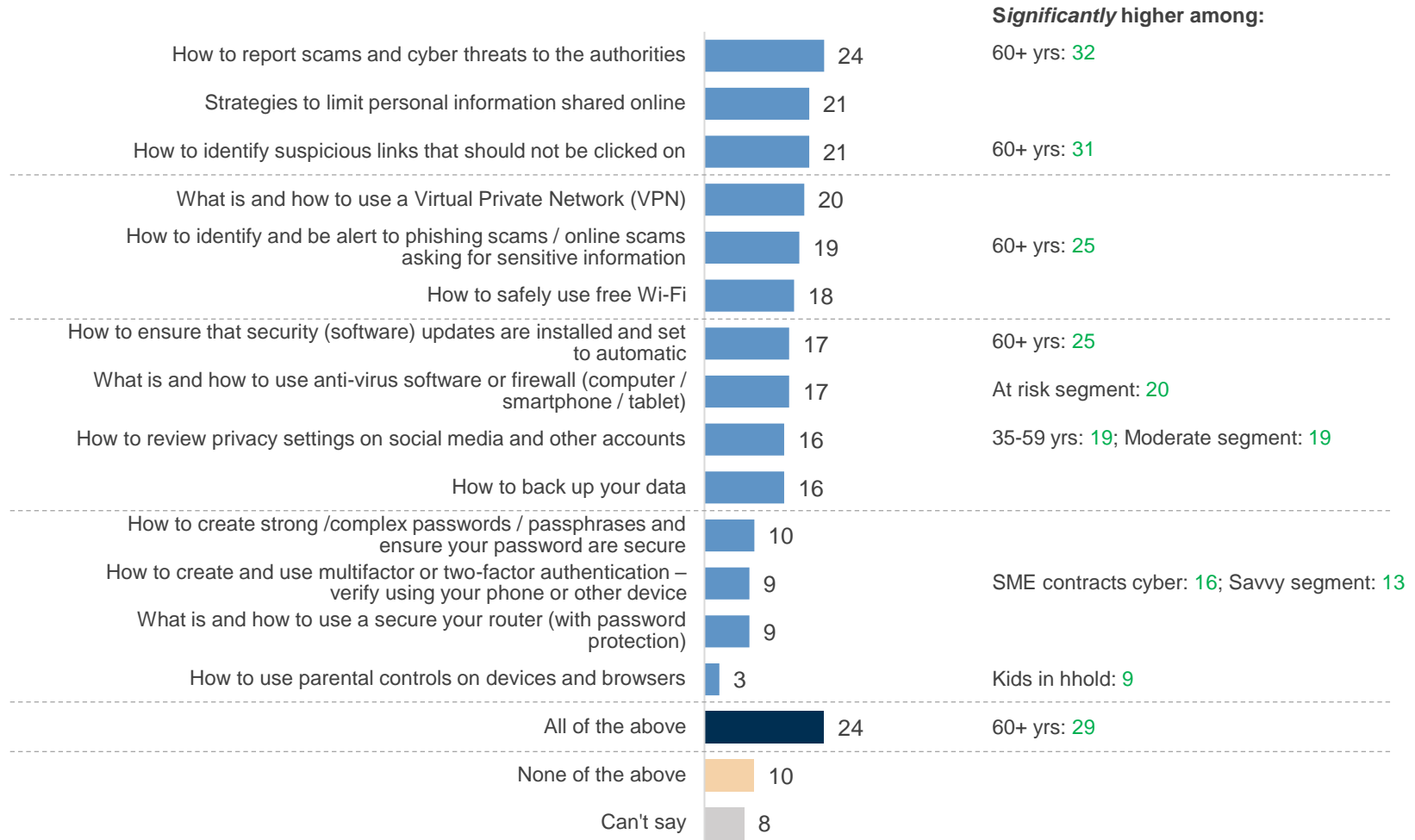
Q35. Which of the following cyber threats are you interested in hearing more about?

Base: All respondents (n=2,000).

There is keen interest in hearing about the many ways to ensure online security



Cyber security solutions interested in hearing more about (%) (Multiple response)



Significantly **higher** than the total at the 95% confidence interval.

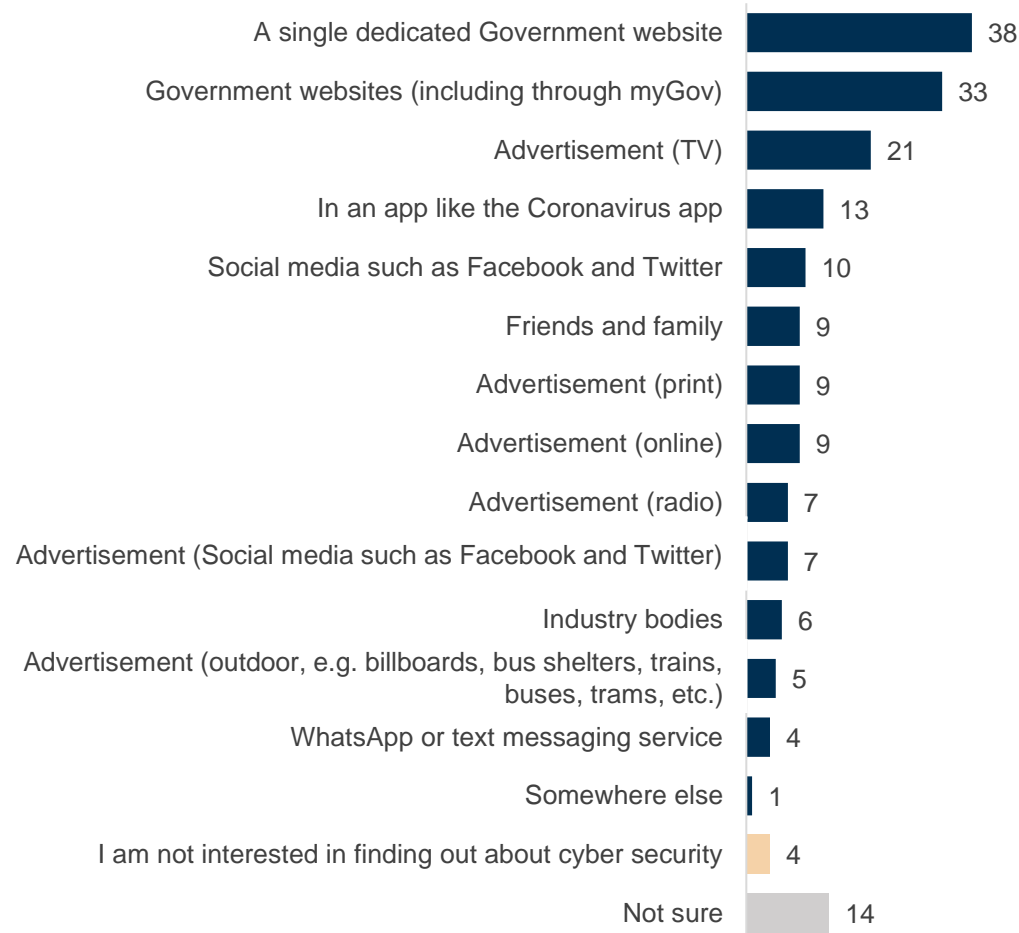
Q36. Which of the following ways to ensure you are secure online are you interested in hearing more about?

Base: All respondents (n=2,000).

Government websites are the preferred source of cyber security information, a single site is the main preference



Preferred source for information about cyber security (%) (Multiple response – up to three)



A single dedicated website is the most preferred source for cyber security information and advice across all groups



Preferred source for information about cyber security (%) (cont'd)
(Multiple response – up to three)

	Total	18-34 yrs	35-59 yrs	60+ yrs	SME	SME contracts CS	CALD	Kids in hhold	Segment		
									Savvy	Moderate	At risk
A single dedicated Government website	38	24	40	52	30	27	35	30	37	44	37
Government websites (including through myGov)	33	23	33	43	26	27	34	28	33	35	33
Advertisement (TV)	21	14	24	24	19	15	17	16	21	20	24
In an app like the Coronavirus app	13	12	12	14	13	19	13	14	16	15	12
Social media such as Facebook and Twitter	10	14	9	7	11	13	11	11	10	12	10
Friends & family	9	12	7	7	12	15	11	10	10	8	9
Advertisement (print)	9	6	7	13	11	12	7	9	10	8	8
Advertisement (online)	9	12	10	5	12	13	10	11	11	9	8
Advertisement (radio)	7	8	6	6	8	12	7	8	8	6	6
Advertisement (social media such as Facebook and Twitter)	7	12	6	3	11	9	11	11	9	7	7
Industry bodies	6	7	6	4	10	9	8	6	9	7	4
Advertisement (outdoor, e.g. billboards, bus shelters, trains, buses, trams, etc)	5	9	4	3	6	7	6	5	9	5	5
WhatsApp or text messaging service	4	5	4	4	7	8	8	5	6	4	4
Somewhere else	1	1	1	2	<1	0	1	1	3	1	1
Not interested in finding out about cyber security	4	4	5	4	3	3	3	5	3	2	6
Not sure	14	17	14	10	10	6	11	13	7	12	14

Significantly **higher** / **lower** than the total at the 95% confidence interval.

Q37. How would you **prefer** to find out about cyber security, including: How to be cyber safe and prevent against attacks; What to do if I you have been a victim of cyber crime; How to find out about scams; Cyber information and resources.

Base: All respondents (n=2,000).

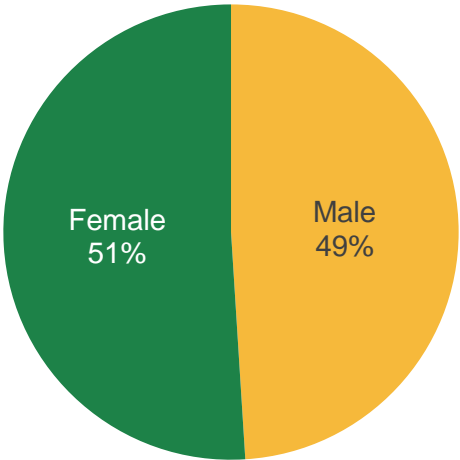
A large, dark blue letter 'W' dominates the right side of the page. It is filled with a complex, glowing pattern of white and light blue lines and dots, resembling a network or a star map. The background of the entire page is white.

Appendix: Demographics



Demographics

Gender



The data set has been weighted to reflect the demographic makeup (by gender, age and location) of the Australian population.

Age	%
18 to 34 years	30
35 to 59 years	42
60+ years	28
Location	%
Metro	67
Regional	33
ATSI	%
Yes	4
No	94
Prefer not to say	2

S1. Please indicate your gender. / S2. To which of the following age groups do you belong? / S3a. And what is your postcode? / D1. Are you of Aboriginal or Torres Strait Islander origin?
Base: All respondents (n=2,000).



Demographics (cont'd)

Dependent children in household	%	Education	%	Employment status	%
Yes	24	Post graduate degree	13	Employed full-time	38
No	75	Graduate certificate or diploma	7	Employed part-time or casual	16
Prefer not to say	2	Bachelor degree	26	Self employed	6
Age(s) of dependent children (multiple response – among those with dependent children in household)	%	Advanced diploma / Diploma	11	At home / Home duties	7
0 to 4 years	31	TAFE / Technical certificate	18	Retired – fully self-funded	6
5 to 9 years	36	Year 12	13	Retired – part self-funded, part pension	5
10 to 12 years	32	Year 11	3	Retired – full pensioner	10
13 to 15 years	27	Year 10 or below	8	Not retired – pensioner or benefits	3
16 to 18 years	22	Don't know / Prefer not to say	2	Unemployed	5
Prefer not to say	1	Household income	%	Student	3
		\$0-\$20,000	5	Prefer not to say	2
		\$20,001-\$50,000	22		
		\$50,001-\$75,000	16		
		\$75,001-\$100,000	15		
		\$100,001-\$200,000	22		
		More than \$200,000	7		
		Can't say / Prefer not to say	13		

D4. Do you have dependent children aged 18 years or under living in your household? / D5. Which age group/s are your child/ren in? / D6. What is your highest completed educational qualification? / D7. What is your current employment status? / D8. Please indicate your household annual income from all sources before tax?

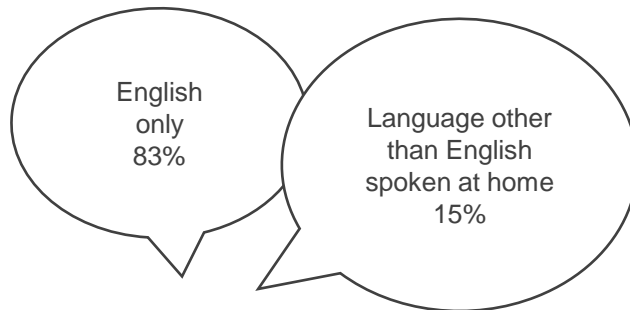
Base: All respondents (n=2,000); those with dependent children in household (n=449).



Cultural and Linguistically Diverse demographics

CALD: 20%

Languages



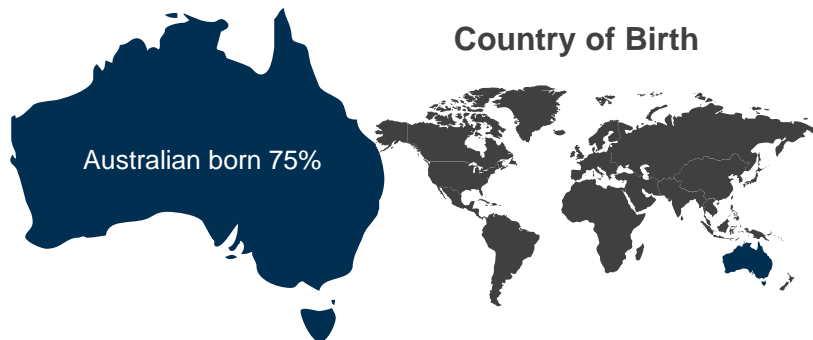
Prefer not to say: 2%

• Chinese	4%	• Arabic	1%
• Vietnamese	1%		
• German	1%		
• Spanish	1%		
• Russian	1%		
• Italian	1%		
• Hindi	1%		
• Greek	1%		
• French	1%		

Other languages mentioned by less than 1% of respondents include Malaysian, Korean, Japanese, Indian and Hungarian.

Note: this not an exhaustive list of languages mentioned.

Country of Birth



Born in a country other than Australia 23%

Prefer not to say: 2%

• United Kingdom	6%		
• New Zealand	3%		
• Other European	2%		
• China	2%		
• Germany	1%		
• Other Asian	1%		
• Malaysia	1%		
• India	1%		
• Korea	1%		

Other countries mentioned by less than 1% of respondents include Canada, United States, Hungary, Greece, France, Vietnam, Japan and Other Americas.

Note: this not an exhaustive list of countries mentioned.



SME demographics

SME	%
Yes, owner / financial partner / main decision maker	18
No	81
Prefer not to say	1
Hire or contract company/provider to manage business IT and CS (among SMEs)	%
Yes, I hire or contract a company/provider to manage IT only	22
Yes, I hire or contract a company/provider to manage cyber security only	14
Yes, I hire or contract a company/provider to manage both IT and cyber security	24
No, I don't hire or contract a company/provider to manage either IT or cyber security	37
Not sure	3

S5. Are you the owner, financial partner or main decision maker in an Australian business turning over more than \$75,000 per annum? /

S6. Do you hire or contract a company/provider to manage your IT and cyber security for your business?

Base: All respondents (n=2,000); SMEs (n=340).

THERE ARE OVER 25 MILLION PEOPLE IN AUSTRALIA...

FIND OUT WHAT THEY'RE THINKING.



Contact us
03 8685 8555



Follow us
[@JWSResearch](https://twitter.com/JWSResearch)

John Scales
Founder
jscales@jwsresearch.com

Mark Zuker
Managing Director
mzucker@jwsresearch.com

Katrina Cox
Director of Client Services
kcox@jwsresearch.com

Jessica Lai
Research Director
jlai@jwsresearch.com

Issued: 9th September 2020



J W S R E S E A R C H