Australian Government
Australian Institute of Criminology

AIC reports

Cybercrime in Australia 2023

Australian Cybercrime Survey

Contents

Acknowledgements

The Australian Institute of Criminology acknowledges the important work of Chris Owen, Gladys Lima and colleagues from Roy Morgan Research in conducting this survey. We are grateful for their support in designing and operationalising the survey.

To enhance readability, most question skips and survey programming have been removed from the questionnaire.

Australian Cybercrime Survey 2023

Screening questions

[These questions are asked to screen out participants when the quota is met for their age, sex and state/territory.]

Thank you for choosing to participate in this survey. We would like you to answer a few basic questions about yourself.

Q1. How do you describe your gender?
Gender refers to current gender, which may be different to sex recorded at birth and may be different to what is indicated on legal documents.

Please select only one option.

1. Man or male
2. Woman or female
3. Non-binary
97. I use a different term (Please Specify) _____
98. Don't know
99. Prefer not to say

Q2. What was your sex recorded at birth?
This may be different to your current gender.

Please select only one option.

1. Man or male
2. Woman or female
97. I use a different term (Please Specify) _____
98. Don't know
99. Prefer not to say

Q3. Please choose your age from the following ranges:

1. 14–15
2. 16–17
3. 18–19
4. 20–24
5. 25–29
6. 30–34
7. 35–39
8. 40–44
9. 45–49
10. 50–54
11. 55–59
12. 60–64
13. 65–69
14. 70+
99. Prefer not to say

Q4. What is the postcode of your usual place of residence?

If you do not know your postcode type 9999

_____

Q5. Please indicate the area in which you live

1. Australian Capital Territory
2. Sydney
3. NSW excluding Sydney
4. Melbourne
5. Victoria excluding Melbourne
6. Brisbane
7. Queensland excluding Brisbane
8. Adelaide
9. South Australia excluding Adelaide
10. Northern Territory
11. Hobart
12. Tasmania excluding Hobart
13. Perth
14. Western Australia excluding Perth
15. Outside Australia
99. Prefer not to say

Main Questionnaire

Consent page

Please read the following information carefully.

What are you asking me to do?

You are being invited to take part in a survey that aims to understand the Australian public's experiences of cybercrime – which is crime that involves a digital device, computer network or other forms of information and communication technology. You do not need to have had any experience of cybercrime to take part in this survey. If you choose to participate you will be asked to answer questions about yourself, your use of different technologies and devices, and whether you have encountered different cybercrimes, such as online harassment and abuse, fraud, identity theft, and malware attacks.

If you do not feel comfortable participating in this research, please close the survey window now.

How long will it take?

The survey will take approximately 25 minutes to complete. You are encouraged to complete the survey by yourself and in a private location where you will not be disturbed or observed by others.

Do I have to participate?

Your participation in the research is voluntary. This means that you do not have to take part unless you want to. If you feel uncomfortable about answering any questions you can choose not to respond. Most questions have an option such as 'prefer not to say'.

If you choose to participate, in recognition of the time and effort taken to complete the survey you will be offered a selection of rewards to choose from at the end.

How will you use my information?

The information you provide will be provided to and analysed by researchers at the Australian Institute of Criminology (AIC) to better understand cybercrime prevalence, risks and impacts. This information is vital for planning responses that can reduce the public's risk of becoming a cybercrime victim and address the harm that victims experience.

How will you protect my information?

We are very grateful for your contribution. To protect your identity, at no time will your name, address, birth date, or any other information that may identify you be made available to the AIC. The AIC will have no way of identifying you from the survey responses. All of your responses to the survey will be completely confidential.

Can I withdraw from the research?

You can withdraw from the research any time up to the survey completion date. Your comments will be deleted from all materials and your information will be destroyed. To pull out after you have submitted the survey, contact Roy Morgan Research at 1800 337 332.

There are no consequences if you choose not to take part in the research or choose to take part and then change your mind and wish to withdraw your input.

What if I need help?

This survey asks about experiences of cybercrime (including online harassment and abuse, fraud, identity theft, and malware attacks) which can be upsetting or distressing.

If you feel upset about anything (now or while completing the survey), the details of someone you can talk to will be made available to you. If you need any kind of help or support, it is available.

I have read all the information provided above	1. Yes 2. No
I consent to participate in the survey	1. Yes 2. No

Section A: Demographics

Q6. How do you describe your sexual orientation?

Please select only one option.

1. Straight (heterosexual)
2. Gay or lesbian
3. Bisexual
97. I use a different term
98. Don’t know
99. Prefer not to say

Q7. What is the highest education level you are in or have completed?

1. Year 9 or below
2. Year 10 or equivalent
3. Year 11 or equivalent
4. Year 12 or equivalent
5. University (undergraduate)
6. University (postgraduate)
7. Vocational qualification (e.g. TAFE)
97. Other (Please Specify) _____
98. Don’t know
99. Prefer not to say

Q8. What is your current relationship status?

1. Single, and have never been married
2. In a non-de-facto relationship (living separately)
3. De-facto relationship (living together)
4. Married
5. Separated or divorced
6. Widowed
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q9. Which of the following best describes your current employment status?

1. Working full-time (i.e. 35 or more hours per week in one or more jobs, including self-employment)
2. Working part-time
3. Semi-retired
4. Unemployed, not looking for work
5. Unemployed, looking for work
6. Full-time homemaker
7. In full-time education only
8. Retired
9. Not working due to health condition, illness or injury
10. Full time carer

11. Casual worker
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q10. Were you employed at any point in the last 12 months?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q11. What best describes the industry in which you were last employed?

1. Agriculture, Forestry and Fishing
2. Mining
3. Manufacturing
4. Electricity, Gas, Water and Waste Services
5. Construction
6. Wholesale Trade
7. Retail Trade
8. Accommodation and Food Services
9. Transport, Postal and Warehousing
10. Information Media and Telecommunications
11. Financial and Insurance Services
12. Rental, Hiring and Real Estate Services
13. Professional, Scientific and Technical Services
14. Administrative and Support Services
15. Public Administration and Safety
16. Education and Training
17. Health Care and Social Assistance
18. Arts and Recreation Services
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q12. Do you own, manage or work for a small to medium sized business (i.e. less than 200 employees)?

1. Yes – small/medium business owner, operator or manager
3. Yes – small/medium business employee
2. No
98. Don't know
99. Prefer not to say

Q13. Do you own or work for a large business or company (i.e. 200 employees or more)?

1. Yes – large business / company owner, operator or executive
3. Yes – large business / company employee
2. No
98. Don't know
99. Prefer not to say

Q14. Do you identify as Aboriginal or Torres Strait Islander?

1. Yes – Aboriginal
2. Yes – Torres Strait Islander
3. Yes – Both Aboriginal and Torres Strait Islander
4. No
98. Don't know
99. Prefer not to say

Q15. What language do you most often speak at your home?

1. English
2. Mandarin
3. Arabic
4. Cantonese
5. Vietnamese
6. Italian
7. Greek
8. Hindi
9. Spanish
10. Punjabi
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q16. Were you born outside of Australia?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q17. What was your individual gross income from all sources for last financial year (i.e. before tax has been deducted)?

1. 0 – $18,200
2. $18,201 – $37,000
3. $37,001 – $80,000
4. $80,001 – $180,000
5. $180,001 and over
98. Don't know
99. Prefer not to say

Q18. Do you have any children?

1. Yes
2. No
98. Don’t know
99. Prefer not to say

Q19. Do you have any children or adult children currently living with you? (Including non-biological step-children, foster children, etc)

1. Yes
2. No
98. Don’t know
99. Prefer not to say

Q20. How old is the oldest child/ adult child currently living with you?

_____

98. Don’t know
99. Prefer not to say

Q21. Do you have any health conditions that have lasted, or are likely to last, 6 months or longer?

For example: intellectual impairments, physical or mobility impairments, vision impairments, hearing impairments, speech impairments and psychiatric conditions

1. Yes
2. No
98. Don’t know
99. Prefer not to say

Q22. Because of your health condition(s), are you restricted in your everyday activities or do you need help or supervision with everyday activities?

1. Yes
2. No
98. Don’t know
99. Prefer not to say

Section B: Internet and technology use

Q23. This next section asks about your everyday use of the internet and electronic devices. This includes work and personal use.

Please indicate how often you undertake each activity.

	DAILY	WEEKLY	MONTHLY	LESS THAN MONTHLY	NEVER	PREFER NOT TO SAY
1. Browsing or looking for information	5	4	3	2	1	99
2. Sending emails	5	4	3	2	1	99
3. Posting or responding to posts on social media (e.g. Facebook, Twitter, TikTok)	5	4	3	2	1	99
4. Posting or responding to posts on online blogs, forums, interest groups (e.g. Reddit, Quora)	5	4	3	2	1	99
5. Purchasing items off online marketplaces (e.g. Ebay, Facebook marketplace)	5	4	3	2	1	99
6. Online banking and other financial activities online	5	4	3	2	1	99
7. Messaging and chatting online (e.g. Facebook messenger, Snapchat)	5	4	3	2	1	99
8. Private video chatting over apps and platforms (e.g. Zoom, Teams, Facetime)	5	4	3	2	1	99
9. Livestreaming videos of myself online (e.g. Youtube, Facebook Live, Instagram Live, OnlyFans)	5	4	3	2	1	99
10. Streaming videos on your computer, phone or TV (e.g. Netflix, Stan, YouTube, etc)	5	4	3	2	1	99

11. Purchasing items off online store websites and apps (excluding classifieds and marketplaces)	5	4	3	2	1	99
12. Reading news articles online	5	4	3	2	1	99
13. Being active on romance / dating websites or apps (e.g. Tinder, Plenty of Fish)	5	4	3	2	1	99
14. Participating in online gaming / sports	5	4	3	2	1	99
15. Accessing sexually explicit adult websites (e.g. Pornhub, Xvideos)	5	4	3	2	1	99
16. Subscribing to sexually explicit adult platforms (e.g. OnlyFans, adultcamdeals)	5	4	3	2	1	99
17. Making donations or payments over gaming, streaming or fundraising platforms	5	4	3	2	1	99
18. Livestreaming videos of content creators, influencers or gamers online (e.g. Twitch, Instagram Live)	5	4	3	2	1	99

Q24. Which of these social media or networking platforms, if any, do you use on a daily or weekly basis?

Select all that apply

1. Bumble
2. Discord
3. eharmony
4. Facebook
5. Gab
6. Google Hangouts
7. Grindr
8. Hinge
9. Incels.is
10. Instagram
11. Kiwi Farms
12. LinkedIn

13. Match.com
14. Messenger
15. OkCupid
16. Omegle
17. Parler
18. Pinterest
19. Plenty of Fish
20. Reddit
21. Rumble
22. Signal
23. Skype
24. Snapchat
25. Steam
26. Telegram
27. TikTok
28. Tinder
29. Tumblr
30. Twitch
31. Twitter
32. WeChat
33. Weibo
34. WhatsApp
35. YouTube
36. 4 Chan
37. 8 Kun
97. Other (Please Specify) _____
96. Don't use social media or networking sites
98. Don't know
99. Prefer not to say

Q25. In an average week, how many hours in total do you spend using social media (e.g. Facebook, Instagram, Twitter, etc.)?

1. More than 8 hours a week
2. Between 3 and 8 hours a week
3. Up to 3 hours per week
4. No Social Media in an average week

Q26. In an average week, how many times in total do you use the internet?

1. 3+ times a day
2. Twice a day
3. Once a day
4. A few times a week
5. Less often

Q27. On average, how many hours on a normal business day would you spend actively using the internet for work-related purposes?

_____

98. Don't know
99. Prefer not to say

Q28. On average, how many hours per day would you spend actively using the internet for personal use?

_____

98. Don't know
99. Prefer not to say

Q29. Thinking about your security and safety online, have you done any of the following in the last 12 months?

Select all that apply

1. I opened emails from people or organisations I didn't know
2. I accepted friend requests from people online who I have not met in person
3. I have checked my privacy settings on social media accounts
4. I purchased or continued to have cyber insurance
5. I accepted cookies from websites that save my browsing information
6. I generally browsed in incognito mode
7. I generally cleared my browsing history, data and cookies frequently
8. I participated in training to stay safe online / protect my online environment and information
9. I shared a password or a code for an account I own with someone I know (or who I thought was someone I know)
10. I installed or used spam filtering software
11. I used freely available WiFi in a public location to conduct a financial transaction (transfer money, purchase something online, etc)
12. I installed or used anti-virus software or firewalls on my devices
13. I regularly updated the security software on my device when prompted by my device's security system
14. I regularly updated my password on secure accounts, including email, banking or online stores and social media
15. I used a secure password manager
16. I used password protection on my router
17. I used a different password for secure online accounts, especially for banking or financial transactions
18. I have changed my privacy settings on social media accounts from the default to a more restricted setting
19. I used a Virtual Private Network (VPN) when using the internet
20. I set, or already had installed, parental controls on devices and browsers that restrict access to certain content
21. I used voice, fingerprint, facial or iris recognition technology to access my devices, such as my mobile phone
22. When I am not certain who the sender of a SMS text or email is, I avoid clicking on links or attachments

23. If I am unsure about a SMS text or email I have received from a company or government department, I independently contact them myself to check
96. None of the above
98. Don't know
99. Prefer not to say

Q30. How would you rate your level of knowledge of digital technologies?

1. Very Low
2. Low
3. Moderate
4. High
5. Very High
98. Don't know
99. Prefer not to say

Q31. How would you rate your ability to use digital technologies?

1. Very Low
2. Low
3. Moderate
4. High
5. Very High
98. Don't know
99. Prefer not to say

Section C: Online abuse and harassment

Q32. Below is a list of experiences people can have interacting with others when using the internet, their personal devices or technology.

Have any of the incidents ever happened to you?

This includes incidents in a personal or work setting.

Please read each option carefully and select all that apply to you.

1. I was threatened with the release of sensitive, personal, compromising or intimate photos, video or information that was stored online, on a digital device or sent in messages
2. Someone shared or published sensitive, personal, compromising or intimate photos or videos of me without my consent
3. Someone stole my online personal information (including photos and videos) and used it without my permission
4. Someone hacked into my social media or network account (including communicating with my contacts or posting messages or status updates from my accounts)
5. Someone used technology to stalk or repeatedly harass me, including being contacted by someone you have blocked or asked to not contact you
6. Someone used coercion, blackmail or demands to try and get me to send them sensitive, personal or compromising photos, video or information that was stored online, on a digital device or sent in messages (e.g. sextortion)
7. Someone set up fake social media or networking profiles pretending to be me (e.g. and communicated with my contacts or posted messages or status updates from my accounts)
8. Someone published identifying information (such as my full name, contact number, address, school,]etc) with malicious intent (i.e. doxing)
9. Someone tried to stop me from communicating with others online or over my mobile
10. Someone restricted my access to online resources (e.g. social media, electronic legal documents, banking and utility accounts, etc)
11. Someone monitored my activity online or on my phone (including installing spyware, going through my private messages, etc)
12. Someone spread rumours about me via electronic communication (e.g. emails, social media or text messages)
13. Someone sent or posted photos and videos of me to others to try and embarrass, hurt or blackmail me
14. Someone created fake videos or photos of me (e.g. “deep fakes”)
15. Someone subjected me to hate speech or made derogatory, malicious or threatening comments directly to me based on my religion, ethnicity, gender, sexuality or ideology
16. Someone sent or posted mean or hurtful messages via electronic communication (e.g. emails, social media or text messages) that made me feel hurt, embarrassed or unsafe
17. I was sent unsolicited sexually explicit messages, images or videos
96. None of the above
98. Don’t know
99. Prefer not to say

[If respondent has not experienced any incidents, they skip to Section D]

Q33. Please indicate whether any of the following incidents you have just selected happened to you in the last 12 months.

This includes incidents in a personal or work setting.

Select all that apply.

96. None of the above
98. Don't know
99. Prefer not to say

Q34. Which of the following incidents that happened to you in the last 12 months happened the most recently?

_____

98. Don't know
99. Prefer not to say

Q35. How old were you the first time this kind of incident happened to you?

"I was threatened with the release of sensitive, personal, compromising or intimate photos, video or information that was stored online, on a digital device or sent in messages"

_____
98. Don't know
99. Prefer not to say

Q36. How old were you the first time this kind of incident happened to you?

"Someone shared or published sensitive, personal, compromising or intimate photos or videos of me without my consent"

_____

98. Don't know
99. Prefer not to say

Q37. You mentioned that the most recent incident that happened to you in the last year was:

Who was involved in this incident?

If multiple people were involved, select the person closest to you.

1. Friend or former friend
2. A partner or former partner
3. Family member
4. A work colleague or former work colleague
5. Someone at my school/ university/ TAFE
6. A stranger online
7. An acquaintance
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q38. Did the perpetrator(s) demand money from you to resolve the most recent incident?

This includes all forms of extortion; for example, paying money to stop the release of intimate images, to stop the release of personal information, to regain control over your account, to take down fake profiles, etc.

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q39. How much did they demand?

This can include payments in money, cryptocurrency and/or gift cards. For cryptocurrency and gift cards, report the AU$ value of the cryptocurrency or gift cards at the time of the incident.

If you were demanded another currency, please provide your answers in approximate AU$ value at the time of the incident.

1. Money (specify) AU$_____
2. Cryptocurrency (specify) AU$_____
3. Gift cards (specify) AU$_____
4. TOTAL AU$_____
98. Don't know
99. Prefer not to say

Q40. Did you pay or attempt to pay the perpetrator?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q41. Did you spend money dealing with the consequences of the most recent incident (e.g. getting legal advice, time off work, installing new software)?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q42. How much money did you spend dealing with the consequences of the most recent incident?

AU$_____
98. Don't know
99. Prefer not to say

Q43. Of the AU$ _____ extorted from you, was any money reimbursed to you by banks or other organisations, or recovered in other ways?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q44. How much was reimbursed?

AU$_____
98. Don't know
99. Prefer not to say

Q45. Did you seek help, advice or support from any of the following people or organisations for the most recent incident?

This includes in-person and over the phone or internet

Select all that apply

1. Told a friend or family member about it
2. Told someone at my workplace (manager, HR, IT, etc)
3. Told a doctor, mental health service or social worker
4. Told a lawyer
5. The police
6. Crime Stoppers
7. ReportCyber / Australian Cyber Security Centre (ACSC) / cyber.gov.au / Australian Cyber Security Hotline: 1300 CYBER1
8. E-Safety Commissioner
9. A social media or networking content provider (e.g. Facebook, Twitter)
10. The moderator or admin of a specific social media or networking group or forum
11. My internet service provider
12. My mobile phone company
13. The manufacturer of my device(s)
14. A media organisation
15. A domestic violence or sexual assault helpline (e.g. 1800RESPECT)
96. I did not seek help, advice or support for the most recent incident
97. To someone or somewhere else (Please Specify) _____
98. Don't know
99. Prefer not to say

Q46. What were the reasons that you did not report the most recent incident to the police or ReportCyber (also known as the Australian Cyber Security Centre and cyber.gov.au)?

Select all that apply

1. I did not know how or where to report the matter
2. Felt ashamed or embarrassed
3. Did not know reporting to the police or the Australian Cyber Security Centre/ ReportCyber was an option
4. Did not want the person responsible arrested
5. Did not regard the incident as a serious offence

6. Did not know or think the incident was a crime
7. Did not think the police or the Australian Cyber Security Centre/ ReportCyber would be able to do anything
8. Have reported before and been dissatisfied with the outcome
9. Did not trust the police or the Australian Cyber Security Centre/ ReportCyber
10. Felt I would not be believed
11 Fear of the person responsible (e.g. fear of retaliation)
12. Fear of legal processes
13. Cultural/language reasons
14. Workplace/on the job incident - internal reporting procedures followed
15. Did not want to ask for help
16. Felt I could deal with it myself
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q47. Why did you report the most recent incident to the police and ReportCyber/ ACSC?

Select all that apply

1. To prevent this from happening to me again
2. To prevent this from happening to someone else
3. To create a safer cyber environment
4. To get my money back or loss or damage compensated
5. Retribution / Justice
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q48. How many days after the most recent incident happened did you make a report to the police?

_____

98. Don't know
99. Prefer not to say

Q49. How many days after the most recent incident happened did you make a report to ReportCyber?

_____

98. Don't know
99. Prefer not to say

Q50. What was the outcome of your report to police or ReportCyber for the most recent incident?

Select the option that best applies

1. I haven't heard anything or I don't know what happened
2. I was told that there was nothing that could be done or that my case wouldn't be investigated
3. I was told that my complaint would be investigated, but haven't heard anything else

4. I was told that my complaint had been investigated and was now closed (e.g. because the perpetrator couldn't be identified)
5. I was told by the police that someone had been arrested, charged or prosecuted
96. None of the above
98. Don't know
99. Prefer not to say

Q51. How satisfied were you with this outcome?

5. Very satisfied
4. Satisfied
3. Neither satisfied nor dissatisfied
2. Dissatisfied
1. Very dissatisfied
98. Don't know
99. Prefer not to say

Q52. In this next section, please indicate whether you have undertaken the following activities in the last 12 months.

Remember, your answers to these questions are completely confidential.

Select all that apply

1. I threatened someone with the release of their sensitive, intimate, compromising or personal photos, video or information that was stored online, on a digital device or sent in messages
2. I used a computer or mobile device to stalk or repeatedly harass someone
3. I tried to stop someone else from communicating with others online or over their mobile
4. I sent photos and videos of someone else to others to try and embarrass or hurt them
5. I sent messages to someone via electronic communication (e.g. emails, social media or text messages) with the intent to make them feel hurt, embarrassed or unsafe
6. I have subjected others to hate speech online or made derogatory, malicious or threatening comments directly to others online based on their religion, ethnicity, gender, sexuality or ideology
7. I sent unsolicited sexually explicit messages, images or videos to someone
96. None of the above
98. Don't know
99. Prefer not to say

Section D: Identity theft, misuse or compromise

Q53. Below is a list of strange or suspicious things which could indicate that your personal information has been compromised.

Personal Information' includes: name, address, date of birth, place of birth, gender, driver's licence information, passport information, Medicare information, health records, biometric information (e.g. fingerprint, voice, facial, iris recognition), signature, bank account information, credit or debit card information, password, personal identification number (PIN), tax file number (TFN), shareholder identification number (HIN), computer and/or other online usernames and passwords, student number, or other types of personal information.

Have any of these incidents ever happened to you where you suspect they may be the result of a privacy breach or information compromise?

This includes incidents in a personal or work setting.

Please read each option carefully and select all that apply to you.

1. Someone tried to obtain money from one of my investments or superannuation accounts
2. Someone tried to open a new bank account, apply for a new loan or obtain credit with my personal information or I received credit/ payment cards in the mail that I did not apply for
3. Someone used my personal information to fraudulently apply for government benefits
4. Someone used my personal information (including images) to create an impersonation account to extort my contacts
5. Suspicious transactions appeared in my bank statements or accounts, credit card or credit report
6. Someone used my personal information to purchase or order something or I received unfamiliar bills, invoices or receipts
7. I received calls from debt collectors asking about unpaid bills I didn't recognize
8. I was unsuccessful in applying for credit, and this was surprising given my credit history
9. Someone used my personal information to open up a mobile phone or utility account, or my current mobile phone or other utility lost service because my service has been transferred to a new unknown device
10. I got a medical bill for a service I didn't receive, or my medical claim was rejected because I had unexpectedly already reached my benefits limit
11. I was unable to file taxes because someone had already filed a tax return in my name
12. Someone gained access to my cryptocurrency wallet or exchange account and made transactions or stole currency
13. Someone used my personal information to create a fake cryptocurrency wallet or exchange account
14. Someone used my personal information to attempt to apply for a job or rent a property
15. Someone used my personal information to attempt to give false info to police

96. None of the above
98. Don't know
99. Prefer not to say

[If respondent has not experienced any incidents, they skip to Section E]

Q54. Please indicate whether any of the following incidents you have just selected happened to you in the last 12 months where you suspect they may be the result of a privacy breach or information compromise.

This includes incidents in a personal or work setting.

Select all that apply.

96. None of the above
98. Don't know
99. Prefer not to say

Q55. Which of the following incidents that happened to you in the last 12 months happened the most recently?

98. Don't know
99. Prefer not to say

Q56. How did you find out about the most recent incident of your identity or personal information being compromised?

1. I discovered myself
2. Someone I know told me
3. A government or financial agency told me
4. I was notified by my email or social media account, internet browser or security software
5. I was contacted by police
97. Some other way (Please Specify) _____
98. Don't know
99. Prefer not to say

Q57. How do you think that your personal information was obtained in the most recent incident?

Select all that apply

1. In a face-to-face meeting (e.g. a job interview or a doorknock appeal)
2. By telephone (excluding SMS)
3. While communicating online (e.g. social media messages, chat rooms or features)
4. By email
5. By SMS text messages
6. From hacking of a computer or other computerised device (e.g. smartphone)
7. Theft of an identity or other personal document (Please specify type) _____
8. Theft of my mail
9. From information lost or stolen from an organisation or government agency (i.e. a data breach)
10. From an online banking transaction
11. From information I placed on social media (e.g. Facebook, LinkedIn etc.)
12. From information I placed on a website (other than social media, e.g. online shopping)
13. From an ATM transaction or EFTPOS or credit card transaction
14. From a person that I know
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q58. Please indicate which of the following types of personal information you think were misused in the most recent incident.

1. Name
2. Address
3. Telephone/Mobile number
4. Date of birth
5. Place of birth
6. Gender
7. Driver's licence information
8. Passport information
9. Medicare information / medical records
10. Health insurance information
11. Biometric information (e.g. fingerprint, voice, facial, iris recognition)
12. Signature
13. Bank account information
14. Credit or debit card information
15. Password
16. Personal Identification Number (PIN)
17. Tax File Number (TFN)
18. Computer username
19. Email address
20. Online account username
21. Photos / images of me
22. Videos of me
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q59. Did this most recent incident result in money or cryptocurrency being stolen or you making a payment with gift cards?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q60. Please indicate the total amount lost.

This can include payments in money, cryptocurrency and/or gift cards. For cryptocurrency and gift cards, report the AU$ value of the cryptocurrency or gift cards at the time it was stolen.

If you were demanded another currency, please provide your answers in approximate AU$ value at the time of the incident.

1. Money (specify) AU$_____
2. Cryptocurrency (specify) AU$_____
3. Gift cards (specify) AU$_____
4. TOTAL AU$_____
98. Don't know
99. Prefer not to say

Q61. Did you spend money dealing with the consequences of the most recent incident? (e.g. getting legal advice, lost income, installing new software)?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q62. How much money did you spend dealing with the consequences [IF Q43=ANY 1-17 SHOW: of the most recent incident]?

AU$_____
98. Don't know
99. Prefer not to say

Q63. Approximately how many hours did you spend dealing with the consequences of having your personal information misused?

Number of whole hours spent_____
98. Don't know
99. Prefer not to say

Q64. Of the AU$ _____ stolen, was any money reimbursed to you by banks or other organisations, or recovered in other ways?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q65. How much was reimbursed?

AU$_____
98. Don't know
99. Prefer not to say

Q66. As a direct result of the most recent incident of having had your personal information misused, in what ways has your behaviour changed?

Select all that apply

1. I am more careful when I use or share personal information
2. I am more careful with who I add on my social media accounts
3. I use biometric technologies more frequently (fingerprints, facial or voice recognition, etc.)
4. I changed my password(s)
5. I implemented two-factor authentication
6. I changed my social media account(s)
7. I made my social media accounts private and secure
8. I closed my social media accounts temporarily or permanently
9. I changed my email address(es)
10. I changed my banking details

11. I changed my telephone number(s)
12. I changed my place of residence
13. I use better security for my computer or other computerised devices
14. I lock my mailbox
15. I redirect my mail when I am away or move residence
16. I shred personal documents before disposing of them
17. I review my financial statements more carefully
18. I applied for a copy of my credit report
19. I signed up for a commercial identity theft alert or protection service
20. I don't trust people as much
21. I avoid using the internet for banking and purchasing goods and services
96. My behaviour has not changed
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q67. Did you seek help, advice or support from any of the following people or organisations for the most recent incident?

This includes in-person and over the phone or internet.

Select all that apply

1. Told a friend or family member about it
2. Told someone at my workplace (manager, HR, IT, etc)
3. Told a doctor, mental health worker or social worker
4. Told a lawyer
5. The police
6. Crime Stoppers
7. ReportCyber / Australian Cyber Security Centre (ACSC) / cyber.gov.au / Australian Cyber Security Hotline: 1300 CYBER1
8. E-Safety Commissioner
9. IDCARE
10. A consumer protection agency (e.g. Scamwatch, Consumer Affairs, Office of Fair Trading)
11. A bank or credit union, a credit / debit card company (e.g. Visa or MasterCard) or an e-commerce provider (e.g. PayPal)
12. A government authority (e.g. Medicare, ATO)
13. Office of the Australian Information Commissioner
14. Australian Passport Office
15. A Road/Traffic Authority
16. The company that runs my security software (e.g. McAfee, Norton)
17. My internet service provider
18. My mobile phone company
19. The manufacturer of my device(s)
20. An insurance company
21. A utility company (e.g. gas, electricity)
22. A media organisation
96. None of the above
97. To someone or somewhere else (Please Specify) _____
98. Don't know
99. Prefer not to say

Q68. What were the reasons that you did not report the most recent incident to the police or ReportCyber (also known as the Australian Cyber Security Centre and cyber.gov.au)?

Select all that apply

1. I did not know how or where to report the matter
2. Felt ashamed or embarrassed
3. Did not know reporting to the police or the Australian Cyber Security Centre/ ReportCyber was an option
4. Did not want the person responsible arrested
5. Did not regard the incident as a serious offence
6. Did not know or think the incident was a crime
7. Did not think the police or the Australian Cyber Security Centre/ ReportCyber would be able to do anything
8. Have reported before and been dissatisfied with the outcome
9. Did not trust the police or the Australian Cyber Security Centre/ ReportCyber
10. Felt I would not be believed
11. Fear of the person responsible (e.g. fear of retaliation)
12. Fear of legal processes
13. Cultural/language reasons
14. Workplace/ on the job incident - internal reporting procedures followed
15. Did not want to ask for help
16. Felt I could deal with it myself

97. Other (Please Specify)_____
98. Don't know
99. Prefer not to say

Q69. Why did you report the most recent incident to the police and ReportCyber?

Select all that apply

1. To prevent this from happening to me again
2. To prevent this from happening to someone else
3. To create a safer cyber environment
4. To get my money back or loss or damage compensated
5. Retribution / justice

97. Other (specify) _____
98. Don't know
99. Prefer not to say

Q70. How many days after the most recent incident happened did you make a report to the police?

_____

98. Don't know
99. Prefer not to say

Q71. How many days after the most recent incident happened did you make a report to ReportCyber?

_____

98. Don't know
99. Prefer not to say

Q72. What was the outcome of your report to police or ReportCyber for the most recent incident?

Select the option that best applies.

1. I haven't heard anything or I don't know what happened
2. I was told that there was nothing that could be done or that my case wouldn't be investigated
3. I was told that my complaint would be investigated, but haven't heard anything else
4. I was told that my complaint had been investigated and was now closed (e.g. because the perpetrator couldn't be identified)
5. I was told by the police that someone had been arrested, charged or prosecuted
96. None of the above
98. Don't know
99. Prefer not to say

Q73. How satisfied were you with this outcome?

5. Very satisfied
4. Satisfied
3. Neither satisfied nor dissatisfied
2. Dissatisfied
1. Very dissatisfied
98. Don't know
99. Prefer not to say

Q74. Have you been successful in resolving all of the financial, credit and other problems associated with the most recent misuse of your personal information?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q75. In this next section, please indicate whether you have undertaken the following activities in the last 12 months.

Remember, your answers to these questions are completely confidential.

Select all that apply.

1. I gained unauthorised access to someone else's social media, email, streaming or shopping account
2. I used someone else's personal information (e.g. name, photos) to set up a fake profile pretending to be them
3. I accessed or attempted to access the darkweb

96. None of these
98. Don't know
99. Prefer not to say

Q76. Have you purchased or traded anything on the darkweb?

1. Fake identity data (e.g. fake passport, fake university degree)
2. Malware or hacking tools or services
3. Compromised identity and financial data (e.g. drivers licenses, credit card numbers)
4. Drugs
5. Sexually explicit content not allowed on the clear web
96. I have not purchased or traded anything on the darkweb
97. Something else (Please Specify) _____
98. Don't know
99. Prefer not to say

Q77. In the last 12 months, have you encountered sexually explicit material of people who are or look under the age of 18 online (whether unintentionally or otherwise)?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q78. Did you encounter this sexually explicit material of people who are or look under the age of 18 unintentionally?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q79. In the last 12 months, has your financial or personal information been exposed in a data breach? (e.g. Optus and Medibank leaks).

'Personal Information' includes: name, address, date of birth, place of birth, gender, driver's licence information, passport information, Medicare information, health records, biometric information (e.g. fingerprint, voice, facial, iris recognition), signature, bank account information, credit or debit card information, password, personal identification number (PIN), tax file number (TFN), shareholder identification number (HIN), computer and/or other online usernames and passwords, student number, or other types of personal information

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q80. Which company was involved in the most recent incident?

98. Don't know
99. Prefer not to say

Q81. Please indicate which of the following types of personal information you think were leaked or exposed?

1. Name
2. Address
3. Telephone/Mobile number
4. Date of birth
5. Place of birth
6. Gender
7. Driver's licence information
8. Passport information
9. Medicare information / medical records
10. Health insurance information
11. Biometric information (e.g. fingerprint, voice, facial, iris recognition)
12. Signature
13. Bank account information
14. Credit or debit card information
15. Password
16. Personal Identification Number (PIN)
17. Tax File Number (TFN)
18. Computer username
19. Email address
20. Online account username
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q82. In the most recent incident, how did you find out that your data had been exposed in the breach?

1. From the news or media
2. A government or financial agency told me
3. The company whose data was leaked contacted me directly
4. Someone I know told me about the leak
97. Some other way (Please Specify)_____
98. Don't know
99. Prefer not to say

Q83. What actions, if any, did you take after being notified of the data breach?

1. Changed my passwords on the relevant account
2. Changed my passwords to bank accounts
3. I monitored my bank account statements more closely
4. Checked my credit report for suspicious activity
5. Asked the Australian Taxation Office to monitor any unusual or suspicious activity with my tax file number
6. I monitored my emails more closely for suspicious activity

97. Some other action (Please Specify) _____
98. Don't know
99. Prefer not to say

Q84. Below is a list of organisations and institutions who may be responsible for preventing data breaches.

Please rank each organisation or institution according to who you think is most responsible for preventing data breaches into the future, where 1 has the highest responsibility and 5 has the lowest responsibility.

To do this, please click first on the box next to the organisation or institution that you believe has the highest responsibility, then click on the institution that you believe has the second highest responsibility, and so on. To remove a selection, just click on the box again.

- ☐ 1. The commonwealth government
- ☐ 2. The state / territory government where you live
- ☐ 3. Law enforcement
- ☐ 4. The private companies holding your data
- ☐ 5. Everyday citizens
- ☐ 98. Don't know
- ☐ 99. Prefer not to say

Section E: Malware and viruses

Q85. Below is a list of strange or suspicious things which could indicate that you have experienced a crime targeting your device (e.g. a virus).

Have any of the incidents ever happened to you, and you believe that they were not just the result of genuine device malfunction or aging?

This includes devices used in a personal or work setting.

Please read each option carefully and select all that apply to you.

1. My device slowed down and acted strangely
2. Popup ads started popping up everywhere
3. My browser kept getting redirected when I tried to search for a familiar site
4. Previously accessible system tools (such as personalised or security settings) were disabled
5. My devices keep crashing for some reason
6. Programs were opening and closing automatically
7. There was a lack of storage space that I couldn't explain
8. My device was working excessively while no programs were currently running
9. People I knew told me that I had been sending them suspicious messages and links over social media or email
10. My files have gone missing or been replaced with odd file extensions (such as .crypted or .cryptor) and the icons for the files were blank
11. My systems, devices or files had a virus or were inaccessible (e.g. locked or unreadable) and I received instructions for paying a ransom to restore access.
12. My devices, servers, service or networks were disrupted (e.g. slowed down, lost connection, had outages) and I received instructions for paying a ransom to restore functionality.
13. I received a ransom message on my device to say my data or information had been stolen and I had to pay to prevent this information from being leaked or sold online.

96. None of these
98. Don't know
99. Prefer not to say

[If respondent has not experienced any incidents, they skip to Section F]

Q86. Please indicate whether any of the following incidents that you have just selected have happened to you in the last 12 months, and you believe that they were not just the result of genuine device malfunction or aging.

This includes devices used in a personal or work setting.

Select all that apply.

96. None of these
98. Don't know
99. Prefer not to say

Q87. Please indicate which of the following incidents that happened to you in the last 12 months happened the most recently.

98. Don't know
99. Prefer not to say

Q88. Did this most recent incident result in money or cryptocurrency being stolen or you making a payment with gift cards?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q89. Please indicate the total amount lost.

This can include payments in money, cryptocurrency and/or gift cards. For cryptocurrency and gift cards, report the AU$ value of the cryptocurrency or gift cards at the time it was stolen.

If you were demanded another currency, please provide your answers in approximate AU$ value at the time of the incident.

1. Money (specify) AU$_____
2. Cryptocurrency (specify) AU$_____
3. Gift cards (specify) AU$_____
4. TOTAL AU$_____
98. Don't know
99. Prefer not to say

Q90. Did you spend money dealing with the consequences of the most recent incident (e.g. getting legal advice, time off work, installing new software)?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q91. How much money did you spend dealing with the consequences of the most recent incident?

AU$_____
98. Don't know
99. Prefer not to say

Q92. Of the AU$ _____ stolen, was any money reimbursed to you by banks or other organisations, or recovered in other ways?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q93. How much was reimbursed?

AU$_____
98. Don't know
99. Prefer not to say

Q94. Did you seek help, advice or support from any of the following people or organisations for the most recent incident? This includes in-person and over the phone or internet.

Select all that apply

1. Told a friend or family member about it
2. Told someone at my workplace (manager, HR, IT, etc)
3. Told a doctor, mental health worker or social worker
4. Told a lawyer
5. The police
6. Crime Stoppers
7. ReportCyber / Australian Cyber Security Centre (ACSC) / cyber.gov.au / Australian Cyber Security Hotline: 1300 CYBER1
8. A consumer protection agency (e.g. Scamwatch, Consumer Affairs, Office of Fair Trading)
9. A bank or credit union, a credit or debit card company (e.g. Visa or MasterCard) or an e-commerce provider (e.g. PayPal)
10. Office of the Australian Information Commissioner
11. A government authority (e.g. Medicare, ATO)
12. The company that runs my security software (e.g. McAfee, Norton)
13. My internet service provider
14. My mobile phone company
15. The manufacturer of my device(s)
16. A media organisation
17. An insurance company
96. I did not seek help, advice or support for the most recent incident
97. To someone or somewhere else (Please Specify) _____
98. Don't know
99. Prefer not to say

Q95. What were the reasons that you did not report the most recent incident to the police or ReportCyber (also known as the Australian Cyber Security Centre and cyber.gov.au)?

Select all that apply

1. I did not know how or where to report the matter
2. Felt ashamed or embarrassed
3. Did not know reporting to police or the Australian Cyber Security Centre/ ReportCyber was an option
4. Did not want the person responsible arrested
5. Did not regard the incident as a serious offence
6. Did not know or think the incident was a crime
7. Did not think the police or the Australian Cyber Security Centre/ ReportCyber would be able to do anything
8. Have reported before and been dissatisfied with the outcome
9. Did not trust the police or the Australian Cyber Security Centre/ ReportCyber
10. Felt I would not be believed

11. Fear of the person responsible (e.g. fear of retaliation)
12. Fear of legal processes
13. Cultural/ language reasons
14. Workplace/on the job incident - internal reporting procedures followed
15. Did not want to ask for help
16. Felt I could deal with it myself
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q96. Why did you report the most recent incident to the police and ReportCyber?

Select all that apply

1. To prevent this from happening to me again
2. To prevent this from happening to someone else
3. To create a safer cyber environment
4. To get my money back or loss or damage compensated
5. Retribution / justice
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q97. How many days after the most recent incident happened did you make a report to the police?

_____
98. Don't know
99. Prefer not to say

Q98. How many days after the most recent incident happened did you make a report to ReportCyber?

_____
98. Don't know
99. Prefer not to say

Q99. What was the outcome of your report to police or ReportCyber for the most recent incident?

Select the option that best applies

1. I haven't heard anything or I don't know what happened
2. I was told that there was nothing that could be done or that my case wouldn't be investigated
3. I was told that my complaint would be investigated, but haven't heard anything else
4. I was told that my complaint had been investigated and was now closed (e.g. because the perpetrator couldn't be identified)
5. I was told by the police that someone had been arrested, charged or prosecuted
96. None of the above
98. Don't know
99. Prefer not to say

Q100. How satisfied were you with this outcome?

5. Very satisfied
4. Satisfied
3. Neither satisfied nor dissatisfied
2. Dissatisfied
1. Very dissatisfied
98. Don’t know
99. Prefer not to say

Section F: Fraud and scams

Q101. This next section asks about whether you have been the victim of online fraud or scams.

In these descriptions - money can include cryptocurrency, and sensitive information includes any personal or financial details (e.g. Name, address, bank account number, credit card information).

Please indicate whether any of the following incidents have ever happened to you.

This includes incidents in a personal or work setting.

Please read each option carefully and select all that apply to you.

1. I paid money or provided sensitive information to a scam offering the false promise of prize money or a holiday package
2. I paid money or provided sensitive information to a scam falsely offering a rebate from the government, a bank or trusted organisation
3. I paid money or provided sensitive information to a scam offering me the false promise of an inheritance or share in a large sum of money in exchange for your assistance
4. I paid money or provided sensitive information to a scammer pretending to be a charity or disaster relief effort
5. I paid money, provided sensitive information or sent intimate images or videos to a scammer pretending to be a potential romantic partner
6. I paid money or provided sensitive information to a fake seller or buyer online
7. I paid money for health products, medicines or drugs from an online pharmacy and the products never arrived or were counterfeit
8. I paid a fake invoice for directory listings, advertising, domain name renewals or office supplies
9. I paid for extremely high call or text rates when replying to unsolicited SMS competitions
10. I paid money or provided sensitive information to a scammer to buy into an illegitimate investment, trading or shares scheme or to get early access to my super fund
11. I lost money buying sports betting prediction software, or becoming the member of a sport betting syndicate or investment scheme because these schemes did not work as advertised
12. I lost money or provided sensitive information to a scammer offering a job or employment
13. I provided sensitive information to a scammer pretending to be a known service institutions or company (bank, internet provider, post office, etc)
14. I allowed someone pretending to be a telecommunications or computer company to remote access my computer, or paid them money or provided sensitive information
15. I paid money or provided sensitive information to someone pretending to be a bank, government or law enforcement official for things like a speeding fine, tax office debt, or immigration or visa issues
16. I sent money to a scammer posing as a known business supplier, service institutions or company telling me that their banking details have changed
17. I lost cryptocurrency to a scammer in a pretend ‘give away’, business opportunity or investment opportunity
18. I lost cryptocurrency in an exit scam or rug-pull – where cryptocurrency developers or promoters abandon a project and disappear with investors’ funds.

96. None of the above
98. Don’t know
99. Prefer not to say

[If respondent has not experienced any incidents, they skip to Section G]

Q102. Please indicate whether any of the following incidents you have just selected happened to you in the last 12 months.

This includes incidents in a personal or work setting.

Select all that apply.

96. None of the above
98. Don't know
99. Prefer not to say

Q103. Which of the following incidents that happened to you in the last 12 months happened the most recently?

98. Don't know
99. Prefer not to say

Q104. Did this most recent incident result in money or cryptocurrency being stolen or you making a payment with gift cards?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q105. Please indicate the total amount lost.

This can include payments in money, cryptocurrency and/or gift cards. For cryptocurrency and gift cards, report the AU$ value of the cryptocurrency or gift cards at the time it was stolen.

If you were demanded another currency, please provide your answers in approximate AU$ value at the time of the incident.

1. Money (specify) AU$_____
2. Cryptocurrency (specify) AU$_____
3. Gift cards (specify) AU$_____
4. TOTAL AU$_____
98. Don't know
99. Prefer not to say

Q106. Did you spend money dealing with the consequences of the most recent incident? (e.g. getting legal advice, lost income, installing new software)?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q107. How much money did you spend dealing with the consequences of the most recent incident?

AU$_____
98. Don't know
99. Prefer not to say

Q108. Of the AU$ _____ stolen, was any money reimbursed to you by banks or other organisations, or recovered in other ways?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q109. How much was reimbursed?

AU$_____
98. Don't know
99. Prefer not to say

Q110. Did you seek help, advice or support from any of the following people or organisations for the most recent incident?

This includes in-person and over the phone or internet.

Select all that apply

1. Told a friend or family member about it
2. Told someone at my workplace (manager, HR, IT, etc)
3. Told a doctor, mental health worker or social worker
4. Told a lawyer
5. The police
6. Crime Stoppers
7. ReportCyber / Australian Cyber Security Centre (ACSC) / cyber.gov.au / Australian Cyber Security Hotline: 1300 CYBER1
8. IDCARE
9. E-Safety Commissioner
10. A consumer protection agency (e.g. Scamwatch, Consumer Affairs, Office of Fair Trading)
11. A bank or credit union, a credit or debit card company (e.g. Visa or MasterCard) or an e-commerce provider (e.g. PayPal)
12. A government authority (e.g. Medicare, ATO, Australian Passport Office, a Road/Traffic Authority)
13. The company that runs my security software (e.g. McAfee, Norton)
14. My internet service provider
15. My mobile phone company
16. The manufacturer of my device(s)
17. A social media or networking content provider (e.g. Facebook, Twitter)
18. The moderator or admin of a specific social media or networking group or forum
19. A media organisation
20. An insurance company
96. I did not seek help, advice or support for the most recent incident
97. To someone or somewhere else (Please Specify) _____
98. Don't know
99. Prefer not to say

Q111. What were the reasons that you did not report the most recent incident to the police or ReportCyber (also known as the Australian Cyber Security Centre and cyber.gov.au)?

Select all that apply

1. I did not know how or where to report the matter
2. Felt ashamed or embarrassed
3. Did not know reporting to the police or the Australian Cyber Security Centre/ ReportCyber was an option
4. Did not want the person responsible arrested
5. Did not regard the incident as a serious offence
6. Did not know or think the incident was a crime
7. Did not think the police or the Australian Cyber Security Centre/ ReportCyber would be able to do anything
8. Have reported before and been dissatisfied with the outcome
9. Did not trust the police or the Australian Cyber Security Centre/ ReportCyber
10. Felt I would not be believed
11. Fear of the person responsible (e.g. fear of retaliation)
12. Fear of legal processes
13. Cultural/language reasons
14. Workplace/on the job incident - internal reporting procedures followed
15. Did not want to ask for help
16. Felt I could deal with it myself
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q112. Why did you report the most recent incident to the police and ReportCyber?

Select all that apply

1. To prevent this from happening to me again
2. To prevent this from happening to someone else
3. To create a safer cyber environment
4. To get my money back or loss or damage compensated
5. Retribution / justice
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q113. How many days after the most recent incident happened did you make a report to the police?

_____
98. Don't know
99. Prefer not to say

Q114. How many days after the most recent incident happened did you make a report to ReportCyber?

_____
98. Don't know
99. Prefer not to say

Q115. What was the outcome of your report to police or ReportCyber for the most recent incident?

Select the option that best applies

1. I haven't heard anything or I don't know what happened
2. I was told that there was nothing that could be done or that my case wouldn't be investigated
3. I was told that my complaint would be investigated, but haven't heard anything else
4. I was told that my complaint had been investigated and was now closed (e.g. because the perpetrator couldn't be identified)
5. I was told by the police that someone had been arrested, charged or prosecuted
96. None of the above
98. Don't know
99. Prefer not to say

Q116. How satisfied were you with this outcome?

5. Very satisfied
4. Satisfied
3. Neither satisfied nor dissatisfied
2. Dissatisfied
1. Very dissatisfied
98. Don't know
99. Prefer not to say

Q117. In this next section, please indicate whether you have undertaken the following activities in the last 12 months.

Remember, your answers to these questions are completely confidential.

Select all that apply.

1. Created a fake social media account
2. Created a fake profile on dating websites, apps or social media with the intent of pretending to be someone's prospective romantic companion
3. Sent emails or text messages with the intention of tricking the recipient into sending money, or personal or financial information
4. Sold fake, counterfeit or substandard products online with the intention of tricking potential buyers into sending money
96. None of the above
98. Don't know
99. Prefer not to say

Section G: Impacts of victimisation

[If respondent has not experienced any cybercrime incidents listed in Sections C – F, then they skip Section G]

Q118. Your answers to the questions about different types of cybercrime indicate that you have been a victim of cybercrime in the last 12 months.

How has this impacted you in your personal life?

Select all that apply

1. I lost my job
2. I have experienced an increase in financial stress
3. I have become more socially isolated
4. I have increased the amount of time and/or money I spend gambling (in person or online)
5. I had to change my place of residence
6. I had to change my personal, banking and/or contact information
7. My relationship with my partner has been negatively impacted (if in current relationship)
8. I lost my trust in other people
9. It is harder to know which information to trust online
10. Less confident using the internet for personal affairs (eg. banking, purchasing items)
11. My relationships with family and friends have been negatively impacted
12. I have experienced mental or emotional distress
13. I experienced difficulty sleeping
14. My overall physical health and wellbeing has deteriorated
15. I had to seek medical treatment
16. I had to seek psychological or counselling treatment
17. I have increased my consumption of alcohol
18. I have increased my consumption of drugs (legal or illegal)
19. I have been in trouble with the police
20. I was embarrassed or my reputation was damaged
21. I had difficulty accessing online accounts and resources (e.g. bank accounts, utilities, email)
22. I had to commence legal action
23. I have been unable to get a loan when I needed one
24. I have had to borrow money from family and friends
25. My work was negatively impacted
26. My studies were negatively impacted
27. I lost important or sentimental data (e.g. photos, contact details, files, etc)
28. I had to pay for computer, phone or other hardware repairs or replacement
29. I had to buy new software
30. I had to buy new backup data storage or data storage devices
31. I had problems communicating with people (e.g. friends, family, employer)
32. I had problems communicating or dealing with businesses
33. I had problems communicating or dealing with government departments
34. I had to take time off work to deal with the consequences of victimisation (e.g. installing new security, going to IT repair shops, etc)
96. None of the above
98. Don’t know
99. Prefer not to say

Q119. [For each harm the respondent selects in Q118] How much of an impact did this have on you?

1. Minor impact
2. Moderate impact
3. Major impact

Q120. How has being a victim of cybercrime in the last 12 months impacted the small to medium business that you own or work for?

Select all that apply

1. There was a disruption to operations and/or trading (e.g. inability to carry out transactions, websites not functioning, etc)
2. Our insurance premiums were increased
3. There was litigation or legal action against the business
4. The business had to notify affected parties of a data breach
5. Theft of intellectual property or corporate information
6. Theft of customer or supplier information (e.g. contact details, financial data)
7. Theft of my information or other staff information (e.g. contact details, financial data)
8. Blocked customer access to the business online store or website
9. Having to shut down the business online store or website (temporarily or permanently)
10. The business' reputation was damaged
11. There was a loss of customers, sales or revenue
12. The business spent time repairing and improving systems
13. Professional relationships were damaged
14. We lost business contracts
15. The business was hit with fines and regulatory sanctions
16. Employees/ owners of the business resigned or lost their job
17. Employees/ owners of the business had to take time off work
18. Having to change the business banking and/or contact information
19. Difficulty accessing online accounts and resources (e.g. bank accounts, utilities, email)
20. Had to pay for computer, phone or other hardware repairs or replacement
21. Had to buy new software
22. Had to buy new backup data storage or data storage devices
23. Had problems communicating or dealing with businesses
24. Had problems communicating or dealing with government departments
96. None of the above
98. Don't know
99. Prefer not to say

Q121. [For each harm the respondent selects in Q120] How much of an impact did this have on the business?

1. Minor impact
2. Moderate impact
3. Major impact

Section H: Addenda

If the participant indicated they had experienced ransomware by answering yes to item 11, 12 or 13 in Q85, they are automatically directed into Addendum 3, the Ransomware Quantitative Addendum.

The remaining sample is split evenly into Addendum 1 (Cybercrime Resilience and Risk Addendum) and Addendum 2 (Identity Theft and Biometrics Addendum).

Addendum 1: Cybercrime Resilience and Risk Addendum

Respondents in this addendum are randomly allocated into one of the four cybercrime types:

- online abuse and harassment (25%)
- identity theft, misuse or information compromise (25%)
- malware and viruses (25%)
- fraud and scams (25%).

[Cybercrime type] is replaced by the cybercrime type that the respondent is allocated to.

This next section asks about your perceptions of [cybercrime type], including the knowledge and resources you have for protecting yourself, and your perceptions of the government response to [cybercrime type].

This section also asks several questions about your personality and mental health. We encourage you to answer these questions honestly. We have no way of identifying you from the survey responses. To protect your identity, at no time will your name, address, birth date, or any other information that may identify you be made available to the Australian Institute of Criminology. If you feel uncomfortable about answering any questions you can choose not to respond.

Q1_A1. How strongly do you agree or disagree with the next statements about cybercrime safety, risk, severity and harm?

	Strongly disagree	Disagree	Neither agree / disagree	Agree	Strongly agree	Prefer not to say
1. I feel safe from [insert cybercrime type] when online or using electronic devices	1	2	3	4	5	99
2. Over the next 12 months, it is likely that I will become the victim of [insert cybercrime type]	1	2	3	4	5	99
3. [insert cybercrime type] attacks are serious crimes	1	2	3	4	5	99
4. [insert cybercrime type] are harmful crimes	1	2	3	4	5	99

Q2_A1. How strongly do you agree or disagree with the next statements about cybercrime resilience?

	Strongly disagree	Disagree	Neither agree / disagree	Agree	Strongly agree	Prefer not to say
1. It is important that I can anticipate my risk of [insert cybercrime type]	1	2	3	4	5	99
2. I must continually monitor for signs of [insert cybercrime type] attempts	1	2	3	4	5	99
3. If I am the victim of [insert cybercrime type], it is important that I know how to respond appropriately	1	2	3	4	5	99
4. I have access to up-to-date information about [insert cybercrime type]	1	2	3	4	5	99
5. I have the resources and information to monitor [insert cybercrime type] attempts	1	2	3	4	5	99
6. If I was to fall victim to [insert cybercrime type], I have access to clearly defined procedures on how to deal with it	1	2	3	4	5	99
7. I know how my behaviour when online or using electronic devices impacts my risk of [insert cybercrime type]	1	2	3	4	5	99
8. I know what attempted [insert cybercrime type] looks like	1	2	3	4	5	99
9. I know what to do if I did fall victim to [insert cybercrime type]	1	2	3	4	5	99

Q3_A1. Please rate your agreement with each of these statements in relation to the Government response.

	Strongly disagree	Disagree	Neither agree / disagree	Agree	Strongly agree	Prefer not to say
1. I know where to go to for helpful information about [insert cybercrime type]	1	2	3	4	5	99
2. More needs to be done to inform online users about how to minimise the risk of [insert cybercrime type]	1	2	3	4	5	99
3. An easy and convenient means for reporting cybercrime is needed	1	2	3	4	5	99
6. I am satisfied with the Australian Government's response to [insert cybercrime type]	1	2	3	4	5	99
8. The Australian Government is doing more to respond to [insert cybercrime type] than it was 12 months ago	1	2	3	4	5	99

Q4_A1. Below are items that relate to the way you consume news and social media content. Please indicate how strongly you agree or disagree with each statement.

	Never	Rarely	Sometimes	Often	Always	Don't know	Prefer not to say
1. I check whether the authors of social media posts are credible (e.g., a qualified professional, official or expert)	1	2	3	4	5	98	99
2. I look at a person's social media history before I take what they say seriously	1	2	3	4	5	98	99
3. I research the claims made in social media posts on Google or another search engine, before sharing, liking or commenting	1	2	3	4	5	98	99
4. I check the original evidence or supporting sources cited in social media posts	1	2	3	4	5	98	99
5. I think about whether social media posts are fact or opinion	1	2	3	4	5	98	99
6. I am wary of websites that look like legitimate news organisations, but may be producing fake or misleading news stories	1	2	3	4	5	98	99
7. I use a range of different sources for developing an opinion on news and current affairs	1	2	3	4	5	98	99
8. I use official and expert sources for developing an opinion on news and current affairs	1	2	3	4	5	98	99
9. I think about whether news articles are fact or opinion	1	2	3	4	5	98	99
10. I think about the purpose of news articles (e.g, to inform, to change opinion or behaviour, to sell something)	1	2	3	4	5	98	99

This next section asks about your personality and feelings. We encourage you to answer these questions honestly. We have no way of identifying you from the survey responses. To protect your identity, at no time will your name, address, birth date, or any other information that may identify you be made available to the Australian Institute of Criminology. If you feel uncomfortable about answering any questions you can choose not to respond.

Q5_A1. Please indicate the extent to which you agree or disagree with each of these statements as it relates to you.

	Strongly disagree	Disagree	Neither agree / disagree	Agree	Strongly agree	Prefer not to say
1. I usually trust people until they give me a reason to not trust them	1	2	3	4	5	99
2. Trusting another person is not difficult for me	1	2	3	4	5	99
3. My typical approach is to trust new acquaintances until they prove I should not trust them	1	2	3	4	5	99
4. My tendency to trust others is high	1	2	3	4	5	99

Q6_A1. Please indicate for each of the statements, the extent to which they apply to your situation, the way you feel now.

	Yes	Somewhat	No	Don't know	Prefer not to say
1. I experience a general sense of emptiness	1	2	3	98	99
2. There are plenty of people I can rely on when I have problems	1	2	3	98	99
3. There are many people I can trust completely	1	2	3	98	99
4. There are enough people I feel close to	1	2	3	98	99
5. I miss having people around	1	2	3	98	99
6. I often feel rejected	1	2	3	98	99
7. When I compare myself to other people I know, most are better off than I am	1	2	3	98	99

Q7_A1. These questions measure some of the ways in which you act and think. Read each statement and select the appropriate response below.

	Rarely/ Never	Occasionally	Often	Almost always/ Always	Don't know	Prefer not to say
1. I don't pay attention	1	2	3	4	98	99
2. I am self-controlled	1	2	3	4	98	99
3. I concentrate easily	1	2	3	4	98	99
4. I am a careful thinker	1	2	3	4	98	99
5. I am a steady thinker	1	2	3	4	98	99
6. I do things without thinking	1	2	3	4	98	99
7. I say things without thinking	1	2	3	4	98	99
8. I act on impulse	1	2	3	4	98	99
9. I act on the spur of the moment	1	2	3	4	98	99
10. I plan tasks carefully	1	2	3	4	98	99
11. I plan trips well ahead of time	1	2	3	4	98	99
12. I plan for job security	1	2	3	4	98	99
13. I am future oriented	1	2	3	4	98	99

Q8_A1. The following questions ask about how you have been feeling during the last 30 days. For each question, please select the option that best describes how often you had this feeling. During the last 30 days, about how often did you feel…

	All of the time	Most of the time	Some of the time	A little of the time	None of the time	Prefer not to say
1. Nervous?	5	4	3	2	1	99
2. Hopeless?	5	4	3	2	1	99
3. Restless or fidgety?	5	4	3	2	1	99
4. So depressed that nothing could cheer you up?	5	4	3	2	1	99
5. That everything was an effort?	5	4	3	2	1	99

Addendum 2: Identity Theft and Biometrics Addendum

We would now like to ask you about your perceptions of the risks and harms of personal information misuse.

Personal information can include names, addresses, dates of birth, places of birth, gender, driver's licence information, passwords and bank account information. Personal information misuse includes obtaining or using someone's personal information without their permission to pretend to be them or to carry out a business in their name without their permission, or other types of activities and transactions. This does not include use of their personal information for direct marketing, even if this was done without their permission.

We would also like to ask you about your knowledge/use of and willingness to use various biometric technologies (fingerprint, facial recognition, iris scans, etc.). The questions also address your acceptance of various government uses of these technologies.

Biometric technologies will soon be employed as a primary verifier for digital identity solutions and applications such as myGovID (https://www.mygovid.gov.au) or AusPost Digital ID (https://www.digitalid.com/personal).

Q1_A2. In terms of harm to the Australian community, how serious do you think that misuse of personal information is?

4. Very serious
3. Somewhat serious
2. Not very serious
1. Not at all serious
98. Don't know
99. Prefer not to say

Q2_A2. Over the next 12 months, do you think the risk of someone misusing your personal information will increase or decrease?

5. Increase greatly
4. Increase somewhat
3. Not change
2. Decrease somewhat
1. Decrease greatly
98. Don't know
99. Prefer not to say

Q3_A2. How frequently have you used any of the following technologies in the past (in any way, not just to prevent misuse of personal information)?

This includes any way you have PERSONALLY used this technology in the past, other than for your pets or other non-personal uses.

	Never	Rarely	Occasionally	Frequently	Don't know	Prefer not to say
1. Passwords/PINs	1	2	3	4	98	99
2. Signatures	1	2	3	4	98	99
3. Voice recognition	1	2	3	4	98	99
4. Fingerprint recognition	1	2	3	4	98	99
5. Facial recognition	1	2	3	4	98	99
6. Iris recognition	1	2	3	4	98	99
7. Computer chip implanted under your own skin (not pets or devices)	1	2	3	4	98	99

Q4_A2. In order to prevent misuse of personal information in the future, how willing would you PERSONALLY be to use any of the following technologies (e.g. at ATMs, at airports, for computers, building access, etc.)?

	Extremely unwilling	Not willing	Willing	Extremely willing	Don't know	Prefer not to say
1. Passwords/PINs	1	2	3	4	98	99
2. Signatures	1	2	3	4	98	99
3. Voice recognition	1	2	3	4	98	99
4. Fingerprint recognition	1	2	3	4	98	99
5. Facial recognition	1	2	3	4	98	99
6. Iris recognition	1	2	3	4	98	99
7. Computer chip implanted under your own skin (not pets or devices)	1	2	3	4	98	99

Q5_A2. To what extent have you used any biometric technology (e.g. voice, fingerprint, face or iris recognition) for each of the following activities in the last 12 months?

	Never	Rarely	Occasionally	Frequently	Not applicable	Don't know	Prefer not to say
1. Logging onto mobile phones	1	2	3	4	96	98	99
2. Logging onto computers	1	2	3	4	96	98	99
3. For ATM/bank transactions	1	2	3	4	96	98	99
4. Opening a bank account	1	2	3	4	96	98	99
5. Applying for a mobile phone	1	2	3	4	96	98	99
6. For airport security processing (SmartGates)	1	2	3	4	96	98	99
7. Applying for a Tax File Number	1	2	3	4	96	98	99
8. For obtaining access to buildings (home, office)	1	2	3	4	96	98	99
9. For unlocking or starting cars	1	2	3	4	96	98	99

Q6_A2. How acceptable do you think it is to use facial recognition technologies for each of the following purposes?

	Extremely unacceptable	Unacceptable	Neither acceptable or unacceptable	Acceptable	Extremely acceptable	Don't know	Prefer not to say
1. ATM/bank transactions	1	2	3	4	5	98	99
2. Matching images on social media	1	2	3	4	5	98	99
3. Airport security processing	1	2	3	4	5	98	99
4. Logging onto mobile phones	1	2	3	4	5	98	99
5. Logging onto computers	1	2	3	4	5	98	99
6. Logging onto government websites	1	2	3	4	5	98	99
7. Applying for evidence of identity documents (e.g. driver's licence)	1	2	3	4	5	98	99
8. Access to buildings	1	2	3	4	5	98	99
9. Detecting criminals by the police	1	2	3	4	5	98	99
10. Detecting terrorists by government authorities	1	2	3	4	5	98	99
11. Public surveillance by law enforcement for crime prevention	1	2	3	4	5	98	99
12. Managing personal health profiles (e.g. vaccinations, allergies, etc.)	1	2	3	4	5	98	99

Q7_A2. How concerned are you about each of the following issues in connection with biometric technologies (e.g. voice, fingerprint, face or iris recognition)?

	Not at all concerned	Not very concerned	Neither concerned nor not concerned	Somewhat concerned	Extremely concerned	Not applicable	Don't know	Prefer not to say
1. Protection of my privacy	1	2	3	4	5	96	98	99
2. Cost involved	1	2	3	4	5	96	98	99
3. Risks of losing my biometric data	1	2	3	4	5	96	98	99
4. Risks of losing my money	1	2	3	4	5	96	98	99
5. Complicated enrolment	1	2	3	4	5	96	98	99
6. Fixing problems if systems fail	1	2	3	4	5	96	98	99
7. Physical injury to myself through using biometrics	1	2	3	4	5	96	98	99
8. My biometric data being compromised	1	2	3	4	5	96	98	99
9. Someone using my biometric data to pretend to be me	1	2	3	4	5	96	98	99
10. Police action against me by mistake through biometric matching	1	2	3	4	5	96	98	99
11. Forcing me to use biometrics without my free consent	1	2	3	4	5	96	98	99
12. Having to use multiple different systems for different purposes	1	2	3	4	5	96	98	99
13. Government surveillance of me	1	2	3	4	5	96	98	99

Q8_A2. How acceptable is it for government to use biometric technologies for the following purposes?

	Extremely unacceptable	Unacceptable	Neither acceptable or unacceptable	Acceptable	Extremely acceptable	Don't know	Prefer not to say
1. Identity verification (general)	1	2	3	4	5	98	99
2. Public surveillance	1	2	3	4	5	98	99
3. Border control	1	2	3	4	5	98	99
4. Passport registration	1	2	3	4	5	98	99
5. Issuing drivers licences	1	2	3	4	5	98	99
6. Australian Tax Office account access/ filing tax returns	1	2	3	4	5	98	99
7. Law enforcement	1	2	3	4	5	98	99
8. Education services	1	2	3	4	5	98	99
9. National security	1	2	3	4	5	98	99
10. Medicare account access/ verification	1	2	3	4	5	98	99
11. Centrelink account access/ verification	1	2	3	4	5	98	99
12. Managing personal health profiles (e.g. vaccinations, allergies, etc.)	1	2	3	4	5	98	99

Q9_A2. Are you currently registered with a digital identification service/ app such as myGovID, Digital iD or another service where you have been required to verify your identity and biometric information?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q10_A2. How willing are you to use a digital identification service/ app secured by your biometric information (e.g. fingerprint, facial recognition, voice recognition, iris scan, etc.)?

1. Extremely unwilling
2. Unwilling
3. Neither willing or unwilling
4. Willing
5. Extremely willing
98. Don't know
99. Prefer not to say

Q11_A2. How acceptable do you think using a digital identification service/ app would be for the following?

	Extremely unacceptable	Unacceptable	Neither acceptable or unacceptable	Acceptable	Extremely acceptable	Not Applicable	Don't know	Prefer not to say
1. ATM/bank transactions	1	2	3	4	5	96	98	99
2. Digital passport mobile app (replaces physical passport book)	1	2	3	4	5	96	98	99
3. Airport security processing	1	2	3	4	5	96	98	99
4. Logging onto mobile phones	1	2	3	4	5	96	98	99
5. Logging onto computers	1	2	3	4	5	96	98	99
6. Logging onto government websites	1	2	3	4	5	96	98	99
7. Applying for/ renewing a driver's licence	1	2	3	4	5	96	98	99
8. Access to buildings	1	2	3	4	5	96	98	99

	Extremely unacceptable	Unacceptable	Neither acceptable or unacceptable	Acceptable	Extremely acceptable	Not Applicable	Don't know	Prefer not to say
9. Accessing education services	1	2	3	4	5	96	98	99
10. Accessing health services	1	2	3	4	5	96	98	99
11. Rental applications	1	2	3	4	5	96	98	99

Addendum 3: Ransomware Quantitative Addendum

Earlier in this survey, you said that in the last 12 months something happened to your device and you received instructions on your device for paying a ransom. This is an indicator of ransomware. We would now like to ask you some more questions about this incident or incidents.

We encourage you to answer these questions honestly. We have no way of identifying you from the survey responses. To protect your identity, at no time will your name, address, birth date, or any other information that may identify you be made available to the Australian Institute of Criminology. If you feel uncomfortable about answering any questions you can choose not to respond.

Q1_A3. How many times in the last 12 months did you receive instructions on your device for paying a ransom?

1. Once
2. Twice
3. Three times
4. Four times
5. Five times or more
98. Don't know
99. Prefer not to say

For the rest of this survey we ask you to focus on the most recent incident of ransomware you experienced.

Q2_A3. On which device did the instructions appear?

Select all that apply

1. On my phone
2. On my computer or laptop
3. On my tablet
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q3_A3. In which format did the instructions appear on your device?

Select all that apply

1. The message was in an email, text or private online chat
2. The message appeared as a pop-up notification on my device
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q4_A3. Did any of the following things happen to your device or systems around the same time?

Select all that apply

1. The device(s) lost functionality (e.g. it was locked, inaccessible or password protected)
2. Data or files on the device(s) were altered, removed or locked (e.g. inaccessible or password protected)
3. Software or a virus was installed on my device(s)
4. My servers, service or networks were disrupted (e.g. slowed down, lost connection, had outages)
96. None of the above
98. Don't know
99. Prefer not to say

Q5_A3. Do you know how your device or system was compromised?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q6_A3. In a few sentences, please describe how your device or system was compromised.

Please do not include any identifying information such as person's names, group names or hyperlinks.

Q7_A3. Before your device was impacted, do you remember clicking on any suspicious links, pop-ups, buttons, files or attachments?

This could be immediately beforehand, or within the days and weeks beforehand.

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q8_A3. Where did you click on this suspicious link, pop-up, button, file or attachment?

Select all that apply

1. In an email
2. On a webpage
3. In a SMS text
4. On a private chat platform
5. On a social media post
97. Other (Please Specify)
98. Don't know
99. Prefer not to say

Q9_A3. Was this email account a personal email or work/ business email?

1. Work or business
2. Personal
97. Other (Please Specify)
98. Don't know
99. Prefer not to say

Q10_A3. Which devices or systems lost functionality or connection, had a virus, or had files or data blocked?

Select all that apply

1. Smart phone (e.g. iPhone, Samsung Galaxy)
2. Laptop computer
3. Tablet or iPad
4. Desktop computer
5. 'Smart' wearables (e. g. Fitbit, smart watch)
6. 'Smart' TV
7. A gaming console connected to the internet or your TV (e.g. Playstation, Xbox)
8. 'Smart' security / alarm / intercom entry system
9. Modem / Router
10. Smart home devices (e.g. Google home, Amazon Home Family)
11. Home automation (e.g. appliances, lights, etc)
12. Servers or networks
13. Webpages / websites
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q11_A3. Was the impacted device (or any of the impacted devices) issued to you from your workplace?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q12_A3. Do you use the impacted device(s) for work-related or business-related tasks?

1. Yes
2. No
98. Don’t know
99. Prefer not to say

Q13_A3. Were the data or files impacted by the incident owned or used by your business or place of employment?

1. Yes
2. No
98. Don’t know
99. Prefer not to say

Q14_A3. Your answers indicate that the ransomware attack occurred within the context of your employment.

Are you employed by a business with a turnover of more than $10 million per annum?

1. Yes
2. No
98. Don’t know
99. Prefer not to say

Q15_A3. Did the ransomware or virus spread to other devices, systems or email accounts in your workplace?

1. Yes
2. No
98. Don’t know
99. Prefer not to say

Q16_A3. Did the incident impact critical infrastructure used to provide essential goods and services, and disrupt the availability of those goods or services?

1. Yes
2. No
98. Don’t know
99. Prefer not to say

Q17_A3. Did the ransom message threaten to sell or share the data (such as datasets, files, photos, videos, etc)?

1. Yes
2. No
98. Don’t know
99. Prefer not to say

Q18_A3. Did the ransom message give you a time limit within which to pay?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q19_A3. What was the time limit?

(00-60) Minutes:_____
(1-100) Hours:_____
(1-365) Days:_____
(1-100) Months: _____

Q20_A3. How much did the ransom message demand?

This can include payments in money, cryptocurrency and/or gift cards. For cryptocurrency and gift cards, report the AU$ value of the cryptocurrency or gift cards at the time of the incident.

If you were demanded another currency, please provide your answers in approximate AU$ value at the time of the incident.

1. Money (specify) AU$_____
2. Cryptocurrency (specify) AU$_____
3. Gift cards (specify) AU$_____
4. TOTAL AU$_____
98. Don't know
99. Prefer not to say

Q21_A3. Did you pay or attempt to pay the ransom?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Q22_A3. Select the reasons why you decided to pay the ransom

Select all that apply

1. I could afford the ransom
2. I believed I would get access back to my files or data
3. I believed my files or data would not be leaked or sold on
4. Based on the advice I received
5. I did not have insurance
6. I did not have backups
7. I did not know what else to do
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q23_A3. Select the reasons why you decided to not pay the ransom

Select all that apply

1. I could not afford the ransom
2. I did not believe the ransom demands were credible
3. I believed I would not get access back to my files or data anyway
4. I believed my files or data would be leaked or sold on anyway
5. Based on the advice I received
6. I had insurance
7. I had backups
8. I was able to get a decryption key
97. Other (Please Specify) _____
98. Don't know
99. Prefer not to say

Q24_A3. What happened following your decision to pay or not pay? E.g. Did the offender carry out their threats? Did you receive any additional communications?

Q25_A3. Did you visit or contact any of the following organisations to gain information on how to deal with the attack?

1. Visited the Australian Cyber Security Centre ReportCyber website (Cyber.gov.au)
2. Visited the Scamwatch website
3. Called the Australian Cyber Security Centre Hotline 1300 CYBER1
4. Visited the No More Ransom website (https://www.nomoreransom.org/)
96. None of the above
97. Gained information from another source (Please Specify)
98. Don't know
99. Prefer not to say

Q26_A3. Did you take any of the following actions in response to the attack?

1. Disconnecting the infected device(s) from the internet or Wifi
2. Disconnecting the infected device(s) from other networks and external storage devices
3. Removing network and data cables
4. Holding the power button until the device shut down
5. Using Task Manager on Microsoft Windows to 'force quit' suspicious or unwanted activity on my device(s)
6. Running an antivirus software or malware scanner to find and remove any malware, including ransomware.
7. Taking a record of the incident details (e.g. the ransom note, weblink, email or Bitcoin address)
8. Contacting an IT professional to help you with backing up my data, resetting my devices and restoring my files.
96. None of the above
98. Don't know
99. Prefer not to say

Q27_A3. Did you or your colleagues take any of the following actions in response to the attack?

Select all that apply

1. Checked whether we had mandatory reporting obligations
2. Notified customers or suppliers of the incident (e.g. that their financial or personal information may have been compromised)
3. Reported the incident to police
4. Reported the incident to the Australian Cyber Security Centre
5. Reported the incident to the Office of the Australian Information Commissioner
96. None of the above
98. Don't know
99. Prefer not to say

Q28_A3. Once you became aware of the incident, how many hours did it take you to report to the Australian Cyber Security Centre?

_____

98. Don't know
99. Prefer not to say

Q29_A3. Were you able to do any of the following?

Select all that apply

1. Back up encrypted files
2. Decrypt encrypted files
3. Reset my devices
4. Restore my files
5. Halt the transaction of money or currency to the ransomware attackers
6. Have my money or currency reimbursed
96. None of the above
98. Don't know
99. Prefer not to say

Q30_A3. Before the most recent incident, have you ever paid the ransom in a ransomware attack before?

1. Yes
2. No
98. Don't know
99. Prefer not to say

Section I: Participation in future research

We would like to invite you to participate in some follow-up research. You will be contacted by Roy Morgan in around 12 months to participate in another cybercrime survey. You may also receive some further information about cybercrime risks and responses. This information and advice would be sent via email and/or SMS text messages. You will not receive any phone calls.

Roy Morgan will contact you on behalf of the Australian Institute of Criminology (AIC) in a way that continues to protect your data and privacy.

This is completely voluntary – you do not have to participate if you do not want to, and you may withdraw your participation at any time. Not everyone who agrees to participate in another survey or to receive information about cybercrime risks and responses will be contacted by Roy Morgan. Participation in this research will include an incentive if you are contacted by Roy Morgan and you decide to participate.

I1. Do you agree to be contacted by Roy Morgan about participating in another cybercrime survey in around 12 months?

1. Yes
2. No

I2. Do you agree to being added to a subscriber list to receive further information about cybercrime risks and responses?

1. Yes
2. No

Please confirm your contact details so we can contact you over the next year. You may use a pseudonym rather than your actual name if you would prefer.

Please only enter a mobile phone number, including the area code "04".

I3_1. Title (MR, MRS, MISS, MS, DR): _____

I3_2. First name (or first initial): _____

I3_3. Last name (or first initial): _____

I3_4. Mobile number: _____

I3_5. Email: _____

I3_99. I do not wish to give my details / I do not want to participate

CONFIRM PHONE

I4. Are these details correct?

1. Yes
2. No

Survey end page

Thank you for your time. If you feel distressed or upset about anything, please contact one of the below listed services:

- Lifeline Australia anytime: call 13 11 14, or visit the website: https://www.lifeline.org.au
- Beyond Blue: call 1300 22 4636, or visit the website: https://www.beyondblue.org.au/
- SANE Australia: call 1800 18 7263, or visit the website: https://www.sane.org/counselling-support/sane-support-services
- 1800 RESPECT: call 1800 737 732, or visit the website: https://www.1800respect.org.au/

The following websites are available for information on cybersafety and how to report cybercrime:

- Report Cyber: https://www.cyber.gov.au/acsc/report/are-you-a-victim-of-cybercrime
- eSafety Commissioner: https://www.esafety.gov.au/
- Australian Cyber Security Centre: https://www.cyber.gov.au/

Finally, IDCARE (https://www.idcare.org/) is Australia's national identify and cyber support service, and offers assistance to people who have experienced data breaches, ransomware, scams, identity theft or who have other cyber security concerns.