Australian Government
Australian Institute of Criminology

AIC reports
Statistical Report 53

Cybercrime in Australia 2024

Isabella Voce
Anthony Morgan

ISSN 2206-7930 (Online)
ISBN 978 1 922877 91 8 (Online)
https://doi.org/10.52922/sr77918

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6268 7166
Email: front.desk@aic.gov.au
Website: www.aic.gov.au

Please note: Minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

Disclaimer: This research report does not necessarily reflect the policy position of the Australian Government.

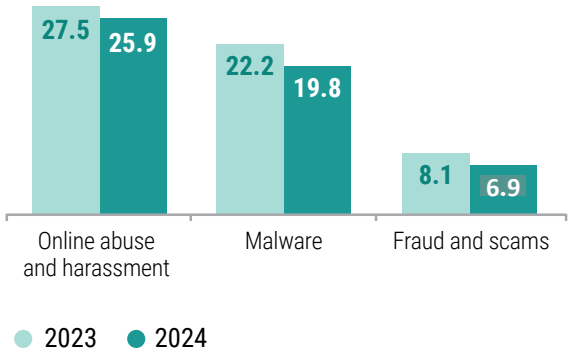
General editor: Dr Rick Brown, Deputy Director, Australian Institute of Criminology

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at www.aic.gov.au

WHAT CHANGED FROM 2023 TO 2024?

RESPONDENTS WERE LESS LIKELY TO BE A VICTIM OF ONLINE ABUSE AND HARASSMENT, MALWARE AND FRAUD AND SCAMS



The proportion of victims who experienced multiple types of cybercrime decreased from

43% to 39%

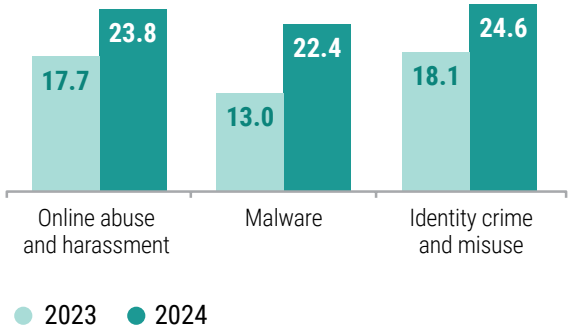
26% fewer respondents

said their information had been exposed in a data breach in 2024

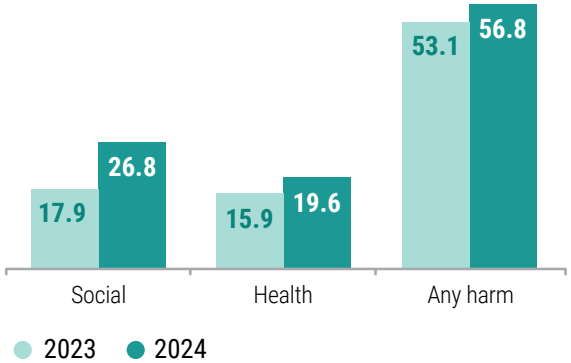
RESPONDENTS WERE LESS LIKELY TO USE IMPORTANT ONLINE SAFETY BEHAVIOURS

- Checking and changing social media privacy settings
- Installing or using antivirus
- Using parental controls (among parents)
- Avoiding clicking on links from unknown senders
- Independently contacting companies when unsure about text or email

SMALL-TO-MEDIUM BUSINESS OWNERS WERE MORE LIKELY TO SEEK HELP FROM POLICE OR REPORTCYBER



INCREASES IN THE OVERALL HARM TO VICTIMS WERE DRIVEN BY INCREASED SOCIAL AND HEALTH IMPACTS



While there was no change in average financial losses after recoveries, the proportion of identity crime and misuse victims who recovered money increased from

75% to 82%

Contents

viii Acknowledgements

ix Acronyms

x Abstract

xi Summary

xi Victimisation decreased for some cybercrimes but remains high overall

xiii Vulnerable sections of the community continue to be over-represented as victims

xv Help-seeking among victims has increased, but cybercrime remains significantly under-reported

xvi Health and social harms were the most common, but financial losses and impacts on small to medium businesses changed little

1 Introduction

1 Australian Cybercrime Survey

2 What has changed this year?

4 Method

- 4 Survey design
- 4 Recruitment, sampling and weighting
- 5 Sample characteristics
- 12 Analysis
- 13 Limitations

16 Victimisation

17 Online abuse and harassment

20 Malware

22 Identity crime and misuse

24 Fraud and scams

29 Changes in victimisation

31 Poly-victimisation

33 Victim characteristics

37 Changes in victimisation among select groups of respondents

39 Digital literacy and online safety strategies

39 Digital literacy

43 Online safety strategies

47 Help-seeking by victims following the most recent incident

47 Sources of help, advice or support

53 Seeking help and reporting to police or to ReportCyber

56 Official reporting to police and ReportCyber among select groups of respondents

58 Changes in help-seeking behaviour

59 Reasons for official reporting to police or ReportCyber

60 Outcomes of official reports to police or ReportCyber

63 Time between cybercrime incidents and official reporting

65 Reasons for not reporting to police or ReportCyber

68 Impacts of victimisation
68 Financial losses
74 Changes in financial losses
76 Impacts on individual victims
80 Impacts on small to medium businesses
82 Changes in harm to individuals and small businesses
85 References
88 Appendix: Survey design, sampling and weighting
88 Key definitions
88 Cybercrime
88 Cyber-dependent crime
88 Cyber-enabled crime
89 Cybersecurity
89 Fraud and scams
89 Identity crime and misuse
89 Malware
89 Online abuse and harassment
90 Survey design
90 Core survey
91 Research ethics
91 Sampling and weighting
97 Comparison between 2023 and 2024 samples

Boxes

3 Box 1: What is covered by this report?
28 Box 2: One in three scams was initiated from a phishing message
31 Box 3: Fewer respondents were notified of a data breach in 2024 than in 2023
32 Box 4: A decline in repeat victimisation?
46 Box 5: Are Australian computer users becoming less vigilant online?
55 Box 6: Better estimating the extent of unreported cybercrime
65 Box 7: Malware reporting, outcomes and satisfaction

Figures

6 Figure 1: Respondents by usual place of residence
16 Figure 2: Prevalence of cybercrime victimisation, lifetime and past year
20 Figure 3: Relationship between victim and offender in the most recent online abuse and harassment incident
29 Figure 4: Adjusted estimates of past-year victimisation for major categories of cybercrime, 2023 and 2024
32 Figure 5: Overlap of cybercrimes experienced by respondents
33 Figure 6: Cybercrime victimisation, by crime type and age group
38 Figure 7: Changes in victimisation from 2023 to 2024, for SME owners
40 Figure 8: Self-rated knowledge of technology, 2023 and 2024
40 Figure 9: Self-rated ability to use technology, 2023 and 2024
48 Figure 10: Help-seeking among online abuse and harassment victims following the most recent incident

49 Figure 11: Help-seeking among malware victims following the most recent incident
50 Figure 12: Help-seeking among identity crime and misuse victims following the most recent incident
51 Figure 13: Help-seeking among fraud and scam victims following the most recent incident
52 Figure 14: Number of sources of help, advice and support among victims who sought help following the most recent incident
54 Figure 15: Help-seeking following the most recent incident, by crime type
58 Figure 16: Help-seeking from police or ReportCyber following the most recent incident, 2023 and 2024
59 Figure 17: Help-seeking from police or ReportCyber among small to medium business owners, operators and managers following the most recent incident, 2023 and 2024
60 Figure 18: Reasons for making an official report to police or ReportCyber following the most recent incident, by crime type
61 Figure 19: Outcomes of reporting among victims who reported the most recent incident to police or ReportCyber, by crime type
62 Figure 20: Satisfaction with the outcome among victims who made an official report to police or ReportCyber, by crime type
63 Figure 21: Length of time taken to submit a report to police following the most recent incident, by crime type
64 Figure 22: Length of time taken to submit a report to ReportCyber following the most recent incident, by crime type
69 Figure 23: Prevalence of victims who recovered any money following most recent incident
70 Figure 24: The average proportion of money recovered among people who lost money directly and who recovered money
72 Figure 25: Financial losses after recoveries for most recent incident
73 Figure 26: Median financial losses before recoveries for most recent incident among victims who lost any money, by whether respondent sought help, advice or support from police or ReportCyber
74 Figure 27: Mean financial losses after recoveries for most recent incident, 2023 to 2024
75 Figure 28: Proportion of victims who said that they recovered any money following the most recent incident, 2023 and 2024
76 Figure 29: Harms from cybercrime among victims
77 Figure 30: Harms from cybercrime among victims, by number of crime types reported
78 Figure 31: Harms from cybercrime among victims, by crime type
81 Figure 32: Harms to business from cybercrime among victims who owned, operated or managed a small to medium business
83 Figure 33: Harms from cybercrime among victims, 2023 and 2024
84 Figure 34: Harms to business from cybercrime among victims who owned, operated or managed a small to medium business, 2023 and 2024

Tables

7 Table 1: Sociodemographic characteristics of respondents
9 Table 2: Education, employment and income of respondents
10 Table 3: Annual income of respondents in the previous financial year
11 Table 4: Online behaviour of respondents
17 Table 5: Incidents of online abuse and harassment
21 Table 6: Incidents of malware
23 Table 7: Incidents of identity crime and misuse
25 Table 8: Incidents of fraud and scams
30 Table 9: Adjusted estimates of past-year victimisation for subcategories of cybercrime, 2023 and 2024
35 Table 10: Cybercrime victimisation by crime type and sociodemographic characteristics
36 Table 11: Cybercrime victimisation by crime type and respondent education, employment and income
37 Table 12: Cybercrime victimisation by crime type and respondent age and gender, 2023 and 2024
39 Table 13: Mean number of hours spent online for personal and work-related use, 2023 and 2024
42 Table 14: Daily or weekly engagement in online activities, 2023 and 2024
44 Table 15: Prevalence of online safety measures, 2023 and 2024
45 Table 16: Prevalence of unsafe online behaviours, 2023 and 2024
57 Table 17: Respondents who made an official report to police or ReportCyber, by sociodemographic characteristics
66 Table 18: Reasons for not reporting to police or ReportCyber, by crime type
69 Table 19: Money lost, money spent on consequences and money recovered following most recent incident of cybercrime, by crime type
71 Table 20: Median financial losses for most recent incident among victims who lost any money, by payment method (range)
79 Table 21: Harms to individual cybercrime victims
81 Table 22: Harms to small business owners, operators and managers who were victims of cybercrime
93 Table A1: Invitation and completion rates, Roy Morgan Single Source panel
93 Table A2: Respondents by usual place of residence
94 Table A3: Respondents by usual place of residence
95 Table A4: Respondents by age
96 Table A5: Selected sociodemographic characteristics of respondents
97 Table A6: Sociodemographic characteristics of respondents, 2023 and 2024
99 Table A7: Education, employment and income of respondents, 2023 and 2024
100 Table A8: Annual income of respondents in the previous financial year, 2023 and 2024
100 Table A9: Online behaviour of respondents, 2023 and 2024

Acknowledgements

We acknowledge the important work of Chris Owen, Gladys Lima and colleagues from Roy Morgan in conducting the survey.

The Australian Cybercrime Survey was developed in consultation with representatives from the Attorney-General's Department, Australian Federal Police, Australian Cyber Security Centre, Department of Home Affairs, eSafety Commissioner, National Anti-Scam Centre and state and territory law enforcement agencies through the Helios Joint Management Group. We are grateful for their support and assistance.

Finally, we acknowledge the thousands of respondents who completed the survey and provided information on their experiences of cybercrime.

Acronyms

ABS	Australian Bureau of Statistics
ACS	Australian Cybercrime Survey
ACSC	Australian Cyber Security Centre
AIC	Australian Institute of Criminology
ASD	Australian Signals Directorate
ICT	information and communication technology
LGB+	lesbian, gay, bisexual or other non-heterosexual identity
SME	small to medium enterprise

Abstract

This is the second report in the Cybercrime in Australia series, which describes cybercrime victimisation, help-seeking and harms among Australian computer users. This year, 10,335 online Australians participated in the Australian Cybercrime Survey. Overall, we found that rates of victimisation remain high, formal help-seeking remains low, and a large proportion of victims are negatively impacted by cybercrime.

Twenty-seven percent of respondents had been a victim of online abuse and harassment in the 12 months prior to the survey, 20.6 percent had been a victim of malware, 21.9 percent had been a victim of identity crime and misuse, and 9.5 percent had been a victim of fraud and scams. The prevalence of online abuse and harassment, malware and fraud and scams was lower among 2024 respondents than in the 2023 survey. Poly-victimisation was also lower this year, and we observed a significant decrease in data breaches.

As with last year, certain sections of the community were more likely than others to fall victim. A smaller proportion of respondents who owned or operated a small to medium business were victims of malware and fraud and scams in 2024 than in 2023. However, respondents were less likely in 2024 than in 2023 to say they were using various online safety strategies, and there was little change in the prevalence of high-risk online behaviours.

While most cybercrime continues to go unreported, a higher proportion of respondents sought help from police or ReportCyber for certain types of cybercrime, particularly among small to medium business owners and operators. Victims were more likely to recover money from identity crime and misuse incidents in 2024 than in 2023. A higher proportion of victims reported being negatively impacted by cybercrime in 2024, particularly for social and health related harms.

Summary

This is the second report in the Cybercrime in Australia series, which provides important data on cybercrime victimisation, help-seeking and harms among Australian computer users. Between July and August 2024, 10,335 computer users were recruited from online panels to participate in the Australian Cybercrime Survey (ACS). The survey measures four broad categories of cybercrime: online abuse and harassment, malware attacks, identity crime and misuse, and fraud and scams.

Victimisation decreased for some cybercrimes but remains high overall

Almost two-thirds of respondents (63.9%) said they had been a victim of at least one type of cybercrime measured by the survey during their lifetime, and nearly half (47.4%) had been the victim of a cybercrime in the 12 months prior to the survey. Online abuse and harassment was the most common type of cybercrime reported. In the 12 months prior to the survey, 26.8 percent of respondents had been a victim of online abuse and harassment, 20.6 percent had been a victim of malware, 21.9 percent had been a victim of identity crime and misuse, and 9.5 percent had been a victim of fraud and scams. One-quarter of respondents had experienced a data breach (25.0%).

The most common forms of online abuse and harassment that victims experienced in the past year were being sent unsolicited sexually explicit messages, images or videos (7.6%); someone hacking into their social media or network account (4.8%); and someone sending or posting mean or hurtful messages via electronic communication that made them feel hurt, embarrassed or unsafe (4.2%). When asked about the most recent incident, nearly half of these victims said it involved a stranger online (47.0%). Fifteen percent of incidents of online abuse and harassment were domestic or family violence related, meaning they involved a current or former intimate partner or a family member (15.1%). The victim did not know who the perpetrator was in around one in 10 incidents (10.1%).

The most common symptom of malware that victims experienced in the past year were ads appearing on their device (5.8%), their device slowing down and acting strangely (4.9%) and people telling them that they had been sending suspicious messages and links over social media or email (2.8%). Overall, 4.9 percent of respondents had in the 12 months prior to the survey received a ransom message on their device demanding payment. 'Pure ransomware' victimisation—defined as having a virus or disruption to devices, systems or data, as well as receiving a ransom message—impacted 2.4 percent of respondents. When limited to incidents involving signs of a malware attack as well as a ransom message, 2.4 percent of respondents had experienced ransomware victimisation in the 12 months prior to the survey. An additional 2.6 percent of respondents received a ransom message indicating their data was stolen and they had to pay to prevent it being sold or leaked online.

The most common incidents of identity crime and misuse that respondents experienced in the past year were suspicious transactions appearing in their bank statements or accounts, credit card or credit report (10.1%); and receiving calls from debt collectors asking about unpaid bills they did not recognise (4.4%).

The most common type of fraud and scams that respondents experienced in the 12 months prior to the survey was paying money or providing sensitive information when they were trying to buy a product or service from a fake or fraudulent seller online (2.3%), followed by paying money or providing sensitive information when they were trying to sell a product or service to a fake or fraudulent buyer online (0.6%), and paying a fake invoice or bill for some other product or service that they did not receive (0.6%).

It was common for cybercrime victims to have experienced multiple incidents, indicators or symptoms of the same type of cybercrime in the 12 months prior to the survey. It was also common for cybercrime victims to report having experienced multiple types of cybercrime. While 27.4 percent of respondents were a victim of one type of cybercrime, 20.0 percent of respondents (42.1% of all victims) were victims of two or more types of cybercrime in the 12 months prior to the survey.

We compared the prevalence of cybercrime among respondents to the 2023 and 2024 ACS, limiting our analysis to comparable crimes and adjusting for differences between the two samples. The prevalence of online abuse and harassment (27.5% in 2023 vs 25.9% in 2024), malware (22.2% vs 19.8%) and fraud and scams (8.1% vs 6.9%) was lower among 2024 respondents than in the 2023 survey. The prevalence of identity crime and misuse had not changed. There were differences in several main categories of cybercrime. Most notably, there were decreases in the proportion of victims who received unsolicited sexual content (from 10.0% to 7.5%), who experienced suspected malware that was not related to ransomware (from 19.4% to 16.8%), and who experienced phishing scams (from 1.6% to 0.9%). The only main category of cybercrime where there was a higher proportion of victims in 2024 was identity crime and misuse that was not related to the compromise of financial accounts (from 3.8% to 4.4%). The prevalence of poly-victimisation was also lower in 2023 than it was in 2024 (43.2% of victims in 2023 vs 39.4% of victims in 2024). Fewer respondents said their information had been exposed in a data breach in 2024 (24.9%) than in 2023 (33.7%).

The prevalence of online abuse and harassment, malware and fraud and scams was lower among 2024 respondents than in the 2023 survey. Poly-victimisation was also lower in 2024, and we observed a significant decrease in data breaches.

Vulnerable sections of the community continue to be over-represented as victims

Cybercrime victimisation is not evenly distributed, with certain sections of the community more likely to be a victim, and certain online activities associated with a higher likelihood of victimisation.

- Younger respondents were consistently more likely than their older counterparts to report having been the victims of online abuse and harassment, malware and fraud and scams.
- Men were more likely than women to be the victim of malware and online abuse and harassment.
- First Nations respondents had a significantly higher prevalence of victimisation across all types of cybercrime.
- Respondents who identified as lesbian, gay, bisexual or another non-heterosexual identity (LGB+) were significantly more likely than heterosexual respondents to have been a victim of online abuse and harassment and fraud and scams.
- Compared with other respondents, respondents who mainly spoke a language other than English at home were more likely to have been a victim of online abuse and harassment, malware, and fraud and scams.
- Respondents with a restrictive health condition were more likely than other respondents to have been a victim of all types of cybercrime.
- Unemployed respondents were the most likely to experience online abuse and harassment and malware, while employed respondents were the most likely to have been a victim of identity crime and misuse.
- Small to medium business owners, operators and managers experienced significantly higher rates of all types of cybercrime than other respondents.
- Respondents who worked for a large business or company were less likely than those who worked for other companies or organisations to have been a victim of all types of cybercrime.
- Respondents with incomes between $120,001 and $180,000 had the highest rates of malware attacks, while respondents with incomes between $45,001 and $120,000 had the lowest.

When we compared results between the 2024 and 2023 surveys, we observed a decline in the proportion of small to medium business owners, operators and managers who said they had been the victim of malware (from 30.8% to 27.2%) and fraud and scams (from 14.6% to 11.9%). There were also declines in victimisation among different age groups, men and women, although it varied according to the type of cybercrime.

Respondents who owned or operated a small to medium business were less likely to be a victim of malware and fraud and scams in 2024 than they were in 2023.

There were some changes in online behaviour, but online safety strategies leave room for improvement

Many respondents are not taking simple but important steps to improve their online safety. Around half used different passwords for secure online accounts (50.7%) or used multifactor or two-factor authentication for personal accounts (57.8%). A minority installed or used spam-filtering software (20.5%), installed or used antivirus software or firewalls on their devices (39.3%) or regularly updated the security software on their device when prompted by their device's security system (38.6%). Moreover, the proportion of respondents who engaged in several of these protective behaviours declined from 2023 to 2024.

There may be several reasons for this. Respondents were more confident in their knowledge of technology in 2024 than in 2023, which may lead them to place less importance on protective behaviours. The frequent use of social media also significantly declined from 2023 to 2024, which could explain why respondents are not checking or adjusting their social media profiles. The decline in the proportion of people who avoided clicking on links or who independently contacted a company may relate to them receiving fewer scam approaches due to government and industry measures such as telecommunications companies blocking scam calls and text messages (Australian Communications and Media Authority 2025).

A reduced proportion of respondents reported that they accepted friend requests from people online who they had not met in person (from 12.3% to 11.2%) and that they accepted cookies from websites that saved their browsing information (from 46.1% to 42.8%). The prevalence of other higher risk behaviours, such as using freely available public wi-fi for financial transactions, sharing passwords and opening emails from unknown senders, was unchanged.

While respondents rated their knowledge of technology and ability to use technology higher in 2024 than respondents did in 2023, they were less likely to use a range of common online safety strategies. There was little change in the use of higher-risk online behaviours that are associated with an increased likelihood of being a victim of cybercrime.

Help-seeking among victims has increased, but cybercrime remains significantly under-reported

Respondents who had been a victim of cybercrime in the 12 months prior to the survey were asked whether they had sought help, advice or support from a range of sources following the most recent incident. For most victims, the most common source of help, support or advice for victims was family and friends. Identity crime and misuse victims most often sought assistance from a financial institution, followed closely by family and friends. Formal help-seeking was higher among identity crime and misuse victims (70.9%) and fraud and scam victims (66.5%) than online abuse and harassment victims (50.0%) and malware victims (42.5%).

Fraud and scam victims were the most likely to seek help, advice or support from the police or ReportCyber (20.7%), followed by online abuse and harassment victims (17.4%), identity crime victims (15.5%) and malware victims (13.1%). The proportion of victims who sought help, advice or support from police or ReportCyber was compared for 2023 and 2024, but was limited to those incidents types that were measured in both surveys. A higher proportion of victims sought help from police or ReportCyber for online abuse and harassment (15.2% in 2023 vs 17.7% in 2024) and for malware attacks (7.9% in 2023 vs 13.3% in 2024). There was also a higher proportion of small to medium business owners who sought help from police or ReportCyber for online abuse and harassment (from 17.9% to 23.8%), malware attacks (from 13.5% to 22.6%) and identity crime and misuse (from 18.2% to 24.3%).

Victims who sought help from police or ReportCyber were also asked if they had made an official report. Across all cybercrime types, around one in 10 victims made an official report, with the highest rate occurring among fraud and scam victims (12.5%). The likelihood of making an official report to police or ReportCyber for particular cybercrime types varied according to the characteristics of the victim, with younger respondents and small to medium business owners, operators and managers being more likely to make an official report for all types of cybercrime.

Most victims made an official report to police or ReportCyber in order to prevent the crime happening to them again or to someone else; however, half of the identity crime and misuse victims (51.7%) and malware victims (50.1%) who made a report did so because they wanted to get their money back or be compensated for loss or damage.

Among those who sought help from police or ReportCyber, between 18.6 and 39.1 percent either heard nothing, did not know what had happened, or were told nothing could be done. Overall, 15.6 percent of online abuse and harassment victims, 21.4 percent of malware victims, 7.5 percent of identity crime victims and 10.6 percent of fraud or scam victims were told by the police that someone had been arrested, charged or prosecuted. Up to 61.3 percent of victims who sought help were satisfied with the outcome and up to 35.7 percent were dissatisfied with the outcome. The most common reasons that victims gave for not reporting to police or ReportCyber were that they felt they could deal with it themselves or they did not regard the incident as a serious offence. Other common reasons related to their awareness of reporting options—they did not know reporting to the police or ReportCyber was an option, did not think the police or ReportCyber would be able to do anything, or did not know how or where to report the matter.

Victims were more likely to have sought help, advice or support from police or ReportCyber following the most recent incident of online abuse and harassment and malware in 2024 than they were in 2023. This was especially true for small to medium business owners, operators and managers, who were also more likely to seek help following identity crime and misuse.

Health and social harms were the most common, but financial losses and impacts on small to medium businesses changed little

Not all victims reported losing money in the most recent incident of cybercrime. Fraud and scam victims were the most likely to report financial losses (29.8%), followed by identity crime victims (28.7%). Direct financial losses were relatively uncommon for malware victims (7.6%) and online abuse and harassment victims (3.4%). The proportion of victims who were able to recover money was lowest among victims of fraud and scams (38.4%) and highest among victims of identity crime and misuse (82.0%). The average proportion of money lost that was recovered ranged from 29.3 percent for online abuse and harassment to 74.0 percent for identity crime and misuse victims.

Approximately one-quarter (27.8%) of online abuse and harassment victims, 19.6 percent of malware victims, 11.6 percent of identity crime victims and 16.5 percent of fraud and scam victims lost more than $1,000 in the most recent incident. Five percent of online abuse and harassment victims lost more than $10,000, along with 2.8 percent of fraud and scam victims, 3.5 percent of malware victims and 2.8 percent of identity crime victims. A small proportion of victims, including 1.2 percent of fraud and scam victims, lost more than $100,000 in the most recent incident. The majority of victims said they lost less than $1,000 in the most recent incident.

The proportion of victims who said that they recovered any money following the most recent incident of identity crime and misuse increased from 75.1 percent in 2023 to 82.0 percent in 2024. There were no statistically significant changes in the mean losses after recoveries for any of the four major categories of cybercrime.

To measure the wider harms associated with cybercrime victimisation, respondents were asked whether they had experienced various impacts as a consequence of having been a victim. Overall, 56.8 percent of cybercrime victims were negatively impacted in some way. This means an estimated 26.1 percent of all respondents were negatively impacted by cybercrime in the 12 months prior to the survey. Forty percent of victims reported practical impacts, 26.8 percent reported social impacts, 19.7 percent reported health-related harms, and 16.7 percent reported financial problems. Legal issues were comparatively rare (2.5%). Victims who experienced more than one type of cybercrime in the 12 months prior to the survey were much more likely than other victims to report experiencing harm. Victims were more likely to say they had been negatively impacted by cybercrime in 2024 (56.8%) than they were in 2023 (53.1%). This was largely due to increases in the prevalence of health impacts (from 15.9% to 19.6%) and social impacts (from 17.9% to 26.8%).

Forty-two percent of small to medium business owners, operators or managers who had been a cybercrime victim in the past year reported at least one impact on their business. This means an estimated 22.2 percent of all small to medium business owners, operators or managers who responded to the survey said cybercrime had impacted their business in some way in the last 12 months. These impacts include disruption to everyday business function (25.6%), additional business expenses (15.3%), harm to their reputation or revenue (12.8%), loss of information (12.8%), effects on staff (5.9%) and legal or regulatory ramifications (4.5%).

Cybercrime victims in the 2024 survey were more likely than their 2023 counterparts to say that they experienced harm resulting from their victimisation. This included an increase in the proportion of victims who said they experienced negative health or social impacts.

Introduction

New technologies are continually being introduced and advanced to bring opportunities for commerce, education, entertainment and leisure. This has also resulted in a significant change in the cybercriminal landscape, with new possibilities for perpetrators to extend their reach, evolve their methods and streamline their attacks. Cybercrime refers to crimes that target or are facilitated by digital devices, computer networks or other forms of information and communication technology (ICT; Australian Government 2022), and has evolved into a pervasive and widespread threat to Australia's government, industries and community. The number of reports made to ReportCyber—the national online cybercrime reporting system run by the Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC), which then forwards reports to the applicable law enforcement agency—has increased by at least 46 percent, from 59,806 reports in 2019–20 to over 87,400 reports in 2023–24 (ASD 2024, 2020). Critically, these reports are only the tip of the iceberg. Most cybercrime victimisation is not reported to police or to ReportCyber, meaning that official reports significantly underestimate the size of the problem (Voce & Morgan 2023a). It has therefore become imperative to collect data to assist in understanding and identifying emerging threats, which can inform the development of law enforcement strategies, prevention initiatives and policy and legislative amendments.

Australian Cybercrime Survey

In June 2023, the Australian Institute of Criminology (AIC) released the first report in our Cybercrime in Australia series. This series aims to provide high-quality and robust evidence on cybercrime victimisation, offending, financial losses and other harms, help-seeking behaviour and, importantly, changes over time. The Cybercrime in Australia series is based on the Australian Cybercrime Survey (ACS), an annual national survey of online Australians aged 18 years and over. The survey asks respondents about their experiences of four broad categories of cybercrime: online abuse and harassment, malware attacks, identity crime and misuse, and fraud and scams. Except for malware, these are crimes that can also occur offline. To be included in this report, the incident must have involved a digital device, computer network or other forms of ICT.

The previous report in this series, *Cybercrime in Australia 2023* (Voce & Morgan 2023), found that 47 percent of respondents had experienced at least one cybercrime in the 12 months prior to the survey, most commonly online abuse and harassment (27.0%), malware (21.8%) and identity crime and misuse (20.1%). Eight percent had been a victim of fraud and scams. Most cybercrime victimisation went unreported to police or to ReportCyber, with victim reporting rates ranging from eight percent for malware victims to 22 percent for fraud and scam victims. Satisfaction with the outcomes of these reports was mixed, and relatively few reports resulted in an offender being apprehended. Rates of help-seeking varied and were influenced by the perceived seriousness of cybercrime and knowledge of how and where to report it. The financial losses experienced by victims were wide ranging, with some victims reporting losing large sums of money but most reporting relatively small financial losses. Overall, 25 percent of all respondents had been negatively impacted by cybercrime in the 12 months prior to the survey, while 22 percent of respondents who owned or operated a small to medium business said their business was negatively impacted by cybercrime.

What has changed this year?

The modus operandi of cybercriminals is constantly evolving in response to both emerging opportunities and disruptive actions taken by authorities. For example, there have been cases of artificial intelligence generated deepfakes being used during video conference calls to convince employees to transfer company funds (Australian Signals Directorate 2024). The constantly changing methods of attack can make it difficult to capture information about the different cybercrimes that people may have fallen victim to. Therefore, while the ACS aims to measure changes in cybercrime trends across time, the survey must also be flexible and evolve over time as well. There are several new additions to the 2024 ACS. Respondents to the 2024 survey had the option to select and describe 'other' types of cybercrime in addition to the incidents listed within the broad cybercrime categories, as those lists can never be exhaustive.

In addition, since the release of the *Cybercrime in Australia 2023* report, the National Anti-Scam Centre was launched to bring together experts from government and the private sector to tackle harmful scams. As a part of this, the National Anti-Scam Centre has developed a typology of scams to classify those with common characteristics. In developing the 2024 version of the ASC, we have taken steps to expand and better align the subcategories of scams and fraud measured in the ASC with the National Anti-Scam Centre's typology.

This year's report includes a new section focused on respondents' online behaviour, digital literacy and online safety. Last year we were focused on the relationship between people's online behaviour and cybercrime victimisation. However, we have now firmly established that people who spend longer online, who engage in certain online activities, and who engage in unsafe behaviour online, are more likely to be victims of cybercrime. With this in mind, we have shifted our focus to measuring changes in online behaviour, digital literacy and online safety. This provides valuable contextual information that helps us better understand the patterns of victimisation we observe.

Finally, given our interest in measuring the rate at which cybercrime is reported to police and ReportCyber, and in measuring the 'dark figure' of unreported cybercrime that does not appear in the official statistics, we have changed the way we measure help-seeking. Specifically, the focus is now on whether victims have made an official report to police or ReportCyber, in addition to whether they have sought help, advice or support. We have also included several new options for respondents to choose when answering questions about the formal sources they sought help from.

Box 1: What is covered by this report?

The focus of this report is on cybercrime, rather than cybersecurity events, although the two are not mutually exclusive. The latter is defined by the ASD ACSC (2025: np) as 'an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security'. Cybersecurity victims tend to be governments and business, and the target is usually a computer network, software or hardware. Some of these crimes, such as malware, are covered in this report. While the ACS measures crimes against individuals, some of these individuals may own or operate a business, and respondents could report cybercrime on a personal or work device.[a] Further, cybercrime experienced by individuals may be a direct consequence of a cybersecurity incident, such as where a data breach targeting an organisation leads to identity crime and misuse against customers.

The types of cybercrime covered by this report fall into four broad categories:

- **Online abuse and harassment**—online communication to or about an individual which may cause them emotional distress. This includes behaviours such as sending abusive messages, image-based abuse, setting up fake social media accounts to harass someone or stalking someone using a phone or other device.
- **Malware**—short for 'malicious software', this refers to software specifically developed and used to harm a computer system or network. It is used to gain access to a computer and can be used to steal confidential information.
- **Identity crime and misuse**—incidents where a person's personal information is obtained or used without their permission. A perpetrator could pretend to be the person, to carry out a business in their name without their permission, or for some other type of activity or transaction.
- **Fraud and scams**—intentionally deceiving someone to obtain money or something else of value, such as personal information.

Except for malware, these are crimes that can also occur offline. To be included in this report, the incident must have involved a digital device, computer network or other forms of ICT.

a: While the survey asks about cybercrime on a personal or work device, the respondent must themselves be the victim of the cybercrime (and not their business or employer). For a small business, they may be one and the same thing. Similarly, the survey does not distinguish between incidents that occur on a work or personal device, since for many small businesses (and, indeed, larger businesses) the same device may be used for both purposes

Method

Survey design

The ACS is a survey of online Australians aged 18 years and over that measures the prevalence and characteristics of cybercrime, risk factors, help-seeking behaviour, financial losses and other harms from victimisation. It captures both cyber-dependent and cyber-enabled crimes, including identity crime and misuse, malware, online fraud and scams and online abuse and harassment (see Box 1).

The questionnaire was developed by the AIC. It includes several components. First, the core survey questionnaire includes questions about respondent demographics, risk factors for victimisation, use of technology and devices, experiences of cybercrime victimisation and repeat victimisation, reporting behaviour and experiences, perpetrators of cybercrime, harms resulting from victimisation and preventative measures.

A bottom-up approach to measuring cybercrime victimisation was necessary because members of the public may not fully understand cybercrime terminology such as 'malware', 'ransomware' and 'spear phishing'. Each crime type was measured using questions about the various incidents or symptoms that would indicate a respondent has been a victim of a particular form of cybercrime. For example, in the case of malware, respondents were asked about specific signs that their computer was infected which they did not believe were the result of genuine device malfunction or aging, such as programs opening and closing automatically, files going missing or being replaced with odd file extensions, or people saying the respondent had been sending them suspicious messages and links over social media or email. This is likely to have elicited more accurate information than questions about whether they were a victim of malware. This approach was adopted for all four categories of cybercrime. Additional information about the survey design, as well as the approach to recruitment, sampling and weighting of data, is provided in the *Appendix*.

Recruitment, sampling and weighting

The survey was conducted by Roy Morgan between 11 July and 29 August 2024 using its Single Source panel and panels managed by PureProfile, Dynata and Octopus. The survey was sent to members of these online panels aged 18 years and over who had voluntarily joined the panel to receive incentives in exchange for completing surveys.

Proportional quota sampling, a non-probability sampling method, was used to ensure the sample was broadly reflective of the spread of people living in Australia. Quotas were based on the Australian adult population stratified by age, gender and usual place of residence, derived from Australian Bureau of Statistics (ABS) population data (ABS 2024a). Participants were first recruited from Roy Morgan's Single Source survey panel, which comprises individuals recruited through a rigorous clustersampled, face-to-face survey approach. The raw completion rate for invitations sent to this panel was 4.4 percent; however, there is no way of verifying how many of these invitations were received. Forty-nine percent of respondents who opened the invitation and who were eligible to participate in the research went on to complete the survey. Information on how to interpret these figures is included in the *Appendix*.

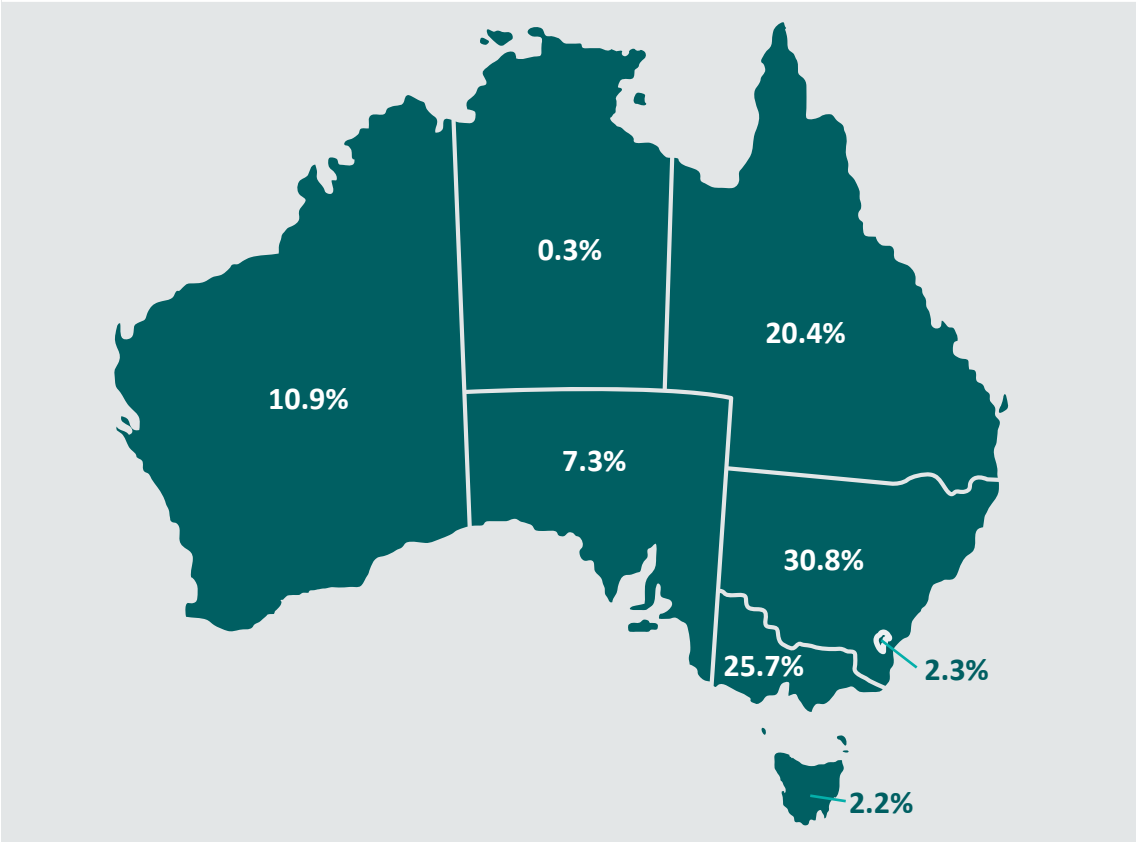
The survey took 12 percent of respondents over an hour to complete. For the remainder, the survey took a median of 23 minutes (*SD*=12.09) to complete. The data were subsequently weighted by age and usual place of residence to ensure they were representative of the spread of the Australian population. Additional random iterative method weights (calculated from Roy Morgan's Single Source survey) were applied to correct for education level, internet use and social media use. This corrected for oversampling of people with higher levels of education and more frequent internet use, which is common among online panels. All of the findings presented in this report are based on weighted data. The final sample size was 10,335 respondents.

There was a high degree of concordance between survey respondent characteristics and ABS demographic data on the sex, age and usual place of residence of the general population (see *Appendix*).

Sample characteristics

The distribution of respondents by their usual place of residence is presented in Figure 1. This was broadly in line with population data for the whole of Australia. The majority of respondents were living in metropolitan areas (73.5%), while 23.4 percent were living in regional areas and 2.8 percent in remote areas (Table 1).

Figure 1: Respondents by usual place of residence (*n*=10,335)



Source: Australian Cybercrime Survey 2024 [weighted data]

Table 1 displays the sociodemographic characteristics of respondents in the 2024 ACS. In 2024, 30.6 percent of respondents were aged 18 to 34 years, 47.5 percent were aged 35 to 64 years, and 21.9 percent of respondents were aged 65 years and over. While 49.2 percent of the sample were male and 50.2 percent were female, 0.6 percent of respondents identified as non-binary. First Nations people accounted for 4.1 percent of respondents, while 9.2 percent of respondents identified as LGB+. One in five respondents were born outside of Australia (22.3%), while 6.0 percent spoke a language other than English most often at home. One in 10 respondents reported having a long-term health condition that restricted their everyday activities or meant they required help or supervision.

As shown in the *Appendix*, the sample for this survey was representative of the spread of the Australian population across key demographics, including age, sex and usual place of residence. In addition, there was a high degree of concordance between the survey respondents and population characteristics for several secondary demographic characteristics. While the survey is not a nationally representative sample, it is largely representative of the Australian population in terms of key demographics.

Table 1: Sociodemographic characteristics of respondents (*n*=10,335)		
	n	%
State or territory		
NSW	3,182	30.8
Vic	2,676	25.9
Qld	2,108	20.4
WA	1,122	10.9
SA	753	7.3
Tas	223	2.2
ACT	237	2.3
NT	33	0.3
Age		
18–24	1,203	11.6
25–34	1,962	19.0
35–49	2,624	25.4
50–64	2,283	22.1
65+	2,262	21.9
Gender		
Female	5,183	50.2
Male	5,086	49.2
Non-binary	66	0.6
First Nations		
Yes	420	4.1
No	9,741	94.3
Unknown	174	1.7
LGB+		
Yes	947	9.2
No	9,215	89.2
Unknown	173	1.7
Born outside of Australia		
Yes	2,302	22.3
No	7,980	77.2
Unknown	52	0.5
Speaks a language other than English most often at home		
Yes	620	6.0
No	9,677	93.6
Unknown	38	0.4

Table 1: Sociodemographic characteristics of respondents (*n*=10,335) (cont.)		
	n	%
Restrictive long-term health condition		
Yes	1,140	11.0
No	8,708	84.3
Unknown	486	4.7
Currently in a relationship		
Yes	6,210	60.1
No	4,038	39.1
Unknown	87	0.8
Children living at home		
Yes	3,419	33.8
No	6,760	65.4
Unknown	83	0.8
Usual place of residence (remoteness)		
Major city	7,595	73.5
Regional	2,423	23.4
Remote	284	2.8
Unknown	33	0.3

Note: Weighted frequencies and percentages may not add to total due to rounding
Source: Australian Cybercrime Survey 2024 [weighted data]

Tables 2 and 3 display information on the education and employment status of respondents in 2024 and how they compare to the 2023 sample. Just under one-third of respondents (30.8%) said their highest level of education was high school, while 41.1 percent of respondents had a university qualification. Two-thirds of respondents (64.9%) were employed, either full or part time, 20.2 percent of respondents were retired and 4.5 percent were unemployed.

Twenty-three percent of respondents who were currently working said they owned, operated or managed a small to medium business (with fewer than 200 employees). A further seven percent of respondents who were currently working said they owned, operated or were the executive of a large business or company (with more than 200 employees).

Table 2: Education, employment and income of respondents (*n*=10,335)		
	n	%
Highest education level		
Year 12 or below	3,181	30.8
Vocational qualification	2,846	27.5
University graduate	4,245	41.1
Unknown	62	0.6
Employment status		
Working full time	4,518	43.7
Working part-time, casual or semi-retired	2,187	21.2
Retired	2,087	20.2
Unemployed	460	4.5
Full-time homemaker or carer	418	4.1
Student full-time (and not working)	163	1.6
Not working for health reasons	366	3.5
Unknown	134	1.3
Owns, operates or works for a small to medium enterprise (SME)		
Owner or manager	1,532	14.8
Employee	1,789	17.3
Does not operate or work for an SME	3,279	31.7
Not currently working	3,629	35.1
Unknown	105	1.0
Owns, operates or works for a large company or business		
Owner or executive	462	4.5
Employee	1,840	17.8
Does not operate or work for a large company	4,268	41.3
Not currently working	3,629	35.1
Unknown	136	1.3

Note: Weighted frequencies and percentages may not add to total due to rounding
Source: Australian Cybercrime Survey 2024 [weighted data]

Table 3: Annual income of respondents in the previous financial year (*n*=10,335)		
	n	%
$0 – $18,200	983	9.5
$18,201 – $45,000	2,373	23.0
$45,001 – $120,000	4,258	41.2
$120,001 – $180,000	1,219	11.8
$180,001 and over	561	5.4
Unknown	940	9.1

Note: Weighted frequencies and percentages may not add to total due to rounding
Source: Australian Cybercrime Survey 2024 [weighted data]

Respondents said they spent 3.4 hours on average using the internet per day for non-work/personal purposes, while those respondents who were working said they spent an average of 4.1 hours using the internet each day for work (Table 4). More than half of respondents (56.8%) said they spent more than three hours a week using social media, while more than three-quarters of respondents (78.1%) said they used the internet three or more times a day. When asked to rate their ability to use technology, 45.7 percent rated their ability as moderate, 42.7 percent rated their ability as high or very high, and 10.8 percent rated their ability as low or very low. While half the respondents rated their knowledge of technology as moderate (49.4%) and 32.7 percent said it was high or very high, 16.8 percent rated their knowledge of technology as low or very low.

Table 4: Online behaviour of respondents		
	n	%
Average hours spent using the internet		
Personal use[a]	8,818	3.4 hours
Work-related[b]	5,457	4.1 hours
Social media use		
No social media use	1,466	14.2
Up to 3 hours per week	2,997	29.0
Between 3 and 8 hours a week	2,771	26.8
More than 8 hours a week	3,101	30.0
Internet use		
A few times a week or less	528	5.1
Once a day	999	9.7
Twice a day	737	7.1
Three or more times a day	8,071	78.1
Self-rated knowledge of technology		
Very low	390	3.8
Low	1,347	13.0
Moderate	5,102	49.4
High	2,471	23.9
Very high	907	8.8
Unknown	118	1.1
Self-rated ability to use technology		
Very low	269	2.6
Low	844	8.2
Moderate	4,724	45.7
High	3,184	30.8
Very high	1,230	11.9
Unknown	84	0.8

a: Excludes 1,517 respondents who did not know or declined to answer the question

b: Limited to respondents who were currently working (*n*=6,706) and excludes 1,249 respondents who did not know or declined to answer the question

Note: Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Analysis

Most of the analysis presented in this report is descriptive. There are some comparisons between groups in terms of the likelihood of certain outcomes, such as victimisation and help-seeking. The focus is on results where there was a statistically significant relationship between two variables, which is marked by an asterisk (*). Given most variables are categorical in nature, chi-square tests of independence were used (unless otherwise stated). This produces a Pearson χ^2 statistic, which is corrected for the survey design and converted into an *F* statistic. A statistically significant result means that the observed distribution between categories was not the same as the expected distribution. The threshold for statistical significance was $p<0.05$, which is the same as saying there was a less than five percent likelihood that the observed result occurred due to chance.

An important new feature of this year's report is that we are able to compare results from the 2023 and 2024 surveys. We used the same online panels and recruitment method for the 2024 survey that we used in 2023. We recruited an entirely new sample of respondents (ie nobody in the main sample completed both the 2023 and 2024 survey). Because we used a non-probability sampling method, in order to be able to compare victimisation rates between years we needed to make a number of corrections to account for differences between the samples. While the differences between the two samples were relatively small (see *Appendix*), there was still a number of statistically significant differences. We were particularly concerned with differences between the samples for respondent characteristics that were shown in the 2023 survey to be associated with the risk of victimisation.

There were small but statistically significant differences between the 2023 and 2024 samples in terms of respondents' usual place of residence, gender, First Nations status, LGB+ status, whether they most often spoke a language other than English at home, whether they had a restrictive long-term health condition and whether they were currently in a relationship. There were also differences in the proportion of respondents who owned or worked for small to medium enterprise or large company and respondents' social media use, self-rated knowledge of technology and the number of hours respondents who were working said they spent using the internet each day for work.

To deal with this we approached our analysis in two stages. To compare the prevalence of victimisation between years we estimated a multivariate regression model, known as logistic regression, with victimisation (or another variable of interest, such as use of online safety measures) as the dependent variable. The model included covariates for those variables that were different between years and/or which were expected to have an important relationship with victimisation. Survey year was also included as an independent variable in the model. If survey year was statistically significant, then we could conclude with some confidence that there was a meaningful difference between respondents in 2023 and 2024 in their likelihood of victimisation. In some cases, the prevalence of victimisation was too low to be able to estimate a logistic regression model (ie <100 respondents or fewer than one percent who were a victim).

We then estimated the average predictive margins, adjusted for covariates using marginal standardisation (Muller & MacLehose 2014), for the 2023 and 2024 respondents. Predictive margins indicate the average predicted probability of the outcome of interest being observed—in this case, being a victim of cybercrime—for each survey year, controlling for the other variables in the logistic regression model. This is, in effect, an adjusted estimate of the prevalence of victimisation, and is presented as such throughout the report. It is not the actual prevalence of victimisation; rather, it provides an estimated probability of victimisation for the two survey years when everything else is the same between the two groups.

This approach was not used when comparing victims in 2023 and 2024 in terms of help-seeking and the harms from cybercrime. In these cases, the differences we observe are just as likely to reflect differences in the types of cybercrimes and severity of incidents as they are differences between victims. We therefore rely on bivariate analyses and discuss the possible explanations for any differences that are observed.

Limitations

This survey provides important data about the prevalence and characteristics of cybercrime, risk factors, help-seeking behaviour, financial losses and other harms from victimisation. While there are several related collections, many of these rely on data reported to police, to ReportCyber, or to other channels such as Scamwatch (Australian Competition and Consumer Commission 2024; Australian Signals Directorate 2024). The data presented in this report are not limited to cybercrime victims who have reported the incidents to anyone. Further, the survey measures different types of cybercrime—an advantage over other more focused collections—and is able to provide a more complete picture of not only the extent, risks and effects of specific forms of cybercrime and responses to them but also the relationship between different forms of cybercrime. Online panels allow for rapid collection of data from large samples, which is particularly useful where the outcome of interest is relatively rare (as is the case with specific types of cybercrimes), where additional information beyond the prevalence of the outcome is required. It allows for detailed analysis of specific issues that would not be possible with a smaller sample. There are, however, several important limitations.

Survey design and sampling

First, and most importantly, the ACS did not use probability sampling and is not a nationally representative sample of the Australian population. The survey used a non-probability sampling method—namely, proportional quota sampling from an opt-in online research panel. Although this is a common approach to surveys, its limitations are worth noting. Because the survey is based on non-probability sampling, meaning not everyone has an equal likelihood of being selected to participate in the research, results cannot be generalised beyond the sample used in this study. This is because it is not possible to determine the extent of non-coverage bias, or the extent to which the opt-in panel from which the sample was selected represents the wider population.

A concern with non-probability sampling methods that use some form of quota sampling and post-hoc weighting is the potential for sampling bias in relation to secondary demographics—characteristics of the population being surveyed that are not used in either the sampling or weighting strategy (Pennay et al. 2023). While surveys using non-probability sampling methods have been shown to be less accurate than surveys using probability sampling on substantive measures of interest (Pennay et al. 2018; Yeager et al. 2011), there is also recent evidence that the difference in accuracy is relatively small and has improved over time (Pennay et al. 2023).

Importantly, data presented in the *Appendix* show that the sample is demographically representative of the spread of the Australian population, particularly in terms of the gender, age and usual place of residence of respondents. Further, there was a high concordance between secondary demographics of the sample and the Australian population—characteristics of the population that were not used in the sampling or weighting procedure. The under-representation of certain groups—including those born overseas or with a restrictive health condition—is noted as a limitation.

While it was made clear that the survey was not limited to victims of cybercrime, self-selection may lead to bias because cybercrime victims may be more willing than other people to participate. However, the opposite can also be true, and there is evidence that self-selection is associated with reduced reporting of health-related harms (Cheung et al. 2017; Kypri et al. 2011), which may also apply to cybercrime victimisation.

These issues are all relevant to making comparisons over time. The approach we have described above allows us to account for important observed differences between respondents in 2023 and 2024. We have to assume, however, that the probability of being a member of the online panels did not meaningfully vary between years for certain respondent groups and that the probability of certain groups participating in the survey was also relatively constant. We are confident that the differences we observe are meaningful differences in the actual rate of victimisation between respondents in the two years, but cannot entirely rule out other explanations and, similar to the results more generally, cannot say with certainty that these differences would apply to the general population.

Measuring cybercrime

Further, while this survey will capture a lot of cybercrime that is not included in data on incidents reported to police or other sources, there are a number of reasons this report may underestimate the prevalence of cybercrime in the wider community. There are several challenges in trying to accurately measure cybercrime using self-report data from victims. Cybercrime comprises an extremely broad range of crime types, each with different targets, risk factors, offender motivations and modus operandi, harms to victims and response requirements. Outside of its defining feature—that it uses a digital device, computer network or other forms of ICT—the boundaries of cybercrime can be amorphous. This report measures some of the most prominent forms of cybercrime, but it is acknowledged that some common types of cybercrime—such as online child exploitation—are not included. This is largely for pragmatic reasons: specifically, the suitability of a self-report survey of people aged 18 years and over to measure victimisation.

Different types of cybercrime are also linked. Some incidents may involve different types of cybercrime, such as malware resulting in identity crime and misuse. One may lead to another, and the victim may be unaware of the link. Even within these broad categories, a person may experience multiple incidents of the same kind, different types of criminal behaviours in the one incident, or multiple incidents of different kinds. Respondents were encouraged to report the incidents or symptoms of cybercrime that best reflected their experience. It is difficult to overcome the potential challenge of double-counting incidents, or to establish a link between different types of cybercrime.

Further, cybercrime is complex and clandestine. A person may not understand what happened to them, simply that they experienced an adverse outcome (such as losing money). Even if they do know, they may not have enough information about the specifics of their case. It may be difficult to describe the incident. A person who has fallen victim—such as by having their identity stolen—may be unaware for some time, especially if they are not sure what to look for. Because of these challenges, cybercrime can resist easy classification. A balance is needed between being specific enough to capture information about different forms of cybercrime and being broad enough to capture as much criminal activity as possible. While a bottom-up approach increases the likelihood of capturing information about actual cybercrime, that quality of information might come at the expense of the breadth of coverage.

Efforts were made to ensure the questions about cybercrimes and prevention strategies were as accessible as possible for a non-technical audience, and a bottom-up approach to asking about victimisation was adopted. Providing a list of cybercrime indicators, rather than simply asking whether someone was a victim, has the benefit of ensuring that only those incidents that are genuinely cybercrime are counted—it prioritises the accuracy of information, potentially at the expense of completeness. As anticipated, the list of indicators used to measure each type of cybercrime was updated in this year's survey, and this needs to be considered when looking at changes in cybercrime over time. It is also possible that some respondents may not have been aware they were a victim of cybercrime, and some respondents may have been reluctant to disclose experiences of victimisation due to shame or embarrassment.

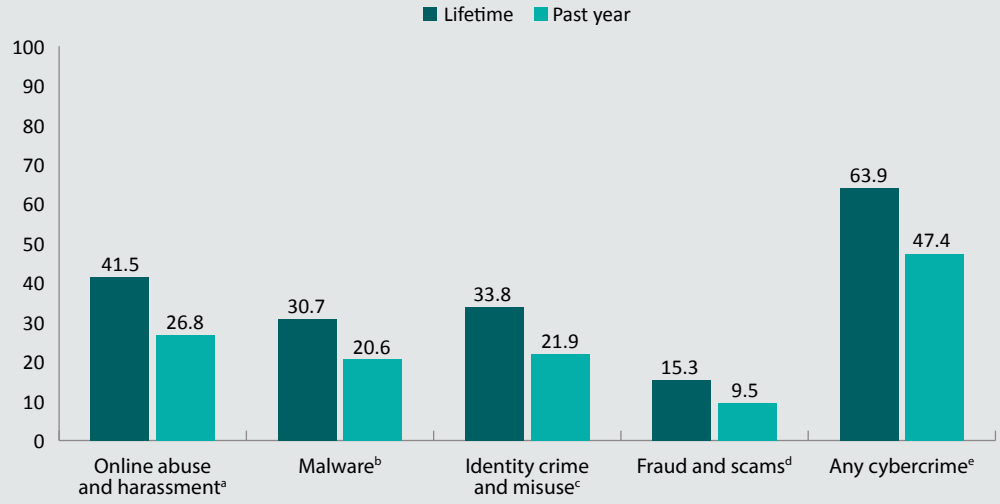
Individuals and businesses

Finally, there was a large group of small to medium business owners and operators who responded to the survey. While this allows for some analysis of the prevalence of cybercrime victimisation among small to medium business operators, this was a survey of Australian individuals. The findings may not be representative of all small to medium business owners. The same is also true for respondents who said they were an owner or executive of a large company or organisation. Further, while there is some detailed analysis of victimisation, help-seeking and cybercrime harms according to respondents' business ownership status, it is important to note that the survey did not distinguish between cybercrime incidents that directly affected work devices and those affecting personal devices (especially as this may not be distinguishable for many respondents, particularly those who operate a small business).

Victimisation

Nearly two-thirds of respondents had been a victim of some type of cybercrime in their lifetime (*n*=6,605, 63.9%), and nearly half had been the victim of a cybercrime in the 12 months prior to the survey (*n*=4,898, 47.4%; Figure 2). In the 12 months prior to the survey, over a quarter of all respondents had been the victim of online abuse and harassment (*n*=2,766, 26.8%), around one in five respondents had been a victim of malware (*n*=2,129, 20.6%) or identity crime and misuse (*n*=2,260, 21.9%), and just under one in 10 respondents were the victim of an online fraud or scam (*n*=985, 9.5%).

Figure 2: Prevalence of cybercrime victimisation, lifetime and past year (%) (*n*=10,335)



a: 463 respondents did not know or declined to answer the question about lifetime prevalence; 672 respondents did not know or declined to answer the question about past-year prevalence

b: 671 respondents did not know or declined to answer the question about lifetime prevalence; 879 respondents did not know or declined to answer the question about past-year prevalence

c: 491 respondents did not know or declined to answer the question about lifetime prevalence; 618 respondents did not know or declined to answer the question about past-year prevalence

d: 384 respondents did not know or declined to answer the question about lifetime prevalence; 447 respondents did not know or declined to answer the question about past-year prevalence

e: 546 respondents did not know or declined to answer the question about lifetime prevalence; 919 respondents did not know or declined to answer the question about past-year prevalence

Note: Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Online abuse and harassment

Respondents were asked about a range of harmful online activities that an individual may experience while interacting with others when using the internet, their personal devices or other technology (Table 5). This includes incidents in a personal or work setting. For the purposes of this report, a respondent was a victim of online abuse or harassment if they had experienced online communication that may have caused them emotional distress. In some instances, these could be one-off incidents, whereas in other cases the communication may have been repeated and occurred over an extended period of time.

The most common forms of online abuse and harassment that respondents said they had experienced in the 12 months prior to the survey were being sent unsolicited sexually explicit messages, images or videos (7.6% of respondents); someone impersonating them online (7.6%); cyberbullying (5.6%); and extortion or harassment involving images or videos (4.8%). Just under four percent of respondents (3.8%) said they had experienced some form of controlling or restricting behaviour relating to their online activity; 3.2 percent of respondents said someone had subjected them to hate speech or made derogatory, malicious or threatening comments directly to them based on their religion, ethnicity, gender, sexuality or ideology; and 2.9 percent of respondents said someone had used technology to stalk or harass them online.

Around one-third of victims of online abuse and harassment—8.6 percent of all respondents—said that they had been a victim of more than one type of incident measured as part of the survey.

Table 5: Incidents of online abuse and harassment (%)

	Past-year prevalence (*n*=10,335)	Most recent incident (*n*=2,766)
Extortion or harassment involving images or videos	**5.4**	**13.3**
Respondent 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	2.9	6.9
Someone used coercion, blackmail or demands to try and get respondent to send them sensitive, personal or compromising photos, video or information that was stored online, on a digital device or sent in messages	1.7	3.5
Someone sent or posted photos and videos of respondent to others to try and embarrass, hurt or blackmail them	0.8	1.3
Someone shared or published sensitive, personal, compromising or intimate photos or videos of respondent without their consent	0.9	1.6

Table 5: Incidents of online abuse and harassment (%) (cont.)		
	Past-year prevalence (*n*=10,335)	Most recent incident (*n*=2,766)
Impersonation	**7.6**	**21.6**
Someone hacked into respondent's social media or network account (including communicating with their contacts or posting messages or status updates from their accounts)	4.8	12.9
Someone set up fake social media or networking profiles pretending to be respondent (eg and communicated with their contacts or posted messages or status updates from their accounts)	3.4	7.7
Someone created fake videos or photos of respondent (eg 'deep fakes')	0.6	1.0
Sharing without consent	**3.1**	**7.0**
Someone stole respondent's online personal information (including photos and videos) and used it without their permission	2.0	4.0
Someone published identifying information (such as respondent's full name, contact number, address, school etc) with malicious intent (ie doxxing)	1.5	3.0
Stalking and harassing	**2.9**	**5.7**
Someone used technology to stalk or repeatedly harass respondent, including being contacted by someone they had blocked or asked to not contact them	2.9	5.7
Controlling and restricting	**3.8**	**8.9**
Someone restricted respondent's access to online resources (eg social media, electronic legal documents, banking and utility accounts, etc)	1.8	3.6
Someone monitored respondent's activity online or on their phone (including installing spyware, going through their private messages, etc)	1.5	2.7
Someone tried to stop respondent from communicating with others online or over their mobile	1.3	2.6
Hate speech	**3.2**	**6.7**
Someone subjected respondent to hate speech or made derogatory, malicious or threatening comments directly to respondent based on their religion, ethnicity, gender, sexuality or ideology	3.2	6.7
Cyberbullying	**5.6**	**13.9**
Someone sent or posted mean or hurtful messages via electronic communication (eg emails, social media or text messages) that made respondent feel hurt, embarrassed or unsafe	4.2	9.8
Someone spread rumours about respondent via electronic communication (eg emails, social media or text messages)	2.3	4.1

Table 5: Incidents of online abuse and harassment (%) (cont.)		
	Past-year prevalence (*n*=10,335)	Most recent incident (*n*=2,766)
Unsolicited sexual content	**7.6**	**22.3**
Respondent was sent unsolicited sexually explicit messages, images or videos	**7.6**	**22.3**
Respondent fell victim to some other type of online abuse and harassment, not specified above	**0.2**	**0.8**
At least one of the above	**26.8**	**–**
More than one type of online abuse and harassment	**8.6**	**–**
None of the above	**73.2**	**–**
Unknown	**6.5[a]**	**1.0[b]**

a: Includes 672 respondents who did not know or declined to answer the question about past-year prevalence

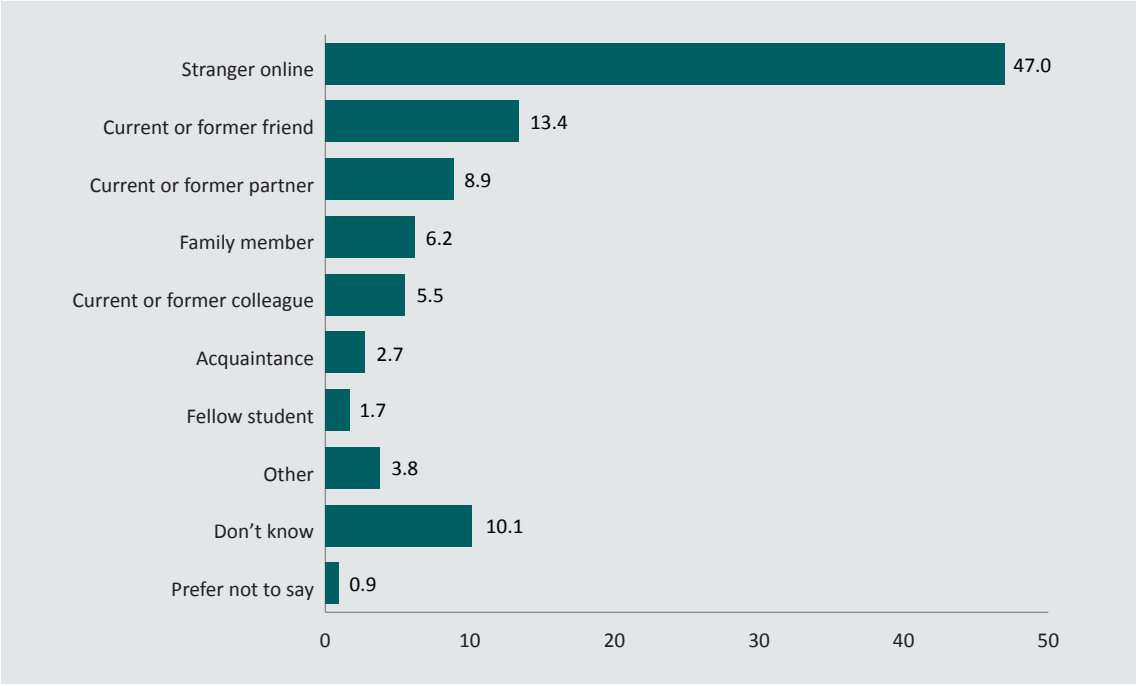
b: Includes 29 respondents who answered the question about past-year prevalence but did not know or declined to answer the question about the most recent incident

Note: Weighted frequencies and percentages may not add to total due to rounding. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2024 [weighted data]

Past-year victims of online abuse and harassment were asked about their relationship to the offender in the most recent incident (Figure 3). Nearly half of the incidents involved a stranger online (47.0%). Fifteen percent of the most recent incidents of online abuse and harassment were domestic or family violence related, meaning they involved a current or former intimate partner or a family member (15.1%). The victim did not know who the perpetrator was in around one in 10 incidents (10.1%).

Figure 3: Relationship between victim and offender in the most recent online abuse and harassment incident (%) (n=2,720)



Note: Results refer to the relationship identified by the victim. If multiple people were involved in the most recent incident, victims were asked to identify the relationship with the person to whom they were closest. Excludes 46 respondents who did not answer the questions about the most recent incident. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Malware

Malware, which is short for malicious software, refers to software specifically developed and used to harm a computer system or network. It is used to gain access to a computer and can be used to steal confidential information. The prevalence of malware can be difficult to measure because it is not always possible for a non-expert to distinguish the work of a malicious actor from other causes, such as the age of a device. Nevertheless, respondents were asked about a range of possible indicators of malware that they believed were not due to genuine malfunction or aging, and which are likely symptomatic of malicious software (Table 6).

We distinguish between suspected malware, which was reported by 17.2 percent of respondents, and ransomware victimisation. The latter includes pure ransomware—where there are obvious signs of the respondent's device having been compromised or access disrupted (2.4% of respondents)—and ransomware-related data theft and extortion, which may or may not involve signs the device had been compromised (2.6% of respondents). Overall, in the 12 months prior to the survey, 4.9 percent of respondents received a ransom message on their device demanding payment.

The most common symptom of suspected malware that victims experienced in the past year were ads starting to pop up everywhere on their device (5.8% of respondents), their device slowing down and acting strangely (4.9% of respondents) and people telling them that they had been sending suspicious messages and links over social media or email (2.8% of respondents).

Table 6: Incidents of malware (%)

	Past-year prevalence (*n*=10,335)	Most recent incident (*n*=2,129)
Suspected malware	**17.2**	**79.0**
Popup ads started popping up everywhere	5.8	20.2
Respondent's device slowed down and acted strangely	4.9	18.0
People respondent knew told them they had been sending suspicious messages and links over social media or email	2.8	3.2
Respondent's devices kept crashing for some reason	2.4	6.8
Respondent's browser kept getting redirected when they tried to search for a familiar site	2.4	6.8
Programs were opening and closing automatically	2.2	5.0
There was a lack of storage space that respondent couldn't explain	2.1	6.1
Respondent's device was working excessively while no programs were running	1.9	11.1
Respondent's files had gone missing or been replaced with odd file extensions and the icons for the files were blank	0.8	0.5
Previously accessible system tools (such as personalised or security settings) were disabled	0.7	1.3
Pure ransomware	**2.4**	**8.8**
Respondent's devices, servers, service or networks were disrupted (eg slowed down, lost connection, had outages) and they received instructions for paying a ransom to restore functionality	1.5	3.7
Respondent's systems, devices or files had a virus or were inaccessible (eg locked or unreadable) and they received instructions for paying a ransom to restore access	1.1	5.1
Ransomware-related data theft and extortion	**2.6**	**10.4**
Respondent received a ransom message on their device to say their data or information had been stolen and they had to pay to prevent this information from being leaked or sold online	2.6	10.4

Table 6: Incidents of malware (%) (cont.)		
	Past-year prevalence (*n*=10,335)	Most recent incident (*n*=2,129)
Respondent fell victim to some other type of malware, not specified above	**0.4**	**1.9**
At least one of the above	**20.6**	**–**
More than one type of malware	**6.3**	**–**
None of the above	**79.4**	**–**
Unknown	**8.5[a]**	**1.0[b]**

a: Includes 879 respondents who did not know or declined to answer the question about past-year prevalence

b: Includes 21 respondents who answered the question about past-year prevalence but did not know or declined to answer the question about the most recent incident

Note: Weighted frequencies and percentages may not add to total due to rounding. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2024 [weighted data]

Identity crime and misuse

Identity crime and misuse refers to incidents where a person's personal information has been obtained or used without their permission. A malicious actor could pretend to be the person, to carry out a business in their name without their permission, or for some other type of activity or transaction. This excludes the use of someone's personal information for direct marketing, even if this was done without their permission.

Overall, 17.5 percent of respondents said that in the past year they had experienced some sort of compromise of their financial accounts, which accounted for three-quarters (76.7%) of the most recent incidents reported by victims of identity crime and misuse victims (Table 7). A much smaller proportion of respondents (4.7%) said they had been a victim of some other form of identity compromise. This included incidents such as a respondent having their identity stolen to apply for government benefits, a job, utility services or medical services, or being impersonated to extort their online contacts. These are the more harmful forms of identity crime and misuse (Voce & Morgan 2025).

In terms of the specific incidents, suspicious transactions appearing in the respondent's bank statements or accounts, credit card or credit report (10.1% of respondents) was the most common type of identity crime and misuse, followed by receiving calls about unpaid bills the respondent did not recognise (4.4% of respondents).

Table 7: Incidents of identity crime and misuse (%)		
	Past-year prevalence (*n*=10,335)	Most recent incident (*n*=2,260)
Compromise of financial accounts	**17.5**	**76.7**
Suspicious transactions appeared in respondent's bank statements or accounts, credit card or credit report	10.1	41.8
Respondent received calls from debt collectors asking about unpaid bills they did not recognise	4.4	18.1
Someone used respondent's details to purchase or order something or they received unfamiliar bills, invoices or receipts	2.9	9.0
Respondent was unsuccessful in applying for credit, and this was surprising given their credit history	1.1	3.6
Someone tried to open a new bank account, apply for a new loan or obtain credit with respondent's personal details or they received credit/payment cards in the mail that they did not apply for	0.8	2.1
Someone tried to obtain money from one of respondent's investments or superannuation accounts	0.6	2.1
Other identity compromise	**4.7**	**18.6**
Someone used respondent's personal details (including images) to create an impersonation account to extort their contacts	1.1	3.8
Someone used respondent's personal details to open a mobile phone or utility account, or their current mobile phone or other utility lost service because their service has been transferred to a new unknown device	0.8	2.3
Respondent got a medical bill for a service they did not receive, or a medical claim was rejected because they had unexpectedly already reached their benefits limit	0.7	2.4
Someone gained access to respondent's cryptocurrency wallet or exchange account and made transactions or stole currency	0.6	2.2
Someone used respondent's personal details to create a fake cryptocurrency wallet or exchange account	0.6	1.8
Someone used respondent's personal details to attempt to apply for a job or rent a property	0.5	1.7
Someone used respondent's personal details to fraudulently apply for government benefits	0.5	1.6
Someone used respondent's personal details to attempt to give false info to police	0.5	1.5
Respondent was unable to file taxes because someone had already filed a tax return in their name	0.5	1.3

Table 7: Incidents of identity crime and misuse (%) (cont.)		
	Past-year prevalence (*n*=10,335)	Most recent incident (*n*=2,260)
Respondent fell victim to some other type of identity crime and misuse, not specified above	**1.1**	**4.7**
At least one of the above	**21.9**	**–**
More than one type of identity crime and misuse	**3.5**	**–**
None of the above	**78.1**	**–**
Unknown	**6.0[a]**	**0.6[b]**

a: Includes 618 respondents who did not know or declined to answer the question about past-year prevalence

b: Includes 14 respondents who answered the question about past-year prevalence but did not know or declined to answer the question about the most recent incident

Note: Weighted frequencies and percentages may not add to total due to rounding. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2024 [weighted data]

Fraud and scams

In this report, fraud and scams involve intentionally deceiving someone to obtain money or something else of value, such as personal details. To be a form of cybercrime, the incident must have involved a digital device, computer network or other forms of ICT. To have been counted as a victim of a fraud or scam, the respondent must have, in most cases, paid money or provided sensitive information to the offender. The subcategories used in this section align with the typology developed by the National Anti-Scam Centre.

The most common types of fraud and scams respondents experienced in the 12 months prior to the survey were all related to buying and/or selling products and services online, reported by 4.4 percent of respondents (Table 8). This most often included paying money or providing sensitive information when they were trying to buy a product or service from a fake or fraudulent seller online (2.3% of respondents), paying money or providing sensitive information when they were trying to sell a product or service to a fake or fraudulent buyer online (0.6% of respondents), and paying a fake invoice or bill for some other product or service that they did not receive (0.6% of respondents). Overall, these buying products or services scams accounted for 42.6 percent of the most recent incidents of fraud and scams reported by victims.

Other common fraud and scam types included investment scams (1.5% of respondents) and phishing scams (1.4% of respondents). Importantly, while phishing scams are included as a specific type of scam reported by victims, many other scam types are initiated by a phishing email (see Box 2).

Table 8: Incidents of fraud and scams (%)		
	Past-year prevalence (*n*=10,335)	Most recent incident (*n*=985)
Investment scams	**1.5**	**11.2**
Respondent lost cryptocurrency in an exit scam or 'rug-pull', where cryptocurrency developers or promoters abandon a project and disappear with investors' funds	0.4	2.6
Respondent lost money or provided sensitive information in another kind of cryptocurrency scam	0.4	2.9
Respondent 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 their super fund	0.4	3.1
Respondent lost cryptocurrency to a scammer in a pretend 'give away', business opportunity or investment opportunity	0.3	2.0
Respondent paid money or provided sensitive information to some other fraudulent scheme related to their super fund	0.2	0.6
Job and employment scams	**0.3**	**2.1**
Respondent lost money or provided sensitive information to a scammer offering a job or employment	0.3	2.1
Buying products or services scams	**4.4**	**42.6**
Respondent paid money or provided sensitive information when trying to buy a product or service from a fake or fraudulent seller online	2.3	21.7
Respondent paid money or provided sensitive information when trying to sell a product or service to a fake or fraudulent buyer online	0.6	5.3
Respondent paid a fake invoice or bill for some other product or service that they did not receive	0.6	5.2
Respondent paid money for health products, medicines or drugs from an online pharmacy and the products never arrived or were counterfeit	0.5	4.7
Respondent sent money to a scammer posing as a known business supplier, service institution or company telling them that their banking details had changed	0.5	4.3
Respondent paid a fake invoice for directory listings, advertising, domain name renewals or office supplies	0.3	1.4
Donation scams	**0.2**	**1.7**
Respondent paid money or provided sensitive information to a scammer pretending to be a charity or disaster relief effort	0.2	1.7
Relationship scams	**0.2**	**1.8**
Respondent paid money, provided sensitive information or sent intimate images or videos to a scammer pretending to be a potential romantic partner	0.2	1.8

Table 8: Incidents of fraud and scams (%) (cont.)		
	Past-year prevalence (*n*=10,335)	Most recent incident (*n*=985)
Remote access scams	**0.9**	**6.9**
Respondent allowed someone pretending to be from a telecommunications or computer company to remotely access their computer, or paid them money or provided sensitive information	0.5	3.7
Respondent allowed some other kind of scammer to remotely access their computer	0.5	3.2
Money recovery scam	**0.3**	**2.5**
Respondent paid money or provided sensitive information to a scammer who was offering to help them recover from a previous scam	0.3	2.5
Unexpected money scams	**0.9**	**6.3**
Respondent paid money or provided sensitive information to a scammer offering them the false promise of an inheritance or share in a large sum of money in exchange for assistance	0.3	1.6
Respondent paid money or provided sensitive information to a scammer offering the false promise of prize money or a holiday package	0.3	1.4
Respondent paid money or provided sensitive information to a scammer falsely offering a rebate from the government, a bank or trusted organisation	0.2	2.1
Respondent paid money or provided sensitive information to a scammer falsely offering some other benefit or payment from the government, a bank or trusted organisation	0.2	1.2
Phishing scams	**1.4**	**12.3**
Respondent paid money or provided sensitive information to a scammer pretending to be from a known service institution or company (bank, internet provider, post office, etc)	0.5	4.5
Respondent paid money or provided sensitive information to a scammer pretending to be someone they personally know, such as a family member, friend or work associate	0.4	3.0
Respondent 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 issue	0.3	3.1
Respondent paid money or provided sensitive information to someone pretending to be a bank, government or law enforcement official for some other fine, bill or debt	0.2	1.7

Table 8: Incidents of fraud and scams (%) (cont.)		
	Past-year prevalence (*n*=10,335)	Most recent incident (*n*=985)
Other scams	**1.5**	**12.8**
Respondent lost money buying sports betting prediction software, or becoming a member of a sport betting syndicate or investment scheme, because these schemes did not work as advertised	0.5	3.6
Respondent paid for extremely high call or text rates when replying to unsolicited SMS competitions	0.1	0.7
Respondent sent money or provided sensitive information to some other kind of scammer who gave them fraudulent bank or payment details	0.4	3.1
Respondent fell victim to some other type of online scam or fraud, not already specified	**0.5**	**5.4**
At least one of the above	**9.5**	**–**
More than one type of fraud or scam	**1.6**	**–**
None of the above	**90.5**	**–**
Unknown	**4.3**[a]	**0.6**[b]

a: Includes 447 respondents who did not know or declined to answer the question about past-year prevalence

b: Includes 6 respondents who answered the question about past-year prevalence but did not know or declined to answer the question about the most recent incident

Note: Weighted frequencies and percentages may not add to total due to rounding. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2024 [weighted data]

Box 2: One in three scams was initiated from a phishing message

Phishing is when scammers email, message or call potential victims pretending to be from reputable companies or known people to induce the victim to reveal personal information or send money. Phishing can be the starting point to many scams, including investment scams, 'Hi mum' scams, or charity scams. The 2024 Australian Cybercrime Survey asked respondents whether the most recent incident began with the scammer sending the respondent an unsolicited text message or email (ie a phishing message). Of the 985 scam victims in the past year, 910 answered the question about whether the incident began with a phishing message. Just over a third (*n*=312, 34.3%) stated that it began with a phishing message.

The likelihood that scams initiated with a phishing message varied by scam type. Unsurprisingly, incidents where the respondent paid money or provided sensitive information to a scammer pretending to be someone they personally knew (such as a family member, friend or work associate) was the scam most likely to be initiated by a phishing message (88.3%). This was followed by incidents where the respondent lost money or provided sensitive information in an unspecified cryptocurrency scam (59.6%), or where the respondent sent money to a scammer posing as a known business supplier, service institution or company telling them that their banking details have changed (58.1%). The scams least likely to begin with a phishing message included where the victim paid money or provided sensitive information when they were trying to buy a product or service from a fake or fraudulent seller online (10.1%), when they were trying to sell a product or service to a fake or fraudulent buyer online (14.6%), or when a scammer was offering to help them recover from a previous scam (29.3%).

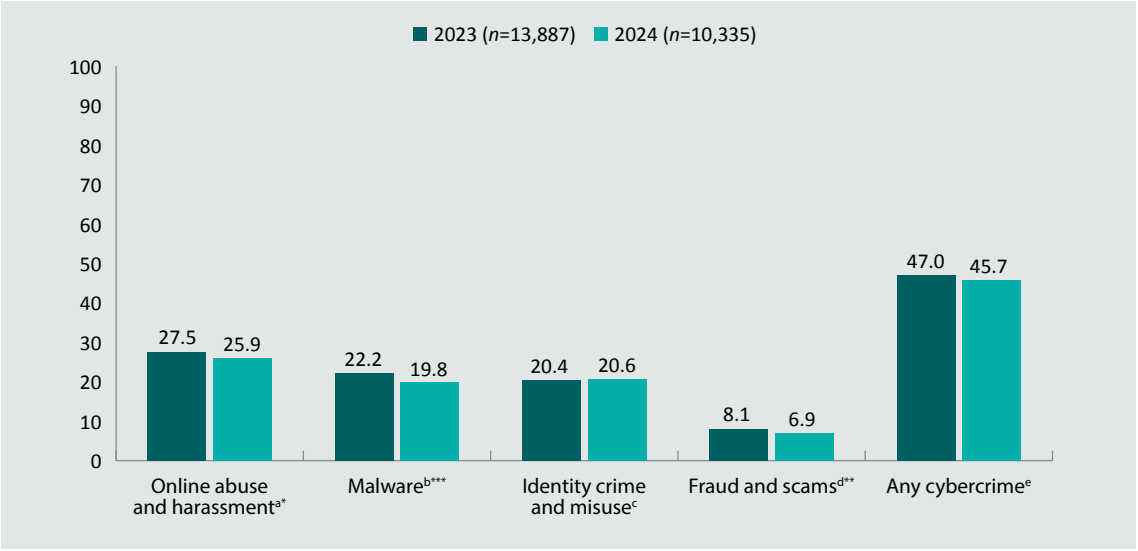
Understanding how scam victims are targeted, whether by a phishing message or some other method, can help inform efforts to reduce the vulnerability of victims to certain types of scams. This includes taking steps to reduce the prevalence of phishing messages, or raising awareness among victims of the link between these messages and certain types of scams.

Respondents who were not victims of a phishing scam in the last year were asked whether they had responded or replied to a phishing message where they subsequently did not provide money or sensitive information because they realised or suspected it was a scam. Of the 9,380 respondents who answered the question, 15.3 percent said they had responded to a sender before realising or suspecting it was a scam and ceasing engagement. This is a significant number of phishing targets who avoided becoming a victim. This may be due to the widespread media coverage, warnings from authorities and public education efforts that have targeted phishing scams in recent years.

Changes in victimisation

We compared the prevalence of cybercrime among respondents to the 2023 and 2024 ACS, limiting our analysis to comparable crimes and adjusting for differences between the two samples. Adjusted estimates of past-year victimisation for the four major categories of cybercrime are presented in Figure 4. This shows that, in 2024, smaller proportions of respondents reported being a victim of online abuse and harassment (27.5% in 2023 vs 25.9% in 2024, $F(39, 24183)=30.20$, $p<0.01$), malware (22.2% vs 19.8%, $F(39, 24183)=18.01$, $p<0.001$) and fraud and scams (8.1% vs 6.9%, $F(39, 24183)=16.44$, $p<0.01$). There was no difference in the estimated likelihood of experiencing identity crime and misuse or any form of cybercrime.

Figure 4: Adjusted estimates of past-year victimisation for major categories of cybercrime, 2023 and 2024 (%)



***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$

Note: Predictive margins derived from separate logistic regression model for each cybercrime type that included controls for key sociodemographic, employment and technology use variables. The outcome variable was past-year victimisation for cybercrime types, incidents or symptoms that were measured in both 2023 and 2024 (see *Method*). Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

a: In 2023, 892 respondents did not know or declined to answer the question about past-year prevalence. In 2024, 672 respondents did not know or declined to answer the question about past-year prevalence

b: In 2023, 1,204 respondents did not know or declined to answer the question about past-year prevalence. In 2024, 879 respondents did not know or declined to answer the question about past-year prevalence

c: In 2023, 833 respondents did not know or declined to answer the question about past-year prevalence. In 2024, 618 respondents did not know or declined to answer the question about past-year prevalence

d: In 2023, 540 respondents did not know or declined to answer the question about past-year prevalence. In 2024, 447 respondents did not know or declined to answer the question about past-year prevalence

e: In 2023, 1,291 respondents did not know or declined to answer the question about past-year prevalence. In 2024, 919 respondents did not know or declined to answer the question about past-year prevalence

Source: Australian Cybercrime Survey 2024 [weighted data]

We then repeated this analysis for the subcategories of cybercrime (Table 9). We note that some of this analysis is limited by the relatively small number of respondents who reported experiencing certain subcategories of online fraud and scams.

The proportion of respondents who said they had received unsolicited sexual content in the 12 months prior to the survey was lower in 2024 (7.5%) than in 2023 (10.0%; $F(39, 24183)=9.23$, $p<0.001$). There was also a smaller proportion of respondents in 2024 who said they were a victim of suspected malware that was not related to ransomware (19.4% in 2023 vs 16.8% in 2024; $F(39, 24183)=14.54$, $p<0.001$), and phishing scams (1.6% in 2023 vs 0.9% in 2024; $F(39, 24183)=6.06$, $p<0.001$). The only subcategory of cybercrime with a higher proportion of victims in 2024 was identity crime and misuse that was not related to the compromise financial accounts (3.8% in 2023 vs 4.4% in 2024; $F(39, 24183)=19.71$, $p<0.05$).

Table 9: Adjusted estimates of past- year victimisation for subcategories of cybercrime, 2023 and 2024

	2023 (*n*=13,887)	2024 (*n*=10,335)
Online abuse and harassment		
Extortion or harassment involving images or videos	4.6	4.7
Impersonation	7.5	7.4
Sharing content without consent	3.1	2.6
Stalking and harassing	2.6	2.7
Controlling and restricting behaviours	4.1	3.7
Hate speech	2.8	2.9
Cyberbullying	4.9	5.6
Unsolicited sexual content	10.0	7.5***
Doxxing	1.6	1.5
Malware attacks		
Pure ransomware	2.5	2.3
Ransomware-related data theft and extortion	2.8	2.6
Other malware	19.4	16.8***
Identity crime and misuse		
Compromise of financial accounts	17.9	17.2
Other identity compromise	3.8	4.4*
Fraud and scams		
Buying products or services scams	3.6	3.8
Phishing scams	1.6	0.8***
Investment scams	1.1	0.9

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$

Note: Predictive margins derived from separate logistic regression model for each cybercrime subcategory that included controls for key sociodemographic, employment and technology use variables. The outcome variable was past-year victimisation. Fraud and scams exclude subcategories that were added in 2024. Excludes types of scams where the prevalence was too low to allow for regression analysis. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2024 [weighted data]

Box 3: Fewer respondents were notified of a data breach in 2024 than in 2023

In 2024, a quarter of respondents (25.0%) said they were notified of a data breach. When we compared the adjusted estimates for 2023 and 2024, we found there was a significant decrease in the proportion of respondents who said they were notified of a data breach in the 12 months prior to the survey (33.7% in 2023 vs 24.9% in 2024; $F(39, 24183)=19.64$, $p<0.001$). In other words, 25.9 percent fewer respondents were notified of a data breach in 2024 than in 2023.

The Office of the Australian Information Commissioner (2024) received 527 notifications of data breaches from January to June 2024, an increase from 409 during the same period in 2023 (Office of the Australian Information Commissioner 2023). However, most of the data breaches in both years impacted fewer than 100 individuals. The January to June period in 2023 had seven data breaches impacting more than one million individuals, whereas there were only two of that scale in the first half of 2024.

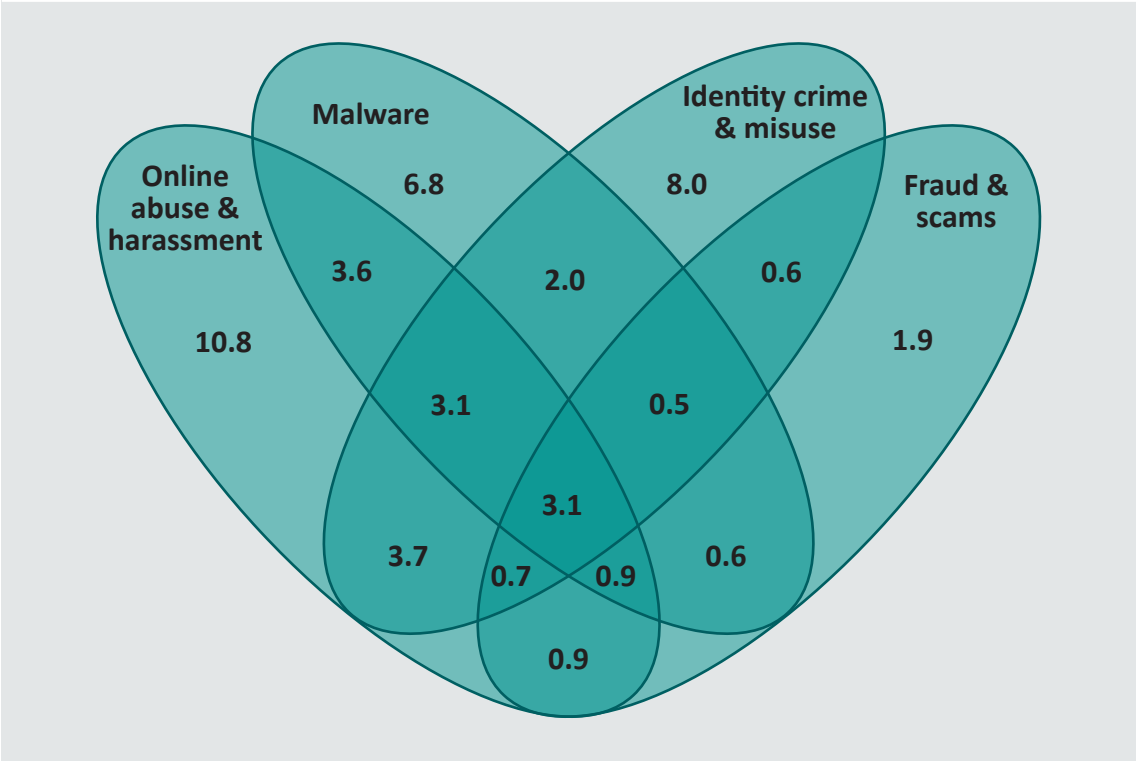
The decrease in large-scale data breaches may be due to large companies implementing stronger proactive prevention strategies in response to increased public scrutiny following several high-profile data breaches in 2022, such as the Optus and Medibank breaches, which were the data breaches most commonly identified by respondents in the 2023 survey. This may also reflect a decreased willingness of customers to provide sensitive information to private companies when that information is not mandatory to provide.

We previously published evidence linking data breaches with cybercrime victimisation (Morgan & Voce 2022). There was a non-significant decrease in ransomware between 2023 and 2024, no change in identity crime, or in overall identity crime and misuse, and a decrease in online fraud and scams, particularly phishing scams. Information obtained through a data breach may help facilitate phishing scams, and this may be one explanation for the decrease observed this year. The overall decrease in data breaches—while relatively large—may still have been insufficient to have generated larger reductions in cybercrime victimisation.

Poly-victimisation

It was common for cybercrime victims to report having experienced multiple types of cybercrime in the 12 months prior to the survey (Figure 5). Victims of fraud and scams were the most likely to also be a victim of another cybercrime type (80.2%), while victims of online abuse and harassment were the least likely to also experience other types of cybercrime (59.6%). Overall, 27.4 percent of respondents were a victim of one type of cybercrime, while 20.0 percent of respondents (42.1% of all victims) were victims of two or more types of cybercrime in the 12 months prior to the survey. A small group of respondents—3.1 percent, or 6.6 percent of all victims—reported having experienced all four types of cybercrime measured by the survey in the 12 months prior to the survey.

Figure 5: Overlap of cybercrimes experienced by respondents (%) (*n*=10,335)



Note: Weighted frequencies and percentages may not add to total due to rounding. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2024 [weighted data]

Box 4: A decline in repeat victimisation?

The proportion of victims who experienced more than one of the four broad types of cybercrime in the past year decreased, from 43.2 percent of victims in 2023 to 39.4 percent in 2024 ($F(1, 11367)=12.53$, $p<0.001$).

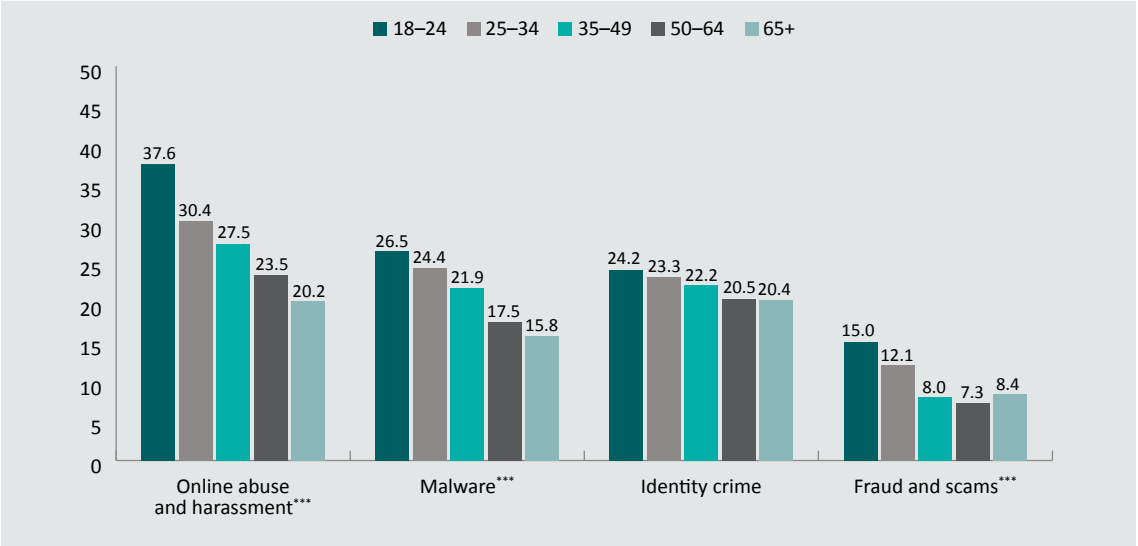
We are unable to tell from these data whether respondents experienced more than one type of cybercrime as part of the same incident, whether the different types of cybercrime were connected but separate incidents, or whether the respondent was a victim of multiple unrelated incidents of cybercrime. It may be that this result indicates a fall in the rate of repeat victimisation. Results reported in the section *Help-seeking by victims following the most recent incident* suggest there has been a rise in help-seeking among victims. Victims who seek help, support and advice following an incident may be more likely to implement online safety strategies that reduce their risk of falling victim a second time.

Further work is needed to measure the effect of support for victims who report cybercrime on repeat victimisation.

Victim characteristics

Younger respondents were consistently more likely to be cybercrime victims than their older counterparts (Figure 6). Respondents aged 18 to 24 were most often the victims of online abuse and harassment (37.6%), malware (26.5%) and fraud and scams (15.0%). Identity crime and misuse was the only cybercrime that did not vary significantly by age, although it did decline slightly from respondents aged 18 to 24 (24.2%) through to respondents aged 65 years and above (20.4%).

Figure 6: Cybercrime victimisation, by crime type and age group (%) (*n*=10,335)



***statistically significant at $p<0.001$

Note: Sample sizes of age groups are as follows: 18–24 years, *n*=1,203; 25–34 years, *n*=1,962; 35–49 years, *n*=2,624; 50–64 years, *n*=2,283; 65 years and over, *n*=2,262. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

The prevalence of different cybercrimes according to respondent characteristics is presented in Table 10. There were several key differences.

- Men were more likely than women to be the victim of malware (21.8% vs 19.4%) and online abuse and harassment (28.2% vs 25.2%).
- First Nations respondents had a significantly higher prevalence of victimisation across all types of cybercrime. They were more likely than non-Indigenous respondents to experience online abuse and harassment (43.4% vs 25.9%) and identity crime (36.4% vs 21.1%), and around twice as likely to become the victim of malware (39.3% vs 19.6%) and fraud or scams (21.8% vs 8.9%).
- Respondents who identified as LGB+ were significantly more likely than heterosexual respondents to have been a victim of online abuse and harassment (38.7% vs 25.6%) and fraud and scams (12.8% vs 9.3%).
- Compared with other respondents, those who mainly spoke a language other than English at home were more likely to have been a victim of online abuse and harassment (32.9% vs 26.4%), malware (27.3% vs 20.2%) and fraud and scams (15.7% vs 9.2%).
- Respondents with a restrictive health condition were more likely than other respondents to have been a victim of online abuse and harassment (43.9% vs 24.8%), malware (30.9% vs 19.3%), identity crime and misuse (32.8% vs 20.5%) and fraud and scams (18.6 vs 8.3%).

Table 10: Cybercrime victimisation by crime type and sociodemographic characteristics (%) (*n*=10,335)

	Online abuse and harassment	Malware	Identity crime and misuse	Fraud and scams
Gender				
Female (*n*=5,086)	25.2**	19.4**	21.5	9.4
Male (*n*=5,183)	28.2	21.8	22.2	9.7
Non-binary (*n*=66)[a]	29.2	23.3	21.0	7.3
First Nations[b]				
Yes (*n*=420)	43.4***	39.3***	36.4***	21.8***
No (*n*=9,741)	25.9	19.6	21.1	8.9
LGB+[c]				
Yes (*n*=947)	38.7***	22.1	24.8	12.8**
No (*n*=9,215)	25.6	20.5	21.7	9.3
Speaks a language other than English most often at home[d]				
Yes (*n*=620)	32.9**	27.3***	26.2*	15.7***
No (*n*=9,677)	26.4	20.2	21.6	9.2
Restrictive long-term health condition[e]				
Yes (*n*=1,140)	43.9***	30.9***	32.8***	18.6***
No (*n*=8,708)	24.8	19.3	20.5	8.3

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$

a: The sample of non-binary respondents is small and care should be taken when interpreting the results. The prevalence of victimisation was compared between men and women, excluding non-binary respondents, due to this small sample size

b: Excludes 174 respondents who did not know or declined to answer the question

c: Excludes 173 respondents who did not know or declined to answer the question

d: Excludes 38 respondents who did not know or declined to answer the question

e: Excludes 486 respondents who did not know or declined to answer the question

Note: Weighted frequencies and percentages may not add to total due to rounding. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2024 [weighted data]

Victimisation varied according to respondents' employment status (Table 11). Unemployed respondents were the most likely to experience online abuse and harassment (31.3%) and malware (23.0%), while employed respondents were the most likely to have been a victim of identity crime and misuse (23.4%). Small to medium business owners, operators and managers experienced significantly higher rates of all types of cybercrime than other respondents.

They were more likely than respondents who worked for some other organisation to have been a victim of online abuse and harassment (38.6% vs 22.7%), malware (28.2% vs 17.6%), identity crime (31.0% vs 19.3%) and fraud and scams (15.2% vs 7.2%). Conversely, respondents who worked for a large business or company were less likely than those who worked for other companies or organisations to have been a victim of online abuse and harassment (23.1% vs 31.5%), a malware attack (16.6% vs 24.7%), identity crime and misuse (18.3% vs 26.2%) and fraud or scams (5.8% vs 11.9%). Respondents with incomes between $120,001 and $180,000 had the highest rates of malware attacks (26.4%), followed by respondents with an income higher than $180,000 (23.1%).

Table 11: Cybercrime victimisation by crime type and respondent education, employment and income (%) (n=10,335)

	Online abuse and harassment	Malware	Identity crime and misuse	Fraud and scams
Employment status[a]				
Employed (*n*=6,706)	28.4***	22.0***	23.4***	10.0
Unemployed (*n*=460)	31.3	23.0	20.0	8.0
Other (*n*=3,115)	22.6	17.2	18.9	8.6
Owns, operates or works for a small to medium enterprise (SME)[b]				
Owner or manager (*n*=1,532)	38.6***	28.2***	31.0***	15.2***
Employee (*n*=1,789)	30.7	24.9	24.8	10.8
Works but not at an SME (*n*=3,279)	22.7	17.6	19.3	7.2
Owns, operates or works for a large company or business[c]				
Large company owner or executive (*n*=462)	25.2***	19.3***	19.7***	8.7***
Large company employee (n=1,840)	23.1	16.6	18.3	5.8
Works but not at a large company (*n*=4,268)	31.5	24.7	26.2	11.9
Annual income[d]				
$0 – $18,200 (*n*=983)	28.7	21.7**	19.5	9.6
$18,201 – $45,000 (*n*=2,373)	26.9	20.8	21.6	9.5
$45,001 – $120,000 (*n*=4,258)	27.3	20.1	23.3	9.8
$120,001 – $180,000 (*n*=1,219)	27.7	26.4	23.7	10.9
$180,001 and over (*n*=561)	32.5	23.1	25.0	11.1

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$

a: Excludes 54 respondents who did not know or declined to answer the question

b: Excludes 105 respondents who did not know or declined to answer the question

c: Excludes 136 respondents who did not know or declined to answer the question

d: Excludes 940 respondents who did not know or declined to answer the question

Note: Weighted frequencies and percentages may not add to total due to rounding. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2024 [weighted data]

Changes in victimisation among select groups of respondents

Using a similar methodology to our analysis of victimisation among all respondents, we compared the rate of victimisation among 2024 and 2023 respondents according to age, gender and whether the respondent was a small to medium business owner, operator or manager (Table 12).

For some crime types and age groups, the prevalence of cybercrime victimisation decreased between 2023 and 2024:

- respondents aged 18 to 24 years were less likely to be a victim of malware (31.0% in 2023 vs 26.3% in 2024, $F(34, 24186)=2.66$, $p<0.05$);
- respondents aged 35 to 49 years were less likely to be a victim of an online fraud or scam (7.6% in 2023 vs 5.7% in 2024, $F(33, 24130)=5.24$, $p<0.05$);
- respondents aged 50 to 64 years were less likely to be a victim of online abuse and harassment (25.3% in 2023 vs 22.8% in 2024, $F(35, 24187)=6.57$, $p<0.05$); and
- respondents aged 65 years and over were less likely to be a victim of online abuse and harassment (23.0% in 2023 vs 19.7% in 2024, $F(34, 24187)=5.85$, $p<0.01$) and malware attacks (21.7% in 2023 vs 18.5% in 2024, $F(35, 24187)=3.07$, $p<0.001$).

Further, the prevalence of malware victimisation was lower among women in 2024 (18.5%) than it was in 2023 (21.7%; $F(37, 24185)=9.60$, $p<0.001$), while there were fewer male victims of online fraud and scams in 2024 (7.2%) than in 2023 (9.4%; $F(34, 24139)=12.53$, $p<0.001$).

Table 12: Cybercrime victimisation by crime type and respondent age and gender, 2023 and 2024 (%)

	Online abuse and harassment		Malware		Identity crime and misuse		Fraud and scams	
	2023	2024	2023	2024	2023	2024	2023	2024
Age								
18–24 (*n*=2,743)	38.6	38.1	31.0	26.3*	24.5	24.3	13.1	12.1
25 – 34 (*n*=4,489)	30.1	29.8	24.7	24.0	23.2	22.2	10.3	9.3
35–49 (*n*=6,188)	26.1	26.2	20.9	20.9	20.6	20.6	7.6	5.7*
50–64 (n=5,472)	25.3	22.8*	18.6	17.0	18.6	18.8	5.6	5.4
65+ (*n*=5,330)	23.0	19.7**	20.5	14.7***	17.7	19.4	6.5	5.5
Gender[a]								
Female (*n*=12,084)	25.9	24.4	21.7	18.5***	20.4	20.1	6.7	6.6
Male (*n*=12,020)	29.0	27.2	22.7	21.1	20.4	21.0	9.4	7.2***

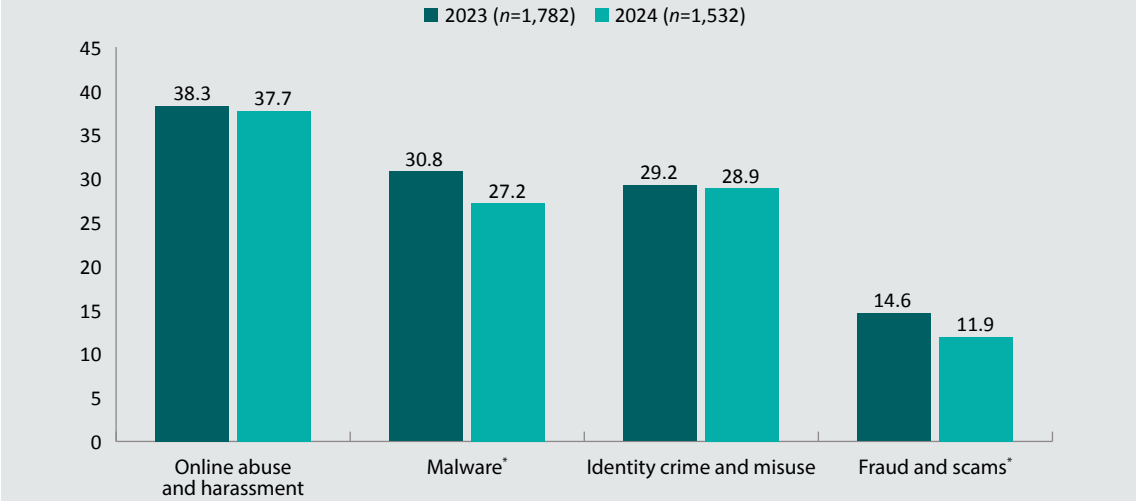
a: Non-binary respondents were excluded from multivariate analysis due to small sample size

Note: Predictive margins derived from separate logistic regression model for each cybercrime type and age group or gender that included controls for key sociodemographic, employment and technology use variables. The outcome variable was past-year victimisation for cybercrime types, incidents or symptoms that were measured in both 2023 and 2024 (see *Method*). For both 18–24 and 65+ age groups, a small number of cases were omitted from the model due to small cell sizes. This does not impact the validity of the overall finding. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2024 [weighted data]

There has been a significant focus on preventing cybercrime among small to medium business owners and operators, given their vulnerability to victimisation. As shown in Figure 7, the proportion of small to medium business owners who responded to the survey and who were a victim of malware was lower in 2024 (27.2%) than it was in 2023 (30.8%; $F(35, 24187)=7.53$, $p<0.05$). The proportion of respondents who were small to medium business owners and who were a victim of fraud and scams was also lower (14.6% in 2023 vs 11.9% in 2024; $F(34, 24,172)=8.25$, $p<0.05$). There was no difference in the prevalence of online abuse and harassment or identity crime and misuse.

Figure 7: Changes in victimisation from 2023 to 2024, for SME owners (%)



*statistically significant at $p<0.05$

Note: Predictive margins derived from separate logistic regression model for each cybercrime type that included controls for key sociodemographic, employment and technology use variables. Model was restricted to small to medium enterprise (SME) owners, operators and managers. The outcome variable was past-year victimisation for cybercrime types, incidents or symptoms that were measured in both 2023 and 2024 (see *Method*). Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2024 [weighted data]

Digital literacy and online safety strategies

This section outlines changes in online behaviour, digital literacy and online safety. This provides valuable contextual information to help better understand findings in relation to patterns of victimisation.

Digital literacy

Respondents were asked to estimate the amount of time they spent using the internet for personal use and, among those respondents who were working, the amount of time they spent using the internet on an average work day for work reasons. It has been shown that the longer a person spends using the internet for personal and work-related use, the more likely they are to be the victim of each form of cybercrime (Voce & Morgan 2023a). The average time spent online for work-related activities increased from 3.86 hours in 2023 to 4.07 hours in 2024 ($F(38, 24184)=31.87$, $p<0.01$), while there was no change in time spent online for personal use (Table 13).

Table 13: Mean number of hours spent online for personal and work-related use, 2023 and 2024

	Mean hours, 2024	Adjusted estimates	
		2023	2024
Personal use[a]	3.41	3.35	3.37
Work-related use[b]	4.13	3.86	4.07**

**statistically significant at $p<0.01$

a: 2023 data exclude 1,815 respondents who did not know or declined to answer the question; 2024 data exclude 1,517 respondents who did not know or declined to answer the question

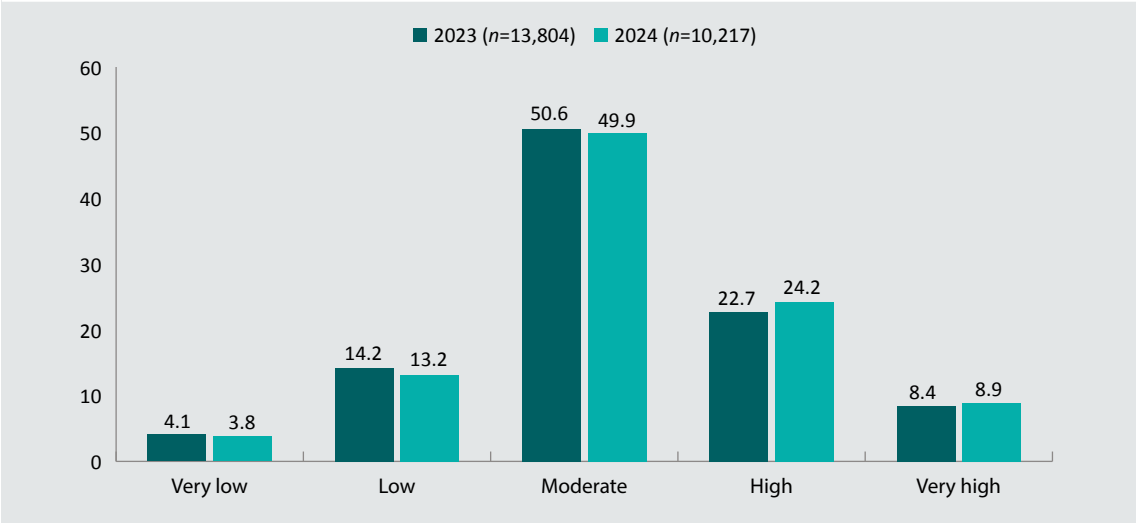
b: 2023 data exclude 5,002 respondents who did not indicate they were currently working and 1,507 who did not know or declined to answer the question; 2024 data exclude 3,629 respondents who did not indicate they were currently working and 1,249 who did not know or declined to answer the question

Note: Predictive margins derived from separate regression models for personal use and work-related use that included controls for key sociodemographic and employment variables. The outcome variable was the number of hours spent online. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Respondents were asked to rate their knowledge of technology and their ability to use technology. Compared to respondents in 2023, respondents in 2024 were more likely to rate their knowledge of technology as high (22.7% vs 24.2%) or very high (8.4% vs 8.9%, F=2.44, p<0.05; Figure 8). There was no difference between 2023 and 2024 in respondents' self-rated ability to use technology (Figure 9).

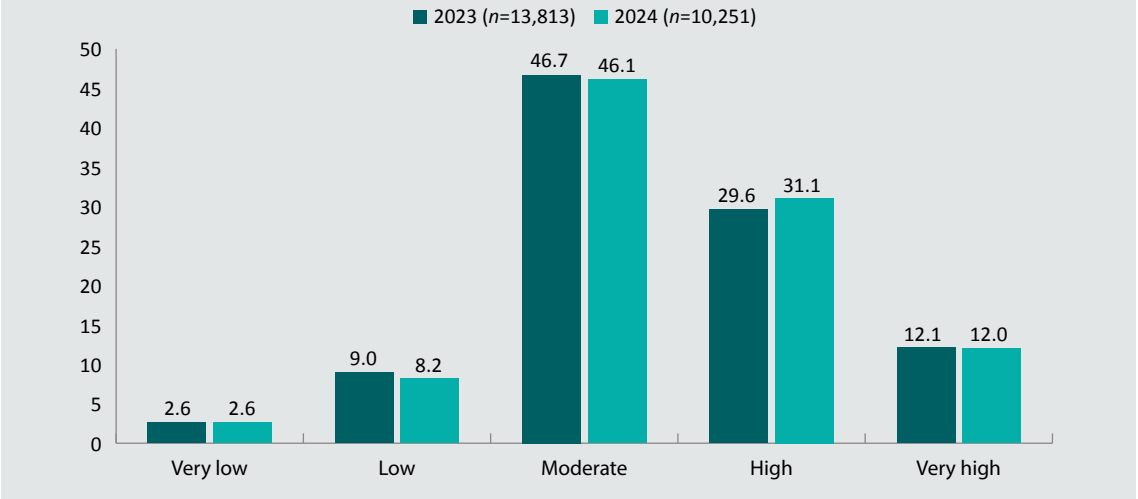
Figure 8: Self-rated knowledge of technology, 2023 and 2024 (%)



Note: To compare respondents in 2023 and 2024 we estimated a regression model that included controls for key sociodemographic, employment and technology use variables. The outcome variable was the rating of knowledge of technology, converted into a 5-point score: B=0.03, F(34, 24188)=112.32, p<0.05. Excludes 83 respondents in 2023 and 118 respondents in 2024 who did not know or declined to answer the question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Figure 9: Self-rated ability to use technology, 2023 and 2024 (%)



Note: To compare respondents in 2023 and 2024 we estimated a regression model that included controls for key sociodemographic, employment and technology use variables. The outcome variable was the rating of ability to use technology, converted into a 5-point score. The results were not statistically significant. Excludes 74 respondents in 2023 and 84 respondents in 2024 who did not know or declined to answer the question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Frequent use—defined as daily or weekly use—of particular platforms or online activities has been associated with a higher risk of both online abuse and harassment and profit-motivated cybercrime victimisation (Voce & Morgan 2023a, 2023b). We compared the prevalence of frequent use of these platforms and activities in 2024 with results from the 2023 survey. As shown in Table 14, in 2024 there was a higher proportion of respondents who:

- used subscription-based sexually explicit interactive adult platforms (4.1% in 2023 vs 5.8% in 2024; $F(39, 24183)=31.45$, $p<0.001$);
- made donations or payments over gaming, streaming or fundraising platforms (6.8% vs 9.4%; $F(39, 24183)=27.50$, $p<0.001$);
- were active on romance/dating websites or apps (7.9% vs 9.2%; $F(39, 24183)=43.93$, $p<0.01$);
- purchased items from online store websites and apps, excluding classifieds and marketplaces (24.2% vs 25.5%; $F(39, 24183)=42.57$, $p<0.05$);
- participated in online gaming/sports (19.4% vs 21.0%; $F(39, 24183)=42.88$, $p<0.01$); and
- live streamed videos of content creators, influencers or gamers online (21.5% vs 22.8%; $F(39, 24183)=50.34$, $p<0.05$).

Conversely, in 2024 there were fewer respondents who:

- live streamed videos of themselves online (14.9% in 2023 vs 13.7% in 2024; $F(39, 24183)=34.86$, $p<0.05$);
- posted or responded to posts on social media (49.9% vs 46.0%; $F(39, 24183)=49.87$, $p<0.001$);
- browsed or looked for information online (93.2% vs 91.2%; $F(39, 24183)=30.87$, $p<0.001$);
- sent emails (84.2% 82.4%; $F(39, 24183)=37.23$, $p<0.01$); and
- read news articles online (76.0% vs 73.8%; $F(39, 24183)=37.95$, $p<0.01$).

Table 14: Daily or weekly engagement in online activities, 2023 and 2024 (%)

	Daily or weekly use in 2024	Adjusted estimates	
		2023	2024
Using subscription-based sexually explicit interactive adult platforms	6.1	4.1	5.8***
Making donations or payments over gaming, streaming or fundraising platforms	9.8	6.8	9.4***
Being active on romance/dating websites or apps	9.8	7.9	9.2**
Live streaming videos of myself online	14.2	14.9	13.7*
Purchasing items from online marketplaces (excluding online store websites and apps)	17.6	16.8	17.0
Posting or responding to posts on social media	47.1	49.9	46.0***
Posting or responding to posts on online blogs, forums or interest groups	22.4	21.0	21.6
Online banking and other online financial activities	81.9	81.7	81.8
Messaging and chatting online	71.	71.4	70.6
Private video chatting over apps and platforms	36.3	35.8	35.8
Streaming videos on your computer, phone or TV	73.3	74.1	73.0
Purchasing items from online store websites and apps (excluding classifieds and marketplaces)	26.0	24.2	25.5*
Participating in online gaming/sports	21.4	19.4	21.0**
Accessing sexually explicit adult websites	18.3	18.4	17.8
Live streaming videos of content creators, influencers or gamers online	23.4	21.5	22.8*
Browsing or looking for information	91.1	93.2	91.2***
Sending emails	82.1	84.2	82.4**
Reading news articles online	73.7	76.0	73.8**

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$

Note: Predictive margins derived from separate regression models for each online activity that included controls for key sociodemographic, employment and technology use variables. The outcome variable was whether respondents had engaged in that activity on a daily or weekly basis or more. Excludes respondents who did not know or declined to answer the question, which varied for different online activities. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Online safety strategies

Respondents were asked whether they had used various online safety measures or engaged in various unsafe behaviours in the 12 months prior to the survey (Tables 15 and 16). While a higher proportion of survey respondents used a secure password manager in 2024 than in 2023 (25.0% in 2023 vs 26.8% in 2024, $F(39, 24183)=15.86$, $p<0.01$), there were fewer respondents in 2024 who:

- checked their privacy settings on social media accounts (42.5% in 2023 vs 39.0% in 2024, $F(39, 24183)=41.55$, $p<0.001$);
- cleared their browsing history, data and cookies frequently (40.7% vs 38.7%, $F(39, 24183)=9.58$, $p<0.01$);
- installed or used antivirus software or firewalls on their devices (43.9% vs 41.0%%, $F(39, 24183)=46.82$, $p<0.001$);
- used password protection on their router (28.1% vs 26.3%, $F(39, 24183)=20.77$, $p<0.01$);
- changed their privacy settings on social media accounts from the default to a more restricted setting (35.1% vs 33.1%, $F(39, 24183)=33.45$, $p<0.01$);
- had children under 18 years living at home and who set, or already had installed, parental controls on devices and browsers to restrict access to certain content (25.4% vs 20.6%, $F(39, 24183)=3.82$, $p<0.001$);
- avoided clicking on links or attachments when they were not certain who the sender of an SMS/text or email was (73.8% vs 68.1%, $F(39, 24183)=44.73$, $p<0.001$); and
- independently contacted a company or government department when they were unsure about an SMS/text or email they had received from them (36.7% vs 32.8%, $F(39, 24183)=18.67$, $p<0.001$).

Table 15: Prevalence of online safety measures, 2023 and 2024 (%)

	Prevalence in 2024	Adjusted estimates	
		2023	2024
Checked privacy settings on social media accounts	37.8	42.5	39.0***
Purchased or continued to have cyber insurance	4.6	6.5	7.0
Generally browsed in incognito mode	15.8	18.1	17.9
Cleared their browsing history, data and cookies frequently	36.8	40.7	38.7**
Participated in training to stay safe online or protect their online environment and information	13.5	15.1	15.8
Installed or used spam-filtering software	20.5	22.4	22.5
Installed or used antivirus software or firewalls on their devices	39.3	43.9	41.0***
Regularly updated the security software on their device when prompted by their device's security system	38.6	41.6	40.3
Regularly updated their password on secure accounts, including email, banking or online stores and social media	25.7	28.3	27.5
Used a secure password manager	24.9	25.0	26.8**
Used password protection on their router	24.3	28.1	26.3**
Used a different password for secure online accounts, especially for banking or financial transactions	50.7	53.2	52.1
Changed their privacy settings on social media accounts from the default to a more restricted setting	31.6	35.1	33.1**
Used a virtual private network (VPN) when using the internet	19.8	22.3	21.9
Set, or already had installed, parental controls on devices and browsers to restrict access to certain content[a]	20.0	25.4	20.6***
Used voice, fingerprint, facial or iris recognition technology to access their devices, such as their mobile phone	46.7	48.3	48.1
Avoided clicking on links or attachments when they were not certain who the sender of an SMS/text or email was	66.8	73.8	68.1***
Independently contacted a company or government department when they were unsure about an SMS/text or email they had received from them	30.9	36.7	32.8***
Used multifactor or two-factor authentication for personal accounts[b]	57.8	–	–
Used apps and platforms because they protect messages and content with end-to-end encryption[b]	20.7	–	–

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$

a: Limited to respondents with children under 18 years living at home who answered the question (n=5,641)

b: Comparison across years is not possible for items which were not included in the 2023 survey

Note: Predictive margins derived from separate regression models for each online safety strategy that included controls for key sociodemographic, employment and technology use variables. The outcome variable was whether respondents had used that online safety measure. 2023 data exclude 381 respondents who did not know or declined to answer the question; 2024 data exclude 291 respondents who did not know or declined to answer the question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

The proportion of respondents who accepted friend requests from people online who they had not met in person was lower in 2024 than it was in 2023 (12.3% in 2023 vs 11.2% in 2024, $F(39, 24{,}183)=24.24$, $p<0.05$), as was the proportion of respondents who accepted cookies from websites that saved their browsing information (46.1% in 2023 vs 42.8% in 2024, $F(39, 24{,}183)=20.66$, $p<0.001$). The former may indicate that the public is becoming better informed about the tactics scammers use to steal personal information. The latter is also a positive change, as accepting cookies from third-party and unencrypted websites can increase the risk of data and identity theft. However, the likelihood of other unsafe online behaviours did not change, despite these being established risk factors for cybercrime victimisation (see Voce & Morgan 2023b).

Table 16: Prevalence of unsafe online behaviours, 2023 and 2024 (%)

	Prevalence in 2024	Adjusted estimates	
		2023	2024
Accepted friend requests from people online who they had not met in person	9.1	12.3	11.2*
Shared a password or a code for an account they own with someone they knew (or thought they knew)	6.5	9.0	8.8
Used freely available wi-fi in a public location to conduct a financial transaction	9.1	11.1	11.4
Opened emails from people or organisations they did not know	11.9	14.7	14.2
Accepted cookies from websites that saved their browsing information	41.2	46.1	42.8***

***statistically significant at $p<0.001$, *statistically significant at $p<0.05$

Note: Predictive margins derived from separate regression models for each unsafe online activity that included controls for key sociodemographic, employment and technology use variables. The outcome variable was whether respondents had engaged in that unsafe online activity. 2023 data exclude 381 respondents who did not know or declined to answer the question; 2024 data exclude 291 respondents who did not know or declined to answer the question

Source: Australian Cybercrime Survey 2024 [weighted data]

Box 5: Are Australian computer users becoming less vigilant online?

This section shows that respondents were less likely to use online safety strategies in 2024 than they were in 2023, and there was only a small decrease in certain unsafe online behaviours. This is despite evidence linking victimisation to the increased use of high-risk behaviours, including using subscription-based sexually explicit interactive adult platforms; making donations or payments over gaming, streaming or fundraising platforms; and being active on romance and dating websites or apps (Voce & Morgan 2023b).

In *Cybercrime in Australia 2023*, we showed that respondents who used online safety strategies were more likely to be a victim of both online abuse and harassment and profit-motivated cybercrime (Voce & Morgan 2023a). We concluded that this may have been because respondents were taking steps to improve their online behaviour after they had fallen victim. Although it is not reported here, the same pattern was also observed in 2024. Another explanation was that people who had fallen victim to cybercrime were more vigilant online because they used higher-risk platforms more frequently, which was also linked to victimisation.

The rate of victimisation among 2024 respondents was lower than in 2023, and this may explain some of the observed decrease in online safety strategies. But this was not consistent across all cybercrime types, and the difference was relatively small. And the increased use of higher risk platforms in 2024 may have had the opposite effect.

External factors may also have played a role. For example, the decreasing prevalence of respondents checking and changing social media privacy settings may be related to the decrease in the frequent use of social media platforms reported by respondents. Similarly, the decrease in the proportion of respondents who independently verified the details of organisations that had contacted them, or who avoided clicking on links from unknown senders, may be because of efforts by government and private sector to block scammers from reaching potential victims, reducing the need to take preventative action.

Overall, there is no obvious explanation for respondents being less likely to use online safety strategies in 2024 than in 2023. It may be related to changes in victimisation or online behaviour, or reflect the fact that computer users were being less vigilant online. In any case, many respondents were not taking simple but important steps to improve their online safety. There is room for improvement in terms of raising awareness and changing behaviour, as well as finding ways to protect online Australians who may be more vulnerable to victimisation.

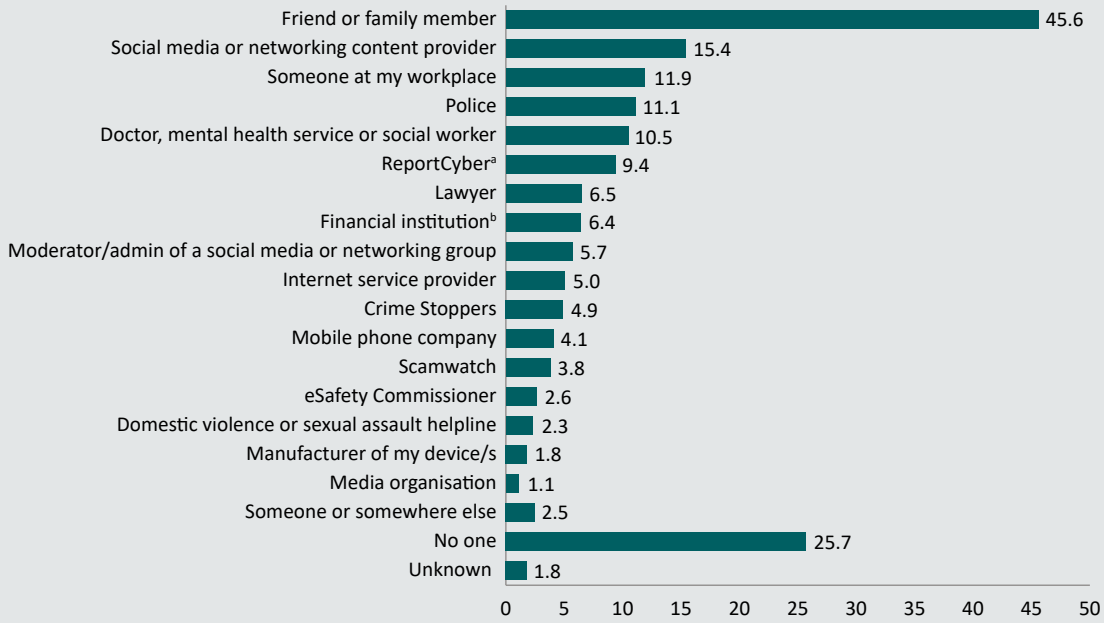
Help-seeking by victims following the most recent incident

Sources of help, advice or support

Respondents who had been a victim of cybercrime in the 12 months prior to the survey were asked whether they had sought help, advice or support from a range of sources following the most recent incident. Victims could seek help, advice or support from multiple people or organisations, including formal and informal sources. The latter refers to friends and family.

Online abuse and harassment victims most commonly told a family member or friend (45.6%); a social media or networking content provider (15.4%); someone at their workplace, such as a manager, human resources or IT support staff (11.9%); and the police (11.1%; Figure 10). Over a quarter of victims (25.7%) did not seek help from anyone about the most recent incident.

Figure 10: Help-seeking among online abuse and harassment victims following the most recent incident (%) (*n*=2,720)



a: Respondents were asked whether they had sought help from ReportCyber, as well as cyber.gov.au, the ACSC and ACSC Hotline

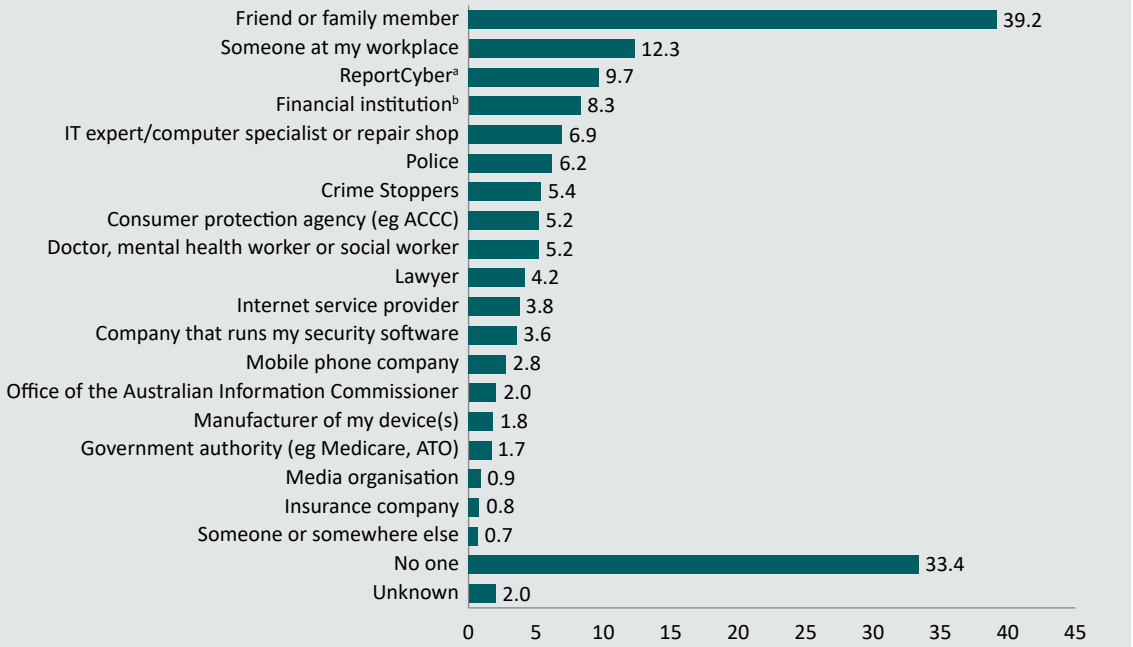
b: Financial institution=bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)

Note: Excludes 46 people who did not answer questions about the most recent incident. Weighted frequencies and percentages may not add to total due to rounding. Respondents could select multiple methods of reporting the most recent incident

Source: Australian Cybercrime Survey 2024 [weighted data]

Victims of malware most commonly told a family member or friend (39.2%), someone at their workplace (12.3%), ReportCyber (9.7%), or a financial institution such as a bank or credit union or a credit or debit card company (eg Visa or MasterCard; 8.3%; Figure 11). Malware had the highest proportion of victims that did not did not tell anyone about the most recent incident (33.4%).

Figure 11: Help-seeking among malware victims following the most recent incident (%)



a: Respondents were asked whether they had sought help from ReportCyber, as well as cyber.gov.au, the ACSC and ACSC Hotline

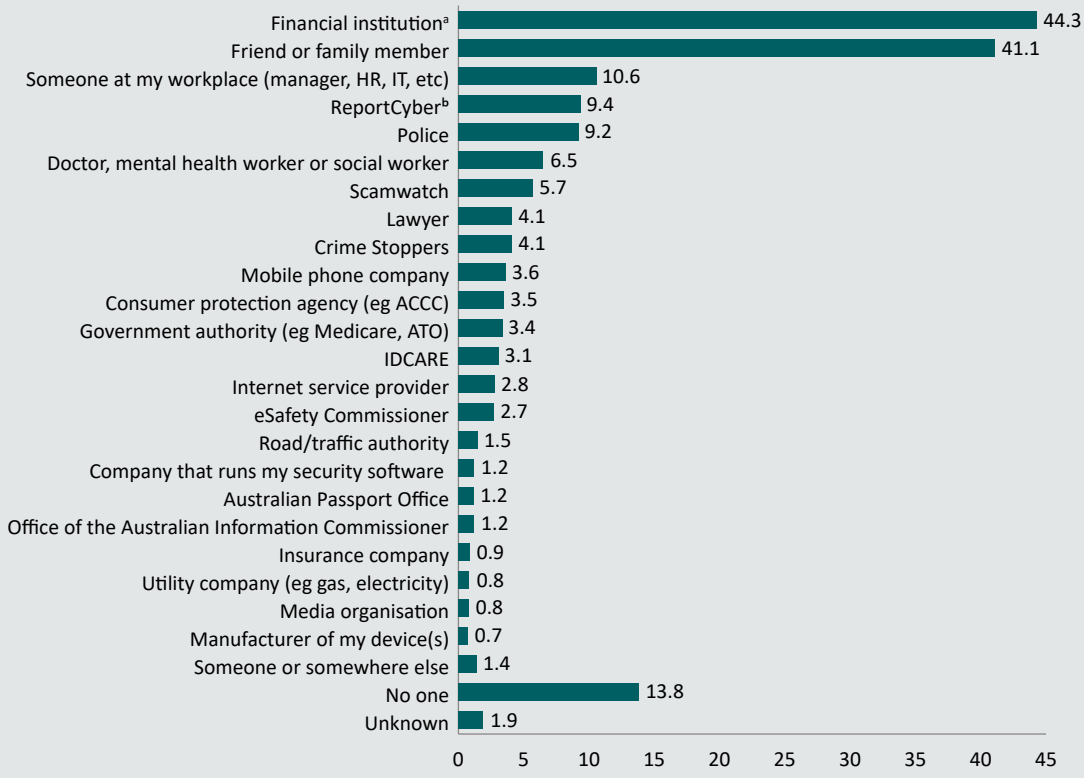
b: Financial institution=bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)

Note: Excludes 21 people who did not answer questions about the most recent incident. Weighted frequencies and percentages may not add to total due to rounding. Respondents could select multiple methods of reporting the most recent incident

Source: Australian Cybercrime Survey 2024 [weighted data]

A large proportion of identity crime victims reported the incident to a financial institution such as a bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal; 44.3%; Figure 12). Victims also commonly told a family member or friend (41.1%); someone at their workplace, such as a manager, human resources or IT support staff (10.6%); and ReportCyber (9.4%). Identity crime and misuse victims were the most likely to seek help, advice or support from at least one source, with around one in seven (13.8%) not telling anyone about the most recent incident.

Figure 12: Help-seeking among identity crime and misuse victims following the most recent incident (%) (*n*=2,246)



a: Financial institution=bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)

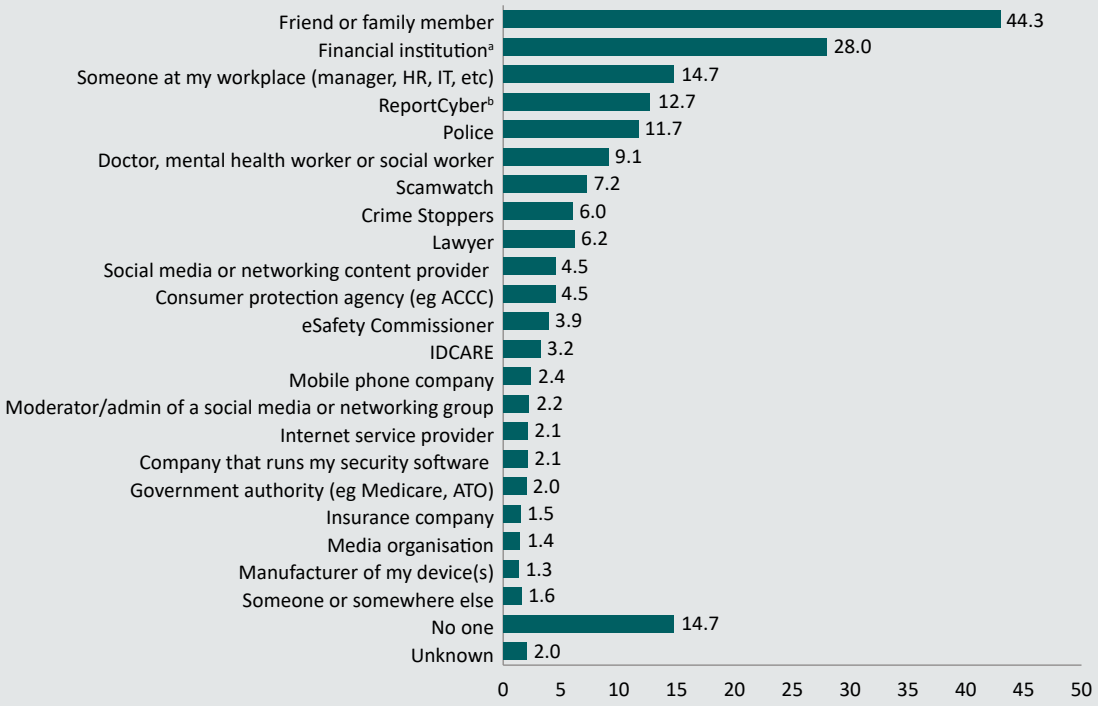
b: Respondents were asked whether they had sought help from ReportCyber, as well as cyber.gov.au, the ACSC and ACSC Hotline

Note: Excludes 14 victims who did not answer questions about the most recent incident. Weighted frequencies and percentages may not add to total due to rounding. Respondents could select multiple methods of reporting the most recent incident

Source: Australian Cybercrime Survey 2024 [weighted data]

Similarly, a large proportion of fraud and scam victims reported the incident to a financial institution such as a bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal; 28.0%; Figure 13). Victims also commonly told a family member or friend (43.0%); someone at their workplace, such as a manager, human resources or IT support staff (14.7%); or ReportCyber (12.7%). Fifteen percent of victims stated that they had not told anyone about the incident.

Figure 13: Help-seeking among fraud and scam victims following the most recent incident (%) (*n*=979)



a: Financial institution=bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)

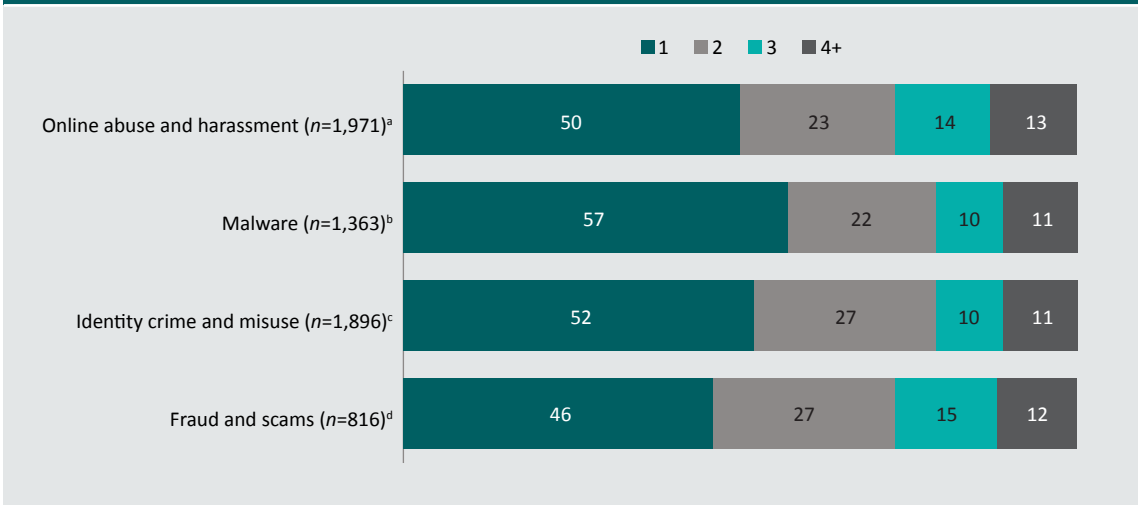
b: Respondents were asked whether they had sought help from ReportCyber, as well as cyber.gov.au, the ACSC and ACSC Hotline

Note: Excludes 6 victims who did not answer questions about the most recent incident. Weighted frequencies and percentages may not add to total due to rounding. Respondents could select multiple methods of reporting the most recent incident

Source: Australian Cybercrime Survey 2024 [weighted data]

Many victims sought assistance from more than one source following the most recent incident of cybercrime (Figure 14). Among victims who sought help from anyone, 50 percent of online abuse and harassment victims, 43 percent of malware victims, 48 percent of identity crime victims and 54 percent of fraud and scam victims sought help from more than one source.

Figure 14: Number of sources of help, advice and support among victims who sought help following the most recent incident (%)



a: Excludes 699 online abuse and harassment victims who did not seek help from anyone, 46 victims who did not answer questions about the most recent incident, and 49 victims who did not know or declined to answer this question

b: Excludes 703 malware victims who did not seek help from anyone, 21 victims who did not answer questions about the most recent incident and 41 victims who did not know or declined to answer this question

c: Excludes 309 identity crime and misuse victims who did not seek help from anyone, 14 victims who did not answer questions about the most recent incident, and 42 victims who did not know or declined to answer this question

d: Excludes 144 fraud and scam victims who did not seek help from anyone, 6 victims who did not answer questions about the most recent incident, and 20 victims who did not know or declined to answer this question

Note: Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Seeking help and reporting to police or to ReportCyber

A major focus of the ACS is on help-seeking from police agencies and via the ReportCyber platform. ReportCyber is a national online system that allows individuals, small businesses and other organisations to securely report instances of cybercrime. These reports can then be forwarded to the most applicable law enforcement agency. According to the latest assessment, a report is submitted to ReportCyber every six minutes (Australian Signals Directorate 2024).

While the survey asks about both police and ReportCyber, it should be noted that police agencies ask victims of cybercrime to report the crime to ReportCyber. Likewise, the ReportCyber platform makes clear to users they will be reporting a cybercrime to police through ReportCyber. For this reason, it is difficult to distinguish between these reporting options, and much of the analysis that follows aggregates the results (noting that some victims may say they reported to police and ReportCyber).

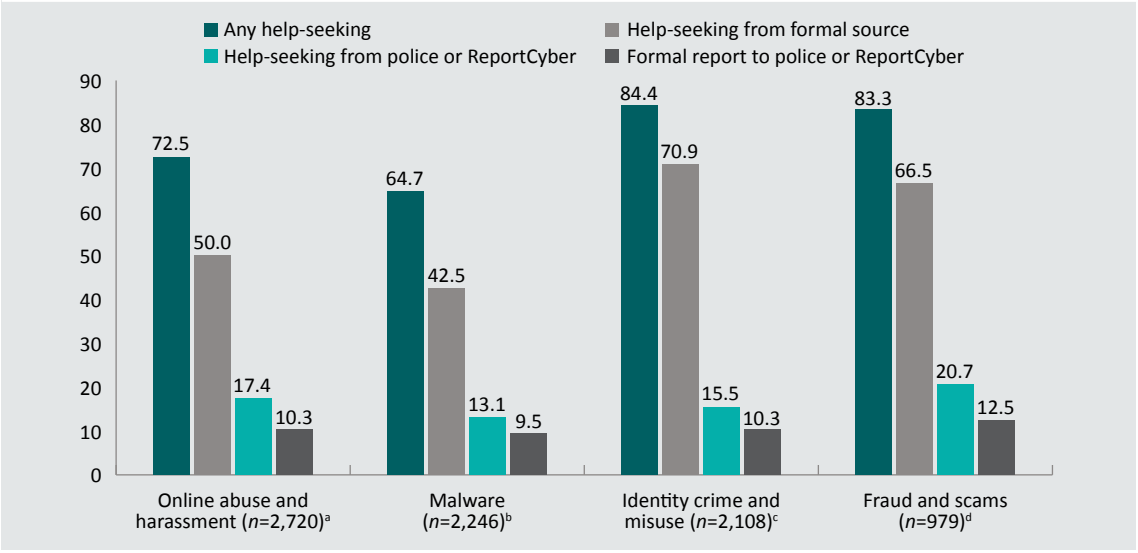
As mentioned in the *Introduction*, we made an important change to how we collect and report information on help-seeking from police and ReportCyber. Respondents who said they sought help, advice or support from police or ReportCyber were then asked whether they had submitted an official report. An official report was defined as one where the respondent would have received some acknowledgement that the incident had been recorded (eg a confirmation screen or email, report number etc). This could be submitted online, over the phone or in person.

We report both the proportion of victims who sought help, advice or support and the proportion of victims who made an official report following the most recent incident. The questions that follow about outcomes from reporting and satisfaction are also limited to victims who made an official report. We are cautious about comparing the results from 2024 and 2023 because of this methodological change.

As shown in Figure 15, formal help-seeking (ie seeking help from someone other than a family member or friend) was higher among identity crime victims (70.9%) and fraud and scam victims (66.5%) than online abuse and harassment victims (50.0%) and malware victims (42.5%). This likely reflects the large proportion of identity crime and fraud and scam victims reporting to financial institutions (44.5% and 28.2%, respectively).

One in five fraud and scam victims sought help, advice or support from the police or ReportCyber (20.7%) and over half of these victims went on to make an official report (12.5%). Online abuse and harassment victims were the next most likely to have sought help, advice or support from the police or ReportCyber (17.4%) and make an official report (10.3%). Nearly one in six identity crime and misuse victims (15.5%) sought help, advice or support from the police or ReportCyber, and just over one in 10 made an official report (10.3%). Malware victims were the least likely to seek help, advice or support from the police or ReportCyber (13.1%) and to make an official report (9.5%).

Figure 15: Help-seeking following the most recent incident, by crime type (%)



a: Excludes 46 victims who did not answer questions about the most recent incident. Denominator includes 49 victims who did not know or declined to answer this question. Denominator for making an official report to police or ReportCyber includes an additional 27 victims who did not know or declined to answer this question

b: Excludes 21 victims who did not answer questions about the most recent incident. Denominator includes 41 victims who did not know or declined to answer this question. Denominator for making an official report to police or ReportCyber includes an additional 8 victims who did not know or declined to answer this question

c: Excludes 14 victims who did not answer questions about the most recent incident. Denominator includes 42 victims who did not know or declined to answer this question. Denominator for making an official report to police or ReportCyber includes an additional 17 victims who did not know or declined to answer this question

d: Excludes 6 victims who did not answer questions about the most recent incident. Denominator includes 20 victims who did not know or declined to answer this question. Denominator for making an official report to police or ReportCyber includes an additional 17 victims who did not know or declined to answer this question

Note: Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Box 6: Better estimating the extent of unreported cybercrime

The previous report in this series, *Cybercrime in Australia 2023* (Voce & Morgan 2023a), used the prevalence of help-seeking from police or ReportCyber to estimate the under-reporting of cybercrime. This analysis produced multipliers which could be applied to the number of recorded cybercrime incidents to estimate the total number of incidents impacting Australian computer users. In that report, we acknowledged that the data were not based on official reports to police or ReportCyber, and that this was a limitation.

Because the 2024 survey asked specifically about official reports, we have calculated new multipliers that are likely to better reflect the extent of under-reporting:

- Since 10.3 percent of online abuse and harassment victims made an official report to police or ReportCyber, the true number of online abuse and harassment incidents involving unique victims will be at least 9.7 times the number recorded by ReportCyber.
- Since 9.5 percent of malware victims made an official report to police or ReportCyber, the true number of malware incidents involving unique victims will be at least 10.5 times the number recorded by ReportCyber.
- Since 10.3 percent of identity crime victims made an official report to police or ReportCyber, the true number of identity crime incidents involving unique victims will be at least 9.7 times the number recorded by ReportCyber.
- Since 12.5 percent of fraud and scam victims made an official report to police or ReportCyber, the true number of fraud and scam incidents involving unique victims will be at least 8.0 times the number recorded by ReportCyber.

We know there are important differences between incidents that are and are not reported to police and ReportCyber, including the value of financial losses (see *Impacts of victimisation* section on page 68) and harm experienced by victims (see Voce & Morgan 2025). We therefore know that reported incidents are not representative of all incidents. Nevertheless, other than for malware (see Box 7 on page 65), these multipliers are larger than they were in the previous report. This further reinforces that the large number of incidents captured by official reports is a significant underestimate of the true scale of cybercrime impacting online Australians.

In addition to asking respondents whether they had made an official report to police or to ReportCyber, we also asked respondents whether they had made an official report to Scamwatch (for crime types other than malware) or to the e-Safety Commissioner (for online abuse and harassment only):

- 2.0 percent of online abuse and harassment victims, 3.1 percent of identity crime and misuse victims, and 4.7 percent of online fraud and scam victims said they made an official report to Scamwatch following the most recent incident.
- 1.4 percent of online abuse and harassment victims said they made an official report to the e-Safety Commissioner following the most recent incident.

Official reporting to police and ReportCyber among select groups of respondents

The prevalence of respondents making an official report to police or ReportCyber following the most recent incident was analysed according to sociodemographic characteristics and business ownership status (Table 17). Several key findings emerged about who was more likely to make an official report:

- younger victims were more likely than older victims to make an official report for all types of cybercrime;
- male victims were more likely than female victims to make an official report to police or ReportCyber for online abuse and harassment, malware and identity crime and misuse;
- First Nations victims were more likely than non-Indigenous victims to make an official report to police or ReportCyber for online abuse and harassment, malware and identity crime and misuse;
- victims who were born overseas were less likely than victims born in Australia to make an official report to police or ReportCyber for online abuse and harassment, malware and identity crime and misuse;
- victims with a restrictive health condition were less likely than other victims to make an official report to police or ReportCyber for malware;
- victims who were small to medium business owners, operators and managers were more likely to make an official report to police or ReportCyber for all types of cybercrime than victims who were small to medium business employees or who were working but not for a small to medium business; and
- Victims who were large company owners and executives were less likely to make an official report to police or ReportCyber for malware and identity crime and misuse than victims who were employed in a large company or who were working somewhere other than a large company.

Table 17: Respondents who made an official report to police or ReportCyber, by sociodemographic characteristics (%)

	Online abuse and harassment	Malware	Identity crime and misuse	Fraud and scams
Age				
18–24 (*n*=426)	10.9***	7.7***	12.4***	17.5*
25–34 (*n*=578)	15.4	14.2	13.5	10.5
35–49 (*n*=688)	12.7	14.8	15.3	16.9
50–64 (*n*=508)	7.3	3.9	7.2	12.3
65+ (*n*=442)	4.6	4.0	3.8	7.5
Gender				
Female (*n*=5,183)	9.0*	5.8***	8.5**	11.2
Male (*n*=5,086)	12.1	13.4	12.6	14.7
First Nations				
Yes (*n*=420)	28.9***	24.9***	28.9***	12.1
No (*n*=9,741)	9.3	8.7	9.2	13.3
LGB+				
Yes (*n*=947)	9.7	6.3	11.0	10.3
No (*n*=9,215)	10.8	10.2	10.4	13.2
Born outside of Australia				
Yes (*n*=2,302)	10.4	5.1***	7.8*	11.1
No (*n*=7,980)	10.7	11.2	11.4	13.4
Restrictive long-term health condition				
Yes (*n*=1,140)	10.1	6.4***	9.9	13.0
No (*n*=8,708)	10.9	14.3	11.2	13.5
Owns, operates or works for a small to medium enterprise (SME)				
Owner or manager (*n*=1,532)	16.5**	18.2***	18.5***	17.6***
Employee (*n*=1,789)	12.2	12.9	10.5	7.4
Works but not at an SME (*n*=3,279)	9.5	8.6	9.8	16.6
Owns, operates or works for a large company or business				
Owner or executive (*n*=462)	9.7	6.7*	6.0**	12.2
Employee (*n*=1,840)	9.6	10.5	8.6	14.1
Works but not at a large company (*n*=4,268)	13.8	14.0	14.6	14.5

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$

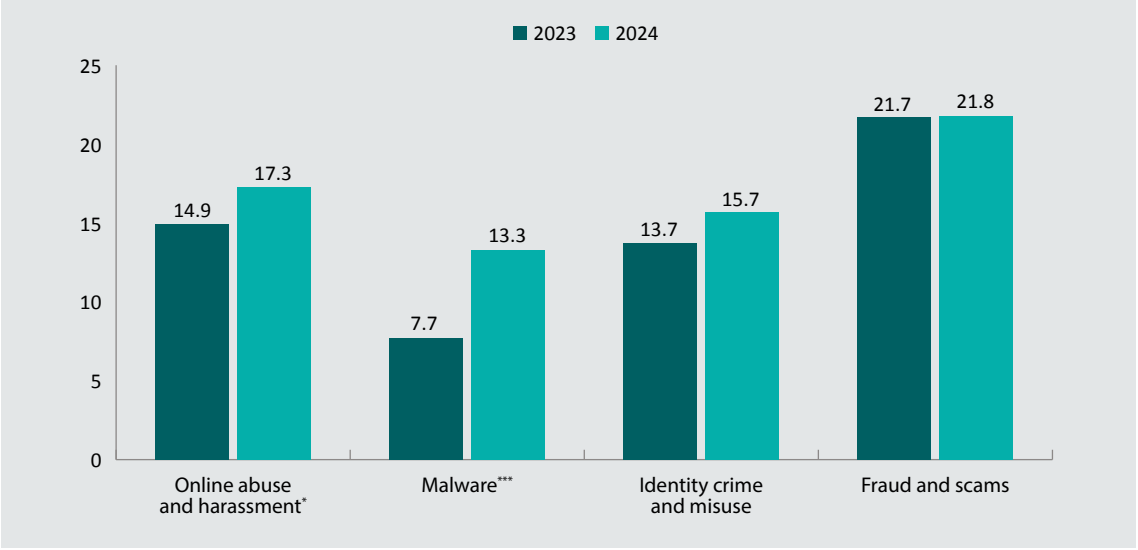
Note: Excludes respondents who did not state whether they made an official report to police or to ReportCyber. Also excludes respondents who declined to provide information about their sociodemographic characteristics. These numbers vary by crime type. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Changes in help-seeking behaviour

We compared the proportion of victims who sought help, advice or support from police or ReportCyber in 2023 and 2024 (Figure 16). We limited this analysis to victims of crime types for which we asked consistent questions in both years. The proportion of victims who sought help from police or ReportCyber increased for online abuse and harassment (14.9% in 2023 vs 17.3% in 2024; $F(1, 24197)=4.60$, $p<0.05$) and for malware attacks (7.7% in 2023 vs 13.3% in 2024; $F(1, 24186)=35.88$, $p<0.001$). There was no statistically significant change in the proportion of victims who sought help, advice or support from police or ReportCyber for identity crime and misuse (13.7% in 2023 vs 15.7% in 2024) or fraud and scams (21.7% in 2023 vs 21.8% in 2024).

Figure 16: Help-seeking from police or ReportCyber following the most recent incident, 2023 and 2024 (%)



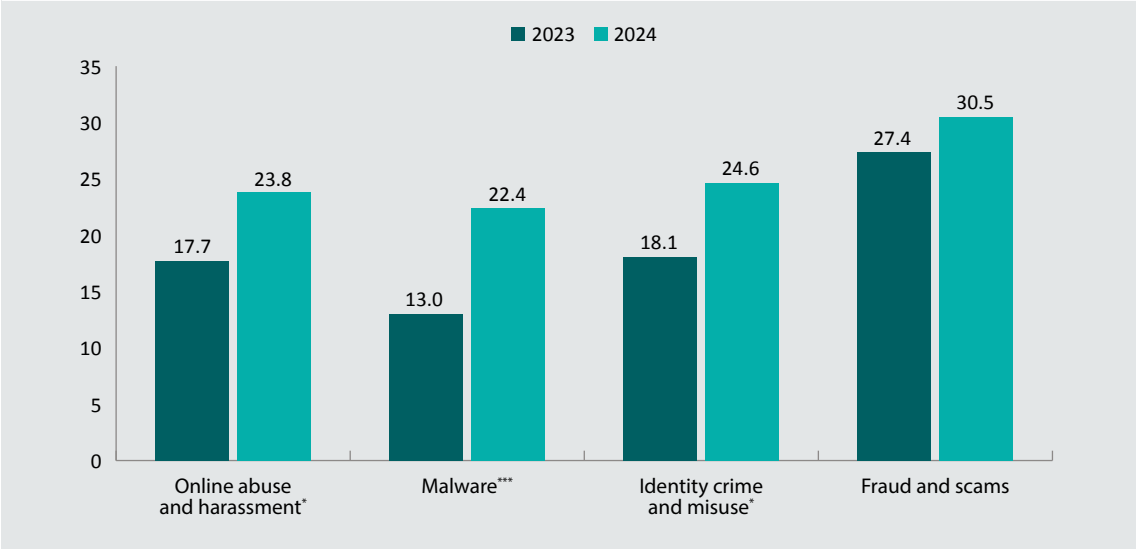
***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$

Note: Denominator includes respondents who did not state whether they sought help, advice or support from police or ReportCyber. These numbers vary by crime type and survey year. Figures for help-seeking from the police or ReportCyber for 2024 do not align with those presented in Figure 15 because this analysis was limited to victims of crime types for which consistent questions were asked in both years. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

We then repeated the analysis for small to medium business owners, operators and managers who were the victims of cybercrime (Figure 17). We again limited the analysis to victims of crime types we asked about consistently in both years. An increasing proportion of small to medium business owners sought help, advice or support from police or ReportCyber for online abuse and harassment (17.7% in 2023 vs 23.8% in 2024; ($F(1, 24215)=5.07$, $p<0.05$); malware attacks (13.0% in 2023 vs 22.4% in 2024; $F(1, 24219)=13.02$, $p<0.001$); and identity crime and misuse (18.1% in 2023 vs 24.6% in 2024; $F(1, 24206)=4.96$, $p<0.05$). There was no statistically significant change in the proportion of small to medium business owners who sought help, advice or support from police or ReportCyber for fraud and scams (27.4% in 2023 vs 30.5% in 2024).

Figure 17: Help-seeking from police or ReportCyber among small to medium business owners, operators and managers following the most recent incident, 2023 and 2024 (%)



***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$

Note: Excludes respondents who did not state whether they sought help, advice or support from police or to ReportCyber. These numbers vary by crime type and survey year. Figures for help-seeking from the police or ReportCyber for 2024 do not align with those presented in Table 17 because this analysis was limited to victims of crime types that were asked consistently in both years. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

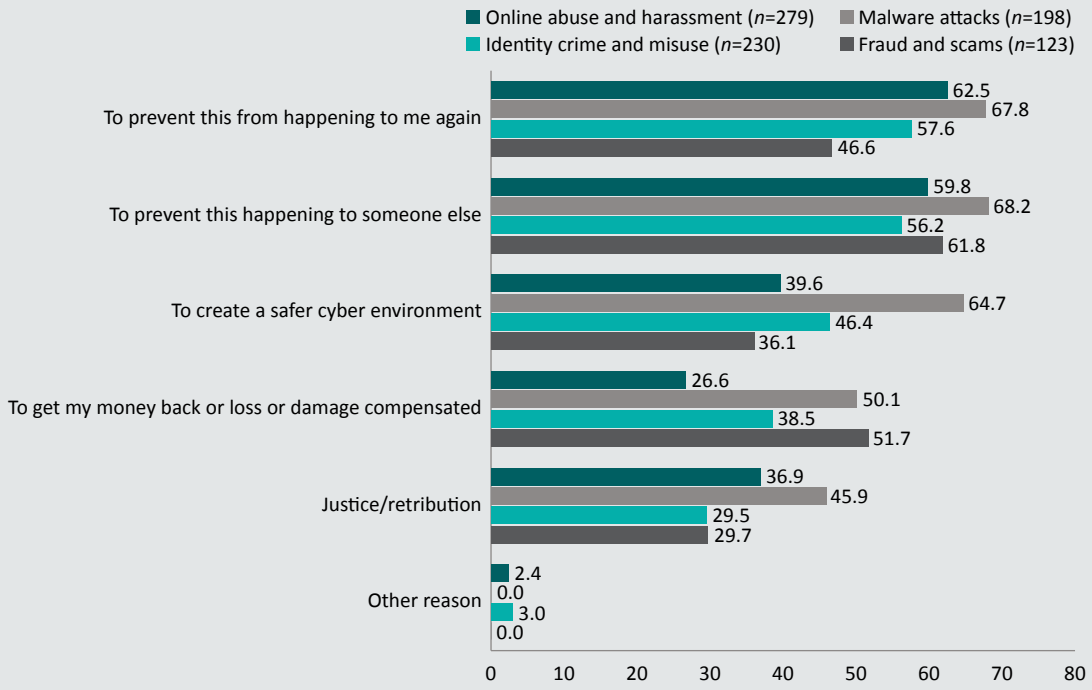
Reasons for official reporting to police or ReportCyber

Respondents who made an official report to police or ReportCyber following the most recent incident were asked about their reasons for reporting the incident, the outcomes of their report and their satisfaction with the outcome.

Across all crime types, the most common reason for reporting to police or ReportCyber was to prevent the crime from happening to them again or to someone else (Figure 18). Online abuse and harassment victims most often stated that they reported the incident to prevent it happening to them again (62.5%), followed by preventing it from happening to someone else (59.8%). Similar proportions of malware victims said they reported the incident to prevent it happening to someone else (68.2%) or to prevent it from happening to them again (67.8%). Similarly, 57.6 percent of identity crime and misuse victims said they reported the incident to stop it from happening to them again, and 56.2 percent said they reported it to prevent it from happening to someone else. Fraud and scam victims most commonly said they reported to police or to ReportCyber to prevent the crime from happening to someone else (61.8%).

Fraud and scam victims were more likely than victims of other types of cybercrime to say they were motivated by the desire to recover lost money or have damages compensated (51.7%), followed closely by malware victims (50.1%). Between 36.1 and 64.7 percent of victims said they reported the most recent incident to create a safer cyber environment. Between 29.5 and 45.9 percent of victims said they had reported the most recent incident to police or ReportCyber for justice or retribution.

Figure 18: Reasons for making an official report to police or ReportCyber following the most recent incident, by crime type (%)



Note: Respondents could nominate more than one reason for reporting the most recent incident. Excludes 1 online abuse and harassment victim, 2 malware victims and 1 identity crime and misuse victim who did not know or declined to answer the question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Outcomes of official reports to police or ReportCyber

Outcomes of reporting to police or ReportCyber ranged from not having heard anything following their report and not knowing what happened, through to being told by police that someone had been arrested, charged or prosecuted for the crime (Figure 19). The focus here is on what victims perceive as the outcome—the actual outcome recorded by police may differ. This was limited to respondents who made an official report to police or ReportCyber (and these findings are therefore not comparable to those in the previous report).

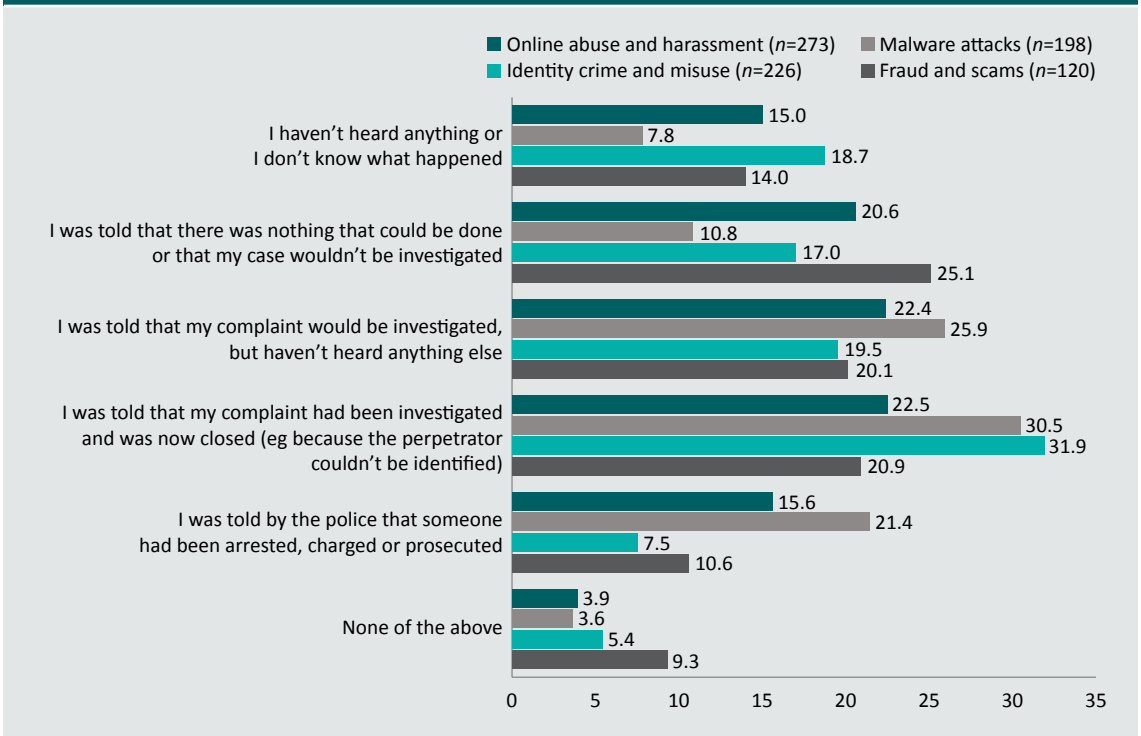
Over one-third of online abuse and harassment victims (35.6%) had not heard anything or did not know what happened with their report, or were told that nothing could be done or that the case would not be investigated. Sixty-one percent of victims said they were told their complaint would be or had been investigated, with 15.6 percent having been told by the police that someone had been arrested, charged or prosecuted.

The majority of malware victims were also told their complaint would be or had been investigated (77.8%), with these victims most commonly being told their case had been investigated and had been closed without an offender being apprehended (30.5%). However, a relatively high proportion were told by the police that someone had been arrested, charged or prosecuted (21.4%).

Identity crime and misuse victims were the most likely to be told their case had been investigated and had been closed without an offender being apprehended (31.9%), with the next most common outcomes being that they were told that nothing could be done or that the case would not be investigated (19.5%).

Half of all fraud and scam victims (51.6%) were told that their case would be or had been investigated, with 20.9 percent told their case had been investigated and had been closed without an offender being apprehended and 10.6 percent being told by the police that someone had been arrested, charged or prosecuted.

Figure 19: Outcomes of reporting among victims who reported the most recent incident to police or ReportCyber, by crime type (%)



Note: Excludes 7 online abuse and harassment victims, 2 malware victims, 5 identity crime and misuse victims and 3 fraud and scam victims who did not know or declined to answer the question. Weighted frequencies and percentages may not add to total due to rounding

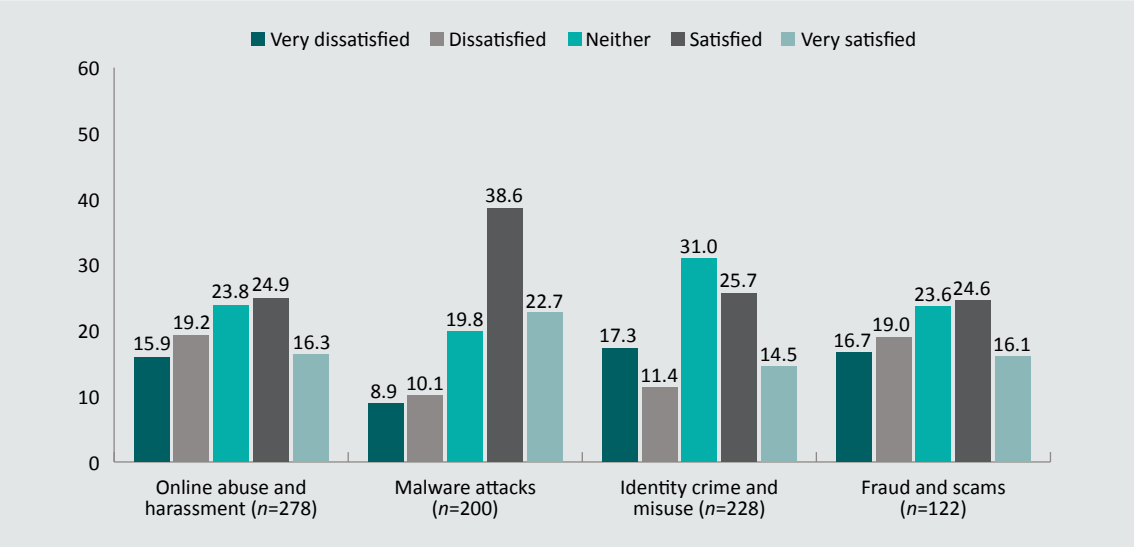
Source: Australian Cybercrime Survey 2024 [weighted data]

Victims who made an official report to police or to ReportCyber following the most recent incident were more likely to be satisfied than dissatisfied with the outcome of their report:

- 35.1 percent of online abuse and harassment victims were dissatisfied or very dissatisfied with the outcome of their report, while 41.2 percent were satisfied or very satisfied with the outcome;
- 19.0 percent of malware victims were dissatisfied or very dissatisfied with the outcome of their report, while 61.3 percent were satisfied or very satisfied with the outcome;
- 28.7 percent of identity crime and misuse victims were dissatisfied or very dissatisfied with the outcome of their report, while 40.2 percent were satisfied or very satisfied with the outcome; and
- 35.7 percent of fraud and scam victims were dissatisfied or very dissatisfied with the outcome of their report, while 40.7 percent were satisfied or very satisfied with the outcome (Figure 20).

The remaining victims were neither satisfied nor dissatisfied with the outcome of the report. This ranged from 19.8 percent for malware victims, to 31.0 percent for identity crime and misuse victims.

Figure 20: Satisfaction with the outcome among victims who made an official report to police or ReportCyber, by crime type (%)



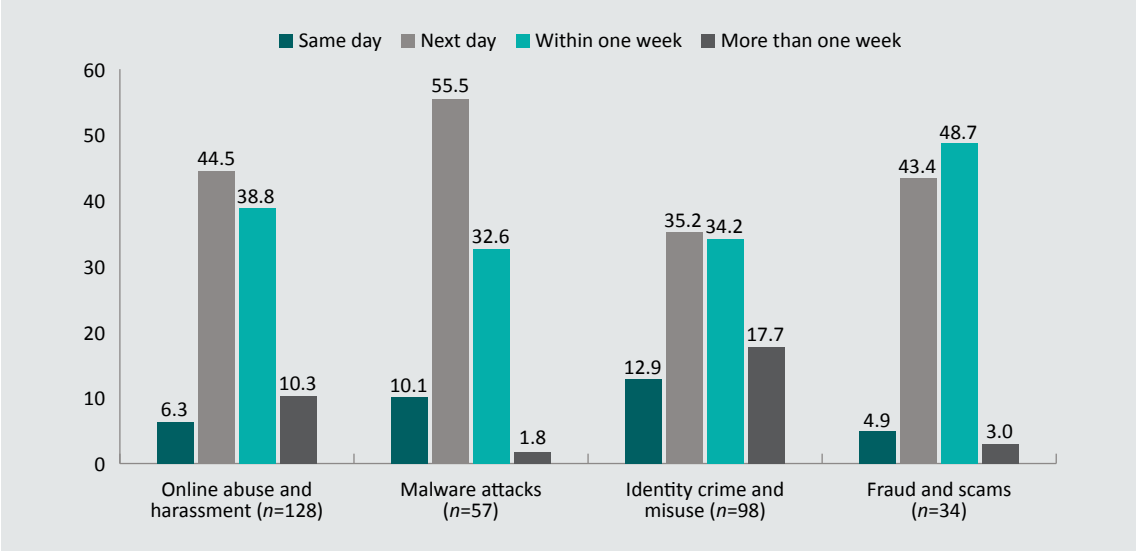
Note: Excludes 3 online abuse and harassment victims and 3 identity crime and misuse victims who did not know or declined to answer the question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Time between cybercrime incidents and official reporting

Victims were asked the number of days between the most recent incident occurring and them making an official report to the police or ReportCyber. Because victims could report to one or both of police and ReportCyber, this question was asked separately for each. The results were similar for police (Figure 21) and ReportCyber (Figure 22). It was most common for victims to say they reported the incident to police the day after it occurred for online abuse and harassment (44.5%), malware (55.6%) and identity crime and misuse (35.2%). Reporting the incident within a week was most common for fraud and scam victims (48.7%). Turning to ReportCyber, victims most commonly reported within a week, including online abuse and harassment victims (48.0%) identity crime and misuse victims (47.3%) and fraud and scam victims (49.9%). Malware victims most often reported the day after the incident (55.6%).

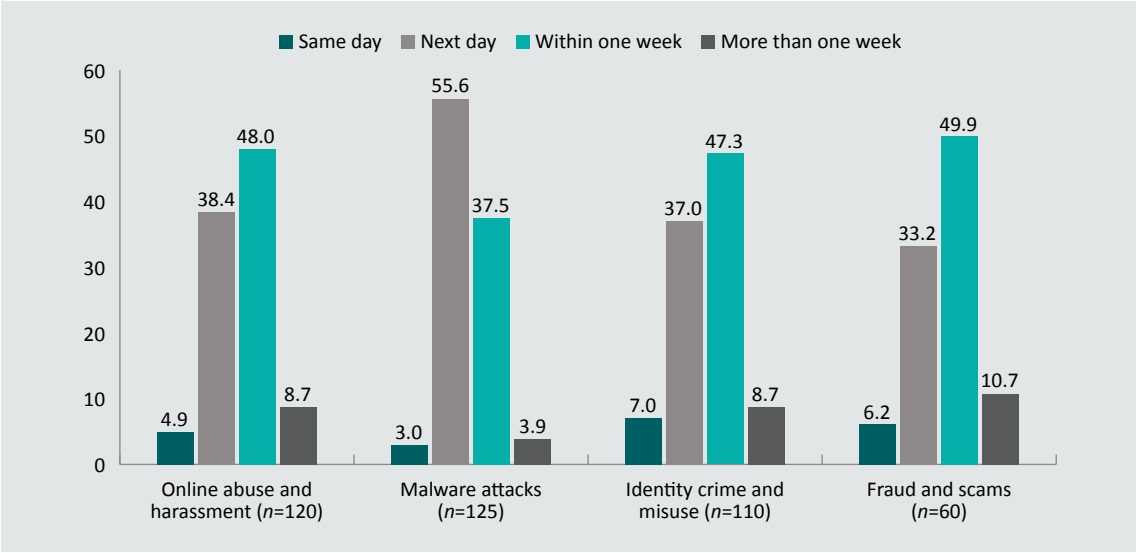
Figure 21: Length of time taken to submit a report to police following the most recent incident, by crime type (%)



Note: Excludes 27 online abuse and harassment victims, 19 malware victims, 21 identity crime and misuse victims and 15 fraud and scam victims who did not know or declined to answer the question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Figure 22: Length of time taken to submit a report to ReportCyber following the most recent incident, by crime type (%)



Note: Excludes 36 online abuse and harassment victims, 27 malware victims, 28 identity crime and misuse victims and 23 fraud and scam victims who did not know or declined to answer the question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Box 7: Malware reporting, outcomes and satisfaction

A number of noteworthy findings regarding malware victims in this section warranted further analysis. Specifically, malware victims were more likely to say they reported to police or ReportCyber within a day of the incident, to say they reported the incidents for altruistic reasons, to say that action had been taken against an offender following the most recent incident, and to say that they were satisfied with the outcome of reporting the incident. There was also an increase from 2023 to 2024 in the proportion of malware victims who sought help, advice or support from police or ReportCyber following the most recent incident.

These findings are unexpected for several reasons. For one, malware incidents tend to be less serious than other cybercrime types, in terms of both financial losses and non-financial harms. Advice from law enforcement suggests that malware offenders are less likely to have action taken against them than other cybercrime offenders. Malware victimisation can also be difficult to differentiate from other explanations for device disruption.

There are several possible explanations for these findings. Malware victims may have had lower expectations of what would happen if they reported to police or ReportCyber, which might explain the higher rates of satisfaction (see Morgan et al. 2016). Malware victims who sought help were more likely than those who did not to say they experienced poly-victimisation, so it is possible that malware was related to other forms of cybercrime, such as certain forms of stalking and harassment involving an intimate partner, where the offender may be more likely to be apprehended (because they are known to the victim).

There is no obvious explanation for these findings. Malware has arguably received less research attention in terms of victim experiences than the other types of cybercrime measured by the ACS—research that may help to better understand the experiences of malware victims who responded to the ACS.

Reasons for not reporting to police or ReportCyber

Respondents who did not make an official report to police or ReportCyber following the most recent incident were asked their reasons for not doing so (Table 18).

Overall, scam and fraud victims were the least likely to say that they did not report because they did not perceive the incident to be serious enough (38.0%). Larger proportions of online abuse victims (61.9%) and malware victims (58.8%) gave this reason. But scam and fraud victims were the most likely to cite reasons relating to their understanding, perceptions or past experiences of reporting (55.1%) and worry about the reaction to or consequences of making a report (37.3%).

The most common reason victims did not report to police or ReportCyber was that they felt they could deal with it themselves; however, this was less common among fraud and scam victims (20.3%) than among victims of online abuse and harassment (34.7%), malware (30.5%) and identity crime (29.4%). For online abuse and harassment (31.8%) and malware (26.2%) victims, the next most common reason was they did not regard the incident as a serious offence. This was much less common among fraud and scam victims (15.6%).

Importantly, a significant proportion of online abuse and harassment victims (17.0%), malware victims (14.8%), identity crime and misuse victims (24.3%) and fraud and scam victims (22.0%) who did not seek help from police or ReportCyber following the most recent incident did not know that this was an option. Similar proportions of victims did not think the police or ReportCyber would be able to do anything. Between 14.9 and 19.6 percent of victims did not know how or where to report the matter. It was rare for victims who did not seek help to say the reason for not reporting was dissatisfaction with previous reporting outcomes (5.7%–8.9% of victims) or that they did not trust the police or ReportCyber (3.5%–5.4%). Notably, fraud and scam victims were much more likely to say the reason for not reporting was that they felt ashamed or embarrassed (15.4%) compared to victims of the other cybercrime types (4.4%–8.3%).

Table 18: Reasons for not reporting to police or ReportCyber, by crime type (%)

	Online abuse and harassment (*n*=2,296)	Malware (*n*=1,751)	Identity crime (*n*=1,869)	Fraud and scams (*n*=800)
Seriousness of the incident				
Felt they could deal with it themselves	34.7	30.5	29.4	20.3
Did not regard the incident as a serious offence	31.8	26.2	18.3	15.6
Did not know or think the incident was a crime	16.2	16.9	7.0	9.9
Any of the above	*61.9*	*58.8*	*46.8*	*38.0*
Understanding, perceptions or past experience of reporting				
Did not know reporting to the police or ReportCyber was an option	17.0	14.8	24.3	22.0
Did not think the police or ReportCyber would be able to do anything	19.3	14.2	20.8	23.5
I did not know how or where to report the matter	14.9	15.8	16.7	19.6
Have reported before and been dissatisfied with the outcome	6.3	5.7	6.4	8.9
Did not trust the police or ReportCyber	5.0	3.5	4.5	5.4
Any of the above	*43.5*	*39.6*	*51.8*	*55.1*

Table 18: Reasons for not reporting to police or ReportCyber, by crime type (%) (cont.)

	Online abuse and harassment (*n*=2,296)	Malware (*n*=1,751)	Identity crime (*n*=1,869)	Fraud and scams (*n*=800)
Worry about the reaction to or consequences of reporting				
Did not want to ask for help	10.5	8.3	5.5	6.8
Felt ashamed or embarrassed	8.3	4.4	4.9	15.4
Felt I would not be believed	6.5	5.2	3.8	6.0
Fear of legal processes	4.7	4.1	3.4	5.7
Fear of the person responsible (eg fear of retaliation)	8.2	4.3	2.9	6.3
Did not want the person responsible arrested	4.6	2.7	1.8	3.4
Cultural or language reasons	2.2	2.2	2.0	4.2
Any of the above	*30.0*	*24.7*	*18.7*	*37.3*
Incident handled by someone else				
Workplace/on-the-job incident—internal reporting procedures followed	3.9	4.6	2.7	4.0
Provider (eg bank, telecommunications company) involved in incident was resolving or had resolved the matter	0.5	0.3	6.3	0.8
Any of the above	*4.4*	*4.9*	*8.9*	*4.8*
Other reason	2.7	3.3	2.6	2.6

Note: Excludes 27 online abuse and harassment victims, 8 malware victims, 17 identity crime and misuse victims and 17 fraud and scam victims who did not know or declined to answer the question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Impacts of victimisation

Financial losses

Victims were asked whether they had directly lost money because of the most recent incident (Table 19). Online abuse and harassment victims were asked if the perpetrator(s) demanded money to resolve the most recent incident (for example, demanding money to stop the release of intimate images, to stop the release of personal information, to give control of an account back to the victim or to take down fake profiles). The crime type with the highest proportion of victims reporting financial losses was fraud and scams (29.8%), followed by identity crime (28.7%). Financial losses were relatively uncommon for online abuse and harassment victims (3.4%) and malware victims (7.6%), with less than 10 percent reporting that they had money directly stolen or lost in the most recent incident. Around 33 percent of malware victims who lost money or had money stolen said the most recent incident involved ransomware (with or without encryption), despite these respondents accounting for only 19.2 percent of malware victims.

Victims were then asked if they had spent money dealing with the consequences of the most recent incident, such as by getting legal advice, taking time off work, or installing new software. Thirteen percent of online abuse and harassment victims, 12.4 percent of malware victims, 10.4 percent of identity crime victims and 18.3 percent of fraud and scam victims lost money dealing with the consequences.

Finally, victims were asked whether any of the money they had directly lost was reimbursed by banks or other organisations, or recovered in other ways. Two percent of online abuse and harassment victims, 2.2 percent of malware victims, 18.5 percent of identity crime victims and 9.0 percent of fraud and scam victims were reimbursed for the money they lost as a direct result of their victimisation.

Table 19: Money lost, money spent on consequences and money recovered following most recent incident of cybercrime, by crime type

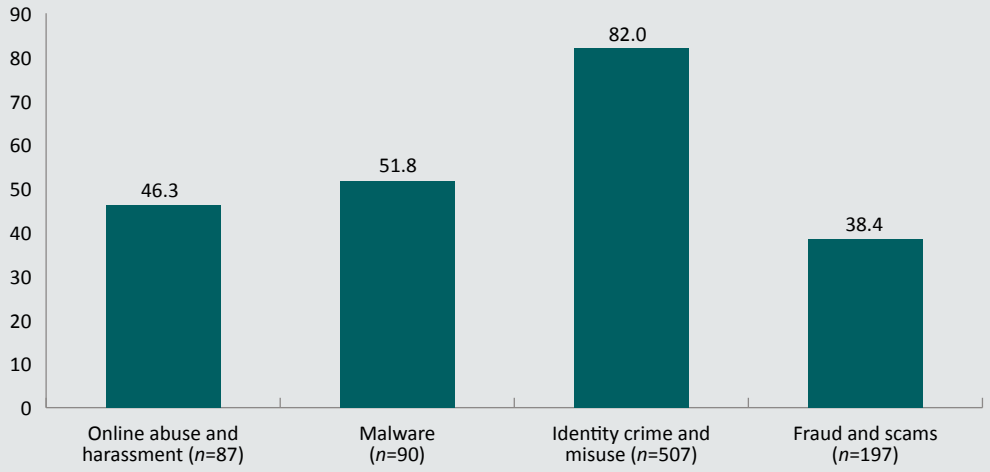
	Online abuse and harassment (*n*=2,720)	Malware (*n*=2,108)	Identity crime (*n*=2,246)	Fraud and scams (*n*=979)
Victims who stated they lost money directly	93 (3.4%)	159 (7.6%)	646 (28.7%)	292 (29.8%)
Victims who could report how much they lost	93 (3.4%)	91 (4.3%)	520 (23.2%)	210 (29.5%)
Victims who stated that they spent money on consequences	361 (13.3%)	262 (12.4%)	233 (10.4%)	180 (18.3%)
Victims who could report how much they spent on consequences	236 (8.7%)	189 (9.0%)	163 (7.3%)	109 (11.1%)
Victims who recovered money	46 (1.7%)	47 (2.2%)	416 (18.5%)	88 (9.0%)
Victims who could report how much they recovered	40 (1.5%)	41 (1.5%)	409 (18.2%)	76 (7.8%)

Note: Weighted frequencies and percentages may not add to total due to rounding. Excludes 46 online abuse and harassment victims, 21 malware victims, 14 identity crime and misuse victims and 6 fraud and scam victims who did not answer questions about the most recent incident

Source: Australian Cybercrime Survey 2024 [weighted data]

Not all cybercrime victims who lost money as a direct result of the incident reported being able to recover money, and those who did recover money did not necessarily recover the full amount (Figure 23). The proportion of victims who were able to recover money was lowest among victims of fraud and scams (38.4%) and highest among victims of identity crime and misuse (82.0%).

Figure 23: Prevalence of victims who recovered any money following most recent incident (%)

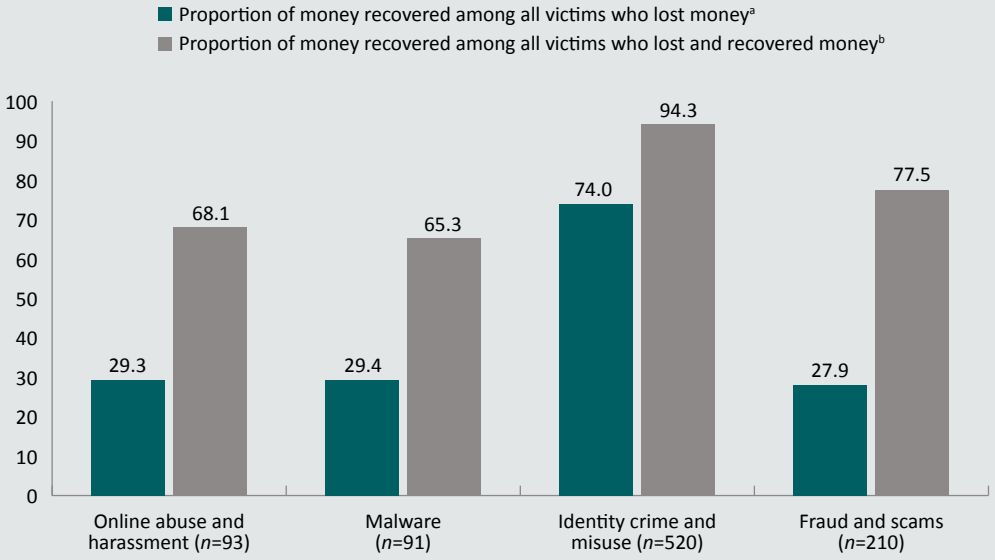


Note: Excludes 6 online abuse and harassment victims, 1 malware victim, 14 identity crime and misuse victims and 13 fraud and scam victims who did not answer whether they had recovered money. Figure only includes victims who lost money directly. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

The average proportion of money lost that was recovered was even lower (Figure 24), ranging from 27.9 percent for fraud and scams to 74.0 percent for identity crime and misuse victims. Among those victims who were able to recover money, the average proportion of money lost that was recovered ranged from 65.3 percent for malware victims to 94.3 percent for identity crime and misuse victims. These figures may exclude individuals who fell victim to cybercrime but were never actually out of pocket—for example, where a financial institution prevented payments being deducted from their account.

Figure 24: The average proportion of money recovered among people who lost money directly and who recovered money



a: Includes all victims who lost money and were able to recall the amounts, including those who did not answer whether they had recovered money

b: Limited to victims who recovered money and could report how much they recovered: online abuse and harassment *n*=40, malware *n*=41, identity crime and misuse *n*=409, fraud and scams *n*=76

Note: Figure limited to victims who lost money, and includes respondents who had $0 of financial losses because they recovered the full amount they lost

Source: Australian Cybercrime Survey 2024 [weighted data]

The median value of losses incurred by victims (through money or cryptocurrency being stolen or payments demanded) was $300 for online abuse and harassment victims, $350 for malware victims, $250 for identity crime victims and $200 for fraud and scam victims. The median amount of money lost dealing with the consequences of the most recent incident was $250 for online abuse and harassment victims, $200 for malware victims, $200 for identity crime victims and $200 for fraud and scam victims. The median amount that victims were able to recover was $100 for online abuse and harassment victims, $190 for malware victims, $250 for identity crime victims and $153 for fraud and scam victims.

The total cost per victim was calculated by summing money directly lost and money spent on consequences, then subtracting amounts recovered. The median total cost after recoveries was $300 for online abuse and harassment victims, $200 for malware victims, $200 for identity crime and misuse victims and $165 for fraud and scam victims (Table 20). The mean value was significantly higher for each type of cybercrime, ranging from $1,906 for identity crime and misuse to $10,409 for fraud and scams; however, these figures are biased by the relatively small group of victims who reported losing very large amounts of money (as shown by the large standard deviations in Table 20; see also Figure 25).

Table 20: Median financial losses for most recent incident among victims who lost any money, by payment method (range)

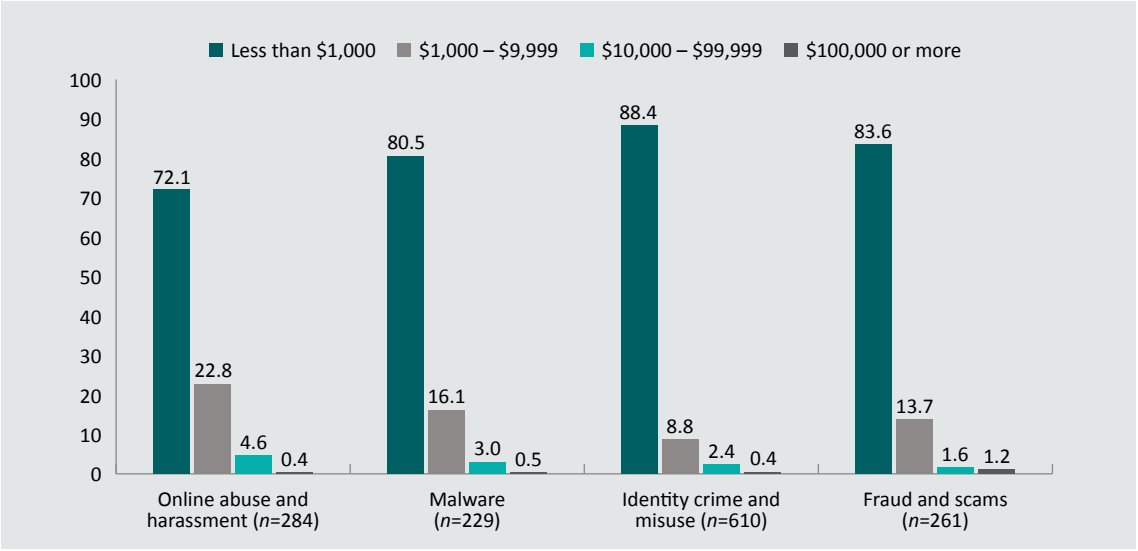
	Online abuse and harassment (*n*=2,720)	Malware (*n*=2,108)	Identity crime (*n*=2,246)	Fraud and scams (*n*=979)
Money	$200 ($10 – $21,000)	$190 ($1 – $222,200)	$230 ($1 – $800,000)	$170 ($1 – $634,000)
Cryptocurrency	$80 ($10 – 271,000)	$100 ($1 – $55,000)	$100 ($2 – $500,000)	$77 ($1 – $6,400)
Gift cards	$50 ($5 – $3,000)	$100 ($10 – $33,330)	$100 ($2 – $3,500)	$50 ($1 – $2,000)
Total losses	$300 ($10 – $292,000)	$350 ($10 – $277,750)	$250 ($1 – $800,000)	$200 ($1 – 634,000)
Median amount spent on consequences	$250 ($1 – $50,000)	$200 ($5 – 19,800)	$200 ($1 – $78,676)	$200 ($1 – $2,000,001)
Median losses from money directly lost and money spent on consequences	$300 ($1 – $317,000)	$256 ($5 – $280,750)	$255 ($1 – $800,000)	$212 ($1 – $2,000,001)
Median amount recovered	$100 ($3 – $6,000)	$190 ($3 – $188,000)	$250 ($1 – $800,000)	$153 ($2 – $634,000)
Median losses after recoveries	$300 ($0 – $317,000)	$201 ($0 – $265,750)	$200 ($0 – $500,000)	$160 ($0 – $2,000,001)
Mean losses after recoveries (*SD*)	$3,051 ($20,798)	$2,657 ($19,276)	$1,906 ($19,250)	$10,409 ($122,491)

Note: Weighted frequencies and percentages may not add to total due to rounding. Excludes 46 online abuse and harassment victims, 21 malware victims, 14 identity crime and misuse victims and 6 fraud and scam victims who did not answer questions about the most recent incident. *SD*=standard deviation

Source: Australian Cybercrime Survey 2024 [weighted data]

The variation in the total amount of money lost after recoveries is illustrated in Figure 25. This excludes victims who were unable to report how much money they had lost. Among those victims who could quantify amounts lost, between 72.1 percent (online abuse and harassment) and 88.4 percent (identity crime and misuse) reported having lost less than $1,000 in the most recent incident. Approximately one-quarter (27.8%) of online abuse and harassment victims, 19.6 percent of malware victims, 11.6 percent of identity crime victims and 16.5 percent of fraud and scam victims lost more than $1,000 in the most recent incident. Five percent of online abuse and harassment victims lost more than $10,000, compared with 2.8 percent of fraud and scam victims, 3.5 percent of malware victims and 2.8 percent of identity crime victims. A small proportion of victims, including 1.2 percent of fraud and scam victims, lost more than $100,000 in the most recent incident.

Figure 25: Financial losses after recoveries for most recent incident (%)

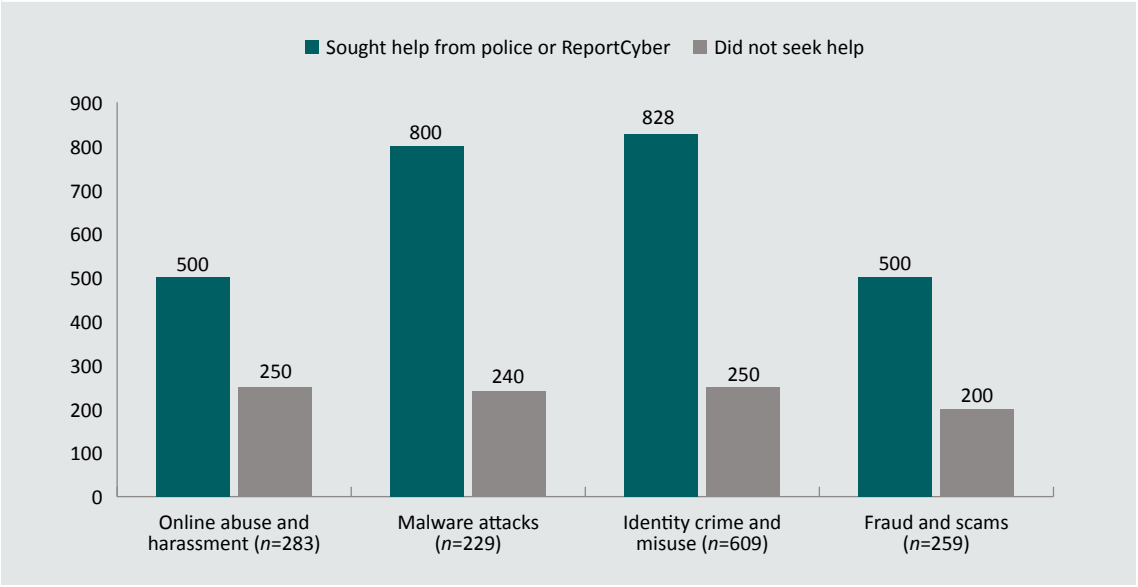


Note: The less than $1,000 category includes respondents who had $0 of financial losses because they recovered the full amount they spent or lost. Limited to victims who reported having lost money or spent money on consequences and who could recall the amounts. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

These results are different to data on the losses from reported cybercrimes (Australian Competition and Consumer Commission 2024; Australian Signals Directorate 2024). There are two main reasons for this. First, there were clear differences between the incidents that were and were not reported to police or ReportCyber in terms of the median financial losses after recoveries (Figure 26). Victims who lost money were more likely to seek help from police or ReportCyber when the amount of money lost was larger. This was especially true for identity crime and misuse victims ($828 vs $250) and malware victims ($800 vs $240). Second, the figures in this report are based on median values, which are less susceptible to bias from very large value cybercrimes. This is especially important given these data are based on all cybercrimes against victims, not only those which were reported to authorities.

Figure 26: Median financial losses before recoveries for most recent incident among victims who lost any money, by whether respondent sought help, advice or support from police or ReportCyber ($)



Note: Limited to victims who reported having lost money or spent money on consequences and who could report how much. Does not account for money recovered or reimbursed. Excludes 1 online abuse and harassment victim, 1 identity crime and misuse victim and 2 fraud and scam victims who did not know or answer the question about reporting to police or ReportCyber

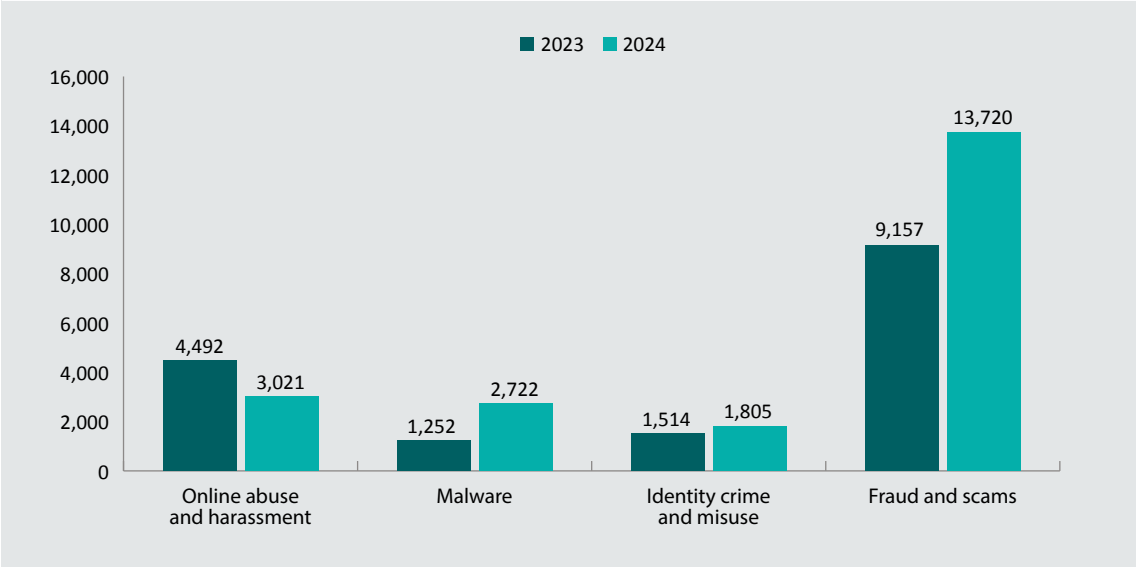
Source: Australian Cybercrime Survey 2024 [weighted data]

Finally, given the propensity of respondents who were owners, operators or managers of a small to medium businesses to have fallen victim to cybercrime in the 12 months prior to the survey, their losses were compared with those of other respondents who were working but did not own, operate or manage a small to medium business. They were more likely to have lost money or spent money on consequences than other working respondents, particularly for malware (26.1% vs 12.6%) and online abuse and harassment (24.6% vs 12.7%), but also for identity crime and misuse (38.2% vs 32.3%) and fraud and scams (45.8% vs 35.0%).

Changes in financial losses

We compared victims in 2023 and 2024 in terms of the mean losses after recoveries and whether they had recovered any money following the most recent incident (Figure 27). We limited this analysis to victims of crime types that were asked about consistently in both years. There were no statistically significant differences between 2023 and 2024 in the mean losses after recoveries for online abuse and harassment ($4,492 vs $3,021), malware attacks ($1,252 vs $2,722), identity crime and misuse ($1,514 vs $1,805) and fraud and scams ($9,157 vs $13,720).

Figure 27: Mean financial losses after recoveries for most recent incident, 2023 to 2024 ($)

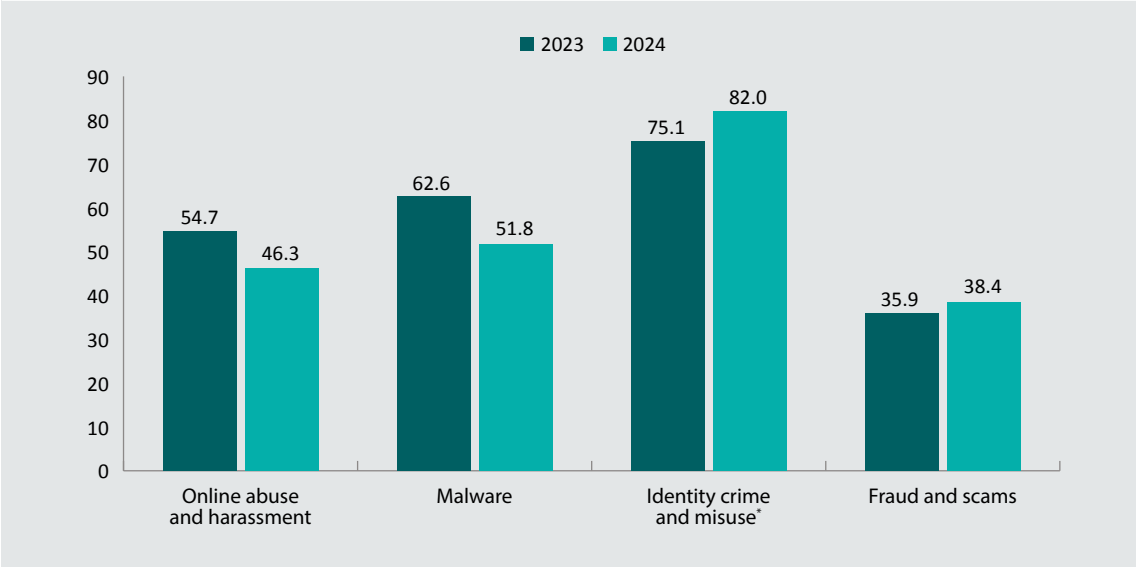


Note: Limited to victims who reported having lost money or spent money on consequences and who could report how much. These numbers vary by crime type and survey year. Figures for mean financial losses after recoveries for 2024 do not align with those presented in Table 20 because this figure is limited to victims of crime types that were asked about consistently in both years. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

There was an increase in the proportion of identity crime and misuse victims who said they recovered any of the money they lost following their most recent incident (Figure 28), from 75.1 percent in 2023 to 82.0 percent in 2024 ($F(1, 1267)=6.00$, $p<0.05$). While the proportion of online abuse and harassment (54.7% vs 46.3%) and malware attack (62.6% vs 51.8%) victims who recovered any money was lower in 2024 than in 2023, this difference was not statistically significant. Likewise, there was no difference in the proportion of fraud and scam victims who recovered money following the most recent incident (35.9% vs 38.4%). This analysis was again limited to victims of crime types that were asked about consistently in both years.

Figure 28: Proportion of victims who said that they recovered any money following the most recent incident, 2023 and 2024 (%)



*statistically significant at $p<0.05$

Note: Figure only includes victims who lost money directly. These numbers vary by crime type and survey year. The proportions of victims who said that they recovered any money following the most recent incident are different to those presented in Figure 18 because the current figure is limited to victims of crime types that were asked about consistently in both years. Weighted frequencies and percentages may not add to total due to rounding

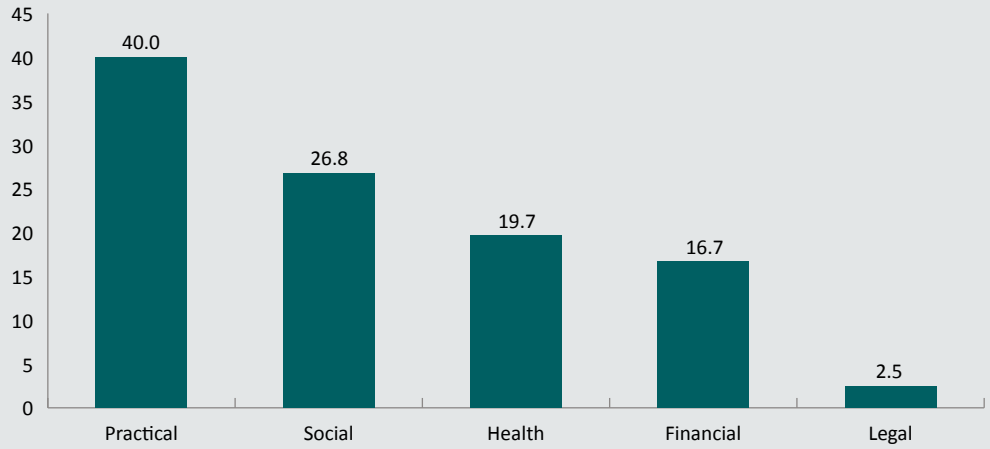
Source: Australian Cybercrime Survey 2024 [weighted data]

Impacts on individual victims

To measure the wider harms associated with cybercrime victimisation, respondents who had fallen victim to any form of cybercrime in the past year were asked about the consequences they had experienced in the 12 months prior to the survey. The survey asked about 35 items in total, grouped into five domains: practical impacts (12 items), social impacts (6 items), health impacts (7 items), financial impacts (8 items) and legal impacts (2 items).

Overall, 56.8 percent of cybercrime victims were negatively impacted in some way. This means an estimated 26.1 percent of all respondents to the survey were negatively impacted by cybercrime in the 12 months prior to the survey. Forty percent of victims reported practical impacts, over a quarter reported social impacts (26.8%), one in five reported health-related harms (19.7%), and 16.7 percent reported financial problems. Legal issues were comparatively rare (2.5%; Figure 29).

Figure 29: Harms from cybercrime among victims (%) (*n*=4,747)

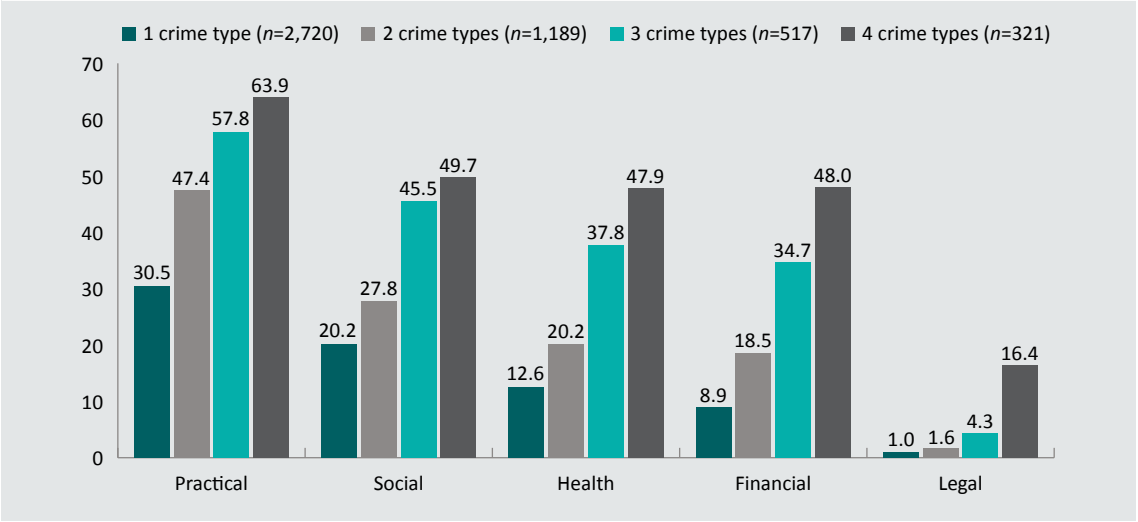


Note: Excludes 151 victims who did not answer this question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Victims who experienced more than one type of cybercrime in the 12 months prior to the survey were much more likely to report harms than those who experienced only one type (Figure 30). For example, while 30.5 percent of victims who experienced one type of cybercrime reported practical impacts, this proportion was much higher among victims who experienced three or four types of cybercrime (57.8% and 63.9% of victims, respectively). Similarly, 20.2 percent of victims who experienced one type of cybercrime reported social impacts, which rose to 49.7 for those who experienced four types of cybercrime. Across the remaining domains, victims who reported three or more types of cybercrime in the 12 months prior to the survey were at least three times more likely to report health, financial and legal impacts than victims of one cybercrime type. Whether these are repeat victims, or victims who experienced multiple, related cybercrimes as part of the one incident, there is a clear relationship between poly-victimisation and cybercrime-related harms.

Figure 30: Harms from cybercrime among victims, by number of crime types reported (%) (*n*=4,747)

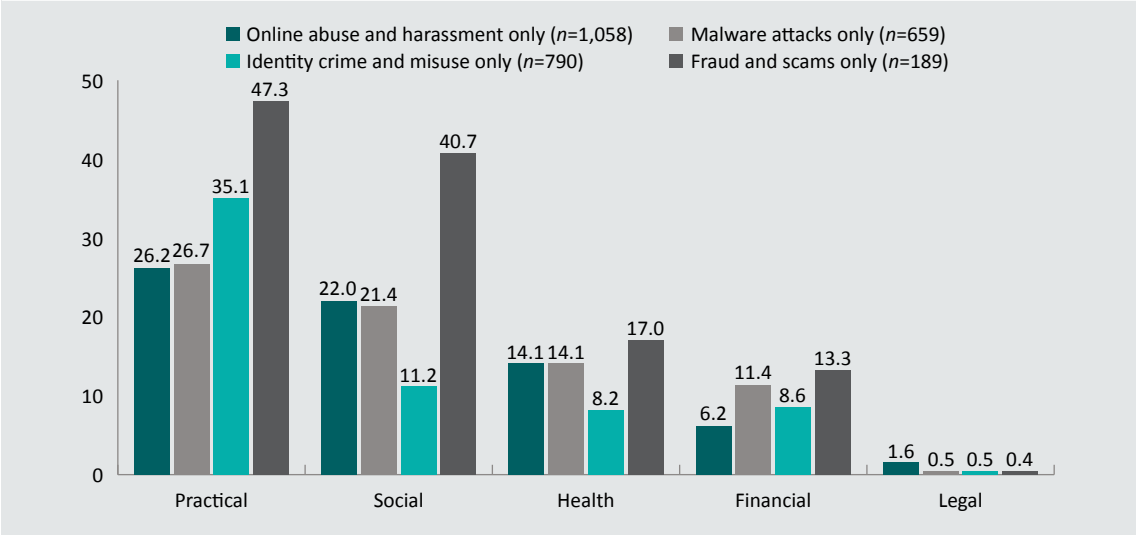


Note: Excludes 151 victims who did not answer this question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

To directly compare harm among victims of different types of cybercrime, it was necessary to limit the analysis to victims who experienced just one type of cybercrime (Figure 31). This eliminates the confounding effects of other types of cybercrime. In terms of practical and social impacts, fraud and scam victims were the most likely to report experiencing at least one harm in these domains (47.3% and 40.7%, respectively). They were also the most likely to report financial impacts (17.0%) and health impacts (13.3%). While still rare, online abuse and harassment victims were the most likely to experience legal impacts (1.6%).

Figure 31: Harms from cybercrime among victims, by crime type (%) (*n*=6,295)



Note: Excludes victims who did not answer the question about harms. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

The most common practical issues victims encountered were difficulty knowing which information to trust online (17.9%); being less confident using the internet for personal affairs (14.3%); and having to change their personal, banking and/or contact information (14.4%; Table 21). For harms within the social domain, 13.9 percent were embarrassed or had their reputation damaged, 13.0 percent of victims lost trust in other people and 4.6 percent became more socially isolated. For harms within the physical and psychological health domain, 10.4 percent of victims experienced mental or emotional distress, 8.7 percent had difficulty sleeping, and 4.5 percent stated that their physical health and wellbeing had deteriorated. For financial harms, 6.3 percent of victims experienced an increase in financial stress; 4.4 percent had to pay for computer, phone or other hardware repairs or replacement; 4.1 percent had to buy new software; and 2.8 percent had to buy new backup data storage or data storage devices. Within the legal domain, 1.9 percent of victims had to commence legal action and less than one percent had been in trouble with the police.

Table 21: Harms to individual cybercrime victims (%) (*n*=6,295)		
	n	%
Practical impacts		
Respondent found it harder to know which information to trust online	848	17.9
Respondent less confident using the internet for personal affairs (eg banking, purchasing items)	677	14.3
Respondent had to change personal, banking and/or contact information	686	14.4
Respondent's studies were negatively impacted[a]	2	2.3
Respondent had difficulty accessing online accounts and resources (eg bank accounts, utilities, email)	211	4.4
Respondent had problems communicating with people (eg friends, family, employer)	155	3.3
Respondent's work was negatively impacted[b]	80	2.5
Respondent lost important or sentimental data (eg photos, contact details, files)	123	2.6
Respondent had to take time off work to deal with the consequences of victimisation[b]	106	2.2
Respondent had problems communicating or dealing with businesses	108	2.3
Respondent had problems communicating or dealing with government departments	128	2.7
Respondent had to change their place of residence	70	1.5
Social impacts		
Respondent was embarrassed	661	13.9
Respondent lost trust in other people	618	13.0
Respondent became more socially isolated	217	4.6
Respondent stated their relationship with their partner had been negatively impacted[c]	130	2.9
Respondent stated their relationships with family and friends had been negatively impacted	150	3.2
Respondent felt their reputation was damaged	137	2.9
Health impacts		
Respondent experienced mental or emotional distress	495	10.4
Respondent experienced difficulty sleeping	412	8.7
Respondent stated their overall physical health and wellbeing had deteriorated	213	4.5
Respondent had to seek psychological or counselling treatment	115	2.4
Respondent increased their consumption of alcohol	145	3.1
Respondent had to seek medical treatment	98	2.1
Respondent increased their consumption of drugs (legal or illegal)	87	1.8

Table 21: Harms to individual cybercrime victims (%) (*n*=6,295) (cont.)		
	n	%
Financial impacts		
Respondent experienced an increase in financial stress	297	6.3
Respondent had to pay for computer, phone or other hardware repairs or replacement	208	4.4
Respondent had to buy new software	194	4.1
Respondent had to borrow money from family and friends	139	2.9
Respondent had to buy new backup data storage or data storage devices	133	2.8
Respondent was unable to get a loan when they needed one	79	1.7
Respondent increased the amount of time and/or money they spent gambling (in person or online)	77	1.6
Respondent lost their job	47	1.0
Legal impacts		
Respondent had to commence legal action	89	1.9
Respondent had been in trouble with the police	39	0.8

a: Only includes victims who were currently studying full time (*n*=56)

b: Only includes victims who were currently working (*n*=3,155)

c: Only includes victims who were in a current relationship (*n*=2,852)

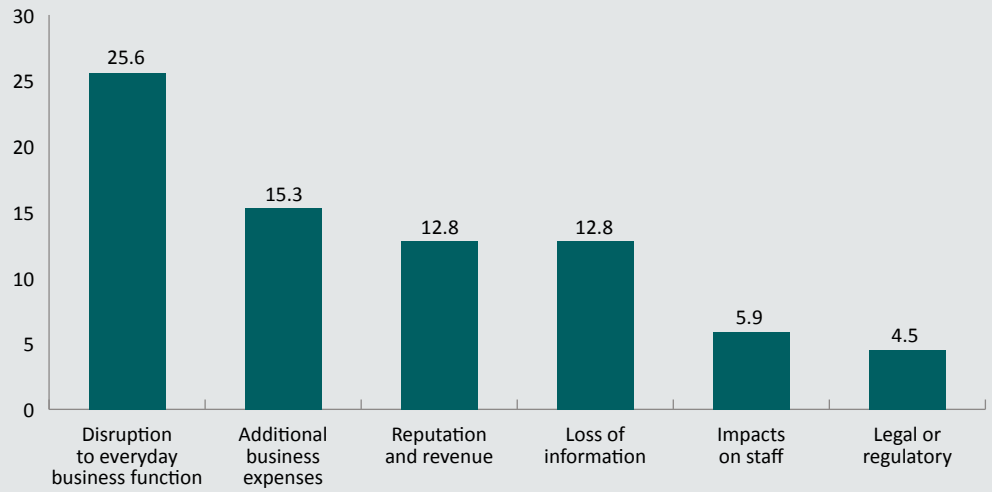
Note: Excludes 151 victims who did not answer this question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Impacts on small to medium businesses

Forty-two percent of small to medium business owners, operators or managers who had been a cybercrime victim in the past year reported at least one impact on their business. This means an estimated 22.2 percent of all small to medium business owners, operators or managers who responded to the survey had their business impacted in some way by cybercrime in the 12 months prior to the survey. These impacts include disruption to everyday business function (25.0%), additional business expenses (15.3%), impacts on their reputation or revenue (12.8%), loss of information (12.8%), impacts on staff (5.9%) and legal or regulatory ramifications (4.5%; Figure 32).

Figure 32: Harms to business from cybercrime among victims who owned, operated or managed a small to medium business (%) (*n*=820)



Note: Excludes 48 small to medium business owners, operators and managers who did not answer this question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

Small to medium business owners, operators and managers reported a variety of impacts on their business (Table 22). Most commonly, they had to spend time repairing and improving systems (8.1%); had to buy new software (6.1%); had to change their business banking or contact information (6.0%); had to buy new backup data storage or data storage devices (5.5%); and had a loss of customers, sales or revenue (5.4%).

Table 22: Harms to small business owners, operators and managers who were victims of cybercrime (%) (*n*=952)

	n	%
Disruption to everyday business function		
The business spent time repairing and improving systems	66	8.1
Had to change the business banking and/or contact information	50	6.0
Disruption to operations and/or trading (eg inability to carry out transactions, websites not functioning)	44	5.3
Difficulty accessing online accounts and resources (eg bank accounts, utilities, email)	42	5.1
Had problems communicating or dealing with government departments	28	3.4
Had problems communicating or dealing with businesses	27	3.3
Blocked customer access to the business online store or website	27	3.2
Had to shut down the business online store or website (temporarily or permanently)	24	2.9

Table 22: Harms to small business owners, operators and managers who were victims of cybercrime (%) (*n*=952) (cont.)		
	n	%
Additional business expenses		
Had to buy new software	50	6.1
Had to buy new backup data storage or data storage devices	45	5.5
Had to pay for computer, phone or other hardware repairs or replacement	43	5.2
Insurance premiums were increased	29	3.5
Loss of information		
The business had to notify affected parties of a data breach	35	4.3
Theft of my information or other staff information (eg contact details, financial data)	32	3.9
Theft of customer or supplier information (eg contact details, financial data)	28	3.4
Theft of intellectual property or corporate information	25	3.1
Reputation and revenue		
There was a loss of customers, sales or revenue	44	5.4
The business reputation was damaged	37	4.5
We lost business contracts	32	3.9
Professional relationships were damaged	24	2.9
Impacts on staff		
Employees/owners of the business had to take time off work	35	4.3
Employees/owners of the business resigned or lost their job	20	2.4
Legal or regulatory sanctions		
The business was hit with fines and regulatory sanctions	25	3.0
There was litigation or legal action against the business	21	2.6

Note: Excludes 48 small to medium business owners, operators and managers who did not answer this question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

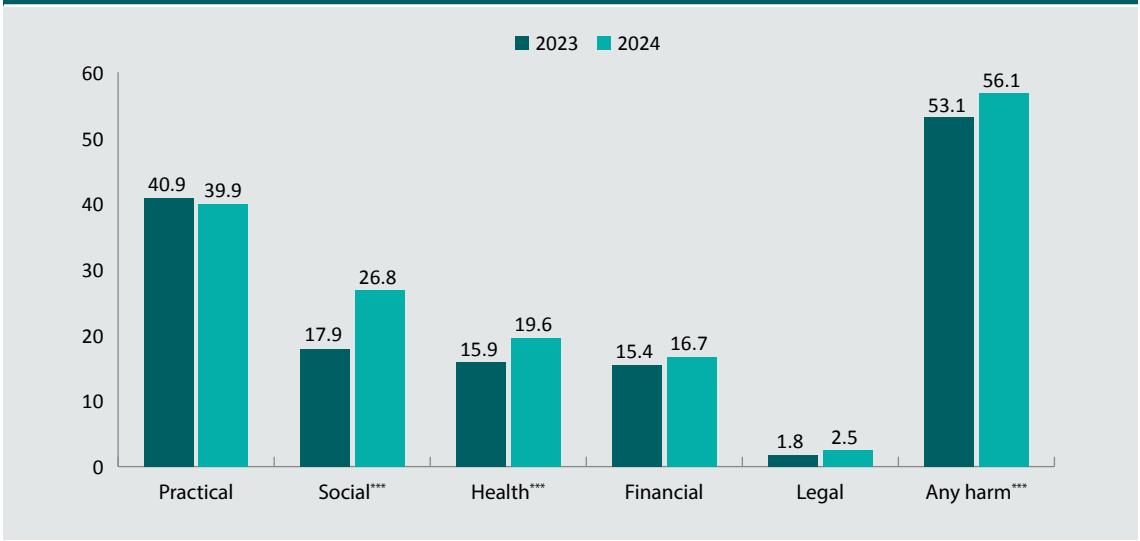
Changes in harm to individuals and small businesses

As shown in Figure 33, the proportion of victims who experienced any harm was higher in 2024 (56.8%) than in 2023 (53.1%, (F(1, 23918)=11.68, p<0.001). The proportion of victims who experienced at least one health impact increased (15.9% in 2023 vs 19.6% in 2024, F(1, 23918)=19.78, p<0.001), as did the proportion who experienced at least one social impact (17.9% in 2023 vs 26.8% in 2024, F(1, 23918)=97.27, p<0.001). There were no differences between 2023 to 2024 in the proportion of victims experiencing financial harm, practical impacts or legal issues.

The increase in social harm appears to be driven by an increase in respondents who said they were embarrassed or their reputation was damaged, from 5.0 percent in 2023 to 15.5 percent in 2024 ($F(1, 23918)=264.64$, $p<0.001$), and that they lost trust in other people, from 11.6 percent to 13.0 percent ($F(1, 23918)=3.89$, $p<0.05$).

The increase in health-related harm was driven by the growing proportion of victims who experienced difficulty sleeping, from 6.6 percent to 8.7 percent ($F(1, 23918)=12.78$, $p<0.001$); who had to seek medical treatment, from 1.3 percent to 2.1 percent ($F(1, 23918)=7.35$, $p<0.01$); who increased their consumption of alcohol, from 1.6 percent to 3.1 percent ($F(1, 23918)=21.67$, $p<0.001$); and who increased their consumption of legal or illegal drugs, from 1.1 percent to 1.8 percent ($F(1, 23918)=6.79$, $p<0.01$).

Figure 33: Harms from cybercrime among victims, 2023 and 2024 (%)



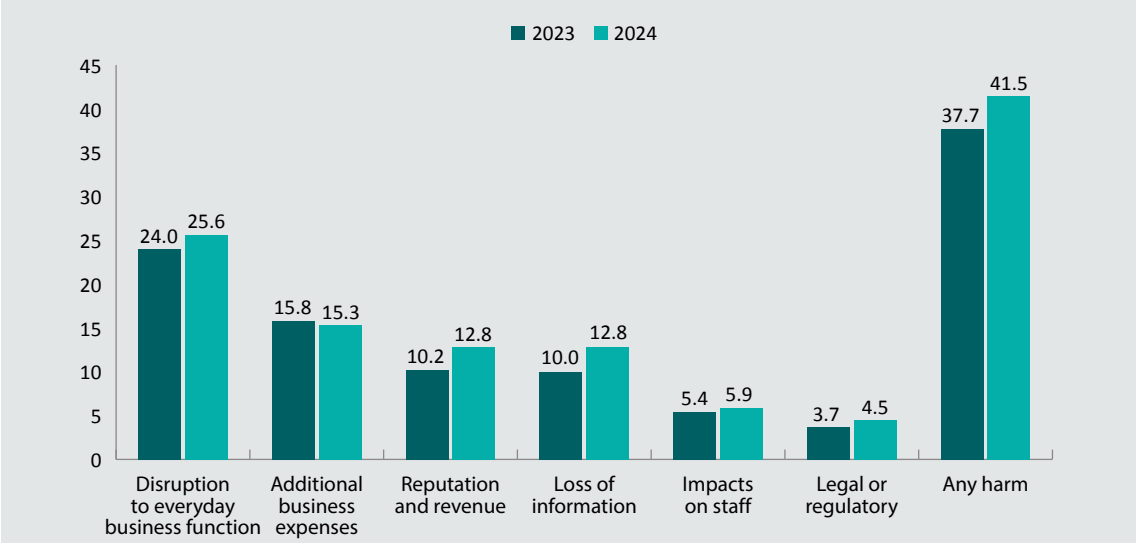
***statistically significant at $p<0.001$

Note: Excludes 174 victims in 2023 and 151 victims in 2024 who did not answer this question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

The prevalence of harms to business among victims who owned, operated or managed a small to medium business in 2024 was compared with results from the 2023 survey (Figure 34). While the prevalence of victimisation among small to medium business owners, operators or managers had decreased for some types of cybercrime, there was no difference in the impact of cybercrime on those respondents who did fall victim.

Figure 34: Harms to business from cybercrime among victims who owned, operated or managed a small to medium business, 2023 and 2024 (%)



Note: Excludes 54 small to medium business owners, operators and managers in 2023 and 48 small to medium business owners, operators and managers in 2024 who did not answer this question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

References

URLs correct as at February 2025

Australian Bureau of Statistics (ABS) 2024a. National, state and territory population, December 2023. https://www.abs.gov.au/statistics/people/population/national-state-and-territory-population/dec-2023

Australian Bureau of Statistics 2024b. Estimated resident and projected Aboriginal and Torres Strait Islander population aged 18 years and over, medium series, sex by states and territories and Australia—2011 to 2031. https://www.abs.gov.au/statistics/people/aboriginal-and-torres-strait-islander-peoples/estimates-and-projections-aboriginal-and-torres-strait-islander-australians/2011-2031/32380DO005_20112031.xlsx

Australian Bureau of Statistics 2024c. Population estimates by LGA, Significant Urban Area, Remoteness Area, Commonwealth Electoral Division and State Electoral Division, 2001 to 2023. https://www.abs.gov.au/statistics/people/population/regional-population/2022-23/32180DS0004_2001-23.xlsx

Australian Bureau of Statistics 2024d. Labour Force, Australia, July 2024. https://www.abs.gov.au/statistics/labour/employment-and-unemployment/labour-force-australia/jul-2024

Australian Bureau of Statistics 2022a. Cultural diversity: Census. https://www.abs.gov.au/statistics/people/people-and-communities/cultural-diversity-census/2021

Australian Bureau of Statistics 2022b. National Health Survey: First results methodology, 2020–21. https://www.abs.gov.au/methodologies/national-health-survey-methodology/2020-21

Australian Competition and Consumer Commission (ACCC) 2024. *Targeting scams: Report of the National Anti-Scam Centre on scams activity 2023*. Canberra: ACCC. https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity/targeting-scams-report-of-the-accc-on-scams-activity-2023

Australian Government 2022. *National Plan to Combat Cybercrime 2022*. Canberra: Attorney-General's Department. https://www.ag.gov.au/crime/publications/2022-national-plan-combat-cybercrime

Australian Institute of Health and Welfare (AIHW) 2022. People with disability in Australia 2022. Canberra: AIHW. https://doi.org/10.25816/5ec5be4ced179

Australian Signals Directorate 2024. *Annual cyber threat report, July 2023 to June 2024*. Canberra: Australian Signals Directorate. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

Australian Signals Directorate 2020. Annual cyber threat report, July 2019 to June 2020. Canberra: ASD. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asdacsc-annual-cyber-threat-report-july-2019-june-2020

Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) 2025. Guidelines for cyber security incidents. https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cybersecurity-incidents

Australian Taxation Office 2024. Tax rates – Australian resident. https://www.ato.gov.au/tax-rates-and-codes/tax-rates-australian-residents

Callegaro M & DiSogra C 2008. Computing response metrics for online panels. *Public Opinion Quarterly* 72(5): 1008–1032. https://doi.org/10.1093/poq/nfn065

Cheung KL, ten Klooster PM, Smit C, de Vries H & Pieterse ME 2017. The impact of nonresponse bias due to sampling in public health studies: A comparison of voluntary versus mandatory recruitment in a Dutch national survey on adolescent health. *BMC Public Health* 17: 276. https://doi.org/10.1186/s12889-017-4189-8

Kypri K, Samaranayaka A, Connor J, Langley JD & Maclennan B 2011. Non-response bias in a web-based health behaviour survey of New Zealand tertiary students. *Preventive Medicine* 53(4–5): 274–277. https://doi.org/10.1016/j.ypmed.2011.07.017

Morgan A & Voce I 2022. *Data breaches and cybercrime victimisation*. Statistical Bulletin no. 40. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78832

Morgan A, Dowling C, Brown R, Mann M, Voce I & Smith M 2016. *Evaluation of the Australian Cybercrime Online Reporting Network*. Report prepared for CrimTrac. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2020-06/acorn_evaluation_report_.pdf

Muller CJ & MacLehose RF 2014. Estimating predicted probabilities from logistic regression: Different methods correspond to different target populations. *International Journal of Epidemiology* 43(3): 962–970. https://doi.org/10.1093/ije/dyu029

Office of the Australian Information Commissioner 2024. Notifiable Data Breaches Report: January to June 2024. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2024

Office of the Australian Information Commissioner 2023. Notifiable Data Breaches Report: January to June 2023. Sydney: OAIC. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2023

Pennay D et al. 2023. *Results from the 2022 Australian Comparative Study of Survey Methods*. Canberra: Australian National University. https://csrm.cass.anu.edu.au/research/publications/results-2022-australian-comparative-study-survey-methods-acssm

Pennay DW, Neiger D, Lavrakas PJ & Borg K 2018. *The Online Panels Benchmarking Study: A total survey error comparison of findings from probability-based surveys and non-probability online panel surveys in Australia*. CSRM & SRC Methods Paper no. 2/2018. Canberra: Australian National University. https://csrm.cass.anu.edu.au/research/publications/online-panels-benchmarking-study-total-survey-error-comparison-findings

Voce I & Morgan A 2025. Developing a harm index for individual victims of cybercrime. *Trends & issues in crime and criminal justice* no. 706. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti77666

Voce I & Morgan A 2023a. *Cybercrime in Australia 2023*. Statistical Report no. 43. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sr77031

Voce I & Morgan A 2023b. Online behaviour, life stressors and profit-motivated cybercrime victimisation. *Trends & issues in crime and criminal justice* no. 675. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti77062

Yeager DS, Krosnick JA, Chang L, Javitz HS, Levendusky MS, Simpser A & Wang R 2011. Comparing the accuracy of RDD telephone surveys and internet surveys conducted with probability and non-probability samples. *Public Opinion Quarterly* 75(4): 709–47. https://doi.org/10.1093/poq/nfr020

Appendix: Survey design, sampling and weighting

This appendix describes the methodology for a survey of 10,335 Australians aged 18 years and over about their experience of cybercrime. It was prepared with input from Roy Morgan. The aim of this survey was to measure the prevalence and characteristics of cybercrime, risk factors, help-seeking behaviour, financial losses and other harms from victimisation.

Key definitions

Cybercrime

According to the National Plan to Combat Cybercrime (Australian Government 2022), cybercrime is any crime that involves the use of a computer or some other digital device, or computer network, and refers to both cyber-dependent and cyber-enabled crimes.

Cyber-dependent crime

Cyber-dependent crimes are those directed at computers or information and communications technologies and that can only exist in the digital world. They include crimes such as ransomware, which relies on the use of malware to extort money from victims, denial-of-service attacks, and hacking networks to steal sensitive personal information.

Cyber-enabled crime

Cyber-enabled crimes are traditional crimes that are committed using computers, computer networks or other forms of information and communications technologies, which enable the offender to increase the scale or reach of the crime. This includes profit-motivated crimes such as online fraud and identity crime and misuse. It also includes crimes such as online abuse and harassment, online child sexual exploitation and technology-enabled forms of domestic and family violence.

Cybersecurity

Cybersecurity is defined by the Australian Cyber Security Centre (2023: np) as 'an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security'. Cybersecurity victims tend to be governments and businesses, and the target is usually a computer network, software or hardware. Some of these crimes, such as malware, are covered in this report.

Fraud and scams

Fraud and scams involve intentionally deceiving someone to obtain money or something else of value, such as personal information. To be included as a victim of fraud or scams in this report, the respondent must have paid money or provided information as part of the fraudulent scheme.

Identity crime and misuse

Identity crime and misuse refers to incidents where a person's personal information is obtained or used without their permission. For example, an offender could pretend to be that person, to carry out a business in their name without their permission, or for another type of activity or transaction. This excludes the use of someone's personal information for direct marketing, even if this was done without their permission.

Malware

Short for 'malicious software', malware refers to software specifically developed and used to harm a computer system or network. It is used to gain access to a computer and can be used to steal confidential information.

Online abuse and harassment

Online abuse and harassment refers to online communication to or about an individual which may cause them emotional distress. This includes behaviours such as sending abusive messages, engaging in image-based abuse, setting up fake social media accounts to harass someone or stalking someone using a phone or other device.

Survey design

In 2021 the Australian Institute of Criminology (AIC) conducted a pilot survey of Australian computer users about their experiences of cybercrime victimisation. It examined a range of cyber-dependent and cyber-enabled crimes, including identity theft, compromise and misuse; malware; online scams and fraud; and online abuse and harassment.

Building on this pilot, and recognising the need for better quality data about cybercrime impacting the Australian community, the AIC ran the inaugural Australian Cybercrime Survey (ACS) in 2023. This is an annual survey which involves several components. There is a core survey of at least 10,000 respondents which measures cybercrime victimisation, financial losses, harms and help-seeking behaviour. A minimum of three addenda each year will address priority issues of interest. There is also a longitudinal component involving a cohort of approximately 3,000 respondents which measures repeat victimisation and provides an opportunity to test the efficacy of intervention strategies to reduce cybercrime victimisation or increase help-seeking.

Core survey

The AIC developed a questionnaire to measure cybercrime victimisation among Australian computer users. The survey included questions about:

- sociodemographic characteristics of respondents;
- use of technology and devices;
- experiences of cybercrime victimisation and repeat victimisation;
- help-seeking behaviour, expectations and outcomes;
- financial costs of being a victim, including direct losses, costs of dealing with the consequences and amounts recovered;
- practical, legal, health, social and financial harms resulting from victimisation;
- involvement in risky online activities; and
- preventative measures.

The survey adopted a bottom-up approach to measuring cybercrime victimisation, focusing on specific symptoms or indicators of cybercrime. This was necessary because members of the public may not fully understand cybercrime terminology (such as ‘malware’, ‘ransomware’ and ‘phishing scams’). Each crime type was measured using questions about the various incidents or symptoms that would indicate they have been a victim of a particular form of cybercrime. For example, in the case of malware, respondents were asked about signs that their computer was infected which they did not believe were the result of genuine device malfunction or aging, such as programs opening and closing automatically, files going missing or being replaced with odd file extensions, or people telling the respondent they had been sending suspicious messages and links over social media or email.

The survey measured lifetime and past-year prevalence, and collected more detailed information about the most recent incident (within each broad category of cybercrime).

While the ACS measures crime against individuals, some of these individuals may own or operate a business, and respondents could report cybercrime occurring on a personal or work device. While the survey asked about cybercrime on a personal or work device, the respondent must themselves have been the victim of the cybercrime (and not their business or employer). For small business, they may be one and the same thing. Similarly, the survey did not distinguish between incidents occurring on a work or personal device, since for many small businesses (and, indeed, larger businesses) the same device may be used for both purposes.

Following internal user testing, the survey was piloted on 4 and 5 July 2024 with a sample of 50 respondents from the Roy Morgan Single Source panel, which allowed design issues to be identified and addressed. All steps were taken to ensure the data collected were as accurate as possible.

Research ethics

The survey and administration methods and protocols were approved by the AIC's Human Research Ethics Committee in March 2022 (Protocol no. P0325A). This project was also carried out in compliance with ISO 20252 (market, opinion and social research).

Sampling and weighting

The survey was conducted between 11 July and 29 August 2024 by Roy Morgan using their Single Source panel and three highly regarded panels managed by PureProfile, Dynata and Octopus. These panels are opt-in panels and members were recruited through various means. The survey was sent to members of these online panels aged 18 years and over, in accordance with the sampling method described below. Panel members were invited to participate in the research and were provided with a small reward.

Proportional quota sampling was used, which is the non-probability version of stratified random sampling. Quotas were set based on known population characteristics—age, gender and usual place of residence—and participants were invited to complete the survey until these quotas were reached, within an agreed margin of error. Roy Morgan based these target populations on latest Australian Bureau of Statistics (ABS) figures for Australians aged 18 years or over (ABS Labour Force Survey – July 2024). The aim was to ensure the final sample was representative of the spread of the Australian population.

Members of the four research panels were randomly selected and sent an invitation to participate in the survey. The survey was first conducted with respondents from the Roy Morgan Single Source panel, which comprises individuals recruited through a rigorous clustersampled, face-to-face survey approach. The majority of respondents (58.4%) were recruited from this panel. PureProfile panel members accounted for 36.6 percent of respondents, Dynata accounted for 3.5 percent of respondents and the remaining 1.6 percent came from Octopus.

Participants were invited until the relevant quotas had been reached. Data on completion rates were available from the Roy Morgan Single Source panel (Table A1). Overall, 141,979 members of the Roy Morgan Single Source panel were sent an invitation to participate; however, there is no way of verifying how many of these invitations were received. A total of 13,632 invitations were opened (9.6%), meaning that the respondent proceeded to the survey landing page. Of these, 1,345 people (0.9%) who opened the invitation were excluded because they did not meet the eligibility criteria or started after the relevant quota had been reached. A further 6,191 respondents (4.4%) started the questionnaire but did not complete it. Many of these respondents read the information sheet but did not consent to participate. A very small proportion (less than 1%) of respondents who started the survey were excluded because they had already completed the survey or for quality reasons. These duplicates—identified on the basis of IP addresses, in combination with selected demographic items—exist because some respondents may be members of multiple panels. Poor-quality responses are those where there was evidence of speeding or straight-lining—for example, selecting the first response to each question without considering the question. A minimum time of seven minutes was used to immediately eliminate these responses, while manual checks were conducted on responses that met this threshold.

The raw completion rate for invitations sent to Roy Morgan Single Source panel members, which offers a relatively simple measure of responses to online surveys drawn from non-probability panels (Callegaro & DiSogra 2008), was 4.3 percent. This is the proportion of the total number of invitations sent that resulted in completed surveys. While this is on par with other online panels, including some probability surveys that are conducted online (Pennay et al. 2018), there are limits to the interpretability of this figure. First, as has already been stated, the total number of invitations received cannot be reliably estimated. There is no certain way of measuring how many prospective participants were actually contacted. Second, invitations were distributed until such time as the relevant quotas had been met. These invitations may far exceed what is needed to achieve the desired sample size.

Importantly, 44.3 percent of people who opened the invitation, and 49.1 percent of those who opened the invitation and were eligible to participate in the research, went on to complete the survey. The latter is a particularly useful measure because it accounts for invitations that were received by eligible potential respondents and the response to the survey by respondents who were aware of what they were being invited to undertake. Importantly, partially completed surveys include those where the respondent closed the survey without indicating whether they consented to participate or not.

The final sample size was 10,335 respondents. Twelve percent of respondents who completed the survey took over an hour to do so, which usually indicates they completed the survey over multiple sessions (ie saved their answers to the survey and returned to it later). Among those who completed the survey in less than one hour, the survey took respondents an average of 23.4 minutes (*SD*=14.1) to complete.

Table A1: Invitation and completion rates, Roy Morgan Single Source panel (unadjusted)		
	n	%
Total invitations sent out (T)	141,979	–
Total not started interview (NS)	128,347	90.4
Total started interview (S)	13,632	9.6
Complete interviews (I)	6,036	4.3
Partial interviews (P)	6,191	4.4
Screened out or quota reached (SQ)	1,345	0.9
Previously responded or poor quality (DQ)	60	<0.1
Non-participation rate (NS)/(T)	–	90.4
Completion rate for accepted invitations by eligible respondents (I)/(S–SQ)	–	49.1
Completion rate (I)/(T)	–	4.3

Note: Information presented in this table is based on Roy Morgan Single Source panel. Percentages may not total 100 due to rounding

Source: Roy Morgan [computer file]

The distribution of the usual place of residence of survey respondents and ABS demographic data, prior to weighting, are presented in Table A2. New South Wales residents were slightly under-represented in the survey data (30.4% vs 31.3%), as were residents of the Northern Territory (0.4% vs 0.9%) and Victoria (25.5% vs 25.7%). Meanwhile, residents of Queensland (20.3% vs 20.2%), South Australia (7.5% vs 7.1%), Tasmania (2.5% vs 2.2%) and the Australian Capital Territory (2.8% vs 1.8%) were slightly over-represented.

Table A2: Respondents by usual place of residence (unweighted data)			
	ABS demographic statistics[a]	Survey respondents (*n*=10,335)	
	%	*n*	%
NSW	31.3	3,141	30.4
Vic	25.7	2,638	25.5
Qld	20.3	2,088	20.2
WA	10.7	1,105	10.7
SA	7.1	774	7.5
Tas	2.2	261	2.5
ACT	1.8	284	2.8
NT	0.9	44	0.4

a: Estimated resident population at December 2023; ABS 2024a

Note: Percentages may not total 100 due to rounding

Source: ABS 2024a; Australian Cybercrime Survey 2024 [computer file]

It is not possible to estimate design weights for non-probability panels because the probability of an individual opting in to the panel is unknown (Pennay et al. 2018). Post-stratification weights were applied to reduce non-coverage errors and ensure the data were representative of the spread of the wider population. The data were weighted using a multi-tiered system. Weights were calculated by first comparing the sample with the proportion of the population in each age group in each state and territory according to the ABS estimate of residential population (ABS 2024a). Random iterative method weighting was then applied to each record based on educational attainment, frequency of internet use, and social media use. These weights were calculated from Roy Morgan's Single Source survey, which is a nationally representative survey conducted with 50,000 Australians over 50 weeks each year. This weighting corrects for the propensity of non-probability panels to have respondents who are more highly educated and more frequent users of the internet and social media than the norm in the general population. Weights were assigned using a program to run multiple iterations to achieve the best result. Under-represented categories were assigned a multiplier larger than one, and over-represented categories were assigned a multiplier smaller than one. Cap weights were applied to avoid heavy weighting being applied to a small group of respondents. The effective sample size for the study after weighting (the weighted sample size) was 10,335 respondents.

Table A3 shows the effect of weighting on the concordance between the adult population in each state and territory according to the ABS (2024a) and the weighted sample. There was a high degree of concordance overall, with the only notable difference an under-representation of respondents from the Northern Territory (0.3% vs 0.9%). Correcting this would have resulted in weights for NT respondents that exceeded the cap.

Table A3: Respondents by usual place of residence (weighted data) (%)

	ABS demographic statistics[a]	Survey respondents (*n*=10,335)
NSW	31.3	31.3
Vic	25.7	25.8
Qld	20.3	20.4
WA	10.7	10.7
SA	7.1	7.3
Tas	2.2	2.2
ACT	1.8	1.9
NT	0.9	0.3

a: Estimated resident population at December 2023; ABS 2024a
Note: Percentages may not total 100 due to rounding
Source: ABS 2024a; Australian Cybercrime Survey 2024 [computer file]

To further examine concordance, the unweighted and unweighted ages of respondents were compared with those of the estimated resident population (Table A4). The weighting did not create any noteworthy imbalances in the age distribution of respondents.

Table A4: Respondents by age (%)

	ABS demographic statistics[a]	Survey respondents (*n*=10,335)	
		Unweighted	Weighted
18–24	11.3	10.9	11.6
25–34	18.7	18.6	19.0
35–49	25.5	25.0	25.4
50–64	22.6	22.8	22.1
65+	21.8	22.6	21.9

a: Estimated resident population at December 2023; ABS 2024a
Source: ABS 2024a; Australian Cybercrime Survey 2024 [computer file]

A concern with non-probability sampling methods that use some form of quota sampling and post-hoc weighting is the potential for sampling bias in relation to secondary demographics—characteristics of the population being surveyed that are not used in either the sampling or weighting strategy (Pennay et al. 2018). To assess the potential consequences of this approach, survey respondents were compared with benchmarks based on ABS data on the characteristics of the general population (Table A5).

Results from this comparison demonstrate a relatively high degree of concordance between ACS respondent characteristics and ABS demographic data for gender (49.9% female in the ACS vs 50.8% in the general population), Aboriginal and Torres Strait Islander status (3.5% vs 2.7%) and usual place of residence (remoteness, 72.9% metropolitan in the ACS vs 72.2% in the general population).

The most significant differences emerged in relation to the presence of a disability and the proportion of respondents with a non-English-speaking background. Differences in non-English-speaking backgrounds are largely explained by the differences in how this was measured. Respondents to the ACS were asked to nominate the language they spoke most often at home. ABS Census participants are asked what languages they speak at home, rather than the language spoken most often (ABS 2022a). That said, ACS respondents were slightly less likely than the general population to say they were born overseas (22.3% vs 27.6%), suggesting that the difference may not be fully explained by different measurement rules.

Relatedly, the ACS relies on a similar definition to the ABS Short Disability Module, and defines disability as a long-term health condition that is expected to last for longer than six months and which restricts everyday activities (Australian Institute of Health and Welfare 2022). The health conditions question is simplified and is not directly comparable to ABS data on long-term or chronic health conditions measured in the National Health Survey (ABS 2022b). Similarly, there are limitations to this method in terms of producing reliable data on disability prevalence, compared with the comprehensive set of questions used in the ABS Survey of Disability, Ageing and Carers to measure disability (Australian Institute of Health and Welfare 2022). The latter serves as the benchmark in Table A6. These issues aside, it appears respondents with a disability are under-represented within the ACS (11.0% vs 17.7%).

These differences should be considered when interpreting the results of the survey. The under-representation of respondents from a non-English-speaking background and respondents with a disability, reasons for this and potential implications are discussed in the *Limitations* section.

Table A5: Selected sociodemographic characteristics of respondents (weighted data) (%)

	ABS statistics	Survey respondents
Female[a]	50.4	50.2
Aboriginal and/or Torres Strait Islander[b]	3.1	4.1
Non-English-speaking background[c]	22.3	6.0
Born overseas[d]	27.6	22.3
Disability[e]	17.7	11.0
Usual place of residence[f]		
Major cities	72.6	73.5
Regional	25.5	23.4
Remote	1.9	2.8

a: Proportion of estimated residential population as at December 2023 who were female based on sex ratio (ABS 2024a)

b: Projected resident Aboriginal and Torres Strait Islander population as proportion of persons aged 18 years and over in 2024 (ABS 2024b). Denominator for survey respondents includes 174 respondents who did not know or declined to answer this question

c: Proportion of Australians who speak a language other than English at home, based on data collected in 2021 Census of Population and Housing (ABS 2022a). For the ACS, proportion of respondents who speak a language other than English most often at home. Denominator includes 38 respondents who did not know or declined to answer the question

d: Proportion of Australians who were born overseas (ABS 2022a). Denominator for survey respondents includes 52 respondents who did not know or declined to answer the question

e: Proportion of persons with a disability (Australian Institute of Health and Welfare 2022). Survey estimate is based on Short Form Disability measure, refers to respondents who self-reported at least one current medical condition which has lasted, or is expected to last, for six months or more and which restricts their everyday activities. Denominator includes 486 respondents who did not know or declined to answer this question

f: Estimated resident population, by remoteness areas (ABS 2024c). Denominator for survey respondents includes 33 respondents where this information was unknown

Source: ABS (various); Australian Institute of Health and Welfare (2022); Australian Cybercrime Survey 2024 [computer file]

Comparison between 2023 and 2024 samples

We compared the samples in 2023 and 2024 to help inform decisions about how best to compare results from the two surveys.

There were statistically significant differences between the samples for the 2023 and 2024 ACS, including in terms of respondents' usual place of residence, gender, First Nations status, sexuality, whether they most often spoke a language other than English at home, whether they had a restrictive long-term health condition and whether they were currently in a relationship (Table A6).

Table A6: Sociodemographic characteristics of respondents, 2023 and 2024

	2023 (*n*=13,887)		2024 (*n*=10,335)	
	n	%	*n*	%
State/Territory*				
NSW	4,401	31.7	3,182	30.8
Vic	3,573	25.7	2,676	25.9
Qld	2,835	20.4	2,108	20.4
WA	1,479	10.6	1,122	10.9
SA	1,024	7.4	753	7.3
Tas	314	2.3	223	2.2
ACT	210	1.5	237	2.3
NT	51	0.4	33	0.3
Age				
18–24	1,540	11.1	1,203	11.6
25–34	2,527	18.2	1,962	19.0
35–49	3,564	25.7	2,624	25.4
50–64	3,189	23.0	2,283	22.1
65+	3,067	22.1	2,262	21.9
Gender*				
Female	6,900	49.7	5,183	50.2
Male	6,935	49.9	5,086	49.2
Non-binary	52	0.4	66	0.6
First Nations**				
Yes	486	3.5	420	4.1
No	13,249	95.4	9,741	9.4
Unknown	153	1.1	174	1.7
LGB+ respondents**				
Yes	1,095	7.9	947	9.2
No	12,618	90.9	9,215	89.2
Unknown	174	1.3	173	1.7

Table A6: Sociodemographic characteristics of respondents, 2023 and 2024 (cont.)				
	2023 (*n*=13,887)		2024 (*n*=10,335)	
	n	%	*n*	%
Born outside of Australia				
Yes	3,058	22.0	2,302	22.3
No	10,796	77.7	7,980	77.2
Unknown	33	0.2	52	0.5
Speaks a language other than English most often at home**				
Yes	632	4.6	620	6.0
No	13,209	95.1	9,677	93.6
Unknown	46	0.3	38	0.4
Restrictive long-term health condition***				
Yes	1,308	9.4	1,140	11.0
No	12,170	87.6	8,708	84.3
Unknown	409	2.9	486	4.7
Currently in a relationship**				
Yes	8,784	63.3	6,210	60.1
No	5,000	36.0	4,038	39.1
Unknown	103	0.7	87	0.8
Children living at home				
Yes	4,618	33.3	3,419	33.8
No	9,174	66.1	6,760	65.4
Unknown	95	0.7	83	0.8
Usual place of residence (remoteness)				
Major city	10,124	72.9	7,595	73.5
Regional	3,325	23.9	2,423	23.4
Remote	397	2.9	284	2.8
Unknown	41	0.3	33	0.3

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$
Note: Weighted frequencies and percentages may not add to total due to rounding
Source: Australian Cybercrime Survey 2024 [weighted data]

Table A7 displays information on the education and employment status of respondents in 2024 and how they compare to the 2023 sample. In the 2024 sample, just under one-third of respondents (30.8%) said their highest level of education was high school, while 41.1 percent of respondents had a university qualification. Two-thirds of respondents to the 2024 survey (64.9%) were employed (either full or part time), 20.2 percent of respondents were retired and 4.5 percent were unemployed.

Twenty-three percent of respondents in the 2024 sample who were currently working said they owned, operated or managed a small to medium business (with fewer than 200 employees). A further 7.0 percent of respondents who were currently working said they owned, operated or were the executive of a large business or company (with more than 200 employees). There were statistically significant differences between the samples for the 2023 and 2024 ACS in terms of whether they owned or worked for a small to medium enterprise or large company.

Table A7: Education, employment and income of respondents, 2023 and 2024

	2023 (*n*=13,887)		2024 (*n*=10,335)	
	n	%	*n*	%
Highest education level				
Year 12 or below	4,453	32.1	3,181	30.8
Vocational qualification	3,761	27.1	2,846	27.5
University graduate	5,586	40.2	4,245	41.1
Unknown	88	0.6	62	0.6
Employment status				
Working full time	5,982	43.1	4,518	43.7
Working part-time, casual or semi-retired	2,902	20.9	2,187	21.2
Retired	3,015	21.7	2,087	20.2
Unemployed	596	4.3	460	4.5
Full-time homemaker or carer	637	4.6	418	4.1
Student full-time (and not working)	169	1.2	163	1.6
Not working for health reasons	434	3.1	366	3.5
Unknown	151	1.1	134	1.3
Owns, operates or works for a small to medium enterprise (SME)**				
Owner or manager	1,782	12.8	1,532	14.8
Employee	2,330	16.8	1,789	17.3
Does not operate or work for an SME	4,612	33.2	3,279	31.7
Not currently working	5,003	36.0	3,629	35.1
Unknown	161	1.2	105	1.0
Owns, operates or works for a large company or business**				
Owner or executive	618	4.5	462	4.5
Employee	2,736	19.7	1,840	17.8
Does not operate or work for a large company	5,356	38.6	4,268	41.3
Not currently working	5,003	36.0	3,629	35.1
Unknown	174	1.3	136	1.3

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$
Note: Weighted frequencies and percentages may not add to total due to rounding
Source: Australian Cybercrime Survey 2024 [weighted data]

For the 2024 ACS, the questions on individual income were updated to reflect the tax thresholds for 2023–24 (Australian Taxation Office 2024), meaning this item is not comparable across the two years (Table A8).

Table A8: Annual income of respondents in the previous financial year, 2023 and 2024

2023 (*n*=13,887)			2024 (*n*=10,335)		
	n	%		*n*	%
$0 – $18,200	1,551	11.2	$0 – $18,200	983	9.5
$18,201 – $37,000	2,576	18.5	$18,201 – $45,000	2,373	23.0
$37,001 – $80,000	4,361	31.4	$45,001 – $120,000	4,258	41.2
$80,001 – $180,000	3,631	26.1	$120,001 – $180,000	1,219	11.8
$180,001 and over	479	3.5	$180,001 and over	561	5.4
Unknown	1,289	9.3	Unknown	940	9.1

Note: Weighted frequencies and percentages may not add to total due to rounding
Source: Australian Cybercrime Survey 2024 [weighted data]

Table A9 presents information on the online behaviour of respondents in the 2024 ACS and how it compares to 2023. More than half of respondents (56.8%) said they spent more than three hours a week using social media, while more than three-quarters of respondents (78.1%) said they used the internet three or more times a day. There were statistically significant differences between the samples for the 2023 and 2024 ACS in terms of respondents' social media use.

Table A9: Online behaviour of respondents, 2023 and 2024

	2023 (*n*=13,887)		2024 (*n*=10,335)	
	n	%	*n*	%
Social media use* **				
No social media use	2,284	16.4	1,466	14.2
Up to 3 hours per week	4,401	29.1	2,997	29.0
Between 3 and 8 hours a week	3,672	26.4	2,771	26.8
More than 8 hours a week	3,890	28.0	3,101	30.0
Internet use				
A few times a week or less	695	5.0	528	5.1
Once a day	1,350	9.7	999	9.7
Twice a day	1,011	7.3	737	7.1
Three or more times a day	10,830	78.0	8,071	78.1

***statistically significant at $p<0.001$

a: Excludes 1,815 respondents in 2023 and 1,517 respondents in 2024 who did not know or declined to answer the question

b: 2023 data limited to respondents who were currently working (*n*=8,884) and excludes 1,507 respondents who did not know or declined to answer the question; 2024 data limited to respondents who were currently working (*n*=6,706) and excludes 1,249 respondents who did not know or declined to answer the question

Note: Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2024 [weighted data]

AIC reports

Statistical Report

Isabella Voce is a Principal Research Analyst in the Serious and Organised Crime, Cybercrime and Radicalisation Research Program at the Australian Institute of Criminology.

Anthony Morgan is Research Manager of the Serious and Organised Crime, Cybercrime and Radicalisation Research Program at the Australian Institute of Criminology.

Australia's national research and
knowledge centre on crime and justice

www.aic.gov.au