Australian Government
Australian Institute of Criminology

AIC reports
Statistical Report 43

Cybercrime in Australia 2023

Isabella Voce
Anthony Morgan

© Australian Institute of Criminology 2023

ISSN 2206-7930 (Online)
ISBN 978 1 922877 03 1 (Online)
https://doi.org/10.52922/sr77031

Apart from any fair dealing for the purpose of private study, research, criticism or review, as permitted under the *Copyright Act 1968* (Cth), no part of this publication may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Inquiries should be addressed to the publisher.

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.

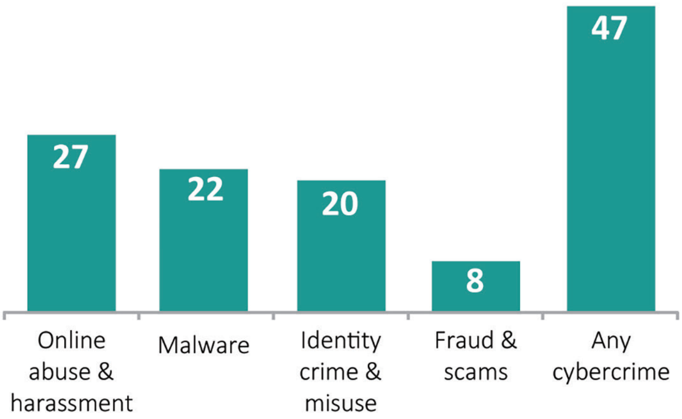
Disclaimer: This research report does not necessarily reflect the policy position of the Australian Government.

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

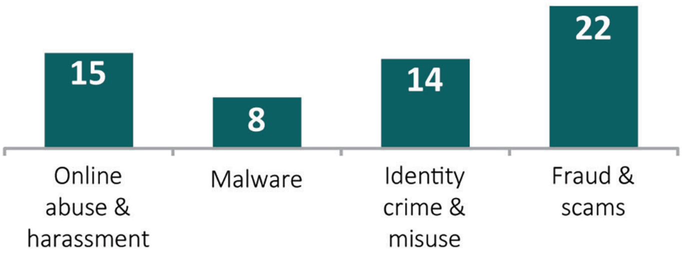
Edited and typeset by the Australian Institute of Criminology

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

PAST YEAR VICTIMISATION (%)



VICTIMS WHO SOUGHT HELP FROM POLICE OR REPORTCYBER (%)



OUTCOMES OF HELP-SEEKING

Around **half** the incidents were investigated

Victim was told someone was apprehended in up to **1 in 20** incidents

Up to **43% of victims satisfied** with the outcome and **36% dissatisfied**

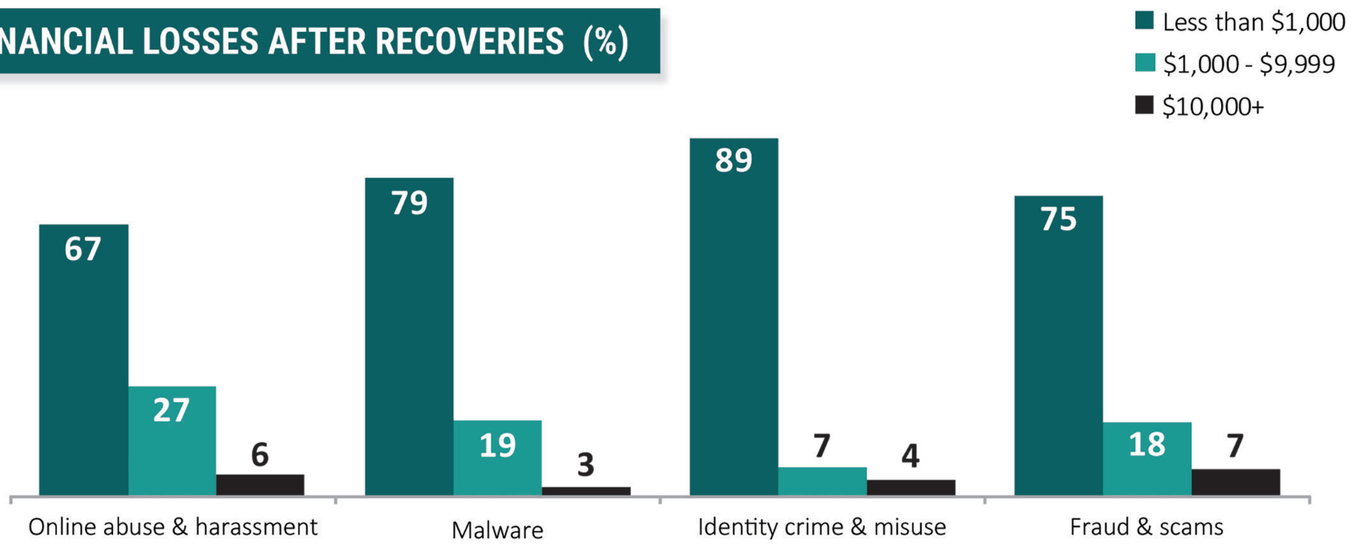
TOP 5 REASONS FOR NOT SEEKING HELP

1. Dealt with it by themselves
2. Not serious enough, didn't think it a crime
3. Didn't know reporting to police or ReportCyber was an option
4. Didn't think they could do anything
5. Didn't know how or where to report

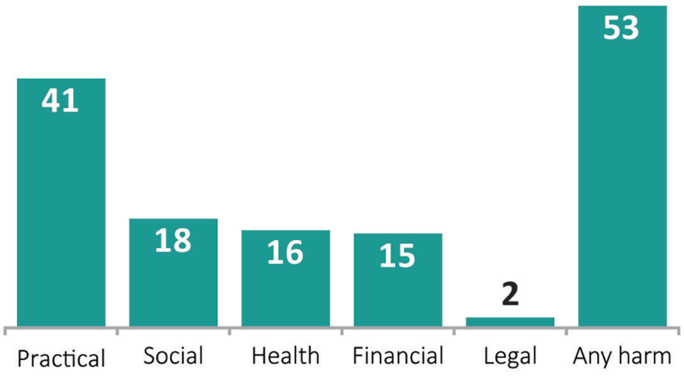
RESPONDENTS WITH HIGHER VICTIMISATION RATES

- Younger people, First Nations, non-English speakers, people with a disability
- Small business owners and operators
- More frequent internet users, more confident users
- Regular users of online subscription & streaming platforms, dating apps, online marketplaces
- Users of prevention measures (likely after falling victim)
- Higher-risk online activites, eg sharing passwords

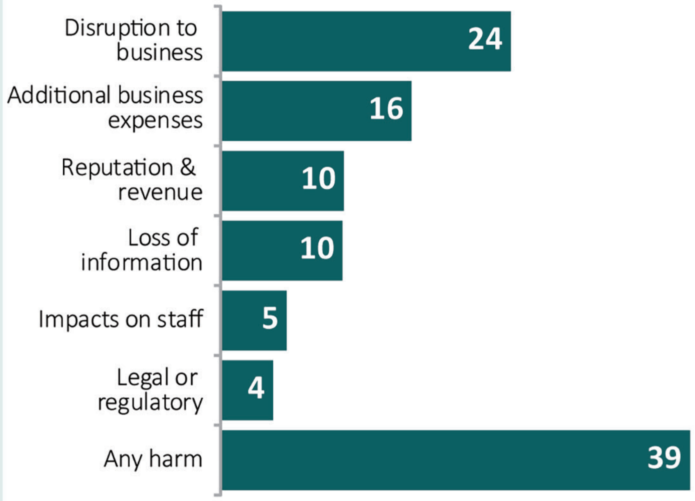
FINANCIAL LOSSES AFTER RECOVERIES (%)



HARMS REPORTED BY ALL VICTIMS (%)



HARMS TO SMALL TO MEDIUM BUSINESS VICTIMS (%)



25% of all respondents were negatively impacted by cybercrime

22% of all small to medium business owners and operators who responded to the survey reported harm to their business from cybercrime

Contents

xi Acknowledgements

xii Acronyms

1 Abstract

2 Summary

2 Victimisation

4 Victim characteristics

5 Help-seeking

6 Impact of victimisation

8 Introduction

11 Method

21 Victimisation

23 Online abuse and harassment

26 Malware

28 Identity crime and misuse

30 Fraud and scams

33 Poly-victimisation

35 Victim characteristics

35 Sociodemographic characteristics

38 Education and employment

40 Technology use and online activities

46 Digital literacy and online safety strategies

52 Help-seeking by victims following the most recent incident

52 Sources of help, advice or support

57 Reporting to police or to ReportCyber

72 Impacts of victimisation

72 Financial losses

79 Impacts on individual victims

85 Impact on small to medium businesses

88 References

92 Appendix: Survey design, sampling and weighting

92 Introduction

92 Key definitions

93 Survey design

96 Research ethics

96 Sampling and weighting

Boxes

10 Box 1: What is covered by this report?
12 Box 2: Challenges with measuring cybercrime
23 Box 3: Data breaches
28 Box 4: Ransomware
33 Box 5: Investment scams
59 Box 6: Estimating the extent of unreported cybercrime
63 Box 7: What influences help-seeking from police following a cybercrime incident?
66 Box 8: What factors influence whether cybercrimes are investigated or an offender is apprehended?
68 Box 9: Has victim satisfaction increased over time?
77 Box 10: Big financial losses or high volume, low yields?
80 Box 11: Why measure other harms from cybercrime?
87 Box 12: Cybercrime and its effects on small to medium business

Figures

14 Figure 1: Respondents by usual place of residence
22 Figure 2: Prevalence of cybercrime victimisation
26 Figure 3: Relationship between victim and offender in the most recent online abuse and harassment incident
34 Figure 4: Overlap of cybercrimes experienced by respondents
35 Figure 5: Cybercrime victimisation, by crime type and age group
40 Figure 6: Cybercrime victimisation, by crime type and social media use
41 Figure 7: Cybercrime victimisation, by crime type and frequency of internet use
42 Figure 8: Cybercrime victimisation, by crime type and number of hours spent using the internet per day for personal use
43 Figure 9: Cybercrime victimisation among respondents who were working, by crime type and number of hours spent using the internet for work
47 Figure 10: Cybercrime victimisation, by crime type and self-rated knowledge of technology
47 Figure 11: Cybercrime victimisation, by crime type and self-rated ability to use technology
53 Figure 12: Help-seeking among online abuse and harassment victims following the most recent incident
54 Figure 13: Help-seeking among malware victims following the most recent incident
55 Figure 14: Help-seeking among identity crime and misuse victims following the most recent incident

56 Figure 15: Help-seeking among fraud and scam victims following the most recent incident

57 Figure 16: Number of sources of help, advice and support among victims who sought help following the most recent incident

58 Figure 17: Help-seeking from selected sources following the most recent incident

64 Figure 18: Reasons for seeking help, advice or support from police or ReportCyber following the most recent incident, by crime type

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

67 Figure 20: Satisfaction with the outcome of reporting among victims who reported to police or ReportCyber, by crime type

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

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

73 Figure 23: Prevalence of victims who recovered any money following most recent incident

74 Figure 24: Prevalence and proportion of money recovered following most recent incident

76 Figure 25: Financial losses after recoveries for most recent incident

78 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

79 Figure 27: Median financial losses for most recent incident after recoveries, by small to medium business ownership status

80 Figure 28: Harms from cybercrime among victims

81 Figure 29: Harms from cybercrime among victims, by number of crime types reported

82 Figure 30: Harms from cybercrime among victims, by crime type

85 Figure 31: Harms to business from cybercrime among victims who owned, operated or managed a small to medium business

Tables

15 Table 1: Sociodemographic characteristics of respondents
16 Table 2: Education, employment and income of respondents
17 Table 3: Online behaviour of respondents
24 Table 4: Incidents of online abuse and harassment
27 Table 5: Symptoms of malware
29 Table 6: Incidents of Identity crime and misuse
31 Table 7: Incidents of fraud and scams
37 Table 8: Cybercrime victimisation by crime type and sociodemographic characteristics
39 Table 9: Cybercrime victimisation by crime type and respondent education, employment and income
45 Table 10: Cybercrime victimisation, by crime type and frequency of online activities
49 Table 11: Cybercrime victimisation, by use of online safety measures
51 Table 12: Cybercrime victimisation, by use of higher risk online behaviours
61 Table 13: Respondents who sought help from police or ReportCyber, by sociodemographic characteristics
62 Table 14: Respondents who sought help from police or ReportCyber following most recent incident, by business ownership status
71 Table 15: Reasons for not reporting to police or ReportCyber, by crime type
73 Table 16: Money lost, money spent on consequences and money recovered following most recent incident of cybercrime, by crime type
75 Table 17: Median financial losses for most recent incident among victims who lost any money, by payment method
83 Table 18: Harms to individual cybercrime victims
86 Table 19: Harms to small business owners, operators and managers who were victims of cybercrime
97 Table A1: Roy Morgan Research Solutions Single Source panel quotas
98 Table A2: Invitation and completion rates, Roy Morgan Single Source panel
99 Table A3: Respondents by usual place of residence (unweighted data)
100 Table A4: Respondents by usual place of residence (weighted data)
100 Table A5: Respondents by age
102 Table A6: Selected sociodemographic characteristics of respondents
102 Table A7: Lifetime prevalence of cybercrime victimisation

Acknowledgements

We acknowledge the important work of Chris Owen and Gladys Lima and colleagues from Roy Morgan Research Solutions 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 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
ACCC	Australian Competition and Consumer Commission
ACORN	Australian Cybercrime Online Reporting Network
ACS	Australian Cybercrime Survey
ACSC	Australian Cyber Security Centre
AIC	Australian Institute of Criminology
ICT	information and communication technology
LGB+	lesbian, gay, bisexual or other non-heterosexual identity
OA	online abuse and harassment
PM	profit-motivated cybercrime

Abstract

This is the first report in the Cybercrime in Australia series, which aims to provide a clearer picture of the extent of cybercrime victimisation, help-seeking and harms among Australian computer users. It is based on a survey of 13,887 computer users conducted in early 2023. In the 12 months prior to the survey, 27 percent of respondents had been a victim of online abuse and harassment, 22 percent had been a victim of malware, 20 percent had been a victim of identity crime and misuse, and eight percent had been a victim of fraud and scams. Overall, 47 percent of respondents experienced at least one cybercrime in the 12 months prior to the survey—and nearly half of all victims reported experiencing more than one type of cybercrime. Thirty-four percent of respondents had experienced a data breach. Cybercrime victimisation was not evenly distributed, with certain sections of the community more likely to have been a victim, and certain online activities associated with a higher likelihood of victimisation.

Most cybercrime victimisation went unreported to police or to ReportCyber, meaning official statistics significantly underestimate the size of the problem. 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. Some victims reported losing large sums of money, but most victims reported relatively small financial losses. This report measures, for the first time, the harms experienced by individual victims and small businesses that extend beyond these financial costs. Twenty-five percent of respondents were 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.

Summary

This is the first report in the Cybercrime in Australia series, a new series that aims to provide a clearer picture of cybercrime victimisation, help-seeking and harms among Australian computer users. Between February and March 2023, 13,887 computer users were recruited from online panels to participate in a survey about cybercrime victimisation. The survey asked about respondents' experiences of four broad categories of cybercrime: online abuse and harassment, malware attacks, identity crime and misuse, and fraud and scams.

Victimisation

Two-thirds of respondents said they had been a victim of at least one type of cybercrime measured by the survey during their lifetime. Forty-seven percent of respondents had been a victim of 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, 27.0 percent of respondents had been a victim of online abuse and harassment, 21.8 percent had been a victim of malware, 20.1 percent had been a victim of identity crime and misuse, and 7.8 percent had been a victim of fraud and scams. One in three respondents had experienced a data breach, and 26.7 percent had been notified of a data breach, a large increase from the 9.3 percent who reported being notified of a data breach in 2021 (Morgan & Voce 2022).

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 (9.8%); someone hacking into their social media or network account (4.9%); and someone sending or posting messages via electronic communication that made them feel hurt, embarrassed or unsafe (3.7%). When asked about the most recent incident, around half of these victims said it involved a stranger online (48.6%). Friends, former friends, partners, former partners, and family members accounted for around a quarter of offenders in the most recent incident (24.4%).

The most common symptom of malware that victims experienced in the past year were ads popping up on their device (6.3%), their device slowing down and acting strangely (5.4%) and people telling them that they had been sending suspicious messages and links over social media or email (4.0%). 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. This does not include victims who received a ransom message indicating their data was stolen and they had to pay to prevent it being sold or leaked online. Overall, 4.8 percent of respondents received a ransom message on their device demanding payment in the 12 months prior to the survey. This was higher than the estimated 2.1 percent of respondents in a 2021 survey who received a ransom message on their device (Voce & Morgan 2022).

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 (9.3%); receiving calls from debt collectors asking about unpaid bills they did not recognise (5.7%); and someone using their details to purchase or order something or receiving unfamiliar bills, invoices or receipts (3.0%).

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 to a fake seller or buyer online (2.2%). These online shopping scams accounted for more than one-quarter of the most recent incidents reported by victims. This was followed by providing sensitive information to a scammer pretending to be a known service institution or company, such as a bank, internet provider or post office—a common form of phishing scam (1.2%). Remote access scams were the next most common (0.7%), while 0.6 percent of respondents had fallen victim to a romance scam. Overall, 1.1 percent of respondents had fallen victim to an investment scam in the 12 months prior to the survey.

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 26.5 percent of respondents were a victim of one type of cybercrime, 20.1 percent of respondents (43.1% of all victims) were victims of two or more types of cybercrime in the 12 months prior to the survey.

Victim characteristics

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 to report having been cybercrime victims than their older counterparts.
- Men were more likely than women to be the victim of fraud and scams and online abuse and harassment.
- For each of the four types of cybercrime, First Nations respondents were significantly more likely than non-Indigenous respondents to become a victim.
- Respondents who identified as LGB+ (lesbian, gay, bisexual or other non-heterosexual orientation) were significantly more likely than heterosexual respondents to have been a victim of online abuse and harassment and malware.
- Respondents who mainly spoke a language other than English at home were more likely to have been a victim of malware, identity crime and misuse, and scams and fraud.
- Respondents with a restrictive health condition were more likely than other respondents to have been a victim of each type of cybercrime.
- Respondents currently in a relationship were less likely than respondents not in a relationship to be a victim of online abuse and harassment.
- Respondents with children living at home were more likely to have been a victim of identity crime and misuse than respondents without children.

Small to medium business owners, operators and managers experienced significantly higher rates of all types of cybercrime. 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. Respondents with higher incomes were also more likely to be the victim of online abuse and harassment, identity crime and misuse, and fraud and scams.

Some of these differences may be due to differences in online behaviour and technology use. More frequent social media use was associated with significantly higher rates of cybercrime victimisation in the 12 months prior to the survey. Among respondents who were able to estimate the amount of time they spent online, the longer they spent online for personal use, the more likely they were to be a victim of cybercrime. There was a similar relationship between internet use for work and the likelihood of cybercrime victimisation; however, the likelihood of being a victim was highest among respondents who said they spent an average of four to five hours online each work day.

Frequent use—defined as daily or weekly use—of different platforms was generally associated with a higher risk of victimisation. More frequent engagement in particular online activities was associated with a much higher likelihood of online abuse and harassment and profit-motivated cybercrime. These include using subscription-based sexually explicit interactive adult platforms; making donations or payments over gaming, streaming or fundraising platforms; being active on dating or romance websites and apps; and purchasing items from online marketplaces. These platforms may be attractive for malicious actors to exploit, as they often involve communication between strangers, registration processes, and payments between parties and the platform. Conversely, the difference in victimisation rates was much smaller—or non-existent—for more mundane uses of the internet, such as browsing or looking for information, sending emails and reading news articles online.

Respondents who used various online safety measures had a higher prevalence of cybercrime victimisation. This may be because respondents who had fallen victim to cybercrime in the 12 months prior to the survey were more likely to implement safety measures to prevent repeat victimisation. While relatively rare among respondents, certain higher risk online activities were associated with a higher likelihood of victimisation. These activities included using freely available wi-fi in a public location to conduct a financial transaction, opening emails from people or organisations they did not know, accepting friend requests from people they had not met in person, and sharing a password or a code for an account with someone else.

Help-seeking

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. The most common source of help, support or advice for victims was family and friends. Formal help-seeking was higher among identity crime and misuse victims (65.6%) and fraud and scam victims (64.4%) than online abuse and harassment victims (42.1%) and malware victims (31.8%).

Fraud and scam victims were the most likely to seek help, advice or support from the police or ReportCyber (or the Australian Cyber Security Centre (ACSC) more broadly, 22.1%), followed by online abuse and harassment victims (14.8%), identity crime victims (13.9%) and malware victims (7.9%). The likelihood of seeking help from police or ReportCyber for particular cybercrime types also varied according to the characteristics of the victim.

Most victims sought help from police or ReportCyber in order to prevent the crime happening to them again or to someone else; however, one in three victims of identity crime and misuse and two in five fraud and scam victims who sought help 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 40.9 and 49.5 percent either heard nothing, did not know what had happened, or were told nothing could be done. Overall, 6.1 percent of online abuse and harassment victims, 5.8 percent of malware victims, 5.4 percent of identity crime victims and 2.5 percent of fraud or scam victims were told by the police that someone had been arrested, charged or prosecuted.

Besides identity crime and misuse victims (where the difference was negligible), victims who reported the most recent incident to police or to ReportCyber were more likely to be satisfied than dissatisfied with the outcome of their report. Up to 43.1 percent of victims who sought help were satisfied with the outcome and up to 36.1 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 the ACSC/ReportCyber was an option, did not think the police or the ACSC/ReportCyber would be able to do anything, or did not know how or where to report the matter.

Impact of victimisation

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 (34.1%), followed by identity crime (28.7%). Direct financial losses were relatively uncommon for malware victims (4.4%) and online abuse and harassment victims (2.7%).

The proportion of victims who were able to recover money was lowest among victims of online abuse and harassment (12.9%) and highest among victims of identity crime and misuse (74.3%). The average proportion of money lost or money spent on consequences that was recovered was even lower, ranging from 5.6 percent for online abuse and harassment to 65.4 percent for identity crime and misuse victims.

Among victims who could report how much they had lost, between 67.3 percent (online abuse and harassment) and 88.7 percent (identity crime and misuse) reported having lost less than $1,000 in the most recent incident. Approximately a third (32.7%) of online abuse and harassment victims, 21.1 percent of malware victims, 11.3 percent of identity crime victims and 25.5 percent of fraud and scam victims lost more than $1,000 in the most recent incident. Seven percent of fraud and scam victims lost more than $10,000, compared with 5.5 percent of online abuse and harassment victims, 2.5 percent of malware victims and 4.1 percent of identity crime victims. A small proportion of victims, including 1.4 percent of online abuse and harassment victims and 1.7 percent of fraud and scam victims, lost more than $100,000 in the most recent incident.

The total cost per victim was calculated by summing money directly lost and money spent on consequences, then subtracting money recovered. The median total cost after recoveries was $300 for online abuse and harassment victims, $250 for malware victims, and $235 for fraud and scam victims. The median cost after recoveries for identity crime victims was $0 because the majority of victims who lost money or spent money on consequences were able to recover their money.

Victims who owned, operated or managed a small business were more likely to have lost money or spent money on consequences than other working respondents, for all types of cybercrime but particularly for malware and online abuse and harassment. Further, among those victims who did lose money or spend money on consequences, they reported a higher median financial loss. Again, this was true for all types 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, 53.1 percent of cybercrime victims were negatively impacted in some way. This means an estimated 24.7 percent of all respondents were negatively impacted by cybercrime in the 12 months prior to the survey. Forty-one percent of victims reported practical impacts, 17.9 percent reported social impacts, 15.9 percent reported health-related harms, and 15.3 percent reported financial problems. Legal issues were comparatively rare (1.8%).

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. Fraud and scam victims were the most likely to report experiencing at least one practical or social impact (48.2 and 21.5%, respectively). They were also the most likely to report financial impacts (12.3%), followed by malware victims (10.5%), while a similar proportion of fraud and scam (12.7%) and online abuse and harassment victims (12.8%) said their health was impacted in some way as a result of being a cybercrime victim in the 12 months prior to the survey.

Thirty-nine 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 22.0 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 (24.0%), additional business expenses (15.8%), harm to their reputation or revenue (10.2%), loss of information (10.0%), effects on staff (5.4%) and legal or regulatory ramifications (4.3%).

Introduction

Cybercrime refers to crime that involves a digital device, computer network or other forms of information and communication technology (ICT), and includes cyber-dependent and cyber-enabled crimes (Australian Government 2022). Cyber-dependent crimes are those directed at computers or ICT and can only exist in the digital world (Australian Government 2022). They include crimes such as ransomware, which relies on the use of malware to extort money from victims. Cyber-enabled crimes are traditional crimes that are committed using computers, computer networks or other forms of ICT, which enable the offender to increase the scale or reach of the crime (Australian Government 2022). These include profit-motivated crimes such as online fraud and identity crime and misuse, as well as online abuse and harassment, online child sexual exploitation and technology-enabled forms of domestic and family violence.

Cybercrime has become a pervasive and persistent threat to individuals, businesses and government. In Australia, as in many other countries, the use of the internet and digital technology has become an integral part of everyday life, including for day-to-day communication, entertainment and work. This reliance on technology, along with the relative wealth of its population, has made Australia an attractive target for opportunistic and motivated cybercriminals (ACSC 2022). Profit-motivated cybercrime has continued to rise in recent years, with over 76,000 reports made to ReportCyber in 2021–22—a 13 percent increase from the previous year, and equivalent to one report every seven minutes (ACSC 2022). The cost of cyber-dependent crime to individuals alone has been estimated to be $3.5 billion annually (Teunissen, Voce & Smith 2021). The Australian Competition and Consumer Commission (ACCC 2023) reported that the combined losses of reported scams were at least $3.1 billion in 2022, a substantial increase compared with the year prior. This is despite the Australian Bureau of Statistics (ABS 2023b) finding a decrease in self-reported victimisation from certain types of scams between 2020–21 and 2021–22.

Technology has also facilitated continuous communication between individuals, creating new avenues for abuse, harassment and bullying. In a survey of 4,783 Australians aged 18 to 65 years, the eSafety Commissioner (2023) found that three-quarters had at least one negative online experience in the 12 months prior to the survey, which was a marked increase from 2019. This most often involved receiving unwanted inappropriate content, being called offensive names or things of a distressing or harmful nature, and having personal information used without their consent. These negative online experiences were associated with a range of harms, and many people did not know what to do when they experienced these harms (eSafety Commissioner 2023). Similarly, a recent survey of dating app users found that three in every four respondents had been subjected to sexual violence facilitated via dating apps in the last five years (Wolbers et al. 2022).

Despite growing concerns about cybercrime in Australia, available data on cybercrimes, including current priority targets like ransomware, significantly underestimates the size of the problem (Klauzner & Pisani 2023; Morgan et al. 2016; Voce & Morgan 2022). Cybercrimes are among those least reported to police (van de Weijer, Leukfeldt & Bernasco 2019). This is partly due to the complex nature of cybercrime, which means victims may not be aware that they have been targeted, or may not know where or how to report the crime (Cross et al. 2021; Morgan et al. 2016). Additionally, many victims may feel that the police cannot help them or be fearful of the people responsible (Voce & Morgan 2022). Police face significant challenges in trying to investigate cybercrime and apprehend the offenders responsible, not least of which is that the offenders are frequently based offshore.

Large-scale surveys of the Australian public are needed to gain a more detailed picture of the nature and extent of cybercrime in Australia. These surveys provide a means of collecting data from victims who may not be captured in official data. While there are surveys that measure certain crimes that might fall within the definition of cybercrime, including scams (ABS 2023b) and online harms (eSafety Commissioner 2023), there is a need for data that can measure victimisation from different types of cybercrime, as well as information that can help inform cybercrime prevention strategies. This includes the characteristics and online activities of victims, their reporting behaviour, and the impact of cybercrime on individuals and businesses, including but not limited to the financial consequences of victimisation.

Recognising the need for better quality data about cybercrime impacting the Australian community, the Australian Cybercrime Survey (ACS) has been developed to monitor trends in cybercrime over time. This will assist in understanding and identifying emerging threats and inform the development of effective prevention and response strategies. It can be used to assess the impact of law enforcement strategies, prevention strategies and policy and legislative changes on the prevalence of cybercrime.

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 ACSC (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 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 Australian Cybercrime Survey measures crime 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 the 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**—involve 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 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 is focused on both cyber-dependent and cyber-enabled crimes, including identity crime and misuse, malware, online scams and fraud and online abuse and harassment (see Box 1).

The questionnaire was developed by the Australian Institute of Criminology. It was originally piloted in mid-2021, and the outcomes of this pilot were used to make various improvements to the design of the survey. 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, perpetration of cybercrime, harms resulting from victimisation and preventative measures. Second, there is a longitudinal component, whereby a subset of respondents from the 2023 survey will be recruited to complete the survey again in 2024. Finally, there are multiple addenda—short surveys which are each completed by a subset of respondents after the main questionnaire and which can be changed each year to explore contemporary topics.

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 ‘phishing scams’. 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. While this is not a perfect solution (eg it still relies on the respondent being able to distinguish whether their device is malfunctioning due to cybercrime or for some other reason), 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*. The survey questionnaire is available in a separate downloadable appendix.

Box 2: Challenges with measuring cybercrime

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. It spans both property and personal offences and intersects with other offline crime types. 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.

The second challenge is that cybercrime is constantly evolving. While it is true to say that the major threats to individuals, business and government are relatively constant, the modus operandi of perpetrators is constantly evolving. This 'arms race' occurs in response to both emerging opportunities and action taken to disrupt prominent forms of cybercrime. An excellent example of this is phishing scams, where the messages are constantly being refreshed. During the COVID-19 pandemic, phishing scams shifted their focus, exploiting people's fear of illness, and need to access health products and financial supports—messages that would have been unlikely to work in other contexts. This can make it difficult to spot scams, but also capture information about the different scams that people may have fallen victim to.

Different types of cybercrime are also linked. The survey measures four types. In reality, 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.

Finally, and 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 yet 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.

Recruitment, sampling and weighting

The survey was conducted by Roy Morgan Research Solutions between 8 February and 13 March 2023 using its Single Source panel and panels managed by PureProfile and Dynata. 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, sex and usual place of residence, derived from ABS population data (ABS 2023a). 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 5.4 percent; however, there is no way of verifying how many of these invitations were received. Importantly, 63.9 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*.

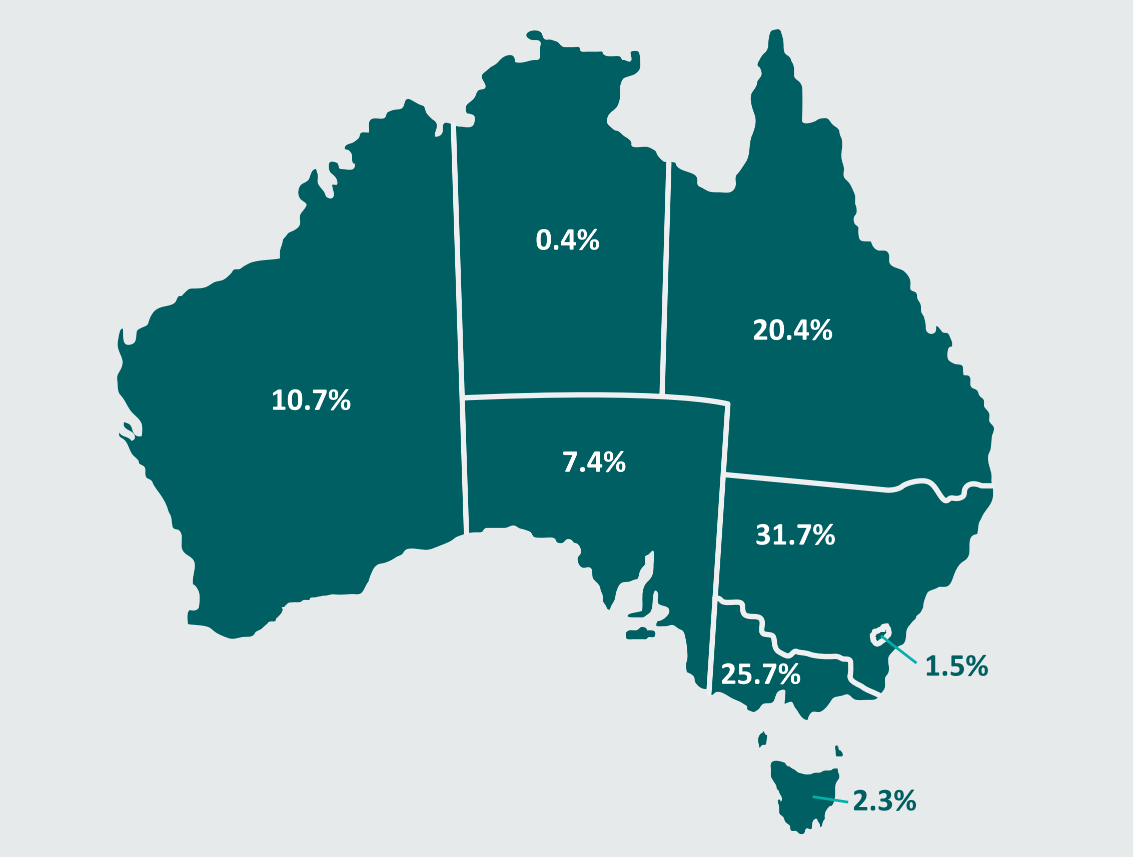
The survey took respondents an average of 24.8 minutes (*SD*=11.2) to complete. The final sample size was 13,887 respondents. The data were subsequently weighted by age, sex and usual place of residence to ensure the data were representative of the spread of the Australian population. Additional random iterative method weights (calculated from Roy Morgan's Single Source survey) were applied to correct for education level, internet 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 data presented in this report are based on weighted data.

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 (72.9%), while 23.9 percent were living in regional areas and 2.9 percent in remote areas (Table 1).

Figure 1: Respondents by usual place of residence (*n*=13,887)



Source: Australian Cybercrime Survey 2023 [weighted data]

As shown in Table 1, 29.3 percent of respondents were aged 18 to 34 years, 48.7 percent were aged 35 to 64 years, and 22.1 percent of respondents were aged 65 years and over. While 49.9 percent of the sample were male and 49.7 percent were female, 0.4 percent of respondents identified as non-binary. First Nations people accounted for 3.5 percent of respondents, while 7.9 percent of respondents identified as gay, lesbian, bisexual or some other non-heterosexual sexual identity. One in five respondents were born outside of Australia, while 4.6 percent spoke a language other than English most often at home. One in three respondents reported having a long-term health condition (33.8%), while 9.4 percent of respondents indicated that they were restricted in their everyday activities or needed help or supervision because of their health conditions.

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 representative of the Australian population in terms of key demographics.

Table 1: Sociodemographic characteristics of respondents (*n*=13,887)

	n	%
Age		
18–24	1,540	11.1
25–34	2,527	18.2
35–49	3,564	25.7
50–64	3,189	23.0
65+	3,067	22.1
Gender		
Female	6900	49.7
Male	6935	49.9
Non-binary	52	0.4
First Nations[a]	486	3.5
LGB+ respondents[b]	1,095	7.9
Born outside of Australia[c]	3,058	22.0
Speaks a language other than English most often at home[d]	632	4.6
Restrictive long-term health condition	1,308	9.4
Currently in a relationship[f]	8,784	63.3
Children living at home[g]	4,618	33.3
Usual place of residence (remoteness)		
Major city	10,124	72.9
Regional	3,325	23.9
Remote	397	2.9

a: Denominator includes 153 respondents who did not know or declined to answer the question
b: Denominator includes 174 respondents who did not know or declined to answer the question
c: Denominator includes 33 respondents who did not know or declined to answer the question
d: Denominator includes 46 respondents who did not know or declined to answer the question
e: Denominator includes 291 respondents who did not know or declined to answer the question
f: Denominator includes 103 respondents who did not know or declined to answer the question
g: Denominator includes 16 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 2023 [weighted data]

Information was also collected on the education and employment status of respondents (Table 2). Around one-third of respondents (32.1%) said their highest level of education was high school, while 40.2 percent of respondents had a university qualification. Two-thirds of respondents (64.0%) were employed, either full or part time, 21.7 percent of respondents were retired and 4.3 percent were unemployed.

Importantly, while this was a survey of individuals, one in eight respondents (12.8%, or 20.4% of respondents who were currently working) said they owned, operated or managed a small to medium business (with fewer than 200 employees). A further 4.5 percent of respondents (7.0% 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*=13,887)

	n	%
Highest education level[a]		
Year 12 or below	4,453	32.1
Vocational qualification	3,761	27.1
University graduate	5,586	40.2
Employment status[b]		
Working full-time	5,982	43.1
Working part-time, casual or semi-retired	2,902	20.9
Retired	3,015	21.7
Unemployed	596	4.3
Full-time homemaker or carer	637	4.6
Student full-time (and not working)	169	1.2
Not working for health reasons	434	3.1
Owning, operating or working for a small-to-medium enterprise (SME)[c]		
Owner or manager	1,782	20.4
Employee	2,330	26.7
Does not operate or work for an SME	4,612	52.9
Owning, operating or working for a large company or business[d]		
Owner or executive	618	7.0
Employee	2,736	30.8
Does not operate or work for a large company	5,356	60.3
Annual income[e]		
$0 – $18,200	1,551	11.2
$18,201 – $37,000	2,576	18.5
$37,001 – $80,000	4,361	31.4
$80,001 – $180,000	3,631	26.1
$180,001 and over	479	3.4

a: Denominator includes 88 respondents who did not know or declined to answer the question

b: Denominator includes 151 respondents who did not know or declined to answer the question

c: Limited to respondents who were currently working (*n*=8,884). Denominator includes 161 respondents who were working but did not know or declined to answer the question about owning or working for an SME

d: Limited to respondents who were currently working (*n*=8,884). Denominator includes 174 respondents who were working but did not know or declined to answer the question about owning or working for a large company

e: Denominator includes 1,289 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 2023 [weighted data]

Finally, information on the online behaviour of respondents is presented in Table 3. On average, respondents said they spent 3.3 hours using the internet per day for non-work/personal purposes, while those respondents who were working said they spent an average of 3.8 hours using the internet each day for work. More than half of respondents (54.4%) said they spent more than three hours a week using social media, while three-quarters of respondents (78.0%) said they used the internet three or more times a day. When asked to rate their ability to use technology, 46.7 percent rated their ability as moderate, 41.7 percent rated their ability as high, and 11.6 percent rated their ability as low. While 50.6 percent rated their knowledge of technology as moderate and 31.1 percent said it was high, 18.3 percent—nearly one in five—rated their knowledge of technology as low.

Table 3: Online behaviour of respondents (*n*=13,887)

	n	%
Average hours spent using the internet		
Personal use[a]	12,072	3.3 hours
Work-related[b]	7,337	3.8 hours
Social media use		
No social media use	2,284	16.4
Up to 3 hours per week	4,401	31.7
Between 3 and 8 hours a week	3,672	26.4
More than 8 hours a week	3,890	28.0
Internet use		
A few times a week or less	695	5.0
Once a day	1,350	9.7
Twice a day	1,011	7.3
Three or more times a day	10,830	78.0
Self-rated knowledge of technology[c]		
Very low	572	4.1
Low	1,958	14.2
Moderate	6,986	50.6
High	3,128	22.7
Very high	1,161	8.4
Self-rated ability to use technology[d]		
Very low	356	2.6
Low	1,237	9.0
Moderate	6,448	46.7
High	4,095	29.6
Very high	1,677	12.1

a: Excludes 1,815 respondents who did not know or declined to answer the question

b: 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

c: Denominator includes 83 respondents who did not know or declined to answer the question

d: Denominator includes 74 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 2023 [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 per cent chance that the observed result occurred due to chance.

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 reporting channels, such as Scamwatch (ACCC 2023; ACSC 2022). 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. 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. 2018). 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). Post-hoc weighting of demographic variables for non-probability online samples has been found to reduce the accuracy of substantive measures (Chang & Krosnick 2009; Yeager et al. 2011), although recent evidence indicates that this impact is slight and varies between surveys (Pennay et al. 2018; Yeager et al. 2011), and likely depends on the strength of the association between these demographic factors and the outcome of interest.

Importantly, data presented in the *Appendix* show that the sample is 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.

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. 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. However, the list of incidents may not capture new forms of cybercrime which were not widespread during the survey development, and some incidents may not easily fit with the descriptions provided to respondents (see Box 2). 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. It is anticipated that the list of possible indicators used to measure each type of cybercrime may need to be updated in future iterations of the survey, and this will need 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.

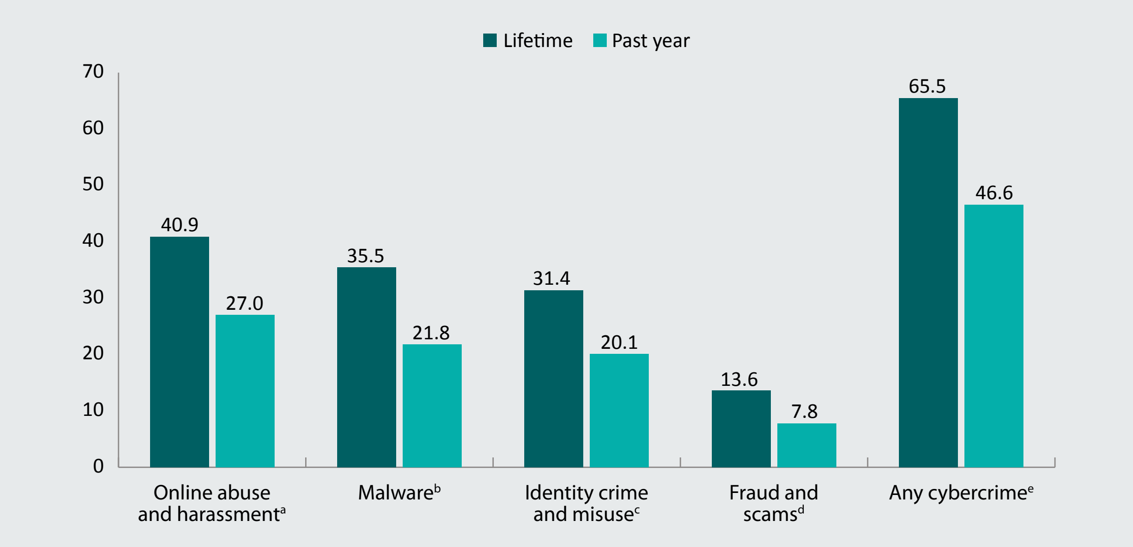
Finally, there was a large group of small to medium business owners and operators among the survey respondents. While this allows for some analysis of the prevalence of cybercrime victimisation among small to medium business operators, this was a survey of Australian individuals. The findings may not 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

Sixty-five percent of respondents had been a victim of at least one of the cybercrime types measured by the survey in their lifetime (65.5%), and nearly half had been a victim in the 12 months prior to the survey (46.6%; Figure 2). Over a quarter of the sample had been a victim of online abuse and harassment in the 12 months prior to the survey (27.0%), while one in five experienced signs of a malware attack (21.8%) or were the victims of identity crime and misuse (20.1%). Fraud and scam victimisation was less common, with eight percent of respondents having been a victim in the 12 months prior to the survey.

Despite the bottom-up approach to measuring cybercrime, a relatively large proportion of respondents—nearly one in 10—were unable or unwilling to disclose whether they had been a victim of cybercrime, or whether the most recent incident had occurred in the 12 months prior to the survey. This may be because the indicators that were used did not reflect their experience of cybercrime, because they were unaware whether they had been a victim, because of difficulties recalling when the most recent incident had occurred, or because of embarrassment. These estimates therefore potentially underestimate the scale of the problem.

Figure 2: Prevalence of cybercrime victimisation (%) (*n*=13,887)



a: 704 respondents did not know or declined to answer the question for lifetime prevalence and a further 188 respondents for past-year prevalence

b: 912 respondents did not know or declined to answer the question for lifetime prevalence and a further 292 respondents for past-year prevalence

c: 655 respondents did not know or declined to answer the question for lifetime prevalence and a further 178 respondents for past-year prevalence

d: 484 respondents did not know or declined to answer the question for lifetime prevalence and a further 56 respondents for past-year prevalence

e: 727 respondents did not know or declined to answer the question for lifetime prevalence and a further 564 respondents for past-year prevalence

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

Source: Australian Cybercrime Survey 2023 [weighted data]

Box 3: Data breaches

Recent data breaches—which are known to have affected millions of Australians—have thrust cybercrime into the public spotlight. The observation period for the survey includes the period in which the customer databases of Optus and Medibank were breached. The Latitude Financial data breach was reported in the days after the completion of data collection, and it is unlikely that respondents would have been aware of it when they completed the survey.

Overall, one in three respondents (33.6%) had their financial or personal information exposed in a data breach in the 12 months prior to the survey. An earlier survey of 14,994 respondents, conducted in mid-2021, found only 9.3 percent of respondents had been notified of a data breach (Morgan & Voce 2022). While the current survey did not specify whether respondents had been notified of a data breach, they were asked how they discovered the data breach. The majority (79.6%) said they were notified by the company whose data was leaked or by a government or financial agency, meaning that 26.7 percent of respondents had been notified of a data breach—a threefold increase on the previous survey.

Data breaches were not included in the prevalence estimate for identity crime and misuse. However, victims of identity crime and misuse may identify these breaches as the way in which their personal information was obtained. Indeed, according to McAlister et al. (2023), one in seven (14.4%) identity crime and misuse victims said that, in the most recent incident, their information was obtained during a data breach. These breaches have been shown to significantly increase the likelihood of identity theft, online scams and fraud and ransomware (Morgan & Voce 2022). The high number of data breaches—likely compounded by further breaches in early 2023, after data collection had been completed—demonstrates the importance of proactive prevention strategies.

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 4). 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 victims experienced in the past year were being sent unsolicited sexually explicit messages, images or videos (9.8%); someone hacking into their social media or network account (4.9%); and someone sending or posting mean or hurtful messages via electronic communication that made them feel hurt, embarrassed or unsafe (3.7%). In addition, 3.0 percent of respondents said that someone had set up fake social media or networking profiles pretending to be them; 2.8 percent of respondents were 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; and 2.6 percent of respondents were personally targeted by hate speech or someone making derogatory, malicious or threatening comments based on their religion, ethnicity, gender, sexuality or ideology.

Table 4: Incidents of online abuse and harassment

	Lifetime (*n*=13,887)		Past year (*n*=13,887)		Most recent incident in past year (*n*=3,750)	
	n	%	*n*	%	*n*	%
Respondent was sent unsolicited sexually explicit messages, images or videos	2,297	16.5	1,366	9.8	1,065	28.7
Someone hacked into respondent’s social media or network account (including communicating with respondent’s contacts or posting messages or status updates from their accounts)	1,459	10.5	673	4.6	497	13.4
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	1,291	9.3	512	3.7	283	7.6
Someone set up fake social media or networking profiles pretending to be respondent (eg communicated with respondent’s contacts or posted messages or status updates from their accounts)	939	6.8	416	3.0	274	7.4
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	815	5.9	391	2.8	258	7.0
Someone subjected respondent to hate speech or made derogatory, malicious or threatening comments directly to them based on religion, ethnicity, gender, sexuality or ideology	785	5.7	355	2.6	169	4.6
Someone used technology to stalk or repeatedly harass respondent, including being contacted by someone they had blocked or asked to not contact them	861	6.2	349	2.5	199	5.4

Table 4: Incidents of online abuse and harassment (continued)

	Lifetime (*n*=13,887)		Past year (*n*=13,887)		Most recent incident in past year (*n*=3,750)	
	n	%	*n*	%	*n*	%
Someone stole respondent's online personal information (including photos and videos) and used it without their permission	700	5.0	303	2.2	156	4.2
Someone spread rumours about respondent via electronic communication (eg emails, social media or text messages)	861	6.2	283	2.0	131	3.5
Someone restricted respondent's access to online resources (eg social media, electronic legal documents, banking and utility accounts)	511	3.7	241	1.7	143	3.9
Someone published identifying information (eg respondent's full name, contact number, address, school) with malicious intent (ie doxxing)	513	3.7	223	1.6	129	3.5
Someone monitored respondent's activity online or on their phone (eg installing spyware, going through their private messages)	547	3.9	221	1.6	115	3.1
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 (eg sextortion)	472	3.4	192	1.4	92	2.5
Someone tried to stop respondent from communicating with others online or over a mobile	439	3.2	173	1.3	72	1.9
Someone shared or published sensitive, personal, compromising or intimate photos or videos of respondent without their consent	366	2.5	128	0.9	58	1.6
Someone sent or posted photos and videos of respondent to others to try and embarrass, hurt or blackmail them	431	3.1	124	0.8	49	1.3
Someone created fake videos or photos of respondent (eg 'deep fakes')	238	1.7	78	0.6	21	0.6
At least one of the above	5,721	41.2	3,749	27.0	–	–
More than one type of online abuse and harassment	3,094	22.3	1,192	8.6	–	–
None of the above	8,165	58.8	10,137	73.0	–	–
Unknown[a]	704	5.1	892	6.4	38	1.0

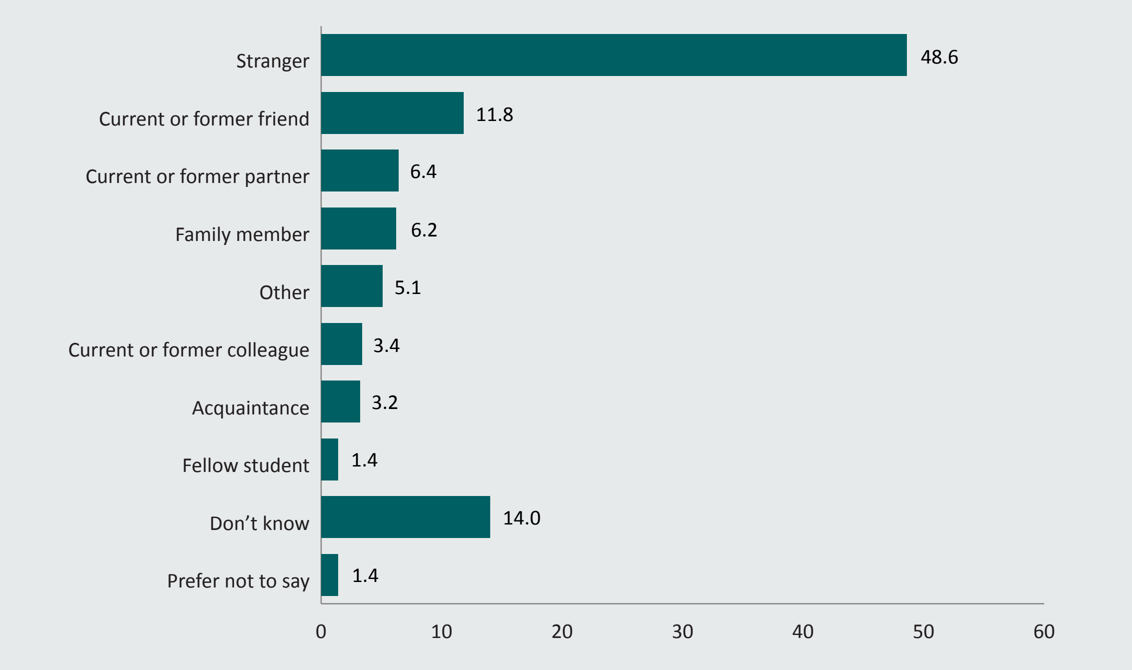
a: Includes respondents who did not know or declined to answer the question

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

Source: Australian Cybercrime Survey 2023 [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). Around half of the incidents involved a stranger online (48.6%). The victim did not know who the perpetrator was in around one in seven incidents (14.0%). Friends, former friends, partners, former partners, and family members accounted for around a quarter of offenders in the most recent incident (24.4%). Most often this was a current or former friend (11.8%) or current or former intimate partner (6.4%). One in eight 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.

Figure 3: Relationship between victim and offender in the most recent online abuse and harassment incident (%) (*n*=3,712)



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 38 respondents who did not answer questions about the most recent incident. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2023 [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 5).

The most common symptom of malware that victims experienced in the past year were ads starting to pop up everywhere on their device (6.3%), their device slowing down and acting strangely (5.4%) and people telling them that they had been sending suspicious messages and links over social media or email (4.0%).

Table 5: Symptoms of malware

	Lifetime (*n*=13,887)		Past year (*n*=13,887)		Most recent incident in past year (*n*=3,031)	
	n	%	*n*	%	*n*	%
Pop-up ads started popping up everywhere	1,948	14.0	869	6.3	629	20.7
Respondent's device slowed down and acted strangely	1,552	11.2	748	5.4	462	15.2
People respondent knew told them they had been sending suspicious messages and links over social media or email	1,139	8.2	549	4.0	436	14.5
Respondent's devices kept crashing for some reason	1,036	7.5	420	3.0	228	7.5
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	776	5.6	381	2.7	315	10.5
Respondent's browser kept getting redirected when they tried to search for a familiar site	855	6.2	315	2.3	182	6.0
Respondent's device was working excessively while no programs were running	718	5.2	283	2.0	151	4.9
There was a lack of storage space that respondent couldn't explain	601	4.3	272	2.0	162	5.3
Programs were opening and closing automatically	642	4.6	232	1.7	110	3.6
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	503	3.6	203	1.5	117	3.9
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	489	3.5	154	1.1	108	3.6
Previously accessible system tools (such as personalised or security settings) were disabled	287	2.1	102	0.7	44	1.5
Respondent's files had gone missing or been replaced with odd file extensions and the icons for the files were blank	304	2.2	99	0.7	57	1.9
At least one of the above	4,922	35.5	3,031	21.8	–	–
More than one type of malware	2,634	19.0	963	6.9	–	–
None of the above	8,964	64.5	10,856	78.2	–	–
Unknown[a]	912	6.6	1204	8.7	31	1.0

a: Includes 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 2023 [weighted data]

Box 4: Ransomware

Ransomware continues to be a major concern. While significant attention has been given to ransomware attacks against companies that have been a target of a mass data breach, as well as critical services and infrastructure, ransomware can also impact individual computer users.

For the purpose of the survey, ransomware victimisation was defined as experiencing signs of a malware attack, usually encryption, along with demands of payment to restore functionality; to restore access to systems, devices or files; or to prevent data or information from being leaked or sold online. Based on this definition, 2.4 percent of respondents (*n*=331) had experienced this kind of ransomware victimisation in the 12 months prior to the survey.

More than half of ransomware victims reported their 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 (*n*=203, 1.5% of all respondents). Others reported that their systems, devices or files had a virus or were inaccessible (eg locked or unreadable) and that they had received instructions for paying a ransom to restore access (*n*=154, 1.1% of all respondents). Further, 11.7 percent of ransomware victims (*n*=39, 0.3 percent of all respondents) said they had been extorted for payment to prevent the data being leaked or sold online, a practice known as 'double extortion'.

However, not all respondents who said they had received a ransom message said their device had been encrypted or disrupted. A further 2.4 percent of respondents said they had received a ransom message in the 12 months prior to the survey that said their data had been stolen and they had to pay to prevent the information being sold or leaked online, but did not report their device as having been disrupted or compromised. These may be true ransomware attacks where the data have actually been stolen, or fake attacks in which malicious actors pretend to have stolen data to demand payment. Overall, 4.8 percent of respondents received a ransom message on their device demanding payment in the 12 months prior to the survey (with or without device disruption or compromise). This was higher than the estimated 2.1 percent of respondents who received a ransom message on their device in a 2021 survey (Voce & Morgan 2021).

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. While the way in which this information is collected has changed, this is the same definition used in the AIC's previous identity crime and misuse surveys (see McAlister & Franks 2021 for the most recent report).

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 (9.3%); receiving calls from debt collectors asking about unpaid bills they did not recognise (5.7%); and someone using their details to purchase or order something or receiving unfamiliar bills, invoices or receipts (3.0%; Table 6).

Table 6: Incidents of Identity crime and misuse

	Lifetime (*n*=13,887)		Past year (*n*=13,887)		Most recent incident in past year (*n*=2,787)	
	n	%	*n*	%	*n*	%
Suspicious transactions appeared in respondent's bank statements or accounts, credit card or credit report	2,337	16.8	1,285	9.3	1,140	40.9
Respondent received calls from debt collectors asking about unpaid bills they did not recognise	1,274	9.2	788	5.7	707	25.4
Someone used respondent's details to purchase or order something or they received unfamiliar bills, invoices or receipts	852	6.1	413	3.0	259	9.3
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	271	2.0	138	1.0	96	3.4
Respondent was unsuccessful in applying for credit, and this was surprising given their credit history	279	2.0	132	1.0	104	3.7
Someone used respondent's personal details (including images) to create an impersonation account to extort their contacts	256	1.8	128	0.9	98	3.5
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	257	1.9	119	0.9	81	2.9
Someone tried to obtain money from one of respondent's investments or superannuation accounts	213	1.5	91	0.7	57	2.1
Someone used respondent's personal details to create a fake cryptocurrency wallet or exchange account	132	1.0	64	0.5	38	1.4
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	151	1.1	62	0.4	44	1.6
Someone gained access to respondent's cryptocurrency wallet or exchange account and made transactions or stole currency	128	0.9	60	0.4	37	1.3

Table 6: Incidents of Identity crime and misuse (continued)

	Lifetime (*n*=13,887)		Past year (*n*=13,887)		Most recent incident in past year (*n*=2,787)	
	n	%	*n*	%	*n*	%
Someone used respondent's personal details to fraudulently apply for government benefits	124	0.9	59	0.4	36	1.3
Someone used respondent's personal details to attempt to give false info to police	150	1.1	46	0.3	30	1.1
Someone used respondent's personal details to attempt to apply for a job or rent a property	131	1.0	44	0.3	24	0.9
Respondent was unable to file taxes because someone had already filed a tax return in their name	117	0.8	35	0.3	21	0.6
At least one of the above	4,361	31.4	2,787	20.1	–	–
More than one type of identity crime and misuse	1,377	9.9	485	3.5	–	–
None of the above	9,527	68.6	11,100	79.9	–	–
Unknown[a]	655	4.7	833	6.0	14	0.5

a: Includes 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 2023 [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 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 to a fake seller or buyer online (2.2%; Table 7). These online shopping scams accounted for more than one-quarter of the most recent incidents reported by victims. This was followed by providing sensitive information to a scammer pretending to be a known service institution or company, such as a bank, internet provider or post office—a common form of phishing scam (1.2%). Next most common were remote access scams, in which the respondent allowed someone pretending to be from a telecommunications or computer company to remotely access their computer, paid them money or provided sensitive information (0.7%). A similar proportion of respondents (0.6%) had fallen victim to a health or medical product scam, while 0.6 percent of respondents had fallen victim to a romance scam, in which they paid money, provided sensitive information or sent intimate images or videos to a scammer pretending to be a potential romantic partner.

Table 7: Incidents of fraud and scams

	Lifetime (*n*=13,887)		Past year (*n*=13,887)		Most recent incident in past year (*n*=1,082)	
	n	%	*n*	%	*n*	%
Respondent paid money or provided sensitive information to a fake seller or buyer online	550	4.0	299	2.2	284	26.2
Respondent provided sensitive information to a scammer pretending to be a known service institution or company (eg bank, internet provider, post office)	283	2.0	166	1.2	136	12.6
Respondent allowed someone pretending to be a telecommunications or computer company to remotely access their computer, or paid them money or provided sensitive information	287	2.1	93	0.7	75	6.9
Respondent paid money for health products, medicines or drugs from an online pharmacy and the products never arrived or were counterfeit	178	1.3	87	0.6	76	7.0
Respondent sent money to a scammer posing as a known business supplier, service institution or company telling them that their banking details had changed	180	1.3	78	0.6	60	5.5
Respondent paid money, provided sensitive information or sent intimate images or videos to a scammer pretending to be a potential romantic partner	133	1.0	70	0.5	53	4.9
Respondent lost money buying sports betting prediction software, or becoming the member of a sport betting syndicate or investment scheme, because these schemes did not work as advertised	108	0.8	57	0.4	35	3.3
Respondent lost cryptocurrency to a scammer in a pretend ‘give away’, business opportunity or investment opportunity	98	0.7	56	0.4	42	3.9
Respondent lost cryptocurrency in an exit scam or ‘rug-pull’, where cryptocurrency developers or promoters abandon a project and disappear with investors’ funds.	120	0.9	54	0.4	41	3.8
Respondent paid money or provided sensitive information to a scam offering the false promise of prize money or a holiday package	124	0.9	53	0.4	28	2.6
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	113	0.8	51	0.4	35	3.2

Table 7: Incidents of fraud and scams (continued)

	Lifetime (*n*=13,887)		Past year (*n*=13,887)		Most recent incident in past year (*n*=1,082)	
	n	%	*n*	%	*n*	%
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	120	0.9	51	0.4	42	3.9
Respondent paid money or provided sensitive information to a scam offering them the false promise of an inheritance or share in a large sum of money in exchange for assistance	80	0.6	42	0.3	34	3.1
Respondent paid money or provided sensitive information to a scammer pretending to be a charity or disaster relief effort	95	0.7	41	0.3	27	2.5
Respondent paid money or provided sensitive information to a scam falsely offering a rebate from the government, a bank or trusted organisation	76	0.6	36	0.3	25	2.4
Respondent paid for extremely high call or text rates when replying to unsolicited SMS competitions	115	0.8	34	0.2	28	2.6
Respondent lost money or provided sensitive information to a scammer offering a job or employment	97	0.7	33	0.2	27	2.5
Respondent paid a fake invoice for directory listings, advertising, domain name renewals or office supplies	83	0.6	33	0.2	17	1.6
At least one of the above	1,890	13.6	1,082	7.8	–	–
More than one type of fraud or scam	499	3.6	150	1.1	–	–
None of the above	11,997	86.4	12,805	92.2	–	–
Unknown[a]	484	3.5	540	3.9	18	1.6

a: Includes 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 2023 [weighted data]

Box 5: Investment scams

The ACCC reported that, in 2022, investment scams caused the most financial loss of any scam activity, accounting for more than two-thirds of all financial losses reported to Scamwatch (ACCC 2023). They defined investment scams as schemes where scammers offer fake opportunities to invest money with the promise of high returns and low risk, and provided examples such as imposter bond scams, initial public offering scams and money recovery scams.

Several questions in the ACS related to investment scams. Respondents were asked whether they had:

- lost cryptocurrency to a scammer in a pretend ‘give away’, business opportunity or investment opportunity (0.4% of respondents);
- 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% of respondents); and
- lost cryptocurrency in an exit scam or ‘rug-pull’, where cryptocurrency developers or promoters abandon a project and disappear with investors’ funds (0.4% of respondents).

Overall, 1.1 percent of respondents fell victim to one of these investment scams in the 12 months prior to the survey.

Poly-victimisation

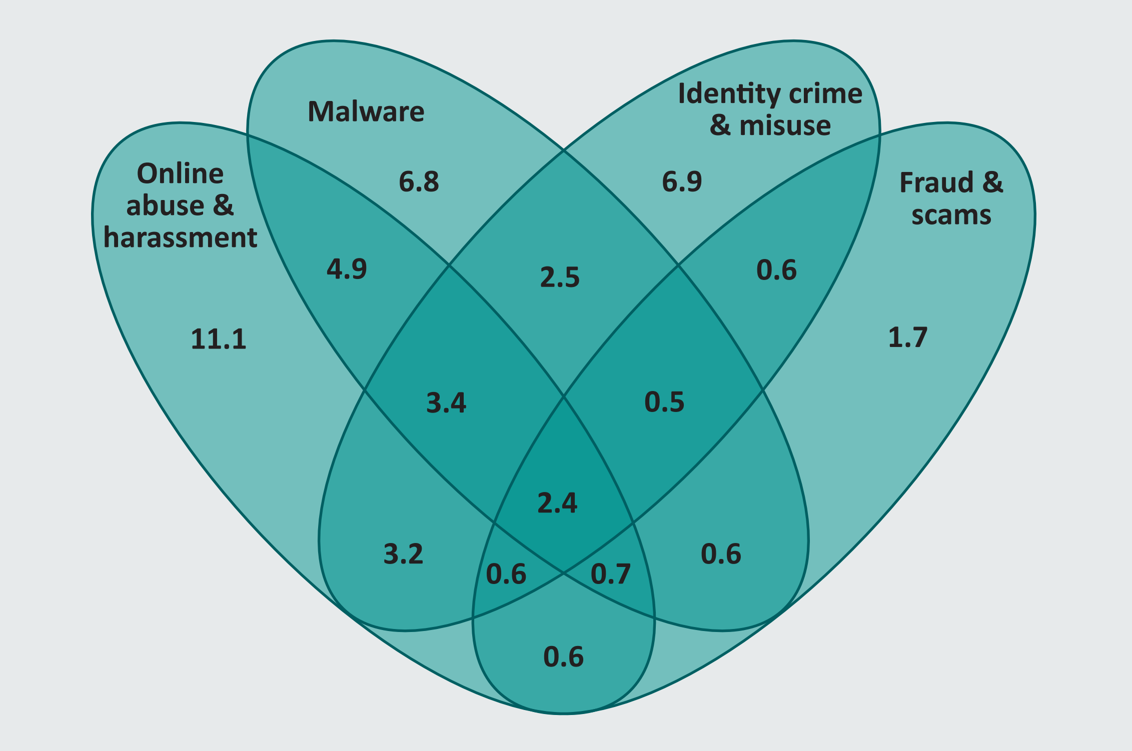
It was common for cybercrime victims to experience multiple incidents, indicators or symptoms of the same type of cybercrime in the 12 months prior to the survey:

- 30.7 percent of online abuse and harassment victims experienced multiple types of online abuse and harassment;
- 30.7 percent of malware victims experienced multiple symptoms of malware;
- 16.9 percent of identity crime and misuse victims experienced multiple types of identity crime and misuse; and
- 12.3 percent of fraud and scam victims experienced multiple types of fraud or scams.

It is not possible to determine with certainty whether these relate to separate incidents, or whether one incident involved different types of offending behaviours. In the case of malware, it is likely that a victim would have experienced multiple symptoms as part of the same malware attack.

It was also common for cybercrime victims to report having experienced multiple types of cybercrime in the 12 months prior to the survey (Figure 4). Victims of fraud and scams were the most likely to also be a victim of another cybercrime type (78.2%), while victims of online abuse and harassment were the least likely to also be victims of other types of cybercrime (58.9%). Overall, 26.5 percent of respondents were a victim of one type of cybercrime, while 20.1 percent of respondents (43.1% of all victims) were victims of two or more types of cybercrime in the 12 months prior to the survey. There was a small group of respondents—2.4 percent of respondents, or 5.1 percent of all victims—who reported having experienced all four types of cybercrime measured by the survey in the 12 months prior to the survey.

Figure 4: Overlap of cybercrimes experienced by respondents (%) (*n*=13,887)



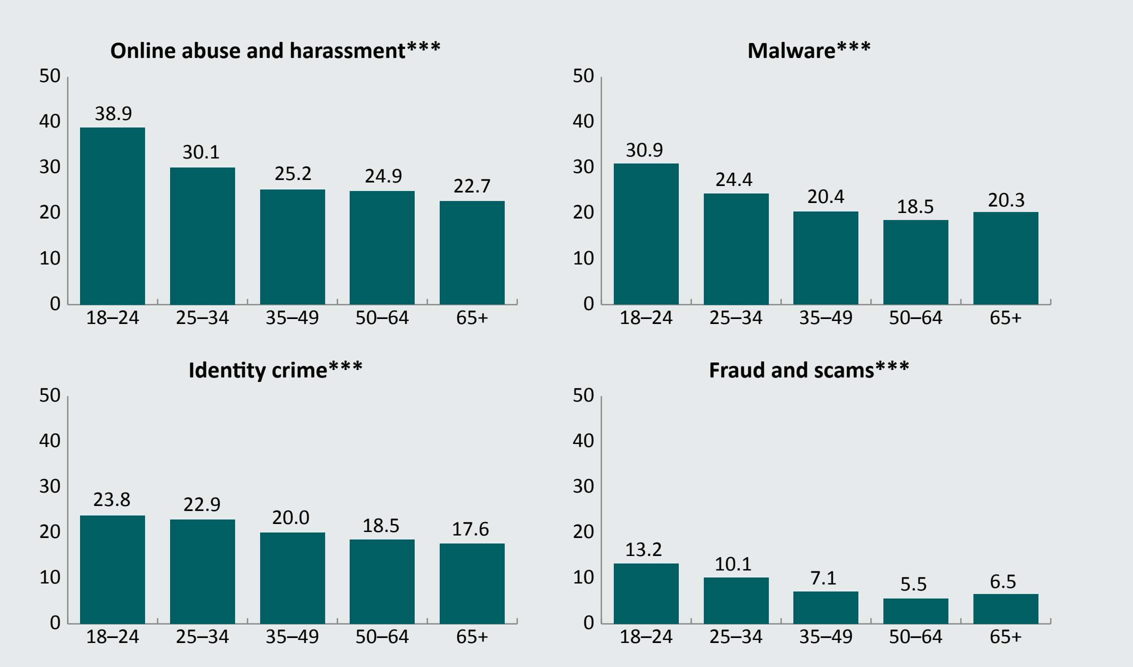
Note: Weighted percentages may not add to total due to rounding
Source: Australian Cybercrime Survey 2023 [weighted data]

Victim characteristics

Sociodemographic characteristics

Younger respondents were consistently more likely to be cybercrime victims than their older counterparts (Figure 5). The prevalence of past-year online abuse and harassment was highest among respondents aged 18 to 24 years (38.9%) and lowest among respondents aged 65 years and above (22.7%). The pattern was similar for malware and identity crime and misuse, which were highest among respondents aged 18 to 24 years (malware: 30.9%, identity crime and misuse 23.8%). However, for malware, the prevalence of victimisation was slightly higher among respondents aged 65 years and over (20.3%) than respondents aged 50 to 64 years (18.5%). The prevalence of fraud and scams was also highest among respondents aged 18 to 24 years (13.2%) and lowest among respondents aged 50 to 64 years (5.5%). The prevalence increased slightly for respondents aged 65 years and over (6.5%).

Figure 5: Cybercrime victimisation, by crime type and age group (%) (*n*=13,887)



***statistically significant at *p*<0.001

Note: Sample sizes of age groups are as follows: 18–24 years, *n*=1,540; 25–34 years, *n*=2,527; 35–49 years, *n*=3,564; 50–64 years, *n*=3,189; 65 years and over, *n*=3,067. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2023 [weighted data]

The prevalence of different cybercrimes according to respondent characteristics is presented in Table 8. Several key differences emerged:

- Men were more likely than women to be the victim of fraud and scams (9.1% vs 6.4%) and online abuse and harassment (28.4% vs 25.4%).
- Non-binary respondents were more likely to be the victim of online abuse and harassment (59.0%) than men (28.4%) and women (25.4%). Non-binary respondents were also more likely to be the victim of fraud and scams (15.0%) than men (9.1%) and women (6.4%).
- First Nations respondents had a significantly higher prevalence of victimisation across all types of cybercrime. They were around twice as likely as non-Indigenous respondents to experience online abuse and harassment (55.3% vs 25.9%), malware (41.6% vs 21.1%), and identity crime (41.0% vs 19.4%), and four times as likely to become the victim of fraud or scams (28.6% vs 7.0%).
- Respondents who identified as LGB+ were significantly more likely than heterosexual respondents to have been a victim of online abuse and harassment (40.5% vs 25.9%) and malware (24.8% vs 21.6%).
- Compared with other respondents, respondents who mainly spoke a language other than English at home were more likely to have been a victim of malware (28.1% vs 21.5%), identity crime and misuse (25.6% vs 19.8%) and scams and fraud (12.6% vs 7.5%).
- Respondents with a restrictive health condition were more likely than other respondents to have been a victim of online abuse and harassment (36.9% vs 25.9%), malware (30.5% vs 20.9%), identity crime and misuse (25.0% vs 19.6%) and fraud and scams (13.2% vs 7.2%).
- Respondents currently in a relationship were less likely than respondents not in a relationship to be the victim of online abuse and harassment (28.7 vs 25.9%).
- Respondents with children living at home were significantly more likely to have been a victim of identity crime and misuse than respondents without children (21.7% vs 19.3%).

Table 8: Cybercrime victimisation by crime type and sociodemographic characteristics (%) (*n*=13,887)

	Online abuse and harassment	Malware	Identity crime and misuse	Fraud and scams
Gender				
Female (*n*=6,935)	25.4***	21.3	20.1	6.4***
Male (*n*=6,900)	28.4	22.3	20.1	9.1
Non-binary (*n*=51)[a]	59.0	21.7	16.5	15.0
First Nations[b]				
Yes (*n*=486)	55.3***	41.6***	41.0***	28.6***
No (*n*=13,249)	25.9	21.1	19.4	7.0
LGB+[c]				
Yes (*n*=1,095)	40.5***	25.4*	22.9	9.7
No (*n*=12,618)	25.9	21.6	19.9	7.7
Born outside of Australia[d]				
Yes (*n*=3,058)	26.9	23.4	19.4	9.0
No (*n*=10,796)	27.0	21.4	22.3	7.4
Speaks a language other than English most often at home[e]				
Yes (*n*=632)	27.9	28.1***	25.6***	12.6***
No (*n*=13,209)	26.9	21.5	19.8	7.5
Restrictive long-term health condition[f]				
Yes (*n*=1,308)	36.9***	30.5***	25.0***	13.2***
No (*n*=12,170)	25.9	20.9	19.6	7.2
Currently in a relationship[g]				
Yes (*n*=8,784)	25.9**	21.9	20.5	7.5
No (*n*=5,000)	28.7	21.7	19.5	8.2
Children living at home[h]				
Yes (*n*=4,618)	26.7	22.4	21.7**	8.1
No (*n*=9,253)	27.1	21.5	19.3	7.1

***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. Excludes 2 respondents who identified as ‘Other’ gender

b: Excludes 153 respondents who did not know or declined to answer the question

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

d: Excludes 33 respondents who did not know or declined to answer the question

e: Excludes 46 respondents who did not know or declined to answer the question

f: Excludes 409 respondents who did not know or declined to answer the question

g: Excludes 80 respondents who did not know or declined to answer the question, and 23 who described their relationship as ‘other’

h: Excludes 16 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 2023 [weighted data]

Education and employment

Victimisation varied according to the respondents' employment status (Table 9). Unemployed respondents were the most likely to experience online abuse and harassment (32.5%) and fraud and scams (9.2%), while employed respondents were the most likely to have been a victim of malware (23.0%) and identity crime and misuse (21.3%).

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 (37.6% vs 24.7%), malware (30.0% vs 19.1%), identity crime (28.4% vs 17.8%) and fraud and scams (14.5% vs 5.4%).

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 (25.1% vs 30.7%), a malware attack (16.9% vs 26.5%), identity crime and misuse (17.1% vs 23.7%) and fraud or scams (4.2% vs 10.4%). Owners or executives of large companies were also more likely than employees to say they had been a victim of malware (24.1%), identity crime and misuse (21.5%) and fraud and scams (9.7%).

Respondents with higher incomes were also significantly more likely to be the victim of online abuse and harassment (31.4%), identity crime and misuse (27.4%) and fraud and scams (10.2%). Rates of victimisation were consistently lowest among respondents in the lowest income bracket.

Table 9: Cybercrime victimisation by crime type and respondent education, employment and income (%) (*n*=13,887)

	Online abuse and harassment	Malware	Identity crime and misuse	Fraud and scams
Employment status[a]				
Employed (*n*=8,884)	28.4***	23.0***	21.3***	8.3*
Unemployed (*n*=596)	32.5	22.2	20.4	9.2
Other (*n*=4,336)	23.5	19.7	17.6	6.7
Owning, operating or working for a small to medium business[b]				
Small business owner or manager (*n*=1,782)	37.6***	30.0***	28.4***	14.5***
Small business employee (*n*=2,330)	29.3	26.0	23.4	9.4
Working, but does not operate or work for a small business (*n*=4,612)	24.7	19.1	17.8	5.4
Owning, operating or working for a large company or business[c]				
Large company owner or executive (*n*=618)	26.3***	24.1***	21.5***	9.7***
Large company employee (*n*=2,736)	25.1	16.9	17.1	4.2
Working, but does not operate or work for a large company (*n*=5,356)	30.7	26.5	23.7	10.4
Annual income[d]				
$0 – $18,200 (*n*=1,551)	24.5	20.4	14.8	5.3
$18,201 – $37,000 (*n*=2,576)	28.9	22.9	20.1	9.4
$37,001 – $80,000 (*n*=4,361)	28.1	22.2	20.5	7.9
$80,001 – $180,000 (*n*=3,631)	27.6	22.5	22.0	8.5
$180,001+ (*n*=479)	31.4*	23.3	27.4***	10.2**

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

a: Excludes 71 respondents who did not know or declined to answer the question

b: Excludes 5,003 respondents who were not currently working and 160 respondents who did not know or declined to answer the question

c: Excludes 5,003 respondents who were not currently working and 174 respondents who did not know or declined to answer the question

d: Excludes 1,289 respondents who did not know or declined to answer the question

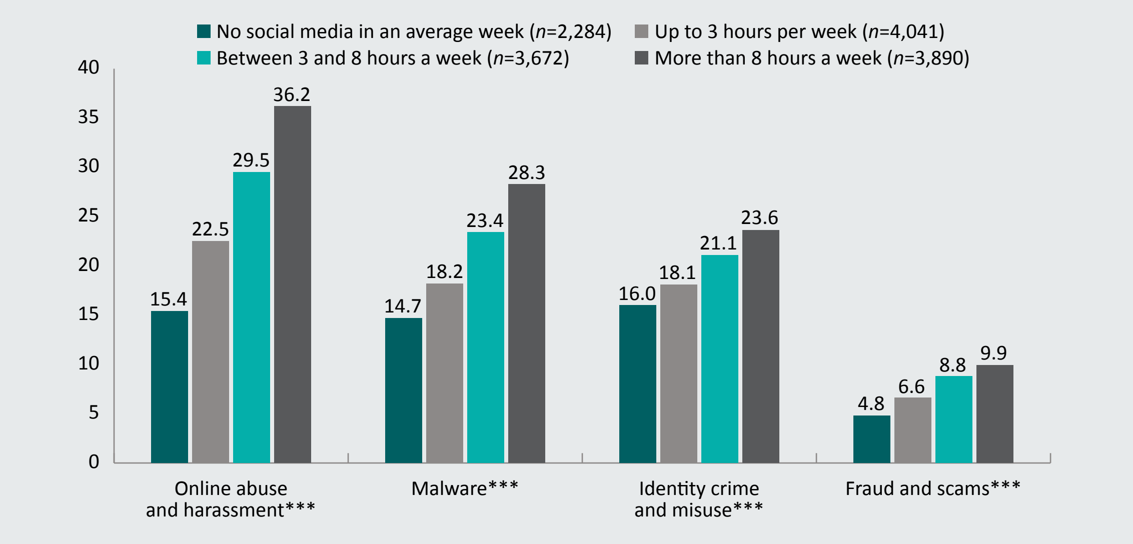
Note: A small to medium business was defined as having fewer than 200 employees, while a large business or company was defined as having 200 or more employees (ABS 2022a). Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2023 [weighted data]

Technology use and online activities

The survey included a range of questions about the nature and frequency of respondents' internet and technology use. This included questions about social media and internet use, hours spent online, and the types of websites and platforms used. More frequent social media use was associated with significantly higher rates of cybercrime victimisation in the 12 months prior to the survey (Figure 6). Respondents who used social media the most frequently—for more than eight hours per week—had the highest prevalence of online abuse and harassment (36.2%), malware (28.3%), identity crime (23.6%) and fraud and scam (9.9%) victimisation. Respondents who said they did not use social media in an average week had the lowest prevalence of online abuse and harassment (15.4%), malware (14.7%), identity crime and misuse (16.0%) and fraud and scam (4.8%) victimisation.

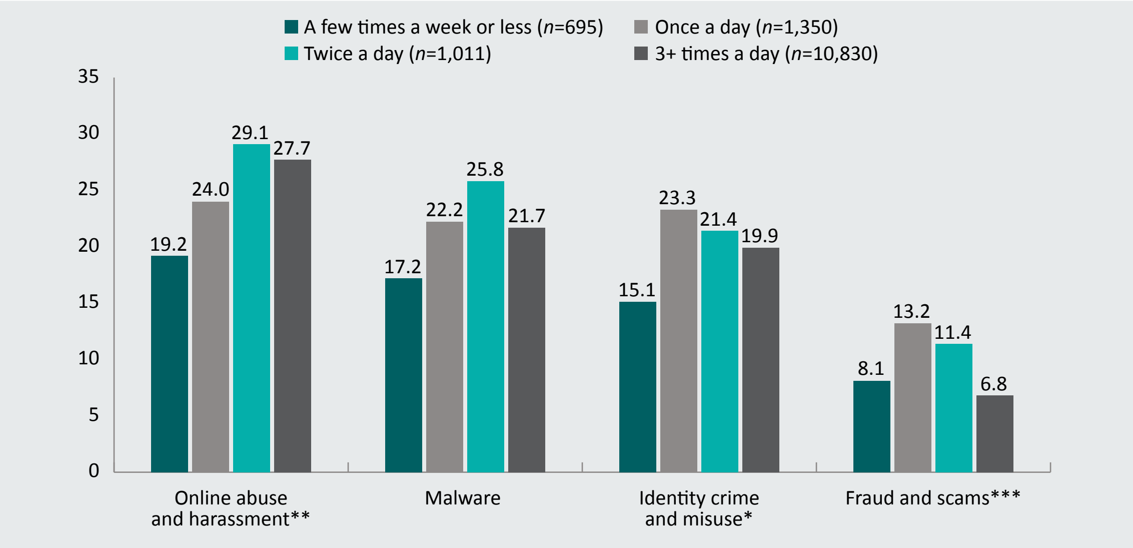
Figure 6: Cybercrime victimisation, by crime type and social media use (%)



***statistically significant at *p*<0.001
Note: Weighted frequencies and percentages may not add to total due to rounding
Source: Australian Cybercrime Survey 2023 [weighted data]

All cybercrimes except malware were related to the frequency of internet use (Figure 7). While the majority of respondents reported using the internet three or more times a day, and frequent internet users accounted for most cybercrime victims, victimisation was most common among respondents who reported using the internet once or twice a day. For online abuse and harassment and malware, victimisation was highest among respondents who said they used the internet twice a day on average (29.1% and 25.8%, respectively). For identity crime and misuse and fraud and scams, victimisation was highest among respondents who reported using the internet once per day (23.3% and 13.2%, respectively).

Figure 7: Cybercrime victimisation, by crime type and frequency of internet use (%)



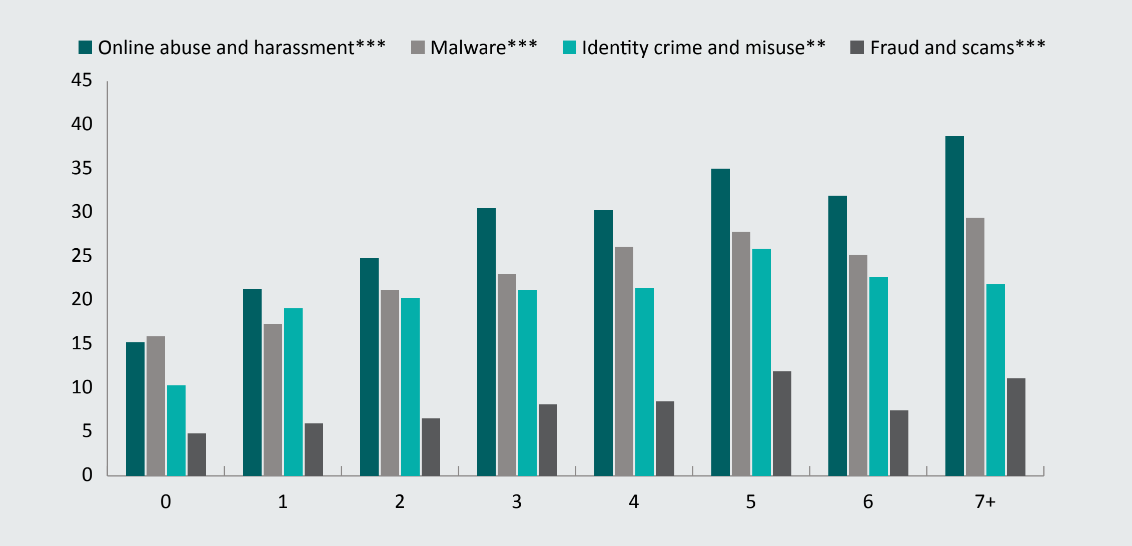
***statistically significant at *p*<0.001, **statistically significant at *p*<0.01, *statistically significant at *p*<0.05
Note: Weighted frequencies and percentages may not add to total due to rounding
Source: Australian Cybercrime Survey 2023 [weighted data]

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. A significant proportion of respondents were unable to estimate the amount of time they spent online, both for personal (13% of respondents) and work use (11% of respondents who were working).

Among those respondents who were able to estimate the amount of time they spent online, the longer they spent online for personal use, the more likely they were to be a victim of cybercrime. This was true for all four forms of cybercrime (Figure 8):

- For online abuse and harassment, the mean number of hours online was 3.4 hours for victims and 2.9 hours for non-victims. Further, 38.7 percent of respondents who said they spent seven or more hours online per day were a victim in the 12 months prior to the survey.
- For malware, the mean number of hours online was 3.3 hours for victims and 3.0 hours for non-victims. Among respondents who said they spent seven or more hours online per day, 29.4 percent were a victim in the 12 months prior to the survey.
- For identity crime and misuse, the mean number of hours online was 3.4 hours for victims and 3.0 hours for non-victims. Around a fifth of respondents who said they spent seven or more hours online were a victim in the 12 months prior to the survey (21.8%).
- For fraud and scams, the mean number of hours online was 3.5 hours for victims and 3.0 hours for non-victims. Among respondents who said they spent seven or more hours online per day, 11.1 percent were a victim in the 12 months prior to the survey.

Figure 8: Cybercrime victimisation, by crime type and number of hours spent using the internet per day for personal use (%)



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

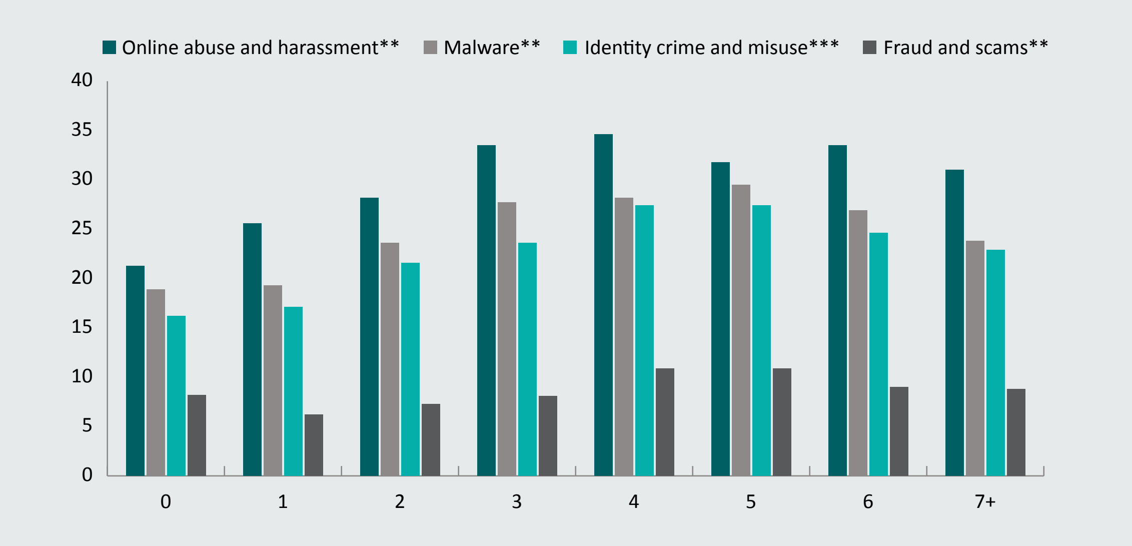
Note: Sample sizes: 0 hours *n*=210; 1 hour *n*=2,464; 2 hours *n*=3,178; 3 hours *n*=2,161; 4 hours *n*=1,543; 5 hours *n*=911; 6 hours *n*=529; 7+ hours *n*=1,076. Excludes 1,815 respondents who did not know or declined to answer the question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2023 [weighted data]

There was a similar relationship between internet use for work and the likelihood of cybercrime victimisation (Figure 9). However, while the likelihood of being a victim increased alongside the time spent online for work, it peaked among respondents who said they spent an average of four to five hours a day online:

- For online abuse and harassment, the mean number of hours online for work was 4.1 hours for victims and 3.7 hours for non-victims.
- For malware, the mean number of hours online for work was 4.1 hours for victims and 3.7 hours for non-victims.
- For identity crime and misuse, the mean number of hours online for work was 4.2 hours for victims and 3.7 hours for non-victims.
- For fraud and scams, the mean number of hours online for work was 4.3 hours for victims and 3.8 hours for non-victims.

Figure 9: Cybercrime victimisation among respondents who were working, by crime type and number of hours spent using the internet for work (%) (*n*=7,377)



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

Note: Limited to respondents who were currently working (*n*=8,884), and excludes 1,507 respondents who were working but did not know or declined to answer the question. Sample sizes: 0 hours *n*=657; 1 hour *n*=1,466; 2 hours *n*=1,205; 3 hours *n*=740; 4 hours *n*=647; 5 hours *n*=649; 6 hours *n*=498; 7+ hours *n*=1,513. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2023 [weighted data]

While it is not possible to link specific platforms or online behaviours with victimisation, examining the prevalence of victimisation according to these online behaviours is useful in determining the risk factors for cybercrime. In the analysis that follows, malware, identity crime and misuse and fraud and scams have been collapsed into a single category of profit-motivated cybercrime (PM) victimisation. The relationship between online behaviours and victimisation has been shown to be similar between these different types of cybercrime because of the role that the routine activities of computer users play in victimisation (Voce & Morgan 2023).

Frequent use—defined as daily or weekly use—of particular platforms was generally associated with a higher risk of victimisation (Table 10). However, the difference in victimisation rates between frequent and infrequent users was substantial for certain types of online activities. There was a minimum 10 percentage point difference in the prevalence of online abuse or harassment (OA) or PM victimisation between respondents who frequently and infrequently engaged in the following online behaviours:

- using subscription-based sexually explicit interactive adult platforms (OA=52.1% vs 25.9%; PM=58.0% vs 34.5%);
- making donations or payments over gaming, streaming or fundraising platforms (OA=51.3% vs 25.3%; PM=55.6% vs 34.0%);
- being active on romance or dating websites or apps (OA=48.5% vs 25.2%; PM=53.1% vs 34.0%);
- live streaming videos online (OA=37.7% vs 25.2%; PM=48.6% vs 33.2%);
- purchasing items from online marketplaces, excluding online stores (OA=40.5% vs 24.4%; PM=46.3% vs 33.4%);
- posting or responding to posts on social media (OA=34.6% vs 19.7%; PM=40.6% vs 30.6%);
- posting or responding to posts on online blogs, forums or interest groups (OA=41.7% vs 23.3%; PM=45.7% vs 32.9%);
- messaging and chatting online (OA=30.1% vs 19.6%; PM=37.3% vs 31.0%);
- purchasing items from online store websites and apps (excluding classifieds and marketplaces) (OA=36.2% vs 24.2%; PM=44.5% vs 32.7%);
- participating in online gaming or sports (OA=36.6% vs 24.8%; PM=41.5% vs 34.1%);
- accessing sexually explicit adult websites (OA=36.7% vs 25.0%; PM=41.7% vs 34.1%); and
- live streaming videos of content creators, influencers or gamers online (OA=39.6% vs 23.6%; PM=45.7% vs 32.7%).

These platforms may be attractive for malicious actors to exploit, as they often involve communication between strangers, registration processes and payments between individuals using the platform and the platform itself. Conversely, the difference in victimisation rates between respondents who frequently and infrequently used the internet for more mundane purposes was small or non-existent (non-significant, or ns):

- online banking and other online financial activities (OA=27.7% vs 24.2%; PM=36.7% vs 30.4%);
- private video chatting over apps and platforms (OA=32.9% vs 23.9%; PM=41.0% vs 32.5%);
- streaming videos on a computer, phone or TV (OA=28.5% vs 22.8%; PM=35.7% vs 34.7%, ns);
- browsing or looking for information (OA=27.1% vs 25.8% ns; PM=35.6% vs 34.2%, ns);
- sending emails (OA=27.5% vs 24.8%, ns; PM=36.3% vs 31.0%); and
- reading news articles online (OA=27.6% vs 25.2%; PM=36.2% vs 33.1%).

Table 10: Cybercrime victimisation, by crime type and frequency of online activities				
		n (%)	Online abuse and harassment victimisation	Profit-motivated cybercrime victimisation
Using subscription-based sexually explicit interactive adult platforms[a]	Daily or weekly	536 (3.9%)	52.1***	58.0***
	Less often or never	13,221 (96.1%)	25.9	34.5
Making donations or payments over gaming, streaming or fundraising platforms[b]	Daily or weekly	928 (6.7%)	51.3***	55.6***
	Less often or never	12,840 (93.3%)	25.3	34.0
Being active on romance/ dating websites or apps[c]	Daily or weekly	1,032 (7.5%)	48.5***	53.1***
	Less often or never	12,754 (92.5%)	25.2	34.0
Live streaming videos of myself online[d]	Daily or weekly	2,004 (14.5%)	37.7***	48.6***
	Less often or never	11,858 (85.5%)	25.2	33.2
Purchasing items from online marketplaces (excluding online store websites and apps)[e]	Daily or weekly	2,266 (16.4%)	40.5***	46.3***
	Less often or never	11,581 (83.6%)	24.4	33.4
Posting or responding to posts on social media[f]	Daily or weekly	6,796 (49.0%)	34.6***	40.6***
	Less often or never	7,065 (51.0%)	19.7	30.6
Posting or responding to posts on online blogs, forums or interest groups[g]	Daily or weekly	2,826 (20.4%)	41.7***	45.7***
	Less often or never	11,026 (79.6%)	23.3	32.9
Online banking and other online financial activities[h]	Daily or weekly	11,264 (81.6%)	27.7**	36.7***
	Less often or never	2,537 (18.4%)	24.2	30.4
Messaging and chatting online[i]	Daily or weekly	9,822 (70.8%)	30.1***	37.3***
	Less often or never	4,056 (29.2%)	19.6	31.0
Private video chatting over apps and platforms[j]	Daily or weekly	4,904 (35.4%)	32.9***	41.0***
	Less often or never	8,945 (64.6%)	23.9	32.5
Streaming videos on your computer, phone or TV[k]	Daily or weekly	10,249 (73.9%)	28.5***	35.7
	Less often or never	3,624 (26.1%)	22.8	34.7
Purchasing items from online store websites and apps (excluding classifieds and marketplaces)[l]	Daily or weekly	3,303 (23.9%)	36.2***	44.5***
	Less often or never	10,547 (76.1%)	24.2	32.7
Participating in online gaming/sports[m]	Daily or weekly	2,648 (19.1%)	36.6***	41.5***
	Less often or never	11,188 (80.9%)	24.8	34.1
Accessing sexually explicit adult websites[n]	Daily or weekly	2,426 (18.1%)	36.7***	41.7***
	Less often or never	10,990 (81.9%)	25.0	34.1

Table 10: Cybercrime victimisation, by crime type and frequency of online activities (continued)

		n (%)	Online abuse and harassment victimisation	Profit-motivated cybercrime victimisation
Live streaming videos of content creators, influencers or gamers online[o]	Daily or weekly	2,926 (21.1%)	39.6***	45.7***
	Less often or never	10,943 (78.9%)	23.6	32.7
Browsing or looking for information[p]	Daily or weekly	12,931 (93.3%)	27.1	35.6
	Less often or never	929 (0.7%)	25.8	34.2
Sending emails[q]	Daily or weekly	11,687 (84.4%)	27.5	36.3***
	Less often or never	2,166 (15.6%)	24.8	31.0
Reading news articles online[r]	Daily or weekly	10,540 (76.1%)	27.6*	36.2**
	Less often or never	3,309 (23.9%)	25.2	33.1

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

a: Excludes 130 respondents who did not know or declined to answer the question

b: Excludes 118 respondents who did not know or declined to answer the question

c: Excludes 101 respondents who did not know or declined to answer the question

d: Excludes 24 respondents who did not know or declined to answer the question

e: Excludes 40 respondents who did not know or declined to answer the question

f: Excludes 25 respondents who did not know or declined to answer the question

g: Excludes 36 respondents who did not know or declined to answer the question

h: Excludes 86 respondents who did not know or declined to answer the question

i: Excludes 9 respondents who did not know or declined to answer the question

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

k: Excludes 15 respondents who did not know or declined to answer the question

l: Excludes 37 respondents who did not know or declined to answer the question

m: Excludes 51 respondents who did not know or declined to answer the question

n: Excludes 470 respondents who did not know or declined to answer the question

o: Excludes 17 respondents who did not know or declined to answer the question

p: Excludes 27 respondents who did not know or declined to answer the question

q: Excludes 35 respondents who did not know or declined to answer the question

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

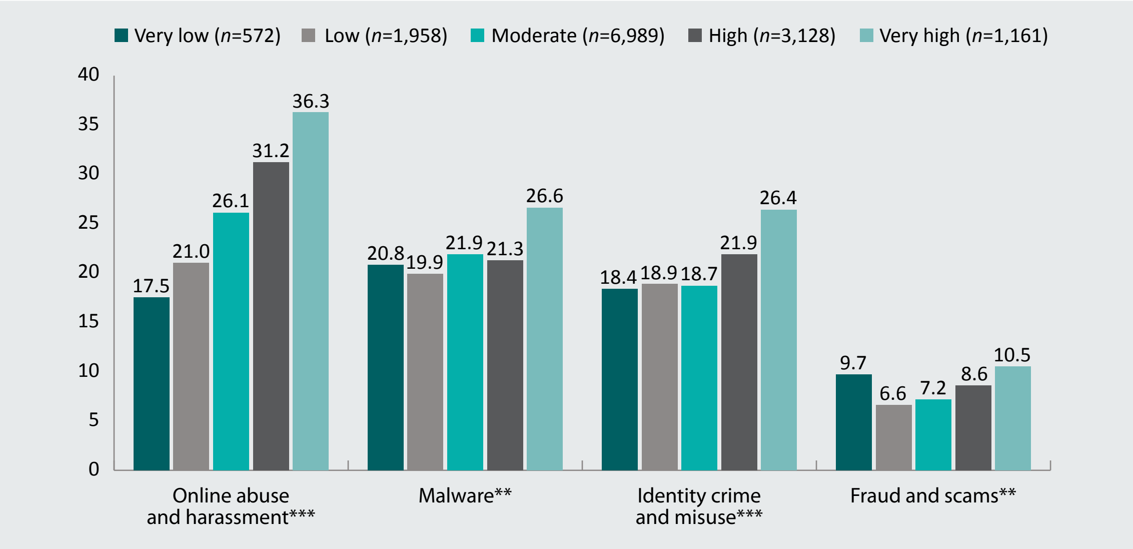
Note: Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2023 [weighted data]

Digital literacy and online safety strategies

Respondents were asked to rate their knowledge of technology and their ability to use technology. Those who rated their knowledge of technology as ‘very high’ had the highest prevalence of cybercrime victimisation in the past year, with 36.3 percent experiencing online abuse and harassment, 26.6 percent experiencing malware, 26.4 percent experiencing identity crime, and 10.5 percent experiencing fraud and scams (Figure 10). This may be because they spent longer online, or because they were better able to identify whether they had fallen victim to cybercrime. However, for fraud and scams, there was also a higher proportion of respondents who rated their knowledge of technology as very low (9.7%).

Figure 10: Cybercrime victimisation, by crime type and self-rated knowledge of technology (%)



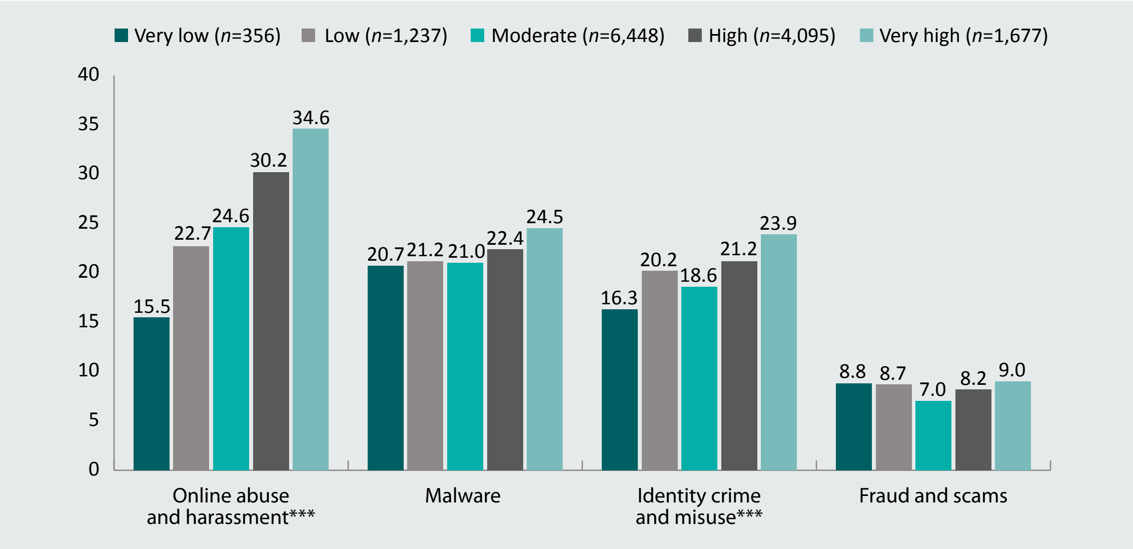
***statistically significant at *p*<0.001, **statistically significant at *p*<0.01

Note: Excludes 83 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 2023 [weighted data]

Similarly, respondents who rated their ability to use technology as very high also had the highest prevalence of online abuse and harassment (34.6%) and identity crime (23.9%; Figure 11). For fraud and scams and malware, there was little variation according to respondents' self-rated ability to use technology.

Figure 11: Cybercrime victimisation, by crime type and self-rated ability to use technology (%)



***statistically significant at *p*<0.001

Note: Excludes 74 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 2023 [weighted data]

Respondents were asked whether they had used various online safety measures in the 12 months prior to the survey (Table 11). The online safety measures respondents most commonly reported using included:

- avoiding clicking on links or attachments when they were not certain who the sender of an SMS/text or email was (73.3%);
- using a different password for secure online accounts, especially for banking or financial transactions (51.8%);
- using voice, fingerprint, facial or iris recognition technology to access devices such as their mobile phone (46.8%);
- installing or using antivirus software or firewalls on their devices (42.3%);
- checking their privacy settings on social media accounts (40.5%);
- regularly updating the security software on their device when prompted by their device's security system (39.9%); and
- generally clearing their browsing history, data and cookies frequently (39.1%).

Participating in training to stay safe online or to protect their information (12.6%) and purchasing or continuing to have cyber insurance (3.6%) were the least common safety measures used by respondents. Among respondents who had children living at home, around one in five (19.1%) said they had set, or had already installed, parental controls on devices and browsers to restrict access to certain content.

Respondents who used some of these online safety measures had a higher prevalence of cybercrime victimisation than respondents who did not use them. This included respondents who:

- checked privacy settings on social media accounts (OA=32.1% vs 24.3%; PM=37.1% vs 35.1%);
- purchased or continued to have cyber insurance (OA=40.7% vs 27.0%; PM=48.4% vs 35.5%);
- generally browsed in incognito mode (OA=34.6% vs 26.1%; PM=39.9% vs 35.2%);
- cleared their browsing history, data and cookies frequently (OA=29.3% vs 26.3%; PM=38.1% vs 34.6%);
- participated in training to stay safe online or protect their online environment and information (OA=34.4% vs 26.5%; PM=39.9% vs 35.4%);
- installed or used spam-filtering software (OA=33.0% vs 26.1%; PM=38.5% vs 35.3%);
- regularly updated their password on secure accounts, including email, banking or online stores and social media (OA=32.4% vs 25.7%; PM=38.5% vs 35.1%);
- used a secure password manager (OA=30.3% vs 26.5);
- used password protection on their router (OA=30.3% vs 26.5%);
- used a different password for secure online accounts, especially for banking or financial transactions (OA=28.5% vs 26.3%);
- changed their privacy settings on social media accounts from the default to a more restricted setting (OA=32.8% vs 24.8%; PM=38.5% vs 34.7%);

- used a virtual private network (VPN) when using the internet (OA=32.1% vs 26.3%);
- set, or already had installed, parental controls on devices and browsers to restrict access to certain content (OA=33.7% vs 25.5%; PM=40.5% vs 36.2%);
- used voice, fingerprint, facial or iris recognition technology to access their devices, such as their mobile phone (OA=30.3% vs 25.0%); and
- independently contacted companies or government departments when they were unsure about an SMS/text or email they had received from them (OA=29.0% vs 26.6%; PM=37.6% vs 35.0%).

This may be because respondents who had fallen victim to cybercrime in the 12 months prior to the survey were more likely than non-victims to implement online safety measures to prevent becoming a repeat victim of cybercrime (including on the advice of sources of help, advice or support). It may also reflect the types of online activities that these individuals engage in, which may be associated with a higher risk of victimisation and which require more stringent safety measures. As such, these results may indicate the types of measures that respondents implemented after they had been a victim of cybercrime.

Table 11: Cybercrime victimisation, by use of online safety measures

		Prevalence of behaviour in sample *n* (%)	Online abuse and harassment victimisation (%)	Profit-motivated cybercrime victimisation (%)
Checked privacy settings on social media accounts	Yes	5,464 (40.5)	32.1***	37.1*
	No	8,042 (59.5)	24.3	35.1
Purchased or continued to have cyber insurance	Yes	499 (3.7)	40.7***	48.4***
	No	13,007 (96.3)	27.0	35.5
Generally browsed in incognito mode	Yes	2,114 (15.7)	34.6***	39.9***
	No	11,392 (84.3)	26.1	35.2
Cleared their browsing history, data and cookies frequently	Yes	5,274 (39.1)	29.3***	38.1***
	No	8,232 (60.9)	26.3	34.6
Participated in training to stay safe online or protect their online environment and information	Yes	1,703 (12.6)	34.4***	39.9***
	No	11,803 (87.4)	26.5	35.4
Installed or used spam-filtering software	Yes	2,712 (20.1)	33.0***	38.5**
	No	10,794 (79.9)	26.1	35.3
Installed or used antivirus software or firewalls on their devices	Yes	5,707 (42.3)	28.4	35.8
	No	7,799 (57.7)	26.8	36.0
Regularly updated the security software on their device when prompted by their device's security system	Yes	5,388 (39.9)	28.1	35.4
	No	8,117 (60.1)	27.0	36.3

Table 11: Cybercrime victimisation, by use of online safety measures (continued)

		Prevalence of behaviour in sample *n* (%)	Online abuse and harassment victimisation (%)	Profit-motivated cybercrime victimisation (%)
Regularly updated their password on secure accounts, including email, banking or online stores and social media	Yes	3,521 (26.1)	32.4***	38.5**
	No	9,984 (73.9)	25.7	35.1
Used a secure password manager	Yes	3,072 (22.7)	31.5***	37.3
	No	10,434 (77.3)	26.3	35.5
Used password protection on their router	Yes	3,502 (25.9)	30.3***	36.4
	No	10,004 (74.1)	26.5	35.8
Used a different password for secure online accounts, especially for banking or financial transactions	Yes	7,002 (51.8)	28.5*	35.9
	No	6,504 (48.2)	26.3	36.0
Changed their privacy settings on social media accounts from the default to a more restricted setting	Yes	4,435 (32.8)	32.8***	38.5***
	No	9,071 (67.2)	24.8	34.7
Used a virtual private network (VPN) when using the internet	Yes	2,697 (20.0)	32.1***	36.2
	No	10,809 (80.0)	26.3	35.9
Set, or already had installed, parental controls on devices and browsers to restrict access to certain content[a]	Yes	860 (19.1)	33.7***	40.5***
	No	3,632 (80.9)	25.5	36.2
Used voice, fingerprint, facial or iris recognition technology to access their devices, such as their mobile phone	Yes	6,324 (46.8)	30.3***	36.7
	No	7,182 (53.2)	25.0	35.2
Avoided clicking on links or attachments when they were not certain who the sender of an SMS/text or email was	Yes	9,900 (73.3)	27.2	35.4
	No	3,606 (26.7)	28.3	37.3
Independently contacted company or government department when they were unsure about an SMS/text or email they had received from them	Yes	4,704 (34.8)	29.0**	37.6**
	No	8,802 (65.2)	26.6	35.0

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

a: Limited to respondents with children living at home, and excludes 126 respondents who did not answer the question (*n*=4,491)

Note: Excludes 381 respondents who did not know or declined to answer the question about online safety measures. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2023 [weighted data]

Finally, victimisation was analysed according to whether respondents had taken part in certain higher risk online behaviours in the 12 months prior to the survey (Table 12). These are behaviours that have been shown to be associated with a higher risk of victimisation (Voce & Morgan 2023). Victimisation was more common among respondents who:

- opened emails from people or organisations they did not know (OA=40.6% vs 25.7%; PM=48.3% vs 34.2%);
- accepted friend requests from people online who they had not met in person (OA=46.1% vs 25.5%; PM=46.6% vs 34.8%);
- accepted cookies from websites that saved their browsing information (OA=30.5% vs 25.0%; PM=38.6% vs 33.8%);
- shared a password or a code for an account they own with someone they knew (or thought they knew) (OA=43.8% vs 26.4%; PM=49.5% vs 35.0%); and
- used freely available wi-fi in a public location to conduct a financial transaction (OA=40.6% vs 26.3%; PM=51.3% vs 34.5%).

Importantly, besides accepting cookies from websites that saved their browsing information, these behaviours were all relatively rare among respondents, with around one in 10 respondents or fewer having engaged in these behaviours in the 12 months prior to the survey.

Table 12: Cybercrime victimisation, by use of higher risk online behaviours

		n (%)	Online abuse and harassment victimisation (%)	Profit-motivated cybercrime victimisation (%)
Accepted friend requests from people online who they had not met in person	Yes	1,274 (9.4)	46.1***	46.6***
	No	12,232 (90.6)	25.5	34.8
Shared a password or a code for an account they own with someone they knew (or thought they knew)	Yes	835 (6.2)	43.8***	49.5***
	No	12,670 (93.8)	26.4	35.0
Used freely available wi-fi in a public location to conduct a financial transaction	Yes	1,131 (8.4)	40.6***	51.3***
	No	12,375 (91.6)	26.3	34.5
Opened emails from people or organisations they did not know	Yes	1,636 (12.1)	40.6***	48.3***
	No	11,870 (87.9)	25.7	34.2
Accepted cookies from websites that saved their browsing information	Yes	6,014 (44.5)	30.5***	38.6***
	No	7,492 (55.5)	25.0	33.8

***statistically significant at *p*<0.001

Note: Excludes 381 respondents who did not know or declined to answer the question about online safety measures. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2023 [weighted data]

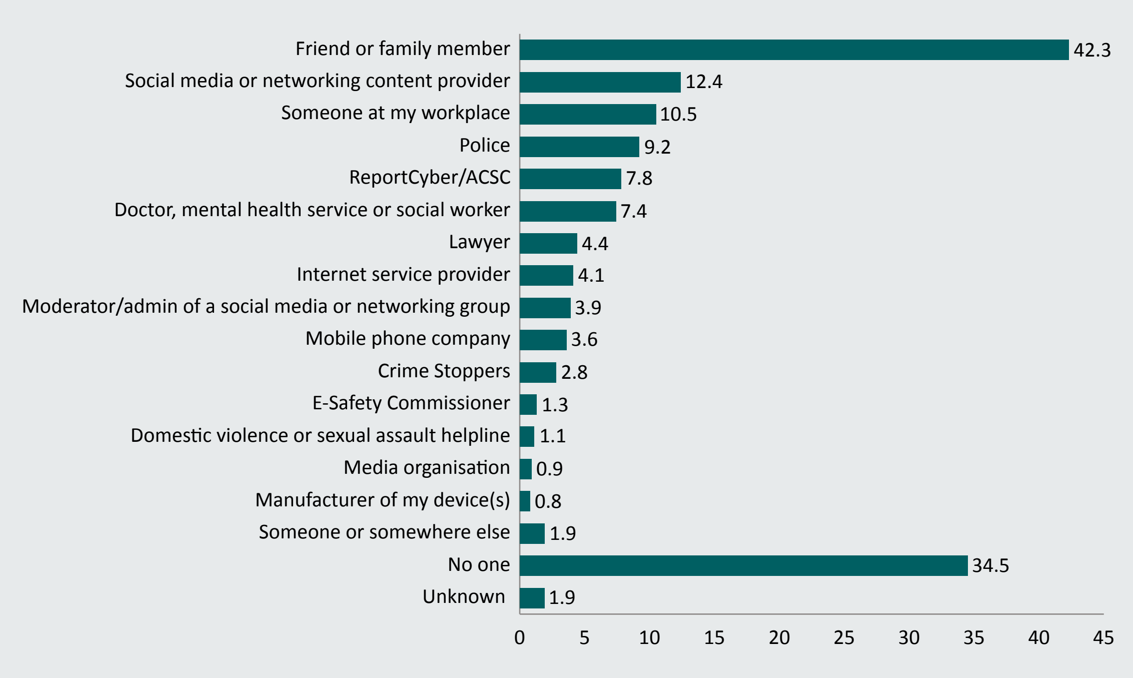
Help-seeking by victims following the most recent incident

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 (42.3%); a social media or networking content provider (12.4%); someone at their workplace, such as a manager, human resources or IT support staff (10.5%); or the police (9.2%; Figure 12). One in three victims (34.5%) did not seek help, advice or support from any sources following the most recent incident.

Figure 12: Help-seeking among online abuse and harassment victims following the most recent incident (%) (*n*=3,712)

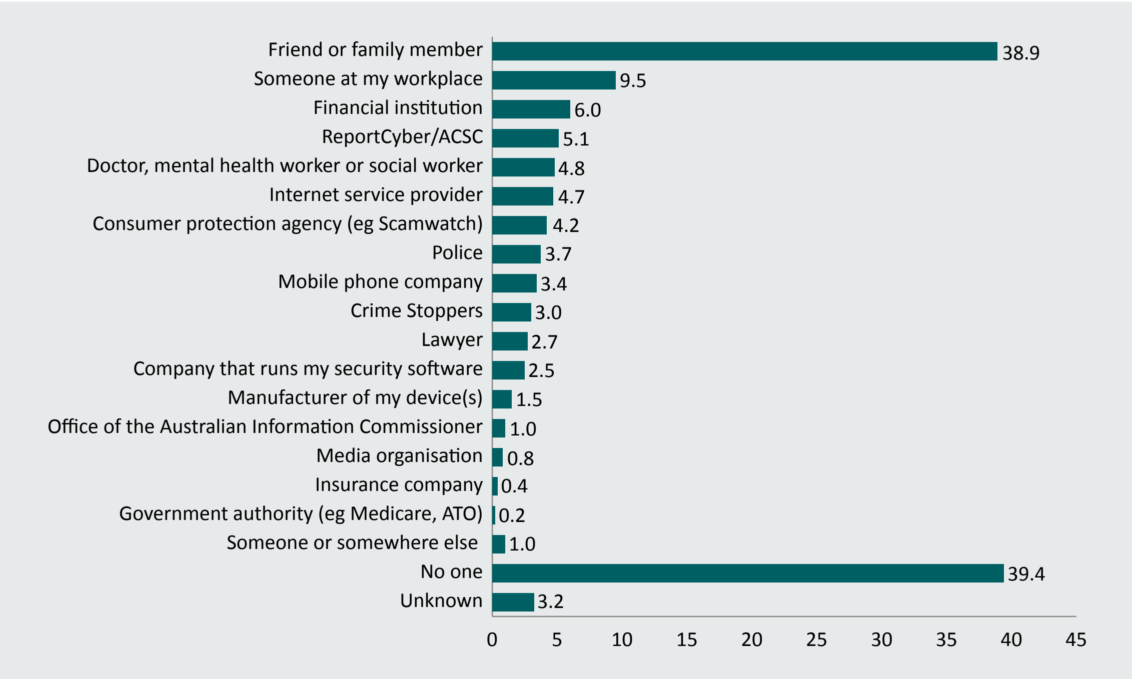


Note: Excludes 38 people who did not answer questions about the most recent incident. Weighted frequencies and percentages may not add to total due to rounding. Respondents could select multiple methods of reporting the most recent incident

Source: Australian Cybercrime Survey 2023 [weighted data]

Victims of malware most commonly told a family member or friend (38.9%); someone at their workplace, such as a manager, human resources or IT support staff (9.5%); 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) (6.0%); or the ACSC, through its ReportCyber portal or telephone helpline (5.1%; Figure 13). Two in five respondents who reported symptoms of malware (39.4%) did not tell anyone about the most recent incident.

Figure 13: Help-seeking among malware victims following the most recent incident (%) (*n*=3,000)

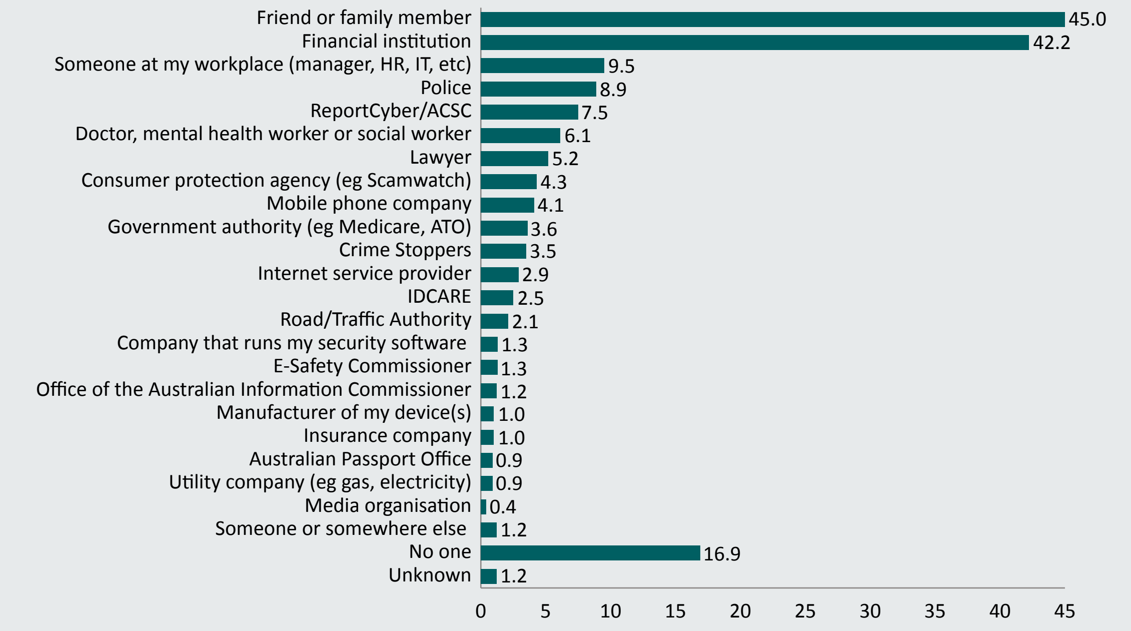


Note: Excludes 31 people who did not answer questions about the most recent incident. Financial institution=bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal). Weighted frequencies and percentages may not add to total due to rounding. Respondents could select multiple methods of reporting the most recent incident

Source: Australian Cybercrime Survey 2023 [weighted data]

A large proportion of identity crime victims reported the incident to financial institutions, such as a bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal) (42.2%; Figure 14). Victims also commonly told a family member or friend (45.0%); someone at their workplace, such as a manager, human resources or IT support staff (9.5%); or the police (8.9%). Around one in six victims of identity crime and misuse (16.9%) did not tell anyone about the most recent incident.

Figure 14: Help-seeking among identity crime and misuse victims following the most recent incident (%) (*n*=2,772)

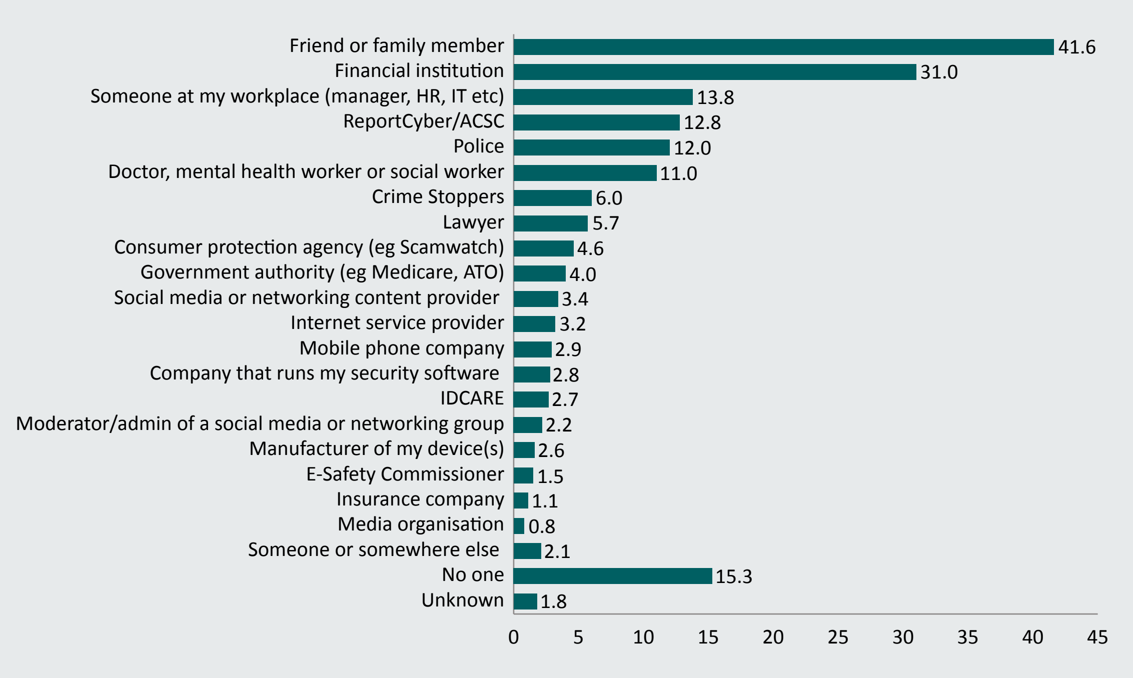


Note: Excludes 14 victims who did not answer questions about the most recent incident. Weighted frequencies and percentages may not add to total due to rounding. Respondents could select multiple methods of reporting the most recent incident

Source: Australian Cybercrime Survey 2023 [weighted data]

Similarly, a large proportion of fraud and scam victims reported the incident to financial institutions, such as a bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal) (31.0%; Figure 15). Victims also commonly told a family member or friend (41.6%); someone at their workplace, such as a manager, human resources or IT support staff (13.8%); or the ACSC, through its ReportCyber portal or telephone helpline (12.8%). Fraud and scam victims were the most likely to seek help, advice or support from at least one source, with only 15.3 percent of victims saying they had not told anyone about the incident.

Figure 15: Help-seeking among fraud and scam victims following the most recent incident (%) (*n*=1,065)

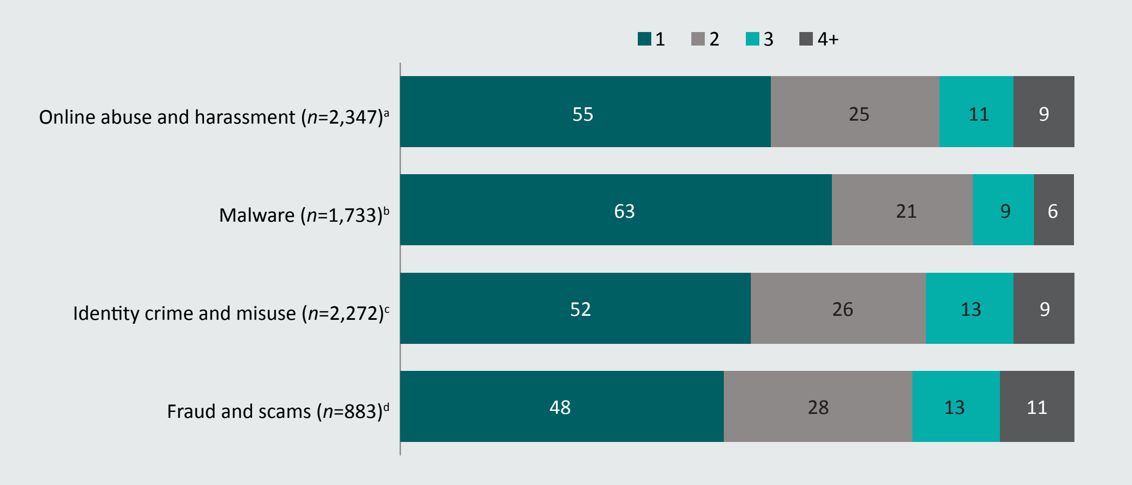


Note: Excludes 18 victims who did not answer questions about the most recent incident. Weighted frequencies and percentages may not add to total due to rounding. Respondents could select multiple methods of reporting the most recent incident

Source: Australian Cybercrime Survey 2023 [weighted data]

Many victims sought assistance from more than one source following the most recent incident of cybercrime (Figure 16). Among victims who sought help from anyone, 45 percent of online abuse and harassment victims, 37 percent of malware victims, 48 percent of identity crime victims and 52 percent of fraud and scam victims sought help from more than one source.

Figure 16: Number of sources of help, advice and support among victims who sought help following the most recent incident (%)



a: Excludes 1,297 online abuse and harassment victims who did not seek help from anyone, 38 victims who did not answer questions about the most recent incident, and 68 victims who did not know or declined to answer this question

b: Excludes 1,170 malware victims who did not seek help from anyone, 31 victims who did not answer questions about the most recent incident and 97 victims who did not know or declined to answer this question

c: Excludes 468 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 33 victims who did not know or declined to answer this question

d: Excludes 162 fraud and scam victims who did not seek help from anyone, 18 victims who did not answer questions about the most recent incident, and 19 victims who did not know or declined to answer this question

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

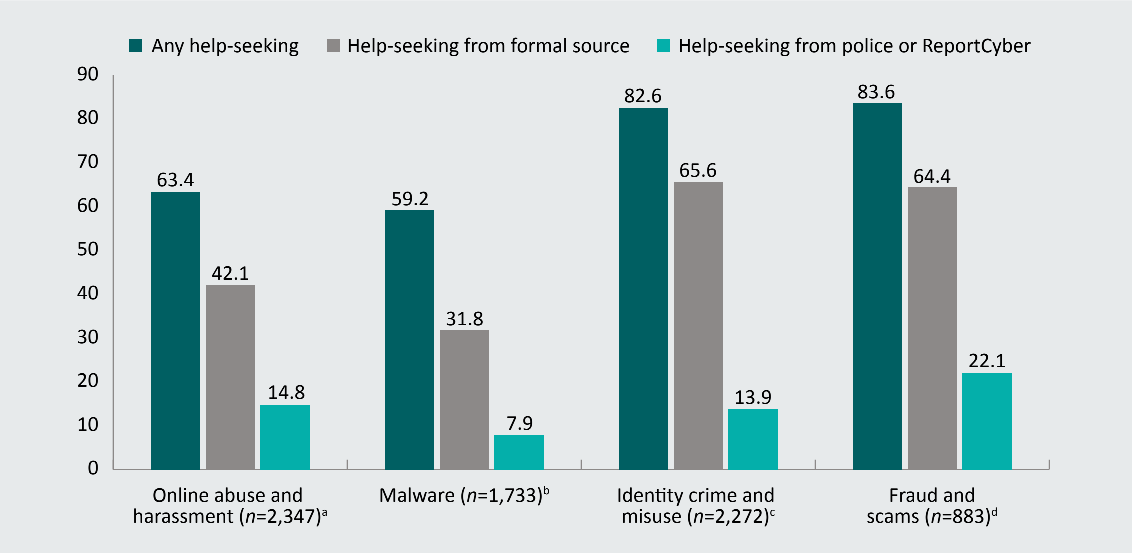
Source: Australian Cybercrime Survey 2023 [weighted data]

Reporting to police or to ReportCyber

A major focus of the survey was on help-seeking from police agencies and from the ACSC, especially through 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. While the survey asks about both police and the ACSC, 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 the ACSC).

As shown in Figure 17, formal help-seeking (ie seeking help from someone other than a family member or friend) was higher among identity crime victims (65.6%) and fraud and scam victims (64.4%) than online abuse and harassment victims (42.1%) and malware victims (31.8%). This likely reflects the large proportion of identity crime and fraud and scam victims reporting to financial institutions. Fraud and scam victims were the most likely to seek help, advice or support from the police or the ACSC (22.1%), followed by online abuse and harassment victims (14.8%), identity crime victims (13.9%) and malware victims (7.9%).

Figure 17: Help-seeking from selected sources following the most recent incident (%)



a: Excludes 38 victims who did not answer questions about the most recent incident and 68 victims who did not know or declined to answer this question

b: Excludes 31 victims who did not answer questions about the most recent incident and 97 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 and 33 victims who did not know or declined to answer this question

d: Excludes 18 victims who did not answer questions about the most recent incident and 19 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 2023 [weighted data]

Box 6: Estimating the extent of unreported cybercrime

The ACSC routinely publishes data on the number of recorded incidents of cybercrime. These figures are based on incidents that victims report using the ReportCyber portal. It is clear that these data are a significant underestimate of the actual number of incidents.

Data on whether victims reported the most recent incident to police or ReportCyber can be used to estimate multipliers, which can be applied to the number of recorded cybercrime incidents to estimate the total number of incidents impacting Australian computer users. Importantly, the survey focused on the most recent incident to ensure accurate data on help-seeking behaviour. Using multipliers is more likely to produce an accurate estimate of the true number of victims than simply counting recorded incidents. The multipliers reported here assume that the rate of reporting to police or the ACSC is consistent for all incidents experienced by victims.

The survey included options for both reporting to police and reporting via ReportCyber. It is possible that victims could nominate both options, even if they only reported through ReportCyber, because the platform mentions referring reports to police. For this reason, multipliers are calculated from the reporting rate to police *and* ReportCyber. This is a conservative estimate and may underestimate the difference between recorded and self-reported victims.

Relatedly, the survey did not ask whether the respondent made an official report to police or the ACSC. It is possible that the respondent contacted police or the ACSC, or accessed information online, and did not submit an official report. These limitations should be taken into consideration when using these multipliers.

The results of this survey indicate the following:

- 14.8 percent of online abuse and harassment victims sought help, advice or support from police or the ACSC. The true number of online abuse and harassment incidents involving unique victims will be *at least* 6.8 times the number recorded by ReportCyber.
- 7.9 percent of malware victims sought help, advice or support from police or the ACSC. The true number of malware incidents involving unique victims will be *at least* 12.7 times the number recorded by ReportCyber.
- 13.9 percent of identity crime victims sought help, advice or support from police or the ACSC. The true number of identity crime incidents involving unique victims will be *at least* 7.2 times the number recorded by ReportCyber.
- 22.1 percent of fraud and scam victims sought help, advice or support from police or the ACSC. The true number of fraud and scam incidents involving unique victims will be *at least* 4.5 times the number recorded by ReportCyber.

While these are broad categories of cybercrime, these multipliers illustrate the large number of incidents not captured by ReportCyber—which already recorded 76,000 reports in 2021–22, equivalent to one report every seven minutes (ACSC 2022).

The prevalence of respondents seeking help from police or ReportCyber following the most recent incident was analysed according to sociodemographic characteristics (Table 13). Several key findings emerged about who was more likely to seek help, advice or support:

- younger victims were more likely than older victims to seek help, advice or support for online abuse and harassment, identity crime and misuse and fraud and scams;
- male victims were more likely than female victims to seek help, advice or support from police or ReportCyber for all types of cybercrime;
- First Nations victims were more likely than non-Indigenous victims to seek help, advice or support from police or ReportCyber for online abuse and harassment, but less likely to seek help for identity crime and misuse and fraud and scams;
- victims who were born overseas were more likely than victims born in Australia to seek help from 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 seek help from police or ReportCyber following the most recent fraud and scam incident; and
- victims with children living at home were more likely than victims without children living at home to seek help from police or ReportCyber for online abuse and harassment.

While there were other differences between groups, these were based on relatively small numbers of victims and the differences were not statistically significant.

Table 13: Respondents who sought help from police or ReportCyber, by sociodemographic characteristics (%)

	Online abuse and harassment	Malware	Identity crime and misuse	Fraud and scams
Age				
18–24 (*n*=1,540)	18.4***	7.6***	16.9***	30.5***
25–34 (*n*=2,527)	21.2	12.6	19.8	31.5
35–49 (*n*=3,564)	16.3	8.2	13.2	15.8
50–64 (*n*=3,189)	10.3	5.2	9.7	13.0
65+ (*n*=3,067)	10.3	5.9	10.9	17.9
Gender				
Female (*n*=6,900)	13.8	5.0***	11.2***	16.8**
Male (*n*=6,935)	16.5	10.7	16.6	25.7
First Nations				
Yes (*n*=486)	32.4***	17.3***	12.7***	38.9**
No (*n*=13,249)	13.9	7.1	26.8	19.7
LQB+ respondents				
Yes (*n*=1,095)	15.1	6.8	10.8	23.9
No (*n*=12,618)	15.1	7.9	14.1	21.8
Born outside of Australia				
Yes (*n*=3,058)	18.5**	11.7***	17.5*	24.3
No (*n*=10,796)	14.1	6.7	12.8	21.4
Speaks a language other than English most often at home				
Yes (*n*=6362)	17.5	12.0	15.0	29.3
No (*n*=13,209)	14.9	7.7	13.8	21.5
Restrictive long-term health condition				
Yes (*n*=4,690)	16.1	8.2	12.9	17.9*
No (*n*=8,906)	14.8	7.8	14.5	25.4
Currently in a relationship				
Yes (*n*=8,784)	15.4	8.4	13.1	22.8
No (*n*=5,000)	15.0	7.0	15.4	21.3
Children living at home				
Yes (*n*=4,618)	18.1**	9.1	15.1	22.2
No (*n*=9,253)	13.8	7.2	13.2	22.0

***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. 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 2023 [weighted data]

Rates of help-seeking from police or ReportCyber following the most recent incident were also analysed according to business ownership status (Table 14):

- Small business owners, operators and managers were more likely than respondents who were an employee of a small to medium business or who were working but did not own or work for a small to medium business to seek help, advice or support from police or ReportCyber following the most recent incident of malware (13.5% of victims compared with 8.9% for small to medium business employees and 6.4% for other workers).
- Large company owners and executives were more likely than people who were employed in a large company or who were working but did not operate or work for a large company to seek help, advice or support from police or ReportCyber for identity crime and misuse (23.7%, 11.6% and 15.7%, respectively) and fraud and scams (43.8%, 13.8% and 24.5%, respectively).

Table 14: Respondents who sought help from police or ReportCyber following most recent incident, by business ownership status (%)

	Online abuse and harassment	Malware	Identity crime	Fraud and scams
Owning, operating or working for a small-to-medium business				
Owner, operator or manager of a small to medium business (*n*=1,782)	17.9	13.5***	18.2	27.7
Small to medium business employee (*n*=2,330)	16.1	8.9	14.7	23.8
Does not own or work for a small to medium business (*n*=4,612)	14.9	6.4	13.8	21.2
Owning, operating or working for a large company or business				
Large company owner or executive (*n*=618)	16.5	9.6*	23.7*	43.8**
Large company employee (*n*=2,736)	13.9	5.2	11.6	13.8
Does not operate or work for a large company (*n*=5,356)	16.7	10.1	15.7	24.5

***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 sought help, advice or support from police or to ReportCyber. Also excludes respondents who declined to provide information about their business owner status. These numbers vary by crime type. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2023 [weighted data]

Box 7: What influences help-seeking from police following a cybercrime incident?

The results presented in this section suggest that rates of help-seeking from police and ReportCyber vary according to the characteristics of victims. It is important to note that the likelihood of a victim reporting cybercrime to police will also vary according to characteristics of the incident and the harm inflicted on the victim.

Numerous studies have found that the seriousness of harm associated with crime incidents, as measured by the degree of bodily injury, economic loss, emotional damage, potential for harm, and perceived wrongfulness, is the strongest correlate of victim reporting (see Xie & Baumer 2019 for a review). This relationship extends to cybercrime, with a study conducted in the Netherlands finding that the seriousness and type of offence were the best predictors of cybercrime reporting, with cyber-enabled crimes being reported to the police more often than cyber-dependent crimes (Van de Weijer, Leukfeldt & van der Zee 2021).

This means that, while certain groups may appear to be less likely to report, there may be other factors that help explain these differences.

Respondents who sought help, advice or support from the 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.

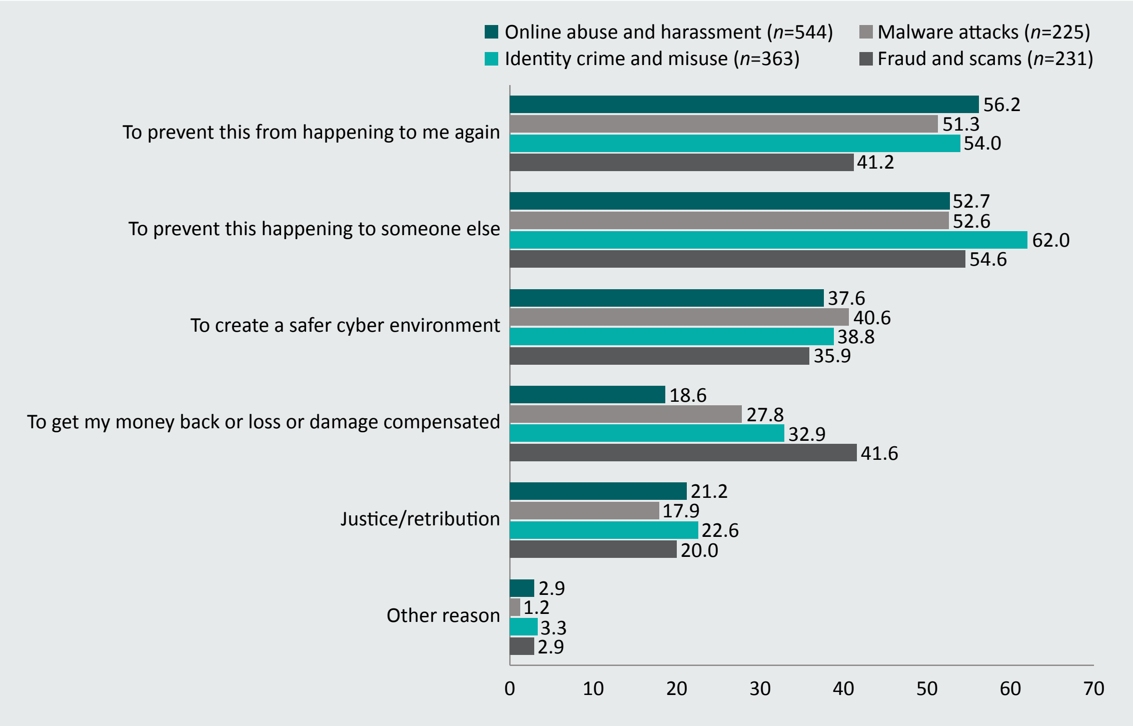
Across all crime types, the most common reason for reporting to police or the ACSC was to prevent the crime from happening to them again or to someone else (Figure 18). Online abuse and harassment victims most often stated that they reported the incident to prevent it happening to them again (56.2%), followed by preventing it from happening to someone else (52.7%).

Similar proportions of malware victims said they reported the incident to prevent it happening to someone else (52.6%) or to prevent it from happening to them again (51.3%). Similarly, 62.0 percent of identity crime and misuse victims said they reported the incident to stop it from happening to someone else, and 54.0 percent said they reported it to prevent it from happening to them again.

While fraud and scam victims most commonly said they reported to police or to ReportCyber to prevent the crime from happening to someone else (54.6%), they 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 (41.6%).

Between 35.9 and 40.6 percent of victims said they reported the most recent incident to create a safer cyber environment. Around one in five victims, irrespective of the type of cybercrime, said they had reported the most recent incident to police or ReportCyber for justice or retribution.

Figure 18: Reasons for seeking help, advice or support from 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 15 online abuse and harassment victims, 5 malware victims and 17 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 2023 [weighted data]

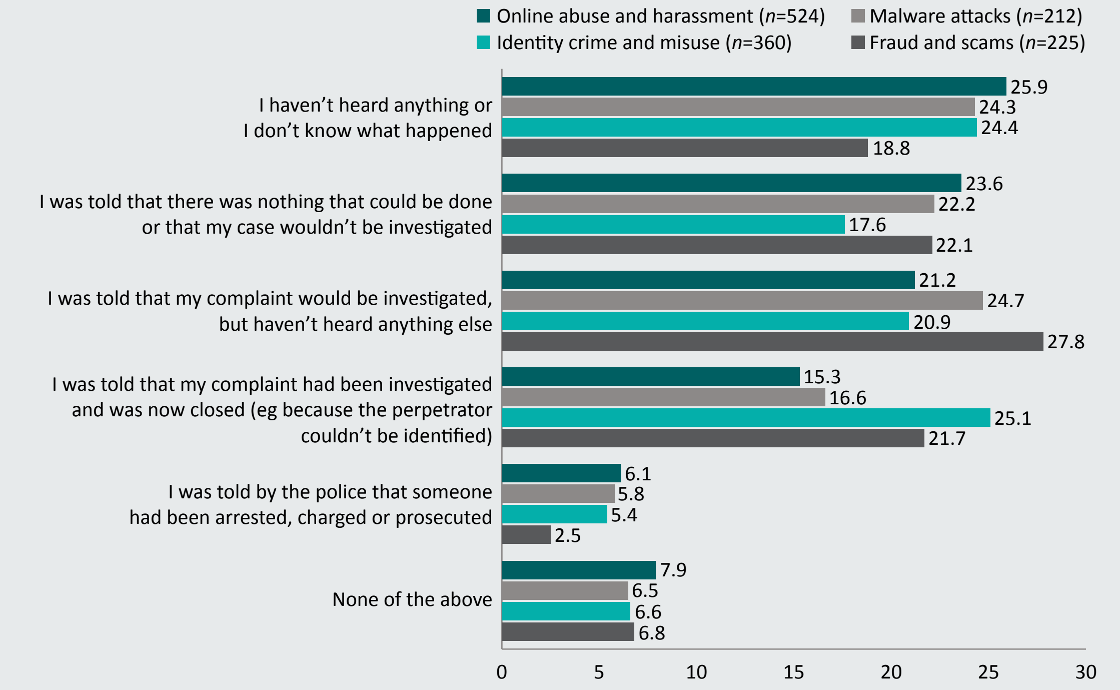
Outcomes from reporting to police or ReportCyber ranged from not having heard anything following their report and not knowing what happened, through to being told by police that someone had been arrested, charged or prosecuted for the crime (Figure 19). The focus here is on what victims perceive as the outcome—the actual outcome recorded by police may differ. The most common outcome for online abuse and harassment victims was that they had not heard anything or did not know what happened with their report (25.9%), followed by being told that nothing could be done or that the case would not be investigated (23.6%). Overall, 42.6 percent of victims said they were told their complaint would be or had been investigated, of which around half (21.2% of victims) had not heard anything else.

Similar proportions of malware victims said they had not heard anything (24.3%), were told nothing could be done (22.2%) or that their complaint would be investigated but nothing else (24.7%). 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 (25.1%), but were also just as likely to say they had not heard anything about their complaint (24.4%).

Half of all fraud and scam victims (52.0%) were told that their case would be or had been investigated, of which around half said they had not heard anything else (27.8% of all fraud and scam victims). They were the least likely to say they had not heard anything (18.8%).

Overall, 6.1 percent of online abuse and harassment victims, 5.8 percent of malware victims, 5.4 percent of identity crime victims and 2.5 percent of fraud or scam victims were 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 34 online abuse and harassment victims, 18 malware victims, 20 identity crime and misuse victims and 6 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 2023 [weighted data]

Box 8: What factors influence whether cybercrimes are investigated or an offender is apprehended?

Many factors can influence whether a cybercrime reported to police (including via ReportCyber) is investigated and, if so, whether the offender will be apprehended.

Some of these factors are not unique to cybercrime. Not every incident reported to police or ReportCyber will meet the threshold for a criminal offence. In other cases there will be a low prospect of arrest, particularly where there is insufficient evidence to proceed with an investigation.

Previous research has highlighted some of the challenges associated with investigating cybercrime. Importantly, there has been a significant enhancement in law enforcement's cybercrime capability, including in the Joint Policing Cybercrime Coordination Centre and in state and territory law enforcement agencies (Australian Government 2022). That said, resources are still limited. There is already a large volume of reports submitted to ReportCyber—one every seven minutes (ACSC 2022)—which far outweighs the capacity of law enforcement to respond.

There are additional challenges specific to cybercrime cases. Limited specialist capability and training impacts the ability and confidence of police to respond (Wilson et al. 2022). These capability gaps are amplified by increasingly complex and technologically sophisticated offenders and offences, which also undermine police surveillance and evidence-gathering efforts (Cross et al. 2021). Further, jurisdictional boundaries and the borderless nature of cybercrimes also hinder investigation and offender identification (Morgan et al. 2016).

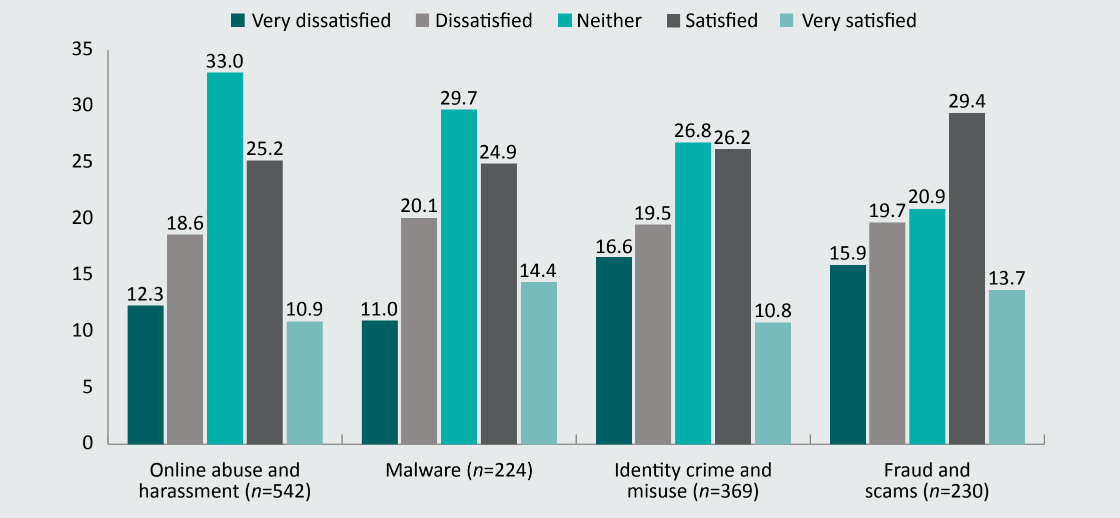
These factors, and others, can all influence the outcomes of incidents reported to police and ReportCyber.

Besides identity crime and misuse victims (where the difference was negligible), victims who reported the most recent incident to police or to ReportCyber were more likely to be satisfied than dissatisfied with the outcome of their report:

- 30.9 percent of online abuse and harassment victims were dissatisfied or very dissatisfied with the outcome of their report, while 36.1 percent were satisfied or very satisfied with the outcome;
- 31.1 percent of malware victims were dissatisfied or very dissatisfied with the outcome of their report, while 39.3 percent were satisfied or very satisfied with the outcome;
- 36.1 percent of identity crime and misuse victims were dissatisfied or very dissatisfied with the outcome of their report, while 37.0 percent were satisfied or very satisfied with the outcome; and
- 35.6 percent of fraud and scam victims were dissatisfied or very dissatisfied with the outcome of their report, while 43.1 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 20.9 percent for fraud and scam victims, to 33.0 percent for online abuse and harassment victims.

Figure 20: Satisfaction with the outcome of reporting among victims who reported to police or ReportCyber, by crime type (%)



Note: Excludes 34 online abuse and harassment victims, 6 malware victims, 11 identity crime and misuse victims and 1 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 2023 [weighted data]

Box 9: Has victim satisfaction increased over time?

Since the introduction of the Australian Cybercrime Online Reporting Network (ACORN)—the predecessor to ReportCyber—the platform has been improved and steps taken to improve the information sharing with law enforcement and the capability of police to respond to cybercrime reports. While there are still significant challenges (see Box 8), it is possible that these changes have led to some improvements in the reporting experiences of victims.

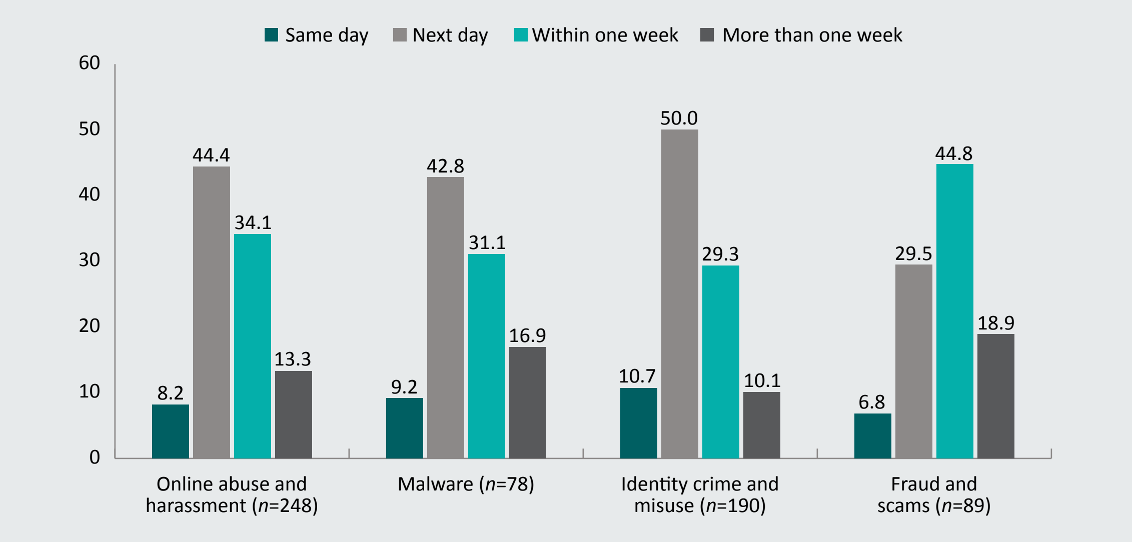
As part of an evaluation of ACORN, cybercrime victims who had reported to ACORN were surveyed about the outcome of their report and their satisfaction with that outcome (Morgan et al. 2016). While the sampling method was different, and there were slight differences in the categories of cybercrime examined, the same questions were used to measure satisfaction in that survey and in the ACS. This allows for some crude comparisons of satisfaction rates between victims who reported to ACORN in mid-2015 and victims who sought help, advice or support from police or ReportCyber in 2022:

- 21 percent of victims of cyberbullying, sexting, online harassment or stalking who reported to ACORN were satisfied with the outcome, compared with 36 percent of online abuse and harassment victims who sought help, advice or support from the police or ReportCyber;
- 32 percent of victims of computer system attacks who reported to ACORN were satisfied with the outcome, compared with 39 percent of malware victims who sought help, advice or support from the police or ReportCyber; and
- 30 percent of victims of online scams and fraud who reported to ACORN were satisfied with the outcome, compared with 43 percent of victims who sought help, advice or support from the police or ReportCyber.

These findings are indicative only, for the reasons already mentioned. However, the consistent upward trend in satisfaction suggests that responses to cybercrime victims may have improved.

Victims were asked the number of days between the most recent incident occurring and them making a report to the police or ReportCyber. Because victims could report to one or both of police and ReportCyber, this question was asked separately of each. The results were similar for police (Figure 21) and ReportCyber (Figure 22). For online abuse and harassment (44.4%), malware (42.8%) and identity crime and misuse (50.0%), it was most common for victims to say they reported the incident to police the day after it occurred. This was also true for reporting to ReportCyber (48.2%, 42.9% and 43.1%, respectively). Fraud and scam victims were most likely to say they reported the incident to police (44.8%) and ReportCyber (38.3%) within one week. Between one in 10 and one in five victims waited longer than a week to report the incident to police or ReportCyber.

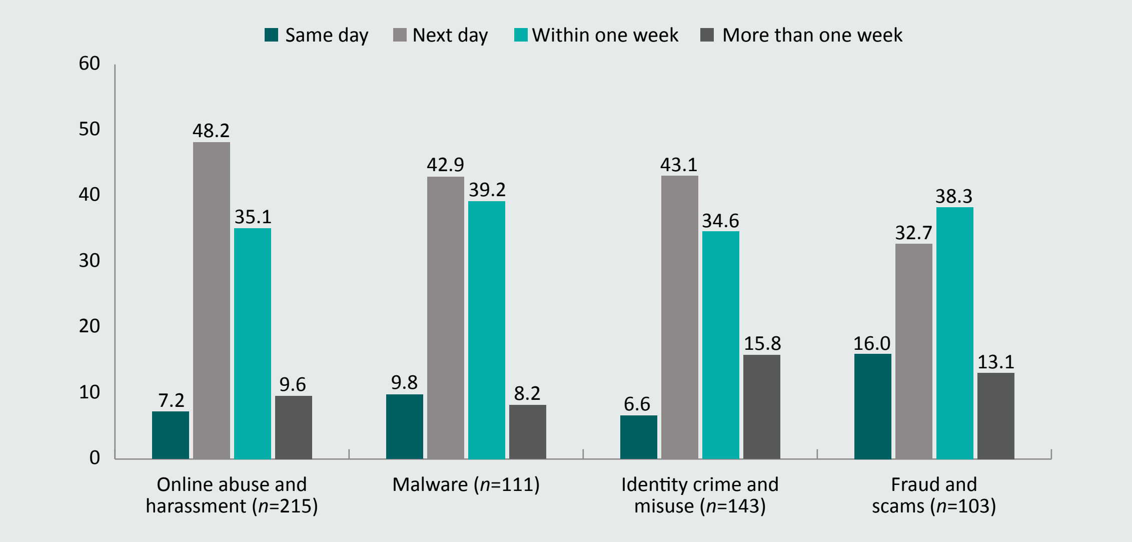
Figure 21: Length of time taken to submit a report to police following the most recent incident, by crime type (%)



Note: Excludes 95 online abuse and harassment victims, 33 malware victims, 56 identity crime and misuse victims and 39 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 2023 [weighted data]

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



Note: Excludes 78 online abuse and harassment victims, 42 malware victims, 64 identity crime and misuse victims, and 34 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 2023 [weighted data]

Respondents who did not report the most recent incident to police or ReportCyber were asked their reasons for not doing so (Table 15). The most common reason victims did not report to police was that they felt they could deal with it themselves; however, this was less common among fraud and scam victims (23.2%) than among victims of online abuse and harassment (39.6%), malware (34.7%) and identity crime (31.2%). For online abuse and harassment (34.2%) and malware (25.7%) 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 (13.4%).

Importantly, a significant proportion of online abuse and harassment victims (16.8%), malware victims (15.1%), identity crime and misuse victims (24.1%) and fraud and scam victims (20.1%) who did not seek help from police or ReportCyber following the most recent incident did not know that this was an option. A similar proportion of victims did not think the police or ReportCyber would be able to do anything. Between 15.1 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 (4.5%–6.7% of victims) or because they did not trust the police or ReportCyber (3.2%–4.1%).

Table 15: Reasons for not reporting to police or ReportCyber, by crime type (%)

	Online abuse and harassment (*n*=2,955)	Malware (*n*=2,467)	Identity crime (*n*=2,206)	Fraud and scams (*n*=770)
Seriousness of the incident				
Felt they could deal with it themselves	39.6	34.7	31.2	23.2
Did not regard the incident as a serious offence	34.2	25.7	21.6	13.4
Did not know or think the incident was a crime	18.1	17.4	9.1	10.4
Understanding, perceptions or past experience of reporting				
Did not know reporting to the police, ACSC or ReportCyber was an option	16.8	15.1	24.1	20.1
Did not think the police, ACSC or ReportCyber would be able to do anything	16.5	14.5	22.0	21.7
I did not know how or where to report the matter	15.1	17.2	19.6	18.3
Have reported before and been dissatisfied with the outcome	4.5	4.6	5.6	6.7
Did not trust the police, ACSC or ReportCyber	3.9	3.2	3.2	4.1
Worry about the reaction or consequences				
Did not want to ask for help	9.6	9.0	6.5	6.9
Felt ashamed or embarrassed	6.4	3.7	5.3	11.1
Felt I would not be believed	4.8	4.0	3.5	6.4
Fear of legal processes	3.3	2.4	3.2	6.0
Fear of the person responsible (eg fear of retaliation)	4.9	2.6	2.8	4.4
Did not want the person responsible arrested	3.5	2.1	1.9	4.6
Cultural or language reasons	1.5	1.2	1.4	2.7
Incident handled by someone else				
Workplace/on-the-job incident—internal reporting procedures followed	2.6	3.2	1.9	4.0
Provider (eg bank, telecommunications company) involved in incident was resolving or had resolved the matter	1.0	0.7	7.4	2.8
Other	3.3	2.6	3.6	2.4

Note: Excludes 134 online abuse and harassment victims, 206 malware victims, 154 identity crime and misuse victims and 45 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 2023 [weighted data]

Impacts of victimisation

Financial losses

The methodology used to estimate the financial losses associated with cybercrime was the same as the methodology Teunissen, Voce and Smith (2021) used in estimating the costs associated with pure cybercrime. However, while the previous study was able to estimate the total cost, extrapolating from data drawn from a random probability sample, the focus of the current study is on estimating the costs of cybercrime for the most recent incident.

First, victims were asked whether they had directly lost money because of the most recent incident (Table 16). For 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). Fraud and scams had the highest proportion of victims reporting financial losses (34.1%), followed by identity crime (28.7%). Financial losses were relatively uncommon for online abuse and harassment victims (2.7%) and malware victims (4.4%), with less than five percent reporting that they had money directly stolen or lost in the most recent incident. Around one-third of malware victims who lost money or had money stolen said the most recent incident involved ransomware (with or without encryption), despite this accounting for only 18 percent of malware victims.

Next, victims were 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) and whether any of the money they had lost was reimbursed by banks or other organisations, or recovered in other ways. For online abuse and harassment victims, 11.0 percent lost money dealing with the consequences and 1.2 percent had money reimbursed. Among malware victims, 10.1 percent lost money dealing with the consequences and 2.3 percent had money reimbursed. Among identity crime victims, 4.9 percent lost money dealing with the consequences and 18.4 percent had money reimbursed. Nineteen percent of fraud and scam victims lost money dealing with the consequences and 10.5 percent had money reimbursed.

Table 16: Money lost, money spent on consequences and money recovered following most recent incident of cybercrime, by crime type

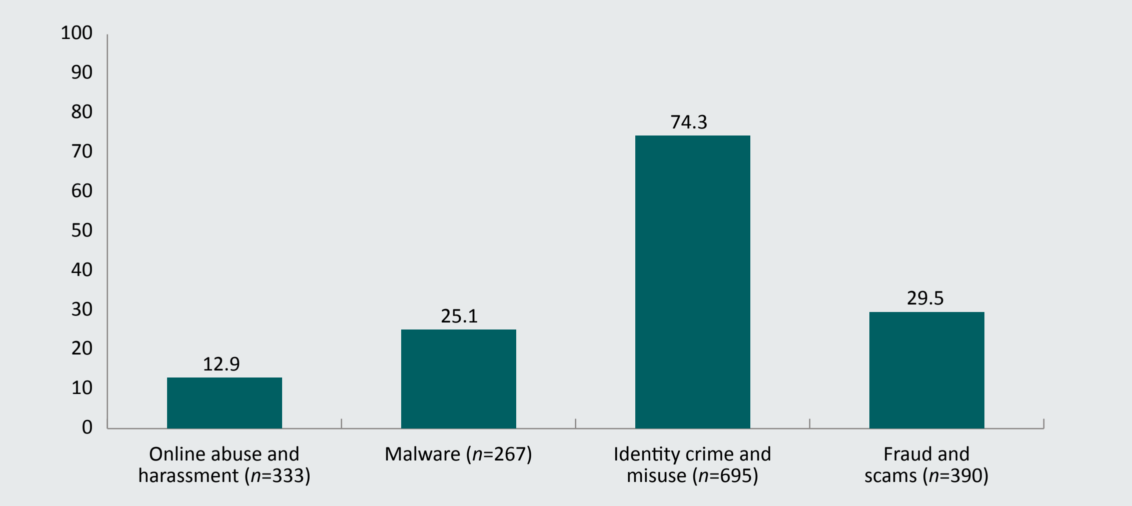
	Online abuse and harassment (*n*=3,712)	Malware (*n*=3,000)	Identity crime (*n*=2,772)	Fraud and scams (*n*=1,065)
Victims who lost money	100 (2.7%)	133 (4.4%)	796 (28.7%)	363 (34.1%)
Victims who could report how much they lost	81 (2.2%)	109 (3.6%)	700 (25.3%)	324 (29.9%)
Victims who spent money on consequences	407 (11.0%)	304 (10.1%)	137 (4.9%)	201 (18.9%)
Victims who could report how much they spent on consequences	308 (8.3%)	221 (7.4%)	53 (1.9%)	148 (13.9%)
Victims who recovered money	44 (1.2%)	68 (2.3%)	513 (18.5%)	114 (10.7%)
Victims who could report how much they recovered	44 (1.2%)	66 (2.2%)	510 (18.7%)	112 (10.5%)

Note: Weighted frequencies and percentages may not add to total due to rounding. Excludes 38 online abuse and harassment victims, 31 malware victims, 14 identity crime and misuse victims and 18 fraud and scam victims who did not answer questions about the most recent incident

Source: Australian Cybercrime Survey 2023 [weighted data]

Not all cybercrime victims who lost money or who spent money on consequences reported being able to recover money (Figure 23). Those who did recover money did not necessarily recover the full amount. The proportion of victims who were able to recover money was lowest among victims of online abuse and harassment (12.9%) and highest among victims of identity crime and misuse (74.3%).

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

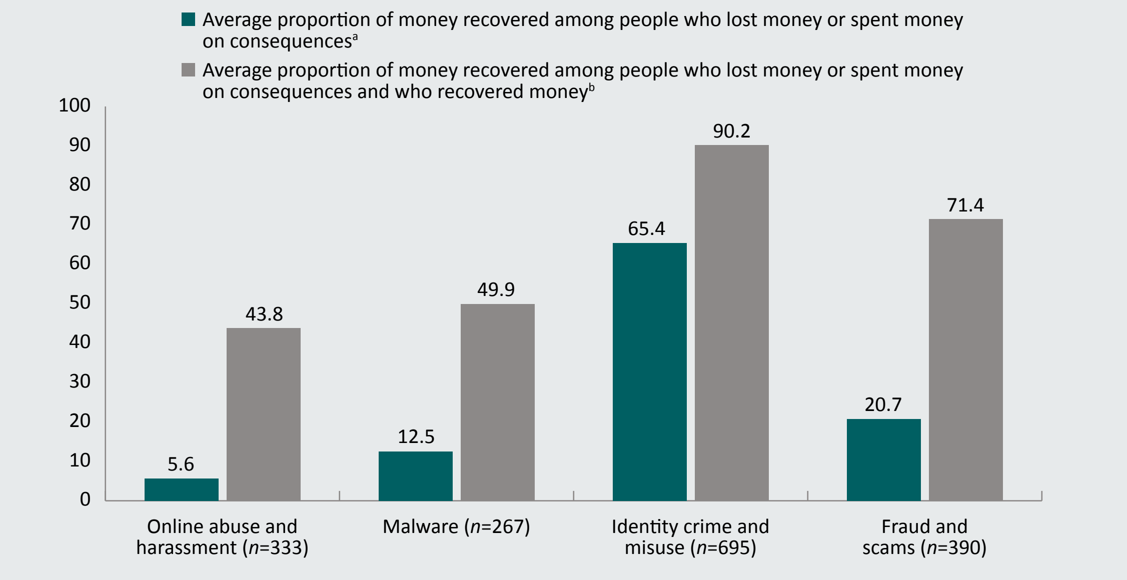


Note: Excludes 1 online abuse and harassment victim, 16 identity crime and misuse victims and 6 fraud and scam victims who did not answer whether they had recovered money. Figure only includes victims who lost money or spent money on consequences. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2023 [weighted data]

The average proportion of money lost or spent on consequences that was recovered was even lower (Figure 24), ranging from 5.6 percent for online abuse and harassment to 65.4 percent for identity crime and misuse victims. Among those victims who were able to recover money, the average proportion of money lost or spent on consequences that was recovered ranged from 43.8 percent for online abuse and harassment to 90.2 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: Prevalence and proportion of money recovered following most recent incident (%)



a: Includes all victims who lost or spent money, including those who did not answer whether they had recovered money

b: Limited to victims who recovered money: online abuse and harassment *n*=43, malware *n*=67, identity crime and misuse *n*=504, scams and fraud *n*=113

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

Source: Australian Cybercrime Survey 2023 [weighted data]

The median value of losses incurred by victims (through money or cryptocurrency being stolen or payments demanded) was $500 for online abuse and harassment victims, $420 for malware victims, $300 for identity crime victims and $300 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, $700 for identity crime victims and $200 for fraud and scam victims. The median amount that victims were able to recover was $200 for online abuse and harassment victims, $200 for malware victims, $250 for identity crime victims and $250 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, $250 for malware victims, and $235 for fraud and scam victims (Table 17). The median cost after recoveries for identity crime victims was $0 because the majority of victims who lost money or spent money on consequences were able to recover their money. The mean value was significantly higher for each type of cybercrime, ranging from $1,252 for malware to $9,157 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 17; see also Figure 25).

Table 17: Median financial losses for most recent incident among victims who lost any money, by payment method (range)

	Online abuse and harassment (*n*=3,712)[a]	Malware (*n*=3,000)[b]	Identity crime (*n*=2,787)[c]	Fraud and scams (*n*=1,082)[d]
Money	$500 ($10 – $50,000)	$300 ($2 – $115,000)	$300 ($1 – $275,000)	$265 ($1 – $410,000)
Cryptocurrency	$50 ($5 – $77,273)	$70 ($2 – $6,000)	$174 ($1 – $110,000)	$120 ($5 – $2,400,000)
Gift cards	$100 ($2 – 5,000)	$50 ($2 – $6,000)	$100 ($2 – $6,000)	$110 ($3 – $64,849)
Total losses	$500 ($20 – $80,088)	$420 ($2 – $115,000)	$300 ($1 – $275,000)	$300 ($1 – $2,400,000)
Median amount spent on consequences	$250 ($1 – $350,000)	$200 ($1 – $34,440)	$700 ($30 – $34,440)	$200 ($1 – $200,000)
Median losses from money directly lost and money spent on consequences	$350 ($20 – $380,000)	$300 ($1 – $115,000)	$300 ($1 – $275,000)	$340 ($1 – $2,400,000)
Median amount recovered	$200 ($5 – $34,440)	$200 ($10 – $115,000)	$250 ($1 – $275,000)	$250 ($2 – $65,000)
Median losses after recoveries	$300 ($0 – $380,000)	$250 ($0 – $50,000)	$0 ($0 – $100,000)	$235 ($0 – $2,400,000)
Mean losses after recoveries (*SD*)	$4,492 ($25,026)	$1,252 ($3,869)	$1,514 ($6,593)	$9,157 ($107,586)

a: Excludes one person who was net positive $8 after recoveries

b: Excludes 3 respondents who were net positive between $1 and $18,776 after recoveries

c: Excludes 8 participants who were net positive between $5 and $48,450 after recoveries

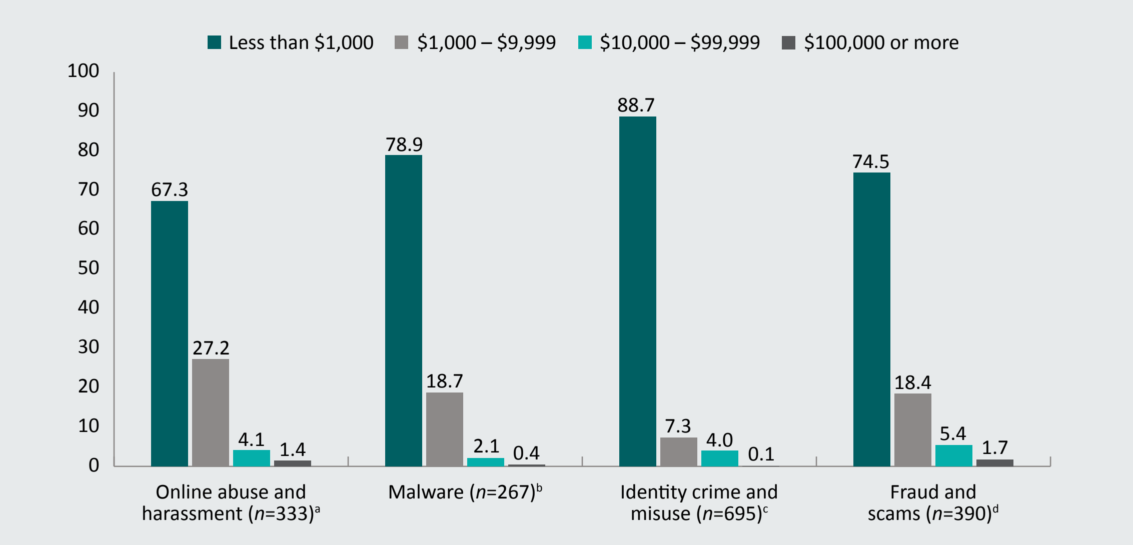
d: Excludes 3 respondents who were net positive between $50 and $9,830 after recoveries

Note: Weighted frequencies and percentages may not add to total due to rounding. Excludes 38 online abuse and harassment victims, 31 malware victims, 14 identity crime and misuse victims and 18 fraud and scam victims who did not answer questions about the most recent incident. *SD*=standard deviation

Source: Australian Cybercrime Survey 2023 [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 67.3 percent (online abuse and harassment) and 88.7 percent (identity crime and misuse) reported having lost less than $1,000 in the most recent incident. Approximately a third (32.7%) of online abuse and harassment victims, 21.2 percent of malware victims, 11.4 percent of identity crime victims and 25.5 percent of fraud and scam victims lost more than $1,000 in the most recent incident. Seven percent of fraud and scam victims lost more than $10,000, compared with 5.5 percent of online abuse and harassment victims, 2.5 percent of malware victims and 4.1 percent of identity crime victims. A small proportion of victims, including 1.4 percent of online abuse and harassment victims and 1.7 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 (%)



a: Excludes one person who was net positive $8 after recoveries

b: Excludes 3 respondents who were net positive between $1 and $18,776 after recoveries

c: Excludes 6 participants who were net positive between $5 and $48,450 after recoveries

d: Excludes 2 respondents who were net positive between $50 and $9,830 after recoveries

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

Source: Australian Cybercrime Survey 2023 [weighted data]

Box 10: Big financial losses or high volume, low yields?

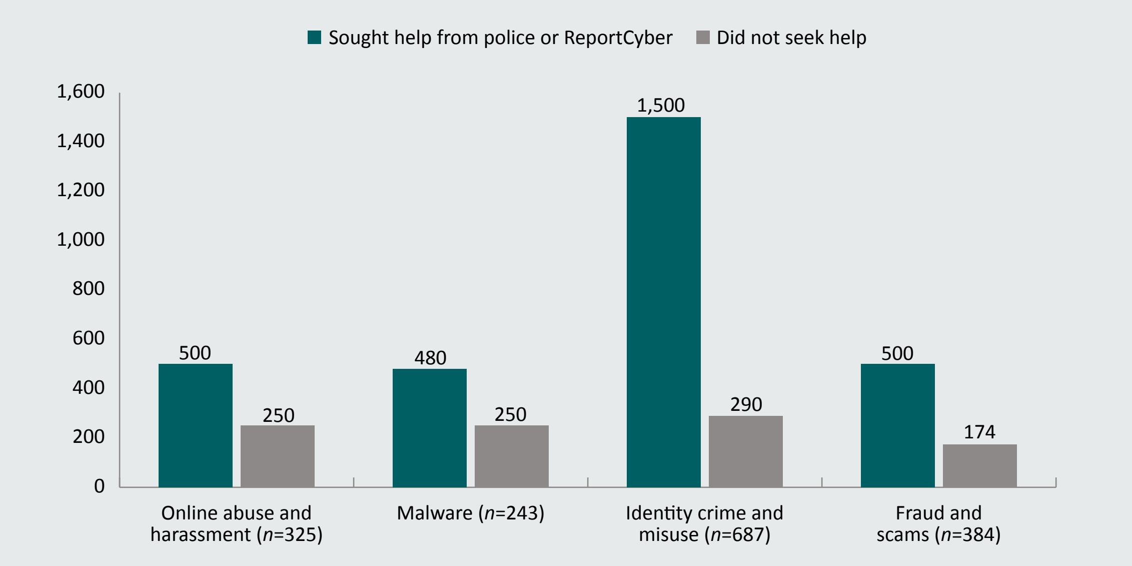
The results presented in this section show that individual losses associated with cybercrime victimisation vary widely. Most report losing no money from the most recent incident. Among those victims who do lose money and who could report how much, the majority lose less than $1,000. For some individuals, this may have little impact on their lives. For others, the impact may be substantial.

A small group of victims did lose substantial amounts of money. This was especially true of online abuse and harassment and fraud and scam victims, with 5.5 percent and 7.1 percent of victims who lost any money losing more than $10,000 in the most recent incident, respectively. The impact of these losses is potentially catastrophic and can have long-term effects on victims. These incidents are more likely to be reported to authorities and tend to be reflected in estimated losses based on recorded data.

What is apparent from these results is that cybercrime is most frequently a high-volume, low-yield crime. While the methodology used in this survey does not allow for the results to be extrapolated to the wider community, the high rate of victimisation means that, even with the relatively small median losses per victim, the overall cost to Australian individuals is likely to be enormous. This result echoes that of previous research into the cost of pure cybercrime, where the amount lost per victim was relatively small, but the total estimated cost to Australian computer users exceeded $3 billion (Teunissen, Voce & Smith 2021). With such a high rate of victimisation, cybercrime targeting Australian computer users is extremely lucrative for cybercriminals, even if the amount lost per victim is relatively low.

These results are different to data on the losses from reported cybercrimes (ACCC 2023; ACSC 2022). There are two main reasons for this. First, there were clear differences between the incidents reported to police or ReportCyber and those that were not 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 ($1,500 vs $290). 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 ($)



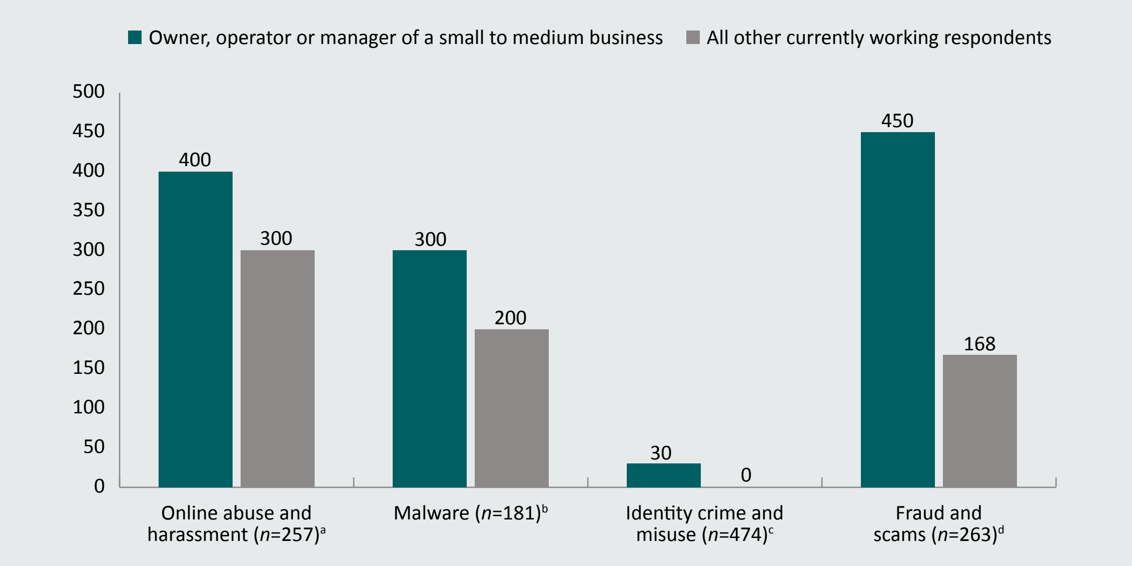
Note: Limited to victims who reported having lost money or spent money on consequences. Does not account for money recovered or reimbursed. Excludes 8 online abuse and harassment victims, 9 malware victims, 8 identity crime and misuse victims and 45 fraud and scam victims who did not know or answer the question about reporting to police or ReportCyber

Source: Australian Cybercrime Survey 2023 [weighted data]

Finally, given the propensity of respondents who were owners, operators or managers of a small to medium business 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 (16.5% vs 6.4%) and online abuse and harassment (17.8% vs 7.7%), but also for identity crime and misuse (29.3% vs 24.5%) and fraud and scams (40.6% vs 34.1%). Further, among those victims who did lose money or spend money on consequences, they reported a higher median financial loss (Figure 27). This was true for all types of cybercrime, including:

- online abuse and harassment ($800 per incident for small business owners, operators and managers, compared with $300 per incident for other respondents);
- malware ($300 vs $200);
- identity crime and misuse ($30 vs $0); and
- fraud and scams ($450 vs $168).

Figure 27: Median financial losses for most recent incident after recoveries, by small to medium business ownership status ($)



a: Includes 119 respondents who were the owner, operator or manager of a small to medium business and 138 respondents who were employees. Excludes 1 respondent who did not disclose whether they owned, operated or managed a small to medium business

b: Includes 87 respondents who were the owner, operator or manager of a small to medium business and 95 respondents who were employees. Excludes 1 respondent who did not disclose whether they owned, operated or managed a small to medium business

c: Includes 143 respondents who were the owner, operator or manager of a small to medium business and 331 respondents who were employees. Excludes 7 respondents who did not disclose whether they owned, operated or managed a small to medium business

d: Includes 104 respondents who were the owner, operator or manager of a small to medium business and 159 respondents who were employees. Excludes 2 respondents who did not disclose whether they owned, operated or managed a small to medium business

Note: Weighted frequencies and percentages may not add to total due to rounding. Includes respondents who had $0 of financial losses because they recovered the full amount they spent or lost. Figure only includes respondents who were past-year victims and currently working

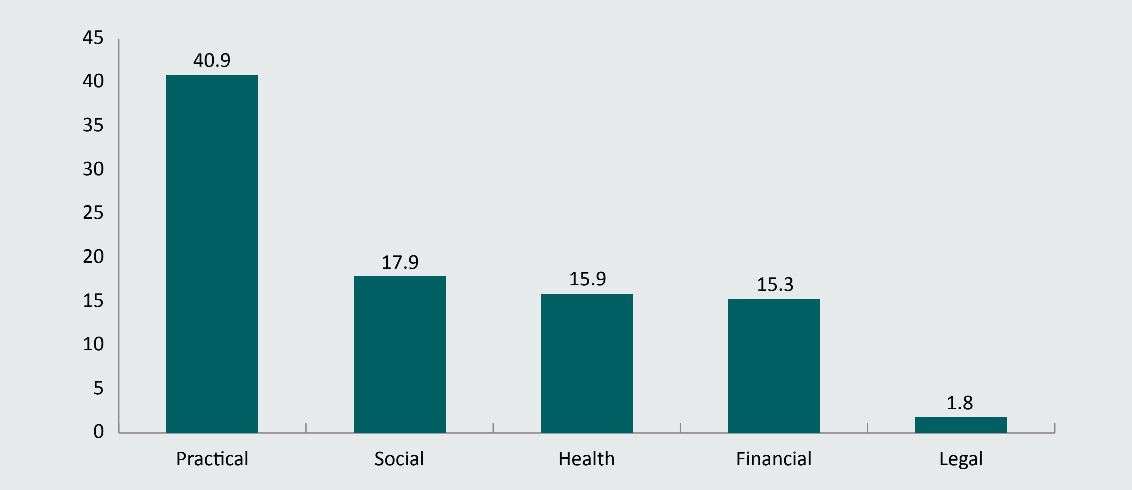
Source: Australian Cybercrime Survey 2023 [weighted data]

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 as a result of victimisation. The survey asked about 34 items in total, grouped into five domains: practical impacts (12 items), social impacts (5 items), health impacts (7 items), financial impacts (8 items) and legal impacts (2 items).

Overall, 53.1 percent of cybercrime victims were negatively impacted in some way. This means an estimated 24.7 percent of respondents to the survey were negatively impacted by cybercrime in the 12 months prior to the survey. Forty-one percent of victims reported practical impacts, 17.9 percent reported social impacts, 15.9 percent reported health-related harms, and 15.3 percent reported financial problems. Legal issues were comparatively rare (1.8%; Figure 28).

Figure 28: Harms from cybercrime among victims (%) (*n*=6,295)



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

Source: Australian Cybercrime Survey 2023 [weighted data]

Box 11: Why measure other harms from cybercrime?

Given the profit-motivated nature of many types of cybercrime, the financial losses victims experience are often emphasised. These are, of course, important. But the impact of cybercrime can extend well beyond these financial losses. Cybercrime can have a profound impact on people's lives, and data on the harms to victims can help inform decisions about how best to support victims after an incident has occurred.

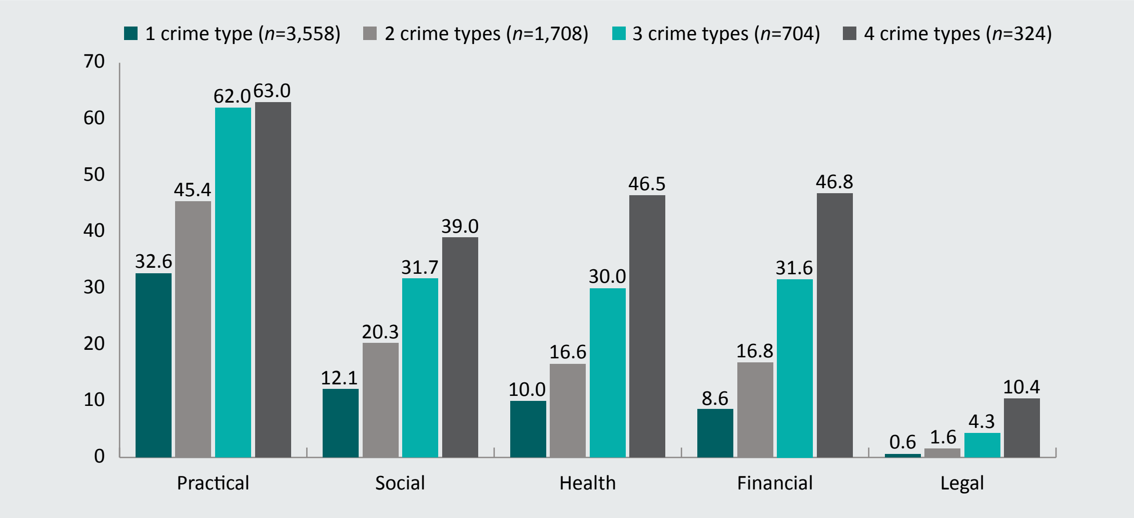
A growing body of evidence shows victims of cybercrime experience trauma and hardship in response to their victimisation. Victims of cyber-enabled crimes can experience financial hardship, emotional distress (eg feelings of embarrassment, shame, anger, sadness and distress), loss of confidence in other people, physical symptoms (eg difficulty sleeping, weight loss and nausea), relationship and family conflict, and, at the extreme end of the spectrum, suicidal thoughts and ideation (Cross, Richards & Smith 2016). Victims of cyber-dependent crime also report problems communicating with friends and family, financial strain, problems dealing with businesses, and even mental or emotional distress requiring treatment (Teunissen, Voce & Smith 2021).

While it is difficult to measure in a survey such as this one, the harms experienced by victims will be influenced by their personal circumstances. Financial losses will have a variable effect on victims. Two victims may lose the same amount of money, but if one of those victims has a much more precarious financial situation then the effect of that loss can be more significant.

Importantly, collecting data on the harm to victims, irrespective of whether they report to police or some other source, can provide a more complete picture of the impact of cybercrime on the Australian community. Some people may choose not to report despite being seriously impacted. However, research shows that victims who experience more harm are more likely to report to police, meaning official data may also overstate the effect of cybercrime on victims.

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 29). For example, while 32.6 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 (62.0% and 63.0% of victims, respectively). 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 social, 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.

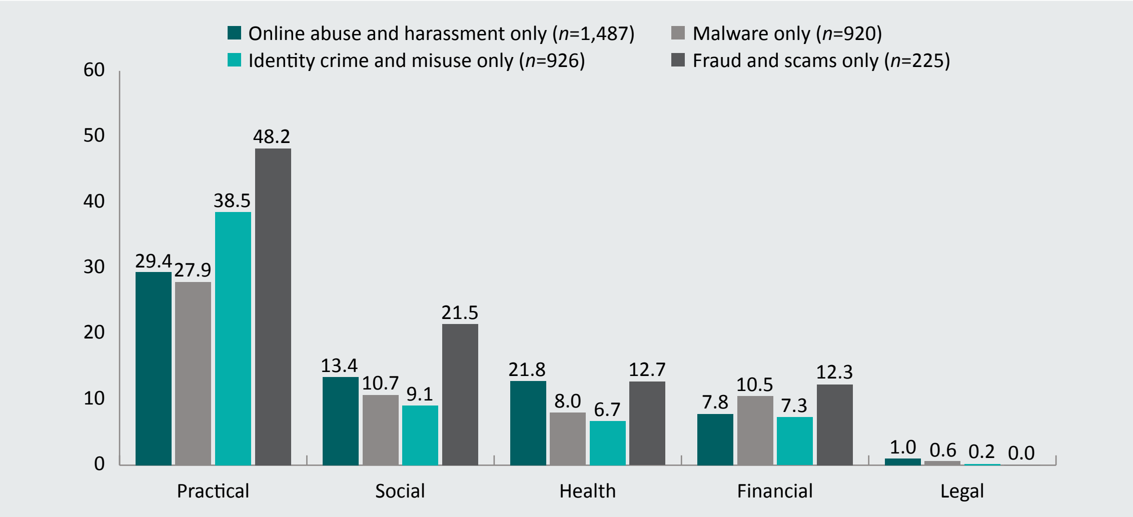
Figure 29: Harms from cybercrime among victims, by number of crime types reported (%) (*n*=6,295)



Note: Excludes 174 victims who did not answer this question. Weighted frequencies and percentages may not add to total due to rounding
Source: Australian Cybercrime Survey 2023 [weighted data]

In order to directly compare harm among victims who were victims of different types of cybercrime, it was necessary to limit the analysis to victims who experienced just one type of cybercrime (Figure 30). 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 (48.2 and 21.5%, respectively). They were also the most likely to report financial impacts (12.3%), followed by malware victims (10.5%), while a similar proportion of fraud and scam (12.7%) and online abuse and harassment victims (12.8%) said their health was impacted in some way as a result of being a victim of cybercrime in the 12 months prior to the survey.

Figure 30: Harms from cybercrime among victims, by crime type (%) (*n*=6,295)



Note: Excludes 55 online abuse and harassment victims, 97 malware victims, 29 identity crime and misuse victims and 28 fraud and scam 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 2023 [weighted data]

The most common practical issues victims encountered were difficulty knowing which information to trust online (22.0%); being less confident using the internet for personal affairs (14.5%); having to change their personal, banking and/or contact information (13.2%); and having their studies negatively impacted (12.8%; Table 18). Less common issues included problems communicating or dealing with businesses (1.8%) or government departments (1.8%) and the respondent having to change their place of residence (1.1%**).**

For harms within the social domain, 11.6 percent of victims lost trust in other people, 5.0 percent were embarrassed or had their reputation damaged, 4.5 percent became more socially isolated, 2.6 percent stated that their relationships with family and friends were negatively impacted, and 2.8 percent stated that their relationship with their partner was negatively impacted. When examining victims who experienced only one type of cybercrime, social harms were most prevalent among fraud and scam victims and least prevalent among identity crime and misuse victims.

For harms within the physical and psychological health domain, 9.6 percent of victims experienced mental or emotional distress, 6.7 percent had difficulty sleeping, and 3.8 percent stated that their physical health and wellbeing had deteriorated. In addition, 2.5 percent sought psychological or counselling treatment, 1.6 percent increased their consumption of alcohol, 1.3 percent had to seek medical treatment, and 1.1 percent increased their consumption of illegal or legal drugs. Compared with other cybercrime types, health-related harms were most prevalent among online abuse and harassment victims and fraud and scam victims.

For financial harms, 5.3 percent of victims experienced an increase in financial stress; 4.1 percent had to buy new software; 3.6 percent had to pay for computer, phone or other hardware repairs or replacement; and 2.7 percent had to buy new backup data storage or data storage devices. It was less common that victims had to borrow money from family or friends (2.6%), were unable to get a loan when they needed one (1.5%), increased the time or money they spent gambling (1.3%) or lost their job (0.8%). Compared with other cybercrime types, financial harms were most common among fraud and scam victims.

Within the legal domain, 1.3 percent of victims had to commence legal action and less than one percent had been in trouble with the police.

Table 18: Harms to individual cybercrime victims (%) (*n*=6,295)

	n	%
Practical impacts		
Respondent found it harder to know which information to trust online	1,382	22.0
Respondent less confident using the internet for personal affairs (eg banking, purchasing items)	911	14.5
Respondent had to change personal, banking and/or contact information	830	13.2
Respondent's studies were negatively impacted[a]	10	12.8
Respondent had difficulty accessing online accounts and resources (eg bank accounts, utilities, email)	248	3.9
Respondent had problems communicating with people (eg friends, family, employer)	178	2.8
Respondent's work was negatively impacted[b]	139	2.7
Respondent lost important or sentimental data (eg photos, contact details, files)	128	2.0
Respondent had to take time off work to deal with the consequences of victimisation[b]	97	2.3
Respondent had problems communicating or dealing with businesses	115	1.8
Respondent had problems communicating or dealing with government departments	116	1.8
Respondent had to change their place of residence	68	1.1
Social impacts		
Respondent lost trust in other people	732	11.6
Respondent was embarrassed or their reputation was damaged	314	5.0
Respondent became more socially isolated	283	4.5
Respondent stated their relationship with their partner had been negatively impacted[c]	110	2.8
Respondent stated their relationships with family and friends had been negatively impacted	166	2.6

Table 18: Harms to individual cybercrime victims (%) (*n*=6,295) (continued)

	n	%
Health impacts		
Respondent experienced mental or emotional distress	604	9.6
Respondent experienced difficulty sleeping	419	6.7
Respondent stated their overall physical health and wellbeing had deteriorated	237	3.8
Respondent had to seek psychological or counselling treatment	155	2.5
Respondent increased their consumption of alcohol	103	1.6
Respondent had to seek medical treatment	82	1.3
Respondent increased their consumption of drugs (legal or illegal)	71	1.1
Financial impacts		
Respondent experienced an increase in financial stress	336	5.3
Respondent had to buy new software	255	4.1
Respondent had to pay for computer, phone or other hardware repairs or replacement	226	3.6
Respondent had to buy new backup data storage or data storage devices	171	2.7
Respondent had to borrow money from family and friends	161	2.6
Respondent was unable to get a loan when they needed one	94	1.5
Respondent increased the amount of time and/or money they spent gambling (in person or online)	80	1.3
Respondent lost their job	53	0.8
Legal impacts		
Respondent had to commence legal action	81	1.3
Respondent had been in trouble with the police	34	0.5

a: Only includes victims who were currently studying full time (*n*=81)

b: Only includes victims who were currently working (*n*=4,129)

c: Only includes victims who were in a current relationship (*n*=3,952)

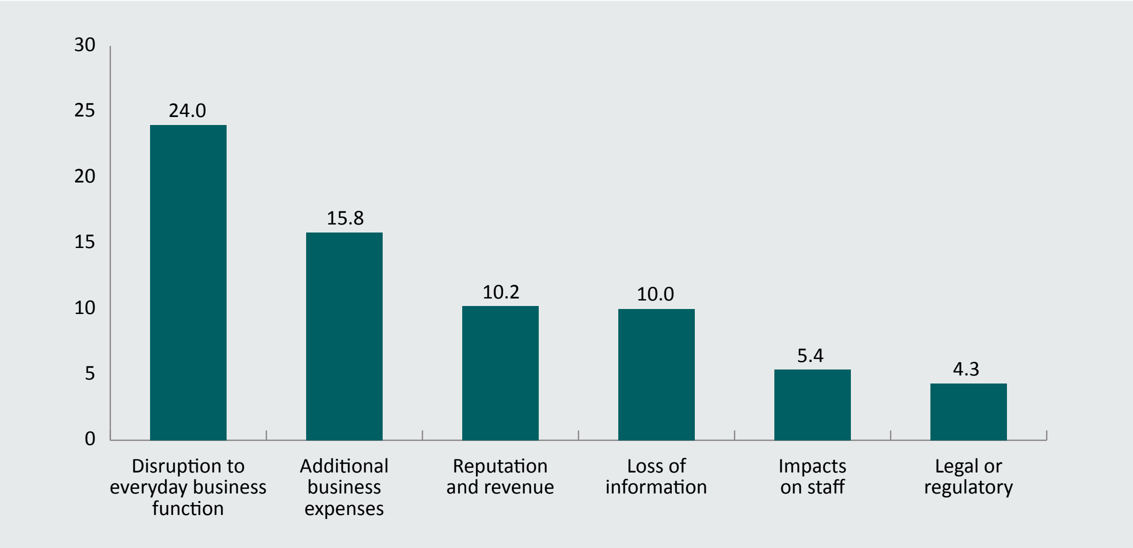
Note: Excludes 174 victims who did not answer this question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2023 [weighted data]

Impact on small to medium businesses

Thirty-nine 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 22.0 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 (24.0%), additional business expenses (15.8%), impacts on their reputation or revenue (10.2%), loss of information (10.0%), impacts on staff (5.4%) and legal or regulatory ramifications (4.3%; Figure 31).

Figure 31: Harms to business from cybercrime among victims who owned, operated or managed a small to medium business (%) (*n*=952)



Note: Excludes 54 small to medium business owners who did not answer this question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2023 [weighted data]

Small to medium business owners, operators and managers reported a variety of impacts on their business (Table 19). Most commonly, they had to spend time repairing and improving systems (7.3%); had to change their business banking or contact information (7.2%); had to buy new backup data storage or data storage devices (6.4%); had to buy new software (6.1%); had to pay for computer, phone or other hardware repairs or replacement (5.7%); and had difficulty accessing online accounts and resources (5.1%).

Table 19: 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	69	7.3
Had to change the business banking and/or contact information	69	7.2
Difficulty accessing online accounts and resources (eg bank accounts, utilities, email)	48	5.1
Disruption to operations and/or trading (eg inability to carry out transactions, websites not functioning)	44	4.6
Blocked customer access to the business online store or website	40	4.2
Had problems communicating or dealing with government departments	33	3.5
Had problems communicating or dealing with businesses	29	3.1
Had to shut down the business online store or website (temporarily or permanently)	30	3.1
Additional business expenses		
Had to buy new backup data storage or data storage devices	61	6.4
Had to buy new software	58	6.1
Had to pay for computer, phone or other hardware repairs or replacement	54	5.7
Insurance premiums were increased	31	3.2
Loss of information		
The business had to notify affected parties of a data breach	43	4.5
Theft of my information or other staff information (eg contact details, financial data)	34	3.6
Theft of intellectual property or corporate information	24	2.5
Theft of customer or supplier information (eg contact details, financial data)	23	2.4
Reputation and revenue		
There was a loss of customers, sales or revenue	40	4.2
Professional relationships were damaged	30	3.2
The business reputation was damaged	30	3.2
We lost business contracts	14	1.5
Impacts on staff		
Employees/owners of the business had to take time off work	36	3.8
Employees/owners of the business resigned or lost their job	20	2.1
Legal or regulatory sanctions		
The business was hit with fines and regulatory sanctions	26	2.8
There was litigation or legal action against the business	19	2.0

Note: Excludes 54 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 2023 [weighted data]

Box 12: Cybercrime and its effects on small to medium business

This study has highlighted the effects of cybercrime on small business owners, operators and managers. Respondents who owned and operated a small to medium business were significantly more likely than other respondents to have fallen victim to cybercrime in the 12 months prior to the survey. This was true for all types of cybercrime measured by the survey. While the survey did not specifically ask whether the cybercrime targeted a work or personal device, for many smaller businesses there may be no such separation.

When they fell victim, small to medium business owners and operators were more likely to have lost money or spent money on consequences and, when they did, they lost larger amounts of money than other victims. Two in five respondents who were small business owners and operators said their business was impacted as a result of cybercrime. Some of these effects—whether they relate to business operations, profitability or reputation—are not easily costed, meaning the businesses likely experienced financial impacts extending beyond those which could be estimated and counted in the survey.

Large corporations and government have access to significant resources for ICT security. Conversely, small to medium businesses may be large enough to have the infrastructure, data holdings (or access to networks of larger organisations) and profits to be attractive targets for cybercrime, but not the resources, expertise and capability to prevent cybercrimes. Despite losing larger amounts of money than other victims, there was little difference in reporting, suggesting that small business owners and operators may be reluctant to report. The effect of cybercrime on small businesses may have flow-on implications, such as for customers who are secondary victims of data breaches, or for larger organisations, if offenders use these smaller businesses in the supply chain to gain access to their systems and networks.

These results highlight the importance of building the capability of small to medium business operators to prevent cybercrime and ensuring that support for victims is both available and accessible.

References

URLs correct as at May 2023

Australian Bureau of Statistics (ABS) 2023a. *National, state and territory population, September 2022*. https://www.abs.gov.au/statistics/people/population/national-state-and-territory-population/latest-release

Australian Bureau of Statistics (ABS) 2023b. *Personal fraud, 2012–22*. https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release

Australian Bureau of Statistics (ABS) 2023c. *Regional population, 2021–22*. https://www.abs.gov.au/statistics/people/population/regional-population/2021-22

Australian Bureau of Statistics (ABS) 2022a. *Australian Industry, 2021–22*. https://www.abs.gov.au/statistics/industry/industry-overview/australian-industry/latest-release

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

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

Australian Bureau of Statistics (ABS) 2022d. *Education and work, Australia, May 2022*. https://www.abs.gov.au/statistics/people/education/education-and-work-australia/latest-release

Australian Bureau of Statistics (ABS) 2019. *Estimates and projections, Aboriginal and Torres Strait Islander Australians, 2006–2031*. https://www.abs.gov.au/statistics/people/aboriginal-and-torres-strait-islander-peoples/estimates-and-projections-aboriginal-and-torres-strait-islander-australians/latest-release

Australian Competition and Consumer Commission (ACCC) 2023. Scam statistics. https://www.scamwatch.gov.au/scam-statistics

Australian Cyber Security Centre (ACSC) 2023. Guidelines for cyber security incidents. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents

Australian Cyber Security Centre (ACSC) 2022. *Annual cyber threat report, July 2021 to June 2022*. Canberra: ACSC. https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

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

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

Chang L & Krosnick JA 2009. National surveys via RDD telephone interviewing versus the internet: Comparing sample representativeness and response quality. *Public Opinion Quarterly* 73(4): 641–78. https://doi.org/10.1093/poq/nfp075

Cheung KL, ten Klooster PM, Smit C, de Vries H & Pieterse ME 2017. The impact of non-response 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

Cross C, Holt T, Powell A & Wilson M 2021. Responding to cybercrime: Results of a comparison between community members and police personnel. *Trends & issues in crime and criminal justice* no. 635. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78207

Cross C, Richards K & Smith RG 2016. The reporting experiences and support needs of victims of online fraud. *Trends & issues in crime and criminal justice* no. 518. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi518

eSafety Commissioner 2022. Australians' negative online experiences 2022. https://www.esafety.gov.au/research/australians-negative-online-experiences-2022

Klauzner I & Pisani A 2023. *Trends in and characteristics of cybercrime in NSW.* Bureau Brief No. 165. Sydney: NSW Bureau of Crime Statistics and Research. https://www.bocsar.nsw.gov.au/Pages/bocsar_publication/Pub_Summary/BB/BB165-Summary-Cybercrime-in-NSW.aspx

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

McAlister M, Faulconbridge E, Voce I & Bricknell S 2023. *Identity crime and misuse in Australia 2023*. Statistical Bulletin no. 42. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb77048

McAlister M & Franks C 2021. *Identity crime and misuse in Australia: Results of the 2021 online survey.* Statistical Bulletin no. 37. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78467

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

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

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

Teunissen C, Voce I & Smith RG 2021. *Estimating the cost of pure cybercrime to Australian individuals.* Statistical Bulletin no. 34. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78269

van de Weijer SGA, Leukfeldt R & Bernasco W 2019. Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology* 16(4): 486–508. https://doi.org/10.1177/1477370818773610

Van de Weijer SGA, Leukfeldt R & van der Zee S 2021. Cybercrime reporting behaviors among small- and medium-sized enterprises in the Netherlands. In M Weulen Kranenbarg & R Leukfeldt (eds), *Cybercrime in context: The human factor in victimization, offending, and policing.* Crime and justice in digital society vol 1. Cham: Springer. https://doi.org/10.1007/978-3-030-60527-8_17

Voce I & Morgan A 2023. 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

Voce I & Morgan A 2022. *Help-seeking among Australian ransomware victims.* Statistical Bulletin no. 38. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78504

Voce I & Morgan A 2021. *Ransomware victimisation among Australian computer users.* Statistical Bulletin no. 35. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78382

Wilson M, Cross C, Holt T & Powell A 2022. Police preparedness to respond to cybercrime in Australia: An analysis of individual and organizational capabilities. *Journal of Criminology* 55(4): 468–494. https://doi.org/10.1177/26338076221123080

Wolbers H, Boxall H, Long C & Gunnoo A 2022. *Sexual harassment, aggression and violence victimisation among mobile dating app and website users in Australia.* Research Report no. 25. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/rr78740

Xie M & Baumer EP 2019. Crime victims' decisions to call the police: Past research and new directions. *Annual Review of Criminology* 2(1): 217–240. https://doi.org/10.1146/annurev-criminol-011518-024748

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

Introduction

This appendix describes the methodology for a survey of 13,887 Australians aged 18 years and over about their experience of cybercrime. It was prepared with input from Roy Morgan Research Solutions. 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 (ICT) 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 ICT, 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 designed the inaugural Australian Cybercrime Survey (ACS). This will be conducted annually and 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 which will measure repeat victimisation among a cohort of approximately 3,000 respondents and provide 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. This questionnaire is available to download. 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, their 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 with a sample of 67 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.

Addenda

In the 2023 survey there were three addenda asking additional questions that did not feature in the core survey. Upon completing the core survey, respondents completed one of the three addenda questionnaires.

Identity crime and biometrics addendum

This addendum measured perceptions of identity crime and prevention measures among the Australian community, including perceptions of the seriousness of identity crime, whether it will change over time, and whether they already use or are willing to use biometric technologies to minimise the risk of identity crime.

Cybercrime resilience and risk addendum

This addendum measured resilience to cybercrime victimisation by examining individuals' motivation to protect themselves, their opportunities to implement protective measures, and their knowledge of how to prevent and address cybercrime. The addendum also measured perceptions of cybercrime seriousness and threat, where respondents get their cybercrime information, and perceptions of law enforcement and government responses. Individual-level risk factors were also measured, including trust in others, loneliness and isolation, impulsiveness and risk-taking, and depression and anxiety. There were four versions of this addenda, and respondents in this subsample were randomly assigned to one of four groups. Each group was asked questions about a specific form of cybercrime covered by the survey: fraud and scams, identity crime and misuse, malware and online abuse and harassment.

Ransomware addendum

The final addendum measured the ways in which ransomware attacks take place, including information about the affected device, how it was compromised, any extortion attempts, the response by the victim and the outcomes of the ransomware attack. This addendum was only completed by respondents who said they had been a victim of a ransomware attack.

Longitudinal study and evaluation of intervention messages

A major component of the survey involves testing the deployment of targeted prevention advice to the Australian community. This required recruiting an additional 3,000 respondents to participate in the longitudinal study, which means they will participate in two waves of the Australian Cybercrime Survey (2023 and 2024).

All respondents who participated in the core survey, besides those from the Dynata panel, were invited to participate in this longitudinal study. They were asked to consent to participate in a longitudinal study and be contacted with cybercrime prevention information.

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 8 February and 13 March 2023 by Roy Morgan Research Solutions using their Single Source panel and two highly regarded panels managed by PureProfile and Dynata. These panels are opt-in panels, 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, sex and usual place of residence (see Table A1)—and participants were invited to complete the survey until these quotas were reached, within an agreed margin of error. The aim was to ensure the final sample was representative of the spread of the Australian population.

Members of the three 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 (61.9%) were recruited from this panel. Pure Profile panel members accounted for 35.0 percent of respondents, and Dynata the remaining 3.1 percent.

Table A1: Roy Morgan Research Solutions Single Source panel quotas (%)

	18–24	25–34	35–49	50–64	65+	Total
Male						
Sydney	1.2	2.2	2.9	2.2	1.9	10.3
Rest of NSW (incl. ACT)	0.7	0.9	1.4	1.5	1.6	6.1
Melbourne	1.1	2.1	2.7	2.1	1.8	9.8
Rest of Victoria	0.3	0.4	0.6	0.7	0.8	2.9
Brisbane	0.6	1.0	1.3	1.1	0.9	4.9
Rest of Queensland	0.5	0.8	1.2	1.2	1.2	5.0
Adelaide	0.3	0.5	0.7	0.6	0.6	2.6
Rest of SA (incl. NT)	0.1	0.2	0.3	0.3	0.3	1.2
Perth	0.5	0.8	1.1	0.9	0.8	4.1
Rest of WA	0.1	0.2	0.3	0.3	0.2	1.1
Hobart	0.1	0.1	0.1	0.1	0.1	0.5
Rest of Tasmania	0.1	0.1	0.1	0.1	0.2	0.6
Total	5.5	9.2	12.7	11.2	10.3	49.0
Female						
Sydney	1.1	2.2	2.9	2.3	2.2	10.7
Rest of NSW (incl. ACT)	0.6	0.9	1.5	1.6	1.8	6.4
Melbourne	1.1	2.1	2.7	2.2	2.1	10.2
Rest of Victoria	0.3	0.4	0.7	0.8	0.9	3.0
Brisbane	0.6	1.0	1.4	1.1	1.0	5.1
Rest of Queensland	0.5	0.8	1.3	1.3	1.3	5.2
Adelaide	0.3	0.5	0.7	0.7	0.7	2.8
Rest of SA (incl. NT)	0.1	0.2	0.3	0.3	0.3	1.2
Perth	0.5	0.8	1.1	1.0	0.9	4.2
Rest of WA	0.1	0.1	0.3	0.3	0.2	1.0
Hobart	0.1	0.1	0.1	0.1	0.1	0.5
Rest of Tasmania	0.1	0.1	0.1	0.2	0.2	0.6
Total	5.3	9.3	13.0	11.8	11.6	51.0

Source: Roy Morgan [computer file]

Participants were invited until the relevant quotas had been reached. Data on completion rates were available from the Roy Morgan Single Source panel (Table A2). Overall, 158,845 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 15,735 invitations were opened (9.9%), meaning that the respondent proceeded to the survey landing page. Of these, 2,282 people (1.4%) 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 4,960 respondents (3.0%) 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 (1.2%) 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 5.4 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, 54.6 percent of people who opened the invitation, and 63.9 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.

The final sample size was 13,887 respondents. The survey took respondents an average of 24.8 minutes (*SD*=11.2) to complete.

Table A2: Invitation and completion rates, Roy Morgan Single Source panel (unadjusted)

	n	%
Total invitations sent out (T)	158,845	–
Total not started interview (NS)	143,110	90.1
Total started interview (S)	15,735	9.9
Complete interviews (I)	8,597	5.4
Partial interviews (P)	4,690	3.0
Screened out or quota reached (SQ)	2,282	1.4
Previously responded or poor quality (DQ)	166	0.1
Non-participation rate (NS)/(T)		90.1
Completion rate for accepted invitations by eligible respondents (I)/(S–SQ)		63.9
Completion rate (I)/(T)		5.4

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 Australian Bureau of Statistics (ABS) demographic data, prior to weighting, are presented in Table A3. New South Wales residents were slightly over-represented in the survey data (32.3% vs 31.4%), as were residents of South Australia (7.5% vs 7.1%) and Victoria (25.9% vs 25.6%). Meanwhile, residents of Western Australia (10.2% vs 10.6%), the Northern Territory (0.4% vs 0.9%) and Queensland (20.0% vs 20.3%) were slightly under-represented.

Table A3: Respondents by usual place of residence (unweighted data; *n*=13,887)

	ABS demographic statistics (June 2022)[a]	Survey respondents	
	%	*n*	%
NSW	31.4	4,480	32.3
Vic	25.6	3,592	25.9
Qld	20.3	2,778	20.0
WA	10.6	1,409	10.2
SA	7.1	1,042	7.5
Tas	2.2	294	2.1
ACT	1.8	235	1.7
NT	0.9	57	0.4

a: Estimated resident population at 30 June 2022
Note: Percentages may not total 100 due to rounding
Source: ABS 2023a; Australian Cybercrime Survey 2023, AIC [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 by age, sex and state and territory according to the ABS estimated residential population (ABS 2023a). 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 the 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 internet or social media users 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 13,887 respondents.

Table A4 shows the effect of weighting on the concordance between the adult population in each state and territory according to the ABS (2023a) 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 (0.4% vs 0.9%). Correcting this would have resulted in weights for NT respondents that exceeded the cap.

Table A4: Respondents by usual place of residence (weighted data, %)

	ABS demographic statistics (June 2022)[a]	Survey respondents (*n*=13,887)
NSW	31.4	31.7
Vic	25.6	25.7
Qld	20.3	20.4
WA	10.6	10.7
SA	7.1	7.4
Tas	2.2	2.3
ACT	1.8	1.5
NT	0.9	0.4

a: Estimated resident population at 30 June 2022
Note: Percentages may not total 100 due to rounding
Source: ABS 2023a; Australian Cybercrime Survey, AIC [computer file]

To further examine concordance, the unweighted and unweighted ages of respondents were compared with the estimated resident population (Table A5). What this shows is that, when the data were weighted, any observable differences in the age profile of respondents effectively disappeared.

Table A5: Respondents by age (%)

	ABS demographic statistics (June 2022)[a]	Survey respondents (unweighted, *n*=13,887)	Survey respondents (weighted, *n*=13,887)
18–24	11.0	10.3	11.1
25–34	18.4	18.4	18.2
35–49	25.7	24.5	25.7
50–64	23.0	23.1	23.0
65+	21.8	23.7	22.1

a: Estimated resident population at 30 June 2022
Source: ABS 2023a; Australian Cybercrime Survey 2023, AIC [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 A6). Results from this comparison demonstrate a relatively high degree of concordance between ACS respondent characteristics and ABS demographic data for gender (49.7% female in the ACS vs 50.8% in the general population), Aboriginal and Torres Strait Islander status (3.5% vs 2.7%), usual place of residence (remoteness, 72.9% metropolitan in the ACS vs 72.2% in the general population), and the proportion of respondents with a non-school qualification as the highest level of education completed (70.7% vs 70.1%).

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 2022b). That said, ACS respondents were slightly less likely than the general population to say they were born overseas (22.0% 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 2022c). Similarly, there are limitations with 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 (9.4% 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 A6: Selected sociodemographic characteristics of respondents (weighted data; %)

	ABS statistics	Survey respondents (weighted)
Female[a]	50.8	49.7
Aboriginal and/or Torres Strait Islander[b]	2.7	3.5
Non-English-speaking background[c]	22.3	4.6
Born overseas[d]	27.6	22.0
Disability[e]	17.7	9.4
Non-school qualification (20–64 years only)[f]	70.1	70.7
Usual place of residence[g]		
Major cities	72.2	72.9
Regional	25.9	23.9
Remote	1.9	2.9

a: Proportion of estimated residential population as at September 2022 who were female (ABS 2023a)

b: Projected resident Aboriginal and Torres Strait Islander population as proportion of persons aged 18 years and over as at September 2022 (ABS 2019, 2023a). Denominator for survey respondents includes 153 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 2022b). For the ACS, proportion of respondents who speak a language other than English most often at home. Denominator includes 46 respondents who did not know or declined to answer the question

d: Proportion of Australians who were born overseas (ABS 2022b). Denominator for survey respondents includes 291 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 409 respondents who did not know or declined to answer this question.

f: Estimated proportion of persons aged 20–64 years with a non-school qualification (ABS 2022d). Denominator for survey respondents includes 42 respondents who selected 'Other', did not know or declined to answer the question

g: Estimated resident population, by remoteness areas (ABS 2023c). Denominator for survey respondents includes 41 respondents where this information was unknown

Source: ABS (various); AIHW (2022); Australian Cybercrime Survey 2023, AIC [computer file]

As a final check to understand the impact of the weighting procedure, the weighted and unweighted results for lifetime prevalence of the four main types of cybercrime were compared (Table A7). This shows the weighting procedure used for the survey did not significantly affect the estimated prevalence of cybercrime among respondents.

Table A7: Lifetime prevalence of cybercrime victimisation (weighted and unweighted data; %)

	Prevalence (unweighted)	Prevalence (weighted)
Online abuse and harassment	42.9	40.9
Malware	36.8	35.5
Identity theft	32.2	31.4
Fraud and scams	13.8	13.6

Source: Australian Cybercrime Survey 2023, AIC [computer file]

AIC reports

Statistical Report

Isabella Voce is an Acting Principal Research Analyst at the Australian Institute of Criminology.

Anthony Morgan is a Research Manager at the Australian Institute of Criminology.

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

www.aic.gov.au