Australian Government
Australian Institute of Criminology

AIC reports
Statistical Report 59

Cybercrime in Australia 2025

Isabella Voce
Anthony Morgan

ISSN 2206-7930 (Online)
ISBN 978 1 922878 35 9 (Online)
https://doi.org/10.52922/sr78359

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

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

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

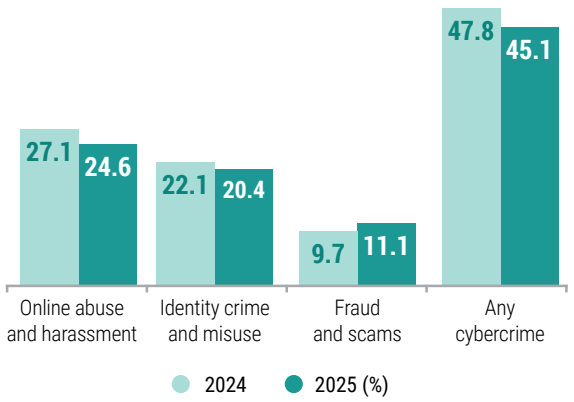
General editor: Dr Rick Brown, Deputy Director, Australian Institute of Criminology

Edited and typeset by the Australian Institute of Criminology

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

WHAT CHANGED FROM 2024 TO 2025?

ONLINE ABUSE AND HARASSMENT, IDENTITY CRIME AND CYBERCRIME OVERALL DECREASED, BUT FRAUD AND SCAMS INCREASED



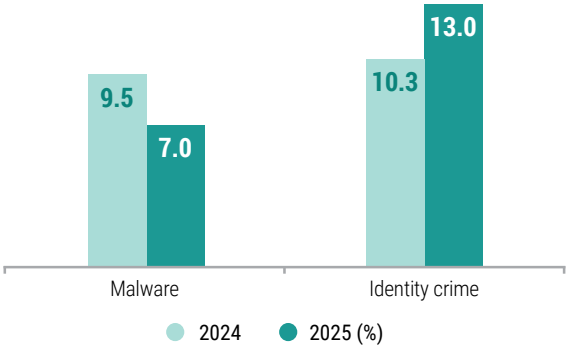
Fewer respondents were impersonated online, received unsolicited sexual material, or had their financial accounts compromised

More respondents fell victim to pure ransomware and other identity compromise

FOR THE SECOND YEAR RUNNING, USE OF IMPORTANT ONLINE SAFETY MEASURES DECREASED

- Checking social media privacy settings
- Purchasing cyber insurance
- Using spam-filters, antivirus software or firewalls
- Using password protection on their router and different passwords for online accounts
- Avoiding clicking on links from unknown senders

REPORTING TO POLICE OR REPORTCYBER DECREASED AMONG MALWARE VICTIMS AND INCREASED AMONG IDENTITY CRIME AND MISUSE VICTIMS



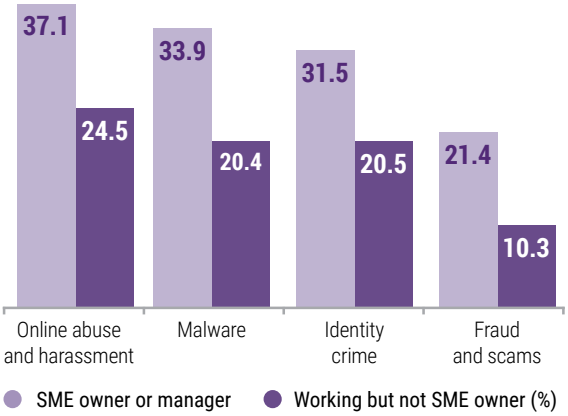
Victims were just **as likely in 2025 as in 2024** to say they did not make an official report to police or ReportCyber because of their understanding, perceptions and past experiences of reporting, or because they were worried about the consequences of reporting—including shame or embarrassment.

The proportion of malware victims who recovered money increased from **52% to 69%**

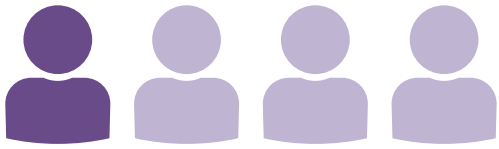
But there was **no change** in average net financial losses for any cybercrime type. Victims were **just as likely** to report financial and non-financial harms in 2025 as in 2024.

SPOTLIGHT ON SMALL TO MEDIUM ENTERPRISE OWNERS AND MANAGERS

MORE LIKELY THAN OTHER RESPONDENTS TO FALL VICTIM TO ALL TYPES OF CYBERCRIME



One in four respondents said their business was negatively impacted by cybercrime in the last 12 months.

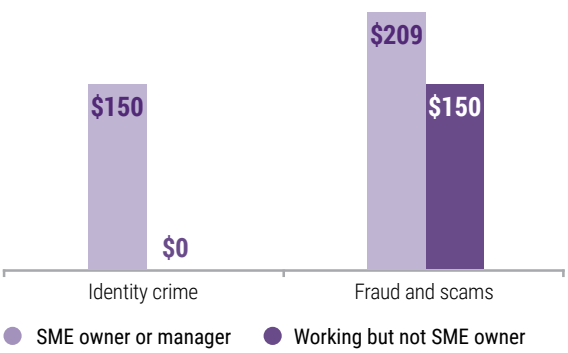


MORE LIKELY THAN OTHERS TO MAKE OFFICIAL REPORTS TO POLICE OR REPORTCYBER, BUT REPORTING IS STILL LOW:

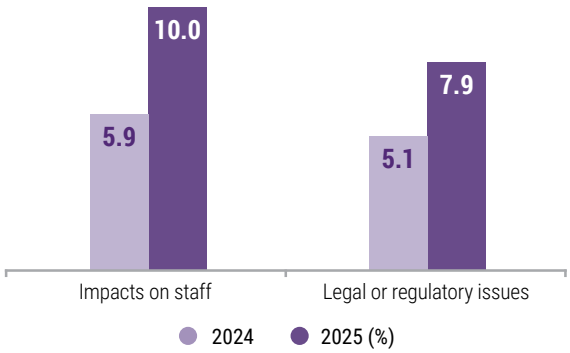
- **1 in 5** for online abuse and harassment
- **1 in 7** for malware
- **1 in 5** for identity crime and misuse
- **1 in 8** for fraud and scams

- **28.7%** of victims said cybercrime impacted the everyday function of their business
- **16.4%** said being a victim created additional business expenses
- **15.9%** said they lost business information
- **14.1%** said cybercrime harmed their reputation or revenue

VICTIMS OF IDENTITY CRIME AND MISUSE AND FRAUD AND SCAMS HAD HIGHER MEDIAN NET LOSSES THAN OTHER RESPONDENTS



MORE CYBERCRIME VICTIMS REPORTED IMPACTS ON STAFF AND LEGAL OR REGULATORY ISSUES IN 2025 THAN IN 2024.



Contents

Boxes

Figures

Tables

Acknowledgements

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

The Australian Cybercrime Survey was developed in consultation with representatives from the Attorney-General's Department, Australian Federal Police, Australian Cyber Security Centre, Department of Home Affairs, eSafety Commissioner, National Anti-Scam Centre and state and territory law enforcement agencies. 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 and abbreviations

ABS	Australian Bureau of Statistics
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
SME	small to medium enterprise

Abstract

In 2025, 10,593 online Australians participated in the Australian Cybercrime Survey. Nearly half of all respondents reported having been a victim of some form of cybercrime in the 12 months prior to the survey. This included online abuse and harassment (24.9% of respondents), followed by malware (21.5%), identity crime and misuse (20.6%) and fraud and scams (11.4%). One in five respondents experienced multiple types of cybercrime. Between 2024 and 2025, the proportion of respondents who had been a victim of online fraud and scams increased.

As with previous years, certain sections of the community were more likely than others to fall victim. For the second year running, the proportion of respondents who said they were using various online safety strategies decreased from the year before. However, fewer respondents participated in online activities associated with a higher risk of victimisation or engaged in unsafe online behaviours like sharing passwords. Most cybercrime continues to go unreported to police and ReportCyber. The harm to individual victims remained steady in 2025, but the proportion of small to medium business operators who reported impacts on their staff and legal or regulatory issues due to cybercrime increased.

Summary

Between May and July 2025, 10,593 computer users were recruited from online panels to participate in the Australian Cybercrime Survey (ACS). The survey measures four broad categories of cybercrime: online abuse and harassment, malware attacks, identity crime and misuse, and fraud and scams.

Victimisation remains high, although there were decreases in online abuse and harassment and identity crime and misuse.

Almost two-thirds of respondents (63.9%) said they had been the victim of at least one type of cybercrime measured by the survey during their lifetime, and nearly half (45.5%) had been a victim in the 12 months prior to the survey. Online abuse and harassment was the most common type of cybercrime reported (24.9% of respondents had been a victim in the past 12 months), followed by malware (21.5%), identity crime and misuse (20.6%), and fraud and scams (11.4%). 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, with 20.2 percent of respondents (44.3% of all victims) being victims of two or more types of cybercrime in the 12 months prior to the survey.

The most common forms of online abuse and harassment that victims experienced in the past year were someone impersonating them online (7.1% of respondents) and being sent unsolicited sexually explicit messages, images or videos (6.3%). Strangers were the most common perpetrators of these types of technology-facilitated abuse and harassment. Fifteen percent of incidents of online abuse and harassment were domestic or family violence related, meaning they involved a current or former intimate partner or a family member. But this was higher for certain forms of online abuse and harassment, including stalking and harassment (32.6% involving current/former intimate partners or family members) and controlling and restricting behaviours (25.3%). While less common, these offences are particularly harmful, often occur as part of an ongoing pattern, and can be difficult for victims to stop.

We compared the prevalence of cybercrime among respondents to the 2024 and 2025 ACS, adjusting for differences between the two samples. The prevalence of online abuse and harassment (27.1% in 2024 vs 24.6% in 2025) was lower among 2025 respondents than in the 2024 survey. This reduction appears to be driven largely by a decline in the proportion of respondents who received unsolicited sexually explicit photos or videos (7.6% in 2024 vs 6.3% in 2025).

This form of cybercrime also declined in the previous year. Following research finding very high rates of sexual aggression and violence on dating apps and websites (Wolbers et al. 2022), and the introduction of the Online Dating Code of Conduct in October 2024 (Rishworth & Rowland 2024), major platforms implemented a number of safety features which may have contributed to this decrease in the prevalence of unsolicited sexually explicit messages being sent online. These include nudity protection features, clear community guidelines prohibiting the behaviour, and the removal of users who violated online safety policies.

Malware victimisation includes suspected malware (17.6% of respondents), pure ransomware victimisation where there are obvious signs the respondent's device had been compromised or access disrupted (3.2%), and ransomware-related data theft and extortion, which may or may not involve signs the device had been compromised (3.1%). From 2024 to 2025, there was an increase in the proportion of respondents who were a victim of pure ransomware (from 2.5% to 3.1%), which is consistent with an increase in the frequency of ransomware reports to the Australian Signals Directorate (2025) in the 2024–25 financial year.

Most identity crime and misuse involved financial accounts compromise, while a much smaller proportion of respondents experienced some other form of identity compromise. From 2024 to 2025, there was a reduction in identity crime and misuse (from 22.1% to 20.4%), which appears to be driven by a decline in the proportion of respondents who had their financial accounts compromised (17.7% in 2024 vs 15.8% in 2025). This may be in part due to actions banks have taken in recent years to harden their identity crime controls which have reduced the opportunities for criminals to compromise financial accounts. In contrast, there was an increase in other forms of identity compromise (4.8% in 2024 vs 5.7% in 2025) which may reflect cybercriminals moving from targeting financial accounts to other online accounts, such as utility and telecommunications accounts, online health service portals and government services.

The proportion of respondents reporting being a victim of online fraud and scams was higher in 2025 (11.1%) than in 2024 (9.7%). Consumer and seller scams related to buying and/or selling products and services online were the most common category of fraud and scams that respondents experienced in the 12 months prior to the survey (4.7%). Overall, these accounted for 37.7 percent of the most recent incidents of fraud and scams reported by victims. Online purchases are typically low value, high volume internet transactions, creating many opportunities for offenders to exploit anonymity, urgency and the verification requirements being simpler than those involved in more complex scams.

The prevalence of online abuse and harassment and identity crime and misuse was lower among 2025 respondents than in the 2024 survey. However, the proportion of respondents who reported being a victim of online fraud and scams was higher in 2025 than in 2024.

Sections of the community continue to be over-represented as victims.

Certain sections of the Australian community are more likely than others to be a victim of cybercrime. Victimisation rates are higher among respondents who are younger, who are First Nations, who are non-heterosexual, who mainly speak a language other than English, who have a restrictive health condition, who have a higher income, and who are small to medium business owners, operators and managers. Offenders may specifically target these groups that they perceive to be more lucrative, vulnerable or accessible.

From 2024 to 2025, changes in cybercrime victimisation were concentrated among respondents of certain ages and genders.

- Online abuse and harassment and malware victimisation decreased among respondents aged 35 to 64 years.
- Identity crime and misuse victimisation decreased among female respondents and respondents aged 35 years and over.
- Malware victimisation increased among respondents aged 18 to 24 years and 65 years and over.
- Fraud and scam victimisation increased among male respondents and respondents aged 25 to 49 years.

We observed no change in profit-motivated cybercrime affecting small to medium business owners, operators and managers.

Respondents who owned or operated a small to medium business were less likely to be a victim of online abuse and harassment in 2025 than they were in 2024.

The use of platforms associated with a higher risk of victimisation declined, but so did the use of online safety strategies.

There were declines in the daily or weekly use of platforms and online activities associated with a higher risk of victimisation. Lower proportions of respondents used subscription-based sexually explicit interactive adult platforms; made donations/payments over gaming, streaming or fundraising platforms; were active on romance/dating websites or apps; live streamed videos of themselves online; and purchased items from online marketplaces.

As in the 2024 survey, we found that many respondents were not taking simple but important steps to improve their online safety. While the use of protective behaviours declined between 2024 and 2025, some of this may reflect changes in technology use and design or be due to upstream interventions. For example, a decline in the proportion of respondents who checked or changed their privacy settings on social media could be related to a decline in the use of social media platforms more generally. The proportion of respondents installing or using antivirus software or firewalls on their devices also decreased, which may indicate that consumers are relying on protection built into new devices rather than installing additional software.

An observed decline in the proportion of respondents who said they avoided clicking on links and attachments from unknown senders may be related to government and private sector efforts to block scammers from reaching potential victims.

The uptake of many online safety strategies remained low, and the proportion of respondents who engaged in key protective behaviours declined from 2024 to 2025. There was, however, a reduction in the daily or weekly use of particular platforms and online activities associated with a higher risk of both online abuse and harassment and profit-motivated cybercrime victimisation.

Cybercrime remains significantly under-reported.

Across all cybercrime types, just over one in 10 victims made an official report to police or ReportCyber. Fraud and scam victims had the highest reporting rate (13.7%). When we compare this to the official reporting rates for common offline crime types, it is clear that cybercrime continues to be significantly under-reported.

From 2024 to 2025, the proportion of victims who made an official report to police or ReportCyber increased for identity crime and misuse victims and decreased for malware victims. First Nations respondents and small to medium business owners, operators and managers were more likely to make an official report for all types of cybercrime. Most victims who made an official report did so to prevent the crime happening to them again or to someone else; however, over a third of identity crime and misuse victims (37.6%) and nearly half of fraud and scam victims (45.3%) who made a report did so because they wanted to get their money back or be compensated for loss or damage.

The most common reasons that victims did not make an official report to police or ReportCyber were that they did not think the incident was serious enough, they were worried about the reaction to or consequences of reporting, or they had a poor understanding, perception or past experience of reporting. This has been consistent over the last several years of the Cybercrime in Australia series. Victims continue to be reluctant to ask for help, feel they will not be believed and fear legal processes. Many victims still do not know that reporting to the police or ReportCyber is an option, do not think the police or ReportCyber can help, or do not know how or where to report the matter. Building knowledge of and trust in reporting systems, and reducing the stigma of victimisation, are important areas for improvement.

From 2024 to 2025, the proportion of victims who made an official report to police or ReportCyber increased for identity crime and misuse and decreased for malware. It did not change for online abuse and harassment or fraud and scams.

Individual victims most commonly reported health and social harms, and small businesses reported increases in harm to their business.

Most victims did not lose money in the most recent cybercrime incident. The proportion of victims reporting financial losses was highest among fraud and scam victims (36.0%) and identity crime and misuse victims (29.6%). The average proportion of money lost that was recovered ranged from 30.7 percent for fraud and scams to 67.1 percent for identity crime and misuse. There was an increase in the proportion of malware victims who said they recovered at least some of the money they lost following their most recent incident (51.8% in 2024 vs 68.5% in 2025). After recoveries, most victims lost less than $1,000 in the most recent incident. Only 4.2 percent of online abuse and harassment victims, 4.3 percent of fraud and scam victims, 3.8 percent of identity crime victims and 2.4 percent of malware victims lost more than $10,000.

Victims experienced a range of harms associated with cybercrime victimisation, with 58.8 percent of cybercrime victims harmed in some way. This means an estimated 26.4 percent of all respondents were negatively affected by cybercrime in the 12 months prior to the survey. Forty percent of victims reported practical impacts, 26.1 percent reported social impacts, 19.5 percent reported health-related harms, 17.1 percent reported financial problems, and 2.4 percent had legal issues.

An estimated 25.0 percent of all small to medium business owners, operators or managers who responded to the survey (47% of whom were victims) said cybercrime had impacted their business in some way in the last 12 months. These impacts include disruption to everyday business function (28.7%), additional business expenses (16.4%), harm to their reputation or revenue (14.1%), loss of information (15.9%), effects on staff (10.0%) and legal or regulatory ramifications (7.9%). The proportion of victims who owned, operated or managed a small to medium business who reported impacts on their staff increased (5.9% in 2024 vs 10.0% in 2025), as did the proportion who experienced legal or regulatory issues (5.1% in 2024 vs 7.9% in 2025). The increase in impacts on staff appears to be driven by growth in the proportion who said employees or owners of the business resigned or lost their job, while the increase in legal or regulatory issues appears driven by an increase in victims who experienced litigation or legal action against their business.

Cybercrime victims who owned, operated or managed a small to medium business in the 2025 survey were more likely than their 2024 counterparts to say that their business was affected by staff impacts and legal or regulatory issues.

Introduction

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

This report offers unique insights into the experience of cybercrime among Australian individuals and small to medium businesses. This includes:

- the prevalence of cybercrime victimisation among a community sample, including poly-victimisation (experiencing multiple types of cybercrime);
- the resilience of Australian computer users to cybercrime, including the use of online safety strategies and engagement in high-risk activities;
- the 'dark figure' of unreported cybercrime that does not appear in the official statistics, and who is more likely to report to police; and
- the impact of cybercrime victimisation, including financial consequences and—more importantly—a range of other harms to individuals and to businesses.

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

Box 1: What is covered by this report?

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

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

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

Method

Detailed information about the survey design and sample characteristics, as well as the approach to recruitment, sampling and weighting of data, is provided in the *Appendix*.

Survey design

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

The questionnaire was developed by the Australian Institute of Criminology (AIC). It includes several components. First, the core survey questionnaire includes questions about respondent demographics, risk factors for victimisation, use of technology and devices, experiences of cybercrime victimisation and repeat victimisation, reporting behaviour and experiences, perpetrators of cybercrime, harms resulting from victimisation and preventative measures. Second, the survey includes more focused modules with questions designed to collect information on contemporary topics of national significance. These topics usually change each year and are completed by a sub-sample of respondents. Third, respondents to the ACS may be recruited to participate in online qualitative interviews, which collect detailed information about people's experiences of cybercrime. Fourth, some respondents are recruited into a longitudinal sample and will go on to repeat the survey in future years.

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

Recruitment, sampling and weighting

The survey was conducted by Roy Morgan between 27 May and 1 July 2025 using its Single Source panel and panels managed by PureProfile, Dynata and Octopus. The survey was sent to members of these online panels aged 18 years and over who had voluntarily joined the panel to receive incentives in exchange for completing surveys.

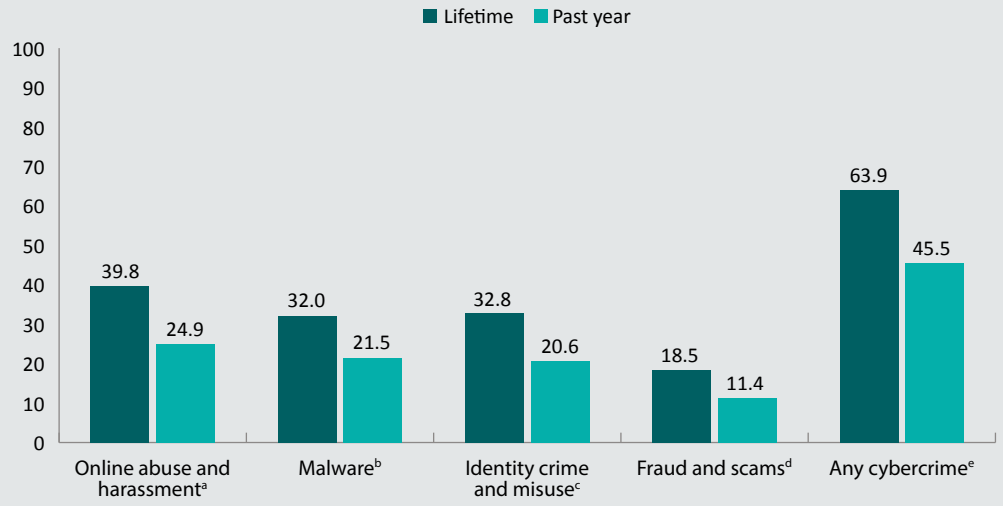
Proportional quota sampling, a non-probability sampling method, was used to ensure the sample was broadly reflective of the spread of people living in Australia. Quotas were based on the Australian adult population stratified by age, gender and usual place of residence, derived from Australian Bureau of Statistics (ABS) population data (ABS 2026). The data were subsequently weighted by age and usual place of residence to ensure they were representative of the spread of the Australian population. Additional random iterative method weights (calculated from Roy Morgan's Single Source survey) were applied to correct for education level, internet use and social media use. This corrected for oversampling of people with higher levels of education and more frequent internet use, which is common among online panels. All of the findings presented in this report are based on weighted data. The final sample size was 10,593 respondents.

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

Victimisation

Nearly two-thirds of respondents had been a victim of some type of cybercrime in their lifetime (*n*=6,768, 63.9%), and nearly half had been the victim of a cybercrime in the 12 months prior to the survey (*n*=4,822, 45.5%; Figure 1). In the 12 months prior to the survey, nearly a quarter of all respondents had been the victim of online abuse and harassment (*n*=2,642, 24.9%), over one in five respondents had been a victim of malware (*n*=2,282, 21.5%) or identity crime and misuse (*n*=2,185, 20.6%), and over one in 10 respondents were the victim of an online fraud or scam (*n*=1,206, 11.4%).

Figure 1: Prevalence of cybercrime victimisation, lifetime and past year (%) (*n*=10,593)



a: 465 respondents did not know or declined to answer the question about lifetime prevalence; 651 respondents did not know or declined to answer the question about past-year prevalence

b: 743 respondents did not know or declined to answer the question about lifetime prevalence; 929 respondents did not know or declined to answer the question about past-year prevalence

c: 562 respondents did not know or declined to answer the question about lifetime prevalence; 693 respondents did not know or declined to answer the question about past-year prevalence

d: 385 respondents did not know or declined to answer the question about lifetime prevalence; 452 respondents did not know or declined to answer the question about past-year prevalence

e: 574 respondents did not know or declined to answer the question about lifetime prevalence; 987 respondents did not know or declined to answer the question about past-year prevalence

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

Source: Australian Cybercrime Survey 2025 [weighted data]

Online abuse and harassment

Respondents were asked about a range of harmful online behaviours that an individual may experience while interacting with others when using the internet, their personal devices or other technology (Table 1). 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 incidents occurring over an extended period of time.

The most common forms of online abuse and harassment that respondents said they had experienced in the 12 months prior to the survey were someone impersonating them online (7.1% of respondents); being sent unsolicited sexually explicit messages, images or videos (6.3%); extortion or harassment involving images or videos (6.1%); and cyberbullying (5.9%). Four percent of respondents said they had experienced some form of controlling or restricting behaviour relating to their online activity; 3.1 percent of respondents said someone had subjected them to hate speech or made derogatory, malicious or threatening comments directly to them based on their religion, ethnicity, gender, sexuality or ideology; 2.9 percent said someone had shared or used their personal information without consent; and 2.5 percent of respondents said someone had used technology to stalk or harass them online.

More than one-third of victims of online abuse and harassment—9.0 percent of all respondents—said that they had been a victim of more than one type of online abuse and harassment measured as part of the survey.

Table 1: Incidents of online abuse and harassment (%)

	Past-year prevalence (*n*=10,593)	Most recent incident (*n*=2,589)
Impersonation	**7.1**	**20.6**
Someone hacked into respondent's social media or network account (including communicating with their contacts or posting messages or status updates from their accounts)	4.1	11.0
Someone set up fake social media or networking profiles pretending to be respondent (eg and communicated with their contacts or posted messages or status updates from their accounts)	3.3	9.0
Someone created fake videos or photos of respondent (eg 'deep fakes')	0.5	0.6
Unsolicited sexual content	**6.3**	**19.2**
Respondent was sent unsolicited sexually explicit messages, images or videos	6.3	19.2

Table 1: Incidents of online abuse and harassment (%) (cont.)		
	Past-year prevalence (*n*=10,593)	Most recent incident (*n*=2,589)
Extortion or harassment involving images or videos	**6.1**	**16.6**
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	3.3	9.0
Someone used coercion, blackmail or demands to try and get respondent to send them sensitive, personal or compromising photos, video or information that was stored online, on a digital device or sent in messages	1.7	3.5
Someone sent or posted photos and videos of respondent to others to try and embarrass, hurt or blackmail them	1.1	2.0
Someone shared or published sensitive, personal, compromising or intimate photos or videos of respondent without their consent	0.9	2.1
Cyberbullying	**5.9**	**15.0**
Someone sent or posted mean or hurtful messages via electronic communication (eg emails, social media or text messages) that made respondent feel hurt, embarrassed or unsafe	4.4	10.3
Someone spread rumours about respondent via electronic communication (eg emails, social media or text messages)	2.4	4.7
Controlling and restricting	**4.0**	**9.0**
Someone restricted respondent's access to online resources (eg social media, electronic legal documents, banking and utility accounts, etc)	1.9	3.7
Someone monitored respondent's activity online or on their phone (including installing spyware, going through their private messages, etc)	1.6	3.0
Someone tried to stop respondent from communicating with others online or over their mobile	1.4	2.3
Hate speech	**3.1**	**6.8**
Someone subjected respondent to hate speech or made derogatory, malicious or threatening comments directly to respondent based on their religion, ethnicity, gender, sexuality or ideology	3.1	6.8
Sharing without consent	**2.9**	**5.9**
Someone stole respondent's online personal information (including photos and videos) and used it without their permission	1.8	3.9
Someone published identifying information (such as respondent's full name, contact number, address, school etc) with malicious intent (ie doxxing)	1.3	2.0
Stalking and harassing	**2.5**	**6.0**
Someone used technology to stalk or repeatedly harass respondent, including being contacted by someone they had blocked or asked to not contact them	2.5	6.0

Table 1: Incidents of online abuse and harassment (%) (cont.)		
	Past-year prevalence (*n*=10,593)	Most recent incident (*n*=2,589)
Respondent fell victim to some other type of online abuse and harassment, not specified above	**0.3**	**1.0**
At least one of the above	**24.9**	**–**
More than one type of online abuse and harassment	**9.0**	**–**
None of the above	**75.1**	**–**
Unknown	**6.2[a]**	**2.0[b]**

a: Includes 651 respondents who did not know or declined to answer the question about past-year prevalence

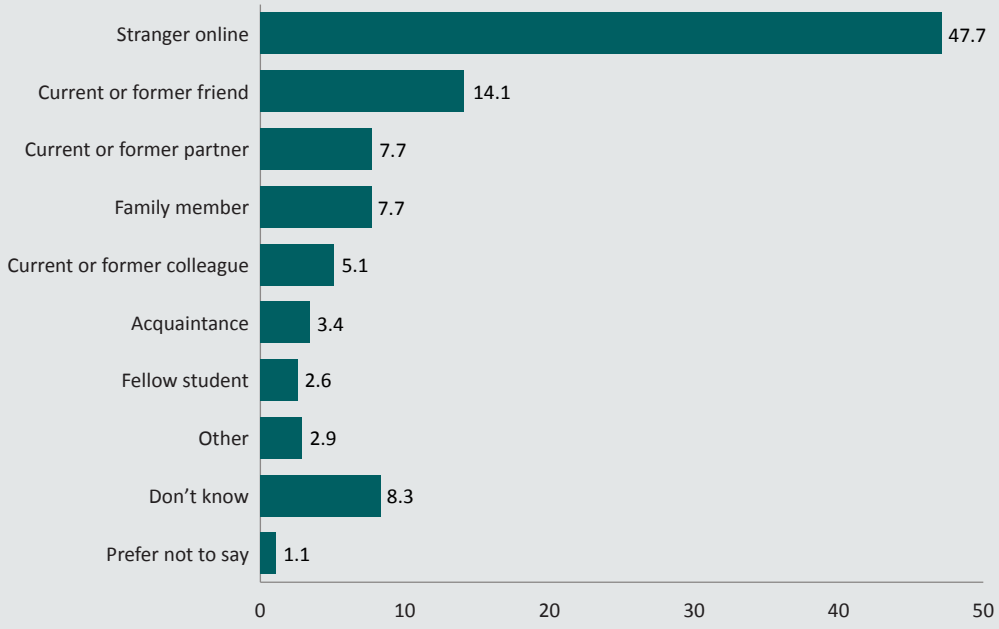
b: Includes 53 respondents who answered the question about past-year prevalence but did not know or declined to answer the question about the most recent incident

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

Source: Australian Cybercrime Survey 2025 [weighted data]

Past-year victims of online abuse and harassment were asked about their relationship to the offender in the most recent incident (Figure 2). Nearly half of the incidents involved a stranger online (47.1%). Fifteen percent of the most recent incidents of online abuse and harassment were domestic or family violence related, meaning they involved a current or former intimate partner (7.7%) or a family member (7.7%). The victim did not know who the perpetrator was in 8.3 percent of incidents.

Figure 2: Relationship between victim and offender in the most recent online abuse and harassment incident (%) (*n*=2,589)



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

Source: Australian Cybercrime Survey 2025 [weighted data]

Box 2: Technology-enabled family and domestic abuse

As with previous cybercrime surveys (Voce & Morgan 2025a, 2023a), online abuse and harassment was most often perpetrated by strangers online (47.1% of victims). This is likely because strangers are more often involved in the most common forms of online abuse and harassment, such as impersonating victims (47.4% strangers), sending unsolicited sexual images and videos (61.0% strangers) and extortion or harassment involving images and videos (43.4% strangers).

The overall prevalence of perpetration by current or former intimate partners or family members (15.4% of victims) and other people known to the victim who were not a partner or family member (25.2% of victims) was lower. But certain forms of online abuse and harassment were much more likely to have involved a known person. Stalking and harassment is commonly perpetrated by current or former intimate partners or family members (32.6%) and other people known to the victim (35.1%). Controlling and restricting behaviours also commonly involve current or former intimate partners or family members (25.3%) and others known to the victim (33.3%).

While these forms of technology-facilitated abuse may be less common than those typically perpetrated by strangers online, they can be incredibly harmful and often occur as part of an ongoing pattern (Boxall & Morgan 2021). For example, stalking and harassment had the highest harm score out of 17 forms of cybercrime in an index based on 34 items measuring the practical, health, social, financial and legal impacts of victimisation. Victims may face greater barriers to ending abuse when the perpetrator is someone they know in person, compared to a stranger they can block or disengage from online.

Overall, we found that 3.8 percent of respondents reported having experienced some form of technology-enabled family or domestic online abuse and harassment in the 12 months prior to the survey.

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 2).

We distinguish between suspected malware, which was reported by 17.6 percent of respondents, and ransomware victimisation. The latter includes pure ransomware—where there are obvious signs of the respondent's device having been compromised or access disrupted (3.2% of respondents)—and ransomware-related data theft and extortion, which may or may not involve signs the device had been compromised (3.1% of respondents).

Overall, in the 12 months prior to the survey, 5.8 percent of respondents received a ransom message on their device demanding payment.

The most common symptom of suspected malware that victims experienced in the past year were ads starting to pop up everywhere on their device (5.0% of respondents), their device slowing down and acting strangely (4.7% of respondents) and people telling them that they had been sending suspicious messages and links over social media or email (2.8% of respondents).

Table 2: Incidents of malware (%)

	Past-year prevalence (*n*=10,593)	Most recent incident (*n*=2,282)
Suspected malware	**17.6**	**71.2**
Popup ads started popping up everywhere	5.0	17.5
Respondent's device slowed down and acted strangely	4.7	14.6
People respondent knew told them they had been sending suspicious messages and links over social media or email	2.8	10.2
Respondent's devices kept crashing for some reason	2.5	6.7
Respondent's browser kept getting redirected when they tried to search for a familiar site	2.0	6.3
Programs were opening and closing automatically	1.5	3.6
There was a lack of storage space that respondent couldn't explain	2.3	7.3
Respondent's device was working excessively while no programs were running	1.8	5.0
Respondent's files had gone missing or been replaced with odd file extensions and the icons for the files were blank	1.2	2.8
Previously accessible system tools (such as personalised or security settings) were disabled	1.0	2.6
Pure ransomware	**3.2**	**10.1**
Respondent's devices, servers, service or networks were disrupted (eg slowed down, lost connection, had outages) and they received instructions for paying a ransom to restore functionality	1.9	5.6
Respondent's systems, devices or files had a virus or were inaccessible (eg locked or unreadable) and they received instructions for paying a ransom to restore access	1.4	4.5
Ransomware-related data theft and extortion	**3.1**	**11.7**
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	3.1	11.7

Table 2: Incidents of malware (%) (cont.)		
	Past-year prevalence (*n*=10,593)	Most recent incident (*n*=2,282)
Respondent fell victim to some other type of malware, not specified above	**0.4**	**1.6**
At least one of the above	**21.5**	**–**
More than one type of malware	**6.1**	**–**
None of the above	**78.5**	**–**
Unknown	**8.8[a]**	**1.1[b]**

a: Includes 929 respondents who did not know or declined to answer the question about past-year prevalence

b: Includes 25 respondents who answered the question about past-year prevalence but did not know or declined to answer the question about the most recent incident

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

Source: Australian Cybercrime Survey 2025 [weighted data]

Identity crime and misuse

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

Overall, 16.0 percent of respondents said that in the past year they had experienced some sort of compromise of their financial accounts, which accounted for just under three-quarters (72.8%) of the most recent incidents reported by identity crime and misuse victims (Table 3). A much smaller proportion of respondents (5.9%) said they had been a victim of some other form of identity compromise. This included incidents such as a respondent having their identity stolen to apply for government benefits, a job, utility services or medical services, or being impersonated to extort their online contacts. These are the more harmful forms of identity crime and misuse (Voce & Morgan 2025b).

In terms of the specific incidents, suspicious transactions appearing in the respondent's bank statements or accounts, credit card or credit report (9.3% of respondents) was the most common type of identity crime and misuse, followed by receiving calls about unpaid bills the respondent did not recognise (3.5% of respondents).

Table 3: Incidents of identity crime and misuse (%)		
	Past-year prevalence (*n*=10,593)	Most recent incident (*n*=2,185)
Compromise of financial accounts	**16.0**	**72.8**
Suspicious transactions appeared in respondent's bank statements or accounts, credit card or credit report	9.3	40.8
Respondent received calls from debt collectors asking about unpaid bills they did not recognise	3.5	14.4
Someone used respondent's details to purchase or order something or they received unfamiliar bills, invoices or receipts	2.6	8.4
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	1.3	3.9
Respondent was unsuccessful in applying for credit, and this was surprising given their credit history	0.8	2.6
Someone tried to obtain money from one of respondent's investments or superannuation accounts using their personal information	0.8	2.7
Other identity compromise	5.9	25.1
Someone used respondent's personal details (including images) to create an impersonation account to extort their contacts	1.5	5.5
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	1.2	4.4
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	0.9	3.0
Someone gained access to respondent's cryptocurrency wallet or exchange account and made transactions or stole currency	0.7	2.2
Someone used respondent's personal details to fraudulently apply for government benefits	0.7	2.4
Someone used respondent's personal details to create a fake cryptocurrency wallet or exchange account	0.6	2.1
Someone used respondent's personal details to attempt to apply for a job or rent a property	0.6	1.9
Respondent was unable to file taxes because someone had already filed a tax return in their name	0.6	2.0
Someone used respondent's personal details to attempt to give false info to police	0.5	1.6

Table 3: Incidents of identity crime and misuse (%) (cont.)		
	Past-year prevalence (*n*=10,593)	Most recent incident (*n*=2,185)
Respondent fell victim to some other type of identity crime and misuse, not specified above	**0.5**	**2.3**
At least one of the above	**20.6**	**–**
More than one type of identity crime and misuse	**3.8**	**–**
None of the above	**79.4**	**–**
Unknown	**6.5[a]**	**0.8[b]**

a: Includes 693 respondents who did not know or declined to answer the question about past-year prevalence

b: Includes 18 respondents who answered the question about past-year prevalence but did not know or declined to answer the question about the most recent incident

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

Source: Australian Cybercrime Survey 2025 [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 form of ICT. To have been counted as a victim of a fraud or scam, in most cases the respondent must have paid money or provided sensitive information to the offender. The subcategories used in this section align with the typology developed by the National Anti-Scam Centre.

The most common types of fraud and scams respondents experienced in the 12 months prior to the survey were all related to buying and/or selling products and services online, reported by 4.7 percent of respondents (Table 4). This most often included paying money or providing sensitive information when they were trying to buy a product or service from a fake or fraudulent seller online (2.2% of respondents) and paying money for health products, medicines or drugs from an online pharmacy which never arrived or were counterfeit (0.7%). Overall, these consumer scams accounted for 37.7 percent of the most recent incidents of fraud and scams reported by victims. Other common fraud and scam types included investment scams (1.6% of respondents) and phishing scams (1.6% of respondents).

Table 4: Incidents of fraud and scams (%)		
	Past-year prevalence (*n*=10,593)	Most recent incident (*n*=1,206)
Consumer and seller scams	**4.7**	**37.7**
Respondent paid money or provided sensitive information when trying to buy a product or service from a fake or fraudulent seller online	2.2	17.5
Respondent paid money for health products, medicines or drugs from an online pharmacy and the products never arrived or were counterfeit	0.7	5.0
Respondent paid a fake invoice or bill for some other product or service that they did not receive	0.6	4.0
Respondent sent money to a scammer posing as a known business supplier, service institution or company telling them that their banking details had changed	0.6	4.5
Respondent paid money or provided sensitive information when trying to sell a product or service to a fake or fraudulent buyer online	0.5	3.8
Respondent paid a fake invoice for directory listings, advertising, domain name renewals or office supplies	0.5	2.9
Investment scams	**1.6**	**12.1**
Respondent lost cryptocurrency in an exit scam or 'rug-pull', where cryptocurrency developers or promoters abandon a project and disappear with investors' funds	0.4	3.2
Respondent paid money or provided sensitive information to a scammer to buy into an illegitimate investment, trading or shares scheme or to get early access to their super fund	0.4	3.1
Respondent lost money or provided sensitive information in another kind of cryptocurrency scam	0.3	2.2
Respondent lost cryptocurrency to a scammer in a pretend 'giveaway', business opportunity or investment opportunity	0.3	2.2
Respondent paid money or provided sensitive information to some other fraudulent scheme related to their super fund	0.3	1.4
Phishing scams	**1.6**	**10.9**
Respondent paid money or provided sensitive information to a scammer pretending to be from a known service institution or company (bank, internet provider, post office, etc)	0.7	5.2
Respondent paid money or provided sensitive information to a scammer pretending to be someone they personally know, such as a family member, friend or work associate	0.4	2.9
Respondent paid money or provided sensitive information to someone pretending to be a bank, government or law enforcement official for things like a speeding fine, tax office debt, or immigration or visa issue	0.3	1.7
Respondent paid money or provided sensitive information to someone pretending to be a bank, government or law enforcement official for some other fine, bill or debt	0.2	1.1

Table 4: Incidents of fraud and scams (%) (cont.)		
	Past-year prevalence (*n*=10,593)	Most recent incident (*n*=1,206)
Unexpected money scams	**1.3**	**8.1**
Respondent paid money or provided sensitive information to a scammer offering them the false promise of an inheritance or share in a large sum of money in exchange for assistance	0.4	2.1
Respondent paid money or provided sensitive information to a scammer offering the false promise of prize money or a holiday package	0.4	1.6
Respondent paid money or provided sensitive information to a scammer falsely offering a rebate from the government, a bank or trusted organisation	0.4	2.7
Respondent paid money or provided sensitive information to a scammer falsely offering some other benefit or payment from the government, a bank or trusted organisation	0.3	1.7
Remote access scams	**1.2**	**8.1**
Respondent allowed someone pretending to be from a telecommunications or computer company to remotely access their computer, or paid them money or provided sensitive information	0.7	5.4
Respondent allowed some other kind of scammer to remotely access their computer	0.5	2.7
Job and employment scams	**0.5**	**3.0**
Respondent lost money or provided sensitive information to a scammer offering a job or employment	0.5	3.0
Romance scams	**0.5**	**3.2**
Respondent paid money, provided sensitive information or sent intimate images or videos to a scammer pretending to be a potential romantic partner	0.5	3.2
Money recovery scam	**0.5**	**3.1**
Respondent paid money or provided sensitive information to a scammer who was offering to help them recover from a previous scam	0.5	3.1
Donation scams	**0.4**	**1.9**
Respondent paid money or provided sensitive information to a scammer pretending to be a charity or disaster relief effort	0.4	1.9

Table 4: Incidents of fraud and scams (%) (cont.)		
	Past-year prevalence (*n*=10,593)	Most recent incident (*n*=1,206)
Other scams	**1.7**	**12.0**
Respondent lost money buying sports betting prediction software, or becoming a member of a sport betting syndicate or investment scheme, because these schemes did not work as advertised	0.5	3.2
Respondent paid for extremely high call or text rates when replying to unsolicited SMS competitions	0.2	1.6
Respondent sent money or provided sensitive information to some other kind of scammer who gave them fraudulent bank or payment details	0.3	2.2
Respondent fell victim to some other type of online scam or fraud, not already specified	0.5	5.0
At least one of the above	**11.4**	**–**
More than one type of fraud or scam	**0.2**	**–**
None of the above	**88.6**	**–**
Unknown	**4.3**[a]	**0.8**[b]

a: Includes 452 respondents who did not know or declined to answer the question about past-year prevalence

b: Includes 9 respondents who answered the question about past-year prevalence but did not know or declined to answer the question about the most recent incident

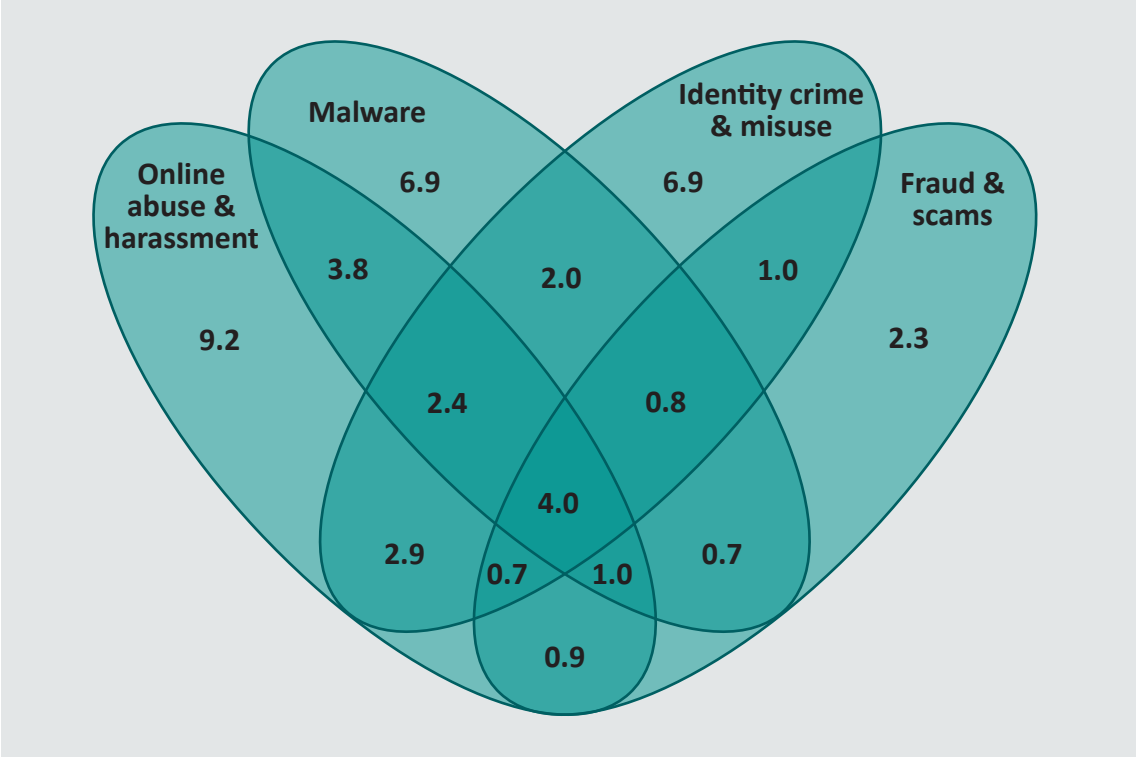
Note: Weighted percentages may not add to total due to rounding. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2025 [weighted data]

Poly-victimisation

It was common for cybercrime victims to report having experienced multiple types of cybercrime in the 12 months prior to the survey (Figure 3). Victims of fraud and scams were the most likely to also be a victim of another cybercrime type (79.5%), while victims of online abuse and harassment were the least likely to also experience other types of cybercrime (63.0%). Overall, 25.4 percent of respondents were a victim of one type of cybercrime, while 20.2 percent of respondents (44.3% of all victims) were victims of two or more types of cybercrime in the 12 months prior to the survey. A small group of respondents—4.0 percent, or 8.8 percent of all victims—reported having experienced all four types of cybercrime measured by the survey in the 12 months prior to the survey.

Figure 3: Overlap of cybercrimes experienced by respondents (%) (*n*=10,593)



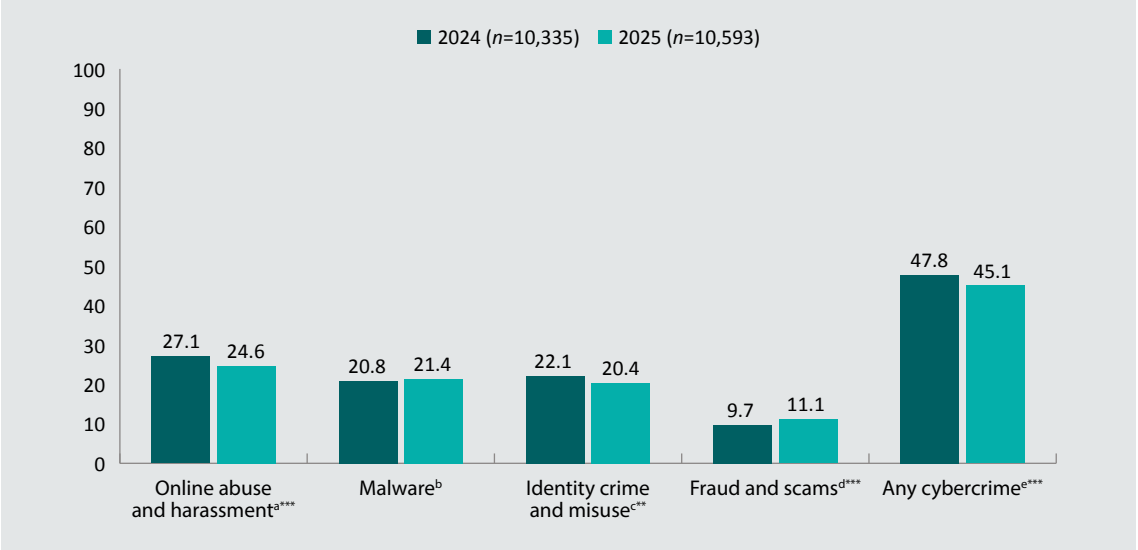
Note: Weighted percentages may not add to total due to rounding. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2025 [weighted data]

Changes in victimisation

We compared the prevalence of cybercrime among respondents to the 2024 and 2025 ACS, adjusting for differences between the two samples. Adjusted estimates of past-year victimisation for the four major categories of cybercrime are presented in Figure 4. This shows that, in 2025, smaller proportions of respondents reported being a victim of online abuse and harassment (27.1% in 2024 vs 24.6% in 2025, $F(39, 20{,}888)=31.69$, $p<0.001$), identity crime and misuse (22.1% vs 20.4%; $F(39, 20{,}888)=16.15$, $p<0.01$) and any cybercrime overall (47.8% vs 45.1%; $F(39, 20{,}888)=22.01$, $p<0.001$). In contrast, the proportion of respondents who reported being a victim of online fraud and scams was higher in 2025 (9.7% in 2024 vs 11.1% in 2025, $F(39, 20{,}888)=20.73$, $p<0.01$). There was no difference in the estimated likelihood of experiencing malware attacks.

Figure 4: Adjusted estimates of past-year victimisation for major categories of cybercrime, 2024 and 2025 (%)



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

Note: Predictive margins derived from separate logistic regression models for each cybercrime type that included controls for key sociodemographic, employment and technology use variables. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

a: In 2024, 672 respondents did not know or declined to answer the question about past-year prevalence. In 2025, 651 respondents did not know or declined to answer the question about past-year prevalence

b: In 2024, 879 respondents did not know or declined to answer the question about past-year prevalence. In 2025, 929 respondents did not know or declined to answer the question about past-year prevalence

c: In 2024, 618 respondents did not know or declined to answer the question about past-year prevalence. In 2025, 693 respondents did not know or declined to answer the question about past-year prevalence

d: In 2024, 447 respondents did not know or declined to answer the question about past-year prevalence. In 2025, 452 respondents did not know or declined to answer the question about past-year prevalence

e: In 2024, 919 respondents did not know or declined to answer the question about past-year prevalence. In 2025, 987 respondents did not know or declined to answer the question about past-year prevalence

Source: Australian Cybercrime Survey 2025 [weighted data]

We then repeated this analysis for the subcategories of cybercrime (Table 5). We note that some of this analysis is limited by the relatively small number of respondents who reported experiencing certain subcategories of online fraud and scams.

Compared to 2024, a smaller proportion of respondents in 2025 said they had received unsolicited sexual content (7.6% in 2024 vs 6.3% in 2025; $F(39, 20{,}888)=7.49$, $p<0.001$) and been impersonated online (7.8% in 2024 vs 6.9% in 2025; $F(39, 20{,}888)=11.74$, $p<0.05$). In 2025, a lower proportion of respondents said their financial accounts had been compromised (17.7% in 2024 vs 15.8% in 2025; $F(39, 20{,}888)=6.88$, $p<0.01$), while a higher proportion experienced other forms of identity compromise (4.8% vs 5.7%; $F(39, 20{,}888)=24.26$, $p<0.01$). A higher proportion of victims also said they experienced pure ransomware in 2025 (3.1%) compared to 2024 (2.5%; $F(39, 20{,}888)=13.79$, $p<0.01$).

Table 5: Adjusted estimates of past-year victimisation for subcategories of cybercrime, 2024 and 2025

	2024 (*n*=10,335)	2025 (*n*=10,593)
Online abuse and harassment		
Extortion or harassment involving images or videos	5.5	6.0
Impersonation	7.8	6.9*
Sharing content without consent	3.1	2.8
Stalking and harassing	2.9	2.5
Controlling and restricting behaviours	3.8	4.0
Hate speech	3.2	3.0
Cyberbullying	5.6	5.8
Unsolicited sexual content	7.6	6.3***
Malware attacks		
Pure ransomware	2.5	3.1**
Ransomware-related data theft and extortion	2.6	3.0
Other malware	17.3	17.5
Identity crime and misuse		
Compromise of financial accounts	17.7	15.8**
Other identity compromise	4.8	5.7**
Fraud and scams		
Consumer and seller scams	4.5	4.6
Phishing scams[a]	1.7	1.6
Investment scams[a]	1.5	1.7
Remote access scams[a]	1.1	1.2
Unexpected money scams[a]	1.3	1.4
Other scams[a,b]	1.6	1.8

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

a: For these types of scams Firth's penalised logistic regression was used. This technique corrects for bias in standard logistic regression with rare events. Employment, charity, romance and money recovery scams were excluded because the prevalence was too low for this analysis

b: Includes scams listed in the 'Other scams' category in Table 4: 'Respondent lost money buying sports betting prediction software, or becoming a member of a sport betting syndicate or investment scheme, because these schemes did not work as advertised', 'Respondent paid for extremely high call or text rates when replying to unsolicited SMS competitions', 'Respondent sent money or provided sensitive information to some other kind of scammer who gave them fraudulent bank or payment details' and 'Respondent fell victim to some other type of online scam or fraud, not already specified'

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

Source: Australian Cybercrime Survey 2025 [weighted data]

As shown in Table 5, in many categories of fraud and scams there were small increases that did not reach statistical significance, such as investment scams (1.5% vs 1.7%), remote access scams (1.1% vs 1.2%), unexpected money scams (1.3% vs 1.4%) and other scams (1.6% vs 1.8%). The number of victims was low in both years.

Box 3: Changes in ransomware, identity crime and misuse and online abuse and harassment

There are several possible explanations for the changes in cybercrime victimisation observed in this year's report.

For the second year running (Voce & Morgan 2025a) there was a decline in the proportion of respondents who received unsolicited sexual content. Following research that found very high rates of sexual aggression and violence over dating apps and websites (Wolbers et al. 2022), the Online Dating Code of Conduct was introduced in October 2024 to combat technology-facilitated abuse (Rishworth & Rowland 2024). Major platforms adopted this code and have since implemented a number of safety features which may have contributed to this decrease in the prevalence of unsolicited sexually explicit messages being sent online. These include nudity protection features which automatically blur photos that contain nudity (Instagram 2026), having clear community guidelines which prohibit the sending of unsolicited sexually explicit images/videos and classify it as sexual harassment (Bumble nd), and taking actions against users found to have violated the online safety policies (Rishworth & Rowland 2024).

The increase in the proportion of respondents experiencing pure ransomware from 2024 to 2025 is consistent with reports by the Australian Signals Directorate (2025) of an increase in the frequency of ransomware attacks in the 2024–25 financial year. According to the latest Annual cyber threat report, cybercriminals are using malware designed to covertly steal information from Australian victims and then launching subsequent attacks compromising corporate networks and accounts. In particular, the number of ransomware incidents against the healthcare sector doubled from the previous financial year.

This year, a lower proportion of respondents said their financial accounts had been compromised, while a higher proportion experienced other forms of identity compromise. This reduction in the compromise of financial accounts may be in part due to banks taking actions in recent years to harden their identity crime controls. For example, in November 2023 many Australian banks began introducing biometric checks for new individual customers opening accounts online, and limiting payments to high-risk channels such as some cryptocurrency platforms (Australian Banking Association 2023). Banks also expanded intelligence sharing across the sector, with a commitment to use intelligence provided by the Australian Financial Crimes Exchange (Australian Banking Association 2023). It is possible that actions such as these have reduced the opportunities for criminals to compromise financial accounts, meaning they have instead found other online accounts to target, such as utility and telecommunications accounts, online health service portals and government services.

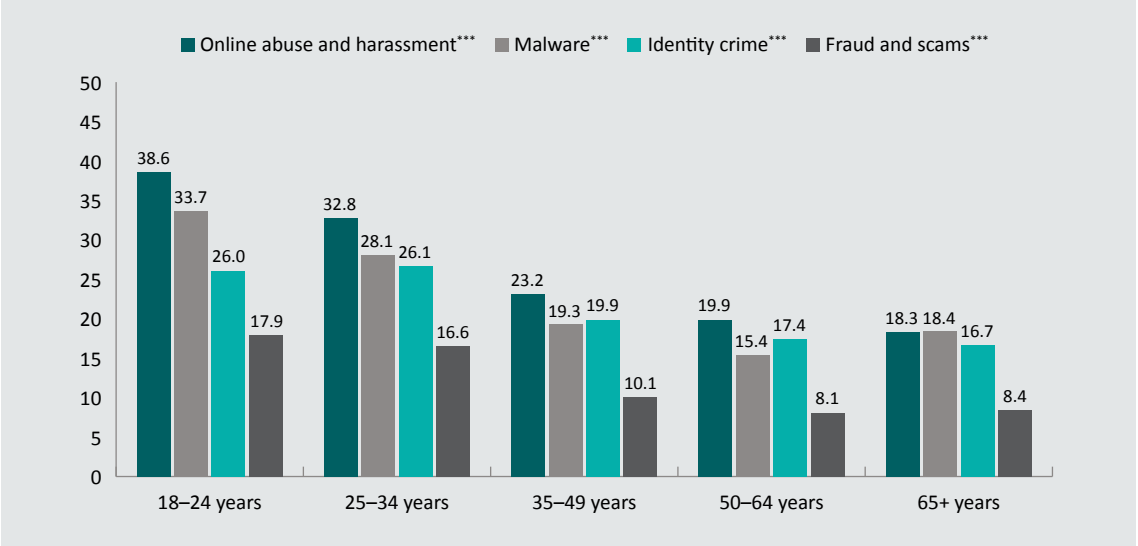
These are potential explanations for the changes we have observed this year. Further work is needed to better understand the changes in victimisation and the effectiveness of the measures described above.

There was no change in the proportion of respondents who were the victims of multiple types of cybercrime between 2024 (20.2%) and 2025 (19.9%, p=0.553). However, a smaller proportion of respondents in 2025 said their data was exposed in a third-party data breach (25.3% in 2024 vs 19.7% in 2025; F(39, 20,888)=14.81, p<0.001). It is important to note that data collection for this year's survey ended on 1 July 2025, which was just prior to a large-scale data breach which impacted 5.7 million customers (Qantas 2025). The true proportion of respondents whose data was exposed in a third-party data breach in 2025 is therefore likely higher than reported in the survey.

Victim characteristics

Younger respondents were consistently more likely to be cybercrime victims than their older counterparts (Figure 5). Respondents aged 18 to 24 were most often the victims of online abuse and harassment (38.6%), malware (33.7%) and fraud and scams (17.9%). Identity crime and misuse followed a similar pattern but was most common among respondents aged 25 to 34 (26.7%).

Figure 5: Cybercrime victimisation for major categories of cybercrime, by age group (%) (*n*=10,593)



***statistically significant at $p<0.001$

Note: Sample sizes of age groups are as follows: 18–24 years, *n*=1,206; 25–34 years, *n*=1,990; 35–49 years, *n*=2,714; 50–64 years, *n*=2,325; 65 years and over, *n*=2,359. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation. Weighted percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2025 [weighted data]

The prevalence of different cybercrimes according to respondent characteristics is presented in Table 6. Several of these findings are similar to those in *Cybercrime in Australia 2024* (Voce & Morgan 2025a), including higher rates of all cybercrime types among First Nations respondents, those who mainly spoke a language other than English and those with a restrictive health condition, and higher rates of online abuse and harassment and malware among men. Respondents who identified as lesbian, gay, bisexual or another non-heterosexual identity (LGB+) had higher rates of online abuse and harassment and fraud and scams, consistent with last year, while also reporting higher rates of malware victimisation.

Table 6: Cybercrime victimisation by crime type and sociodemographic characteristics (%) (*n*=10,593)

	Online abuse and harassment	Malware	Identity crime and misuse	Fraud and scams
Gender				
Female (*n*=5,439)	23.2***	20.3***	20.3	10.8
Male (*n*=5,102)	26.6	23.1	21.0	12.0
Non-binary (*n*=51)[a]	49.7	5.5	15.1	7.5
First Nations[b]				
Yes (*n*=436)	50.0***	46.4***	42.1***	32.2***
No (*n*=10,040)	23.8	20.5	19.7	10.5
LGB+[c]				
Yes (*n*=982)	39.5***	25.6**	22.3	14.5**
No (*n*=9,450)	23.5	21.2	20.6	11.1
Speaks a language other than English most often at home[d]				
Yes (*n*=620)	30.9***	27.7***	26.3***	17.9***
No (*n*=9,677)	24.6	21.2	20.2	11.0
Restrictive long-term health condition[e]				
Yes (*n*=1,140)	38.7***	33.6***	32.4***	23.0***
No (*n*=8,708)	22.9	19.7	18.9	9.6

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

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

b: Excludes 117 respondents who did not know or declined to answer the question

c: Excludes 161 respondents who did not know or declined to answer the question

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

e: Excludes 553 respondents who did not know or declined to answer the question

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

Source: Australian Cybercrime Survey 2025 [weighted data]

Box 4: Why is cybercrime more common among respondents with a disability or who speak a language other than English at home?

Consistent with previous years (Voce & Morgan 2025a, 2023a), respondents living with a disability and who mainly speak a language other than English are at higher risk of all forms of cybercrime. This could be for a range of reasons. Offenders may target groups that they perceive to be more vulnerable, less likely to report and more trusting of authority or service providers. For example, in recent years there has been an increase in scams targeting the Mandarin-speaking community, particularly students of Chinese background, where scammers pretend to be Chinese officials threatening arrest or deportation (Scamwatch nd; Victoria Police 2025). These individuals may be targeted for their unfamiliarity with Australian processes, insecurities about their visas and a tendency to comply with or be fearful of authorities (Stringer & Michailova 2019).

Individuals with a disability or who mainly speak a language other than English may experience communication and information barriers, such as difficulty verifying the legitimacy of emails and websites, particularly those which employ complex financial, legal or technical terminology to sound authoritative or intimidating.

Individuals with non-English-speaking backgrounds and disabilities might have difficulty accessing to up-to-date information on online safety and emerging threats and technologies (eSafety Commissioner 2020; Ngo 2024). It is important to have plain language and multi-language educational materials, which could be delivered through disability services, migrant skills programs and community organisations, tailored to an individual's online activity and needs.

This may be especially important for people with a disability, who might have a greater reliance on online services to access banking, shopping, social connection, health appointments and government services. They may also use assistive technologies that limit their ability to pick up on warning signs of suspicious websites or communications, such as screen readers not conveying visual indicators of phishing sites (Australian Human Rights Commission 2025).

Finally, people living with a disability and from non-English-speaking backgrounds in Australia tend to have high levels of social isolation and loneliness (Emerson et al. 2020; Lam 2022). This means that they are more susceptible to scams and may not have trusted people who they can get second opinions from when something seems suspicious (Nicholson, Coventry & Briggs 2019; Xing et al. 2020). It highlights the benefits of outreach services and proactive efforts to offer support and assistance to these groups.

Victimisation also varied according to respondents' employment status (Table 7). Like previous years (Voce & Morgan 2025a), 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 (37.1% vs 21.4%), malware (33.9% vs 17.6%), identity crime (31.5% vs 18.1%) and fraud and scams (21.4% vs 8.1%). 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 (20.7% vs 30.4%), a malware attack (16.9% vs 26.4%), identity crime and misuse (17.0% vs 25.7%) and fraud or scams (7.1% vs 15.2%). Respondents with incomes over $180,000 had higher rates of all types of cybercrime than other respondents, including online abuse and harassment (31.9%), malware (25.4%), identity crime (27.2%) and fraud and scams (15.9%). The higher the respondent's income, the more likely they were to report having been a victim of all types of cybercrime.

Table 7: Cybercrime victimisation by crime type and respondent education, employment and income (%) (*n*=10,593)

	Online abuse and harassment	Malware	Identity crime and misuse	Fraud and scams
Employment status[a]				
Employed (*n*=6,732)	27.2***	23.4***	22.9	12.6***
Unemployed (*n*=564)	28.6	20.0	16.5	12.6
Other (*n*=3,247)	19.4	17.9	16.8	8.6
Owns, operates or works for a small to medium enterprise (SME)[b]				
Owner or manager (*n*=1,447)	37.1***	33.9***	31.5***	21.4***
Employee (*n*=1,851)	30.2	25.6	24.8	14.2
Works but not at an SME (*n*=3,328)	21.4	17.6	18.1	8.1
Working but not an SME owner/manager (n=5,179)[c]	*24.5*	*20.4*	*20.5*	*10.3*
Owns, operates or works for a large company or business[d]				
Large company owner or executive (*n*=428)	26.9***	23.7***	23.3***	13.2***
Large company employee (*n*=1,927)	20.7	16.9	17.0	7.1
Works but not at a large company (*n*=4,224)	30.4	26.4	25.7	15.2

Table 7: Cybercrime victimisation by crime type and respondent education, employment and income (%) (*n*=10,593) (cont.)

	Online abuse and harassment	Malware	Identity crime and misuse	Fraud and scams
Annual income[e]				
$0 – $18,200 (*n*=963)	23.0**	19.7	16.8***	10.0***
$18,201 – $45,000 (*n*=2,309)	24.7	21.9	18.9	10.8
$45,001 – $120,000 (*n*=4,377)	25.4	22.6	21.7	11.5
$120,001 – $180,000 (*n*=1,397)	27.2	22.9	24.6	14.9
$180,001 and over (*n*=557)	31.9	25.4	27.2	15.9

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

a: Excludes 50 respondents who did not know or declined to answer the question

b: Excludes 107 respondents who did not know or declined to answer the question

c: Combines 'Employee' and 'Works but not at an SME' categories

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

e: Excludes 989 respondents who did not know or declined to answer the question

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

Source: Australian Cybercrime Survey 2025 [weighted data]

Changes in victimisation among select groups of respondents

Using a similar methodology to our analysis of victimisation among all respondents, we compared the rate of victimisation among 2025 and 2024 respondents according to age, gender and whether the respondent was a small to medium business owner, operator or manager (Table 8).

Online abuse and harassment victimisation was lower in 2025 than in 2024 among respondents aged 35 to 49 years (27.7% in 2024 vs 23.1% in 2025%; $F(35, 20{,}893)=9.69$, $p<0.001$), respondents aged 50 to 64 years (23.6% in 2024 vs 19.9% in 2025; $F(35, 20{,}893)=6.75$, $p<0.01$), and for both men (28.6% in 2024 vs 26.2% in 2025; $F(35, 20{,}891)=15.64$, $p<0.01$) and women (25.6% in 2024 vs 22.8% in 2025; $F(35, 20{,}891)=17.65$, $p<0.01$).

Malware victimisation was higher in 2025 than 2024 for respondents aged 18 to 24 years (27.4% in 2024 vs 32.7% in 2025; $F(35, 20{,}892)=3.92$, $p<0.05$) and respondents aged 65 years and over (15.8% in 2024 vs 18.4% in 2025; $F(35, 20{,}889)=1.94$, $p<0.05$), while it was lower among those in the middle, aged 35 to 49 years (21.9% in 2024 vs 19.3% in 2025; $F(35, 20{,}893)=6.70$, $p<0.05$) and 50 to 64 years (17.5% in 2024 vs 15.4% in 2025; $F(35, 20{,}893)=2.84$, $p<0.05$).

In 2025, identity crime and misuse victimisation was less common than it was in 2024 among women (21.8% in 2024 vs 20.0% in 2025), and respondents aged 35 and over—that is, respondents aged 35 to 49 years (22.6% in 2024 vs 20.1% in 2025; $F(35, 20{,}851)=6.05$, $p<0.05$), 50 to 64 years (20.7% in 2024 vs 17.2% in 2025; $F(35, 20{,}893)=2.97$, $p<0.01$) and 65 years and over (20.4% in 2024 vs 16.7% in 2025; $F(35, 20{,}892)=1.88$, $p<0.01$).

Finally, the prevalence of fraud and scams increased among respondents aged 25 to 34 years (13.1% in 2024 vs 15.7% in 2025; $F(34, 20{,}875)=8.74$, $p<0.05$) and 35 to 49 years (8.1% in 2024 vs 10.1% in 2025; $F(34, 20{,}867)=7.46$, $p<0.05$), and among men (9.8% in 2024 vs 11.9% in 2025; $F(37, 20{,}891)=13.01$, $p<0.01$).

Table 8: Adjusted estimates of past-year victimisation for major categories of cybercrime, by respondent age and gender, 2024 and 2025 (%)

	Online abuse and harassment		Malware		Identity crime and misuse		Fraud and scams	
	2024	2025	2024	2025	2024	2025	2024	2025
Age								
18–24	38.7	37.4	27.4	32.7*	24.7	25.6	15.5	17.6
25–34	31.7	31.5	25.6	26.8	24.5	25.5	13.1	15.7*
35–49	27.7	23.1***	21.9	19.3*	22.6	20.1*	8.1	10.1*
50–64	23.6	19.9**	17.5	15.4*	20.7	17.2**	7.5	8.0
65+	20.5	18.1	15.8	18.4*	20.4	16.7**	8.6	8.4
Gender[a]								
Female	25.6	22.8**	19.5	20.1	21.8	20.0*	9.6	10.5
Male	28.6	26.2**	22.0	22.9	22.4	20.8	9.8	11.9**

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

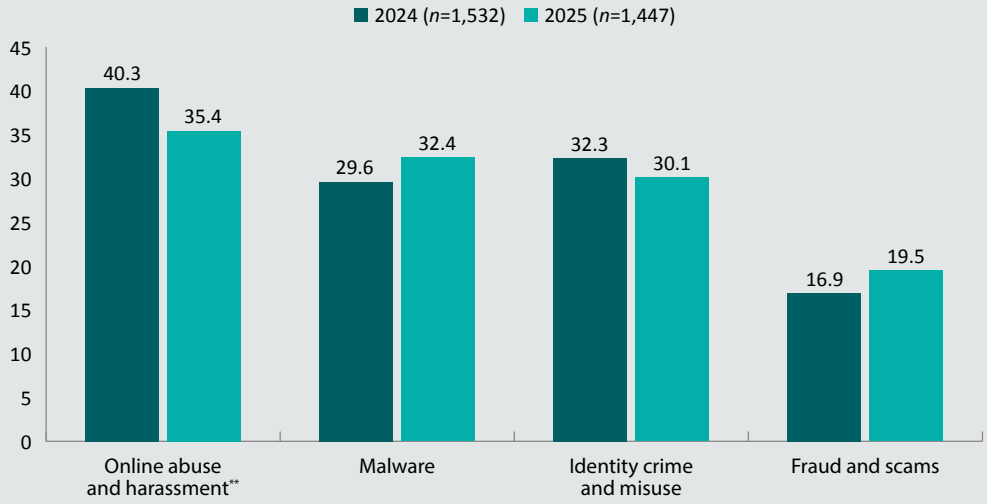
a: Non-binary respondents were excluded from multivariate analysis due to small sample size

Note: Predictive margins derived from separate logistic regression models for each cybercrime type and age group or gender that included controls for key sociodemographic, employment and technology use variables. For both 18–24 and 65+ age groups, a small number of cases were omitted from the model due to small cell sizes. This does not affect the validity of the overall finding. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2025 [weighted data]

There has been a significant focus on preventing cybercrime among small to medium business owners and operators, given their vulnerability to victimisation. The proportion of small to medium business owners who responded to the survey and who were a victim of online abuse and harassment was lower in 2025 (35.4%) than it was in 2024 (40.3%; $F(35, 20{,}893)=8.68$, $p<0.01$). The differences in the prevalence of malware, identity crime and misuse and fraud and scams were not statistically significant (Figure 6).

Figure 6: Adjusted estimates of past-year victimisation for major categories of cybercrime, small to medium business owners and operators, 2024 and 2025 (%)



**statistically significant at $p<0.01$

Note: Predictive margins derived from separate logistic regression models for each cybercrime type that included controls for key sociodemographic, employment and technology use variables. Model was restricted to small to medium enterprise owners, operators and managers. Respondents who did not know or declined to answer the question were included in the denominator when calculating the prevalence of victimisation

Source: Australian Cybercrime Survey 2025 [weighted data]

Use of online safety strategies

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

Digital literacy

Respondents were asked to estimate the amount of time they spent using the internet for personal use and, among those respondents who were working, the amount of time they spent using the internet on an average work day for work reasons. It has been shown that the longer a person spends using the internet for personal and work-related use, the more likely they are to be the victim of each form of cybercrime (Voce & Morgan 2023a). The average time spent online for personal activities increased from 3.44 hours in 2024 to 3.55 hours in 2025 ($F(40, 20{,}888)=76.75$, $p<0.01$), while there was no change in time spent online for work-related tasks (Table 9).

Table 9: Mean number of hours spent online for personal and work-related use, 2024 and 2025

	Mean hours, 2025	Adjusted estimates	
		2024	2025
Personal use[a]	3.56	3.44	3.55**
Work-related use[b]	4.16	4.14	4.16

**statistically significant at $p<0.01$

a: 2024 data exclude 1,517 respondents who did not know or declined to answer the question; 2025 data exclude 1,515 respondents who did not know or declined to answer the question

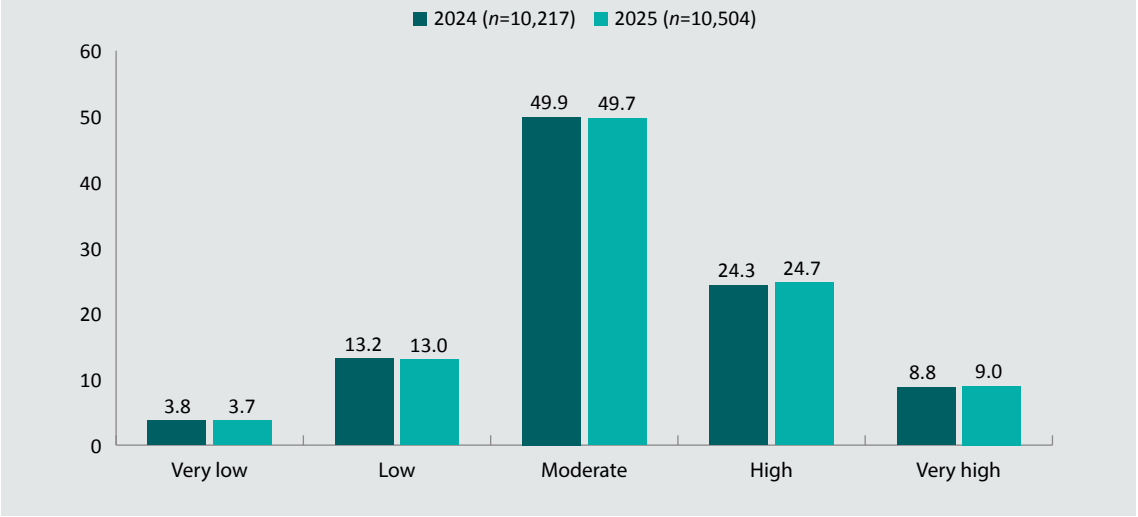
b: 2024 data exclude 3,629 respondents who did not indicate they were currently working and 1,249 who did not know or declined to answer the question. 2025 data exclude 3,860 respondents who did not indicate they were currently working and 1,278 who did not know or declined to answer the question

Note: Predictive margins derived from separate regression models for personal use and work-related use that included controls for key sociodemographic and employment variables. The outcome variable was the number of hours spent online

Source: Australian Cybercrime Survey 2025 [weighted data]

Respondents were asked to rate their knowledge of technology and their ability to use technology. There was no difference between 2024 and 2025 in respondents' self-rated knowledge of technology (Figure 7) or ability to use technology (Figure 8).

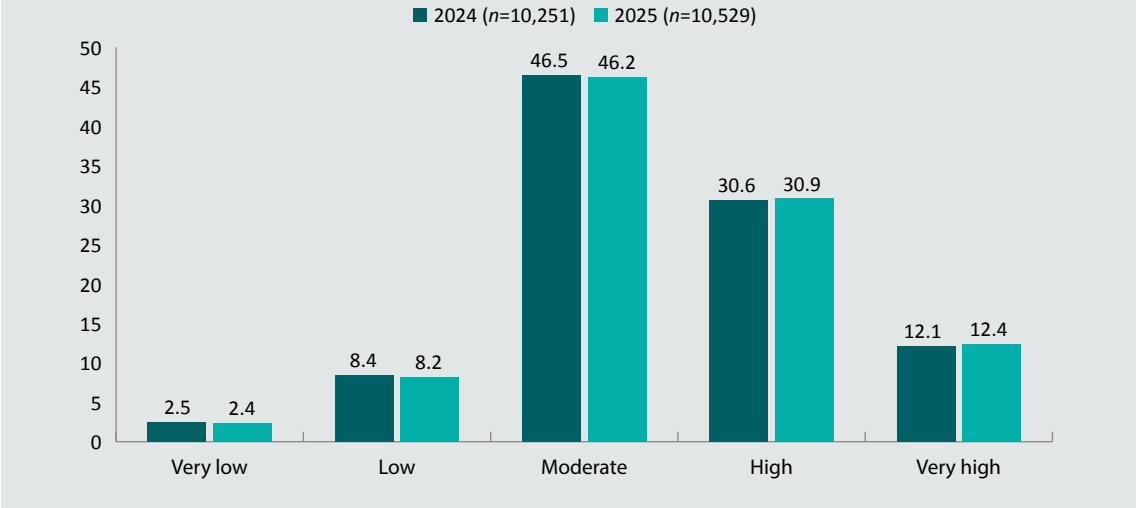
Figure 7: Self-rated knowledge of technology, 2024 and 2025 (%)



Note: To compare respondents in 2024 and 2025 we estimated a regression model that included controls for key sociodemographic, employment and technology use variables. The outcome variable was the rating of knowledge of technology, converted into a 5-point score. Excludes 118 respondents in 2024 and 89 respondents in 2025 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 2025 [weighted data]

Figure 8: Self-rated ability to use technology, 2024 and 2025 (%)



Note: To compare respondents in 2024 and 2025 we estimated a regression model that included controls for key sociodemographic, employment and technology use variables. The outcome variable was the rating of ability to use technology, converted into a 5-point score. Excludes 84 respondents in 2024 and 64 respondents in 2025 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 2025 [weighted data]

Frequent use—defined as daily or weekly use—of particular platforms or online activities has been associated with a higher risk of both online abuse and harassment and profit-motivated cybercrime victimisation (Voce & Morgan 2023a, 2023b). We compared the prevalence of frequent use of these platforms and activities in 2025 with results from the 2024 survey. As shown in Table 10, in 2025 there was a lower proportion of respondents who:

- used subscription-based sexually explicit interactive adult platforms (6.2% in 2024 vs 5.0% in 2025; $F(39, 20{,}888)=29.24$, $p<0.001$);
- made donations or payments over gaming, streaming or fundraising platforms (9.9% vs 8.4%; $F(39, 20{,}888)=30.56$, $p<0.001$);
- were active on romance/dating websites or apps (9.8% vs 8.4%; $F(39, 20{,}888)=40.12$, $p<0.01$);
- live streamed videos of themselves online (14.4% vs 12.8%; $F(39, 20{,}888)=40.12$, $p<0.01$); and
- purchased items from online marketplaces, excluding online store websites and apps (17.8% vs 16.3%; $F(39, 20{,}888)=34.16$, $p<0.01$)
- posted or responded to posts on social media (48.4% vs 45.9%; $F(39, 20{,}888)=44.23$, $p<0.001$);
- posted or responded to posts on online blogs, forums or interest groups (22.8% vs 21.8%; $F(39, 20{,}888)=42.11$, $p<0.05$); and
- accessed sexually explicit adult websites (18.2% vs 16.5%; $F(39, 20{,}888)=69.43$, $p<0.01$)

The decrease in using subscription-based sexually explicit interactive adult platforms, making donations or payments over gaming, streaming or fundraising platforms, and being active on romance/dating websites or apps, follows statistically significant increases in these activities in the previous year (Voce & Morgan 2025a).

Table 10: Daily or weekly engagement in online activities, 2024 and 2025 (%)

	Daily or weekly use in 2025	Adjusted estimates	
		2024	2025
Using subscription-based sexually explicit interactive adult platforms	5.1	6.2	5.0***
Making donations or payments over gaming, streaming or fundraising platforms	8.4	9.9	8.4***
Being active on romance/dating websites or apps	8.4	9.8	8.4**
Live streaming videos of myself online	13.0	14.4	12.8**
Purchasing items from online marketplaces (excluding online store websites and apps)	16.5	17.8	16.3**
Posting or responding to posts on social media	47.0	48.4	45.9***
Posting or responding to posts on online blogs, forums or interest groups	21.7	22.8	21.8*
Online banking and other online financial activities	83.7	82.4	83.2
Messaging and chatting online	74.4	72.5	73.3
Private video chatting over apps and platforms	36.6	36.6	36.3
Streaming videos on your computer, phone or TV	76.2	73.8	75.7**
Purchasing items from online store websites and apps (excluding classifieds and marketplaces)	25.9	26.3	25.7
Participating in online gaming/sports	21.8	21.6	21.6
Accessing sexually explicit adult websites	16.4	18.2	16.5**
Live streaming videos of content creators, influencers or gamers online	23.1	23.8	22.8
Browsing or looking for information	92.0	91.4	91.7
Sending emails	82.6	82.5	82.2
Reading news articles online	73.7	74.1	73.3

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

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

Source: Australian Cybercrime Survey 2025 [weighted data]

Online safety strategies

Respondents were asked whether they had used various online safety measures or engaged in various unsafe behaviours in the 12 months prior to the survey (Tables 11 and 12). While a higher proportion of survey respondents used a secure password manager in 2025 than in 2024 (25.0% in 2024 vs 27.4% in 2025, $F(39, 20{,}888)=18.96$, $p<0.001$), there were fewer respondents in 2025 who:

- checked their privacy settings on social media accounts (38.5% in 2024 vs 36.6% in 2025, $F(39, 20{,}888)=38.10$, $p<0.01$);
- purchased or continued to have cyber insurance (4.6% vs 3.7%, $F(39, 20{,}888)=9.82$, $p<0.01$);
- installed or used spam-filtering software (20.5% vs 17.8%, $F(39, 20{,}888)=23.75$, $p<0.001$);
- installed or used antivirus software or firewalls on their devices (39.3% vs 36.2%, $F(39, 20{,}888)=46.95$, $p<0.001$);
- used password protection on their router (24.5% vs 22.9%, $F(39, 20{,}888)=22.53$, $p<0.05$);
- used different passwords for secure online accounts, especially for banking or financial transactions (50.9% vs 47.7%, $F(39, 20{,}888)=35.24$, $p<0.001$);
- changed their privacy settings on social media accounts from the default to a more restrictive setting (32.2% vs 30.0%, $F(39, 20{,}888)=31.83$, $p<0.01$); and
- avoided clicking on links or attachments when they were not certain who the sender of a text message or email was (67.1% vs 64.8%, $F(39, 20{,}888)=50.69$, $p<0.01$).

Table 11: Prevalence of online safety measures, 2024 and 2025 (%)

	Prevalence in 2025	Adjusted estimates	
		2024	2025
Checked privacy settings on social media accounts	37.3	38.5	36.6**
Purchased or continued to have cyber insurance	3.7	4.6	3.7**
Generally browsed in incognito mode	15.2	15.9	15.2
Cleared their browsing history, data and cookies frequently	35.9	36.9	35.9
Participated in training to stay safe online or protect their online environment and information	13.6	13.4	13.7
Installed or used spam-filtering software	17.8	20.5	17.8***
Installed or used antivirus software or firewalls on their devices	36.1	39.3	36.2***
Regularly updated the security software on their device when prompted by their device's security system	37.9	38.7	37.8
Regularly updated their password on secure accounts, including email, banking or online stores and social media	24.6	25.8	24.5
Used a secure password manager	27.4	25.0	27.4***
Used password protection on their router	23.1	24.5	22.9*
Used different passwords for secure online accounts, especially for banking or financial transactions	47.9	50.9	47.7***
Changed their privacy settings on social media accounts from the default to a more restrictive setting	30.6	32.2	30.0**
Used a virtual private network (VPN) when using the internet	19.1	19.8	19.1
Set, or already had installed, parental controls on devices and browsers to restrict access to certain content[a]	19.3	20.1	19.2
Used voice, fingerprint, facial or iris recognition technology to access their devices, such as their mobile phone	47.8	47.0	47.5
Avoided clicking on links or attachments when they were not certain who the sender of an SMS/text or email was	65.1	67.1	64.8**
Independently contacted a company or government department when they were unsure about an SMS/text or email they had received from them	30.5	31.1	30.4
Used multifactor or two-factor authentication for personal accounts	58.7	58.0	58.5
Used apps and platforms because they protect messages and content with end-to-end encryption	20.3	21.0	20.1

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

a: Limited to respondents with children under 18 years living at home who answered the question (n=5,589)

Note: Predictive margins derived from separate regression models for each online safety strategy that included controls for key sociodemographic, employment and technology use variables. The outcome variable was whether respondents had used that online safety measure. 2024 data exclude 291 respondents who did not know or declined to answer the question; 2025 data exclude 284 respondents who did not know or declined to answer the question

Source: Australian Cybercrime Survey 2025 [weighted data]

The proportion of respondents who shared a password or a code for an account they owned with someone they knew or thought they knew was lower in 2025 than it was in 2024 (6.5% in 2024 vs 5.5% in 2025, $F(39, 20{,}888)=12.69$, $p<0.01$), as was the proportion of respondents who accepted cookies from websites that saved their browsing information (41.5% in 2024 vs 39.0% in 2025, $F(39, 20{,}888)=19.90$, $p<0.001$). The former may be related to the increased use of secure password managers, which mean respondents do not need to remember individual passwords for different accounts. The proportion of respondents accepting cookies also declined from 2023 to 2024 (Voce & Morgan 2025a), and is a positive trend, as accepting cookies from third-party and unencrypted websites can increase the risk of data and identity theft.

Table 12: Prevalence of unsafe online behaviours, 2024 and 2025 (%)

	Prevalence in 2025	Adjusted estimates	
		2024	2025
Accepted friend requests from people online who they had not met in person	8.9	9.1	8.9
Shared a password or a code for an account they own with someone they knew (or thought they knew)	5.6	6.5	5.5**
Used freely available wi-fi in a public location to conduct a financial transaction	9.4	9.2	9.3
Opened emails from people or organisations they did not know	12.0	11.9	12.0
Accepted cookies from websites that saved their browsing information	39.3	41.5	39.0***

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

Note: Predictive margins derived from separate regression models for each unsafe online activity that included controls for key sociodemographic, employment and technology use variables. The outcome variable was whether respondents had engaged in that unsafe online activity. 2024 data exclude 291 respondents who did not know or declined to answer the question; 2025 data exclude 284 respondents who did not know or declined to answer the question

Source: Australian Cybercrime Survey 2025 [weighted data]

Box 5: Changes in online safety behaviours

In both the current report and the Cybercrime in Australia 2024 report (Voce & Morgan 2025a), there were declines in the proportions of respondents who checked their privacy settings on social media accounts and who changed their privacy settings on social media accounts from the default to a more restrictive setting. This could be related to a decline in the use of social media platforms more generally, meaning privacy on these apps is not front of mind for respondents. There was a decline last year in respondents posting or responding to posts on social media, which occurred again this year, along with a decline in the proportion posting or responding to posts on online blogs, forums or interest groups. These findings are supported by research from Deloitte (Deloitte 2025) which found that weekly social media use among a nationally representative sample of 2,000 Australians declined from six hours and 20 minutes in 2024 to five hours and 20 minutes in 2025, and that these declines occurred across all age groups.

In both the 2025 and 2024 surveys, there were also declines in the proportion of respondents who installed or used antivirus software or firewalls on their devices. These findings are consistent with the 2025 Digital Lives of Australians research report, which used data from an online survey of 2,000 Australian consumers and 400 small businesses and found that there was a decline from 2024 to 2025 in the proportion of consumers who maintain up-to-date antivirus software on their computers and have hardware firewalls installed on their home computer networks (auDA 2025). One explanation for this trend is that the public is increasingly relying on built-in antivirus protection when they buy new devices and products, and tend to feel this sufficient, rather than needing to spend money on additional software (Koebert 2026).

In both the current report and the Cybercrime in Australia 2024 report (Voce & Morgan 2025a), there were also declines in the proportion of respondents accepting cookies from websites that saved their browsing information. Rejecting non-essential cookies is a positive online behaviour that limits the tracking of respondents' browsing habits and blocks third-party data sharing. This is consistent with Australians being more cautious about what data is being collected online (Office of the Australian Information Commissioner 2023).

Finally, both this year and last year, there were declines in the proportion of respondents who avoided clicking on links or attachments when they were not certain who the sender of a text message or email was. This may be because of government and private sector efforts to block scammers from reaching potential victims, resulting in fewer phishing phone calls, texts and emails with malicious attachments (Australian Communications and Media Authority 2025).

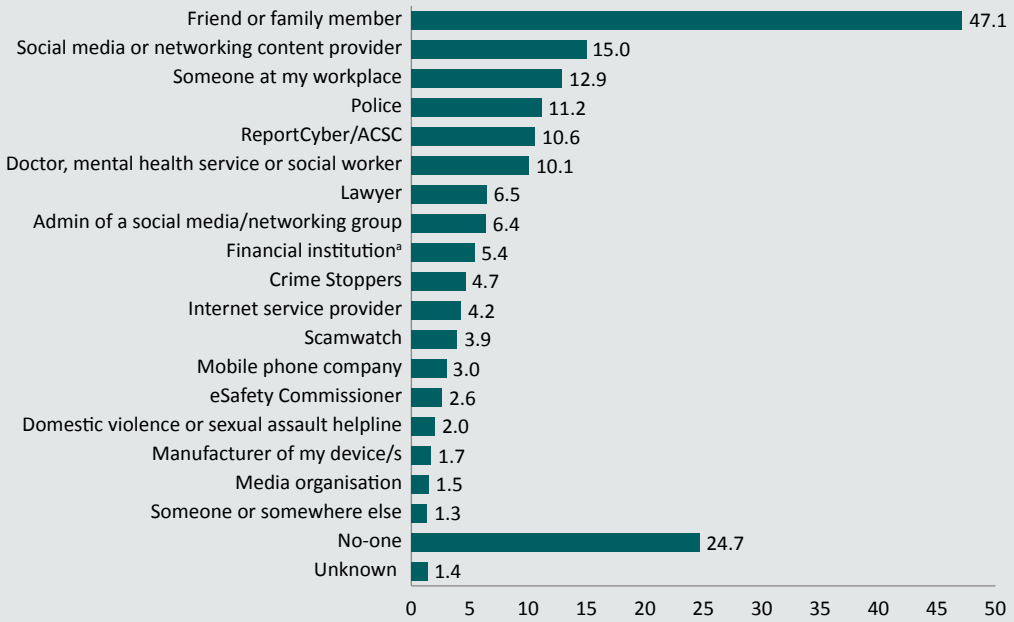
Help-seeking by victims following the most recent incident

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 sought help, advice or support following the most recent incident from a family member or friend (47.1%); a social media or networking content provider (15.0%); someone at their workplace, such as a manager, human resources or IT support staff (12.9%); and the police (11.2%; Figure 9). Just under a quarter of victims (24.7%) did not seek help from anyone about the most recent incident.

Figure 9: Help-seeking among online abuse and harassment victims following the most recent incident (%) (*n*=2,589)



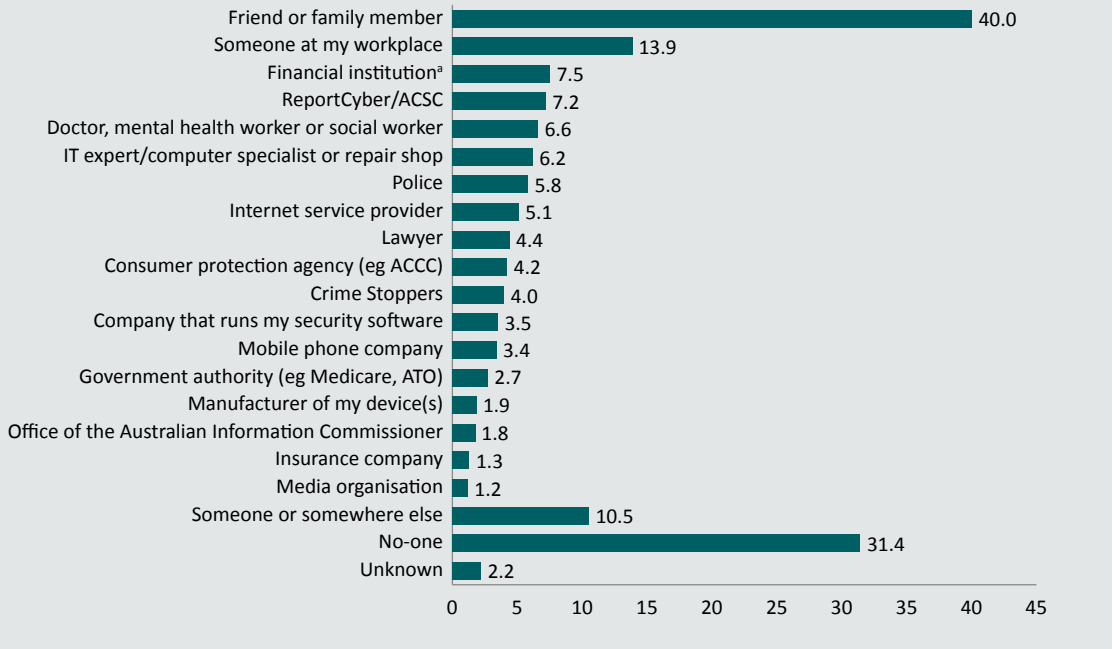
a: Financial institution=bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)

Note: ACSC= Australian Cyber Security Centre. Excludes 53 people who did not answer questions about the most recent incident. Weighted percentages may not add to total due to rounding. Respondents could select multiple methods of reporting the most recent incident

Source: Australian Cybercrime Survey 2025 [weighted data]

Victims of malware most commonly sought help, advice or support following the most recent incident from a family member or friend (40.0%), someone at their workplace (13.9%), a financial institution such as a bank or credit union or a credit or debit card company (7.5%) or ReportCyber (7.2%; Figure 10). Malware had the highest proportion of victims who did not seek help from anyone about the most recent incident (31.4%).

Figure 10: Help-seeking among malware victims following the most recent incident (%) (*n*=2,282)



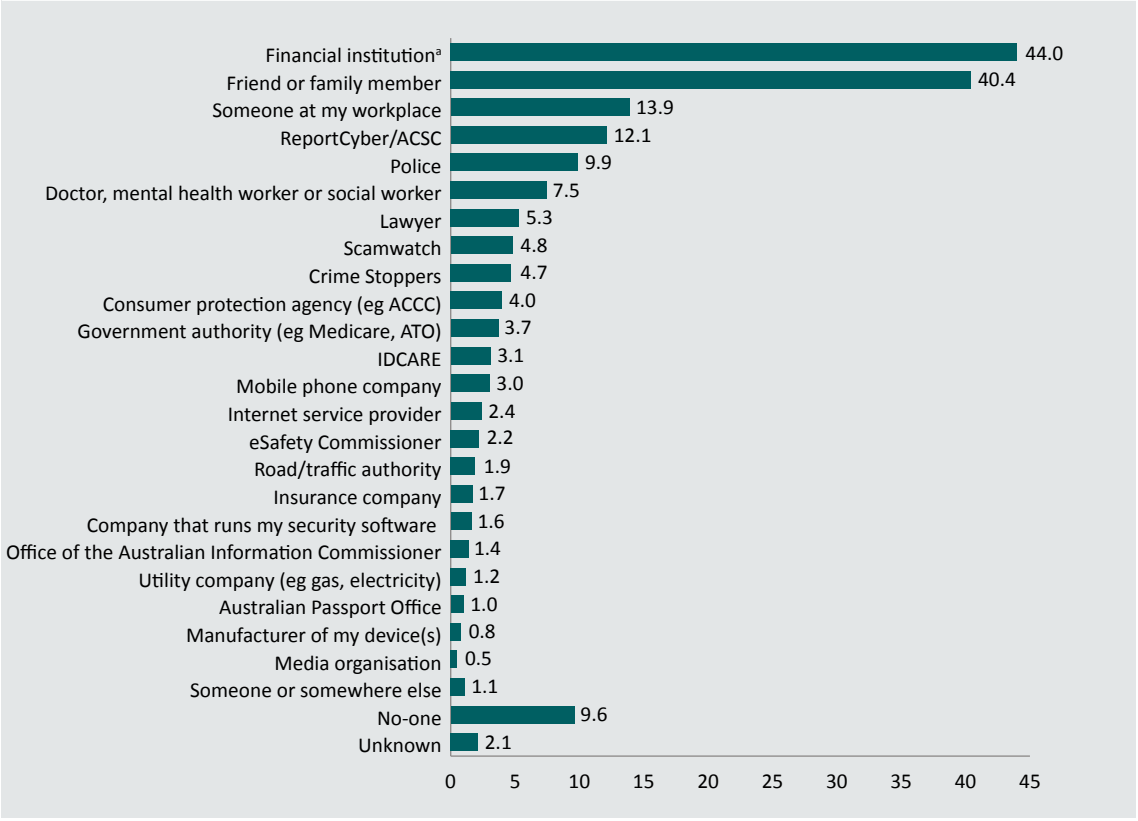
a: Financial institution=bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)

Note: ACCC=Australian Competition and Consumer Commission; ACSC=Australian Cyber Security Centre; ATO=Australian Taxation Office. Excludes 25 people who did not answer questions about the most recent incident. Weighted percentages may not add to total due to rounding. Respondents could select multiple methods of reporting the most recent incident

Source: Australian Cybercrime Survey 2025 [weighted data]

A large proportion of identity crime victims sought help, advice or support following the most recent incident from a financial institution such as a bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal; 44.0%; Figure 11). Victims also commonly told a family member or friend (40.4%); someone at their workplace, such as a manager, human resources or IT support staff (13.9%); and ReportCyber (12.1%). Identity crime and misuse victims were the most likely to seek help, advice or support from at least one source, with around one in 10 (9.6%) not telling anyone about the most recent incident.

Figure 11: Help-seeking among identity crime and misuse victims following the most recent incident (%) (*n*=2,185)



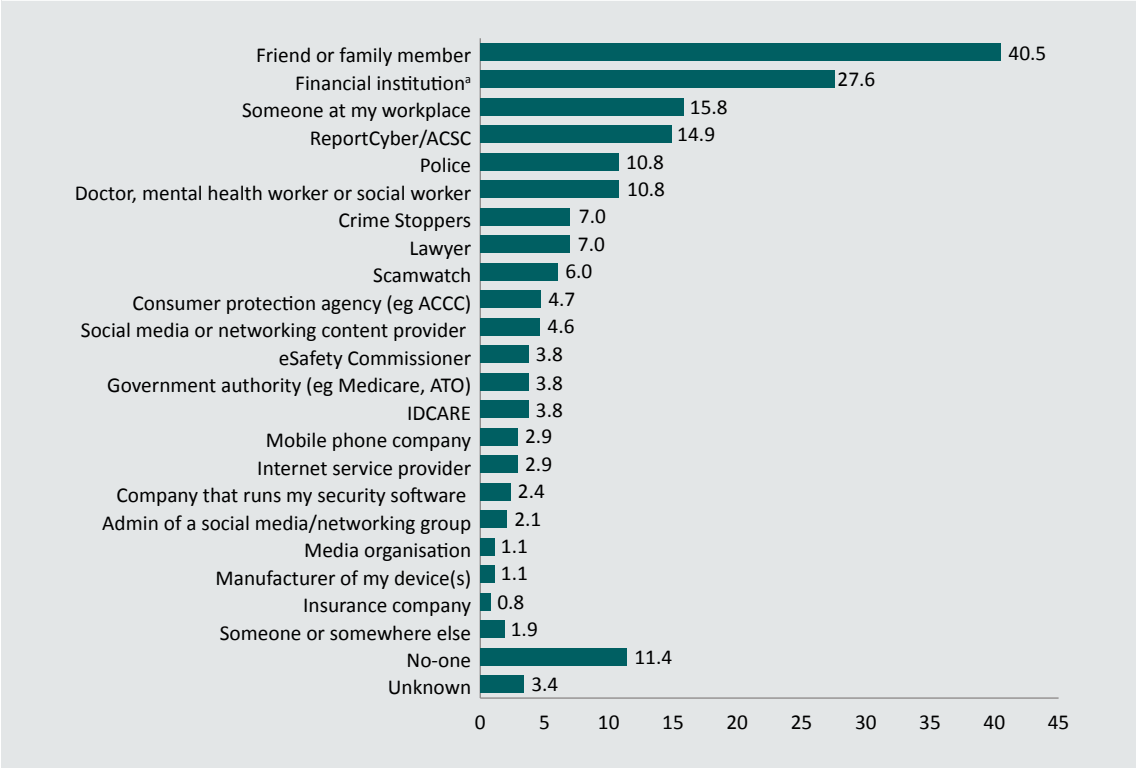
a: Financial institution=bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)

Note: ACCC=Australian Competition and Consumer Commission; ACSC=Australian Cyber Security Centre; ATO=Australian Taxation Office. Excludes 18 victims who did not answer questions about the most recent incident. Weighted percentages may not add to total due to rounding. Respondents could select multiple methods of reporting the most recent incident

Source: Australian Cybercrime Survey 2025 [weighted data]

Similarly, a large proportion of fraud and scam victims sought help, advice or support following the most recent incident from 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; 27.6%; Figure 12). Victims also commonly told a family member or friend (40.5%); someone at their workplace, such as a manager, human resources or IT support staff (15.8%); or the Australian Cyber Security Centre (ACSC) through its ReportCyber portal or telephone helpline (14.9%). Just over one in 10 victims stated that they had not sought help from anyone about the incident (11.4%).

Figure 12: Help-seeking among fraud and scam victims following the most recent incident (%) (*n*=1,206)



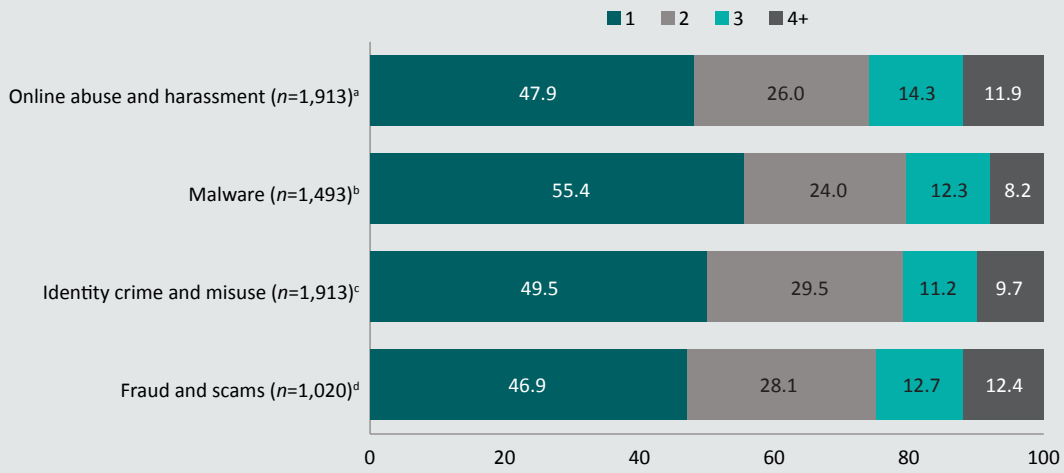
a: Financial institution=bank or credit union, a credit or debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)

Note: ACCC=Australian Competition and Consumer Commission; ACSC=Australian Cyber Security Centre; ATO=Australian Taxation Office. Excludes 9 victims who did not answer questions about the most recent incident. Weighted percentages may not add to total due to rounding. Respondents could select multiple methods of reporting the most recent incident

Source: Australian Cybercrime Survey 2025 [weighted data]

Many victims sought assistance from more than one source following the most recent incident of cybercrime (Figure 13). Among victims who sought help from anyone, 52 percent of online abuse and harassment victims, 45 percent of malware victims, 51 percent of identity crime victims and 53 percent of fraud and scam victims sought help from more than one source.

Figure 13: Number of sources of help, advice and support among victims who sought help following the most recent incident (%)



a: Excludes 639 online abuse and harassment victims who did not seek help from anyone, 53 victims who did not answer questions about the most recent incident, and 37 victims who did not know or declined to answer this question

b: Excludes 710 malware victims who did not seek help from anyone, 25 victims who did not answer questions about the most recent incident and 49 victims who did not know or declined to answer this question

c: Excludes 209 identity crime and misuse victims who did not seek help from anyone, 18 victims who did not answer questions about the most recent incident, and 45 victims who did not know or declined to answer this question

d: Excludes 136 fraud and scam victims who did not seek help from anyone, 9 victims who did not answer questions about the most recent incident, and 40 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 2025 [weighted data]

Seeking help and reporting to police or ReportCyber

A major focus of the ACS is on seeking help from police agencies and 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. According to the latest assessment, a report is submitted to ReportCyber every six minutes (Australian Signals Directorate 2025).

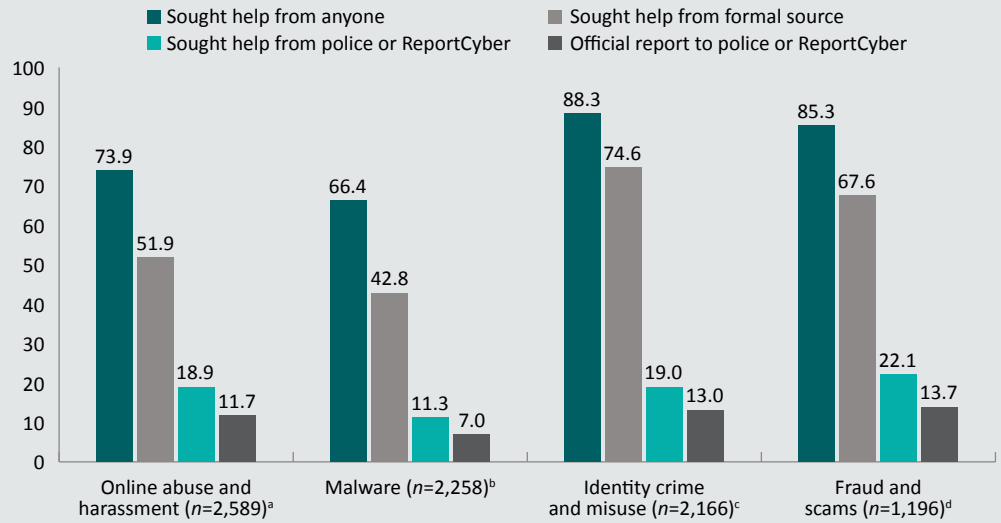
While the survey asks about both police and ReportCyber, it should be noted that police agencies ask victims to report cybercrimes to ReportCyber. Likewise, the ReportCyber platform makes clear to users they will be reporting a cybercrime to police through ReportCyber. For this reason, it is difficult 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 both police and ReportCyber).

Respondents who said they sought help, advice or support from police or ReportCyber were then asked whether they had submitted an official report. An official report was defined as one where the respondent received some acknowledgement that the incident had been recorded (eg a confirmation screen or email, report number etc). Official reports could be submitted online, over the phone or in person. The questions that follow about outcomes from reporting and satisfaction are also limited to victims who made an official report.

As shown in Figure 14, formal help-seeking (ie seeking help from someone other than a family member or friend) was higher among identity crime victims (74.6%) and fraud and scam victims (67.6%) than online abuse and harassment victims (51.9%) and malware victims (42.8%). This likely reflects the large proportion of identity crime and fraud and scam victims reporting to financial institutions (44.0% and 27.6%, respectively).

Over one in five fraud and scam victims sought help, advice or support from the police or ReportCyber (22.1%) and over half of these victims went on to make an official report (13.7%). Identity crime and misuse victims were the next most likely to have sought help, advice or support from the police or ReportCyber (19.0%) and make an official report (13.0%), followed closely by online abuse and harassment victims, of whom 18.9 percent sought help, advice or support from the police or ReportCyber and 11.7 percent made an official report. Malware victims were the least likely to seek help, advice or support from the police or ReportCyber (11.3%) and to make an official report (7.0%).

Figure 14: Help-seeking following the most recent incident, by crime type (%)



a: Excludes 53 victims who did not answer questions about the most recent incident. Denominator includes 37 victims who did not know or declined to answer this question. Denominator for making an official report to police or ReportCyber includes an additional 22 victims who did not know or declined to answer this question

b: Excludes 25 victims who did not answer questions about the most recent incident. Denominator includes 49 victims who did not know or declined to answer this question. Denominator for making an official report to police or ReportCyber includes an additional 17 victims who did not know or declined to answer this question

c: Excludes 18 victims who did not answer questions about the most recent incident. Denominator includes 45 victims who did not know or declined to answer this question. Denominator for making an official report to police or ReportCyber includes an additional 14 victims who did not know or declined to answer this question

d: Excludes 9 victims who did not answer questions about the most recent incident. Denominator includes 40 victims who did not know or declined to answer this question. Denominator for making an official report to police or ReportCyber includes an additional 13 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 2025 [weighted data]

Box 6: Understanding the extent of unreported cybercrime

Throughout the Cybercrime in Australia report series (Voce & Morgan 2025a, 2023a), the prevalence of victims seeking help from police or ReportCyber has been consistently low. This year, between 7.0 and 13.7 percent of victims made an official report to police or ReportCyber. When we compare this to the official reporting rate for other types of crime, it is clear that cybercrime continues to be significantly under-reported.

According to the ABS (2025), police reporting rates in 2023–24 were 75 percent for house break-ins, 84 percent for motor vehicle thefts, 55 percent for malicious property damage, and 37 percent for other forms of theft. This may be due to victims experiencing a direct financial loss for these types of crimes or needing to make a police report to claim insurance, whereas most cybercrimes in this report did not involve the victim directly losing money. However, even the reporting rate for attempted break-ins (48%) was significantly higher than for all types of cybercrime.

Among those victims who did lose money directly from the most recent incident, the prevalence of official reports to police or ReportCyber was 31.9 percent for online abuse and harassment victims, 28.6 percent for malware victims, 16.5 percent for identity crime and misuse victims and 23.3 percent for scam and fraud victims. This is still much lower than for 'in person' acquisitive crimes.

ReportCyber received over 84,700 cybercrime reports in 2024–25, which equates to one report every six minutes (Australian Signals Directorate 2025). This illustrates the likely true scale of cybercrime incidents in the Australian community.

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

- Only 2.3 percent of online abuse and harassment victims, 2.9 percent of identity crime and misuse victims and 4.0 percent of online fraud and scam victims said they made an official report to Scamwatch following the most recent incident.
- Just 1.4 percent of online abuse and harassment victims said they made an official report to the eSafety Commissioner following the most recent incident.

Official reporting to police and ReportCyber among select groups of respondents

The prevalence of respondents making an official report to police or ReportCyber following the most recent incident was analysed according to sociodemographic characteristics and business ownership status (Table 13). Several key findings emerged about who was more likely to make an official report:

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

Table 13: Respondents who made an official report to police or ReportCyber, by sociodemographic characteristics (%)

	Online abuse and harassment	Malware	Identity crime and misuse	Fraud and scams
Age				
18–24	11.3***	8.6***	16.0***	13.6
25–34	16.9	12.7	18.9	17.3
35–49	13.2	7.0	15.0	17.2
50–64	8.2	3.1	8.2	11.1
65+	7.4	2.5	6.7	9.1
Gender				
Female	11.7	6.4	11.6*	12.5
Male	12.5	8.0	15.1	16.2
First Nations				
Yes	24.1***	15.3***	33.1***	23.4**
No	10.7	6.4	11.6	13.2
LGB+				
Yes	9.2	7.7	14.3	15.5
No	12.4	7.2	13.4	14.3
Born outside of Australia				
Yes	10.3	7.2	12.6	14.8
No	12.5	7.0	13.3	14.3
Restrictive long-term health condition				
Yes	12.4	7.6	15.0*	14.6
No	11.2	6.5	11.5	14.1
Owns, operates or works for a small to medium enterprise (SME)				
Owner or manager	20.8***	13.9***	20.9***	21.5*
Employee	13.4	8.5	16.5	17.2
Works but not at an SME	8.1	4.4	10.3	11.3
Owns, operates or works for a large company or business				
Owner or executive	13.8***	9.4*	14.7***	11.1*
Employee	6.8	4.3	7.5	10.7
Works but not at a large company	15.8	10.0	17.6	18.9

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

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

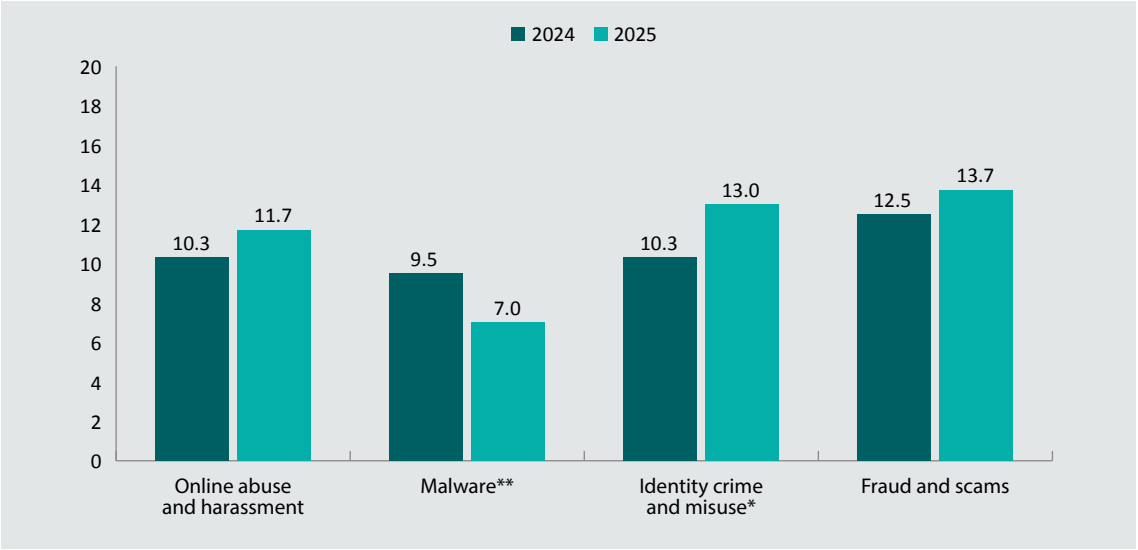
Source: Australian Cybercrime Survey 2025 [weighted data]

Changes in official reporting to police or ReportCyber

We compared the proportion of victims who made an official report to police or ReportCyber in 2024 and 2025 (Figure 15). The proportion of victims who officially reported to police or ReportCyber increased for identity crime and misuse (10.3% in 2024 vs 13.0% in 2025; $F(1, 4{,}413)=36.81$, $p<0.05$) and decreased for malware (9.5% in 2024 vs 7.0% in 2025; $F(1, 4{,}365)=43.19$, $p<0.01$). There was no statistically significant change in the proportion of victims who officially reported online abuse and harassment (10.3% in 2024 vs 11.7% in 2025) or fraud and scams (12.5% in 2024 vs 13.7% in 2025).

Despite the decline in the proportion of malware victims who made an official report to police or ReportCyber, there was no statistically significant change in the proportion of ransomware victims who officially reported (12.2% in 2024 vs 11.9% in 2025).

Figure 15: Official reporting to police or ReportCyber following the most recent incident, by crime type, 2024 and 2025 (%)



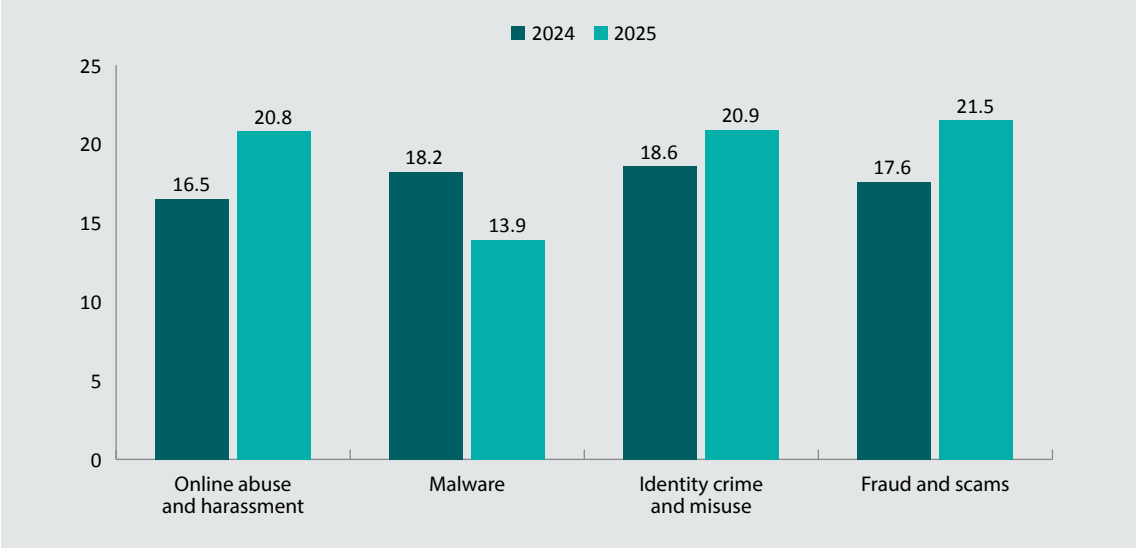
*statistically significant at $p<0.05$, **statistically significant at $p<0.01$

Note: Denominator includes respondents who did not state whether they made an official report to police or ReportCyber. These numbers vary by crime type and survey year. Weighted percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2025 [weighted data]

We then repeated the analysis for small to medium business owners, operators and managers who were the victims of cybercrime (Figure 16). While official reporting rates among small to medium business owners slightly increased for all types of cybercrime besides malware, these changes were not statistically significant.

Figure 16: Official reporting to police or ReportCyber among small to medium business owners, operators and managers following the most recent incident, 2024 and 2025 (%)



Note: Excludes respondents who did not state whether they reported to police or ReportCyber. These numbers vary by crime type and survey year. Weighted percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2025 [weighted data]

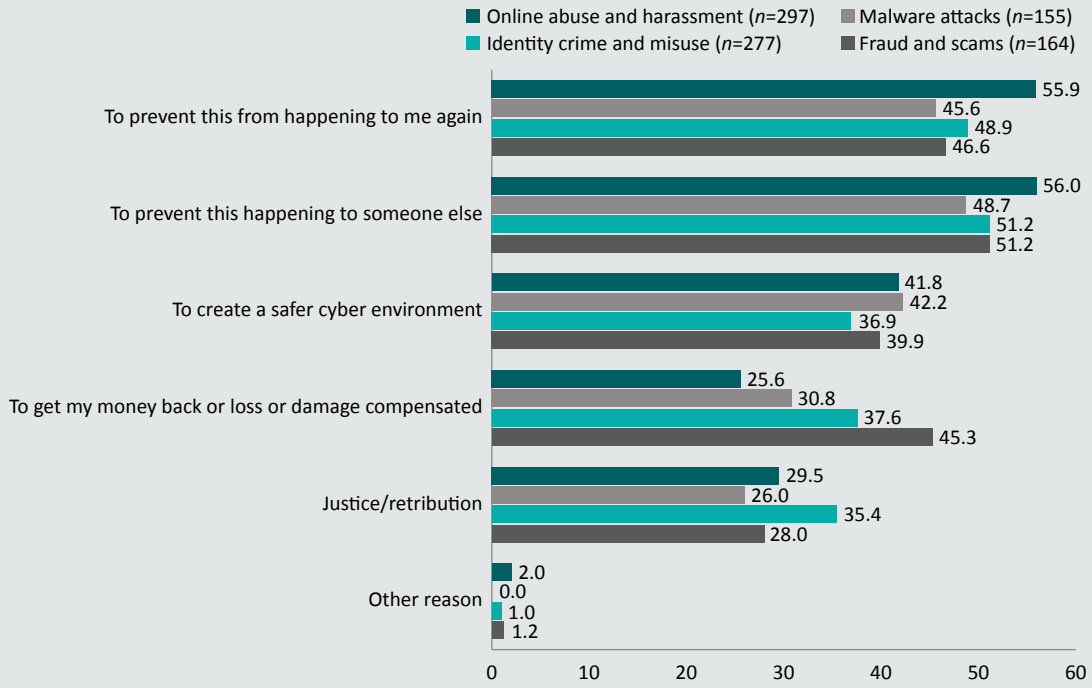
Reasons for official reporting to police or ReportCyber

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

Across all crime types, the most common reason for reporting to police or ReportCyber was to prevent the crime from happening to them again or to someone else (Figure 17). About half of the respondents who made official reports gave these reasons.

Malware victims were the most likely to say they reported the most recent incident to create a safer cyber environment (42.2%), while fraud and scam victims were more likely than victims of other types of cybercrime to say they were motivated by the desire to recover lost money or have damages compensated (45.3%) and a sense of justice or retribution (35.4%).

Figure 17: Reasons for making an official report to police or ReportCyber following the most recent incident, by crime type (%)



Note: Respondents could nominate more than one reason for reporting the most recent incident. Excludes 6 online abuse and harassment victims, 3 malware victims and 4 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 2025 [weighted data]

Outcomes of official reports to police or ReportCyber

Outcomes of reporting to police or ReportCyber ranged from not having heard anything following their report and not knowing what had happened, through to being told by police that someone had been arrested, charged or prosecuted for the crime (Figure 18). The focus here is on what victims perceived as the outcome—the actual outcome recorded by police may differ. This was limited to respondents who made an official report to police or ReportCyber.

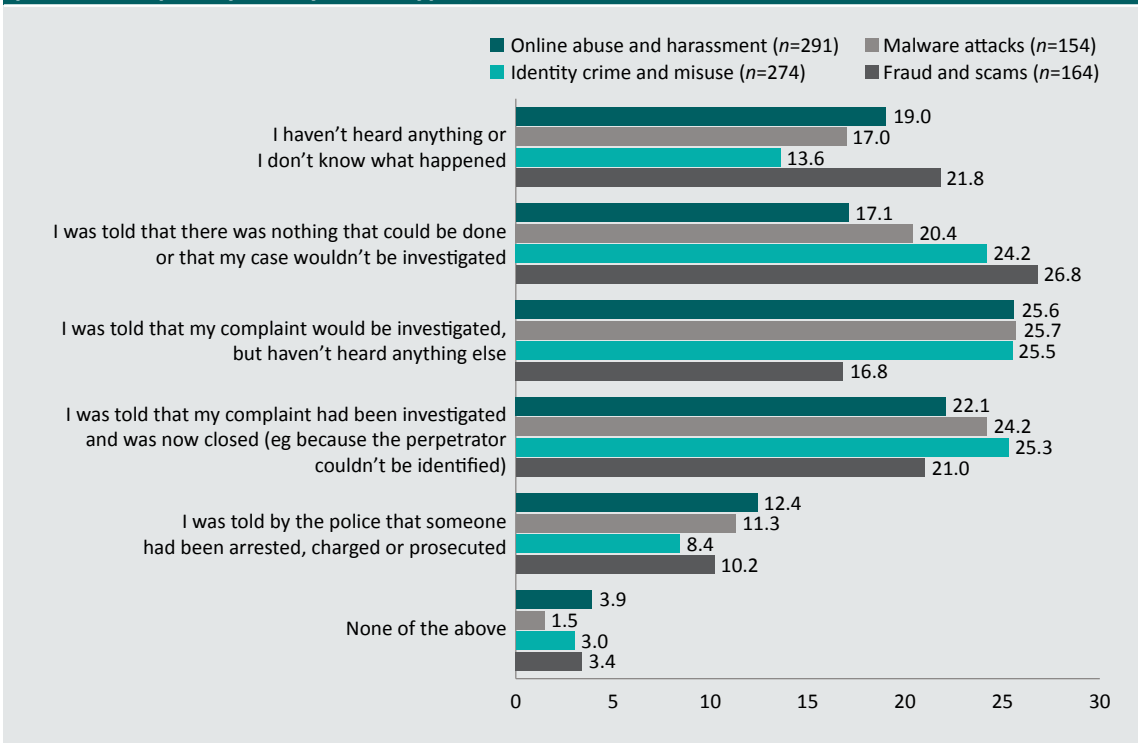
Over one-third of online abuse and harassment victims (36.1%) had not heard anything or did not know what happened with their report, or were told that nothing could be done or the case would not be investigated. Sixty percent of victims said they were told their complaint would be or had been investigated, with 12.4 percent having been told by the police that someone had been arrested, charged or prosecuted.

The majority of malware victims were also told their complaint would be or had been investigated (61.2%), with 11.3 percent having been told by the police that someone had been arrested, charged or prosecuted.

Identity crime and misuse victims were the most likely to have been told their case had been investigated and closed without an offender being apprehended (25.3%), with 8.4 percent having been told by the police that someone had been arrested, charged or prosecuted.

Fewer than half of all fraud and scam victims (48.0%) were told that their case would be or had been investigated, with 21.0 percent told their case had been investigated and closed without an offender being apprehended and 10.2 percent being told that someone had been arrested, charged or prosecuted.

Figure 18: Outcomes of reporting among victims who reported the most recent incident to police or ReportCyber, by crime type (%)



Note: Excludes 12 online abuse and harassment victims, 4 malware victims and 7 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

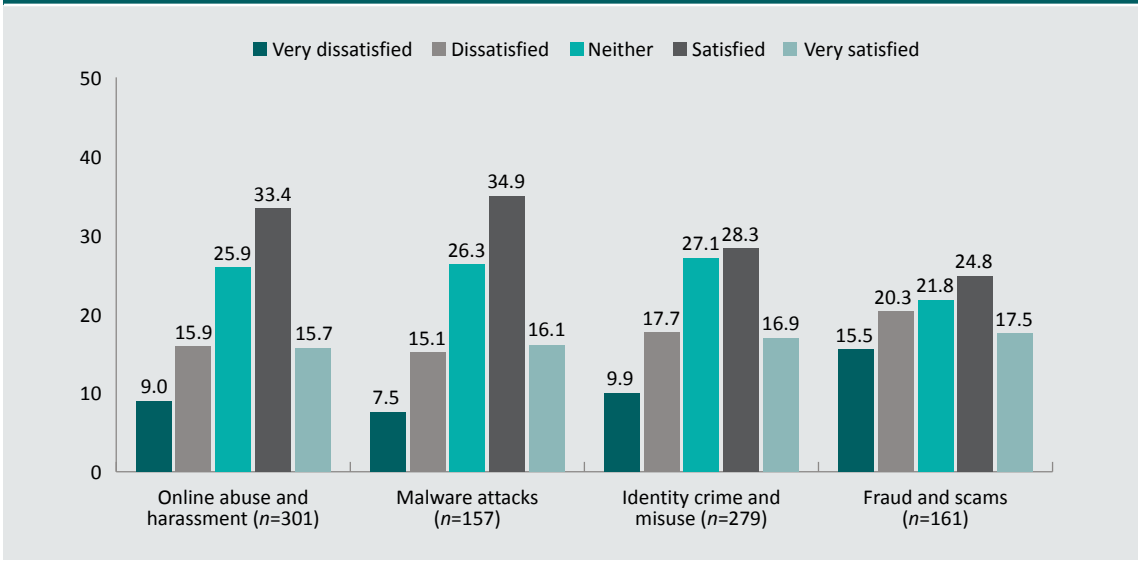
Source: Australian Cybercrime Survey 2025 [weighted data]

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

- 24.9 percent of online abuse and harassment victims were dissatisfied or very dissatisfied with the outcome of their report, while 49.1 percent were satisfied or very satisfied with the outcome;
- 22.6 percent of malware victims were dissatisfied or very dissatisfied with the outcome of their report, while 51.0 percent were satisfied or very satisfied with the outcome;
- 27.6 percent of identity crime and misuse victims were dissatisfied or very dissatisfied with the outcome of their report, while 45.2 percent were satisfied or very satisfied with the outcome; and
- 35.8 percent of fraud and scam victims were dissatisfied or very dissatisfied with the outcome of their report, while 42.3 percent were satisfied or very satisfied with the outcome (Figure 19).

The remaining victims were neither satisfied nor dissatisfied with the outcome of the report. This ranged from 21.8 percent for fraud and scam victims to 27.1 percent for identity crime and misuse victims.

Figure 19: Satisfaction with the outcome of reporting among victims who made an official report to police or ReportCyber, by crime type (%)



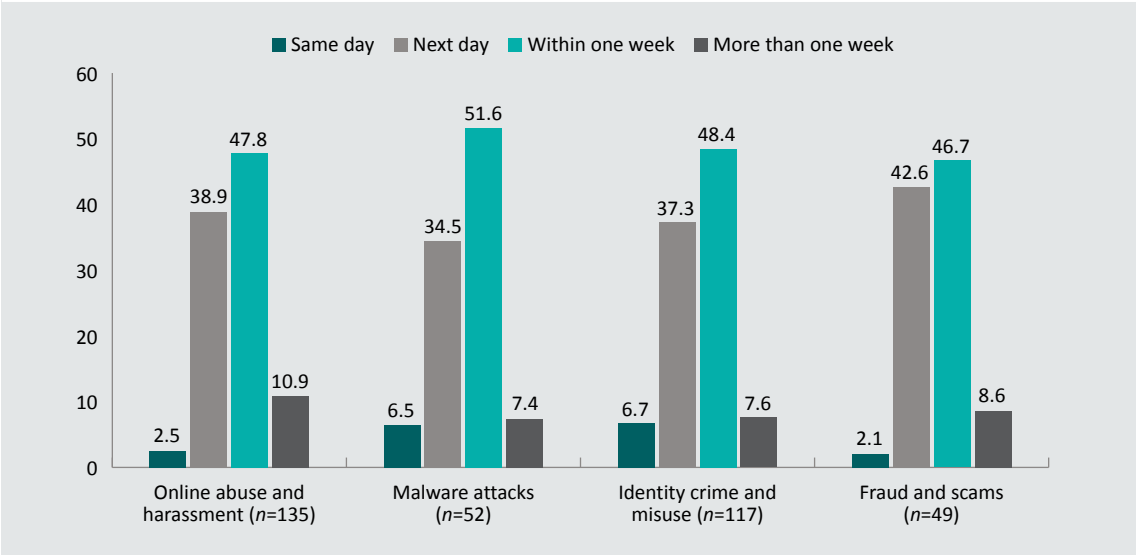
Note: Excludes 2 online abuse and harassment victims, 1 malware victim, 2 identity crime and misuse victims and 3 fraud and scam victims who did not know or declined to answer the question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2025 [weighted data]

Time between cybercrime incidents and official reporting

Victims were asked the number of days between the most recent incident occurring and their official report to the police or ReportCyber. Because victims could report to one or both of police and ReportCyber, this question was asked separately for each. The results were similar for police (Figure 20) and ReportCyber (Figure 21). It was most common for victims to say they reported to police within one week of the incident for online abuse and harassment (47.8%), malware (51.6%), identity crime and misuse (48.4%) and fraud and scam victims (46.7%). Victims also most commonly reported to ReportCyber within a week, including online abuse and harassment victims (43.7%), malware victims (53.9%), identity crime and misuse victims (58.3%) and fraud and scam victims (43.0%). Overall, respondents indicated that they submitted an official report to police more quickly than they did to ReportCyber.

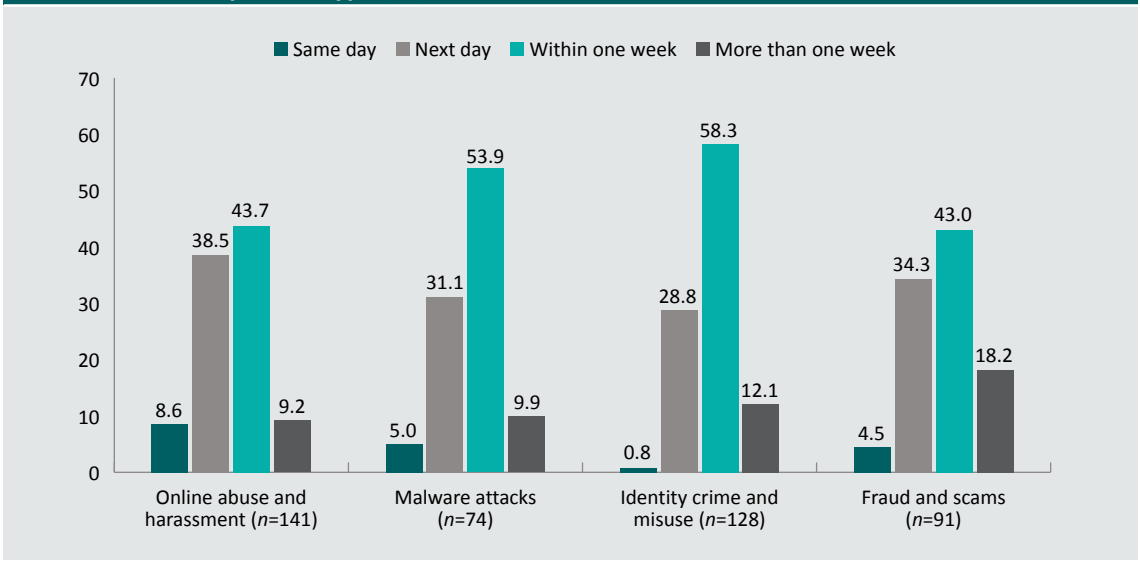
Figure 20: Length of time taken to submit a report to police following the most recent incident, by crime type (%)



Note: Excludes 26 online abuse and harassment victims, 16 malware victims, 22 identity crime and misuse victims and 18 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 2025 [weighted data]

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



Note: Excludes 32 online abuse and harassment victims, 34 malware victims, 28 identity crime and misuse victims and 25 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 2025 [weighted data]

Reasons for not reporting to police or ReportCyber

Respondents who did not make an official report to police or ReportCyber following the most recent incident were asked their reasons for not doing so (Table 14). The various reasons for not reporting were aggregated into five main categories:

- seriousness of the incident;
- understanding, perceptions or past experience of reporting;
- worry about the reaction to or consequences of reporting;
- incident handled by someone else; and
- other reasons.

Nearly two-thirds of online abuse and harassment (61.8%) and malware (62.4%) victims said they did not report the most recent incident because of the perceived seriousness of the incident. Fraud and scam victims (39.5%) were much less likely to say that they did not report because they did not perceive the incident to be serious enough, as were identity crime and misuse victims (49.9%). In terms of the specific reasons given, the most common reason victims did not report to police or ReportCyber was that they felt they could deal with it themselves; however, this was less common among fraud and scam victims (21.0%) than among victims of online abuse and harassment (36.7%), malware (34.2%) and identity crime and misuse (31.4%). For online abuse and harassment (31.8%) and malware (26.2%) victims, the next most common reason was they did not regard the incident as a serious offence.

Fraud and scam victims (51.8%) were the most likely to cite reasons relating to their understanding, perceptions or past experiences of reporting, followed by identity crime and misuse victims (49.7%). However, there was less variation between the different types of cybercrime for this broad category (39.8% to 51.8% of victims). Between 15.2 and 21.8 percent of victims still did not know that reporting to the police, ACSC or ReportCyber was an option, while between 14.2 and 21.2 percent of victims did not think the police, ACSC or ReportCyber would be able to do anything. Between 13.8 and 17.2 percent of victims did not know how or where to report the matter. It was rare for victims who did not seek help to say the reason for not reporting was dissatisfaction with previous reporting outcomes (5.7% to 8.7% of victims) or that they did not trust the police or ReportCyber (4.5% to 6.3%).

Fraud and scam victims (37.3%) were the most likely to say that they did not report the most recent incident because they were worried about the reaction to or consequences of making a report, followed by online abuse and harassment victims (31.7%). Notably, fraud and scam victims were much more likely to say the reason for not reporting was that they felt ashamed or embarrassed (16.0%) compared to victims of the other cybercrime types (5.1% to 9.9%).

Table 14: Reasons for not reporting to police or ReportCyber, by crime type (%)

	Online abuse and harassment (*n*=2,169)	Malware (*n*=1,939)	Identity crime (*n*=1,744)	Fraud and scams (*n*=980)
Seriousness of the incident				
Felt they could deal with it themselves	36.7	34.2	31.4	21.0
Did not regard the incident as a serious offence	29.2	23.5	17.8	14.3
Did not know or think the incident was a crime	18.3	17.4	8.9	11.6
Any of the above	*61.8*	*62.4*	*49.9*	*39.5*
Understanding, perceptions or past experience of reporting				
Did not know reporting to the police, ACSC or ReportCyber was an option	17.0	15.2	21.8	20.6
Did not think the police, ACSC or ReportCyber would be able to do anything	19.9	14.2	19.0	21.2
I did not know how or where to report the matter	14.0	13.8	14.5	17.2
Have reported before and been dissatisfied with the outcome	6.8	5.7	5.7	8.7
Did not trust the police, ACSC or ReportCyber	5.0	4.5	4.6	6.3
Any of the above	*43.3*	*39.8*	*49.7*	*51.8*

Table 14: Reasons for not reporting to police or ReportCyber, by crime type (%) (cont.)				
	Online abuse and harassment (*n*=2,169)	Malware (*n*=1,939)	Identity crime (*n*=1,744)	Fraud and scams (*n*=980)
Worry about the reaction to or consequences of reporting				
Did not want to ask for help	11.3	9.4	5.2	8.4
Felt ashamed or embarrassed	9.9	5.1	5.2	16.0
Felt I would not be believed	6.3	5.2	4.4	5.9
Fear of legal processes	5.1	3.9	3.5	4.5
Fear of the person responsible (eg fear of retaliation)	6.2	3.4	4.0	5.8
Did not want the person responsible arrested	4.2	3.0	2.6	4.4
Cultural or language reasons	2.5	2.2	2.7	4.6
Any of the above	*31.7*	*24.9*	*21.4*	*37.3*
Incident handled by someone else				
Workplace/on-the-job incident—internal reporting procedures followed	4.4	5.1	3.2	4.2
Provider (eg bank, telecommunications company) involved in incident was resolving or had resolved the matter	0.3	0.2	5.3	1.9
Any of the above	*4.7*	*5.3*	*8.4*	*6.1*
Other reason	2.0	2.2	1.9	1.9

Note: Excludes 95 online abuse and harassment victims, 145 malware victims, 126 identity crime and misuse victims and 40 fraud and scam victims who did not know or declined to answer the question. Weighted percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2025 [weighted data]

Box 7: Have there been changes in the reasons that victims don't report cybercrime?

There have been some minor shifts in the reasons victims give for not reporting to police or ReportCyber. Positively, a lower proportion of online abuse and harassment victims said they were fearful of how the person responsible would react (8.2% in 2024 vs 6.2% in 2025; $F(1, 4{,}553)=4.71$, $p<0.05$). Also, a higher proportion of fraud and scam victims did not report because a service provider (eg a bank or telecommunications company) involved in the incident was resolving or had resolved the matter (1.0% in 2024 vs 2.0% in 2025; $F(1, 1{,}781)=4.39$, $p<0.05$). There were also increases in the proportion of malware victims who said they felt they could deal with it themselves (30.5% in 2024 vs 34.2% in 2025; $F(1, 3{,}739)=4.85$, $p<0.05$) and identity crime and misuse victims who said they did not think the incident was serious enough (7.0% in 2024 vs 9.0% in 2025; $F(1, 3{,}729)=3.94$, $p<0.05$). This may indicate increased confidence in knowing where to seek help and what actions to take in response to these incidents. But these are very small changes.

Many reasons that victims give for not reporting cybercrime to police or ReportCyber have remained largely consistent over the past few years (Voce & Morgan 2025a, 2023a). A sizeable proportion of victims in 2025 (ranging from 21.4% for identity crime and misuse victims to 37.3% for fraud and scam victims) said that they were worried about the reaction to or consequences of reporting, and this has not changed since 2024. Victims continue to feel ashamed or embarrassed or that they will not be believed. Similarly, victims' understanding, perceptions and past experiences of reporting continue to be barriers (ranging from 39.8% for malware victims to 51.8% for fraud and scam victims). These patterns have not changed in recent years. In particular, many victims continue to say that they did not know that reporting to the police or ReportCyber was an option, did not think the police or ReportCyber could help, or did not know how or where to report the matter.

While it is likely to take some time to shift attitudes and raise awareness, building knowledge of and trust in reporting systems, and reducing stigma around victimisation, are important areas for improvement.

Impacts of victimisation

Financial losses

Victims were asked whether they had directly lost money because of the most recent incident (Table 15). Online abuse and harassment victims were asked if the perpetrator(s) had demanded money to resolve the most recent incident (eg to prevent the release of intimate images or personal information, to give control of an account back to the victim or to take down fake profiles). The crime type where the highest proportion of victims reported financial losses was fraud and scams (36.0%), followed by identity crime (29.6%). Financial losses were relatively uncommon for online abuse and harassment victims (6.7%) and malware victims (9.7%). Thirty-six percent of malware victims who lost money or had money stolen said the most recent incident involved ransomware (with or without encryption), despite these respondents accounting for only 21.8 percent of malware victims.

Victims were then asked if they had spent money dealing with the consequences of the most recent incident, such as by getting legal advice, taking time off work, or installing new software. Fourteen percent of online abuse and harassment victims, 13.7 percent of malware victims, 13.9 percent of identity crime victims and 19.0 percent of fraud and scam victims spent money dealing with the consequences.

Finally, victims were asked whether any of the money they had directly lost was recovered by banks or other organisations, or recovered in other ways. Three percent of online abuse and harassment victims, 4.5 percent of malware victims, 19.4 percent of identity crime victims and 12.1 percent of fraud and scam victims recovered the money they lost as a direct result of their victimisation.

Table 15: Money lost, money spent on consequences and money recovered following most recent incident of cybercrime, by crime type

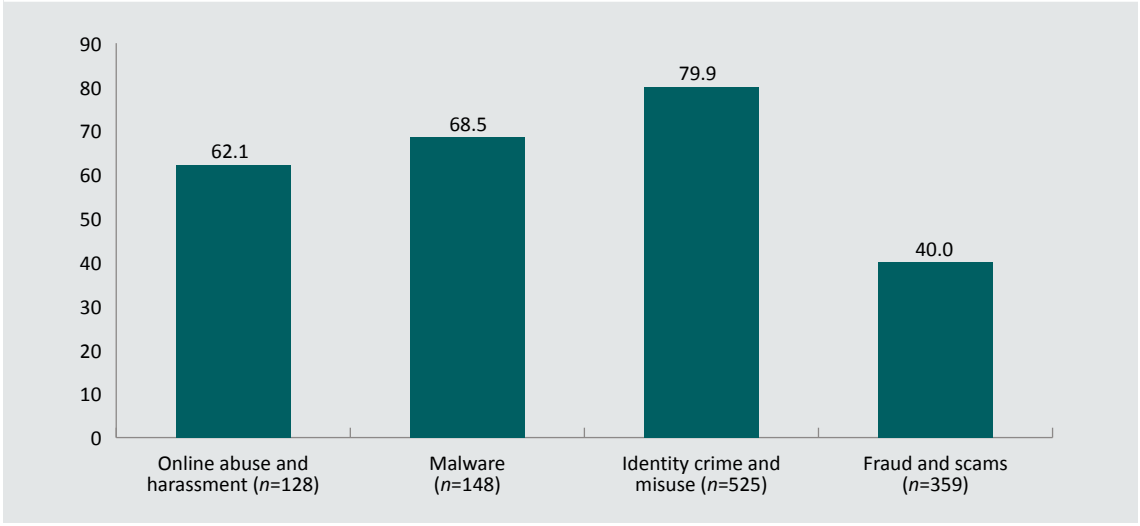
	Online abuse and harassment (*n*=2,589) *n* (%)	Malware (*n*=2,258) *n* (%)	Identity crime (*n*=2,166) *n* (%)	Fraud and scams (*n*=1,196) *n* (%)
Victims who stated they lost money directly	172 (6.7)	219 (9.7)	641 (29.6)	431 (36.0)
Victims who could report how much they lost	130 (5.0)	153 (6.8)	534 (24.7)	362 (30.3)
Victims who stated that they spent money on consequences	372 (14.4)	309 (13.7)	300 (13.9)	227 (19.0)
Victims who could report how much they spent on consequences	279 (10.8)	218 (9.7)	231 (10.7)	179 (15.0)
Victims who recovered money	79 (3.1)	102 (4.5)	420 (19.4)	145 (12.1)
Victims who could report how much they recovered	79 (3.1)	95 (4.2)	412 (19.0)	145 (12.1)

Note: Weighted frequencies and percentages may not add to total due to rounding. Excludes 53 online abuse and harassment victims, 25 malware victims, 18 identity crime and misuse victims and 9 fraud and scam victims who did not answer questions about the most recent incident

Source: Australian Cybercrime Survey 2025 [weighted data]

Not all cybercrime victims who lost money as a direct result of the incident reported being able to recover money (Figure 22). The proportion of victims who were able to recover money was lowest among victims of fraud and scams (40.0%) and highest among victims of identity crime and misuse (79.9%).

Figure 22: Proportion of victims who lost money who were able to recover any money following most recent incident, by crime type (%)

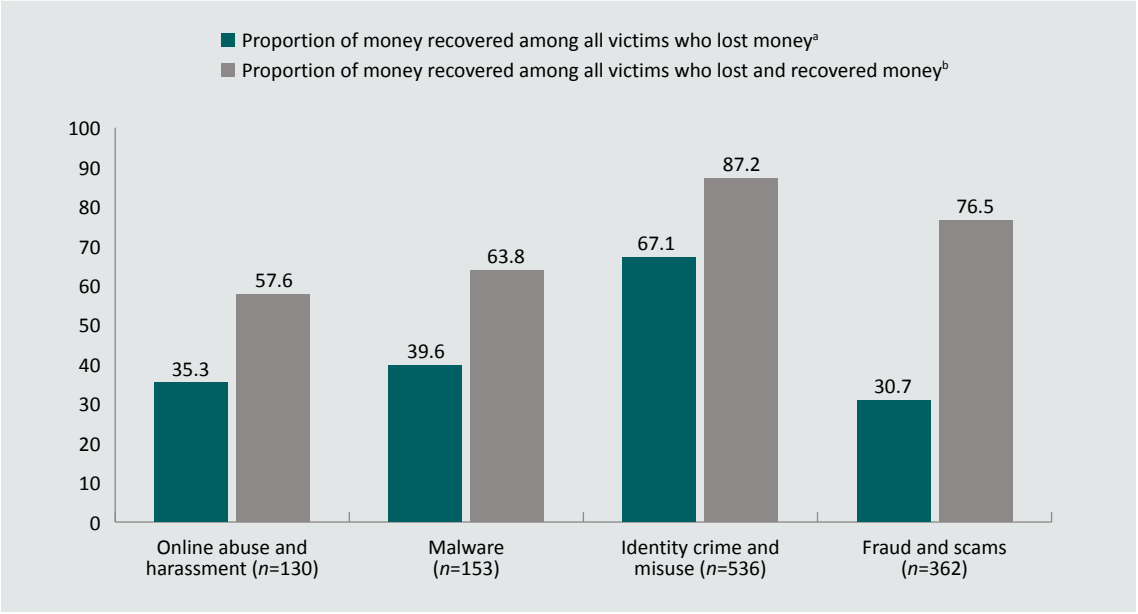


Note: Excludes 2 online abuse and harassment victims, 4 malware victims, 9 identity crime and misuse victims and 3 fraud and scam victims who did not answer whether they had recovered money. Figure only includes victims who lost money directly. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2025 [weighted data]

The average proportion of money lost that was recovered was even lower (Figure 23), ranging from 30.7 percent for fraud and scam victims to 67.1 percent for identity crime and misuse victims. Among those victims who were able to recover money, the average proportion of money lost that was recovered ranged from 57.6 percent for online abuse and harassment victims to 87.2 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 23: Average proportion of money recovered among people who lost money directly and who recovered money, by crime type (%)



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

b: Limited to victims who recovered money and could report how much they recovered: online abuse and harassment *n*=79, malware *n*=95, identity crime and misuse *n*=412, fraud and scams *n*=145

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

Source: Australian Cybercrime Survey 2025 [weighted data]

The median value of losses incurred by victims (through money or cryptocurrency being stolen or payments demanded) was $230 for online abuse and harassment victims, $215 for malware victims, $300 for identity crime victims and $250 for fraud and scam victims. The median amount of money spent dealing with the consequences of the most recent incident was $250 for online abuse and harassment victims, $1,900 for malware victims, $200 for identity crime victims and $150 for fraud and scam victims. The median amount that victims were able to recover was $100 for online abuse and harassment victims, $100 for malware victims, $250 for identity crime victims and $129 for fraud and scam victims.

The total cost per victim was calculated by summing money directly lost and money spent on consequences, then subtracting amounts recovered. The median total cost after recoveries was $300 for online abuse and harassment victims, $200 for malware victims, $300 for identity crime and misuse victims and $180 for fraud and scam victims (Table 16). The mean value was significantly higher for each type of cybercrime, ranging from $946 for malware to $4,214 for online abuse and harassment; 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 for mean values in Table 16; see also Figure 24).

Table 16: Median financial losses for most recent incident among victims who lost any money, by payment method (range)

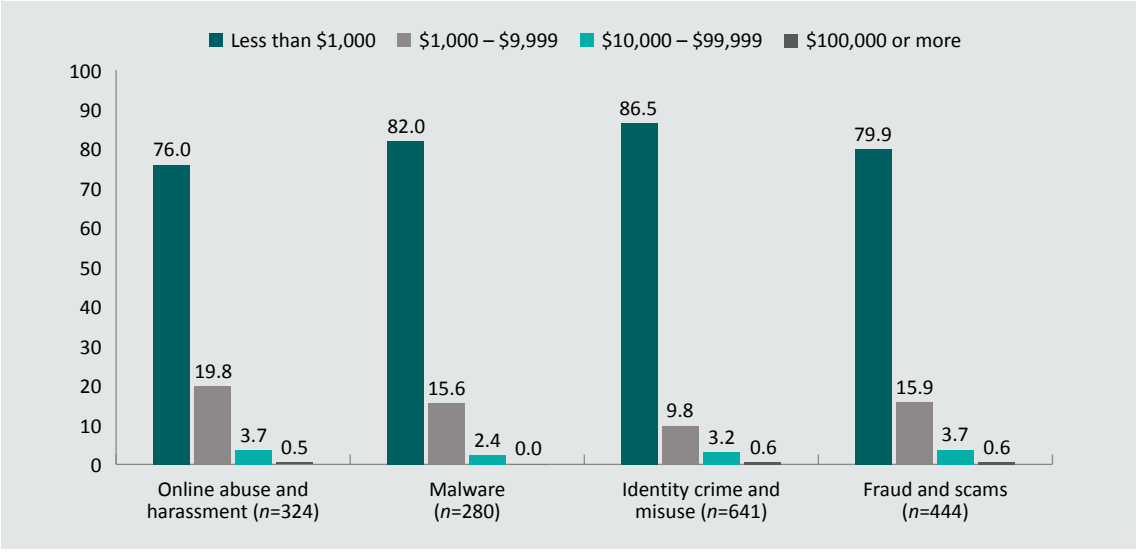
	Online abuse and harassment (*n*=2,589)	Malware (*n*=2,258)	Identity crime (*n*=2,166)	Fraud and scams (*n*=1,196)
Money	$100 ($1–$6,500)	$100 ($1–$15,000)	$250 ($1–$100,000)	$180 ($1–$100,000)
Cryptocurrency	$77 ($1–$22,000)	$60 ($1–$16,000)	$100 ($1–$220,000)	$100 ($1–$220,000)
Gift cards	$56 ($1–$7,000)	$56 ($1–$8,000)	$100 ($1–$5,000)	$70 ($1–$7,384)
Total losses	$230 ($3–$22,000)	$215 ($5–$16,000)	$300 ($1–$220,000)	$250 ($1–$220,000)
Median amount spent on consequences	$250 ($5–$1,000,000)	$190 ($3–$8,650)	$200 ($1–$100,000)	$150 ($3–$30,000)
Median losses from money directly lost and money spent on consequences	$300 ($3–$1,000,000)	$250 ($3–$19,000)	$313 ($1–$220,500)	$250 ($1–$220,000)
Median amount recovered	$100 ($1–$3,000)	$100 ($5–$3,000)	$250 ($1–$23,500)	$129 ($1–$50,000)
Median losses after recoveries	$300 ($0–$1,000,000)	$200 ($0–$19,000)	$300 ($0–$220,500)	$180 ($0–$220,000)
Mean losses after recoveries (SD)	$4,214 ($51,571)	$946 ($2,513)	$1,997 ($13,575)	$3,022 ($16,467)

Note: Excludes 53 online abuse and harassment victims, 25 malware victims, 14 identity crime and misuse victims and 9 fraud and scam victims who did not answer questions about the most recent incident. *SD*=standard deviation

Source: Australian Cybercrime Survey 2025 [weighted data]

The variation in the total amount of money lost after recoveries is illustrated in Figure 24. This excludes victims who were unable to report how much money they had lost. Among those victims who could quantify amounts lost, between 76.0 percent (online abuse and harassment) and 86.5 percent of victims (identity crime and misuse) reported having lost less than $1,000 in the most recent incident. Approximately one-quarter (24.0%) of online abuse and harassment victims, 18.0 percent of malware victims, 13.6 percent of identity crime victims and 20.2 percent of fraud and scam victims lost more than $1,000 in the most recent incident. Four percent of online abuse and harassment victims lost more than $10,000, compared with 4.3 percent of fraud and scam victims, 2.4 percent of malware victims and 3.8 percent of identity crime victims. A small proportion of victims lost more than $100,000 in the most recent incident.

Figure 24: Financial losses after recoveries for most recent incident, by crime type (%)

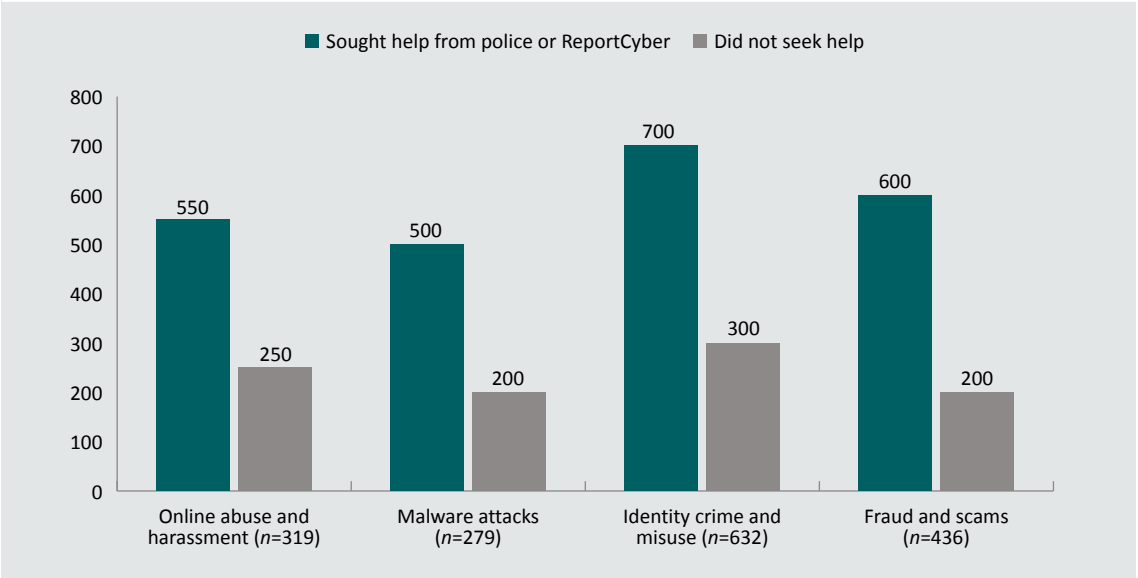


Note: The less than $1,000 category includes respondents who had $0 of financial losses because they recovered the full amount they spent or lost. Limited to victims who reported having lost money or spent money on consequences and who could recall the amounts. Weighted frequencies and percentages may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

Source: Australian Cybercrime Survey 2025 [weighted data]

These results are different to data on the losses from reported cybercrimes (Australian Competition and Consumer Commission 2026; Australian Signals Directorate 2025). There are two main reasons for this. First, there were clear differences between the incidents that were and were not reported to police or ReportCyber in terms of the median financial losses after recoveries (Figure 25). Victims who lost larger amounts of money were more likely to seek help from police or ReportCyber than victims with smaller losses. This was especially true for identity crime and misuse victims (a median of $700 among victims who reported vs $300 among those who did not) and fraud and scam victims ($600 vs $200). 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 25: Median financial losses before recoveries for most recent incident among victims who lost any money, by whether respondent sought help, advice or support from police or ReportCyber ($)



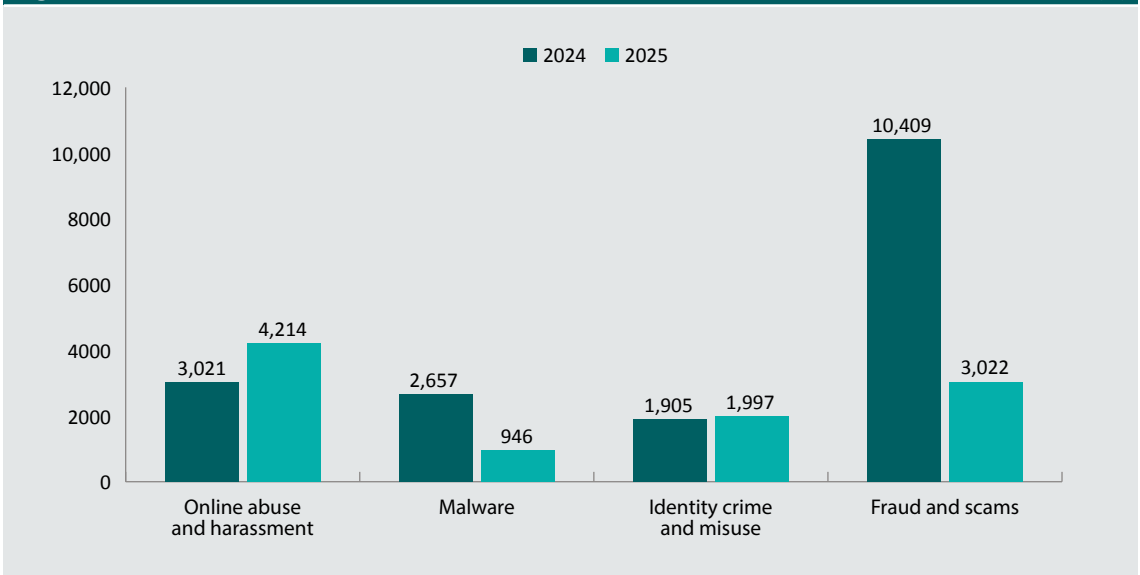
Note: Limited to victims who reported having lost money or spent money on consequences and who could report how much. Does not account for money recovered. Excludes 6 online abuse and harassment victims, 1 malware victim, 8 identity crime and misuse victims and 9 fraud and scam victims who did not know or answer the question about reporting to police or ReportCyber

Source: Australian Cybercrime Survey 2025 [weighted data]

Changes in financial losses

We compared victims in 2024 and 2025 in terms of the mean losses after recoveries and whether they had recovered any money following the most recent incident (Figure 26). We limited this analysis to victims of crime types that were asked about consistently in both years. There were no statistically significant differences between 2024 and 2025 in the mean losses after recoveries for victims of online abuse and harassment ($3,021 vs $4,214), malware attacks ($2,657 vs $946), identity crime and misuse ($1,905 vs $1,997) and fraud and scams ($10,409 vs $3,022). The large difference in the mean losses for fraud and scam victims was due to a small number of large losses in 2024.

Figure 26: Mean financial losses after recoveries for most recent incident, 2024 and 2025 ($)

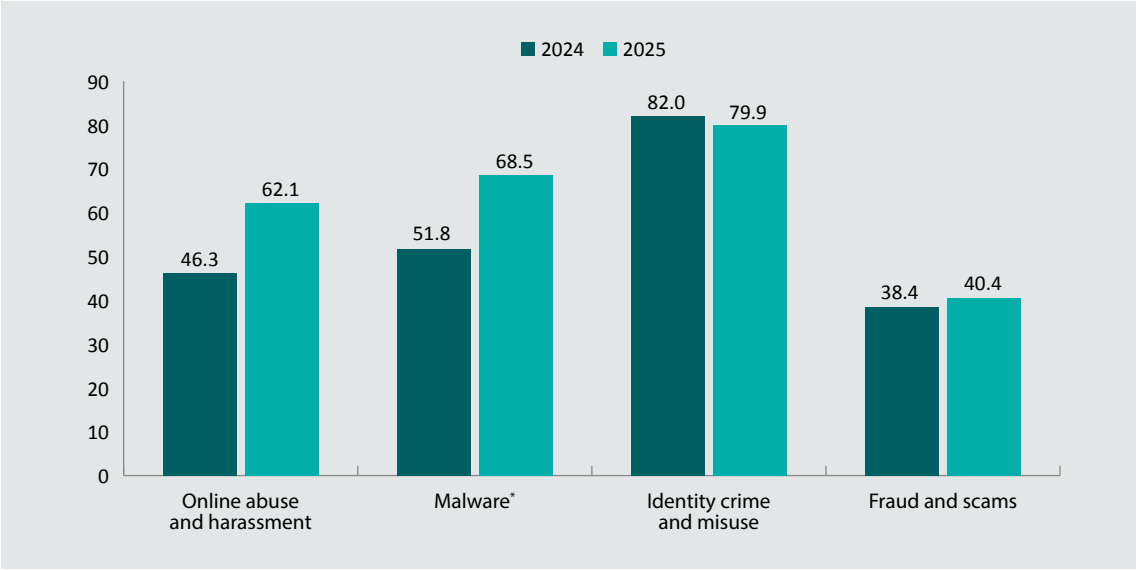


Note: Limited to victims who reported having lost money or spent money on consequences and who could report how much. These numbers vary by crime type and survey year

Source: Australian Cybercrime Survey 2025 [weighted data]

There was an increase in the proportion of malware victims who said they recovered any of the money they lost following their most recent incident (Figure 27), from 51.8 percent in 2024 to 68.5 percent in 2024 ($F(1, 238)=6.99$, $p<0.05$). While the proportion of online abuse and harassment (46.3% vs 62.1%) and fraud and scam (38.4% vs 40.4%) victims who recovered any money was higher in 2025 than in 2024, these differences were not statistically significant. Likewise, there was no difference in the proportion of identity crime and misuse victims who recovered money following the most recent incident (82.0% vs 79.9%).

Figure 27: Proportion of victims who said that they recovered any money following the most recent incident, 2024 and 2025 (%)



*statistically significant at $p<0.05$

Note: Figure only includes victims who lost money directly. These numbers vary by crime type and survey year. Weighted percentages may not add to total due to rounding

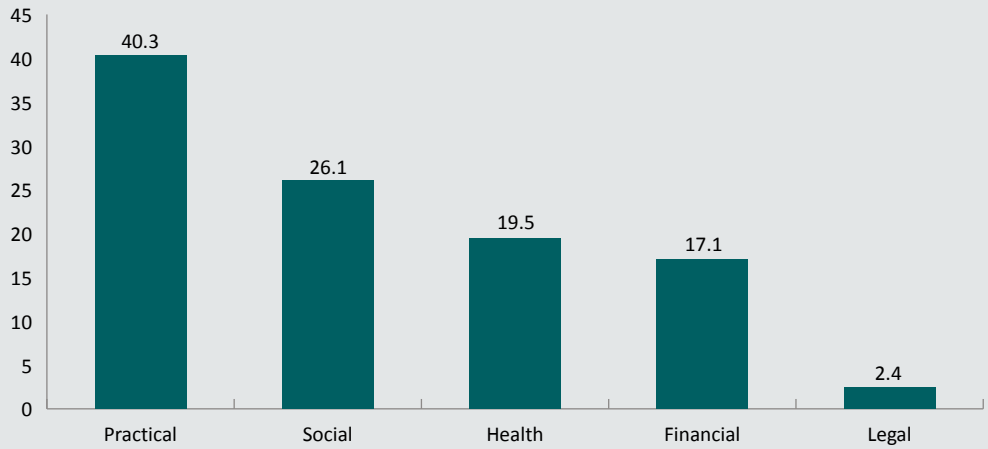
Source: Australian Cybercrime Survey 2025 [weighted data]

Impacts on individual victims

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

Overall, 58.8 percent of cybercrime victims were negatively affected in some way. This means an estimated 26.4 percent of all respondents to the survey were harmed by cybercrime in the 12 months prior to the survey. Forty percent of victims reported practical impacts, over a quarter reported social impacts (26.1%), one in five reported health-related harms (19.5%), and 17.1 percent reported financial problems. Legal issues were comparatively rare (2.4%; Figure 28).

Figure 28: Harms from cybercrime among victims (%) (*n*=4,694)

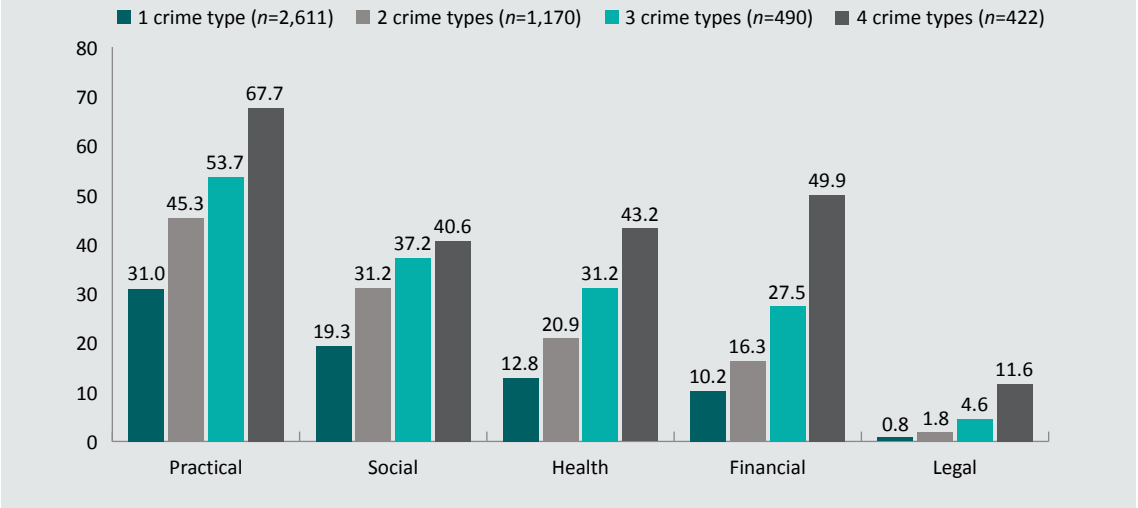


Note: Excludes 128 victims who did not answer this question. Weighted percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2025 [weighted data]

Victims who experienced more than one type of cybercrime in the 12 months prior to the survey were much more likely to report harms than those who experienced only one type (Figure 29). For example, while 31.0 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 (53.7% and 67.7% of victims, respectively). Similarly, 19.3 percent of victims who experienced one type of cybercrime reported social impacts, but this proportion rose to 40.6 percent for those who experienced four types of cybercrime. Compared with victims of one cybercrime type, victims who reported three or more types of cybercrime in the 12 months prior to the survey were more than twice as likely to report health impacts, nearly three times as likely to report financial impacts and more than four times as likely to report legal impacts. 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*=4,822)

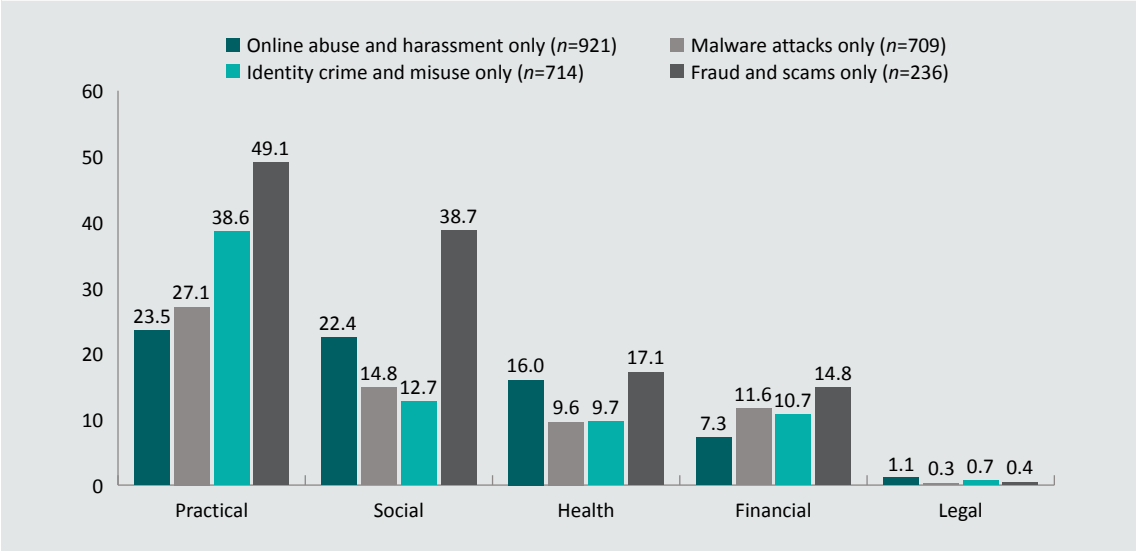


Note: Excludes 128 victims who did not answer this question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2025 [weighted data]

To directly compare harm among victims of different types of cybercrime, it was necessary to limit the analysis to victims who experienced just one type of cybercrime (Figure 30). This eliminates the confounding effects of other types of cybercrime. Fraud and scam victims were the most likely to report experiencing at least one harm in the practical (49.1%), social (38.7%), health (17.1%) and financial (14.8%) domains, while online abuse and harassment victims were the most likely to experience legal impacts (1.1%).

Figure 30: Harms from cybercrime among victims, by crime type (%) (*n*=2,686)



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

Source: Australian Cybercrime Survey 2025 [weighted data]

The most common practical issues victims encountered were difficulty knowing which information to trust online (16.2%); having to change their personal, banking and/or contact information (14.4%); and being less confident using the internet for personal affairs (12.4%; Table 17). For harms within the social domain, 14.3 percent of victims were embarrassed, 10.7 percent lost trust in other people, and 4.8 percent became more socially isolated. For harms within the physical and psychological health domain, 9.8 percent of victims experienced mental or emotional distress, 7.8 percent had difficulty sleeping, and 3.7 percent stated that their physical health and wellbeing had deteriorated. For financial harms, 5.4 percent of victims experienced an increase in financial stress; 4.4 percent had to pay for computer, phone or other hardware repairs or replacement; 3.7 percent had to buy new software; and 3.1 percent had to borrow money from family and friends. Within the legal domain, 1.3 percent of victims had been in trouble with the police and 1.2 percent had to commence legal action.

Table 17: Harms to individual cybercrime victims (*n*=4,694)		
	n	%
Practical impacts		
Respondent found it harder to know which information to trust online	758	16.2
Respondent had to change personal, banking and/or contact information	677	14.4
Respondent was less confident using the internet for personal affairs (eg banking, purchasing items)	583	12.4
Respondent's studies were negatively impacteda	6	5.8
Respondent had difficulty accessing online accounts and resources (eg bank accounts, utilities, email)	188	4.0
Respondent's work was negatively impactedb	99	3.2
Respondent had problems communicating with people (eg friends, family, employer)	144	3.1
Respondent lost important or sentimental data (eg photos, contact details, files)	129	2.7
Respondent had to take time off work to deal with the consequences of victimisationb	115	2.5
Respondent had problems communicating or dealing with government departments	117	2.5
Respondent had problems communicating or dealing with businesses	100	2.1
Respondent had to change their place of residence	67	1.4
Social impacts		
Respondent was embarrassed	670	14.3
Respondent lost trust in other people	502	10.7
Respondent became more socially isolated	224	4.8
Respondent stated their relationships with family and friends had been negatively impacted	149	3.2
Respondent felt their reputation was damaged	144	3.1
Respondent stated their relationship with their partner had been negatively impactedc	76	2.7
Health impacts		
Respondent experienced mental or emotional distress	459	9.8
Respondent experienced difficulty sleeping	365	7.8
Respondent stated their overall physical health and wellbeing had deteriorated	172	3.7
Respondent had to seek psychological or counselling treatment	130	2.8
Respondent increased their consumption of alcohol	115	2.4
Respondent had to seek medical treatment	84	1.8
Respondent increased their consumption of drugs (legal or illegal)	70	1.5

Table 17: Harms to individual cybercrime victims (*n*=4,694) (cont.)		
	n	%
Financial impacts		
Respondent experienced an increase in financial stress	255	5.4
Respondent had to pay for computer, phone or other hardware repairs or replacement	207	4.4
Respondent had to buy new software	175	3.7
Respondent had to borrow money from family and friends	147	3.1
Respondent had to buy new backup data storage or data storage devices	136	2.9
Respondent was unable to get a loan when they needed one	81	1.7
Respondent increased the amount of time and/or money they spent gambling (in person or online)	73	1.6
Respondent lost their job	54	1.2
Legal impacts		
Respondent had been in trouble with the police	59	1.3
Respondent had to commence legal action	57	1.2

a: Only includes victims who were currently studying full time (*n*=95)

b: Only includes victims who were currently working (*n*=3,100)

c: Only includes victims who were in a current relationship (*n*=2,868)

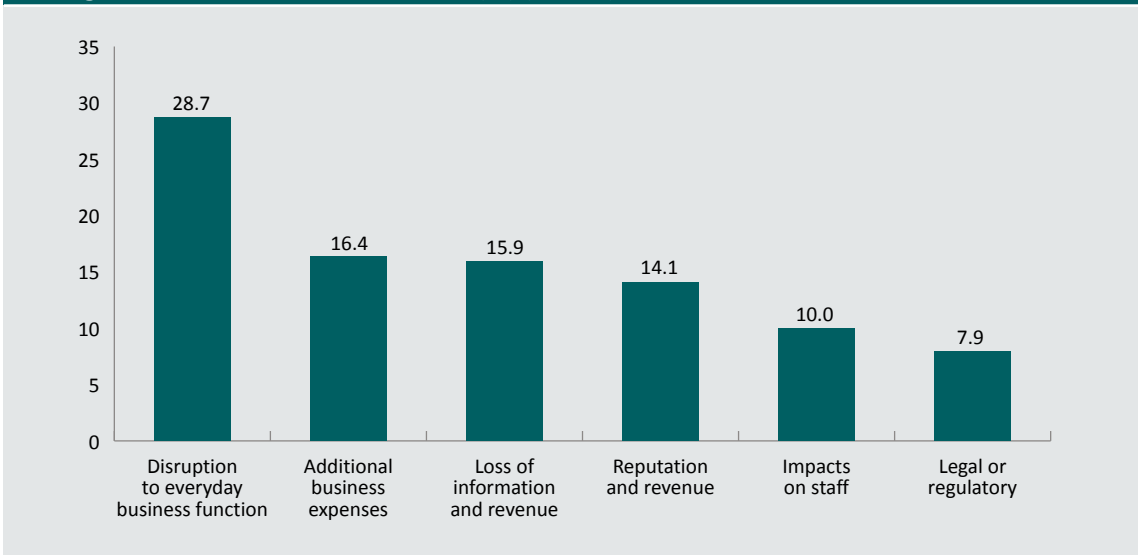
Note: Excludes 128 victims who did not answer this question. Weighted percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2025 [weighted data]

Impacts on small to medium businesses

Forty-seven 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 25.0 percent of all small to medium business owners, operators or managers who responded to the survey had their business affected by cybercrime in some way in the 12 months prior to the survey. These impacts include disruption to everyday business function (28.7%), additional business expenses (16.4%), loss of information (15.9%), impacts on their reputation or revenue (14.1%), impacts on staff (10.0%) and legal or regulatory ramifications (7.9%; Figure 31).

Figure 31: Harms to business from cybercrime among victims who owned, operated or managed a small to medium business (%) (*n*=770)



Note: Excludes 57 small to medium business owners, operators and managers who did not answer this question. Weighted percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2025 [weighted data]

Small to medium business owners, operators and managers reported a variety of impacts on their business (Table 18). Most commonly, they experienced disruption to operations and/or trading, such as the inability to carry out transactions and websites not functioning (7.7%); having to spend time repairing and improving systems (6.9%); having to buy new software (6.3%); and having difficulty accessing online accounts and resources like bank accounts, utilities and email (5.9%).

Table 18: Harms to small business owners, operators and managers who were victims of cybercrime (*n*=770)		
	n	%
Disruption to everyday business function		
Disruption to operations and/or trading (eg inability to carry out transactions, websites not functioning)	60	7.7
The business spent time repairing and improving systems	53	6.9
Difficulty accessing online accounts and resources (eg bank accounts, utilities, email)	45	5.9
Had to change the business banking and/or contact information	43	5.5
Had to shut down the business online store or website (temporarily or permanently)	39	5.1
Had problems communicating or dealing with businesses	37	4.8
Blocked customer access to the business online store or website	36	4.7
Had problems communicating or dealing with government departments	35	4.5
Additional business expenses		
Had to buy new software	49	6.3
Insurance premiums were increased	42	5.5
Had to pay for computer, phone or other hardware repairs or replacement	40	5.2
Had to buy new backup data storage or data storage devices	35	4.5
Loss of information		
The business had to notify affected parties of a data breach	42	5.4
Theft of my information or other staff information (eg contact details, financial data)	41	5.3
Theft of intellectual property or corporate information	35	4.5
Theft of customer or supplier information (eg contact details, financial data)	31	4.0
Reputation and revenue		
We lost business contracts	38	4.9
Professional relationships were damaged	36	4.7
There was a loss of customers, sales or revenue	34	4.5
The business reputation was damaged	32	4.2
Impacts on staff		
Employees/owners of the business had to take time off work	41	5.3
Employees/owners of the business resigned or lost their job	39	5.0
Legal or regulatory sanctions		
There was litigation or legal action against the business	41	5.3
The business was hit with fines and regulatory sanctions	25	3.2

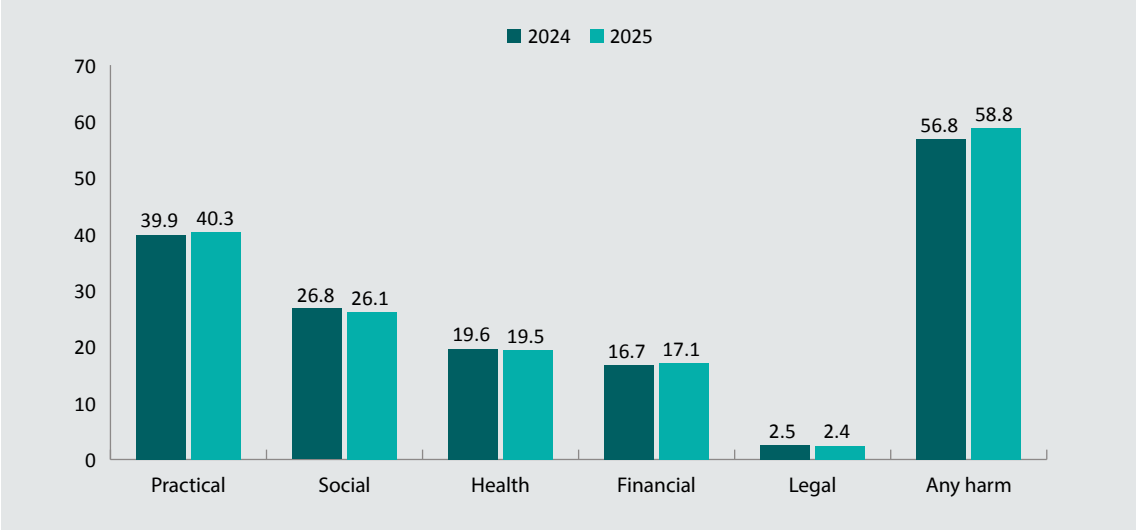
Note: Excludes 57 small to medium business owners, operators and managers who did not answer this question. Weighted frequencies and percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2025 [weighted data]

Changes in harm to individuals and small businesses

As shown in Figure 32, there were no statistically significant differences between 2024 to 2025 in the proportion of victims experiencing any type of harm or any harm overall.

Figure 32: Harms from cybercrime among victims, 2024 and 2025 (%)



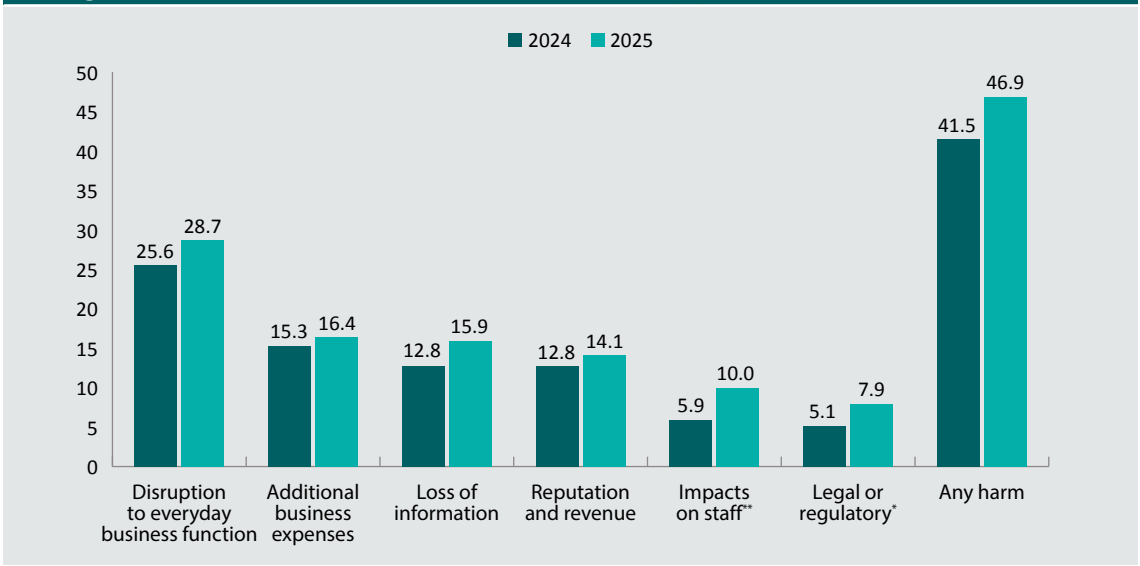
Note: Excludes 151 victims in 2024 and 128 victims in 2025 who did not answer this question. Weighted percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2025 [weighted data]

The prevalence of harms to business among victims who owned, operated or managed a small to medium business in 2025 was compared with results from the 2024 survey (Figure 33). The proportion of victims who owned, operated or managed a small to medium business who reported impacts on their staff increased (5.9% in 2024 vs 10.0% in 2025; $F(1, 1{,}590)=9.49$, $p<0.01$), as did the proportion who experienced legal or regulatory issues (5.1% in 2024 vs 7.9% in 2025; $F(1, 1{,}590)=5.51$, $p<0.05$). The increase in the proportion who reported any harm (41.5% in 2024 vs 46.9% in 2025) was not statistically significant.

The increase in impacts to staff appears to be driven by growth in the proportion who said employees or owners of the business resigned or lost their job (2.4% in 2024 vs 5.0% in 2025; $F(1, 1{,}590)=58.36$, $p<0.01$), while the increase in legal or regulatory issues appears to be driven by the larger number of victims who experienced litigation or legal action against their business (2.6% in 2024 vs 5.3% in 2025; $F(1, 1{,}590)=8.12$, $p<0.01$).

Figure 33: Harms to business from cybercrime among victims who owned, operated or managed a small to medium business, 2024 and 2025 (%)



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

Note: Excludes 48 small to medium business owners, operators and managers in 2024 and 57 small to medium business owners, operators and managers in 2025 who did not answer this question. Weighted percentages may not add to total due to rounding

Source: Australian Cybercrime Survey 2025 [weighted data]

References

URLs correct as at April 2026

auDA 2025. *Digital lives of Australians 2025*. https://www.auda.org.au/news-insights/research-reports/digital-lives-of-australians/

Australian Banking Association 2023. Banks unite to declare war on scammers. https://www.ausbanking.org.au/new-scam-safe-accord/

Australian Bureau of Statistics (ABS) 2026. National, state and territory population, September 2025. https://www.abs.gov.au/statistics/people/population/national-state-and-territory-population/latest-release

Australian Bureau of Statistics 2025. Crime victimisation, 2023–24 financial year. https://www.abs.gov.au/statistics/people/crime-and-justice/crime-victimisation/2023-24

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

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

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

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

Australian Communications and Media Authority 2025. Action on scams, spam and telemarketing. https://www.acma.gov.au/action-spam-and-telemarketing

Australian Competition and Consumer Commission 2026. *Targeting scams: Report of the National Anti-Scam Centre on scams data and activity 2025.* Canberra: Australian Competition and Consumer Commission. https://www.scamwatch.gov.au/research-and-resources/targeting-scams-report/targeting-scams-report-of-the-national-anti-scam-centre-on-scams-data-and-activity-2025

Australian Cyber Security Centre (ACSC) 2026. *Guidelines for cyber security incidents*. https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cybersecurity-incidents

Australian Human Rights Commission 2025. *Guidelines on equal access to digital goods and services.* Sydney: Australian Human Rights Commission. https://humanrights.gov.au/?a=47358

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

Australian Signals Directorate 2025. *Annual cyber threat report, July 2024 to June 2025.* Canberra: Australian Signals Directorate. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025

Boxall H & Morgan A 2021. *Intimate partner violence during the COVID-19 pandemic: A survey of women in Australia.* Sydney: Australia's National Research Organisation for Women's Safety (ANROWS). https://www.aic.gov.au/publications/special/special-11

Bumble nd. Guidelines. https://bumble.com/en-au/guidelines

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

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

Deloitte 2025. *Media and entertainment consumer insights 2025*. https://www.deloitte.com/au/en/Industries/tmt/research/media-and-entertainment-consumer-insights.html

Department of Home Affairs 2022. *National Plan to Combat Cybercrime*. https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime/2022-national-plan-to-combat-cybercrime

Emerson E, Fortune N, Llewellyn G & Stancliffe R 2020. Loneliness, social support, social isolation and wellbeing among working age adults with and without disability: Cross-sectional study. *Disability and Health Journal* 14(1): 100965. https://doi.org/10.1016/j.dhjo.2020.100965

eSafety Commissioner 2020. *Online safety for young people with intellectual disability.* https://www.esafety.gov.au/research/online-safety-for-young-people-with-intellectual-disability

Instagram 2026. Nudity protection in chats on Instagram. https://help.instagram.com/503437025160040/

Koebert J 2026. 2025 antivirus statistics and consumer report, 75% of users say antivirus protection is effective at keeping them safe. All About Cookies. https://allaboutcookies.org/antivirus-protection-survey

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

Lam J 2022. Neighborhood characteristics, neighborhood satisfaction, and loneliness differences across ethnic–migrant groups in Australia. *Journals of Gerontology* 77(11): 2113–2125. https://doi.org/10.1093/geronb/gbab219

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

Ngo F 2024. Cybercrime victims who aren't proficient in English are undercounted – and poorly protected. *The Conversation*, 30 January. https://theconversation.com/cybercrime-victims-who-arent-proficient-in-english-are-undercounted-and-poorly-protected-207466

Nicholson J, Coventry L & Briggs P 2019. "If it is important it will be a headline": Cybersecurity information seeking in older adults. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3290605.3300579

Office of the Australian Information Commissioner 2023. *Australian Community Attitudes to Privacy Survey*. https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023

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

Pennay D, 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

Qantas 2025. *Update on Qantas cyber incident: Wednesday 9 July 2025.* Media release, 9 July. https://www.qantasnewsroom.com.au/media-releases/update-on-qantas-cyber-incident-wednesday-9-july-2025

Rishworth A & Rowland M 2024. *New online dating industry code now in place*. Media release, 5 July. https://ministers.dss.gov.au/media-releases/15161

Scamwatch nd. Chinese authority scams. https://www.scamwatch.gov.au/types-of-scams/threat-scams/chinese-authority-scams

Stringer C & Michailova S 2019. *Understanding the exploitation of temporary migrant workers: A comparison of Australia, Canada, New Zealand and the United Kingdom*. Report prepared for the Ministry of Business, Innovation and Employment, New Zealand. https://www.mbie.govt.nz/dmsdocument/7110-understanding-the-exploitation-of-temporary-migrant-workers-a-comparison-of-australia-canada-new-zealand-and-the-united-kingdom

Victoria Police 2025. Fake authority scams targeting the Chinese community. https://www.police.vic.gov.au/scams-targeting-mandarin-speaking-community

Voce I & Morgan A 2025a. *Cybercrime in Australia 2024.* Statistical Report no. 53. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sr77918

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

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

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

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

Xing T et al. 2020. Vulnerability to fraud among Chinese older adults: Do personality traits and loneliness matter? *Journal of Elder Abuse & Neglect* 32(1): 46–59. https://doi.org/10.1080/08946566.2020.1731042

Yeager DS et al. 2011. Comparing the accuracy of RDD telephone surveys and internet surveys conducted with probability and non-probability samples. *Public Opinion Quarterly* 75(4): 709–47. https://doi.org/10.1093/poq/nfr020

Appendix: Survey design, sampling and weighting

This appendix describes the methodology of a survey of 10,593 Australians aged 18 years and over about their experience of cybercrime. It was prepared with input from Roy Morgan. The aim of this survey was to measure the prevalence and characteristics of cybercrime, risk factors, help-seeking behaviour, financial losses and other harms from victimisation.

Key definitions

Cybercrime

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

Cyber-dependent crime

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

Cyber-enabled crime

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

Cybersecurity

Cybersecurity is defined by the Australian Cyber Security Centre (2026: 1) 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 affecting the Australian community, the AIC ran the inaugural Australian Cybercrime Survey (ACS) in 2023. This is an annual survey which involves several components. There is a core survey of at least 10,000 respondents which measures cybercrime victimisation, financial losses, harms and help-seeking behaviour. A minimum of three addenda each year address priority issues of interest. There is also a longitudinal component involving a cohort of approximately 3,000 respondents which measures repeat victimisation and provides an opportunity to test the efficacy of intervention strategies and legislative changes aimed at reducing cybercrime victimisation or increasing online safety and help-seeking.

Core survey

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

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

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

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

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

Following internal user testing, the survey was piloted from 19 to 22 May 2025 with a sample of 69 respondents from the Roy Morgan Single Source panel, which allowed design issues to be identified and addressed. All steps were taken to ensure the data collected were as accurate as possible.

Research ethics

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

Sampling and weighting

The survey was conducted between 27 May and 1 July 2025 by Roy Morgan using their Single Source panel and three highly regarded panels managed by PureProfile, Dynata and Octopus. These panels are opt-in panels and members were recruited through various means. The survey was sent to members of these online panels aged 18 years and over, in accordance with the sampling method described below. Panel members were invited to participate in the research and were provided with a small reward.

Proportional quota sampling was used, which is the non-probability version of stratified random sampling. Quotas were set based on known population characteristics—age, gender and usual place of residence—and participants were invited to complete the survey until these quotas were reached, within an agreed margin of error. Roy Morgan based these target populations on latest Australian Bureau of Statistics (ABS) figures for Australians aged 18 years or over (ABS 2026). 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 invited 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. Most respondents (52.8%) were recruited from this panel. PureProfile panel members accounted for 41.8 percent of respondents, and the remaining 5.5 percent came from Octopus.

Participants were invited until the relevant quotas had been reached. Data on completion rates were available for the Roy Morgan Single Source panel (Table A1). Overall, 122,546 members of the Roy Morgan Single Source panel were invited to participate; however, there is no way of verifying how many of these invitations were received. A total of 10,330 invitations were opened (8.4%), meaning that the respondent proceeded to the survey landing page. Of these, 1,683 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 2,844 respondents (2.3%) 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 (0.2%) 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 completion time of seven minutes was used to eliminate these responses, while manual checks were conducted on responses that met this threshold.

The raw completion rate for invitations sent to Roy Morgan Single Source panel members, which offers a relatively simple measure of responses to online surveys drawn from non-probability panels (Callegaro & DiSogra 2008), was 4.6 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, 54.1 percent of people who opened the invitation, and 64.6 percent of those who opened the invitation and were eligible to participate in the research, went on to complete the survey. The latter is a particularly useful measure because it accounts for invitations that were received by eligible potential respondents and the response to the survey by respondents who were aware of what they were being invited to undertake. Importantly, partially completed surveys include those where the respondent closed the survey without indicating whether or not they consented to participate.

The final sample size was 10,593 respondents. Under five percent of respondents (3.3%) who completed the survey took over an hour to do so, which usually indicates they completed the survey over multiple sessions (ie saved their answers and returned to it later). Among those who completed the survey in less than one hour, the survey took respondents an average of 23.0 minutes (*SD*=11.4) to complete.

Table A1: Invitation and completion rates, Roy Morgan Single Source panel (unadjusted)

	n	%
Total invitations sent out (T)	122,546	–
Total who did not start survey (NS)	109,578	89.4
Total who started survey (S)	10,330	8.4
Complete surveys (I)	5,590	4.6
Partial surveys (P)	2,844	2.3
Screened out or quota reached (SQ)	1,683	1.4
Previously responded or poor quality (DQ)	213	0.2
Non-participation rate (NS)/(T)	–	89.4
Completion rate for accepted invitations by eligible respondents (I)/(S−SQ)	–	64.6
Completion rate (I)/(T)	–	4.6

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 ABS demographic data and survey respondents, prior to weighting, are presented in Table A2. Western Australian residents were slightly under-represented in the survey data (10.9% vs 10.5), while residents of Victoria (25.7% vs 26.1%) and the Australian Capital Territory (1.8% vs 2.3%) were slightly over-represented.

Table A2: Respondents by usual place of residence (unweighted data)

	Survey respondents (*n*=10,593)		ABS demographic statistics[a]
	n	%	%
NSW	3,299	31.1	31.3
Vic	2,759	26.1	25.7
Qld	2,131	20.1	20.3
WA	1,116	10.5	10.9
SA	747	7.1	7.0
Tas	233	2.2	2.2
ACT	247	2.3	1.8
NT	61	0.6	0.9

a: Estimated resident population at September 2025; ABS 2026

Note: Percentages may not total 100 due to rounding

Source: ABS 2026; Australian Cybercrime Survey 2025 [computer file]

It is not possible to estimate design weights for non-probability panels because the probability of an individual opting in to the panel is unknown (Pennay et al. 2018). Post-stratification weights were applied to reduce non-coverage errors and ensure the data were representative of the spread of the wider population. The data were weighted using a multi-tiered system. Weights were calculated by first comparing the sample with the proportion of the population in each age group in each state and territory according to the ABS (2026) estimate of residential population. Random iterative method weighting was then applied to each record based on educational attainment, frequency of internet use, and social media use. These weights were calculated from Roy Morgan's Single Source survey, which is a nationally representative survey conducted with 50,000 Australians over 50 weeks each year. This weighting corrects for the propensity of non-probability panels to have respondents who are more highly educated and more frequent users of the internet and social media than the norm in the general population. Weights were assigned using a program to run multiple iterations to achieve the best result. Under-represented categories were assigned a multiplier larger than one, and over-represented categories were assigned a multiplier smaller than one. Cap weights were applied to avoid heavy weighting being applied to a small group of respondents. The effective sample size for the study after weighting (the weighted sample size) was 10,593 respondents.

Table A3 shows the effect of weighting on the concordance between the adult population in each state and territory according to the ABS (2026) and the weighted sample. There was a high degree of concordance overall.

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

	ABS demographic statistics[a]	Survey respondents (*n*=10,593)
NSW	31.3	30.9
Vic	25.7	25.8
Qld	20.3	20.4
WA	10.9	11.0
SA	7.0	7.1
Tas	2.2	2.1
ACT	1.8	2.1
NT	0.9	0.6

a: Estimated resident population at September 2025; ABS 2026
Note: Percentages may not total 100 due to rounding
Source: ABS 2026; Australian Cybercrime Survey 2025 [computer file]

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

Table A4: Respondents by age (%)

	ABS demographic statistics[a]	Survey respondents (*n*=10,593)	
		Unweighted	Weighted
18–24	11.5	9.6	11.4
25–34	18.8	18.1	18.8
35–49	25.5	26.4	25.6
50–64	22.2	23.0	21.9
65+	22.0	23.0	22.3

a: Estimated resident population at September 2025; ABS 2026
Source: ABS 2026; Australian Cybercrime Survey 2025 [computer file]

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

Results from this comparison demonstrate a relatively high degree of concordance between ACS respondent characteristics and ABS demographic data for gender (51.3% female in the ACS vs 50.8% in the general population), Aboriginal and Torres Strait Islander status (4.1% vs 3.1%) and usual place of residence (remoteness, 74.2% metropolitan in the ACS vs 72.6% in the general population).

The most significant differences emerged in relation to the presence of a disability and the proportion of respondents with a non-English-speaking background. Differences in non-English-speaking backgrounds are largely explained by the differences in how this was measured. Respondents to the ACS were asked to nominate the language they spoke most often at home. ABS Census participants are asked what languages they speak at home, rather than the language spoken most often (ABS 2022a). That said, ACS respondents were slightly less likely than the general population to say they were born overseas (22.8% vs 27.6%), suggesting that the difference may not be fully explained by the different measurements. It may also reflect reduced participation due to language barriers among those with lower English proficiency.

Relatedly, the ACS relies on a similar definition to the ABS Short Disability Module, and defines disability as a long-term health condition that is expected to last for longer than six months and which restricts everyday activities (Australian Institute of Health and Welfare 2022). The health conditions question is simplified and is not directly comparable to ABS data on long-term or chronic health conditions measured in the National Health Survey (ABS 2022b). Similarly, there are limitations to this method in terms of producing reliable data on disability prevalence, compared with the comprehensive set of questions used in the ABS Survey of Disability, Ageing and Carers to measure disability (Australian Institute of Health and Welfare 2022). The latter serves as the benchmark in Table A6. These issues aside, it appears respondents with a disability are under-represented within the ACS (11.8% vs 17.7%).

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

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

	ABS/AIHW statistics	Survey respondents
Female[a]	50.8	51.3
Aboriginal and/or Torres Strait Islander[b]	3.1	4.1
Non-English-speaking background[c]	22.3	6.1
Born overseas[d]	27.6	22.8
Disability[e]	17.7	11.8
Usual place of residence[f]		
Major cities	72.6	74.2
Regional	25.5	23.0
Remote	1.9	2.5

a: Proportion of estimated residential population as at September 2025 who were female based on sex ratio (ABS 2026)

b: Projected resident Aboriginal and Torres Strait Islander population as proportion of persons aged 18 years and over in 2024 (ABS 2024a). Denominator for survey respondents includes 117 respondents who did not know or declined to answer this question

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

d: Proportion of Australians who were born overseas (ABS 2022a). Denominator for survey respondents includes 31 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 553 respondents who did not know or declined to answer this question

f: Estimated resident population, by remoteness areas in 2023 (ABS 2024b). Denominator for survey respondents includes 33 respondents where this information was unknown

Source: ABS (various); Australian Institute of Health and Welfare (2022); Australian Cybercrime Survey 2025 [computer file]

Characteristics of 2025 sample and comparison to the 2024 sample

Table A6 displays the sociodemographic characteristics of respondents in the 2025 ACS. In 2025, 30.6 percent of respondents were aged 18 to 34 years, 47.5 percent were aged 35 to 64 years, and 21.9 percent of respondents were aged 65 years and over. While 48.2 percent of the sample were male and 51.3 percent were female, 0.5 percent of respondents identified as non-binary or a different gender. First Nations people accounted for 4.1 percent of respondents, while 9.3 percent of respondents identified as LGB+. One in five respondents were born outside of Australia (22.8%), while 6.1 percent spoke a language other than English most often at home. One in 10 respondents reported having a long-term health condition that restricted their everyday activities or meant they required help or supervision (11.8%).

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. While the survey is not a nationally representative sample, it is largely representative of the Australian population in terms of key demographics.

We also compared the samples in 2024 and 2025 to help inform decisions about how best to compare results from the two surveys (Table A6). There were statistically significant differences between the 2024 and 2025 ACS samples in terms of whether respondents were not First Nations (94.3% vs 94.8%) and currently in a relationship (60.1% vs 61.6%).

Table A6: Sociodemographic characteristics of respondents, 2024 and 2025				
	2024 (*n*=10,335)		2025 (*n*=10,593)	
	n	%	*n*	%
State/territory				
NSW	3,182	30.8	3,274	30.9
Vic	2,676	25.9	2,735	25.8
Qld	2,108	20.4	2,164	20.4
WA	1,122	10.9	1,165	11.0
SA	753	7.3	747	7.1
Tas	223	2.2	226	2.1
ACT	237	2.3	221	2.1
NT	33	0.3	61	0.6
Age				
18–24	1,203	11.6	1,203	11.6
25–34	1,962	19.0	1,962	19.0
35–49	2,624	25.4	2,624	25.4
50–64	2,283	22.1	2,283	22.1
65+	2,262	21.9	2,262	21.9
Gender				
Female	5,183	50.2	5,439	51.3
Male	5,086	49.2	5,102	48.2
Non-binary	66	0.6	53	0.5
First Nations*				
Yes	420	4.1	436	4.1
No	9,741	94.3	10,040	94.8
Unknown	174	1.7	117	1.1
LGB+ respondents				
Yes	947	9.2	982	9.3
No	9,215	89.2	9,450	89.2
Unknown	173	1.7	161	1.5
Born outside of Australia				
Yes	2,302	22.3	2,413	22.8
No	7,980	77.2	8,148	76.9
Unknown	52	0.5	31	0.3

Table A6: Sociodemographic characteristics of respondents, 2024 and 2025 (cont.)				
	2024 (*n*=10,335)		2025 (*n*=10,593)	
	n	%	*n*	%
Speaks a language other than English most often at home				
Yes	620	6.0	646	6.1
No	9,677	93.6	9,909	93.5
Unknown	38	0.4	38	0.4
Restrictive long-term health condition				
Yes	1,140	11.0	1,246	83.0
No	8,708	84.3	8,793	11.8
Unknown	486	4.7	553	5.2
Currently in a relationship*				
Yes	6,210	60.1	6,525	61.6
No	4,038	39.1	4,011	37.9
Unknown	87	0.8	57	0.5
Children living at home[a]				
Yes	2,693	26.1	2,896	27.3
No	7,569	73.2	7,623	72.0
Unknown	73	0.7	74	0.7
Usual place of residence (remoteness)				
Major city	7,595	73.5	7,862	74.2
Regional	2,423	23.4	2,433	23.0
Remote	284	2.8	264	2.5
Unknown	33	0.3	33	0.3

*statistically significant at $p<0.05$
a: Children under the age of 18 years
Note: Weighted frequencies and percentages may not add to total due to rounding
Source: Australian Cybercrime Survey 2025 [weighted data]

Table A7 displays information on the education and employment status of respondents in 2025 and how they compare to the 2024 sample. Just under one-third of respondents (30.9%) said their highest level of education was high school, while 42.4 percent of respondents had a university qualification. Two-thirds of respondents (63.5%) were employed either full or part time, 21.1 percent of respondents were retired and 5.3 percent were unemployed.

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

There were statistically significant differences between the two samples in terms of their employment, with slightly fewer respondents in 2025 working full time (43.7% vs 42.1%) and slightly more being retired (20.2% vs 21.2%) or unemployed (4.5% vs 5.3%).

Table A7: Education, employment and income of respondents, 2024 and 2025				
	2024 (*n*=10,335)		2025 (*n*=10,593)	
	n	%	*n*	%
Highest education level				
Year 12 or below	3,181	30.8	3,277	30.9
Vocational qualification	2,846	27.5	2,761	26.1
University graduate	4,245	41.1	4,486	42.4
Unknown	62	0.6	68	0.6
Employment status*				
Working full time	4,518	43.7	4,464	42.1
Working part time, casual or semi-retired	2,187	21.2	2,268	21.4
Retired	2,087	20.2	2,237	21.1
Unemployed	460	4.5	564	5.3
Full-time homemaker or carer	418	4.1	428	4.0
Student full time (and not working)	163	1.6	176	1.7
Not working for health reasons	366	3.5	365	3.5
Unknown	134	1.3	91	0.9
Owns, operates or works for a small to medium enterprise (SME)				
Owner or manager	1,532	14.8	1,447	13.7
Employee	1,789	17.3	1,851	17.5
Does not operate or work for an SME	3,279	31.7	3,328	31.4
Not currently working	3,629	35.1	3,860	36.4
Unknown	105	1.0	107	1.0
Owns, operates or works for a large company or business				
Owner or executive	462	4.5	428	4.0
Employee	1,840	17.8	1,927	18.2
Does not operate or work for a large company	4,268	41.3	4,224	39.9
Not currently working	3,629	35.1	3,860	36.4
Unknown	136	1.3	153	1.5

Table A7: Education, employment and income of respondents, 2024 and 2025 (cont.)				
	2024 (*n*=10,335)		2025 (*n*=10,593)	
	n	%	*n*	%
Annual income[a]				
$0 – $18,200	294	4.4	271	4.0
$18,201 – $45,000	919	13.7	882	13.1
$45,001 – $120,000	3,423	51.1	3,420	50.8
$120,001 – $180,000	1,120	16.7	1,237	18.4
$180,001 and over	495	7.4	506	7.5
Unknown	454	6.8	417	6.2

*statistically significant at $p<0.05$
a: Data limited to respondents who were currently working (*n*=6,706 in 2024, *n*=6,732 in 2025)
Note: Weighted frequencies and percentages may not add to total due to rounding
Source: Australian Cybercrime Survey 2025 [weighted data]

Table A8 presents information on the online behaviour of respondents in the 2025 ACS and how it compares to 2024. In 2025, more than half of respondents (56.8%) said they spent more than three hours a week using social media, while more than three-quarters of respondents (78.1%) said they used the internet three or more times a day. When asked to rate their knowledge of technology, half the respondents rated their knowledge of technology as moderate (49.4%), a third (32.7%) said it was high or very high, and 16.8 percent rated their knowledge of technology as low or very low.

There were statistically significant differences between the samples for the 2024 and 2025 ACS in terms of respondents' internet and social media use, with more respondents in 2025 saying they use social media between three and eight hours a week (26.8% vs 35.8%) and they use the internet twice a day (7.1% vs 11.8%) as opposed to less frequently.

Table A8: Online behaviour of respondents, 2024 and 2025				
	2024 (*n*=10,335)		2025 (*n*=10,593)	
	n	%	*n*	%
Social media use* **				
No social media use	1,466	14.2	1,313	12.4
Up to 3 hours per week	2,997	29.0	2,384	22.5
Between 3 and 8 hours a week	2,771	26.8	3,787	35.8
More than 8 hours a week	3,101	30.0	3,109	29.3
Internet use* **				
A few times a week or less	528	5.1	401	3.8
Once a day	999	9.7	607	5.7
Twice a day	737	7.1	1,249	11.8
Three or more times a day	8,071	78.1	8,337	78.7
Self-rated knowledge of technology				
Very low	390	3.8	374	3.5
Low	1,347	13.0	1,368	12.9
Moderate	5,102	49.4	5,239	49.5
High	2,471	23.9	2,591	24.5
Very high	907	8.8	933	8.8
Unknown	118	1.1	89	0.8

***statistically significant at $p<0.001$
Note: Weighted frequencies and percentages may not add to total due to rounding
Source: Australian Cybercrime Survey 2025 [weighted data]

Analysis

Comparisons between groups

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

Comparisons over time

We used the same online panels and recruitment method for the 2025 survey that we used in 2024. We recruited an entirely new sample of respondents (ie nobody in the main sample completed both the 2024 and 2025 survey). Because we used a non-probability sampling method, in order to be able to compare victimisation rates between years we needed to make a number of corrections to account for differences between the samples. While the differences between the two samples were relatively small, there were still a number of statistically significant differences. In particular, we were concerned with differences between the samples for respondent characteristics that have been shown to be associated with the risk of victimisation. There were small but statistically significant differences between the 2024 and 2025 samples in terms of respondent's First Nations status, employment status, whether they were currently in a relationship, and their internet and social media use (Tables A6, A7 and A8).

To deal with this we approached our analysis in two stages. To compare the prevalence of victimisation between years we estimated a multivariate regression model, known as logistic regression, with victimisation (or another variable of interest, such as use of online safety measures) as the dependent variable. The model included covariates for those variables that were different between years and/or which were expected to have an important relationship with victimisation. Survey year was also included as an independent variable in the model. If survey year was statistically significant, then we could conclude with some confidence that there was a meaningful difference between respondents in 2024 and 2025 in their likelihood of victimisation.

In the case of some types of fraud and scams, the prevalence of victimisation was too low to be able to estimate a logistic regression model (ie <390 respondents, which represents a less than 1:10 ratio of model parameters to events), in which case a Firth's penalised logistic regression was used. This corrects for bias in standard logistic regression with rare events. Firth's regression was not able to be used in the cases of employment, charity, romance and money recovery frauds and scams because the prevalence was too low for this analysis (fewer than 117 victims, or a less than 1:3 ratio of model parameters to events).

We then estimated the average predictive margins, adjusted for covariates using marginal standardisation (Muller & MacLehose 2014), for the 2024 and 2025 respondents. Predictive margins indicate the average predicted probability of the outcome of interest being observed—in this case, being a victim of cybercrime—for each survey year, controlling for the other variables in the logistic regression model. This is, in effect, an adjusted estimate of the prevalence of victimisation, and is presented as such throughout the report. It is not the actual prevalence of victimisation; rather, it provides an estimated probability of victimisation for the two survey years when everything else is the same between the two groups.

This approach was not used when comparing victims in 2024 and 2025 in terms of official reporting to police or ReportCyber and the harms from cybercrime. In these cases, the differences we observed are just as likely to reflect differences in the types of cybercrimes and severity of incidents as differences between victims. We therefore relied on bivariate analyses and discuss the possible explanations for any differences observed.

Limitations

This survey provides important data about the prevalence and characteristics of cybercrime, risk factors, help-seeking behaviour, financial losses and other harms from victimisation. While there are several related collections, many of these rely on data reported to police, to ReportCyber, or to other channels such as Scamwatch (Australian Competition and Consumer Commission 2026; Australian Signals Directorate 2025). 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 provides a more complete picture of not only the extent, risks and effects of specific forms of cybercrime and responses to them but also the relationship between different forms of cybercrime. Online panels allow for rapid collection of data from large samples, which is particularly useful where the outcome of interest is relatively rare (as is the case with specific types of cybercrimes), where additional information beyond the prevalence of the outcome is required. It allows for detailed analysis of specific issues that would not be possible with a smaller sample. There are, however, several important limitations.

Survey design and sampling

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

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

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

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

These issues are all relevant to making comparisons over time. The approach we described above allows us to account for important differences observed between respondents in 2024 and 2025. We have to assume, however, that the probability of being a member of the online panels did not meaningfully vary between years for certain respondent groups and that the probability of certain groups participating in the survey was also relatively constant. We are confident that the differences we observe are meaningful differences in the actual rate of victimisation between respondents in the two years, but cannot entirely rule out other explanations and, similar to the results more generally, cannot say with certainty that these differences would apply to the general population.

Measuring cybercrime

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

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

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

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

Individuals and businesses

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

AIC reports

Statistical Report

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

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

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

www.aic.gov.au