

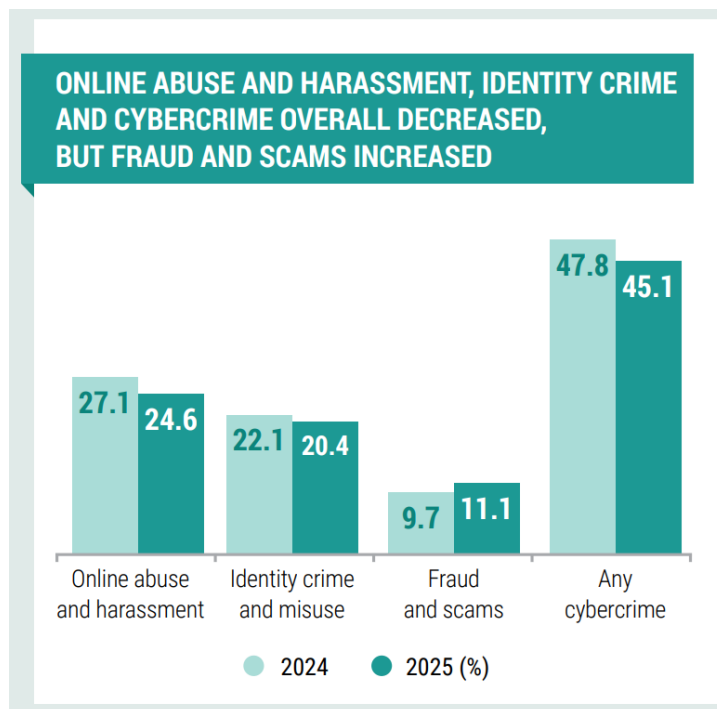
Tuesday, 28 July 2026

Australian Institute of Criminology (AIC) report with Roy Morgan shows Cybercrime in Australia down in 2025

Majority of Australian computer users (63.9%) have experienced cybercrime in their lifetime; and nearly half (45.1%) have in the last 12 months.

Roy Morgan has undertaken the fieldwork for the Australian Cybercrime Survey on behalf of the Australian Institute of Criminology (AIC) for several years. The AIC analyses the data from the surveys and publishes details of the results on their website [Cybercrime in Australia 2025](#).

Roy Morgan interviewed 10,593 Australian computer users online for the 2025 survey and the AIC's analysis found overall, 45.1% (down 2.7% points) of Australians experienced at least one form of cybercrime in 2025, fewer respondents were impersonated online, received unsolicited sexual material, had their financial accounts compromised, or were subject to online abuse and harassment than a year earlier. However, the share of respondents reporting being the victim of online fraud and scams increased in 2025.



Source (AIC Report): Roy Morgan Online Survey.

Base: Australian computer users 18+, n=10,338 (2024) and n=10,593 (2025).

Although victimisation rates remain high, there were declines from a year ago for some key measures:

- 24.6% (down 2.5% points from 2024) experienced online abuse and harassment.
- 20.4% (down 1.7% points) experienced identity crime and misuse.
- 11.1% (up 1.4% points) fell victim to fraud and scams.
- As with previous years, certain sections of the community were more likely than others to fall victim. e.g. people who are younger, First Nations, non-heterosexual, mainly speak a language other than English, have a restrictive health condition, have a higher income, and those who are small to medium business owners, operators and managers.
- 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.

Summary of key results from the Australian Cybercrime Survey (ACS) in 2025

- 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 (45.1%) had been a victim in the 12 months prior to the survey.
- It was common for cybercrime victims to have experienced multiple incidents, indicators or symptoms of the same type of cybercrime in the 12 months prior to the survey. It was also common for cybercrime victims to report having experienced multiple types of cybercrime, 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.

Online abuse and harassment is the largest category of cybercrime

Focusing on the largest category of cybercrime – abuse and harassment reported by 24.6% of respondents. The most common forms of online abuse that victims experienced in the past year were someone impersonating them online (7.1%) 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 (TFA) 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.

AIC compared the prevalence of cybercrime (online abuse and harassment), among respondents to the 2024 and 2025 ACS, adjusting for differences between the two samples. The prevalence of online abuse and harassment 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 introduction of the Online Dating Code of Conduct in October 2024 (Rishworth & Rowland 2024), major platforms implemented safety features which may have contributed to a 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.

Identity crime and misuse is the second largest category of cybercrime

The second largest category of cybercrime, identity crime and misuse, mostly involved financial accounts compromise, while a smaller proportion of respondents experienced other forms 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 (from 17.7% to 15.8%).

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.

About the collaboration between the AIC and Roy Morgan

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.

Related Research:

- [October 2, 2025 – Australian Institute of Criminology \(AIC\) report with Roy Morgan: Cybercrime in Australia 2024.](#)
- [August 26, 2025 - Crime concerns surge 'post-pandemic' to highest levels in more than a decade.](#)
- [August 26, 2025 - Roy Morgan Update: Australian Crime, Mortgage Stress and Federal Vote.](#)

The full report is available here: [Cybercrime in Australia 2025. \(PDF\)](#)

For comments or more information about Roy Morgan's data please contact Julian McCrann for more details. Email: julian.mccrann@roymorgan.com.

Reports available for sale:

The latest Roy Morgan data is available on the [Roy Morgan Online Store](#). It provides demographic breakdowns for Age, Sex, State, Region (Capital Cities/ Country), Generations, Lifecycle, Socio-Economic Scale, Work Status, Occupation, Home Ownership, Voting Intention, Roy Morgan Value Segments, Helix Personas, Media Consumption, and more

About Roy Morgan

Roy Morgan is Australia's largest independent Australian research company, with offices in each state, as well as in the U.S. and U.K. A full-service research organisation, Roy Morgan has over 80 years' experience collecting objective, independent information on consumers.

Margin of Error

The margin of error to be allowed for in any estimate depends mainly on the number of interviews on which it is based. Margin of error gives indications of the likely range within which estimates would be 95% likely to fall, expressed as the number of percentage points above or below the actual estimate. Allowance for design effects (such as stratification and weighting) should be made as appropriate.

Sample Size	Percentage Estimate			
	40%-60%	25% or 75%	10% or 90%	5% or 95%
10,000	±1.0	±0.9	±0.6	±0.4
20,000	±0.7	±0.6	±0.4	±0.3