# CYBERCRIME VICTIMISATION IN AUSTRALIA

## SHAME, FEAR AND UNDERREPORTING

2026 REPORT

DELIVERED IN PARTNERSHIP WITH

WOMEN IN DIGITAL

sekuro
An Insight company

# TABLE OF CONTENTS



# ACKNOWLEDGEMENTS


Women in Digital and Sekuro acknowledge this research was developed on Aboriginal and Torres Strait Islander lands, and pay respect to all First Nations peoples as Traditional Custodians of Country across Australia.

For tens of thousands of years, Aboriginal and Torres Strait Islander peoples have built and maintained systems of knowledge transfer, community connection and intelligence, passing wisdom across generations, distances, and lifetimes. Women in Digital and Sekuro pay respect to Elders past and present and recognise that in building a more inclusive digital future, Australia has much to learn from the world's oldest and most enduring knowledge systems.

# Foreword

Holly Hunt

CHIEF EXECUTIVE OFFICER
WOMEN IN DIGITAL

Noel Allnutt

CHIEF EXECUTIVE OFFICER
SEKURO

**Cybercrime has become one of the most common crimes in Australia, yet it remains one of the least understood and least reported. This report sets out to address that gap.**

Drawing on a nationally representative survey of more than 2,000 Australian adults, this research provides an evidence base that has been missing from the national conversation: a clearer picture of how cybercrime is experienced and, importantly, why current reporting systems are failing them.

The headline data suggests parity. At first glance, cybercrime appears to fall evenly across the population. Men and women report near-identical rates of victimisation, and the headline figures are dominated by high-volume, high-target crimes like financial scams, data breaches and hacking. But this surface-level parity conceals a more troubling reality. When cybercrime is targeted, personalised and sustained, including coercive control, stalking, image-based abuse and sexual extortion, women bear a disproportionate share of the harm.

These are also the crimes least likely to be reported. Underreporting runs across every category of cybercrime, but it is deepest precisely where the harm is most gendered and most severe. The majority of victims of technology-facilitated abuse never report to authorities. Shame, isolation and fear of further exposure keep them silent, and the systems designed to help them are too fragmented to make reporting feel safe.

That silence distorts the threat picture. It weakens disruption and deterrence. It denies victims access to support and recourse. And it reinforces the conditions that make reporting feel impossible in the first place. Furthermore, it strengthens the shame that produces it.

Sekuro is one of Australia's leading cybersecurity firms, with deep expertise in digital risk, threat intelligence and organisational resilience. Women in Digital is a profit-for-purpose organisation dedicated to building a workforce that reflects the society it serves. Together, we believe that creating a safer digital environment for all Australians depends on understanding who is being harmed, how, and why non-reporting persists. That understanding must be grounded in evidence, and it must take the gendered dimensions of cybercrime seriously.

A safer digital environment for all Australians starts with understanding who is being harmed, how, and why the current response is falling short. This report is our contribution to that understanding, and to a national conversation that separates victimisation from shame, builds clearer reporting pathways, and centres the safety of those most at risk.

# Introduction

Cybercrime causes significant financial and personal harm to Australians, with victimisation rates remaining high despite growing public awareness and investment in cyber resilience. According to the Australian Signals Directorate's (ASD) Cyber Threat Report 2024–25, the average self-reported cost of cybercrime for individuals now sits at $33,000 per incident.[1]

Cybercrime is now one of the most common forms of crime experienced by Australians, yet it remains one of the least understood and one of the least reported.

Therefore, to help better understand how cybercrime is experienced across the Australian community, and in particular how it is experienced by women, this report draws on a nationally representative survey of 2,003 Australian adults.

The headline numbers tell a story of broad exposure, with 27% of Australians falling victim to cybercrime in the past five years, and a further 15% targeted without being successfully exploited. Repeat victimisation is a defining feature of the national cybercrime landscape, with 12% of all adults and 40% of those who have been hacked being victimised on more than one occasion. The average self-reported cost of cybercrime to an individual now sits at $33,000 per incident.[2]

At first glance, cybercrime in Australia appears to be a gender-neutral phenomenon. Men and women report near-identical overall victimisation rates (26% and 27% respectively), and men aged 50 and over are the cohort most likely to report having been targeted. This surface-level parity has shaped much of the public conversation about cybercrime, framing it as a broadly distributed, equal-opportunity harm.

That framing is incomplete. The aggregate figures are dominated by high-volume, low-personalisation crime types like financial scams, data breaches and hacking, which together account for the overwhelming majority of incidents and affect men and women in similar proportions. However, when the lens is shifted to targeted, highly personalised cybercrime, like digitally-enabled coercive control, stalking and image-based extortion, the gendered pattern becomes sharper and more troubling. As a result, women bear a disproportionate share of harm from cybercrimes that depend on sustained psychological manipulation, digital monitoring and the weaponisation of personal content.

Romance scams, including highly engineered 'pig butchering' scams, are a key example. According to Scamwatch, while men made more romance scam reports than women in 2025 (55.5% vs 37.4%), women accounted for about 63% of the total financial losses.[3]

Similarly, digitally-facilitated abuse via monitoring, cyberstalking, harassment, sexual extortion and coercive control, is overwhelmingly gendered. National research has found women are significantly more likely than men to experience this abuse from an intimate or former partner, more likely to face co-occurring forms of abuse from the same perpetrator, and twice as likely to fear for their physical safety as a result.[4]

## This distinction matters for policy, prevention and service design.

Cybercrime in Australia is also profoundly underreported. This gap between victimisation and reporting is known as the 'dark figure' of cybercrime, which results in a structural blind spot that distorts official statistics, hinders effective prevention and constrains the ability to design proportionate responses. Underreporting is driven by multiple factors including confusion regarding who to report to, low confidence authorities will be able to act, the perceived inconvenience of the reporting process, and, critically, victim shame. It is important to note that shame is not an incidental feature of cybercrime victimisation and, across the most personally targeted typologies, an engineered outcome.

For victims of significant financial loss, particularly losses incurred through romance fraud and investment scams, harm and shame are compounded by a sense of personal culpability. In many cases, the result is that those who have lost life savings, retirement funds or have borrowed money do not tell their families of their victimisation, let alone the authorities.

The dynamic is more acute for victims of image-based abuse and sexual extortion. The threat of non-consensual sharing of intimate images as a tool of coercion sits at the intersection of cybercrime and gender-based violence. Victims face stigma, judgement and, in many cases, fear of professional, social or familial consequences as a result of this type of offending. ANROWS research on technology-facilitated abuse has found 97.6% of victims did not report the abuse to eSafety and 91.7% did not report to police, figures that illustrate how effectively shame and fear suppress disclosure.[5]

The cumulative effect is that cybercrimes which cause the deepest harm – those with the highest financial losses, the most severe psychological consequences, and the most pronounced gendered dimensions – are the cybercrimes least likely to be officially recorded.

This report aims to bring the national cybercrime landscape into clearer view. It maps the typologies of cybercrime experienced by Australians, examines demographic and victimology characteristics, and analyses patterns of revictimisation across crime types. Importantly, it examines the gendered nature of digitally-enabled crimes that disproportionately impact women, many of which go unreported.

In doing so, this report asserts that treating cybercrimes as evenly distributed in terms of impact and harm hinders effective prevention, reporting and support mechanisms. Furthermore, it finds that while shame, fear and a fragmented reporting system continue to prevent reporting of cybercrimes that cause the deepest harm, official figures will understate the problem, resources will be misdirected, and those most impacted will remain the least visible.

POLICY SNAPSHOT

# The legislative landscape: Coercive control and tech-facilitated abuse in Australia

Australia's approach to coercive control has undergone significant legislative transformation, with jurisdictions increasingly recognising that domestic and family violence is a pattern of behaviour and that technology plays a key role in perpetuating these patterns.

In 2023, Queensland was the first Australian jurisdiction to criminalise coercive control as a standalone offence. New South Wales followed, with coercive control laws commencing in February 2024, and South Australia passing laws, expected to come into effect in 2027, in 2025. In May 2026, the ACT introduced a coercive control bill to its legislative assembly.

Victoria, Western Australia, Tasmania and the Northern Territory are yet to adopt coercive control-specific legislation.

In Victoria, the government pursued reforms through the Justice Legislation Amendment (Family Violence, Stalking and Other Matters) Act 2026, which expanded the definition of family violence to capture stalking behaviours and systems abuse.

Western Australia has committed to reform, but at a measured pace. In November 2023, the government announced it would take a phased approach to criminalising coercive control, beginning with reforms to the Restraining Orders Act 1997 and implementing training for police officers and educators.

Tasmania occupies an unusual position, with the Family Violence Act 2004 including criminal offences for economic abuse and emotional abuse. In 2024, the definition of family violence was broadened to include coercive control behaviours against a spouse or partner. Tasmania therefore has some of the earliest legislative groundwork in the country, but no standalone coercive control offence.

The Northern Territory has strengthened existing provisions rather than creating a standalone offence, with the government strengthening existing criminal law protections regarding coercive practices, such as compulsion and the use of violence or pressure to compel conduct, through the Justice Legislation Amendment (Domestic and Family Violence) Act 2023.

# What is cybercrime?

The AFP defines 'cybercrime' as:

*"crimes directed at computers or other information communications technologies (ICTs), such as computer intrusions and denial of service attacks; or crimes where computers or ICTs are an integral part of an offence, such as online fraud".*[6]

This two-pronged definition encapsulates cyber-dependent and cyber-enabled crimes. The key distinction between these two methods of cybercrime is the role of ICT – whether it is the target of an offence or used as a means through which to commit a crime.[7]

According to the Australian Criminal Intelligence Commission (ACIC), cybercrime covers a wide variety of offences that present a significant threat to Australians, including identity crime, computer hacking, phishing, botnet activity, computer-facilitated crime, and cyber intrusion directed at private and national infrastructure.[8]

According to the Australian Criminal Intelligence Commission (ACIC), cybercrime covers a wide variety of offences that present a significant threat to Australians, including identity crime, computer hacking, phishing, botnet activity, computer-facilitated crime, and cyber intrusion directed at private and national infrastructure.[9]

Cybercrime can be highly lucrative for perpetrators, as it is relatively low cost to execute with potentially high returns. As noted by the Australian Institute of Criminology (AIC), cybercrime targeting individual computer users is a "high volume, low yield crime", that results in significant losses because of the large number of people impacted.

As the digital environment continues to evolve and technologies like generative artificial intelligence (AI) become increasingly inherent in day-to-day life, the definition of what constitutes cybercrime will continue to expand. This is important to note, especially in the context of the impacts that cybercrime has on different sections of the community.

As noted by researchers, how cybercrime is defined matters because of the impacts it has on "estimates about the extent of cybercrime, policies used to respond to the problem, strategies used to prevent the behaviour, and theories used to explain the behaviour, it is demonstrated that cybercrime can be conceptualised as either traditional criminal activity, deviant behaviours, a legal issue, a political issue, a white-collar crime, the product of a social construction, or a technological problem".[10]

It also affects perceptions of cybercrime by the community and, consequently, stigma associated with victimisation of some forms of cybercrime, such as romance scams. In addition, such an approach recognises the demographic and gendered nature of victimisation of specific types of cybercrimes, which ultimately supports more targeted and holistic interventions.

Furthermore, while 'traditional' definitions of cybercrime are useful, they fail to capture the human dimensions that define almost all crime, treating cybercrime as a discrete category separate from the physical world. In reality, the boundary between online and offline harm is blurred, and cybercrime and 'real world' crime are not mutually exclusive. Rather, they intersect with and reinforce one another.

For example, digitally-enabled coercive control plays out through tracking apps, spyware, and surveillance devices, but may also exist alongside in-person abuse. Romance scams can culminate in physical extortion, and online harassment may precede stalking and assault. Similarly, large-scale organised crime groups responsible for ransomware attacks and high-volume phishing campaigns may also be involved in other crime types like drug importation and violent crime-as-a-service typologies.[11] Treating the digital and physical as separate domains fails to recognise this innate interconnectedness.

AFP Commissioner Krissy Barrett has acknowledged this reality, recently stating that "just about every crime we investigate or disrupt is tech enabled", and referred to the "data tsunami" that is the reality of contemporary policing.

Hence, a more expansive conceptualisation of what cybercrime is and its real-world impacts needs to be considered, recognising cybercrime as a technological, social, and physical phenomenon.[12]

CASE STUDY

# Weaponised by Design: How Everyday Devices Enabled Coercive Control

In 2025, a woman presented to her local police station with a laptop belonging to her partner. During her (consensual) use of the laptop, the woman inadvertently discovered a trove of illicit materials. What began as routine domestic technology use unfolded into a complex case of technology-facilitated abuse (TFA).

**Section 308H of the Crimes Act 1900 (NSW) (Unauthorised access to or modification of restricted data)**
The laptop contents revealed that the woman's partner had systematically conducted PIN-cracking (brute-force) attempts against the woman's mobile phone until gaining access. Once compromised, her partner had exfiltrated her private correspondence across all social media applications and transferred the data directly onto their personal device. The partner operationalised Large Language Models (LLMs), specifically ChatGPT, to convert raw private text into strategic psychological manipulation tools:

- Psychological Analysis: Private conversations between the woman and family members discussing relationship concerns were pasted directly into the LLM.
- Strategy Generation: The partner prompted the AI to analyse the conversation and construct strategic psychological countermeasures.
- Scripted Execution: The AI generated tailored speeches and counter-arguments for her partner to use during interpersonal debates, actively neutralising the woman's external support systems and distorting her perception of the relationship.

**Crimes Act 1900 (NSW) Section 91P / Section 91K)**
Also on the laptop were extensive file archives containing non-consensual media spanning decades.

- This included videos capturing consensual sexual encounters between the couple throughout their relationship, recorded without the woman's knowledge or consent. There were also video archives of sexual interactions with other women dating back over 20 years.
- Deepfake Generation: Stills extracted from the covertly recorded intimate videos were processed through synthetic media tools to generate explicit deepfake pornography of the woman and other women. At the time of reporting in 2025, legislative frameworks faced distinct enforcement gaps regarding the creation and storage of synthetic sexual material.

**(Crimes (Domestic and Personal Violence) Act 2007 Section 13)**
The physical home environment served as an active monitoring network. The residence was equipped with Artificial Intelligence of Things (AI IoT) devices, security cameras, and shared account permissions. Shared subscriptions, network profiles, and location permissions provided real-time visibility into her physical position and online activities

**Conclusion**
Following the initial police report, the woman's partner was arrested over the non-consensual filming, however, on appeal, the sentence was successfully overturned, and the conviction was removed.
Key Takeaways for Policy and Legal Frameworks

- Consumer AI as a Force Multiplier: Standard productivity tools like LLMs can be weaponised to automate coercion and gaslighting strategies. Wearable products such as video-recording "smart" glasses make it easier to record other people without detection.
- Connected Ecosystem Vulnerabilities: Smart home platforms blur the boundary between domestic convenience and continuous physical surveillance.
- Evidentiary and Legal Lag: The appeal outcome illustrates the persistent challenges legal systems face when applying traditional statutes to rapid advancements in generative AI, synthetic media, and pervasive IoT tracking.

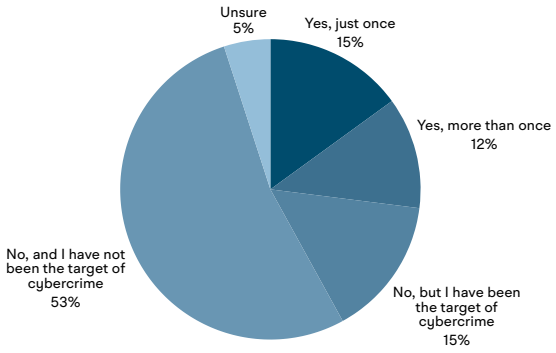
# Cybercrime in Australia

## The big picture

**This report draws on a nationally representative online survey of 2003 Australian citizens aged 18 and over, conducted between 23 April and 5 May 2026. The sample comprised 1071 women, 927 men and five participants who did not specify a gender.**

Our research indicates 27% of Australians have fallen victim to cybercrime in the past five years, with a further 15% say they have been targeted without being successfully exploited. Therefore, 42% have experienced exposure to cybercrime in the past five years. Notably, repeat victimisation is a key feature of the national cybercrime landscape, with 12% of all adults and 40% of those who have been hacked reporting they had been victimised on multiple occasions.

Figure 1. In the past 5 years, have you personally been a victim of cybercrime?




Exposure cuts across demographic lines. Men and women report near-identical victimisation rates (26% and 27% respectively), and while older men aged 50 and over are the most likely to report having been targeted, victimisation itself is broadly distributed.

The landscape is dominated by three main categories of cybercrime: financial scams (experienced by 47% of those targeted), data breaches (45%) and hacking (32%). Victimisation of other forms of cybercrime including online harassment, digital stalking, romance scams, and coercive control, was significantly lower, noting they are not characterised by high volume deployment of malicious emails, agents or malware.

Despite high rates of victimisation, reporting of cybercrime is low. Importantly, the research indicates underreporting is structural, with 44% of victims not reporting the incident through any channel, increasing to 51% for data breaches.

Police reporting is rare (12% of victims), with most reports flowing to the digital platform on which the incident occurred (27%) or to Scamwatch (19%). Despite low rates of reporting, 71% of Australians are concerned about cybercrime affecting them or their family, and 59% said their concern has increased over the past two years. This may be driven by fears relating to artificial intelligence, with 84% of Australians worried AI will increase the rate of cybercrime.

**Despite high rates of victimisation, reporting of cybercrime is low. Importantly, the research indicates underreporting is structural, with 44% of victims not reporting the incident through any channel, increasing to 51% for data breaches.**

Despite low reporting rates, Australians are taking action to avoid cybercrime victimisation. Our data shows 98% are actively taking steps to protect themselves online. Most report avoiding suspicious links and emails (79%), use multi-factor authentication (71%) and limit the personal information they share online (65%).

There is a notable gap between the threats Australians experience and the threats they say worry them most. While financial scams top both lists, data breaches, which were experienced by nearly as many people as scams, generate the lowest level of strong concern of any of the three dominant threats. Only 26% of those exposed to data breaches said they were very concerned, compared with 34% for financial scams and 37% for hacking. This indicates as data breach notifications have become more prevalent, public concern has dulled.

Additionally, Australians are rapidly adopting AI technologies, with 74% reporting AI use and 45% using it at least weekly. At the same time, eight in ten are concerned AI will increase their vulnerability to cyber-attacks, including 37% who are very concerned. Older Australians are significantly more likely to express strong concern about this emerging threat, with 45% of those aged 50-64 and 49% of those aged 65 and over saying they are very concerned, compared to just 25% of 18-34-year-olds and 29% of those aged 35-49.

# The scale of victimisation

Exposure to cybercrime is now widespread and gender-neutral at the surface level, dominated by financial scams, data breaches and hacking, with high rates of repeat victimisation and growing concern about AI-driven threats. Our research has found:

### 41% of Australians

have been exposed to cybercrime over the past five years

### Men aged 50–64 and 65 and over

are more likely to report having been targeted (50% and 59% respectively)

### Among those who report being hacked

75% affected became victims and 40% say they were victimised multiple times

### 84% of Australians

are worried AI will increase the rate of cybercrime

### Victimisation rates are similar

for men (26%) and women (27%)

### There are three dominant categories of cybercrime

financial scams (experienced by 47% of those targeted), data breaches (45%) and hacking (32%)

### For data breaches

63% affected became victims, with 37% suffering repeat victimisation

### 98% of Australians

are taking active taking steps to protect themselves online

CASE STUDY

# Changing perspectives: the need to shift online victim-blaming

Charlize Liebrand
CYBER SECURITY ANALYST
CHALLENGER

In her role as a cyber security analyst at Challenger, Charlize Liebrand's focus is on third party risk and vendor due diligence, keeping her close to the enterprise threat landscape. Her perspectives on the gendered dimensions of cybercrime, however, extend well beyond the corporate world.

Ms Liebrand draws a direct parallel between victim-blaming in digital crime and its established presence in the physical domain. Questions like "why were you posting photos online?" are, she observes, no different to asking "what were you wearing?". The only difference is the medium. That cultural reflex, she believes, is one reason why serious digitally enabled crimes like sextortion remain chronically underreported.

The other reason, she says, is rational calculation. As the daughter of a police officer, Ms Liebrand knows cybercrime prosecution rates are low and, for victims of crimes like sextortion, reporting often means exposing themselves to further scrutiny while the content continues to circulate.

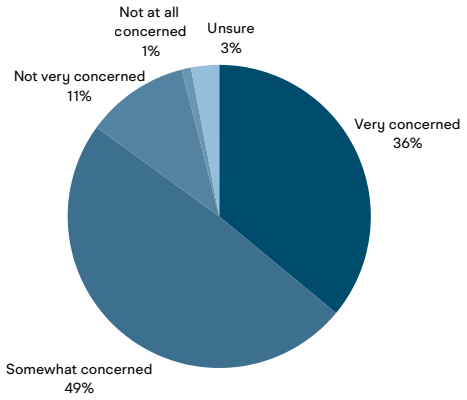
Ms Liebrand believes community attitudes towards digitally enabled crimes like sextortion need to shift, because they do create significant real-world harms. And by shifting community attitudes, victims may feel less cautious of reporting.

# The ‘dark figure’ of cybercrime

Our data indicates that reporting rates of cybercrime are low. This correlates with AIC research, which found that most cybercrime victimisation goes unreported either to police or to ReportCyber, “meaning official statistics significantly underestimate the size of the problem”.[13] According to the AIC, there is a significant discrepancy between the number of people who have experienced a cybercrime incident (82%) and the number who reported the incident to law enforcement (17%). [14] Therefore, it is clear that underreporting not only skews official figures but also limits the ability of policymakers to accurately assess threats and develop appropriate responses. This underreporting is known as ‘the dark figure of cybercrime’.

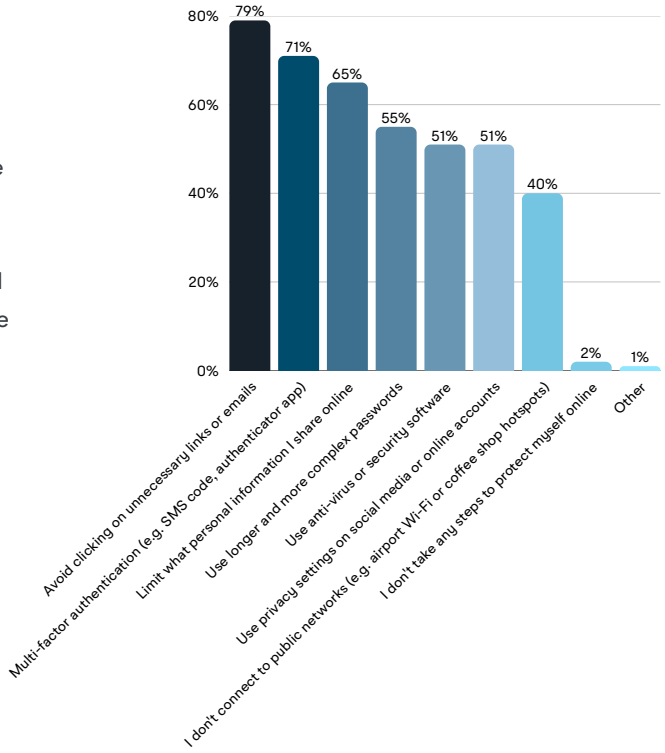
Cybercrime underreporting occurs for a variety of reasons, including victim stigmatisation, the belief that law enforcement will not be able to effectively respond and convenience (or inconvenience) of reporting.[15] Another key causal factor is pervasive community confusion regarding who to report cybercrime to, as highlighted by a previous survey undertaken by the Cyber Security Cooperative Research Centre (CSCRC), indicating that only 28% of respondents would contact the ACSC to report a cybercrime, followed by state or territory police (25%), the AFP (22%), Scamwatch (21%) and the eSafety Commissioner (5%).[16]

Figure 2. How concerned are you about your personal data being stolen by cyber criminals?




Help-seeking behaviour, however, remains uneven. Family and friends were the most common source of support for most victims, while those affected by identity crime and identity misuse most often turned first to their financial institution. AIC research has found formal help-seeking is substantially higher among victims of identity crime and misuse (70.9%) and fraud and scams (66.5%) than among victims of online abuse and harassment (50%) or malware (42%).[17] The disparity suggests that victims are more likely to engage formal channels when financial loss is tangible and less likely to do so when harm is reputational or psychological - a gap with clear implications for service design and public education.

Figure 3. What steps do you take to protect yourself online?



CASE STUDY

# Corporate responsibility and the cyber safety gap

During my years working at the intersection of enterprise technology and cybersecurity, I've seen the threat landscape evolve at a pace that outstrips our ability to respond. What has changed most dramatically, however, is not the sophistication of the attacks. Rather, it is how technology is being manipulated to exploit peoples' good nature. And when we look at certain types of cyber-enabled crimes – the ones that prey on emotions and vulnerability - women bear a disproportionate share of the harm.

Cybercrime is not just something that happens to organisations - it happens to people. And the way it impacts women can be deeply personal. Image-based abuse, financial sextortion and digital coercive control - these are crimes that exploit vulnerability, and they carry a burden of shame criminals deliberately cultivate.

However, this does not mean business does not have a vital role in keeping Australians safe online. For example, when I think about the healthcare sector and the type of data health- based organisations hold, the stakes are high. Medical records containing information about reproductive health, mental health history, or other acutely personal matters are a class of data whose exposure can be life-altering for women. The threat of that information being made public does not just cause distress - it can determine whether a woman is safe. Organisations that hold this data carry a duty of care that extends well beyond their IT infrastructure.

The case for always-on awareness is not abstract. Despite spending my professional life advising organisations on cyber risk, I've clicked on dodgy links. The message was calibrated to my behaviour and, while the manipulation was not technically sophisticated, it was psychologically precise. If it can happen to me, the implications for someone with fewer resources and less knowledge are plain to see.

For organisations, therefore, a mindset change is required. This means cybercrime victimisation needs to be treated as a workplace wellbeing issue. For example, when an employee experiences a crisis, most large organisations have a referral pathway. But when an employee becomes the victim of financial fraud, image-based abuse, or coercive control, support infrastructure is not explicit. This is a gap employers can close without significant investment and can go a long way to breaking down the stigma and shame associated with cybercrime victimisation.

The technology sector has a particular responsibility here. We create and distribute tools that connect people but that is, in too many contexts, still unsafe for women. That obligates us to do more than secure the perimeter. It means designing and deploying these tools with adequate safeguards in place, not just policies. And it means that, by treating cybercrime victimisation as a workplace wellbeing issue, we are setting an example for others to follow.

Noel Allnutt
CHIEF EXECUTIVE OFFICER
SEKURO

# The threat profile

Among the 846 Australians surveyed who have been a target or victim of a cyberattack in the past five years, the threat profile is heavily concentrated. High-volume financial scams, primarily phishing and investment scams, are unsurprisingly the most commonly experienced type of cybercrime, affecting 47% of those targeted. Data breaches affected 45% and hacking 32%. All other categories, which represent more malicious, targeted and time-consuming forms of cybercrime - online harassment or threats, digital stalking, romance scams and coercive control - sit at or below 10%.

Cybercrime underreporting occurs for a variety of reasons, including victim stigmatisation, the belief that law enforcement will not be able to effectively respond and convenience (or inconvenience) of reporting.[15] Another key causal factor is pervasive community confusion regarding who to report cybercrime to, as highlighted by a previous survey undertaken by the Cyber Security Cooperative Research Centre (CSCRC), indicating that only 28% of respondents would contact the ACSC to report a cybercrime, followed by state or territory police (25%), the AFP (22%), Scamwatch (21%) and the eSafety Commissioner (5%).[16]

Help-seeking behaviour, however, remains uneven. Family and friends were the most common source of support for most victims, while those affected by identity crime and identity misuse most often turned first to their financial institution. AIC research has found formal help-seeking is substantially higher among victims of identity crime and misuse (70.9%) and fraud and scams (66.5%) than among victims of online abuse and harassment (50%) or malware (42%).[17] The disparity suggests that victims are more likely to engage formal channels when financial loss is tangible and less likely to do so when harm is reputational or psychological - a gap with clear implications for service design and public education.

Figure 4. What type(s) of cybercrime were you a victim/target of?

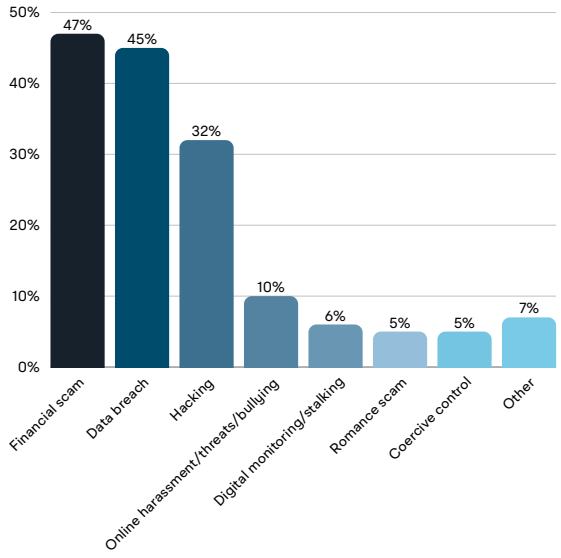
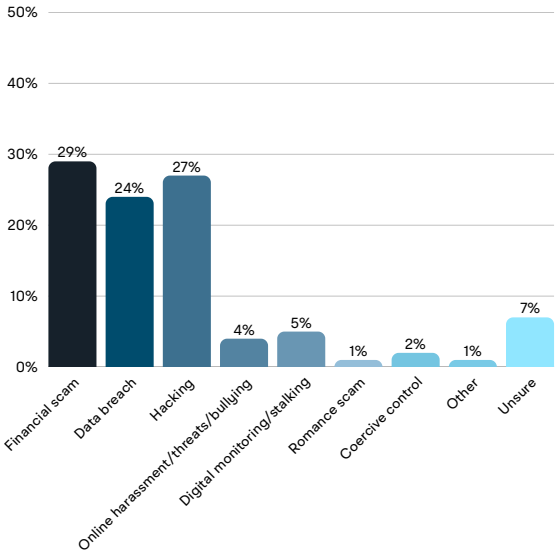



Figure 5. What type of cybercrime concerns you the most ?

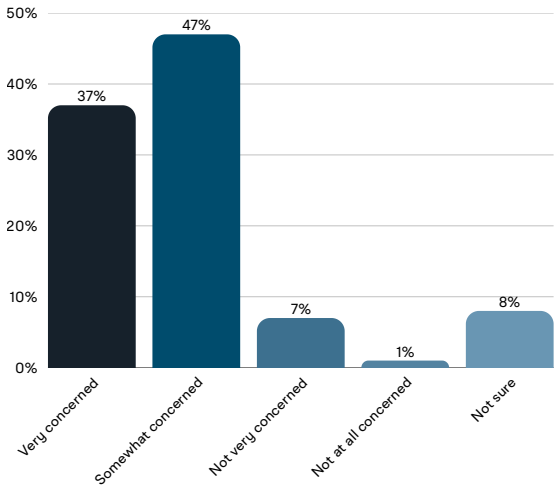


# Concern is rising fastest among older women

When we talk about cybercrime, the conversation often centres on younger, digitally native Australians. The research challenges that directly, with concern rising fastest among older women.

The survey found 71% of Australians are concerned about cybercrime affecting them or their family, including 22% who are very concerned. The level of concern increases sharply with age, with 83% of Australians aged 65 and over concerned, including 35%. Among women in this age group, 39% are very concerned, compared with 30% of men of the same age. Younger Australians aged 18–34 are the least concerned cohort, with 55% expressing any level of concern, with just 14% reporting they are very concerned.

Figure 6. How concerned are you that artificial intelligence will increase the rate of cybercrime in Australia?




Concern is also trending upward, with 59% of Australians reporting they are more concerned about cybercrime than they were two years ago, including 24% who are much more concerned. Only 3% said their concern has decreased. The shift is sharper among women than men (62% vs 56% more concerned), and particularly pronounced among women aged 65 and over, 39% of whom report they are much more concerned than two years ago.

When asked specifically about personal data theft, concern climbs further, with 85% of Australians concerned about cyber-criminals stealing their personal data, and 36% very concerned. Among those who have been a victim of or targeted by cybercrime, concern reaches 91%, with 44% very concerned.

# Cybercrime typologies

For the purposes of this report, we focused on several key cybercrime typologies. These were:

- Data breach (e.g. personal details were compromised)
- Financial scam (e.g. phishing, investment scams, fake invoices)
- Hacking (e.g. account/device was compromised via intrusion or malware)
- Online harassment/threats/bullying (e.g. abusive messages, threats, or repeated unwanted contact online)
- Digital monitoring/stalking (e.g. tracking your activity, or communications without consent)
- Coercive control (e.g. using technology to control, monitor, or intimidate in a relationship)
- Romance scam (e.g. you met online and built a relationship with the other party gaining money or personal information from you)
- Coercive control (e.g. using technology to control, monitor, or intimidate you in a relationship)

# The silence in the data

As the 'dark figure' of cybercrime illustrates, one of the most consistent findings across our data and broader cybercrime discourse is also one of the most consequential - that the official record captures only a fraction of what occurs. This phenomenon is not evenly distributed and it is deepest where the harm is most gendered. That is, in the targeted, personalised and relational forms of cybercrime that disproportionately impact women.

Therefore, understanding why Australian women do not report should not be a peripheral question. Rather, it is central to understanding the true scale of cybercrime in Australia and in designing effective responses.

CASE STUDY

## Recognising digital weapons: Australia's HEAR training to help police response to tech-facilitated abuse

Technology-facilitated abuse (TFA) has become one of the defining features of gendered cybercrime in Australia, yet for years it has occupied an awkward space in law enforcement response. It is visible enough to cause serious harm but invisible enough to escape frontline recognition.

In May 2026, the Albanese Government announced the national rollout of the HEAR training package, a key initiative developed under the National Plan to End Violence against Women and Children 2022–32. Designed for police officers across every state and territory, with at least 10,000 set to receive the training in 2026, HEAR is the first package of its kind in Australia to explicitly include technology-facilitated abuse as a core training module alongside coercive control, misidentification, and trauma-informed response.


The inclusion of TFA is significant. Digital monitoring, location tracking, account takeover, the non-consensual sharing of intimate images, and online harassment are not peripheral features of intimate partner violence, but key elements of this type of offending. For women already reluctant to engage with police, failure to recognise TFA as abuse, or to treat it as a separate matter, can compound reluctance into non-disclosure.

HEAR addresses this failure point. Developed in consultation with family, domestic and sexual abuse violence experts, HEAR combines virtual reality scenarios drawn from lived experience with real case studies. Officers in regional and remote locations can access the training online for self-paced learning. The eSafety Commissioner is among the design and delivery partners, ensuring the TFA content reflects current threat typologies.

The implications for cybercrime underreporting problem are meaningful. Trained, and trauma-informed police officers who can identify patterns of digital abuse can provide better advice and support to victims deciding whether to come forward.

HEAR does not solve the structural underreporting problem, but it does represent a key uplift in the capability of frontline responders to meet gendered cybercrime where it often occurs - in the lives of women simultaneously navigating physical danger and digital harm.

# Underreporting is concentrated where harm is gendered

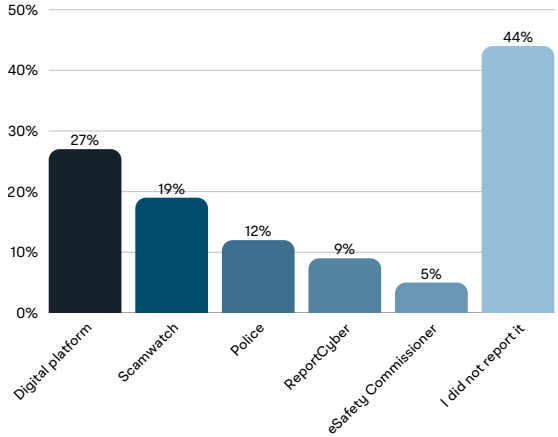
This is where the national picture breaks down. The crimes women are most likely to experience are the same crimes least likely to appear in official data. As previously discussed, cybercrime is underreported across the board, with our data showing 44% of victims surveyed did not report the incident through any channel, rising to 51% for data breaches, and that police reporting is rare across all typologies (12%). But aggregate reporting rates obscure a sharp variation by crime type, and it is this variation that reveals the gendered nature of underreporting.

AIC research shows formal help-seeking is substantially higher among victims of crimes with tangible financial loss than among victims of crimes whose harm is reputational, psychological or relational.[18] Victims of identity crime and misuse seek formal help at a rate of 70.9%, and victims of fraud and scams at 66.5%, compared with 50% for victims of online abuse and harassment.[19] The crimes that sit at the lower end of this spectrum – online abuse, harassment, stalking, image-based abuse and technology-facilitated coercive control – are precisely those that disproportionately target women.

## This pattern is most starkly visible in the data on technology-facilitated abuse.

Research has found 97.6% of all victims did not report abuse to the eSafety Commissioner, 91.7% did not report to police, and 91.5% did not seek legal advice. One in three (34.3%) told no one at all about their victimisation.[20] These are not figures that describe a minor or marginal harm. They describe a category of offending overwhelmingly impacting women with tangible harms and real-world impacts.

Figure 7. Did you report this incident to any of the following?



CASE STUDY

# Make it work: building employee confidence key to online safety

Leana El-Hourani

HEAD OF INFORMATION SECURITY AND GRC
MISSION AUSTRALIA

Leana El-Hourani has spent more over 25 years in technology, navigating male-dominated sectors long before diversity became a boardroom priority. Now, as Head of Information Security and GRC at Mission Australia, she brings rich professional experience to issues surrounding cyber security and how digital systems can be weaponised.

Ms El-Hourani is passionate about workplace culture and firmly believes online safety and confidence to report begin in the workplace. She said reporting cybercrime victimisation requires trust - in management, in organisational culture, in the belief that victims will be believed.

During her time in the technology sector, Ms El-Hourani has watched the confidence gap between women and men narrow considerably when it comes to using technology and pursuing it as a profession. She remains clear-eyed, however, that confidence itself is still unevenly distributed, and is committed to mentoring the next generation of female technology professionals to build confidence and shift workplace culture to enhance trust.

# Why not report?

Women do not fail to report cybercrime for a single reason. Underreporting is the product of multiple factors, including shame and self-blame, perceived reputational and professional impacts and fear pervasive preventative factors.

Shame is not an incidental by-product of cybercrime victimisation. In many of the most damaging typologies, it is an engineered outcome, deliberately cultivated by offenders and reinforced by the surrounding culture of judgement.

Romance fraud and pig butchering scams are designed around the manipulation of trust and intimacy over weeks or months and, when the deception is revealed, the victim is left not only with financial loss but with a profound sense of personal culpability.[21] The perception of such victims as naive ignores the professionalised, scripted nature of these operations and places the burden of fault on the person harmed. The predictable consequence is shame – and silence.

There is clear evidence that women are more acutely impacted, with data indicating in 2025 women accounted for 63% of the total financial losses to dating and romance scams reported to Scamwatch, despite having lower victimisation rates than men.[22]

Where lost sums are large, shame compounds. This results in victims frequently concealing these losses, removing support structures and the possibility of early intervention. The financial harm is then layered with isolation and secrecy, and the absence of official reporting hinders the development and application of prevention and disruption mechanisms.

For victims of image-based sexual abuse and sexual extortion, the barriers to reporting are more acute.
The non-consensual sharing of intimate images, and the threat of such sharing as a tool of coercion, sits at the intersection of cybercrime and gender-based violence. Here, the act of reporting carries its own perceived risk, with victims fearing disclosure to police may increase the exposure of intimate content, and result in professional, social and familial consequences.

**This presents a disclosure paradox that lies at the heart of gendered cybercrime.**

The features that make image-based abuse so harmful – its capacity for humiliation, its permanence, and its reach – are the features that make victims less willing to bring it to official attention. Offenders understand and exploit this dynamic, with the threat to release intimate images a recurring instrument of control in both romance fraud and coercive relationships.[23]

Even where a woman is willing to report, the system is fragmented and confusing for victims to navigate. Furthermore, pervasive confusion about who is responsible for receiving cybercrime reports not only hinders responses but also erodes confidence in the ability of authorities to respond.

Furthermore, pervasive confusion about who is responsible for receiving cybercrime reports not only hinders responses but also erodes confidence in the ability of authorities to respond.

Research by the Cyber Security Cooperative Research Centre (CSCRC) found no clear consensus among the public about where to turn to report a cybercrime. A survey conducted by the CSCRC found 28% of respondents would report to the Australian Cyber Security Centre (ACSC), followed by state or territory police (25%), the AFP (22%), Scamwatch (21%) and the eSafety Commissioner (5%).[24]

This has significant ramifications for crimes such as image-based abuse and tech-facilitated coercive control, with the reporting maze presenting another barrier to reporting.

Underpinning these barriers is concern about the outcome of reporting.

Many victims do not believe that reporting will lead to recovery of funds, removal of content, or accountability for the offender.[25] Given the extraterritorial nature of much cybercrime, these concerns are warranted, with investigation and law enforcement responses severely limited when a perpetrator is located overseas. Furthermore, the perception that nothing can be done interacts with shame and fear to make non-reporting the path of least resistance, particularly when harm is not exclusively financial in nature.

# Perception, severity and the gendering of seriousness

The decision to report is shaped not just by barriers, but also by how seriously a harm is perceived. Here too the evidence points to a gender divide.

For example, research applying feminist theory to cybercrime typologies has found that while economic forms of cybercrime such as online fraud are regarded as equally serious by men and women, psychosocial cybercrime types like cyberbullying, cyberstalking, online harassment and image-based abuse are rated as significantly more serious by women, who are also disproportionately their victims.[26]

Figure 8. What type of cybercrime concerns you the most? (Female Respondents)

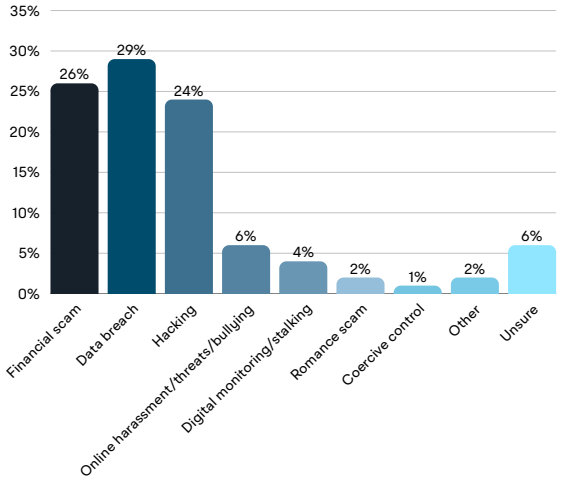
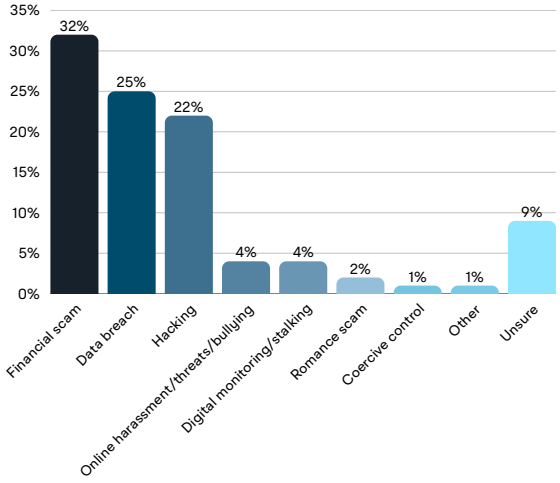



Figure 9. What type of cybercrime concerns you the most? (Male Respondents)



This divergence has direct consequences for reporting. When perceptions of seriousness among institutions and informal networks a victim relies upon do not align, the perceived cost of disclosure rises. As a result, a woman who experiences the harm as grave but anticipates that it will be minimised is incentivised to stay silent.

Data from the eSafety Commissioner reiterates this observation. Women are more likely than men to experience tech-based abuse, to experience it more frequently and over longer periods, and to suffer abuse that is more severe in nature and more damaging in its psychological impact. Ultimately, this leaves women twice as likely as men to fear for their safety (26.3% compared with 12.6%).[27]

# What are the implications?

The underreporting of cybercrime by Australian women has concrete consequences for how the problem is understood and addressed:

### It distorts the threat picture.

Because the most gendered cybercrimes are the least reported, official statistics systematically understate their prevalence and the degree to which they impact women. Policy is calibrated to reflect visible data, which means effective responses for gendered cybercrimes remain under-resourced and targeted interventions are difficult to implement.

### It weakens disruption and deterrence.

Reports form the basis of law enforcement intelligence. Where these crimes go unreported, offenders face little risk of detection, and other potential victims receive no warning.

### It deprives victims of recourse and support.

Non-reporting prevents access to financial remediation, content removal, protective orders and specialist support services. The harm is not only sustained but compounded by isolation.

### It entrenches the shame that produces it.

Silence is self-reinforcing. The fewer victims who come forward, the more anomalous and culpable victims feel, reinforcing perceptions that cybercrime victimisation is a personal failure rather than a crime.

Closing the gap requires more than encouraging victims to report - it requires removing the structural and cultural conditions that incentivise non-reporting. There are clear opportunities to streamline and improve reporting mechanisms, to reframe cybercrime victimisation to reduce stigma, and to introduce trauma-informed reporting pathways that do not require victims of image-based abuse to risk further exposure as a result of help-seeking activity. Until the conditions that produce silence are addressed, the dark figure will remain, and the cybercrimes that fall hardest on women will continue to be those least visible.

# Implications for the cybersecurity sector

The cybersecurity industry has traditionally oriented itself around protecting systems, networks and data, and around high-volume, technical threats that impact organisations. That focus remains essential. However, as this report makes clear, cybercrimes that have the most significant impacts on individuals are generally not technical breaches but personalised, relational forms of offending that exploit trust, intimacy and the features of everyday consumer technology.

There is a clear appetite among Australians to be protected. The overwhelming majority are already taking active steps to safeguard themselves online, and concern about cybercrime is both high and rising, particularly among older women. This represents an opportunity - and a responsibility - for the sector to meet individuals where they are. Uplifting individual cybersecurity cannot rest on the assumption that victimisation reflects personal carelessness. As this report has shown, the shame that suppresses reporting is, in many cases, deliberately engineered by offenders, and security advice that blames the victim perpetuates underreporting.

The sector therefore has a key role to play. It can design products and security guidance that account for the misuse of monitoring, location and content-sharing features in coercive contexts. It can develop and promote tools accessible to those at greatest risk, including older Australians and people experiencing technology-facilitated abuse. It can lend its technical expertise to the disruption of professionalised, organised cybercrime operations. Most importantly, it can shape public conversation by communicating in ways that reduce stigma.

CASE STUDY

## From enterprise to education: It's a joint responsibility to build individuals' resilience

Across the cybersecurity ecosystem, conversations generally converge around enterprise issues – data and asset management, identity and access, and business continuity. One thing that rarely comes to the fore, however, is the impact cybercrime has on individuals. This is something Adele Smith, CrowdStrike's ANZ Channel Director is keen to change.

Adele is particularly passionate about shedding light on the realities of digital crimes she describes as "hyper-personal" – offences that disproportionately impact women. These include things such as identity theft, coercive control, sexual image exploitation, romance scams, financial impersonation, and technology-facilitated stalking. The overlap with domestic and family violence patterns is, in her view, not incidental. Adele was clear that victims of cybercrime can be targeted through both personal and professional channels.

Tackling the issue effectively also requires a fundamental shift in how "loss" is defined – moving away from purely material terms and toward a broader recognition of the psychological and social toll these crimes take on victims.

"If we don't equip people early with the skills to navigate cybercrime and its psychological impacts, we risk leaving them vulnerable for the rest of their lives," Adele said. "The flow-on effects – through their relationships, their confidence, and the way they engage with the world – can be lasting and profound. As a society, we need to get ahead of this. That means investing in early education that builds not just awareness, but genuine resilience, critical thinking, and psychological strength before people ever encounter these threats."

Adele believes AI is accelerating these vulnerabilities, with deepfakes and synthetic identity tools enabling new forms of image-based abuse at scale, further amplified by algorithmic online environments. She is also concerned that as AI becomes more ingrained in the way we communicate, 'we' are losing the problem-solving and interpersonal skills that serve as informal defences against manipulation and victimisation. This creates a "layer-on-layer" of psychological impact that compounds across a young person's development, perpetuating a vicious cycle.

But Adele does see a path forward and believes the cybersecurity industry has a meaningful role to play.

First, she argues that cybersecurity companies are well placed to develop enablement programs that teach people to exercise critical thinking, beyond consuming what the 'tools' tell them. This means fostering human-centred decision-making, problem solving, communication skills, and the kind of moral reasoning that AI simply cannot replicate... yet.

Adele Smith

ANZ CHANNEL DIRECTOR
CROWDSTRIKE

Second, there needs to be a concerted push for detection capabilities that extend beyond enterprise infrastructure, leveraging tools capable of identifying deepfakes, online abuse patterns, targeted campaigns, social engineering threats and identity theft that are most likely to harm individuals rather than organisations.

At the heart of it all, Adele says, education and joint responsibility for human safety are paramount. "These are problems we need to be teaching people about early – not waiting until they're already in the workforce," she said. "So how do we go further down the chain? How do we get this type of education into universities and school curriculums?"

# Recommendations

The findings of this report point to a clear conclusion – that cybercrimes that cause the deepest harm, and that fall most heavily on women, are also the least likely to be reported, recorded and acted upon. Closing this gap will not be achieved by encouraging victims to come forward alone. Indeed, it requires dismantling the structural and cultural conditions that cause victims not to report.
The following recommendations are directed at governments, law enforcement, regulators, industry and the support sector, and are intended to reduce the dark figure of cybercrime by treating its gendered dimensions as central rather than peripheral.

**Recommendation 1:**

## Establish a single, clearly signposted national reporting pathway, accommodating the full spectrum of cybercrime.

Public confusion about who to report cybercrime to is one of the most consistent barriers identified in this report and broader research. A single entry point which clearly directs victims and connects them with the correct agencies would reduce the cognitive and emotional cost of reporting. A victim of image-based abuse should be able to report through the same entry point as a victim of a financial scam, without needing to determine which agency holds jurisdiction before seeking help. That is not the case today.

Currently, ReportCyber sits within the remit of the ASD's Australian Cyber Security Centre, which is not responsible for law enforcement responses to cybercrime. This creates a structural disconnect between the point of reporting and the agencies equipped to investigate and respond. Consideration should be given to moving a single front door reporting mechanism into the purview of the Australian Federal Police, in collaboration with state and territory police forces, to create a pathway that connects victims directly with the agencies that can act.

This is not without precedent. The United Kingdom's Action Fraud operates as a centralised reporting portal that triages and routes reports to the relevant law enforcement body. Canada's Anti-Fraud Centre performs a similar function. Both models demonstrate that a single, clearly signposted entry point can coexist with distributed policing responsibilities.

Critically, this pathway must accommodate the full spectrum of cybercrime, including image-based abuse, technology-facilitated coercive control and stalking, rather than orienting around high-volume cybercrime. A reporting system designed around the most common offences will continue to fail the victims of the most harmful ones.

**Recommendation 2:**

## Design trauma-informed reporting that does not require victims to risk further harm because, for victims of image-based abuse and sexual extortion, the act of reporting is a form of revictimisation.

For victims of image-based abuse and sexual extortion, the act of reporting is itself a form of revictimisation. Victims are required to describe deeply personal experiences, often multiple times to different agencies, and in many cases to retain, locate or re-access the very content that was used to harm them. A system that asks this of victims is a system designed around institutional convenience, not victim safety.

Reporting processes should be built around the disclosure paradox these victims face. In practice, this means enabling a victim to provide a single, recorded initial disclosure that travels with them through the reporting and response process, rather than requiring retelling at each institutional handover. A designated case coordination function, whether through a single point of contact or a shared case file accessible to authorised agencies, would reduce the number of times a victim is asked to revisit their experience.

Evidence handling must also be reconsidered. Victims of image-based abuse should not be required to retain harmful material on personal devices or re-access it as a condition of progressing a report. Reporting pathways should include secure evidence intake mechanisms that allow content to be submitted once and preserved by the receiving agency, removing the burden of evidence custody from the victim.

Importantly, trauma-informed practice cannot be confined to specialist services. Education and training should be provided across the entire response chain, from frontline police who receive initial reports through to investigators, prosecutors and support services. A trauma-informed entry point loses its value if the victim is re-traumatised at the next stage of the process.

**Recommendation 3:**

## Reframe cybercrime victimisation to separate harm from shame.

Shame is, in many of the most damaging cybercrime typologies, an engineered outcome rather than an incidental by-product. Offenders deliberately cultivate shame to prevent disclosure, and the language used in public communications, media reporting and even victim-facing services can inadvertently reinforce it. When victims are described as having "fallen for" a scam or having "allowed" access to personal content, the framing locates responsibility with the person who was harmed rather than the person who caused the harm.

Whole-of-government awareness campaigns should adopt language frameworks that consistently name cybercrime as offender behaviour, not victim failure, and sustain that messaging over time rather than limiting it to short-term campaign cycles.

Reframing victimisation as a crime, and not a personal failing, may support higher reporting rates and should be a sustained public-education objective. If victims believe they will be judged for what happened to them, they will not come forward. The efficacy of reframing efforts can and should be measured through sustained monitoring of reporting rates, public attitudes and victim willingness to engage with support services.

**Recommendation 4:**

## Improve the measurement of gendered cybercrime.

Policy responses are calibrated to the data that is available. When gendered cybercrime is systematically underreported and inconsistently measured, it is systematically under-resourced. Closing the gap between recorded incidents and the true scale of harm is not only a research priority. It is a precondition for directing prevention funding, support services and law enforcement capability to where they are most needed.
Three specific measurement reforms would materially improve the evidence base.

First, gendered disaggregation should be mandated across all cybercrime data collected by federal, state and territory agencies. At present, much of the data captured through reporting mechanisms like ReportCyber is not consistently broken down by gender, making it difficult to identify patterns in who is being targeted, by which crime types, and with what consequences. Without disaggregation as a baseline, gendered patterns remain invisible in the data that informs policy.

Second, national survey instruments should be expanded to capture the digital dimensions of gendered violence. The ABS Personal Safety Survey is Australia's primary data source on experiences of violence, including domestic, family and sexual violence, but it does not adequately capture technology-facilitated abuse, image-based exploitation or digitally-enabled coercive control. Including these categories in future iterations of the survey would bring the measurement of gendered cybercrime into the same framework used to measure gendered violence more broadly, and would support a more complete national picture.

Third, consideration should be given to establishing a recurring national prevalence study focused specifically on gendered cybercrime. This report demonstrates that a nationally representative survey can surface patterns that administrative data alone does not capture, including the scale of underreporting, the role of shame in suppressing disclosure, and the gendered distribution of harm across crime types. A regular, repeated study using a comparable methodology would allow trends to be tracked over time, the impact of policy interventions to be assessed, and emerging threats to be identified early.

Improving measurement is not a substitute for improving reporting pathways. But without an accurate evidence base, the reforms outlined in this report cannot be effectively targeted, resourced or evaluated.

**Recommendation 5:**

## Treat the digital and physical as a continuum in policy and practice.

The boundary between online and offline harm is blurred, and in almost every crime, there is a digital element. These are treated as separate matters, belonging to a different category of crime, often requiring a separate report to a different agency. The result is that the digital dimensions of the harm go unrecorded, the full picture of the offending is never captured, and the victim is left to navigate multiple systems to report what they experience as a single, continuous pattern of abuse.

At the institutional level, mechanisms for bridging this gap already exist. The AFP's Joint Policing Cybercrime Coordination Centre (JPC3) provides a framework through which digital and physical crime responses can be coordinated. Expanding the remit of JPC3 and similar coordination bodies to explicitly include technology-facilitated abuse alongside traditional cybercrime categories would be a practical step toward integration. But coordination at the top is only effective if it reaches the frontline. Routine screening for digital dimensions should be embedded in police intake processes for domestic violence, stalking and sexual assault as standard, not treated as an optional add-on or a specialist referral.

Legislative frameworks have not kept pace with this reality either. Where laws draw hard distinctions between digital and physical offending, gaps emerge in protection, jurisdiction and sentencing that do not reflect the experience of victims. A cross-jurisdictional review of how existing legislation treats the digital dimensions of gendered violence would identify where these gaps are most acute and where harmonisation is needed.

The principle is straightforward: if victims experience digital and physical harm as a continuum, the systems designed to protect them must be built the same way.

**Recommendation 6:**

## Prepare for AI-enabled cybercrime now.

The overwhelming majority of Australians are concerned AI will increase their vulnerability to cybercrime. AI is already lowering the cost and increasing the sophistication of deception, enabling offenders to generate synthetic media, clone voices, and conduct hyper-personalised social engineering at a scale and quality that existing awareness campaigns do not prepare the public to recognise. A two-pronged approach is required.

The first is public education uplift. Australians need practical guidance on how AI changes the threat landscape. Current awareness campaigns focus primarily on traditional cybercrime typologies and do not adequately address AI-specific threats such as deepfake video and audio, synthetic voice cloning in fraud and impersonation, or the use of AI to generate and scale phishing and social engineering attacks. Public education should be updated to help Australians identify these emerging threats and to build realistic expectations about the increasing difficulty of distinguishing genuine communications from fabricated ones.

The second is enhanced institutional readiness. Law enforcement and reporting agencies need specific capability uplift to detect and respond to AI-enabled offending. This includes investment in detection tools for synthetic media, training for frontline officers in identifying AI-generated content and evidence, and updated assessment frameworks for evaluating the credibility of digital communications. Without this capability, the gap between the sophistication of offending and the capacity of the response system will continue to widen.

Critically, the gendered implications of AI-enabled cybercrime must be recognised from the outset. As AI tools become more accessible and more capable, the gendered harms identified throughout this report are likely to deepen and accelerate. Policy responses to AI-enabled cybercrime that do not account for this gendered dimension will repeat the same blind spots this report has worked to expose.

Law enforcement and reporting agencies need capability uplift to detect and respond to AI-enabled offending before it scales, which requires specialised training and tech tools to be adopted.

# Conclusion

There is no doubt cybercrime is now among the most common crimes experienced by Australians. More than a quarter of Australians have been victimised in the past five years, repeat victimisation is common, and men and women report near-identical overall rates. And were the analysis to stop there, cybercrime would appear to be an evenly distributed, gender-neutral harm.

However, the reality is different.

High-volume crimes like scams, data breaches and hacking dominate the headline figures. But when cybercrime becomes targeted, personalised and relational, the gender divide sharpens. Women are disproportionately harmed by offending built on sustained manipulation, digital surveillance and the exploitation of personal content. They also bear the majority of financial losses to romance fraud, despite reporting lower victimisation rates than men.

The most concerning finding in this research is not what it surfaces. It is what it confirms is still missing. The cybercrimes with the lowest reporting rates are the same ones where women are most overrepresented as victims. Shame, fear of re-exposure and a reporting system that asks too much of the people it should be protecting create a cycle of silence. That cycle has consequences: it warps the national threat picture, undermines deterrence and leaves victims without support or recourse.

We cannot build a safer digital environment without confronting this directly.

Women in Digital and Sekuro are clear on what needs to happen next. Reporting pathways must be simplified so that victims are not forced to navigate a fragmented system at their most vulnerable. Responses must be trauma-informed, designed around the safety of the person reporting rather than the convenience of the institution receiving the report. The national conversation must shift so that shame sits with offenders, not with victims. Measurement frameworks must capture gendered cybercrime accurately, because what is not counted is not addressed. The false distinction between digital harm and physical harm must be retired. And the threat landscape must be assessed honestly, including the acceleration that AI-enabled offending will bring.

Together, these shifts represent something bigger than incremental reform. They represent a commitment to ensuring that the Australians most at risk are no longer the least visible in the data.

# References


1. ASD Cyber Threat Report 2024-25
2. Annual Cyber Threat Report 2024-2025 | Cyber.gov.au
3. Tainted love: romance scam victims climb in 2025 | Western Australian Government
4. Intimate partner violence - Australian Institute of Health and Welfare
5. Technology-facilitated abuse: National survey of Australian adults' experiences - ANROWS
6. Cybercrime | Australian Federal Police (afp.gov.au)
7. Cybercrime Key Issues: Cybercrime in Brief (unodc.org)
8. Cybercrime | Australian Criminal Intelligence Commission (acic.gov.au)
9. AIC Submission – PJCIS: Inquiry into the capability of law enforcement to respond to cybercrime
10. https://www.springerprofessional.de/en/defining-cybercrime/18055580
11. OPENING THE BOOKS. The impact of serious and organised crime on Australia in 2025
12. AFP Commissioner Krissy Barrett address: Australian Information Industry Association
13. Cybercrime in Australia 2023 | Australian Institute of Criminology (aic.gov.au)
14. Responding to cybercrime: Perceptions and need of Australian police and the general community (aic.gov.au)
15. D19156-CCJ-1-1-UK-Cybercrime-Victims-Reporting--Sikra-et-al.pdf (production-new-commonwealth-files.s3.eu-west-2.amazonaws.com)
16. Hitting the mark: Effective cybercrime communications across demographic divides, CSCRC
17. https://www.aic.gov.au/sites/default/files/2025-08/sr53_cybercrime_in_australia_2024.pdf
18. Cybercrime in Australia 2023
19. Cybercrime in Australia 2024 | Australian Institute of Criminology
20. Technology-facilitated abuse:
21. Pig butchering scam targeting Australians as AFP warns lonely hearts to be wary this Valentine's Day
22. CQUniversity, "Love bombing and pig butchering: how romance scams are evolving", drawing on Scamwatch 2025 data.
23. Image-based abuse quick guide
24. Cyber Security Cooperative Research Centre, Hitting the mark: Effective cybercrime communications across demographic divides.
25. Responding to cybercrime: Results of a comparison between community members and police personnel | Australian Institute of Criminology
26. Harvey et al., "Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types", The Howard Journal of Crime and Justice.
27. eSafety Commissioner, Online risks for women; Track, harass, repeat: attitudes around tech-based coercive control.

# Appendix

## Methodology - Quantitative Research

This report is also informed by qualitative interviews conducted with four subject matter experts, whose insights and commentary are cited throughout. Interviews were conducted via video and phone call, and were used to contextualise and add depth to the quantitative survey findings, drawing on professional expertise in cybercrime, digital harm and gendered violence.

## Methodology - Qualitative Research

This survey has been conducted using an online interview administered to members of the YouGov Plc Australian panel of 71,000+ individuals who have agreed to take part in surveys. Emails are sent to panellists selected at random from the base sample. The e-mail invites them to take part in a survey and provides a generic survey link. Once a panel member clicks on the link they are sent to the survey that they are most required for, according to the sample definition and quotas. (The sample definition could be "adult population" or a subset such as "adult females"). Invitations to surveys don't expire and respondents can be sent to any available survey. The responding sample is weighted to the profile of the sample definition to provide a representative reporting sample. The profile is normally derived from census data or, if not available from the census, from industry accepted data.

All figures, unless otherwise stated, are from YouGov Plc.  Total sample size was 2003 Australian voters. Fieldwork was undertaken between 23rd April - 5th May 2026. The survey was carried out online. The figures are representative of the voting population by age, gender, region, income, education, 2025 Federal Election vote and 2023 Voice Vote.

DELIVERED IN PARTNERSHIP WITH

WOMEN IN DIGITAL

sekuro
An Insight company

Women in Digital is passionate about creating a connected world where everyone can shape, contribute to, and succeed through technology and digital innovation.

hi@womenindigital.org | womenindigital.org

CONNECT EDUCATE EMPOWER