Safer Internet Lab

Research report

Online Fraud and Scams in Australia

Safer Internet Lab

ONLINE FRAUD AND SCAMS IN AUSTRALIA

A Research Report by Safer Internet Lab

The views expressed here are solely those of the author(s) and do not represent an official position of SAIL, CSIS, Google, or any other organization. Please contact the author(s) directly with any comments or questions.

Online Fraud and Scams in Australia

Billy Esratian[3]

INTRODUCTION

Australia is deemed to be a lucrative market for online scams. In 2022-2023, the Australian Bureau of Statistics estimates that Australia's real net national disposable income per capita reached AU$71.774. Such a relatively wealthy society serves as one of the motivating factors for online scammers to target Australians in their operations. The lure for online scammers to target Australia is also induced by Australia's highly digitized society, with internet users' proportion in 2023 reaching up to 97,1% of its population (International Telecommunication Union, 2024). Such a high dependence into the digital online activities concurrently allows the scammers to have more entry points to reach the Australian society.

Current trends of online scams in Australia witness an accelerated diversification method to primarily obtain and exploit the target's personally identifiable information (PII) for illegal gains. This diversification effort is facilitated via the use of generative AI by the scammers. Harnessing the collaborative ecosystem and multilayered approaches between the government, private sectors, law enforcement and the public in general, efforts to address this AI-powered online scams are underway. While the improvement of the situation is evident, several challenges to respond the ever-advancing scams operations still need to be addressed.

PATTERNS AND TRENDS

As a disclaimer, there are several reporting platforms available for Australians to report scams, namely through Scamwatch, ReportCyber, IDCARE, Australian Financial Crimes Exchange (AFCX), and Australian Securities and Investment Commission (ASIC). In 2024 alone, these collective reporting mechanisms garnered a total of 494.732 reports, with losses accumulating up to AU$2.03 billion (National Anti-Scam Centre of Australia [NASC], 2025). Given that uniformed methodology and data consistency are essential to observe patterns and trends, for the purpose of the *Patterns and Trends Section*, the Scamwatch data as one of the derivatives of all said reporting mechanisms will be solely used as the baseline study for the subsequent discussions. This is because Scamwatch wields a relatively more consistent and detailed extent of data compared to the other reporting mechanisms.

In the aggregate, throughout the space of 2023 to February 2025, Scamwatch which is run by the NASC, received 587.744 reports of scams with losses totalling AU$ 861,022,129.19. Delving into the data, three types of scams contribute the most to the losses, namely investment, dating and romance, and phishing scams. Despite the differences of conduct in these three types of scams, one commonality remains, for in each type of these scams, the use of generative AI was evident to a certain extent, and served as an early precaution of the trends that may lurk ahead for one's personal safety.

Investment Scams

Investment scams dominated the typology of reported scams in Australia, with losses amassing at AU$ 519,126,719.13 from 17,382 reported investment-related scams (NASC, 2025). The median number of losses is estimated to be around AU$8500-AU$10,000. Two types of scams are prevalent in this corpus:

[3] Ph.D. in Law Candidate, The Australian National University

a) the use of convincing marketing and advanced technology, with promises of big payouts and little losses, done with pressure tactics; and b) gambling made in the form of investment scam, through computer prediction software, betting syndicates, and sports investment (NASC, 2025).

As a modus operandi, the use of AI was identified as an emerging trend in investment scams, particularly, by way of AI trading platform scams (RMIT, 2023). To this end, the scammers claim that the trading platform is harnessed using AI software and other emerging technology, such as the quantum computing, to maximize the returns, and therefore would compensate the lack of expertise from the investors' side. In luring these inexperienced investors, the scammers use deepfake prominent figures' endorsements to initiate the online trading. One notable example in Australia was the use of AI-engineered doctored videos of Elon Musk and Chris Hemsworth that promoted the Quantum AI, a fake investment trading platform (ASIC, 2024). In 2023 alone, it was estimated that the losses from AI trading platform scams amounted to nearly AU$20 million, with more than 600 reports to NASC's Scamwatch noting the use of common methodology in AI trading platform scams (RMIT, 2023).

Dating and Romance Scams

Dating and romance scams contribute second to the cumulative losses due to scams in Australia (Scamwatch, 2025). Out of 7.403 reports, the losses peaked at AU$63,709,074.97 with the median of AU$1,792.50. Dating and romance scams manifest through a perceived real and genuine relationship offered by the scammers to the victim. (Cross & Layt, 2022) Once the trust is gained, manipulations to give the scammers money, gift, or personal data will then proceed as the subsequent step. The avenues to practice this scam are diverse, encompassing social media, gaming and dating apps or websites, and direct text and email. To achieve the objective, the scammers often disguise themselves in a fake identity, including famous person. (Cross & Layt, 2022).

The Emerging use of AI is particularly apparent to sustain the romance scams in two models. First, through the deepfake technology to help create a new identity. Second, through the use of Chatbots in the conversation. To this end, two indicants may hint said usage of AI, namely flawless looking photos, and vague and repetitive answers (Australian Banking Association, 2025). In one instance, the use of deepfake AI was noted to be as sophisticated as materializing into a live video call (ABC, 2024). This is particularly concerning because the use of deepfake video begins to erode the traditional predicates to detect romance scammers, such as the scammers' avoidance to meet in person or to have a video call. Another trend observable from Australia is that romance scams may be cross-jurisdictional in its practice. In one instance, some 5000 Australians were targeted as potential victims of the Philippines-based romance scammers. (Australian Federal Police [AFP], 2025).

Phishing Scams

The reported losses caused by phishing scams amounted to AU$54,918,571.93 as accumulated from 218.591 reports, with the median losses reaching up to AU$2,345.60. (Scamwatch, 2025). Phishing scams use impersonation to obtain certain information from the target, usually through the sending of a message that is characterized as if it is coming from a solid entity, claiming the sense of urgency and importance, and inviting the target to open a deceptive website (Desolda et al., 2022). Phishing also often includes a stressor statement to stimulate the recipient to act promptly without proper consideration (Grimes, 2024).

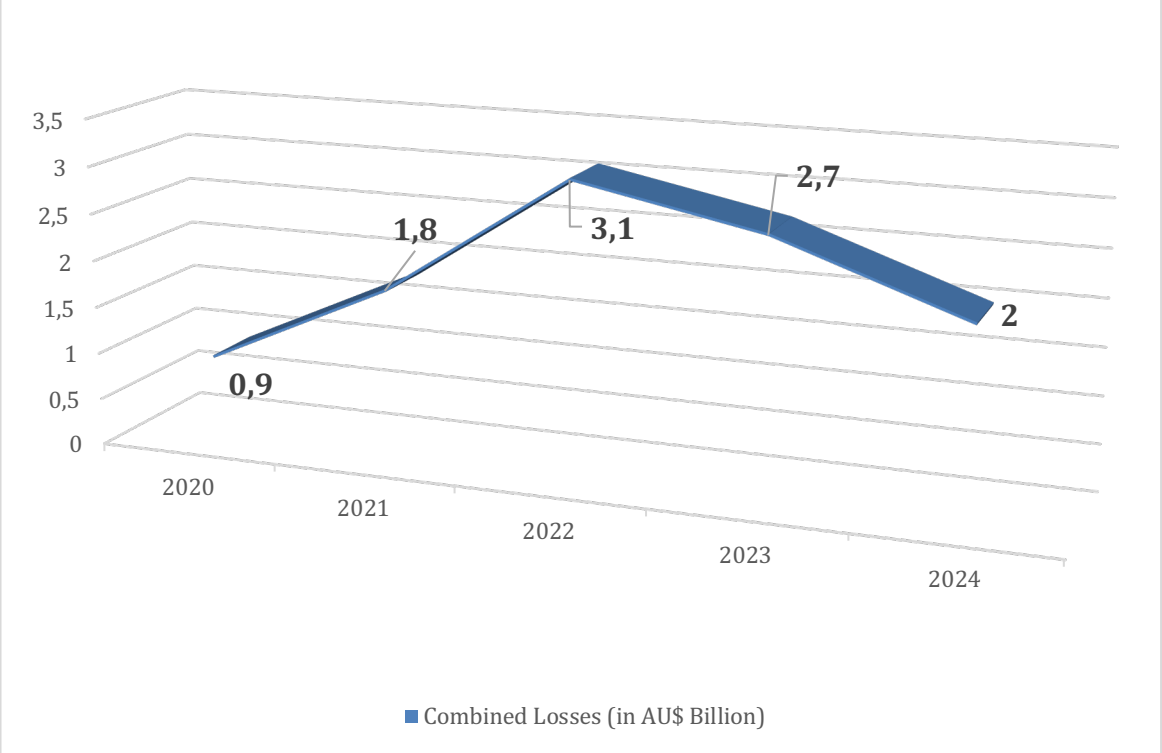
Various models of phishing scam's sophistication can be attributed to the use of generative AI (Das, 2024). Corollary to this trend, the Australian Signals Directorate detected a variant of phishing, called Vishing (video phishing) wherein the scammers use the deepfake technology to interact with the victim

via video conference to dupe the victim into doing what is told by the scammers (ASD, 2024). One example of this vishing technique impersonated the Sunshine Coast Mayor, Rosanna Natoli. In this regard, the scammer(s) created Facebook accounts, engaged in live video calls through facial alteration technology to mimic Rosanna Natoli, and requested bank details via messenger (ABC, 2024). Another notable trend of phishing variants in Australia is the Quishing (Quick Response (QfR) Phishing) which uses the QR code technology to deceive the target into giving a personal information or downloading malware to the target's device (ASD, 2024). One example of this practice involved the scam email impersonating the Australian Taxation Office with QR code directing the target to a fake myGov login page, with the purpose of stealing the target's myGov account details (ASD, 2024). Through the spreading of publicly sourced AI-powered QR generators, the practice of QR Phishing thus needs to also be anticipated. In another observation, the exponential increase of AI-generated phishing text message scams activities may contingent upon certain occasions. In this context, the AFP highlights that sales events, such as the Black Friday and Cyber Monday may be exploited through the impersonation of legitimate retailers and postal and delivery services (AFP, 2024).

IMPLICATIONS OF ONLINE FRAUD AND SCAMS

At the outset, economic losses are one indicant of the negative impact that scams operations brought to the society. To this end, Australia experiences a relatively sizable economic losses from scams where the yearly losses can reach as high as AU$3,1 billion.

Figure 2.1 Combined Losses from Scams in Australia



Source: NASC (2025)

Beyond said economic losses, three societal and legal ramifications further exacerbate the impacts of online scams in Australia, namely the disproportionate victimisation of the elderly generation, the heightened risk on personal safety, and the cross-jurisdictional issue in law enforcement.

The Disproportionate Victimisation of the Elderly Generation

Scams affect different age groups dissimilarly. Focusing on the three types of scams from 2023-February 2025 as previously discussed, Scamwatch data revealed that the elderly generation (age 65 and over) is disproportionately affected by online scams. This group accounts to 68.639 out of 243.376 reported scams, with losses amounted to AU$196,979,844.96 (Scamwatch, 2025). This figure is even higher than the number of reports of the other five age groups (under 18 (690 reports), 18-24 (5.056 reports), 25-34 (13.516 reports), 35-44 (20.368 reports), 44-54 (24.999 reports)) combined (64.629 reported scams) (Scamwatch, 2025).

A variety of explanations may be offered to rationalize why the older generation is more susceptible to online scams. From financial standpoint, this generation is relatively considered to be a suitable target due to their relatively stable finance from the accumulated lifesavings and retirement funds (Button et al, 2024). From medical standpoint, cognitive impairments along with health problems may increase their risk of victimisation (Button et al, 2024). From psychological standpoint, the condition of living alone or lack of social networks may also add as an aggravating factor. (Button et al, 2024). Additionally, misplaced trust and lack of digital literacy may also be invoked as alternative explanations (ANZ, 2024).

While the rationale may diverge, the disproportionate victimisation of online scams targeting the elderly generation in Australia needs to be meticulously and promptly addressed, particularly in the wake of the incorporation of AI in online scam schemes. The data shows that this group of population is the most vulnerable and susceptible to online scams. Tailored policy and intervention need to be the paradigmatic approach to address the predicament, and to prevent further illegal encroachment to this generation's hard-earned savings, tranquillity, and time.

The Heightened Risk on Personal Safety

Recent online scams operations have seen a diversification of entry point to reach the target. Scamwatch data shows that while email (194.501 reports) and text messages (191.227), with a combined number of 385.728 reports, remain the top contact methods for scams throughout 2023-February 2025, social media (38.311) and mobile apps (14.247) contribute considerably as another entry points for scams to the overall reports with 52.558 reports (NASC, 2025).

The use of social media and mobile apps for malicious purposes, such as scams, presents another unsolicited intrusion on the personal space, and therefore safety. In one method, the operation involves the sending of direct messages through LinkedIn, offering work-from-home job offers and in return, requesting the sending of personal data as one of the requirements to accept the job offers (Cross, 2014). In another method, one Sydney bank worker lost AU$157,000 as she was tricked to trade in a cryptocurrency scam by a verified profile account persona that she met on Tinder (9News, 2023).

People use different social media for different purposes, including but not limited to the search for entertainment, professional advancement, and social interaction (Sheldon, 2015). The pervasive spread of online scams in various social media and mobile apps, suppresses the attainment of these varied personal objectives of social media use, and put the users at risk. The responsibility to eradicate the spreading of scams via social media and mobile apps should not lie solely on the users, a significant portion of it should also be rendered to the online platforms. This includes the improvement over the security of the platforms, such as enhancing the reliability of users' verification, and the detection of scam patterns and activities, especially in the wake of AI-powered scams.

The Cross-Jurisdictional Issue in Law Enforcement

Online scams are traditionally considered to be a low to medium risk crime for the perpetrator, primarily because direct encounter between the target and the perpetrator is not necessarily needed. Furthermore, with the usage of AI, the traceability of the crime leading to the direct perpetrator is even more convoluted. This indirect nature of interaction, often involving third parties, such as email and social media platforms, flourishes the cross-jurisdictional proclivity for online scams operations. Particularly in Australia's context, such a cross-jurisdictional scams operations are motivated to target Australia given the comparative wealth that Australia has in the region (The Australian Transaction Reports and Analysis Centre [AUSTRAC], 2024).

AUSTRAC estimates that the scams targeting Australians are substantially organized by offshore criminals, particularly the transnational serious and organised crime groups (AUSTRAC, 2024). In multiple online scams cases targeting the Australians, AUSTRAC's estimate is confirmed. In one cryptocurrency scam case, the culprit launched his operation from the Ukraine by specifically targeting Australians (ABC, 2024). In another case, particularly in romance scam case, some 250 suspects were based in Manila, the Philippines and managed to potentially swindle around 5000 Australians (AFP, 2025). Another account also noted the large-scale scam operations from Cambodia, with around 100,000 people confined in cyber-scam compounds around Cambodia, and are forced to engage in cybercriminal activities, including fraudulent investment, romance and cryptocurrency scams (United Nations Office on Drugs and Crime, 2023).

This cross-jurisdictional operations may present a challenge for Australia's law enforcement to immediately act, for traditionally, law enforcement measure will be led by the law enforcement authority of the respective State where the crime or the criminal is situated. To this end, offshore criminal intelligence sharing is vital. However, several issues may still hamper this effort, including the transactional tendency of intelligence sharing and the lack of mutual trust between offshore law enforcements (Phil et al., 2018). While a notification on possible scams operations to the respective State may be useful to start build the trust and assist said law enforcement measure, a more robust and well-rounded approach may yield a more promising and expedient result. To this end, the institutionalization of both bilateral and regional assistance needs to be considered in order to garner trust and close the looming disparity of law enforcement's capacity between States in the region.

THE ROLE OF KEY STAKEHOLDERS AND STRATEGY IN ADDRESSING ONLINE FRAUD AND SCAMS

Key Stakeholders Mapping in Australia

The Australian Competition and Consumer Commission (ACCC), the Australian Signals Directorate (ASD), and FPD are deemed to be the key actors involved in addressing AI-generated online scams and fraud in Australia. Combined, these three institutions hold the regulatory, administrative, and law enforcement powers requisite to generally prevent and disrupt the spread of online scams in digital platforms. It should also be noted that various other sectorized institutions contribute to the scams control in Australia, including, but not limited to AUSTRAC, ASIC, and the Australian Communications and Media Authority (ACMA).

Table 2.1 Australia's Governmental Initiatives to Address Online Scams

Stakeholder	Statutory Basis	Strategic Role on Online Scams Control
ACCC	Competition and Consumer Act 2010.	Leads the NASC.
ASD	Public Governance, Performance and Accountability Act 2013; and the Intelligence Services Act 2001	Prevent and disrupt offshore cyber-enabled crime; runs the Australian Cyber Security Centre; coordinates with NASC.
FPD	Federal Police Act 1979	Enforcing criminal law; leads the Joint Policing Cybercrime Coordination Centre; coordinates with NASC.
AUSTRAC	Anti-Money Laundering and Counter-Terrorism Financing Act 2006.	Involved when online scams use money laundering technique to transfer and layer the criminal proceeds; coordinates with NASC.
ASIC	Securities and Investments Commission Act 2001; Business Names Registration Act 2011; Corporations Act 2001; Insurance Contracts Act 1984; National Consumer Credit Protection Act 2009; and Financial Accountability Regime Act 2023	Regulate and enforce scams related issues in financial product and services, such as the taking down of investment scam websites, and evaluation over banks' scams prevention mechanism; seek civil penalties and prosecute offenders for the purpose of consumer protection in financial product and services; coordinates with the NASC.
ACMA	Telecommunications Act 1997; Broadcasting Services Act 1992; and Australian Communications and Media Authority Act 2005.	Register and enforce rules to telecommunications sector on scams issues; coordinates with the NASC.

Australian Competition and Consumer Commission

ACCC is tasked with the administering and enforcing of primarily, the Australia's Competition and Consumer Act 2010. In this regard, the ACCC for instance managed to bring a case against Qantas pertaining to the offering and selling of an already cancelled flight tickets which misled the consumers (Federal Court of Australia, 2024). Additionally, since 2023, the ACCC is also mandated to run the Australia's NASC, a collaborating platform involving representatives from the industry and government to disrupt scammers and raise awareness on the issue.

Australian Federal Police

The AFP can be classified within the law enforcement function as it enforces Australia's criminal law, contributes to combat the transnational, serious, and organised crime impacting the Australia's national security, and protect Australia's interest from criminal activity both home and offshore. In relation to online scams, AFP by collaboration with partners both home and abroad, was particularly involved in Operation Aquila which addresses cybercrimes, including identity fraud, Operation Nebulae which brough about the global take down of a phishing-as-a-service platform known as LabHost. and Operation Firestorm, which concentrated to cyber criminals and human trafficking targets in Southeast Asia and Eastern Europe (AFP, 2024).

Australian Signals Directorate

ASD is a government agency which holds the responsibility for foreign signals intelligence and cyber security. In relation to online scams issue, within the ASD, sits the Australian Cyber Security Centre (ACSC), which is tasked as the technical authority of the government on cyber security. In contributing to scams control, ACSC is involved in several related services, including the reporting mechanisms via CyberReport and 1300 CYBER1 (1300 292 371), and the updating of relevant alerts, advisories, and notifications on potential cyber security threats.

Strategy in Addressing Online Fraud and Scams

Three approaches form the hallmark of Australia's current response to online scams, encompassing the regulatory framework, institutional governance, and law enforcement. While generally deemed to having brought about positive outcome, assessment on these approaches is still warranted to detect possible space for improvement.

Regulatory Framework

Scams Prevention Framework Bill 2025

Receiving the Royal Assent on 20 February 2025, the Bill came into force on 21 February 2025. Under this Bill, providers are obliged to take steps to comply with the standardized principles to protect Australians from scams. These principles encapsulate the governance arrangements relating to scams and the prevention, report, disruption, and response to scams. This Bill also tasks the government to create an enforceable Scams Prevention Framework Code containing more detailed provisions on the principles, including sector-specific requirements for the service providers (Scams Prevention Framework Bill 2025).

While the Bill is still relatively new, some concerns are levied upon this Bill, such as the legislation process which was deemed to not substantially take into account the inputs from public consultation by the Senate Standing Committees on Economics, the need for a 12-month transitional period from the industry, clarification for '*actionable scams intelligence,*' and the risk of misconduct by vexatious or speculative litigants within the system (GT Law, 2025).

Institutional Governance

National Anti-Scam Centre

The Australian Government in July 2023 invested AU$58 million for the establishment and the running of the NASC. Sitting within and led by the ACCC, the NASC orchestrates the coordinated measures by various entities, both from within the government and representatives from the industry in controlling scams. One of the products of the NASC is a reporting mechanism named the Scamwatch, which data is essential to the overall reading of scams pattern in Australia. Additionally, the NASC establishes various fusion cells, time-constraint task forces designed to address specific scams. Apart from the collaboration and disruption function, NASC also holds outreach function to raise the awareness on scams. However, the disproportionate victimisation of the elderly generation indicates the need for Anti-Scam Centre to diversify its method of public awareness campaign and its presence within the society.

Safe-Scam Accord

Launched in 2023 and applicable to all members of the Australian Banking Association and the Customer Owned Banking Association, this private sector-led initiative provides common thresholds for Australian banks in addressing scams and specific timeline for its fulfilment. These thresholds cover the disrupt, detect, and respond strategies, whereby some of the determined outputs of these strategies include, the name checking technology to mitigate the potential scam when the name does not match, the use of biometric check for new individual customer to verify the customer's identity, scams intelligence sharing involving the AFCX, and the limiting of payments to high-risk channels such as some crypto currency platforms (Australia Banking Association, 2023).

However, the advancement of scams tactics and methods may have surpassed the security thresholds set within this Accord. In one scam case, a person was duped to disclose two six-digit passcodes to a scammer who was able to contact him through a 1300 phone number. Such a 1300 phone number drew

a similarity with the phone number used multiple times in legitimate messages by the HSBC Bank Australia Limited. Following the disclosure of passcodes, an unauthorized transaction was made by the scammer. The issue was brought to AFCA. In its Determination, AFCA holds that the complainant is entitled for compensation from the bank in this sophisticated bank impersonation scam for the involuntary disclosure of his passcodes and for the bank's conduct in mishandling said scam issue (AFCA, 2024).

Law Enforcement

Joint Policing Cybercrime Coordination Centre (JPC3)

Under the coordination of the AFP, JPC3, which was launched in March 2022, coordinates Australia's policing response to high volume cybercrime. To do so, JPC3 collaborates with representatives from relevant government agencies, banking and financial sectors, and other key stakeholders, including international law enforcement agencies. One example of this collaborative ecosystem was Operation WICKHAM with the United States Secret Service that pursued an attempt to launder US$100 million stolen from victims who invested in a global investment scam (AFP, 2024). In another case, through Operation Guardian, JPC3 collaborated with various private entities to minimise the misuse of PII due to the data breaches in Medibank, Optus, MyDeal, Latitude; and Go-Anywhere.

Nevertheless, while serves as a collaborative model, JPC3 prioritises high volume cybercrimes. Such a threshold provides a room for JPC3 to determine which case to pursue based on its internal discretion and assessment. In online scams cases, the perpetrators are not always associated with sophisticated syndicates. Many acts on their own and separately, may not necessarily be deemed to have caused systematic losses. This is a trend that JPC3 does not necessarily cover.

BEST PRACTICES AND POLICY RECOMMENDATION

With economic losses of reported scams continue to decrease from 2023 to February 2025, Australia's approach to online scams indicates a degree of efficacy. This progress can be attributed to three traits of Australia's effort to control online scams, namely the whole-of-nation approach, the multilayered reporting mechanism, and the data-centric movement.

Best Practices

Whole-of-Nation Approach

Scams control becomes a priority of all fabrics of the State, not only the government. As discussed in the previous section, private entities-led initiative also colours Australia's overall effort to combat online scams, such as through the Safe-Scam Accord. In the government-led initiative, such as the NASC, representatives from the industries are also given with a say in helping to identify the surging trend of online scams. This indicates the blurring of the traditional work division, making the combating of online scams an interest of all, which simultaneously contributes to the raising of awareness among the population, wherein Commonwealth Bank research finds that 60% of Australians are now more concerned about online scams than a year ago (Commonwealth Bank, 2025).

Multilayered Reporting Mechanisms

There are multiple reporting mechanisms available for scams cases, from Scamwatch, ReportCyber, IDCARE, to others. While some of these reporting mechanisms may eclipse each other, one key takeaway that may serve as the best practice is that these multiple reporting avenues provide Australians with more access and alternatives to respond to scams. These multiple reporting mechanisms also allow the Australian Government

to amass and wield a substantially comprehensive set of data pertaining to scams from the submitted reports, from the prevalent modus operandi to the contour of the most impacted group in the society.

Data-Centric Movement

The accumulated data from Australia's scams reporting mechanisms equip the government to periodically evaluate its effectiveness in addressing scams issue. The evaluation allows the government to recalibrate upon the changing landscape of online scams, as indicated by the passing of the Scams Prevention Framework Bill 2025. Additionally, to a certain extent, a significant portion of said data is also widely disseminated to the public, allowing anti-scam initiatives driven by the community to flourish.

Policy Recommendations

Australia's robust intervention, particularly since 2023, has done reasonably well in attempting to curb the losses from online scams. To improve this, several additional measures can still be considered to size up the government's response's efficacy against the AI-powered online scams.

Enhanced Collaboration with Private Sector

Private sector contributes significantly to the developing of generative AI. Some of the latest breakthroughs in various disciplines, such as the use of AI for flood forecasting, detecting wildfires, to teaching personalization, can be attributed to private entities-led AI development initiatives. Through their inventive nature, these private entities should also be involved in the overall effort to combat scams. Additionally, to entities serving as online platforms, their collaboration is indispensable to help detect and supress the spread of scams.

Development of AI for Law Enforcement Purpose

Contrary to its malicious use, AI can also be used to counter crimes. The AFP in collaboration with Monash University for instance established the AiLECS (the Artificial Intelligence for Law Enforcement and Community Safety) Lab to develop AI for automated detection and triage of child sexual exploitation material (AFP, 2022). Initiatives to develop the use of AI for law enforcement purpose like AiLECS should be multiplied by the relevant stakeholders and expanded to address other forms of crimes, including scams. Collaborating with and maximising the resources in the academics and industries, law enforcement apparatus can be benefited in developing AI-driven counter measures to disrupt the use of deepfake, chatbots technologies often used by scammers.

Elderly Generation Intervention

The disproportionate victimisation of the elderly generation indicates a concerning knowledge disparity between age groups on the current scams control response. A more robust intervention is therefore needed. Identification upon the avenues which the elderly generation engage the most should be a priority and the baseline for the NASC to intervene. This intervention should encompass a nation-wide awareness campaign for a family-oriented protection mechanism for the elders. Members of the family should be encouraged to proactively check on the elders on the digital activities that they are engaging with. A fusion cell specifically tasked to decrease the proportion of the elderly generation as victims of online scam can be considered.

Regional Arrangement

From multiple examples as previously discussed, scammers targeting Australians can be based offshore, particularly from across Southeast Asia. Regional policy framework to tackle these offshore criminals needs to be further materialized. One viable avenue to do so is by maximising the Plan of Action to Implement the Association of Southeast Asian Nations (ASEAN)-Australia Comprehensive Strategic Partnership (2025-2029). The detailing of this regional arrangement should address multiple contemporary issues within the spheres of cyber security and transnational crime, such as, common definition and threshold on the malicious use of AI,

the mechanism for joint law enforcement operations, and joint research initiative to develop generative AI to counter AI-powered scams.

Bilateral Support

There exists a considerable capacity gap between states in handling online scams. With the relatively advanced mechanism that Australia has established in eradicating scams, technical assistance to the government of other states, particularly where scammers predominantly operate, should take place. This can be achieved through the secondment of relevant Australian personnels in the respective state for knowledge sharing, and where possible the institutionalization of *ad-hoc* joint operations or a more permanent criminal intelligence exchange mechanism.

REFERENCES

Articles and Reports

Association of Southeast Asian Nations, Plan of Action to Implement the ASEAN-Australia Comprehensive Strategic Partnership (2025-2029) (2024).

Attorney-General's Department, National Plan to Combat Cybercrime 2022 (2022).

Australia and New Zealand Banking Group Limited, Cyber Security for Seniors, available at https://www.anz.com.au/security/protect-your-family/seniors-cyber-security/#:~:text=This%20could%20be%20due%20to,the%20signs%20of%20a%20scam, last accessed on 28 March 2025.

Australian Banking Association, Protect Your Heart and Bank Account from Romance Scams, available at https://www.ausbanking.org.au/protect-your-heart-and-bank-account-from-romance-scams/#:~:text=ABA%20CEO%20Anna%20Bligh%20said,paradise%2C%E2%80%9D%20Ms%20Bligh%20said, last accessed on 28 March 2025.

Australian Banking Association, Scam-Safe Accord, available at, https://www.ausbanking.org.au/new-scam-safe-accord/, last accessed on 28 March 2025.

Australian Broadcasting Corporation, Australians Targeted for Cryptocurrency Scams by Overseas Call Centres because They are 'Easy Prey', Former Worker Says, available at https://www.abc.net.au/news/2024-10-07/scammers-are-targeting-australians-in-offshore-call-centres/104406170, last accessed on 28 March 2025.

Australian Broadcasting Corporation, Authorities Warn AI, Deepfake Technology in Romance Scams Costing WA Victims Thousands, available at https://www.abc.net.au/news/2024-08-28/deepfake-ai-used-in-wa-romance-scams/104279902, last accessed on 28 March 2025.

Australian Broadcasting Corporation, Scammers Use Artificial Intelligence to Impersonate Sunshine Coast Mayor as Experts Warn of Video Call Cybercrime Tactic, available at https://www.abc.net.au/news/2024-05-02/scammers-ai-impersonate-sunshine-coast-mayor-video-call/103794690, last accessed on 28 March 2025.

Australian Bureau of Statistics, Australian National Accounts: National Income, Expenditure and Product (https://www.abs.gov.au/statistics/economy/national-accounts/australian-national-accounts-national-income-expenditure-and-product/mar-2024) (2024).

Australian Competition and Consumer Commission, Report of the National Anti-Scam Centre on scams data and activity 2024 (2025).

Australian Cyber Security Centre, Types of Scams, available at https://www.cyber.gov.au/learn-basics/watch-out-threats/types-scams, last accessed on 28 March 2025.

Australian Federal Police, AFP Reveals 'Rom-Con' Script Used to Scam Victims on Dating Apps, available at https://www.afp.gov.au/news-centre/media-release/afp-reveals-rom-con-script-used-scam-victims-dating-apps#:~:text=The%20script%20was%20uncovered%20during,with%20on%20online%20dating%20apps, last accessed on 28 March 2025.

Australian Federal Police, AFP Submission to the Parliamentary Joint Committee on Law Enforcement: Inquiry into the Capability of Law Enforcement to Respond to Cybercrime (2024).

Australian Federal Police, AFP Takes the Fight to Cybercriminals in 2024, available at https://www.afp.gov.au/news-centre/media-release/afp-takes-fight-cybercriminals-2024, last accessed on 28 March 2025.

Australian Federal Police, Australian Federal Police Annual Report 2021-22 (2022).

Australian Federal Police, Beware of Black Friday and Cyber Monday Scams, available at https://www.afp.gov.au/news-centre/media-release/beware-black-friday-and-cyber-monday-scams, last accessed on 28 March 2025.

Australian Securities and Investments Commission, ASIC Enforcement and Regulatory Update July to December 2024 (2025).

Australian Signals Directorate, Annual Cyber Threat Report 2023–2024 (2024).

Australian Transaction Reports and Analysis Centre, The Money Laundering in Australia National Risk Assessment 2024 (2024).

Button, Mark, Vasileios Karagiannopoulos, Julak Lee, Joon Bae Suh, and Jeyong Jung. 2024. "Preventing Fraud Victimisation against Older Adults: Towards a Holistic Model for Protection." *International Journal of Law, Crime and Justice* 77 (June):100672. https://doi.org/10.1016/j.ijlcj.2024.100672.

Commonwealth Bank, Less Than 10% of Aussies Would Discuss Their Scam Experience with Family, available at https://www.commbank.com.au/articles/newsroom/2025/03/scams-talk-to-a-loved-one.html, last accessed on 29 March 2025.

Cross, C., & Layt, R. (2021). "I Suspect That the Pictures Are Stolen": Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities. Social Science Computer Review, 40(4), 955-973. https://doi.org/10.1177/0894439321999311 (Original work published 2022).

Cross, Michael. 2014. *Social Media Security: Leveraging Social Networking While Mitigating Risk*. Waltham, MA: Syngress.

Das, Ravindra. 2024. *Generative AI: Phishing and Cybersecurity Metrics*. 1st ed. Cyber Shorts Series. Boca Raton: Taylor & Francis Group.

Desolda, Giuseppe, Lauren S. Ferro, Andrea Marrella, Tiziana Catarci, and Maria Francesca Costabile. 2022. "Human Factors in Phishing Attacks: A Systematic Literature Review." *ACM Computing Surveys* 54 (8): 1–35. https://doi.org/10.1145/3469886.

Gilbert + Tobin Law, The Scams Prevention Framework Legislation Passes Parliament: Time to Get Your House in Order, available at https://www.gtlaw.com.au/insights/the-scams-prevention-framework-legislation-passes-parliament-time-to-get-your-house-in-order2, last accessed on 28 March 2025.

Grimes, Roger A. 2024. *Fighting Phishing: Everything You Can Do to Fight Social Engineering and Phishing*. 1st ed. Indianapolis: John Wiley and Sons.

International Telecommunication Union, Individuals Using the Internet: Australia (https://datahub.itu.int/data/?e=AUS&c=701&i=11624) (2024).

Kowalick, Phil, David Connery, and Rick Sarre. 2018. "Intelligence-Sharing in the Context of Policing Transnational Serious and Organized Crime: A Note on Policy and Practice in an Australian Setting." *Police Practice and Research* 19 (6): 596–608. https://doi.org/10.1080/15614263.2018.1507899.

National Anti-Scam Centre, National Anti-Scam Centre Advisory Board Terms of Reference (2023).

National Anti-Scam Centre, Scams Statistics Interactive Data (https://www.nasc.gov.au/scam-statistics) (2025).

RMIT University, Elon Musk Used in Fake AI Videos to Promote Financial Scam, available at https://www.rmit.edu.au/news/factlab-meta/elon-musk-used-in-fake-ai-videos-to-promote-financial-scam, last accessed on 28 March 2025.

Sheldon, Pavica. 2015. *Social Media: Principles and Applications*. Lanham : Boulder : New York : London: Lexington Books.

United Nations Office on Drugs and Crime, Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia (2023).

9News, News, Sydney Bank Worker Loses $157,000 in 'Pig Butchering' Romance Scam, available at https://www.9news.com.au/national/sydney-bank-worker-loses-157000-in-pig-butchering-romance-scam/3fc559d6-163a-48c8-8317-283eb806a7c0 last accessed on 28 March 2025.

Legislations and Cases

Australian Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

Australian Broadcasting Services Act 1992.

Australian Business Names Registration Act 2011

Australian Communications and Media Authority Act 2005.

Australian Competition and Consumer Act 2010.

Australian Corporations Act 2001.

Australian Financial Accountability Regime Act 2023.

Australian Financial Complaints Authority, Determination, Case number 12-00-1016692 (2024).

Australian Insurance Contracts Act 1984.

Australian Intelligence Services Act 2001.

Australian National Consumer Credit Protection Act 2009.

Australian Public Governance, Performance and Accountability Act 2013.

Australian Scam Prevention Framework Bill 2025 (as passed by both Houses version).

Australian Securities and Investments Commission Act 2001.

Australian Telecommunications Act 1997.

Federal Court of Australia, Judgment, Australian Competition and Consumer Commission v Qantas Airways Limited [2024] FCA 1219 (2024).

Safer Internet Lab

saferinternetlab.org

Jl. Tanah Abang III no 23-27
Gambir, Jakarta Pusat. 10160

Find Us On

CSIS Indonesia | Safer Internet Lab