





Year in Review 2023







Overview

The Department of Energy, Mines, Industry Regulation and Safety – Consumer Protection Division (Consumer Protection) receives thousands of enquiries concerning scam-related problems. Many of these are enquiries from people wanting to advise Consumer Protection of a potential scam.

Consumer Protection's Contact Centre provides information on whether they are scams, how to avoid losing personal and financial information and how to better protect themselves in the future.

The WA ScamNet team manages more complicated enquiries, often including situations where victims have fallen for a scam, where they have lost monetary amounts or personal information.

WA ScamNet uses the same scam categories as the Australian Competition and Consumer Commission's (ACCC) Scamwatch. This enables comparisons to be made between the reports received in Western Australia (WA) and nationally.



WA ScamNet

WA ScamNet receives reports of scams from several sources including:

- Online Scam Reporting tool (OSR) on www.scamnet.wa.gov.au;
- Consumer Protection Contact Centre:
- Crime Stoppers WA;
- WA Police; and
- other state and national government agencies.

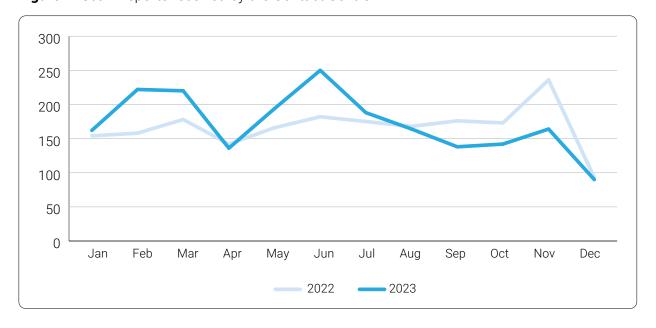
WA ScamNet receives calls about scams in WA, other areas in Australia and overseas. This report focuses only on reports and victims within WA.

WA ScamNet's OSR allows people to report a scam anonymously, or on behalf of someone else or a business. Data, including demographic information, is collected relating to the scammer, the victim, and the type of scam.

Contact Centre

In 2023, Consumer Protection's Contact Centre received 2,070 calls relating to scams, three per cent more than in 2022. The average number of calls each month also increased from 167 to 173.

Figure 1. Scam reports received by the Contact Centre



The top two scams reported to the Contact Centre in 2023 were Facebook scams (159 enquiries, 62 per cent increase from 2022) and cryptocurrency investment scams (72 enquiries, 13 per cent increase from 2022). Case studies of these scams are provided at the end of this report.

Losses

Table 1 shows the number of reports and amounts lost to scams in 2023. This includes the reporting of four significant losses through investment scams:

- \$1.7 million in November;
- \$1.6 million in April;
- \$1.4 million in July; and
- \$960,000 in March.

Table 1. Total amount lost and number of reports to WA ScamNet in 2023

Amount lost	Number of reports	Victim reports with financial losses
\$21,995,489 (+36%1)	4,117 (-2%)	1,398 (+14%)

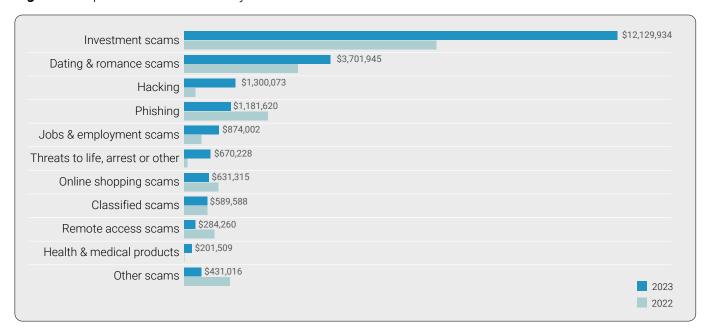
Figure 2. Monthly comparison of amount lost and number of reports for 2022 and 2023



^{1.} The database is updated as new information comes to light. Therefore 2022 figures reported may differ from the 2022 WA ScamNet Year in Review report.

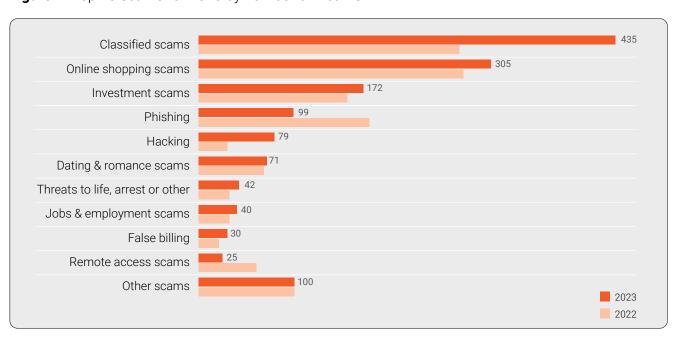
The top 10 scam categories in 2023, by amount lost, accounted for 98 per cent of the total losses recorded, with investment scam losses contributing to 55 per cent of losses (Figure 3). The "Other scams" category consists of scams not included in the top 10 categories.

Figure 3. Top 10 scams for 2023 by amount lost



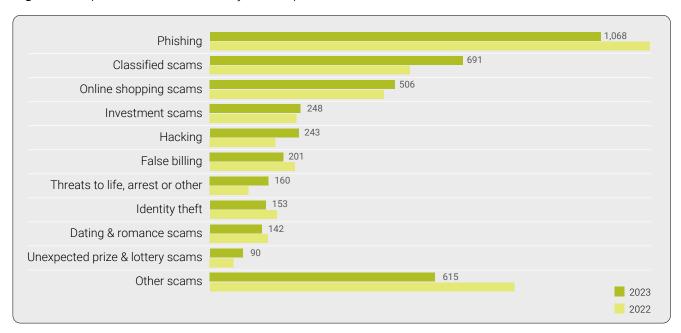
In 2023, 1,398 victims reported losing money to a scam, with 22 per cent falling for an online shopping scam (Figure 4). The top 10 scams, by number of victims, account for 93 per cent of victims.

Figure 4. Top 10 scams for 2023 by number of victims



Phishing scams accounted for 26 per cent of the total scam reports in 2023 (Figure 5) with the top 10 reported scams making up 85 per cent of the total reports.

Figure 5. Top 10 scams for 2023 by total reported







Demographics

Age group information is only captured through the OSR. Age groups were provided in a total 1,799 reports in 2023, 74 per cent of total reports received through the OSR. The 35 to 44 year-old age group reported the highest losses (Figure 6) with a total loss of \$1,857,724. This represents 34 per cent of losses with demographic information. This was due to three victims with a combined loss of over \$1.3 million to investment and dating and romance scams.

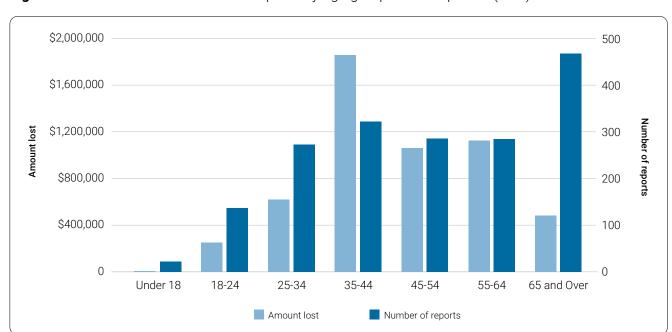
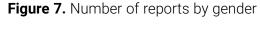


Figure 6. Amount lost and number of reports by age group where reported (OSR) in 2023

Females accounted for a higher proportion of the reports made (Figure 7). However males accounted for the majority of the money lost to scammers (Figure 8) in 2023.



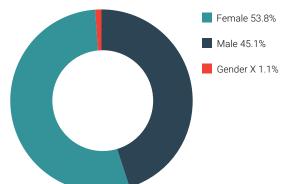
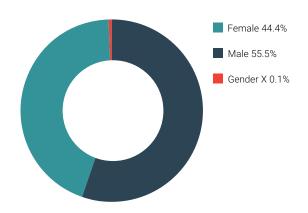


Figure 8. Amount lost by gender



CASE STUDY:

Investment/romance scam

Victim reported loss: \$89,000

A man fell victim to a romance scam that ended with a cryptocurrency investment scam.

The victim started communicating with the scammer on Tinder, who encouraged him to invest in a cryptocurrency platform www.wtnvso.com.

He made payments totalling \$60,000 USD (\$89,000 AUD) which were paid through Binance. These included \$9,000 in fees and taxes.

The victim was told the investment would keep growing as long as more funds were deposited. After some time, the scammer sought further payments as the victim wanted to release the funds. The victim handed over personal identification information when trying to have the fees released.

WA ScamNet assessed the website which appeared to have been shut down. The website had many negative reviews online stating other people had invested money and not been able to retrieve any.

The company name was not found to be registered with the Australian Securities and Investments Commission or any overseas regulator.

Scammers are using the hook of romance to get the victim on the line, and by manipulating their emotions, steer the relationship towards investments. This usually ends with a cryptocurrency investment scam.

2023 **Fact Bank**



Number of reports

354 Number of victims (with reported losses)

\$20,087,973 Reported losses

WA ScamNet's role:

- Advised the victim on what to look out for regarding investments scams and how scammers are using romance and companionship to lure unsuspecting victims.
- Provided details for IDCare, a national identity and cyber support service, as the victim had handed over personal information.
- Assessed the website for business registrations, contacts and reviews.
- Provided information to Consumer Protection's Community and Media Engagement team to be used to educate the public on how to spot the scam.

CASE STUDY:

Facebook Marketplace scam

Victim reported loss: \$3,600

A female victim responded to a rental listing on Facebook Marketplace. She was told to send through her details to an email address supposedly for the partner of the owner of the property.

Emails were sent back and forth discussing the property and went through an application process. The victim was advised they were successful in the process and needed to send through rent and bond via bank transfers.

After doing further research into the property, the victim found the actual online listing of the property by a property management group. The group was aware the pictures were being used fraudulently through fake listings online.

The victim had sent through payslips, identification documents, family relationship history and their signature to the scammers.

WA ScamNet's role:

- Reported Facebook listing.
- Reported receiving bank account.
- Updated WA ScamNet page to alert people of rising amount of fake rental listings on Facebook Marketplace and other online platforms.



Number of reports

Number of victims (with reported losses)

Government of Western Australia Department of Energy, Mines, **Industry Regulation and Safety**

Regional offices:

Goldfields/Esperance (08) 9021 9494 Great Southern (08) 9842 8366 Kimberley (08) 9191 8400 (08) 9920 9800 Mid West North West (08) 9185 0900 South West (08) 9722 2888

Consumer Protection Division

Gordon Stephenson House Level 2/140 William Street Perth Western Australia 6000

Locked Bag 100 East Perth WA 6892

Call: 1300 30 40 54

Email: consumer@dmirs.wa.gov.au











This publication is available on request in other formats.

National Relay Service: 13 36 77

Translating and Interpreting Service (TIS): 13 14 50