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

Year in Review 2021
Scam Report

CONSUMER PROTECTION
WESTERN AUSTRALIA

WAScamNet

Overview

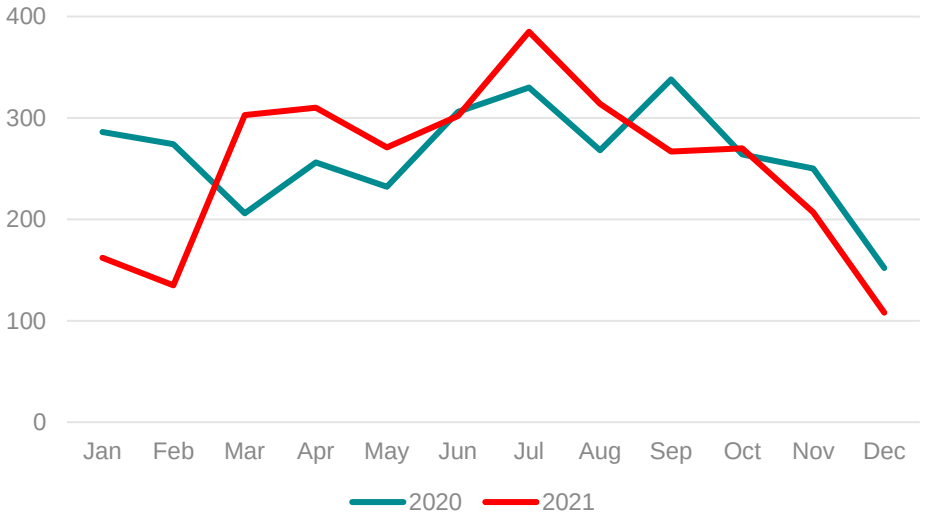
Each year, Consumer Protection receives a large number of enquiries concerning scam-related problems. Many of these enquiries are lower level enquiries where consumers wish to advise of an email, phone call or some form of interaction they have had with a potential scam. These types of enquiries are dealt with by Consumer Protection's Contact Centre. Other more detailed enquiries are managed by Consumer Protection's WA ScamNet team; these enquiries tend to be more detailed in nature often including situations where consumers have fallen victim to a scam and lost money, personal information, banking information or commercial information.

WA ScamNet uses the same scam categories used by the Australian Competition and Consumer Commission's (ACCC) ScamWatch to enable a comparison to be made between the reports received in Western Australia and nationally.

Contact Centre

In 2021, Consumer Protection's Contact Centre received 3,034 calls relating to scams, four per cent fewer than in 2020 continuing a downward trend from 2019. The average number of calls each month was also down from 264 to 253 calls a month.

Figure 1. Scam reports received by the Contact Centre



The top two scams reported to the Contact Centre were the Australian Tax Office scam (94 enquiries, 13 per cent decrease from 2020) and the Amazon scam (81 enquiries, 25 per cent increase from 2020). Scams relating to eBay increased 58 per cent from 19 enquiries in 2020 to 30 in 2021. In most cases, the scammers attempted to gain access to consumers' banking details by claiming there was an unsolicited purchase made on their eBay account. This increase is partially due to the COVID-19 pandemic and scammers taking advantage of consumers relying heavily on online shopping to buy goods.

WA ScamNet

WA ScamNet receives reports of scams from several different sources including an Online Scam Reporting tool (OSR), referrals from the Contact Centre and through collaboration with Crime Stoppers WA, WA Police and other state and national government agencies. Although WA ScamNet receives calls about scammers from WA, other areas in Australia and overseas, this WA ScamNet Year in Review only focuses on reports and victims in WA.

The OSR allows people to report a scam to WA ScamNet which they have been a victim of anonymously, or on behalf of, someone they know or a business. Data, including demographic information, is collected relating to the scammer, the victim and the type of scam. Other sources of information received by WA ScamNet do not include demographic information.

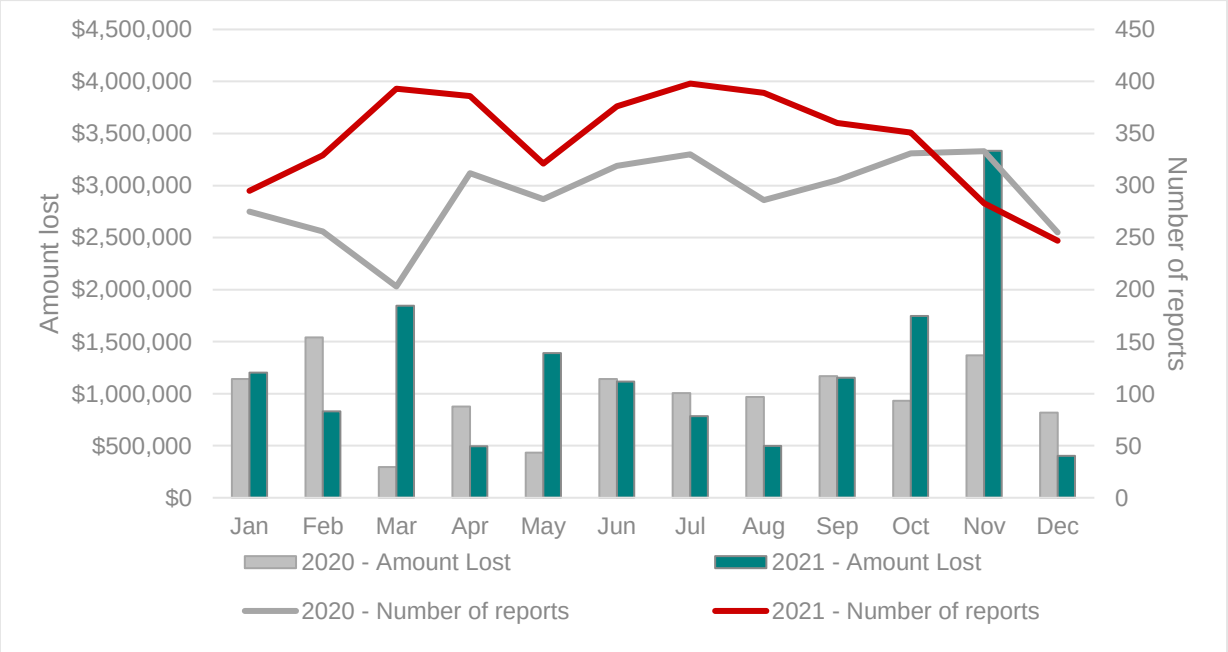
Losses

Table 1 shows the number of reports, and amounts lost, in 2021. This included two reported losses of $858,000 in January (psychic and clairvoyant) and $730,000 in October (investment scams).

Table 1. Statistics for reports to WA ScamNet for 2021

Amount lost	Number of reports	Reports with financial losses
$14,791,708 (+27%[1])	4,128 (+18%)	1,041 (+10%)

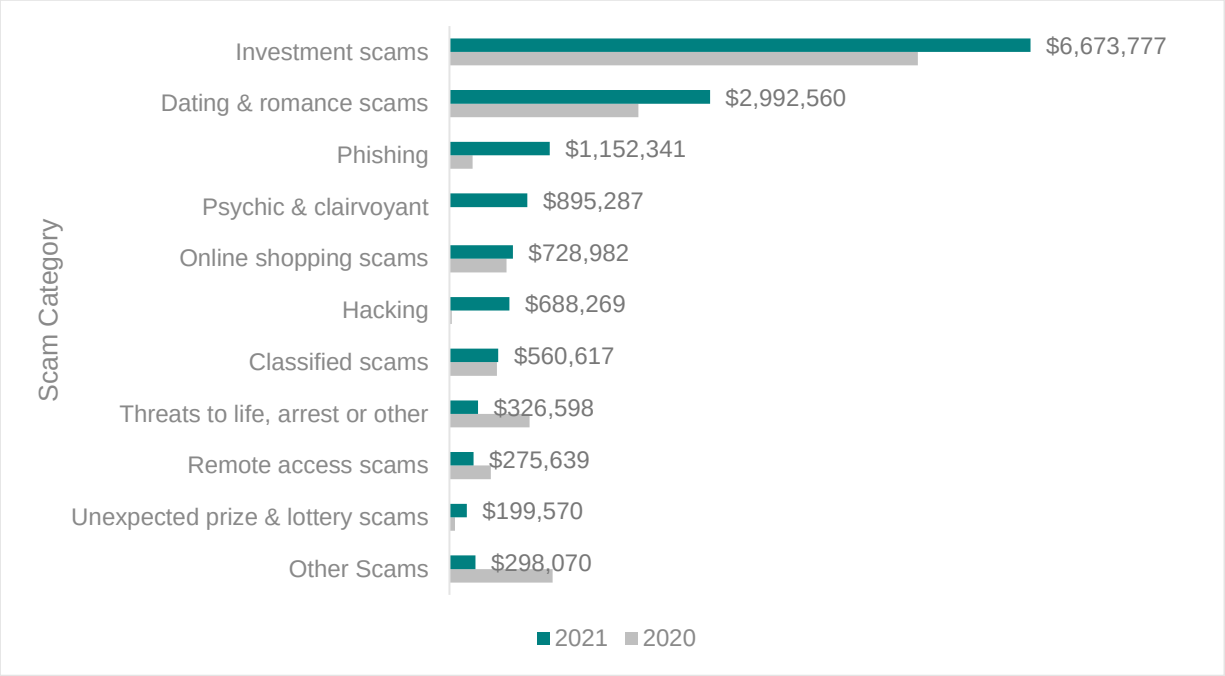
Figure 2. Total amount lost and number of reports to WA ScamNet



[1] As new information comes to light the database is updated. As such, the figures for 2020 for this report may differ from the 2020 WA ScamNet Year in Review.

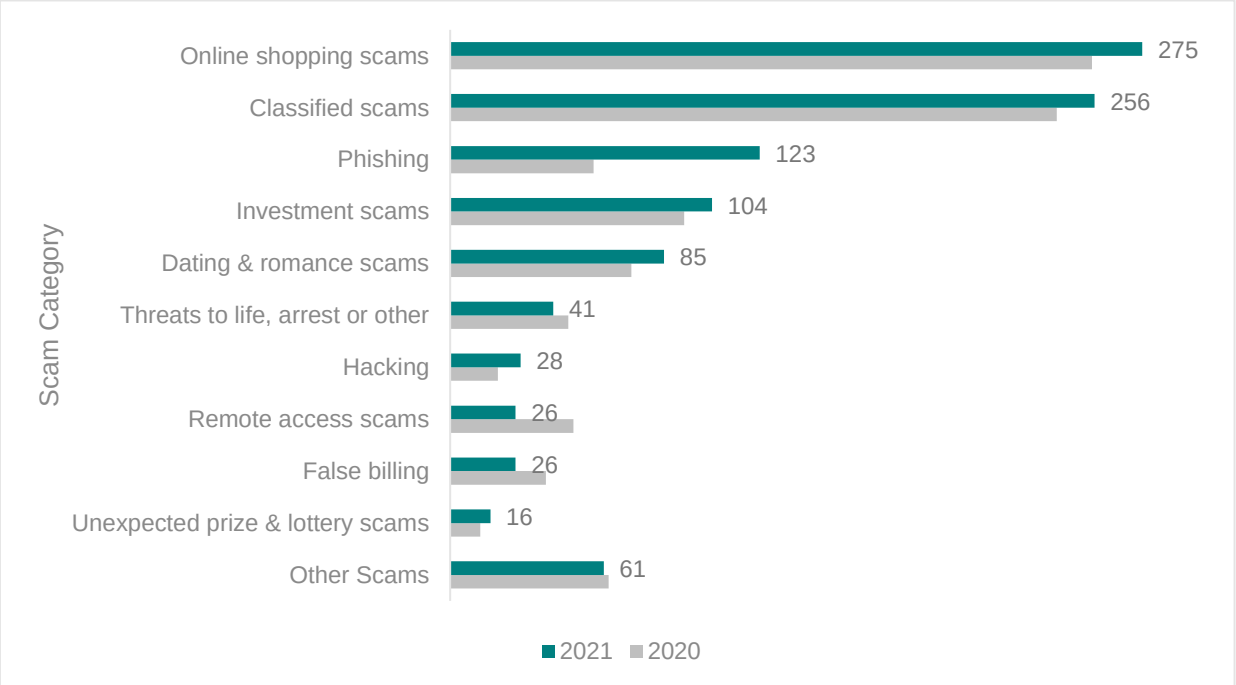
The top 10 scams, by amount lost, accounted for 98 per cent of the total losses recorded with investment scam losses contributing to 45 per cent of losses (Figure 3). The “Other Scams” category consists of those scams that are not in the top 10 categories.

Figure 3. Top 10 scams reported to WA ScamNet for 2021 by amount lost



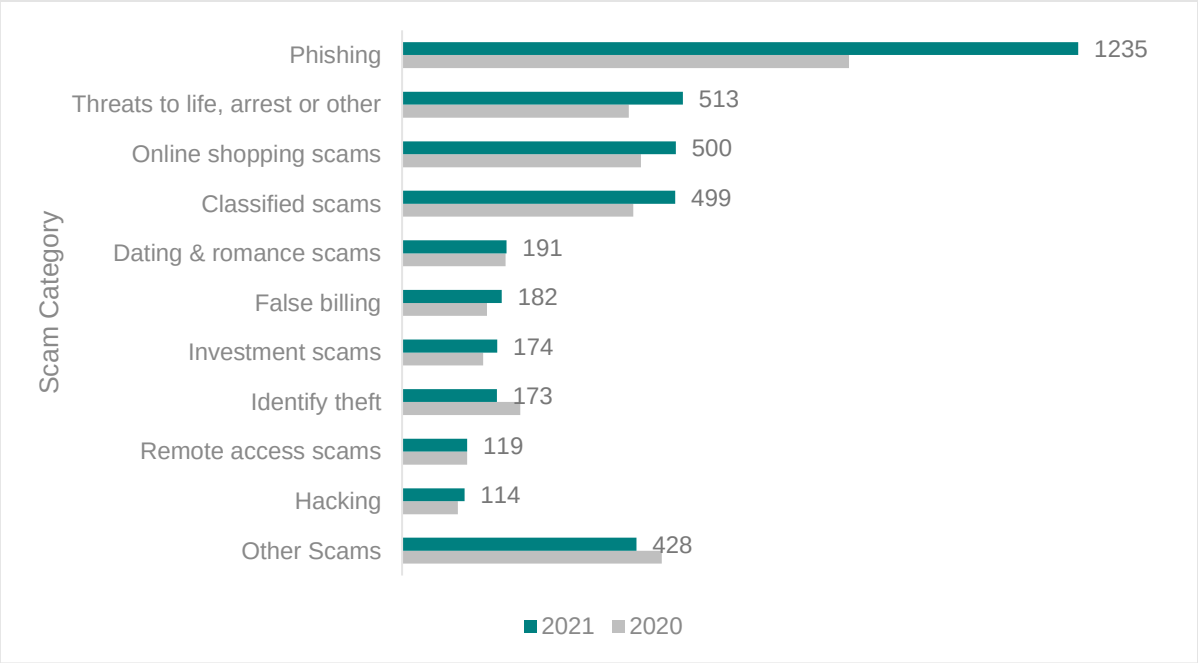
In 2021, 1,041 victims reported losing money to a scam with 26 per cent falling for an online shopping scam (Figure 4). The top 10 scams, by number of victims, account for 94 per cent of victims.

Figure 4. Top 10 scams by number of victims for 2021



Phishing scams accounted for 30 per cent of the total scam reports in 2021 (Figure 5) with the top 10 reported scams making up 90 per cent of the total reports.

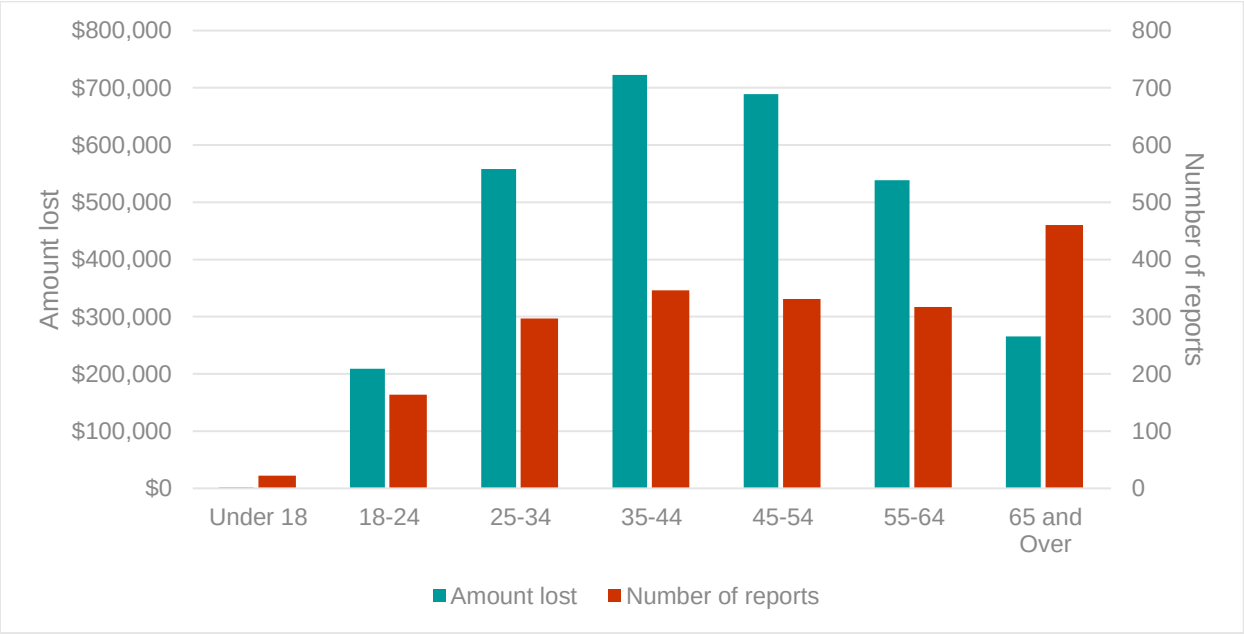
Figure 5. Top 10 scams reported to WA ScamNet for 2021 by total report



Demographics

Age group information is only captured through the OSR and was available for 1,937 reports in 2021 (72 per cent of total reports received through the OSR). The 35-44 year old age group reported the highest losses (Figure 6) with a total loss of $722,306 (24 per cent of losses with demographic information).

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



Not only did females account for a higher proportion of the reports made (Figure 7), they also accounted for the majority of the money lost to scammers (Figure 8) in 2021.

Figure 7. Gender by number of reports

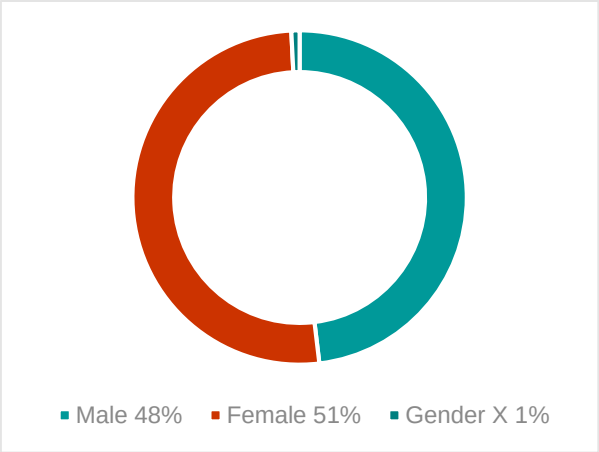
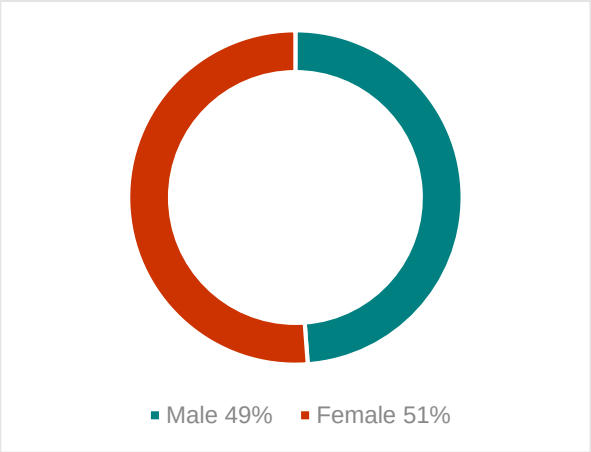


Figure 8. Gender by amount lost



Case Studies

Real life example: Payment redirection (Property Industries)

Scammers stole about $375,000 intended to fund the aged care costs of a 102 year old woman.

The woman's grand-daughter, who has enduring power of attorney, was organising the transfer of the funds from her grandmother's home sale to the aged care home through a settlement agent. Scammers intercepted email communications between the grand-daughter and the aged care facility and sent a bogus email purporting to be the nursing home advising of a change of bank account details for the transfer.

The grand-daughter sent these bank account details along with instructions to the settlement agent. When settlement occurred, the proceeds of $374,251 were transferred to the scammers' bank account in Sydney.

How the scam worked:

- The people behind this scam hack into email accounts (either the seller or buyer) and obtain information about financial transactions underway between sellers or buyers and real estate or settlement agents.
- The scammers may appear to take control of the business' email address or create a new, almost identical, email address (phishing) that is difficult to distinguish from the original.
- Using the new email address, the scammers try to have the parties to pay funds involved in the transaction into an alternative bank account/s under their control.

Assistance provided by WA ScamNet

- WA ScamNet reported the bank accounts and liaised with all affected parties to ensure their networks were not, or no longer, compromised.
- Information was provided to Consumer Protection's Property Industries Directorate to inform the industry of the issue and take the necessary steps to minimise its impact.
- Consumer Protection is currently working on providing an easy to follow guide for businesses to be able to consider their options for securing online payment and invoicing methods.

Real life example: Classified scam – AFL Grand Final Ticket Scam

Scammers target popular events and advertise fake tickets on online marketplace platforms, such as Gumtree and Facebook Marketplace, as people are using unsecured payment methods to purchase sought-after event tickets. Ultimately these platforms are designed for face to face transactions (such as paying cash or completing a bank transfer in sight of all parties when accepting the physical goods).

The AFL Grand Final was held in Perth's Optus Stadium for the first, and probably only, time. With only 10,000 public tickets available (not including club membership, corporate or box seating), they sold very quickly which caused a lot of fans to attempt to purchase tickets through online marketplaces.

How the scam worked:

- The victims posted 'wanted' ads on online marketplaces requesting tickets to the Grand Final, usually implying they would pay considerably more than the actual ticket price.
- They would then receive a response from someone who advised that they have tickets available. Usually with an excuse such as 'unable to come to Perth, family member not a fan of footy' etc.
- AFL Grand Final tickets were sold through Ticketmaster and were only available digitally, unless printed on a ticket stub at a Ticketmaster location. Due to COVID-19, tickets were required to be registered in each individuals name and held within the appropriate Ticketmaster account. If a consumer decided to sell a ticket, they were required to forward the ticket through their Ticketmaster account to the purchaser, where they would then have to accept through a Ticketmaster account. There was no limit on how many times a ticket could be forwarded and once a ticket was accepted this process was unable to be reversed.
- Victims were shown a screenshot of the ticket as proof the seller had one available, usually with the barcode crossed out so the ticket wasn't able to be stolen. They were requested to pay via bank transfer and the seller would then send a screenshot of the ticket/barcode, rather than them being forwarded the tickets through Ticketmaster.
- Victims attended Optus Stadium on game day only to find the ticket had already been used. They were not able to enter the venue.

Assistance provided by WA ScamNet

- Reported all bank accounts involved.
- Published media statement and email alert to advise consumers to beware.
- Provided the details to WA Police for their intelligence.

Real life example: Online shopping scam – Shipping Container Sales Scam

How the scam worked:

Victims respond to advertisements for shipping containers through Facebook Marketplace and Gumtree where they are then directed to a website which claims to be selling shipping containers at discounted prices.

Victims are presented with ABN information of legitimate businesses on the website and in correspondence and are directed to pay via bank transfer.

Once payment is received, minimal updates are provided on the arrival of the sea container. Victims also reported further demands for funds due to issues with the delivery, such as customs fees, insurance fees etc.

Websites identified by WA ScamNet were using stolen ABN details within the content of the websites and on invoices provided to victims to build trust that the purchase was legitimate.

Assistance provided by WA ScamNet

- ScamNet sent letters to ABN holders to advice their details has been used in what appears to be a scam website selling seat containers. The letters encouraged the ABN Holders to contact WA ScamNet and take steps to warn consumers of the fraudulent use of their information.
- WA ScamNet reported the scam websites to domain/network hosts to have the websites shutdown.
- WA ScamNet reported the bank accounts used in the scam to limit the impact on consumers and assist those who had sent funds to potentially obtain a refund.
- A new page was created on the WA ScamNet website listing the scam websites.
- Issued a scam alert email to the WA ScamNet email subscribers.

Real life example: Investment scam – Bitcoin

In 2021 WA ScamNet has received 72 reports (57 victim loss a total of $4,172,694.05) in relation to bitcoin investment scams.

WA ScamNet received a report that a lady in her 60's had fallen victim to a Bitcoin Investment scam. The victim thought, for the last year, she had been chatting to 'May Anderson', a financial advisor working for an investment company located outside of Australia, who was going to help her invest and make money through Bitcoin.

Contact with May and the investment company was through Whatsapp and a Gmail account. May instructed the victim to create an account on CoinSpot and Blockchain so she could invest through their platform. The victim was directed to purchase various amounts of Bitcoin and send them to Bitcoin wallet hashes (addresses) provided by May which she claimed was the victim's investment account that they held and managed on her behalf. May would also send information and updates about the investment via email and text message. At times, the victim provided the investment company remote access to her computer to assist with the transactions.

During the scam, the victim was told that May was on holiday and Chris would now assist her. The victim attempted to withdraw funds but Chris claimed there was suspicious activity on her account. The victim was advised she needed to pay tax before receiving funds. The victim had invested over $200,000 and still believed she was going to recover her investment.

The victim was told to "validate her wallet" by sending $40,000 worth of Bitcoin. As she was sending the extra money requested, Chris claimed she did it wrong and had her redo the transaction again. To encourage the victim throughout the scam that it was all legitimate, she was provided screenshots of her investment Bitcoin wallet which had 14 Bitcoin (worth about $900,000 at that time). Unknown to her, this wallet did not belong to her.

WA ScamNet showed the victim the differences between her Bitcoin Wallets (on CoinSpot or Blockchain) and the wallet she was shown as well as how she had been fooled into sending Bitcoin to numerous wallets and the ones she had control of were empty. Once cryptocurrency has been sent, the transaction cannot be reversed. The owners of the Bitcoin wallets are unidentifiable.