SCAMS PROTECTION AND AWARENESS SEMINAR

DEFINITIONS

Fraud

Fraud occurs when you did not authorise the transaction and/or method of loss.

Scam

A scam is when you willingly participated in the transaction but have been misled regarding the benefit or purpose.

AUSTRALIAN COMMUNITY IMPACT

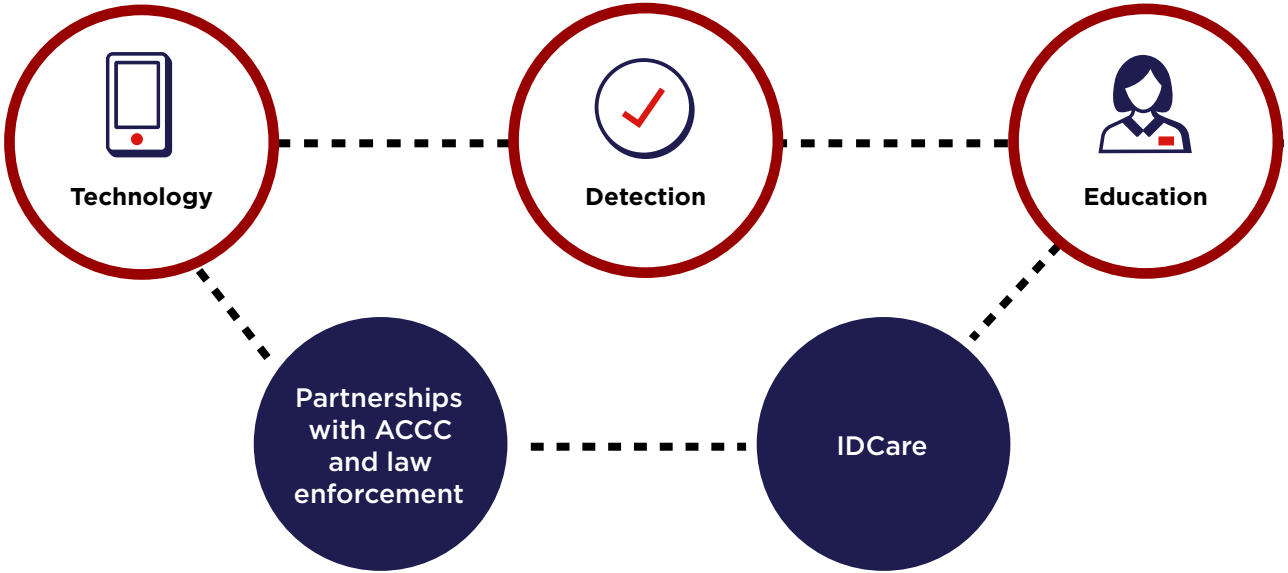
2020

Combined financial losses to scams (Statistic from the ACCC, Targeting scams report for 2020).

$851 million

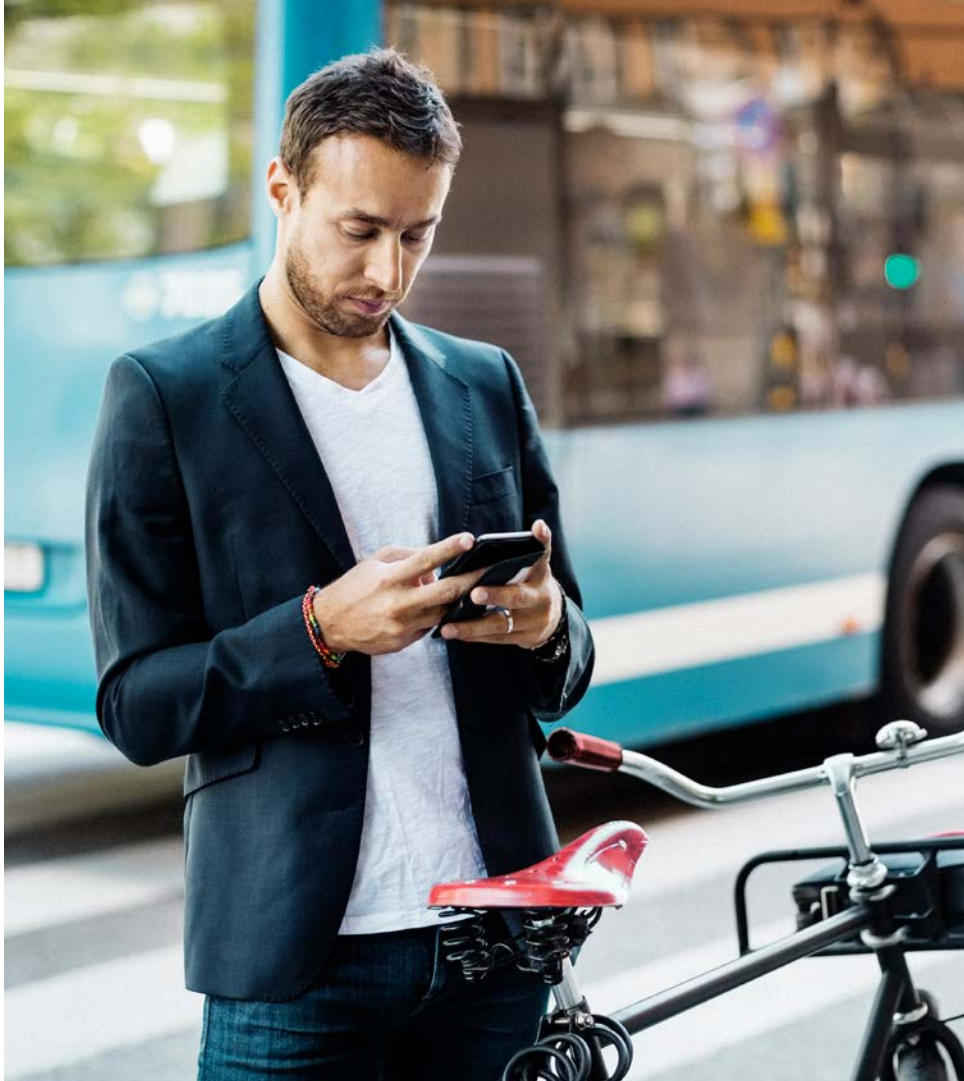
$7,677
average loss per report

PROTECTION


Technology
Detection
Education
Partnerships with ACCC and law enforcement
IDCare

AGENDA

- Types of scams and how they target you
- Scam prevention, case studies and warning signs
- Reporting and support



TYPES OF SCAMS

- Information gathering
- Threat and penalty
- Romance
- Charities
- Unexpected winning/money
- Buying/selling
- Employment
- Investment

PHONE

- Investment/unexpected money
- Information gathering
- Threat and penalty
- Charities
- Buying/selling
- Remote access

CASE STUDY

REMOTE ACCESS SCAM*

*This case study is based on a real scenario. For privacy purposes the names, personal details and images of victims have not been used.

Dani receives a call from Telstra

- The caller advised Dani that help was needed to catch a fraudster and Dani could not tell anyone.
- Dani was told to download and install software on her computer.
- The caller asked Dani to log in to online banking and confirm her account number to receive a deposit.
- Dani was asked to wait a moment and then check her balance again. She confirmed her balance had been increased by $10,000.
- The caller requested the $10,000 deposit be withdrawn in cash and returned via a wire transfer.

HOW TO SPOT THIS SCAM?

- Unsolicited call
- Advised not to tell anyone
- Instructed to download software
- Unusual payment method – money transfer agent rather than online banking

CASE STUDY

THREAT AND PENALTY SCAM*

Jane was contacted by the Australian Tax Office (ATO)

If Jane did not immediately pay her tax debt she would be arrested.

- The instruction was to purchase crypto currency.
- In fear of arrest, Jane followed the callers instructions and transfered $3,000.00.

HOW TO SPOT THIS SCAM?

- Unsolicited call
- Caller was threatening
- Urgency or time pressure
- Payment method uncommon for organisation

*This case study is based on a real scenario. For privacy purposes the names, personal details and images of victims have not been used.

CASE STUDY

CHARITY SCAM*

Sally received a phone call to donate money to support her local community impacted by fire

- The caller directed Sally to a website to make the donation.
- The site looked legitimate so she did not suspect that it was a fake website.

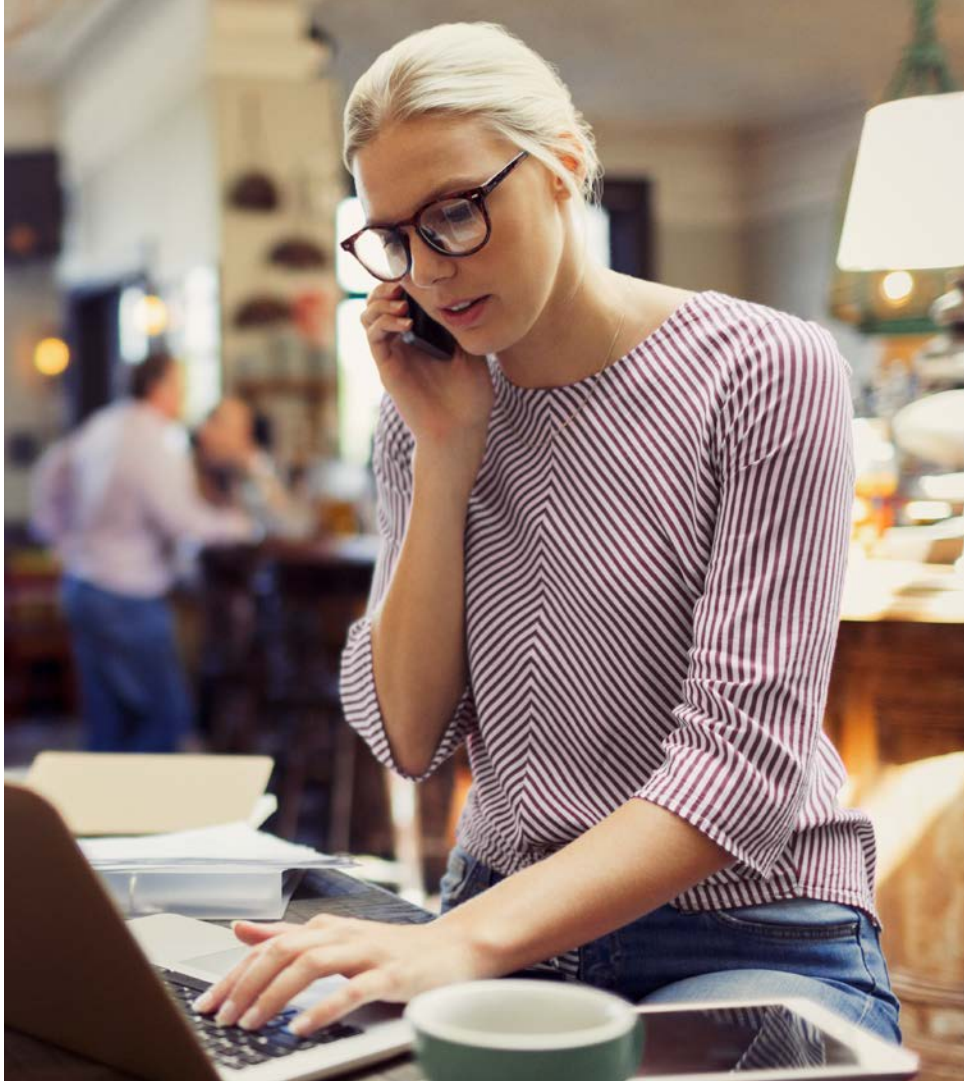
HOW TO SPOT THIS SCAM?

- Unsolicited contact
- Put under pressure or made to feel guilty through dramatic stories
- No security features on the website like https or a padlock symbol

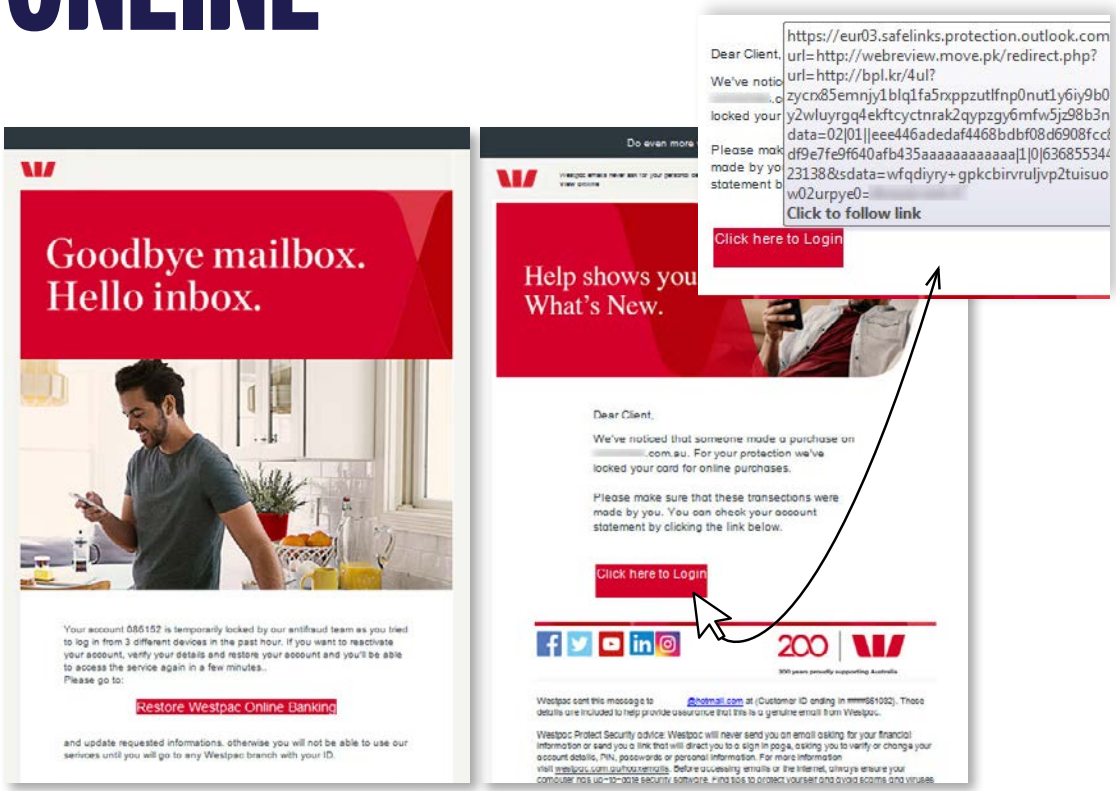
*This case study is based on a real scenario. For privacy purposes the names, personal details and images of victims have not been used.

ONLINE

- Identity theft
- Phishing
- Malicious software
- Email compromise
- False billing
- Dating/romance
- Threat/penalty
- Unexpected money
- Prize and lottery
- Employment/job advertisements



ONLINE

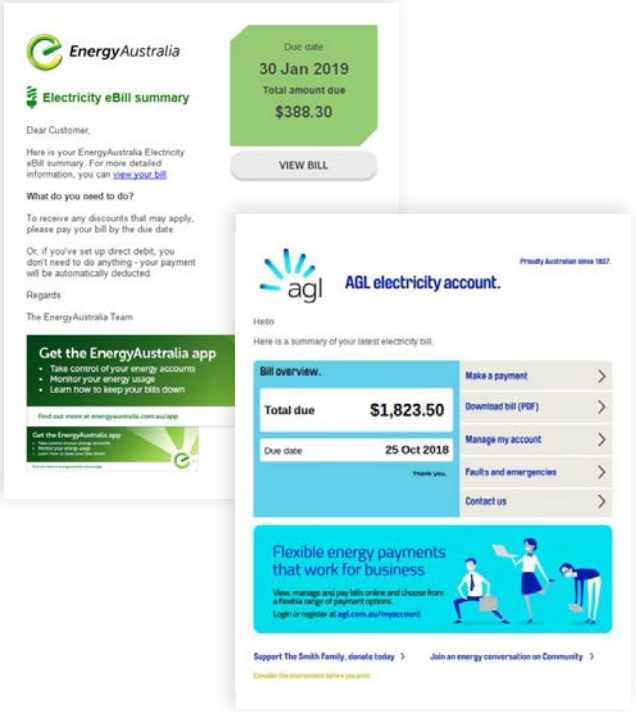


HOW TO SPOT THIS SCAM?

- No salutation or personalisation
- Sense of urgency to complete actions
- Link to sign in to Online Banking
- Threatening language
- Hover your mouse over the link to see the web address

CASE STUDY

HOAX UTILITY BILLS*



HOW TO SPOT THIS SCAM?

- Official bills contain account number
- Look for changes in payment details from previous bills or requests to click on links to pay or links to update your details/unlock accounts

*This case study is based on a real scenario. For privacy purposes the names, personal details and images of victims have not been used.

CASE STUDY

ROMANCE SCAM*

Mr Smith met Maureen online – she lives overseas

- They never met face-to-face.
- Within four months they were engaged.
- Maureen indicated she was involved in a serious accident and needed money for her medical bills.
- Mr Smith completed 10 transfers totalling $320,000.

HOW TO SPOT THIS SCAM?

- Quick to move the conversation to social media or chat app
- Confessed love very quickly
- Never met face to face and/or lives overseas
- Have elaborate stories why they're unable to meet or need money

*This case study is based on a real scenario. For privacy purposes the names, personal details and images of victims have not been used.

CASE STUDY

INVESTMENT SCAM*

Steve received an email offering an investment opportunity promising high returns

Steve initially transferred $10,000.

- Over 12 months the online investment website showed his investment increasing in value.
- Steve made further transfers totalling $200,000.
- The website went down – he could not access his account, or contact the offshore group by phone.

HOW TO SPOT THIS SCAM?

- Unsolicited contact
- Guaranteed high returns
- Pressure and intimidation (once in a life time opportunity)

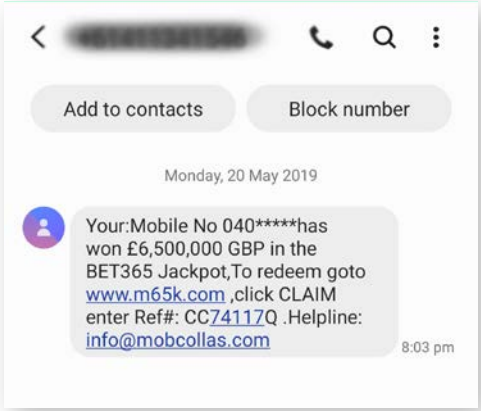
*This case study is based on a real scenario. For privacy purposes the names, personal details and images of victims have not been used.

CASE STUDY

UNEXPECTED WINNING/ MONEY SCAM

Frank was sent a text message

- Frank clicked on the link and was advised he needed to pay $250 to receive the prize money.



HOW TO SPOT THIS SCAM?

- Unsolicited contact
- Offer too good to be true
- Had not entered any competitions

*This case study is based on a real scenario. For privacy purposes the names, personal details and images of victims have not been used.

CASE STUDY

BUYING AND SELLING SCAM*

Alex advertised his car on Gumtree for $20,000

- An interstate buyer quickly responded and insisted on paying immediately.
- The buyer sent a photograph of their payment receipt and a copy of their driver licence.
- Alex shipped the car to the requested location and never received the money.
- The payment receipt and driver licence were fake.

HOW TO SPOT THIS SCAM?

- Quick response to advertisement
- The potential buyer is willing to purchase your item without having viewed it in person
- Requested car be sent with courier due to location

*This case study is based on a real scenario. For privacy purposes the names, personal details and images of victims have not been used.

CASE STUDY

EMPLOYMENT SCAM*

John was contacted by a talent acquisition specialist for an urgent job opportunity

- John was advised he would be placed in the role once he completed mandatory training.
- John was asked to email a copy of his drivers license to begin the role.
- $800 was needed upfront, which would be reimbursed in his first pay.
- Once payment was made there was no further correspondence and no training provided.

HOW TO SPOT THIS SCAM?

- Beware of offers or schemes claiming guaranteed income
- Upfront payment
- Request for personal data e.g. tax file number, copy of identification documents, bank account details

*This case study is based on a real scenario. For privacy purposes the names, personal details and images of victims have not been used.

AT YOUR DOOR

- Fake tradies
- Identity theft
- Unexpected money
- Prize and lottery
- Charity and medical
- Threat and penalty

CASE STUDY

FAKE TRADIE SCAM*

Connie answered the door to a friendly trades person advising repairs were urgently required on her property

Worried she had a huge issue with her roof, she asked if the trades person could fix the problem.

- Upfront payment was needed to secure the work.
- Connie paid upfront in cash to secure the appointment.
- The trades person did not show up.

HOW TO SPOT THIS SCAM?

- Unsolicited contact – unable to show you identification
- Unable to provide any contact information, written quotes or receipts
- Urgency, demand you accept the offer on the spot
- Requested up front deposits or full payments

*This case study is based on a real scenario. For privacy purposes the names, personal details and images of victims have not been used.

WARNING SIGNS

- You are asked to share your passwords, security number or SMS code
- Too good to be true/Win Win/can't lose/ no risk
- Unsolicited contact/pressure/intimidation
- Personal information requested
- Money/fees required
- Vague details/confusing/lack of return contact details
- You are told not to tell anyone
- Something doesn't feel right

PROTECT YOURSELF

1. Is the request genuine? Research who you are dealing with, or get a trusted second opinion.
2. Keep security software up to date on all devices. Do not open suspicious texts, pop-up windows or emails – delete.
3. Keep personal/business details secure, includes passwords and security codes.
4. Use unique passwords for all online accounts, change frequently and do not share with anyone.
5. Beware of requests for your details and/or money; this includes unusual payments/deposits.
6. Be open with the bank regarding your transactions. The bank needs all the information to protect you and your money.
7. Regularly visit your banks' security page.
8. Never give a stranger remote access to your computer.

HELP AND SUPPORT

Information:

- westpac.com.au/security
- idcare.org

Scam alert services and government awareness sites:

- cyber.gov.au
- scamwatch.gov.au

The Little Black Book of Scams Publication:

- accc.gov.au/publications/the-little-black-book-of-scams

- Your bank or credit union
- Trusted family member or friend
- Local police

REPORTING

If you have been involved in a scam or attempted scam, report it.

- **Your bank/credit union**
- **Report a scam** scamwatch.gov.au
- **Report cybercrime** cyber.gov.au

Stay safe

- Read the Tips to Protect Yourself (The Little Black Book of Scams) - page 32
- For more information visit westpac.com.au/security
- Share the message with your friends and family.