



EASTERN COMMUNITY
LEGAL CENTRE

COMMON SCAMS



CONTENTS



PAGE 2

What is a scam?



PAGE 4

Types of scams



PAGE 6

What to do if you
have been scammed



PAGE 3

Scam warning signs



PAGE 5

How to avoid scams



PAGE 7

More Information



WHAT IS A SCAM

WHAT IS A SCAM?

A SCAM IS A TRICK



TO GET YOUR
PERSONAL
DETAILS



TO GET
MONEY
FROM YOU



TO GET YOU
INVOLVED IN
CRIMINAL ACTIVITIES
(OFTEN WITHOUT YOU KNOWING)

SCAMMERS MIGHT TRY TO CONTACT YOU



ONLINE



OVER THE
PHONE



IN-PERSON



SCAM WARNING SIGNS

COMMON SCAMS:

Special offer scams

- For a job, housing or rental offers
- To sell or buy something expensive online
- Investment schemes

Scams about a problem

- Visa or Immigration problems
- Tax or other money owed
- Threats of legal action

Romance scams

- Being asked for money from a person you've met and formed a relationship with online

Personal details scams

- Bank or company wants to 'check' your details

Lump sum money scams

- Lottery or prize wins
- Unclaimed inheritance
- Early access to superannuation

IT MIGHT BE A SCAM IF:

- There is sense of urgency or a deadline.
- There is a promise of financial benefit.
- They threaten you with fines, legal action or jail.
- The phone call, email or text is unexpected.
- You are asked to pay for something in an usual way, such as gift cards or wire transfers.
- You are given a link to login.
- An email or letter is not directly addressed to you - For example, 'Dear ABL bank customer'.
- You are asked to pay for something in advance.
- You are asked for personal information - For example, your My Gov or bank details, or access to your computer.
- There is pressure to buy something or make a decision quickly.
- You are offered something that sounds too good to be true - For example, an online shopping deal, a prize for winning a competition, an inheritance or an invitation to invest in an amazing scheme.



COMMON SCAM STORIES

MARY

Mary received a text message saying ‘we have stopped your payments.,, to revive them you need to verify your details. We also noticed your myGov account details are incorrect. Please click on the link at the bottom of this message to upload personal documents’.

NICK

Nick received a call from someone claiming to be an employee of the Australian Tax Office. The caller said they had done an audit and Nick had a debt that needed to be settled urgently to avoid legal action against him. Nick was asked to buy iTunes gift cards worth \$1000 and give the serial number of the gift cards to the caller.

ANJA

Anja, an international student studying at a Melbourne university, received a phone call claiming she had incorrectly completed her passenger card upon arrival at Melbourne airport. The caller claimed that Anja had no immigration clearance from her home country and that she was on an immigration ‘black list’. Anja was told she may be deported and was ordered not to contact Australian authorities about the matter. The caller said that Anja had two options: either return to her home country or pay \$2,000 via an online portal to clear the case.

LAURA

Laura received an email from her bank that said she had overdrawn her account - Laura was sure that she had not overdrawn it. The caller then asked Laura to login and verify her information. To do that, she was asked to click the link in the email.

NAVI

Navi received an email from an organisation claiming that they could help Navi to get early access to his superannuation. He was advised to click the link in the email to provide his details.

LUCILE

Lucile is semi-retired and met John through Facebook. They call and text each other daily. From the start, John was so nice to her and said he had special feelings for her. John told Lucile he owned a successful gem business in Africa. One day Lucile received a message from John, saying the police had arrested him because someone had made a false allegation about his business. John then asked Lucile to send \$20,000 – claiming this was his only way out – to bribe the officials. He promised Lucile that he would pay her back the \$20,000 as soon as he was free.

(Source - Services Australia, Victoria, Scamwatch, Australian Tax office, Consumer Affairs Victoria, ECLC Deakin Student Legal Service)



HOW TO AVOID SCAMS

TIPS TO AVOID BEING SCAMMED:

- When someone calls you, check whether it's real - hang up and call back the official number.
- Check with the company or authority, via their official phone number - not the number given to you - if they had sent an email or letter.
- Be careful when an offer seems too good to be true - it usually is.
- Ask yourself - is it normal to get paid a lot for only a few hours work?
- Never allow a stranger to access your account.
- No company should use your personal bank account to transfer money.
- Never transfer money to a stranger via Western Union or Bitcoin or iTunes Gift cards.
- Be careful who you send your personal details to - your identity can be used to take out loans, or scam other people.
- Never follow instructions to buy a gift card or voucher such as iTunes or Google Play.
- Verify a charity's authenticity before making donations.
- Never click on a link in an email or message without checking if the website is genuine.



WHAT TO DO IF YOU HAVE BEEN SCAMMED

If you are worried you may have been scammed there are steps you can take to get help.

1. REPORT

[Scamwatch](#) - information about all types of scams and you can report scams online

[Consumer Affairs Victoria](#) - information and advice or to report a scam

[ACORN](#) (Australian Cybercrime Online Reporting Network) - Australian government cyber security Centre

[Department of Home Affairs](#) – Migration fraud and scams

[IDCARE](#) – Contact IDCARE if you think your personal or identity information has been misused. This is a free national identity support service.

[Stay Smart Online](#) Information about online scams and how you can protect yourself when online.

[Services Australia](#) – Information on Centrelink, Medicare, Child Support and myGov related scams -*Information in Multicultural languages available.*

[Victoria Police](#)

2. GET LEGAL ADVICE

[Consumer Action Law Centre](#)

[Eastern Community Legal Centre](#)

WHAT TO DO IF YOU HAVE BEEN SCAMMED



MORE INFORMATION

SCAMWATCH

<https://www.scamwatch.gov.au/>

<https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams>

CONSUMER AFFAIRS VICTORIA

<https://www.consumer.vic.gov.au/resources-and-tools/scams>

<https://www.consumer.vic.gov.au/resources-and-tools/scams/avoiding-scams>

<https://www.consumer.vic.gov.au/resources-and-tools/advice-in-a-disaster/coronavirus-covid19-and-your-rights>

ACORN (AUSTRALIAN CYBERCRIME ONLINE REPORTING NETWORK)

<https://www.cyber.gov.au/COVID-19>

STAY SMART ONLINE

<https://www.staysmartonline.gov.au/alert-service/continued-widespread-reports-covid-19-malicious-scams>

<https://www.staysmartonline.gov.au/alert-service/beware-scam-emails-threatening-reveal-personal-and-sensitive-information>

SERVICES AUSTRALIA

<https://www.servicesaustralia.gov.au/individuals/subjects/scams-and-identity-theft>

<https://www.servicesaustralia.gov.au/individuals/subjects/scams-and-identity-theft/how-know-if-its-scam>

<https://www.servicesaustralia.gov.au/individuals/subjects/scams-and-identity-theft/how-protect-against-scams>

MORE INFORMATION