

Scams Awareness

How to identify, avoid and report scams.

Acknowledgement of Country

The University of Queensland (UQ) acknowledges the Traditional Owners and their custodianship of the lands on which we meet.

We pay our respects to their Ancestors and their descendants, who continue cultural and spiritual connections to Country.

We recognise their valuable contributions to Australian and global society.

The Brisbane River pattern from A Guidance Through Time by Casey Coolwell and Kyra Mancktelow.



Types of scams

A scam is when someone deceives you into providing personal or financial information so they can steal from you. There are many ways that scammers can reach people, some of these are below:



Text or SMS scams

Scam messages look like they are from the government, businesses you deal with or even your own family or friends to try to catch you out.



Phone scams

1 in 3 reported scams happen by phone. Scammers call, claiming to be from well-known organisations.



Email scams

Scammers send 'urgent' emails pretending to be from the government, law enforcement and businesses. They use the same logo and a similar email address as the real organisation.



Social media scams

Be suspicious of anyone who contacts you out of the blue on social media – scams losses are on the rise here.



Website scams

Scammers can pretend to be anyone online to deceive you into trusting them.



In-person scams

Scammer may knock on your door or approach you in public and ask you to do something (like ask for payment for goods and services; pressure you to complete a survey; ask for donations).

Find out more: <https://www.scamwatch.gov.au/types-of-scams>

Protect yourself

Scams are successful because they:

- Look like the real thing
- Catch you off-guard when you are not expecting it
- Can take advantage of new technology, products or services to create believable stories that convince you to give money or personal details
- Rely on you NOT spotting the warning signs
- Might make you feel rushed or hurried
- Look like a great deal you won't want to miss
- Appear to be from someone you trust or an organisation you know or belong to



What is a scam?

Scams are economic crimes run by criminals who are often very organised and sophisticated.

A scam is:

- When someone deceives you into providing personal or financial information so they can steal from you
- Scams can involve accessing personal information, buying or selling, dating and romance, fake charities, jobs and investments, threats and extortion, unexpected money or unexpected winnings.



A scam is NOT:

- Someone hacking your computer, device or account to steal from you
- Buying something that turns out to be poor quality
- Paying more than something is worth



Common signs of a scam

- **It's an amazing opportunity to make or save money**
 - *Scammers trick you into believing you're getting an incredible deal or offer.*
- **Someone you haven't met needs your help – and money**
 - *Scammers try and use your good nature against you by telling heartbreaking or tragic stories to convince you to help them and give money.*
- **The message contains links or attachments**
 - *Scammers try to catch you off guard and send you to scam websites designed to steal your information and money.*
- **You feel pressured to act quickly**
 - *Scammers don't want you to take your time to think things through, by saying if you don't do something you'll miss out or threatening that someone bad will happen.*
- **They ask you to pay in an unusual or specific ways**
 - *Scammers might ask you to pay with pre-loaded debit cards, iTunes cards or virtual currency like Bitcoin.*
- **They ask you to setup new accounts or PayIDs**
 - *Scammers can ask you to setup a new bank account or PayID in order to pay them or be paid by them.*

Steps to protect yourself

Steps you can take to protect yourself

1

STOP – Don't give money or personal information to anyone if unsure

Scammers will offer to help you or ask you to verify who you are. They will pretend to be from organisations you know and trust like, Services Australia, police, a bank, government or a fraud service.

2

THINK – Ask yourself could the message or call be fake?

Never click a link in a message. Only contact businesses or government using contact information from their official website or through their secure apps. If you're not sure say no, hang up or delete.

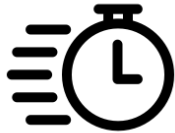
3

PROTECT – Act quickly if something feels wrong.

Contact your bank if you notice some unusual activity or if a scammer gets your money or information. Seek help from IDCARE and report to ReportCyber and Scamwatch.

<https://www.scamwatch.gov.au/protect-yourself/ways-to-spot-and-avoid-scams>

What to do if you have been scammed



Act Fast

Contact your bank or card provider immediately to report the scam. Ask them to stop transactions



Get help to recover

<https://www.idcare.org/>
IDCARE is Australia and New Zealand's national identity and cyber support service.



Warn others & report

After securing your details, warn others and report the scam
<https://www.scamwatch.gov.au/report-a-scam>



Watch out for follow-up scams

Successful scammers will try to get more money. One in three victims of a scam have been scammed more than once.



Get support

Getting scammed can happen to anyone and is a horrible experience. Reach out to family and friends or support organisations.



UQ Crisis Support

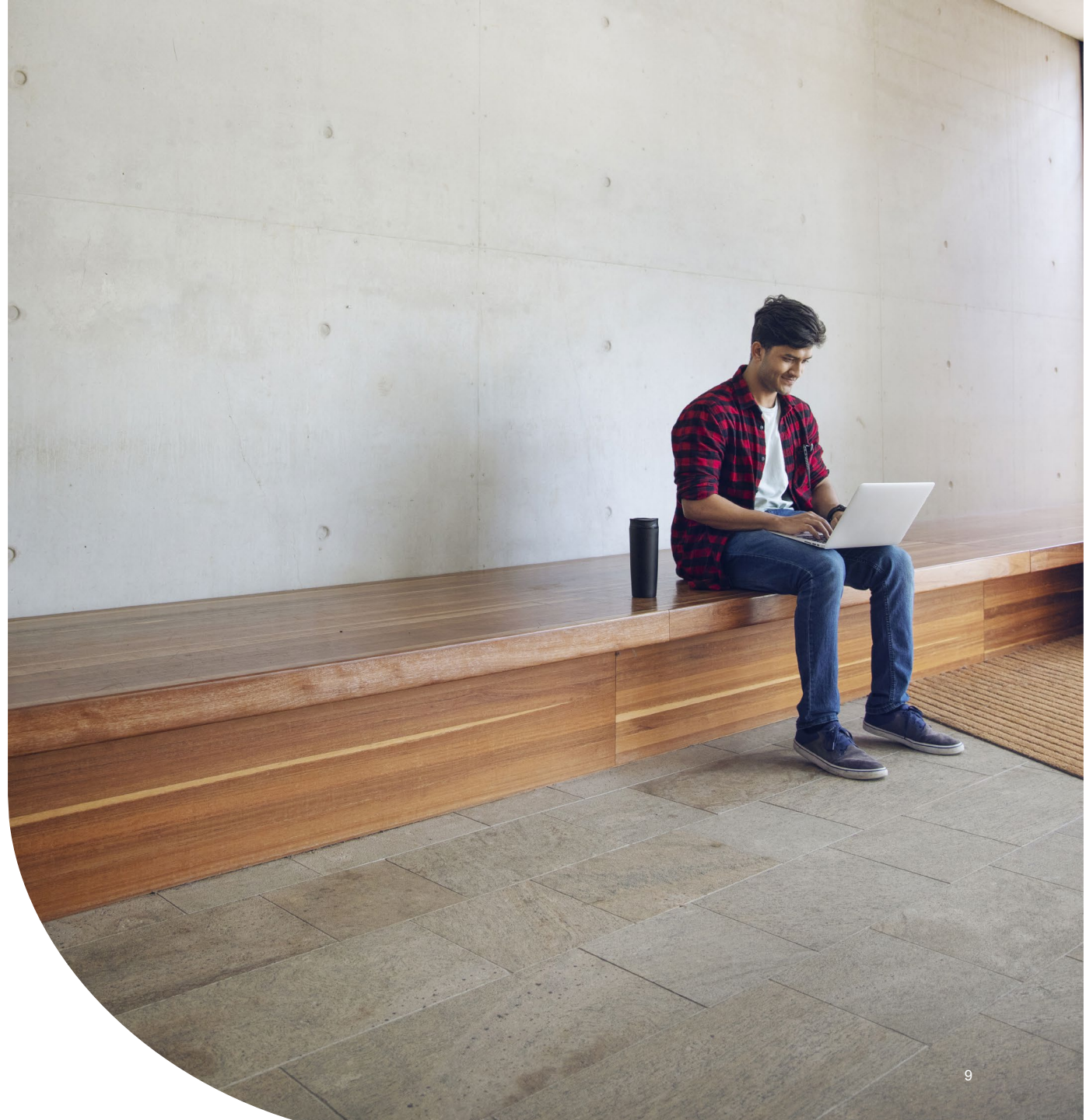
<https://my.uq.edu.au/information-and-services/student-support/health-and-wellbeing/crisis-support>

<https://www.scamwatch.gov.au/protect-yourself/what-to-do-if-youve-been-scammed>

Report a scam

Australian authorities rely on people who have been scammed or experienced an attempted scam to report it. This helps catch scammers and protect others.

<https://www.scamwatch.gov.au/report-a-scam>



Research and resources

Scam statistics

Interactive data from scam reports including amount lost, scam types, types of scam and delivery methods.



The Little Black Book of Scams

The Little Black Book of Scams is recognised internationally as an important tool for consumers and small businesses to learn about scams



Targeting scams report

The ACCC produces an annual Targeting scams report, explaining key trends in scam activity and highlighting the impact of scams on the community.



Resources

We produce a range of videos, factsheets, reports and guidelines designed to assist consumers, small businesses and industry in understanding and preventing harm from scams.



In your language

Scams target people of all backgrounds, ages and income levels across Australia. Find out how to protect yourself from scams in your language.



Scams awareness network

The scams awareness network is a group of government regulatory agencies and departments in Australia and New Zealand. We work with partners to raise awareness about scams and disrupt them.



Scamwatch is an Australian Government organisation run by the National Anti-Scam Centre which collect reports about scams to help warn others and take action to stop scams.

Scam reports help the National Anti-Scam Centre make Australia a harder target for scammers and protect people from becoming victims in the future.

<https://www.scamwatch.gov.au/research-and-resources>

UQ provides information and support to protect yourself from cyber security risks:

<https://my.uq.edu.au/information-and-services/information-technology/cyber-security-uq/protect-yourself>

Contact

Student Services

<https://my.uq.edu.au/contact/student-central>

Student.services@uq.edu.au
1300 275 870