

# Money Scams: How to Stay Safe & Recover

**This factsheet is about common scams targeting international students, how to stay safe and what to do.**

## Scams Targeting International Students

International students in NSW are increasingly being targeted by financial scams.

These include:

- phishing (fake emails or messages designed to steal your details)
- identity theft (using your personal information without permission)
- social media marketplace scams
- fake online stores
- rental accommodation scams

Rental scams are especially common.

Scammers may:

- ask for money before you've seen a property
- pretend to be a landlord or real estate agent
- send fake rental agreements or receipts

Students have lost thousands of dollars through these scams, often because they felt pressured to act quickly.

## Tips: Spotting a scam

Before you click, reply, or pay anything, take a moment to check the message carefully.

- **Check who sent it**  
Tap on the email or phone number.

Does it look official, or slightly unusual?

Scammers often use addresses that look similar to real ones.

- **Preview links without opening them**  
Long-press or right click links to see where they lead.

If the website looks strange or unrelated, don't click.

- **Look at the email ending**  
Real government emails end in *.gov.au* and universities in *.edu.au*.

Anything different should raise suspicion.

- **Watch for mistakes**  
Spelling errors, odd wording are an indication of a scam.

- **Watch for urgent demands**  
For example, "Pay Now!" or "Act Immediately!"

These are common scam tactics to make you panic and act quickly without thinking.

- **Remember: scams can look real**  
Messages may appear to come from your bank, university, tax office, or delivery companies.

# Money Scams: How to Stay Safe & Recover

## Tips: Do Your Own Checks

Do not rely on the contact details in the message. Always verify independently.

Do this by:

- **Use official contact details**  
Look up the organisation yourself (e.g. Google, your bank card, official website) and contact them directly.
- **Ask them to confirm the message**  
For example: "Can you see this message on my account?"
- **For NSW Government messages**, verify through Service NSW or the relevant agency website.
- **Check trusted sources**  
Search for similar scams on Scamwatch or official government websites.
- **Don't click links - search instead**  
If a message says it's from your bank or a government agency, go to their website yourself rather than using the link provided.
- **Ask someone you trust**  
If you're unsure, show the message to a friend, your university, or a legal service before acting.

## Tips: Ask Yourself

A quick "sense check" can help you spot a scam:

- Is the message urgent or threatening?
- Does the tone sound strange, robotic, or overly formal?
- Is it asking for money or personal information?

If the answer is yes to any of these, stop and double-check.

## Tips: Slow Down

Scammers rely on pressure and urgency.

Taking your time is one of the best ways to stay safe.

Make sure you:

- **Pause before paying**  
Always verify who you're dealing with first.
- **Check businesses and properties**  
Confirm ABNs, inspect rental properties in person where possible, and research sellers or landlords.
- **Avoid risky payment methods**  
Never pay deposits using wire transfer, cryptocurrency, or gift cards - these are almost impossible to recover.
- **Trust your instincts**  
If something feels off, it probably is. Stop and get advice.

## Bank Scams

If you think you've been scammed or lost money:

### Step 1: Contact your bank immediately

Ask them to:

- freeze the transaction
- try to reverse the payment
- give you a reference number
- Send written confirmation

### Step 2: Stop all contact with the scammer

Do not reply to any emails, messages or calls from the scammer.

### Step 3: Report the scam

You can report the scam to:

# Money Scams: How to Stay Safe & Recover

- ReportCyber - for online fraud and cybercrime
- Scamwatch (ACCC) - helps track scam activity and trends

## Step 4: Secure your accounts

- Change your passwords
- Activate multi-factor authentication
- Check if any accounts were accessed without permission

Step 5: Contact IDCARE (free support)

IDCARE provides free help with identity theft and recovery plans.

## Step 6: Keep records

Write down:

- Dates and times you contacted your bank
- Case numbers
- Names of staff you spoke to
- Screenshots of messages and emails

This can help if you need to dispute anything with the bank later.

## Scam Payments to Overseas Accounts

Many scams involve sending money overseas, especially for rental properties.

Important to know:

- It is often very hard to recover money sent overseas.
- Acting quickly gives you the best chance of stopping or reversing the payment.

## What you should do:

- Contact your bank immediately
- Ask for all possible recovery options

- Collect evidence (screenshots, receipts, emails)
- Report the scam (ReportCyber, Scamwatch, NSW Police)
- Contact IDCARE if your personal information was shared

## Legal recovery

Taking legal action against overseas scammers is usually very difficult, expensive, and rarely successful.

## Debt Collector Scams

If someone contacts you about a debt, you have rights—even as an international student.

### You can ask for:

- the creditor's full name
- a copy of the contract
- an itemised statement
- how the debt was calculated

They must provide this before demanding payment.

### You can dispute the debt if:

- it resulted from a scam
- it is not yours
- the amount is wrong

### If the debt is from a scam:

Tell the collector:

- the debt is disputed due to fraud
- you have reported the scam
- you are seeking legal advice

They must pause collection while the dispute is being investigated.

*This fact sheet is for information only and is not legal advice*