Scams

Scammers use many tricks to convince you to part with your money. Remember, if the offer sounds too good to be true, it probably is.

How to spot a scam

Unexpected contact

Scammers will contact you out of the blue or may pretend they accidentally got the wrong person. They may pretend to be someone you know or a company you're familiar with, such as your internet provider. Online contact is very common, using social media platforms, social messaging apps or email. But they may also phone or text you.

Promise you something

Scammers make promises of money saying you've won it or will make unusually high investment returns. They may offer an item for sale, a charity receipt, a high-paying job, even a promise of love and romance. They may also promise to 'fix' a computer problem, even if there's nothing wrong.

Ask you to do something

Scammers want your money or your personal details. For you to get what they promise, they may ask you to give them money to:

- invest
- buy something
- help them personally
- donate
- release funds that belong to you

For access to your personal details, a scammer may ask you to:

- fill out a form online
- give them access to your computer
- confirm your bank details
- confirm your passwords or PIN
- click on a link in an email (that downloads malware)

They can even threaten you if you don't do something for them.

Tip: Get Support

If you're the victim of a scam and you need support, contact Lifeline on **13 11 14**. For free and confidential help with money issues, contact the National Debt Helpline on **1800 007 007**.

Reduce the risk of scams

Protect yourself

- Do your own checks on any opportunity to get or make money, to make sure it's real.
- Make sure your PIN and passwords are secure and complex. Remember, a bank would NEVER ask you to confirm your PIN.
- Make sure your privacy settings are up to date on your social media accounts.

Be cautious

- Be wary of unexpected contact, particularly if you have replied to something on a website or social media platform.
- Don't click on any links in suspicious emails or text messages. Look for spelling mistakes and unrealistic promises.
- Don't trust any offer to invest or make money if approached through social media. You don't know who you are dealing with.
- Get independent financial advice before you invest your money.

Do your own checks

- Check your bank and credit card statements every month to make sure every transaction was made by you.
- Shred all documents with your personal information on them.
- Choose passwords that are hard to work out and don't give your password to anyone.
- Before you give callers any information, double check they are really from that company. Phone them back using a number listed for that company in the phone directory.
- Remember that a real company will never ask you to disclose your PIN.

If you think you've been scammed

- Stop sending money to the individual or business.
- Report it to your bank or financial institution.
- Be wary of falling for a follow-up scam or offers to recover your money.
- Report financial scams to ASIC (search 'complain to ASIC') or your local police.