

# Safe & Savvy

Keep yourself safe: be aware of scams and fraud.

This guide provides practical steps to safeguard yourself and your loved ones against scams and fraud. We want you to stay safe and savvy when managing your finances.

Even the most savvy and successful people can become victims of scams and fraud.

## What is the difference between a scam and fraud?



A **scam** is when someone gains your confidence in order to steal your money or information. Scammers often use sophisticated lies to trick you.



**Fraud** usually happens when someone accesses your funds without your knowledge or authority. You may not be aware of the fraud until you see it on your statement or receive a call from your bank.

## Why are fraudsters and scammers so effective?

- **They play on emotions** such as fear, loneliness, desire and compassion to trick you into making decisions that you wouldn't otherwise make.
- **They identify and prey on vulnerabilities** such as isolation, age, financial hardship, language barriers and low computer skills to take advantage of your situation.
- **They are experts** at manipulating your trust and imitating honest people or organisations.
- **They may threaten you** with a fine, disconnection of your services, arrest or even deportation.

**\$3.1bn** lost to scams in 2022<sup>1</sup>

**30%** of victims do not report scams<sup>1</sup>

People aged **65+** lost more money than any other age group<sup>1</sup>

## Top tips to protect yourself:

### Avoiding Scams

- Hang up on suspicious phone calls from people you don't know asking for personal information, even if they say they are from a big/well-known company.
- Never share passwords, personal information, PINs or SMS codes. Anyone who asks for your password is probably scamming you.
- If you are sharing a computer, don't save your passwords and always log out.
- Be wary when reviewing email attachments, links and suspicious texts. If in doubt, delete the message.
- If you think you have been scammed, report it to your bank immediately.
- If in doubt, talk to a friend or family member, or contact the organisation directly and ask.

### Avoiding Fraud

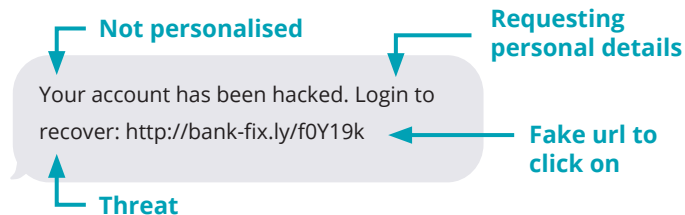
- If you shop online, always use secure websites. Make sure the web address (URL) starts with "https" or has a padlock symbol at the front before entering your details.
- Avoid swiping your card, inserting or tapping your card is often more secure. Opt to use a PIN rather than signing for purchases.
- Always keep your personal and account information safe and don't keep a record or tell anyone your PINs or passwords. Contact your bank if you have forgotten your password.
- Regularly check your bank account and statements for suspicious transactions.
- Tell your bank if you are travelling overseas.

## Warning Signs to look out for:

### Protect yourself:

Keep on the lookout for these warning signs and act straight away to protect yourself:

- **Incredible offers to make easy money**  
If it sounds too good to be true, it almost certainly is!
- **Unknown, unsolicited contact**  
Be wary of unexpected phone calls, texts, emails, requests for logins or remote access to your computer. It may look legitimate at a glance, but check the url or email address.



- **Feeling bullied or rushed**  
Be sceptical of anyone claiming to be from a big and legitimate organisation (bank, ATO, phone/utilities companies etc) who try to rush you into anything. Particularly if you're asked for an up-front deposit or immediate payment.
- **Unknown transactions**  
Keep an eye out for unusual and unknown transactions, whether small or large, particularly for \$1 or \$2 (these small amounts are used to test if your account is active before taking out larger sums of money).
- **Romantic money requests**  
Scammers can create fake profiles to gain trust and ask for money or gifts. Internet search the person's name and photos to see if they have been reported on any scam sites.

### Protect your family:

If your older loved ones start to show signs of decline or diminished capacity, look out for these red flags::

- Making significant withdrawals, unusual purchases, or other uncharacteristic activity.
- Making sudden changes to their will or power of attorney.
- Carrying or withdrawing large amounts of cash.
- Being scared that they will be evicted if they don't hand over money.
- Not receiving products, services or care that you know they've paid for.
- Failing to buy groceries or pay utility bills.

If you see any of these signs, get advice from one of the expert services listed. Remember, it is important to treat relatives with respect and dignity; they have the right to choose or refuse your help, even if you disagree.

## Have you been a victim of a scam or fraud?



**Contact your bank immediately** as they may be able to stop the money transfer or close an account if you believe the scammer has your details.



**Change your passwords and PINs** straight away if you suspect your security has been compromised. We recommend changing your passwords and PINs regularly as a preventative measure.



**Report the scam** to a government agency such as [scamwatch.gov.au](http://scamwatch.gov.au) to help them identify the scammer and prevent the scam from spreading. For fraud, you can contact the police on 131 444.

If you have accidentally clicked a link, downloaded any attachments, or shared your details in response to a hoax phone call, email or text, contact your bank right away; even if you're not sure.

## Stay up to date

### Scamwatch

[www.scamwatch.gov.au](http://www.scamwatch.gov.au)

Provides information to consumers and small businesses about how to recognise, avoid and report scams. Provides ways to report scams and obtain support if you have experienced a scam.

### ASIC MoneySmart

[www.moneysmart.gov.au](http://www.moneysmart.gov.au)

Provides financial management resources, tools and information.

### National Debt Helpline

[www.ndh.org.au](http://www.ndh.org.au) 1800 007 007

Offers free and confidential services from professional financial counsellors to help you tackle your debt problems.

### Australian Financial Complaints Authority (AFCA)

[www.afca.org.au](http://www.afca.org.au) 1800 242 636

Provides accessible, fair, and independent dispute resolution for consumers and financial service providers.

### IDCARE

[www.idcare.org](http://www.idcare.org) 1300 432 273

Provides free, Government-funded support to victims of identity crime. Can help develop a response plan for repairing damage to your reputation, credit history, and identity, when your personal information has been taken.

### QBANK

[www.qbank.com.au](http://www.qbank.com.au) 13 77 28

Contact us immediately if you think you have been scammed or notice missing money from your account.