Scams

This fact sheet is for information only. You should get professional advice about your personal situation.

Main ideas

• Scams aim to trick you into giving money or information.

• If something looks/sounds too good to be true, it probably is.

• Never click on a link in an unsolicited text, email or social media post.

• Immediately contact your bank if you have been scammed or your account has been compromised.

• Get help if you've been scammed.

In this fact sheet:

Be on the lookout for scams

Scams are attempts to steal money and personal data by tricking you. Scams can be very sophisticated and can seem genuine. There are many scams operating and new ones are developed every day. You must be very careful, especially when answering the phone and responding to texts, email and social media.

The Australian Government's Scamwatch website gives information about the latest scams.

Examples of scams include:

- Email, phone or SMS messages that try to trick you into giving out personal details, passwords, or remote access to your computer. Scammers can fake their return number and make scam messages show up in the same SMS chain as genuine SMS messages from your bank.
- Romance scams – these can stretch out for many months before you are asked for money.
- Fake companies or products – especially cryptocurrencies.
- Fake companies pretending to help people who have been scammed to get money back.
- Unexpected money or winnings – trying to trick you into giving information or money so you can get a big prize.

Scams often include time pressure. Scammers make the situation sound urgent to try to force you to act without taking the time to consider properly.

Protecting yourself from scams

If something looks or sounds too good to be true, it probably is. Don't be tricked by a promised short-cut to riches.

Be very wary of anybody you do not know contacting you. If they claim to be from a reputable organisation, contact the organisation directly on their published website or phone number. Do not click on links in emails, SMS, or social media. Never give phone security or verification codes out to anyone, even your bank (your bank will never need it).

Other information about protecting yourself from scams is available at Scamwatch and through the Australian Competition and Consumer Commission (ACCC) website.

What to do if you have been scammed

If you have been scammed or if you think the security of your account has been compromised, tell your banks and finance companies immediately. Use their priority line for reporting security breaches (all banks must have a priority number that is convenient for you to use).
The sooner you tell them, the sooner they can change passwords and secure accounts to stop you losing money.

If your identity was stolen:

1. Talk to IDCare (1800 595 160), Australia's national identity and cyber support service. They can connect you with a specialist identity and cyber security counsellor.

2. Contact Service NSW if you need to replace NSW government documents. If you are outside NSW, contact the government department that issues driver licences in your states.
3. Look at your credit report to see if there is anything you do not recognise. You can ask for a free credit report every 3 months. Some credit reporting agencies offer a paid service that alerts you if something happens. Read our fact sheet about Credit Reports.
4. Consider putting a temporary credit ban on your credit report. IDCare have details about how to put a credit ban on your report.
5. If you discover you have debts that you did not apply for, tell the lender straight away that your identity was stolen and ask for copies of the loan application and loan documents. Most banks will ask for evidence that your identity was stolen (such as a police report). Banks may remove the debt if they are convinced you did not apply for the loan or receive the money from the loan.

   Get legal advice if you have any problems.

Ask your bank to refund money lost

Whether your bank or financial institution is liable (responsible) for the money you have lost depends on how aware they were of the scam, and what role they played in the transaction.

Banks/finance companies aren't responsible for picking up or blocking every scam or fraudulent transaction, but they have some obligations including:

- Responsibilities around chargebacks, unauthorised transactions and mistaken payments – read our fact sheet about Reversing Bank Transactions.
- The bank or financial institution has responsibilities set out in the terms and conditions of your account. Check they have met those responsibilities.
- Banks are members of the Code of Banking Practice and have general obligations about acting fairly and reasonably.
- Banks and financial institutions may also have obligations under common law, contract or various consumer protection legislation.

Unfortunately, there are only limited situations where a bank would be liable for money lost due to a scam. Some examples include:

- If the bank or financial institution had prior warning that an account was fraudulent (for example, previous complaints or ASIC notifications) and failed to close the account before your transaction happened.
- If a clearly suspicious transaction happened in a branch, you may be able to argue the bank should take some responsibility for the loss.
- If you called the bank's priority number to tell them about a security breach, but were left on hold for 50 minutes, you can argue the bank should be liable for transactions that happened while you were on hold (you should still stay on hold and report the

breach as soon as possible).
- If the bank didn't block your card, or allowed more transactions, after you reported that the account was compromised.

Get legal advice about your situation if you think your bank played a role or acted unfairly. If you are in NSW, you can ring our Credit & Debt Legal Advice line on 1800 844 949.

Consider legal action

You could talk to a private solicitor immediately about whether there are options available to recover your money.

Be realistic about your chances of getting any money back – don't throw good money after bad.

Get financial support

If you are in financial hardship, you can ring the National Debt Helpline 1800 007 007 to speak to a free financial counsellor.

The Ask Izzy website has a directory of community assistance available across Australia – from food or accommodation assistance to energy vouchers.

Protect your emotional/mental wellbeing

Being scammed can be devastating emotionally as well as financially. Being tricked by a sneaky scammer can make you feel silly and incompetent – but it is the scammer who has done wrong, not you. It is important you look after yourself and get support if you are struggling.

Consider talking with:

- Lifeline crisis support service. Ph. 13 11 14, available 24/7.
- For First Nations people, 13 YARN (13 92 76) is available 24/7. You'll be connected with an Aboriginal or Torres Strait Islander crisis supporter.
- Your local doctor (GP).

Need more help?

For a list of other resources, visit our Useful Links page.

Last updated: January 2023