

Bulletproofing against scams & frauds

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

In this pack you will:

- Learn about the types of fraud and scams to look out for
- Discover how to better protect yourself from frauds and scams
- Learn from real-life case studies what can go wrong.

What is the difference between a scam and a fraud?

- A scam happens when somebody gains your confidence in order to steal your money or information. Scammers often use sophisticated lies to trick you.
- Account fraud usually happens when somebody accesses your funds without your knowledge or authority. You might not even be aware of the fraud until you notice it on your statement or receive a call from your bank.

For more information, please visit
[Commbank.com.au/scams](https://www.commbank.com.au/scams)



Many victims, huge losses



\$2b

Is how much Australians lost in 2021 to scams as reported to Scamwatch, ReportCyber, 12 financial institutions and government agencies.ⁱ

Across the CBA group, job and investment scams, remote access scams, and romance scams were ranked as the top three scams in terms of customer losses.



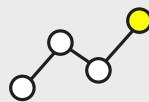
\$100m

Was recovered or prevented in scams targeted at our customers, including \$32 million that was directly targeted at those over 70.ⁱⁱ



29%

of Australians report fending off a scam attempt every day.ⁱⁱⁱ



92%

Of Australian adults have been exposed to a scam or fraud.^{iv}



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.

i ACCC report on scams activity 2021

ii CommBank study

iii Scams & Cybercrime: ABA Webinar - Australian Banking Association

iv Australian Banking Association (<https://www.ausbanking.org.au/insight/scammers-a-dirty-industry/>)

Common scams & frauds

Watch out for these common scams and frauds.

Scams

- **IT Support** – The scammer contacts you by phone or email pretending to be technical support staff from a telecommunications or computer company. They sometimes request remote access to your computer and often try to convince you to transfer money or to buy a prepaid gift card to fix a fake technical issue.
- **Romance & dating scams** – The scammer forms a relationship with you to extract money or gifts. They may convince you to transfer assets into their name or ask to become a beneficiary of your will. Often they will ask you for money to fix a non-existent health, travel or family problem.
- **Investment scams** – The scammer claims to be a stockbroker or portfolio manager offering you financial or investment advice. They will try to convince you to hand over money for an investment opportunity.
- **Job opportunities** – The scammer offers you a quick and guaranteed way of making money with little effort. So-called 'pyramid' schemes often masquerade as multi-level marketing businesses by using payments from new recruits as "profit" for earlier investors.
- **Unexpected money** – The scammer offers you the false promise of an inheritance or a share in a large sum of money in return for paying them a smaller up-front fee.
- **Travel scams** – The scammer tricks you into claiming a free or discounted fictional holiday. To secure your 'booking', you may be asked to give the scammer personal information and credit card numbers.
- **Fake charities** – The scammer takes advantage of your generosity and compassion by posing as a charity, or claiming to need money to help a child who is ill.

- **Buying or selling products** – The scammer tricks you into paying for fake invoices, shopping at fake websites, or purchasing products at discount prices – products that you don't receive or don't work as described.

Account frauds

- **'Phishing'** – The fraudster tricks you into giving them usernames, passwords or credit card details by posing as someone you can trust such as a suspicious phone call or link to a fake website.
- **Malware** – The fraudster sends you an email or text that looks legitimate but when you click on the link it installs software on your computer, phone or tablet that gives the criminal online access to your bank accounts.
- **Skimming** – The fraudster installs a device on an ATM or EFTPOS machine that reads and stores information from your card, which is then used to withdraw money or make purchases.
- **Card fraud** – The fraudster uses your credit card details without your authorisation, either through card skimming or by convincing you to give out the information under false pretences.
- **Missed call** – The fraudster calls you but then hangs up quickly, prompting you to call them back on a premium number with high call charges.
- **Identity fraud** – The fraudster uses your identity or personal information to commit a crime. This can involve the theft of your identify or the production of false identities and financial documents.
- **Cheque fraud** – The fraudster attempts to use fake, forged or altered cheques to pay for goods and services.



Top tips

Scams

- ✓ Hang up on suspicious phone calls, even if they say they are from big companies. Call back using a number from a trusted source, such as the phone book or the company's website.
- ✓ Never share passwords and personal information. Anyone who asks you for your password is probably scamming you.
- ✓ Be a sceptic when reviewing email attachments, links and suspicious texts. If you're in doubt, delete the message.
- ✓ Use up-to-date anti-virus software to protect your computer. You can find more information at [scamwatch.gov.au](https://www.scamwatch.gov.au).
- ✓ Don't send money or personal information to people from unusual locations.

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.
- ✓ Avoid swiping your card when making purchases. Inserting or tapping your card is often more secure, or opt to use a PIN over signing for purchases.
- ✓ Always keep your personal and account information safe and don't keep a record or tell anybody your PINs or passwords. Contact your bank if you have forgotten your password.
- ✓ Check your bank account and statement regularly, keep an eye out for any unfamiliar transactions.
- ✓ Tell your bank if you are travelling.

Warning signs

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 contact

Be wary of unexpected phone calls, emails or requests for remote access to your computer.



Feeling bullied or rushed

Be sceptical of anyone claiming to be from a big and legitimate organisation (bank, telephone company, utilities company, government) who tries to rush you into anything.



Unknown transactions

Keep an eye out for unusual and unknown transactions, whether small or large, particularly for \$1 (these small amounts are used to test if your account is active before taking out larger sums of money).



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. Change your passwords and PINs regularly as a preventative measure.
- ✔ **Report the scam** to a government agency (such as 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.
- ✔ **Contact IDCARE** on 1800 595 160 or via idcare.org. IDCARE is a free, Government-funded service that provides support to victims of identity crime to help them plan a response when they have had their personal information taken.
- ✔ **Apply for a Commonwealth victims' certificate** if you're a victim of identity crime. The certificate can be used to help you regain your identity credentials with different government and financial institutions.

Eddie's story

A romance scam

Eddie, a successful 52-year-old business executive, was devastated when his wife of 26 years passed away. After a year of terrible loneliness, Eddie struck up a friendship with Kali, a beautiful 40-year-old woman of African descent, on an internet dating site. Eddie says he was drawn to Kali's exotic background, and he felt flattered by her attention and care.



“She implored Eddie to lend her more money for just a short period of time.”

Kali confided in Eddie that she had recently moved from Australia to the United States because her father had died suddenly, and her frail mother needed support. She had become very distressed about her mother's declining health and the rising medical costs. As Kali was unable to work while caring for her mother, Eddie offered to give her \$933 to help pay for some tests.

A devastated Kali then told Eddie that her mother had cancer and needed a \$54,000 operation immediately. Money was tight because her parents' joint account was frozen while her father's estate was in probate, so she asked if Eddie could help out for a short time. Kali reminded Eddie that she desired to meet him. Eddie took out a personal loan to help Kali and her mother.

Then came more bad news. Not all the cancer had been removed and Kali's mother would need further treatment. A teary Kali declared that she couldn't bear to lose another parent, and still didn't have the money from her father's estate. She implored Eddie to lend

her more money for just a short period of time. She detailed the amounts to Eddie for chemotherapy and radiation therapy and other related support services, all of which had to be paid up-front. Eddie was stunned at the costs – a total of \$492,000. How lucky were Australians to have a public health care system? He wasn't comfortable about it, but Kali had told him that her father's accident included a \$1 million insurance pay out. Eddie arranged to take out a second, temporary mortgage on his house for the full amount that Kali needed to borrow.

After this last transfer was made, Eddie waited patiently for Kali's call. He knew she would be at her mother's hospital bed. When he called her a week later, he was shocked to find the number was disconnected. In a horrifying moment, it finally dawned on him that he had been scammed. Shocked and embarrassed, he approached the bank to see if anything could be done. He had given away a total of \$546,933.

The bank immediately froze Eddie's account and blacklisted the recipients. Unfortunately, the bank was unable to recover the funds because too much time had passed.

Eddie's story is based on a real-life Commonwealth Bank case study.



Susy's story

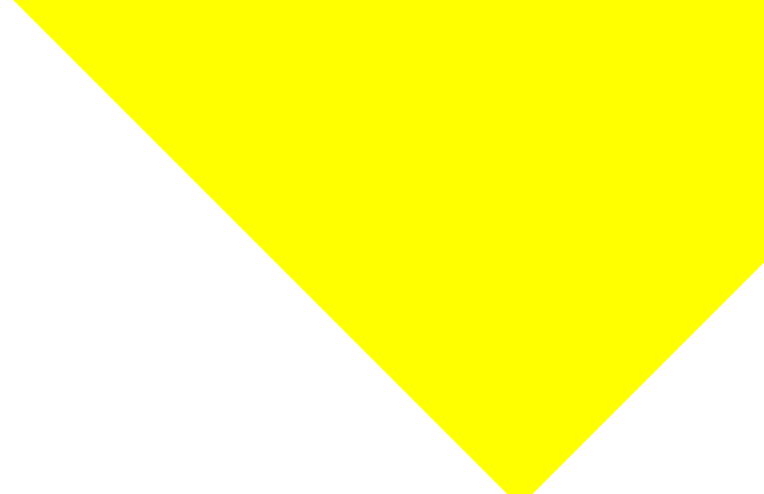
A remote access scam

62-year-old Susy received an urgent call from Tim, who said he was from the security department of her telephone company. Tim had detected a hacker who was sending her random advertising emails with malware (a malicious computer program) that could be used to access all of Susy's personal details.

Susy was understandably scared about theft of her personal details – as well as the chance that the hacker could access a large inheritance in one of her accounts. Tim

explained that if they acted quickly they could find and remove the malware to prevent, or at least minimise, any theft. Susy agreed to receive Tim's help, and so downloaded and installed a computer program that gave Tim access to her computer.

Unknown to Susy, transfers were made ranging from \$2,000 and up to \$20,000



Soon after Tim began his check, he told Susy he had detected a sophisticated malware program that had accessed all her bank accounts. He removed the malware, but advised Susy to purchase anti-malware software for future protection. At \$9,700, this seemed quite expensive to Susy, but she knew she had more to lose if she didn't act quickly.

A week later, Tim called Susy to check that the anti-malware software was working well. As new malware was being developed constantly, Tim recommended insurance to protect her from any future hacking of her accounts. Generously, he suggested she could use his 'family and friends' discount; for only \$8,000, Susy would have 10 years of protection through an offshore insurance company. Given her earlier experience, Susy thought this was a good idea.

Tim then told Susy that he had become a shareholder in this insurance company about a year ago. In the last six months, he boasted, he had received dividends equal to five times his original investment. He explained that the greater the investment, the bigger the payback. Susy imagined the round-the-world trip she had always wanted to take, and asked if she could make an initial small investment, and then regular payments to build up her shares. Tim said he didn't want her to miss out on the holiday so, if she liked, he was willing to help her set up an online (NetBank) account to make regular transfers of \$2,000. When the NetCode came through to Susy's phone, she gave it to Tim, as he explained he needed it to help her set up her account.

The change in banking, and the large international transfer, created a flag in CommBank's system and triggered a lock on Susy's account. She then received a call from John, a CommBank employee. Susy told John that she had organised this transfer to a new online account. John went through the warning signs of scams with Susy, but she assured John that this was not a scam. A week after Tim's internet 'help', a transfer of \$2,000 was made as agreed by Susy. Once more the bank contacted Susy, who again assured them that she had approved the transfer.

Over the next two months, automatic transfers continued. Unknown to Susy, transfers were made ranging from \$2,000 and up to \$20,000.

During a visit to the bank, Susy realised her account was almost empty. She admitted to the teller that she had given her bank details and NetCode to Tim, allowing him to set up an online account that gave him access to all her money.

The bank locked Susy's NetBank account, blacklisted the recipient and tried to recover the lost funds. Of the \$90,000 Susy had lost, the bank was only able to retrieve the initial transfer of \$9,700 made to another financial institution. All of the money 'Tim' had transferred from Susy's account had disappeared.

Susy's story is based on a real-life Commonwealth Bank case study.