BankVic
For police, emergency and health workers

CRIME STOPPERS .com.au 1800 333 000 Victoria

VICTORIA POLICE

Smart Scam Guide

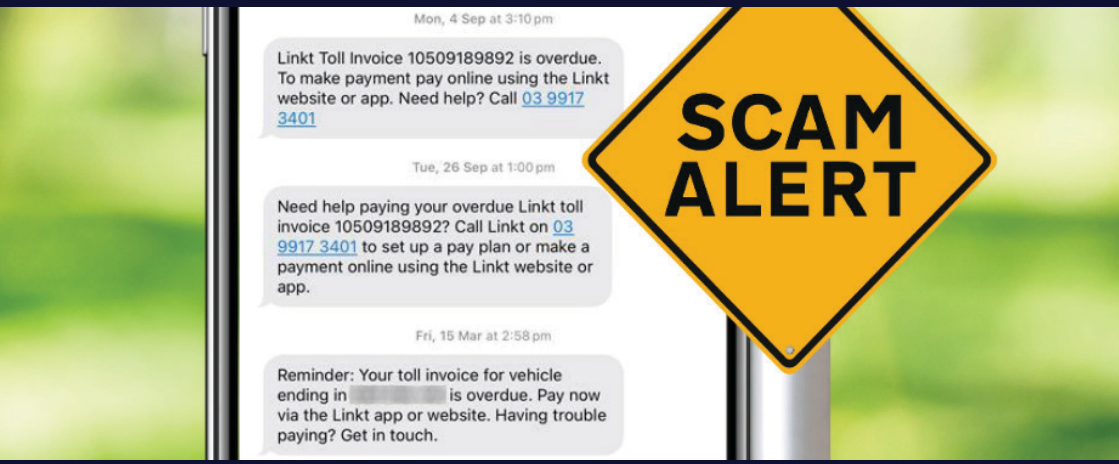
What is a scam?

A scam is deception used to steal your money or personal information. Scammers are becoming more sophisticated which means anyone can fall victim. Scammers often prey on people's trust, ignorance, or emotions to achieve their outcome.

Scammers are after:

- **Your money.** They might try to trick you into paying them for something that doesn't exist or get you to send them money directly.

- **Your personal information.** This could be things like your credit card number or passwords. They can then use this information to steal your money or commit identity theft.

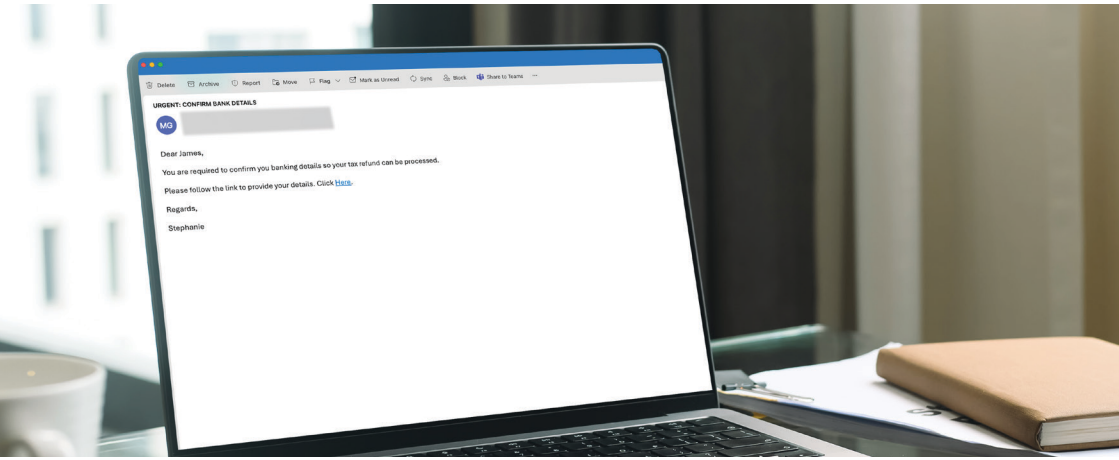


How to identify a scam?

Scams can come in many forms, so you should always be wary of anything that seems too good to be true. This could be amazing deals or quick ways to get rich.

Scammers often pressure you to act fast, so you do not have time to think clearly or do your own research. They might ask you to pay with unusual methods like gift cards or cryptocurrency, which legitimate businesses would not do. Look out for poorly written messages with bad grammar and spelling, as well as threats or scare tactics designed to panic you into giving them what they want.

To stay safe, avoid clicking suspicious links or attachments, research investments thoroughly, and never share personal information with strangers. By recognising these scam techniques and talking to your loved ones, you can help each other avoid falling victim to scams.



Phishing Scams:

Scammers send emails or messages impersonating legitimate organisations, such as banks, tricking recipients into revealing sensitive information like passwords or banking details. Phishing scams can even be tailored to specific individuals or organisations with personalised emails and calls.

- Email Phishing
- Phone Call Phishing
- SMS Phishing
- Social Media Phishing

Online Shopping Scams:

Fake online stores offer enticing deals on products, but either deliver substandard goods or never deliver anything at all.

These scam stores often operate during holiday periods and events such as Black Friday Sales. The fake online shops often look legitimate with scammers now paying for their phony websites to appear at the top of internet search lists.

Verify buyers and sellers when using online marketplaces.

Remote Access Scams:

If you are ever unsure about who you are speaking to, disengage, and contact your bank or telecommunications provider directly. Scammers pretend to be from tech support or Government Agency, they claim there is a problem with the victim's computer or device and offer to help fix it remotely.

They trick victims into granting remote access to their computers to install malware or steal personal information.

Remember that banks and telecommunications will not require access to your online banking.

Rental Scams:

A rental scam involves someone posing as a landlord or property manager to advertise a nonexistent or unavailable rental property.

These scammers ask for upfront payments or deposits, then disappear with the money. They might also show a property they do not own, taking payments from multiple renters for the same place. Victims often lose their money and face significant inconvenience without a place to live.

Tax Scams:

Imposters pose as tax officials, demanding immediate payment for fake debts or offering fake refunds to trick individuals into providing personal or financial information.

- ATO Impersonation Scams
- Fake Tax Refunds
- Fake Tax Preparation Services

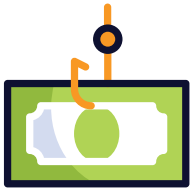
Investment Scams:

Fraudulent schemes promise high returns with low risk but end up swindling investors through fake ventures.

- Cryptocurrency scams
- Ponzi schemes
- Fake initial public offering scams
- Superannuation scams
- Celebrity endorsement scams

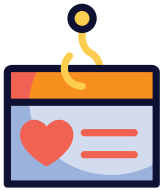
Lottery and Prize Scams:

Victims receive notifications of winning the lottery or prizes but are required to pay fees or provide personal information upfront, only to never receive the promised winnings.



Romance Scams:

Scammers create fake profiles on dating sites to develop relationships and then request money under false pretences, preying on emotions for financial gain.



If you have fallen victim to a scam and someone contacts you claiming they can help you recover your lost money, be cautious—this is likely another scam.

What to do if you've been scammed?

Step 1:

If you have given any financial details or have already lost money, contact your bank immediately.

Step 2:

Report the scam to police at cyber.gov.au or at your nearest police station.

Additionally, you can report the scam to Scamwatch at scamwatch.gov.au.
They also have valuable resources about different scam types.

If you think you have been scammed online, IDCARE can help for free! Call 1800 595 160 or visit their website www.idcare.org.

Step 3:

Getting scammed online does not mean you are not smart. Cybercrime keeps changing, so anyone can be a target. Do not be embarrassed or hard on yourself! Learn about new scams and take steps to stay safe instead.

If you need support after falling victim to a scam talk to friends and family or contact:

Lifeline: 13 11 14

Beyond Blue: 1300 22 4636

Step 4:

Finally, talk about different types of emerging scams and if you have been scammed share your experience with family and friends so they can better recognise the signs of scams.

BankVic
For police, emergency and health workers

CRIME STOPPERS .com.au 1800 333 000 Victoria

VICTORIA POLICE