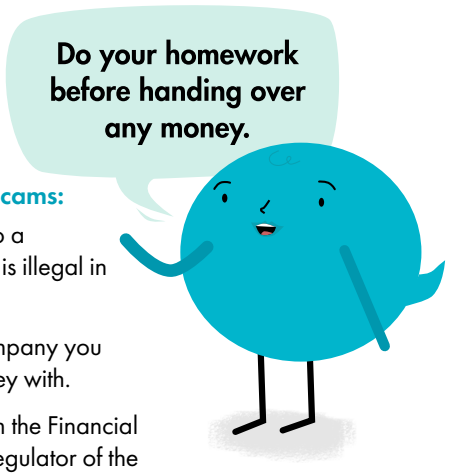
Banking Ombudsman Scheme

Top five scams – and how to avoid them

Scammers are finding ever more sophisticated ways to con people out of their money. Here are the most common scam complaints made to the scheme, along with tips on how to avoid them.

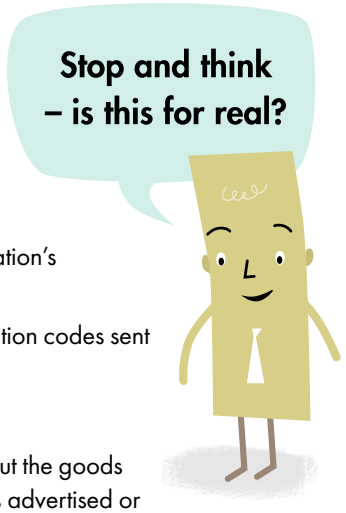


Phoney emails, calls and texts

Victims receive an email, phone call or text from what appears to be their bank or another trusted organisation for an apparently legitimate purpose, but the scammers are actually seeking banking details such as credit card numbers and verification codes.

How to avoid "information-harvesting" scams:

- Never click on links sent in an email or text message.
- Only give out your card or banking account number if you initiated the contact.
- Make sure emails from government departments or companies match the organisation's web address.
- Never reveal payment verification codes sent in bank text messages.



Dodgy online purchases

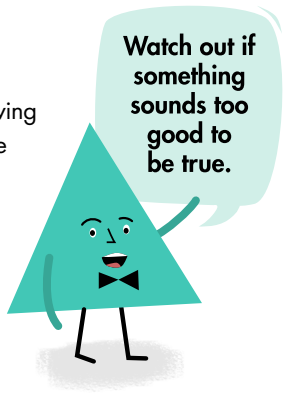
Scammers take victims' money, but the goods or services don't match what was advertised or don't turn up. Cheap or free trials can require subscriptions, which can be hard to cancel. See our Quick Guide to chargebacks about getting your money back if you used your credit card to buy dodgy goods or services online.

How to avoid online purchase scams:

- Pick up any goods bought through social media platforms in person and pay cash.
- Make a note in your calendar to cancel a subscription before a free trial period ends if you want only the free trial.
- Buy concert and event tickets from reputable ticket agencies to ensure they are genuine.

Fake investment scams

Online investments, especially those involving cryptocurrency and foreign exchange, are popular, and it is hard to tell legitimate from scam services. Some scammers even produce false trading records so victims don't realise their money has been stolen.



How to avoid investment scams:

- Never invest in response to a cold-call – a practice that is illegal in New Zealand.
- Look up reviews of the company you intend investing your money with.
- Check scam warnings from the Financial Markets Authority or the regulator of the country where the company is incorporated.
- Contact the company on its publicly listed contact details to confirm account details before transferring any funds.

Remote-access scams

Scammers call pretending to be victims' telecommunications provider or bank – or even the police – and persuade them to download remote-access software on to their computer and/or mobile, supposedly to solve some problem, but in truth so they can steal money from the victim's bank accounts.

How to avoid remote-access scams:

- Never log in to internet banking while someone has remote access to your device.
- Set up payments limits and two-factor authentication on your internet banking.
- Be honest with your bank if it calls to query a transaction and you have given someone access to your device.

Stolen cards and devices

The theft of a credit card or mobile phone can result in your bank accounts being cleaned out.

How to avoid the theft of a card or device:

- Password-protect all your devices, whether a mobile phone, tablet or laptop.
- Use a biometric log-in or a strong unique password so you alone can access your bank accounts.
- Don't leave your card or devices in places, such as a parked car or unattended handbag, where they can be removed without your noticing.

See our Quick Guide to scams for information about other scams, such as romance scams, invoice scams and money mules, and how to protect against them.