Scams and Fraud

How-to guide to help keep your money safe

This guide covers some of the most common scams and ways to keep you and your money safe.

Contents

Have you been scammed?

Here's what to do

1. Call us immediately on 0800 269 296 (international +64 4 440 3142, charges may apply).
2. Stop communicating with the scammer. Block their number or email address.
3. If you think your card details are compromised, block or cancel your card immediately either in ANZ Internet Banking or the ANZ goMoney app or by calling us. Review your account activity to make sure you made every transaction.
4. Change your passwords. Use a different device that's not at risk of being hacked by the scammer, or contact the relevant organisation for help if your accounts are locked.

Make sure you also:

- Ask a trusted family member or friend for help and support.
- Report the scam or fraud to any other financial providers or banks you use and the Police or CertNZ, if relevant.

Our top tips to help protect your money

1. Be confidently sceptical; if something doesn't seem right, take a moment to think about it and talk to a trusted friend or family member if you're unsure.
2. Be wary of unexpected phone calls, as scammers pretend to be from legitimate organisations. Contact the organisation on their publicly listed phone number to see if it's a genuine call.
3. Never click on links or download attachments in unexpected emails, texts, or social media messages.
   - Be mindful if you expect an invoice to come through, as they can be intercepted by scammers. It's best practice to check you're paying the right person or organisation by contacting them on a known or listed number to confirm they sent the invoice and that the bank details are correct.
   - Delete unsolicited emails or messages from people or organisations you don't recognise.
4. Don't access your Internet Banking by clicking a link. Always type the full address (www.anz.co.nz) into your web browser.
5. Never share or confirm your passwords, credit card details, Internet Banking or goMoney login details, or two-factor authentication codes (a code you receive in a text) in response to an unexpected phone call or through a link in an email or text.
6. Never give someone remote access to your devices or let them convince you to download or install software.

Visit the ANZ Scams and Fraud hub to stay up-to-date with the latest scams, anz.co.nz/banksafe

Cold call scams

When you're contacted unexpectedly and asked for personal details, which could give the scammer access to your money.

Common signs of this scam

The scammer may say to keep your accounts and money safe you need to:

- Transfer money to another account.
- Give them personal or bank information, like credit card details or a Visa Secure code.
- Verify a suspicious transaction on your account or they'll inform you about a refund.
- Have cash, cards, and PINs ready for them to pick up from your home.
- Help catch hackers or bank staff involved in fraudulent activity by transferring funds to New Zealand or offshore accounts.
- Set up a cryptocurrency account or other types of accounts.

Top tips

- Hang up if unknown callers ask for personal information.
- If you think the request might be genuine, phone the organisation back on their official, publicly listed number.
- Always say no if you're asked to buy pre-loaded debit cards, gift cards, cryptocurrency, iTunes cards, or use third-party money transfer agencies.

Remote access scams

When someone gains access to your device (i.e. smartphone, tablet or computer), it could allow them to access your Internet Banking or goMoney app, steal your personal details or any data saved on that device, or impersonate you.

Common signs of this scam

Scammers will phone, text or email to say:

- There's a problem with your internet connection.
- Your device has an issue or needs maintenance.
- You're being hacked, and they can help stop it.
- They've seen unauthorised transactions and can help stop it. Scammers might even provide step-by-step instructions or offer to walk you through the process, including logging into your Internet Banking or goMoney.

Top tips

- Never give strangers access to your devices.
- Never save your Internet Banking passwords or login details to the browser.

Phishing scams

When someone tries to trick you into giving them information or money, usually via text or email.

Common signs of this scam

- A call to action, like ‘pay your toll’ via a link.
- A sense of urgency or pressure to act quickly, such as ‘your accounts have been locked’.
- Poor spelling and grammar, including typos.
- Incorrect sender email addresses or an email address that doesn’t look right.
- Texts sent from overseas phone numbers.
- Messages that ask you to ‘confirm’ or ‘verify’ account information which could be ‘stolen’, ‘lost’, or requires ‘updating’.
- Links to fake websites that look real and attachments that could download a virus onto your device.

Top tips

- Don’t click links in unexpected texts or emails.
- Ask a trusted family member or friend if you’re not sure, or call the company on its publicly listed number to check if it’s real.

Card Fraud

When someone steals and uses your card or its details. Note, scammers don’t need your physical card to make fraudulent transactions.

You might notice

- Unexpected emails, text messages, or cold calls where you’re asked for your card details.
- Your transactions show unusual or unfamiliar transactions at stores or locations you don’t recognise.

Top tips

- Review your account activity regularly to make sure you made every transaction.
- See who may have your card details stored using ANZ Card Tracker in goMoney.
- Keep your PIN a secret. Never write it down and make sure it’s hard to guess.
- Don’t provide your credit card number, expiry date, CVV code, and/or Visa Secure codes to someone who calls, emails, messages (including via social media), or texts you. This includes automated voice messages saying you have an unexpected charge or refund on your account.
- Use a different PIN for all your cards, goMoney and phone banking.
- If your card is lost or stolen, block or cancel it immediately in Internet Banking or goMoney, or call us.
- Use card settings in goMoney to change how your ANZ Visa Debit or credit card and mobile wallet can be used. You can turn on and off online shopping, overseas in-person purchases, contactless purchases and online gambling transactions.

Block or cancel your card in Internet Banking or goMoney. See how at anz.co.nz/guides

Investment scams

When you're invited to invest in a fake money-making opportunity or looking to invest.

Common signs of this scam

You're offered an opportunity to:

- Purchase shares in a company.
- Invest funds in a term deposit.
- Invest in foreign exchange.
- Invest in gold or other precious metals.
- Invest in property.
- Buy cryptocurrency.

There is usually urgency behind the offer, with the scammer pushing you to act quickly so you don't miss out.

Top tips

- Before investing money, thoroughly research the organisation, the investment opportunity, and the people behind it. Look for information from independent sources, including regulatory agencies, financial analysts, and reputable news outlets.
- Before making any decisions, consult a licensed financial adviser or investment professional.
- Remember, if an investment opportunity sounds too good to be true, it probably is.

Protect your money

Be very sceptical if the investment opportunity comes from:

- A organisation that isn't registered with regulatory agencies or doesn't provide clear and transparent information.
- An unexpected phone call, social media posts or social media chat seeking a relationship, and ultimately asking for money or to invest.

Be wary if you're contacted to get your funds back from previous investments.

Romance and Friendship Scams

When someone tries to gain your trust and trick you into giving them money.

Common signs of this scam

If you've met someone online, they may:

- Quickly profess their admiration or love for you.
- Have a heart-wrenching story or compelling reason to borrow money – often small amounts to begin with.
- Constantly have excuses why they can't meet in person.
- Claim to be working overseas.
- Have their camera off or image blurred if you video call.

Top tips

- Romance scams can happen to anyone, so it's important to be cautious when interacting with people online.
- Talk to a trusted family member or friend if you feel uneasy or unsure about requests from an online acquaintance or partner.

Talk to a trusted family member or friend.

Hang up if unknown callers ask you for personal information.

Don’t click links on unexpected texts or emails.

Never give strangers access to your devices.

Have a secret family code word to check if it’s really your loved one.

Use additional banking security measures, like ANZ OnlineCode or Voice ID.

Protect your banking information and devices by using unique passwords and PINs. Never save your customer number, passwords or PINs to your browsers or devices.

Verify all requests for personal details or money - contact the organisation on their official number.

Don’t be pressured into quick decisions.

Regularly check your transactions.

Have you been scammed, or want to find out more about scams and how to protect your money?

Visit anz.co.nz/banksafe

Call 0800 269 296

Come into any branch