BANKING SECURELY

HANDY TIPS TO HELP KEEP YOU PROTECTED

ANZ

WE HAVE A SPECIALIST TEAM ON HAND TO HELP YOU

24 hours a day, 7 days a week

Report suspicious messages: 13 33 50

+61 3 9683 8833 (if overseas)

or send a screenshot of the message to
hoax@cybersecurity.anz.com

- Stop communicating with the scammer. Block their number or email address.
- Change passwords. Use a different device that's not at risk of being hacked by the scammer. Or contact the relevant company for help if your accounts are locked.
- If you think your card details are compromised, block or cancel your card immediately either in ANZ Internet Banking or the ANZ app or by calling us. Review your account activity to make sure you made every transaction.

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

KEEP AN EYE OUT FOR RED FLAGS

We won't email or message you asking for personal information like passwords, PINs or account details. If you get a suspicious call or message, ignore it and let us know immediately.

An email or SMS prompting you to open a link or an attachment to access your banking platform.

Phone calls with automated voice messages asking you to take action on your bank account.

Any unfamiliar online payment requests including direct bank transfers or other unusual methods (like gift cards or cryptocurrency).

A request to remotely access your computer. This means allowing someone to access your computer device from another device, at any time, and from anywhere.

Any messages urgently requesting personal information or a payment.

Unsolicited loans or offers that sound too good to be true.

SOME SCAMS TO WATCH OUT FOR

BUSINESS EMAIL COMPROMISE

A scammer posing as a supplier or vendor may email you to advise their banking details have changed and ask that all future payments are processed to the new account. Or you may receive an invoice from a compromised business email.

BANK IMPERSONATION SCAMS

Often commences with a text message either with a request to call the bank or a link to website requesting personal information. A follow up phone call then seeks to convince the customer that their account is compromised and that they should transfer funds to a "safe account".

REMOTE ACCESS SCAMS

Also known as technical support scams, this usually involves scammers requesting access to a person's computer or charging them for fake software or security products.

THREATS AND EXTORTION SCAMS

Happens when you are threatened, coerced, blackmailed or frightened into complying with the scammers' demand. This could include paying money immediately or disclosing personal information.

INVESTMENT SCAMS

Getting you or your business to send money on the promise of financial opportunity. The scammers will often call or email you claiming to be a stock broker or portfolio manager and offer low-risk investments with high returns.

ROMANCE SCAMS

Typically involves faking romantic interest towards a victim, gaining their trust and affection, and then committing financial fraud. This could involve asking to be sent money.

TIPS TO HELP SAFEGUARD YOUR INFORMATION

TIP 01 Talk to a trusted family member or friend

TIP 02 Hang up if unknown callers ask you for personal information

TIP 03 Don't click links on unexpected texts or emails

TIP 04 Never give strangers access to your devices

TIP 05 Have a secret family code word to check if it's really your loved one

TIP 06 Don't be pressured into quick decisions

TIP 07 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

TIP 08 Verify all requests for personal details or money - contact the company on their official number

TIP 09 Use additional banking security measures, like one-time passcodes for payment, Shield or token codes

TIP 10 Regularly check your transactions

This is provided as general information only and does not take into account your specific objectives/circumstances etc. Consider obtaining your own advice in respect of any matters raised here.

Connect with us

Visit anz.com/security

Call us on 13 33 50, 7 days a week

Visit your nearest ANZ branch

facebook.com/anzaustralia

@anz_au

youtube.com/anzaustralia

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. Australian Credit Licence Number 234527.
Item No. 98078 09.2023 WZ135420

anz.com