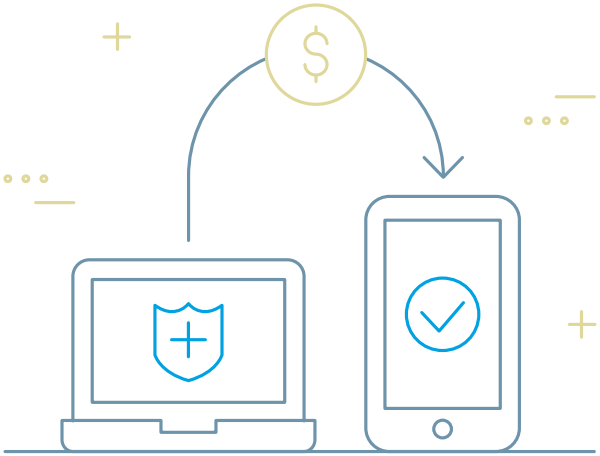
THE ANZ BANKING SAFELY GUIDE

We're committed to keeping you and your banking safe, and you have a role to play too. Working together, we can keep you even safer. This guide will tell you what security measures we have in place, the tips for how you can keep yourself and your banking safe, and the types of scams to look out for. Print it off and keep it in a place you can easily reference, like on the fridge, near your home phone, or your desk. And, if you have a friend or family member who you think would benefit from knowing this information, please share it with them.



WAYS TO BANK

We offer a variety of ways for you to do your everyday banking.

As well as visiting a branch or calling our contact centre, you can use your smart phone or computer to bank where and when it's convenient for you.

These options provide flexibility, and they're very secure ways to bank. Each one allows you to check account balances and transaction history, transfer funds between accounts and make payments to other people or businesses (e.g. to pay a bill).

- **ANZ Internet Banking**

  Access your bank accounts at any time through a safe, password protected internet site.

- **ANZ Pacific App**

  Download our mobile banking app to your iPhone, iPad or Android device and you can access all your bank accounts at any time while protected by a PIN, your fingerprint or Face ID.

BANKS AND SECURITY

We have a range of security measures to help protect your personal information:

- **Two-factor authentication** is an added security feature used to confirm your identity, comprising two additional steps

  (i) site key image and phrase and

  (ii) security questions,

  within the log in process for ANZ Internet Banking and when initially logging in to the ANZ Pacific App.

- **Visa Secure** helps protect you against unauthorised use of your card online. It works automatically most of the time, but sometimes you may be sent a verification code to your ANZ Bank Mail, which you'll need to enter to continue with your transaction.

- **Fraud monitoring systems** allow us to identify potentially fraudulent activity on your accounts. If we suspect fraudulent activity we'll contact you and may temporarily suspend your banking or block your cards in order to prevent further fraudulent transactions.

Remember, ANZ will never ask for your password, PINs or security codes over the phone or email. We'll also never request remote access to your computer or phone or leave pre-recorded messages with instructions. You should not give your password, PIN or security code to anyone, not even ANZ staff or the Police.

Australia and New Zealand Banking Group Limited, Tonga Branch 12/22 22573

TIPS FOR SAFE BANKING

These tips will help to ensure you and your banking is safe.

BANKING ONLINE

- Access internet banking by typing in the full address (e.g. anz.com/tonga). Don't click on links you may receive in emails. ANZ will not send you emails that ask you to click on links to log in to your internet banking.
- If you suspect your password or security questions have been compromised, give us a call on **+676 20500**. Please note, we will not be able to help you with queries relating to passwords or security questions via Bank Mail.
- Make sure all software and apps are the latest versions. Also, ensure you have up to date anti-virus software installed.
- Don't save your User ID, passwords, PIN(s), security code, security questions, site key or biometric identification to your browser or device.
- Never disclose your User ID, passwords, PIN(s), security code, security questions or site key to anyone, even if they say they are calling from the bank or the Police.

MOBILE BANKING

- Keep your PIN secret, make it hard to guess and don't use the same PIN for anything else.
- Keep your devices locked when not in use, always log off the ANZ Pacific App when you're finished.
- Set your software, operating system and apps to automatic update to make sure you get the latest security features.
- Never download apps you're not familiar with or give anyone remote access to your device.

PROTECT YOUR PERSONAL INFORMATION

- Keep your personal details, such as legal documents and bank statements, in a safe place. Treat these personal details like you would treat money – don't give them away!
- Ensure all your devices are protected with a PIN, password or biometrics like FaceID or TouchID so your information is always protected, even if the device is lost.
- Don't save your User ID, passwords, PIN(s), security code, security questions or site key to your browser.
- Check statements and call your bank immediately if you see anything suspicious.
- Destroy papers with your personal details on them before throwing them away (shredding is recommended).
- Your personal information is highly valuable and can be used to commit fraud. Be cautious about who you provide your information to, whether online or over the phone.

USING YOUR CARD

- Always sign the back of your card in ink as soon as you get it.
- Use a different PIN for each of your cards, and don't make it easy for others to guess (like your date of birth). Memorise your PIN (don't write it down) and change it regularly.
- Keep your PIN secret, even if people claim to be from your bank or the Police.
- Keep your card in a safe place and don't let others use it. Don't let it out of your sight, for example, at a restaurant.
- Cover your hand when entering your PIN at ATMs or EFTPOS machines.

Australia and New Zealand Banking Group Limited, Tonga Branch 12/22 22573

HOW TO KEEP YOURSELF SAFE BY KNOWING WHAT SCAMS ARE OUT THERE AND SPOTTING THE RED FLAGS

Anyone, including you, can fall victim to a scam. That's because scammers don't discriminate and will target people of any gender, age-group or socio-economic background. It's important that you familiarise yourself with how scams can target you.

KNOW WHAT'S OUT THERE

- Tech support/remote access phone scams
- Catch the Hackers Scam
- Romance scams
- Investment scams
- Fake charities
- Fake offers of employment
- Threat and extortion scams
- Lottery scams
- Unexpected get rich quick schemes
- Outstanding debt scams
- Phone scams
- Government grant scams
- Business email compromise/Invoice scams

SPOT THE RED FLAGS

- Have you met the person you're sending funds to?
- Have you been asked to download software to access your computer or mobile devices remotely?
- Have you been asked to receive and send funds on behalf of a third party?
- Have you received a phone call where a demand was made to send money?
- Are you being asked for an excessive amount of personal information, or information the caller should already know?
- Are you being told that you must act urgently or to keep things confidential?

HAVE YOU HAD AN UNUSUAL REQUEST?

Scammers try to use payments that can't be traced such as pre-loaded debit cards, gift cards, bitcoins, iTunes cards or money transfer systems. They may ask you to transfer funds to local or offshore accounts for the purpose of assisting with an investigation or to 'catch the hackers/scammers'.

HAVE YOU BEEN ASKED TO DOWNLOAD REMOTE ACCESS SOFTWARE?

Don't let anyone who calls you out of the blue convince you to install software in order to access your computer or mobile device, even if they say they're from the Police, your phone company or bank. Hang up immediately and call the company back on their listed number to check if it's legitimate.

HAVE YOU VERIFIED YOUR PAYMENT DETAILS?

Ensure that you verify all changes to payment instructions, especially those received via email. Contacting an organisation using their listed contact details enables you to confirm that the changes were genuine and not the result of a fraudster intercepting communications.

THINK TWICE

- Do you understand the reason you are sending funds?
- Have you received an invoice for this payment or transfer?
- Why are you sending funds overseas?
- Does what they're saying really sound true?

HOW TO KEEP YOURSELF SAFE BY KNOWING WHAT SCAMS ARE OUT THERE AND SPOTTING THE RED FLAGS

DOES SOMEONE NEED YOUR URGENT FINANCIAL HELP?

Scammers take advantage of people in an attempt to get them to provide money, gifts or personal details.

They may use a fictitious name or falsely take on the identities of real, trusted people and often claim to be locals but working overseas. Think twice before you send money to someone you're unfamiliar with or haven't met.

IS IT TOO GOOD TO BE TRUE?

You should make your own reasonable enquiries and check online if they say they're a business or financial advisor – if you can't find anything, do not deal with them. Searching online for a company name will often quickly alert you to if it is a scam or not.

MAKE SURE THAT YOU PERFORM SUFFICIENT CHECKS BEFORE GIVING YOUR DETAILS TO AN UNSOLICITED CALLER OR REPLYING TO EMAILS OFFERING FINANCIAL ADVICE OR URGENT INVESTMENT OPPORTUNITIES

BE AWARE OF PHISHING

A common tactic used by fraudsters is to pretend to be from a bank or another reputable organisation, in an attempt to steal your personal information or gain access to your bank accounts.

Ways phishing attacks can occur:

- Email
- Text message (sometimes called Smishing)
- Phone calls.

Things to be wary of:

- Being asked to click an attachment that downloads malware.
- Being asked for your personal information such as User ID, passwords, PIN(s), security code, security questions or site key.
- Being asked to click a link to access your internet banking.
- Being asked to download software that allows remote access to your devices.

HOW TO PROTECT YOURSELF FROM SCAMMERS

Be very wary of unexpected calls

Don't give anyone remote access to your phone or computer. Be careful about sharing personal information and if you're unsure, just hang up and call the organisation back on their listed phone number to check. Make sure you report scam calls to your phone company and bank.

Be careful about clicking on links or attachments in emails and text messages

Hover your cursor over the link to see which website it leads to and if you have doubts, don't click. On a mobile device you can press and hold a link and the website address it leads to will pop up for you to check first.

Only shop at websites you trust

Beware of sites that you and others you know have never heard of or used. Never set your computer to auto-save passwords or other personal information.

Always type URLs (website addresses) directly

When visiting shopping websites or logging into your internet banking, type the URL directly. That way you'll know you're on the right site and not a 'fake' one.

Act quickly

If you think you've downloaded an attachment or clicked on a link in an ANZ branded email or text message that may be suspicious, contact ANZ immediately.

Australia and New Zealand Banking Group Limited, Tonga Branch 12/22 22573