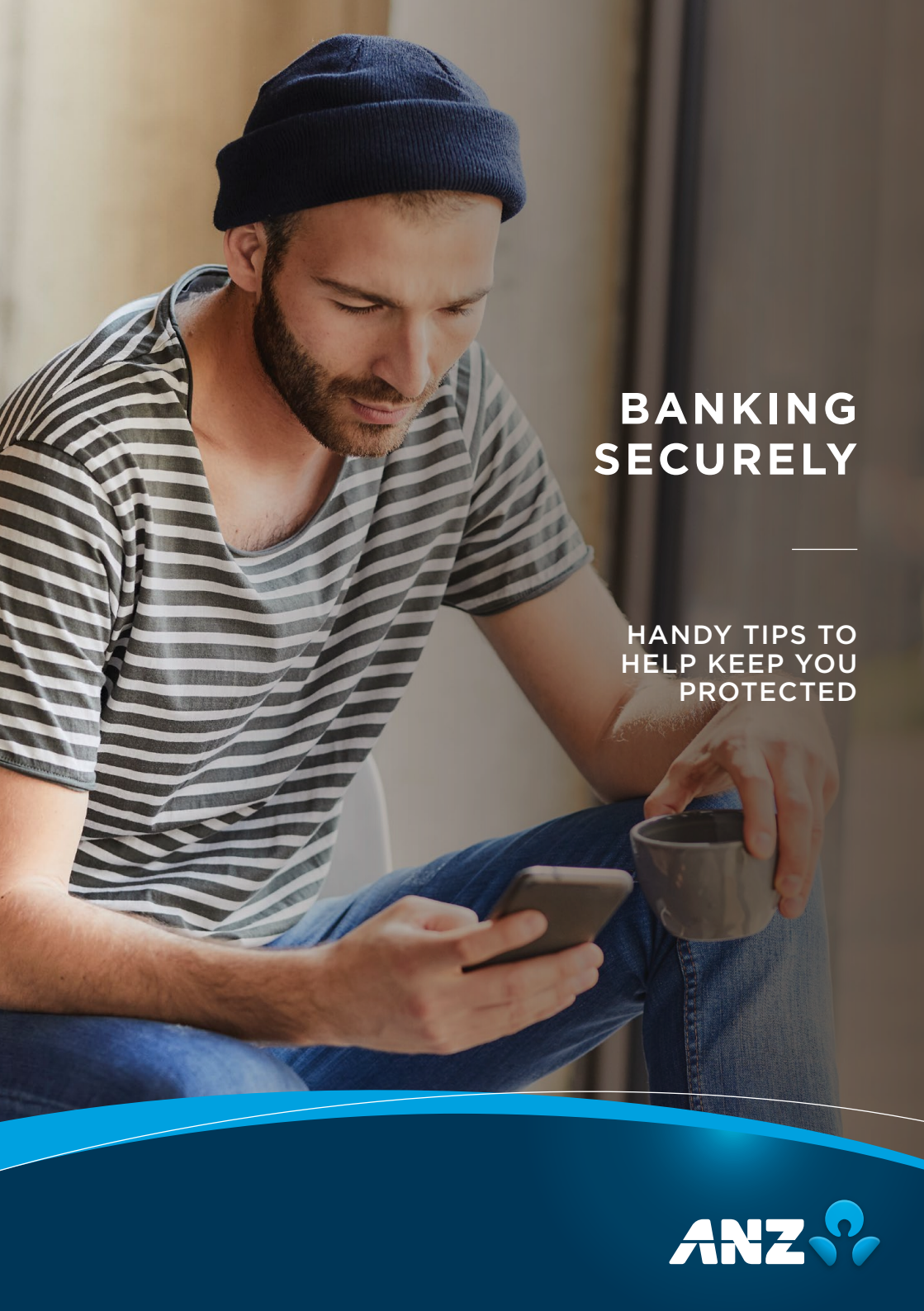

BANKING SECURELY

HANDY TIPS TO HELP KEEP YOU PROTECTED

ANZ

KEEPING YOUR MONEY SECURE

To support you on your journey to better financial wellbeing, here are some handy tips to help you stay safe online so you can protect what you own.

To find out more visit, anz.com.au and search 'financial wellbeing'.

SOME TIPS TO HELP SAFEGUARD YOUR INFORMATION

USE SECURE ACCESS

- Use secure connections when accessing your account.
- Protect your Wi-Fi network with a password and avoid using public computers or Wi-Fi hotspots to access online banking or provide personal information.
- Your personal devices can be monitored when using these non-secure connections to access your personal and financial information.

CREATE A STRONG PASSWORD

- Choose a password or passphrase that's easy to remember but hard for someone else to guess.
- Never share your passwords or PINs. If you share your passwords and PINs you may become liable for any unauthorised transactions on your account.
- Use different passwords for online banking, social media and email accounts.
- Avoid saving passwords to your browser or writing them down.

CHECK THE EMAIL OR SMS DETAILS

Verify the email sender's name and contact details before clicking on any links.

Here are some things to look out for:

- Messages that are poorly written with spelling or grammatical errors.
- Are the links legitimate? Hover over them to make sure that the website is linked directly to the company website.
- Is the email too general? For example, does the email or text begin with 'Dear valued member' or 'Dear Customer' rather than use your first and/or last name.
- If you're suspicious about the link, contact the sender directly using another channel, such as a phone to confirm that you should have received the email and that the link address is correct.

REVIEW YOUR ACTIVITY

Check your transactions and statements regularly in the ANZ App and Internet Banking to spot any transactions or transfers you don't recognise.

Please call us on 13 13 14 about any transactions or transfers you don't recognise.

BE WARY OF SUSPICIOUS CALLS OR MESSAGES

If you get a phone call or message relating to your ANZ banking that seems unusual:

- Do not share any personal information like your date of birth, address and bank details (information that can be used to uniquely identify you) if you get an unusual call or message.
- Simply hang up or report the call to us immediately if you believe a scammer may be impersonating a company or government organisation asking for your personal information.

TAP AND PAY

Use your eligible ANZ debit or credit card or your digital wallet on your mobile device (such as phone or watch) to make payments by simply holding your card or device over the reader.

The fact that the card never leaves your hand during the transaction makes it even more secure. Contactless technology also prevents accidental payments, even if you touch the card reader twice.

KEEP YOUR BANKING SECURE

- Set an automatic lock on your phone.
- Use a PIN, fingerprint or facial recognition password for your phone.
- Sign out of online banking sessions every time.
- Turn on automatic updates for the software and apps on your devices to get the latest security features.
- Back-up your device regularly to keep your data safe.

USE VOICE ID

- You can use Voice ID in the ANZ App to help protect high value payments. Voice ID is a secure way for us to check that you're the correct person initiating the payment. With just your voice, you can make Pay Anyone payments over $1000 and pay BPay® bills over $10,000 without needing to generate a special code or password. For more information, visit anz.com/voiceid

ADD A LAYER OF PROTECTION

- Use two-factor authentication when prompted – this is an additional layer of security to keep your information safe and secure. The first factor will be something you know, like your password. The second factor is something you have, like a one-time passcode sent to your mobile phone.
- Download and use ANZ Shield app on your device to add an extra layer of security for transactions. The app verifies your banking activity and provides access to other security features.
- Install an Anti-Virus program on your device to give you added protection from hackers.

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. Here are some red flags to look out for.

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

A request to remotely access your computer. This means allowing someone to access your computer or 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.

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

Incorrect or missing personal details on any form of communication (be sure to check the spelling).

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

Altered or unusual branding and logos on any form of communication.

SOME SCAMS TO WATCH OUT FOR

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.

ROMANCE SCAMS

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

QR CODE SCAMS

When you've scanned a QR code always double check the website name it directs you to. If anything looks odd or suspicious, immediately close your browser.

Be wary of QR codes asking for your personal information, always visit the official website on your browser.

Never download phone applications from QR Codes. Always visit the official App Store* or Google Play Store** to download the application.

PHISHING SCAMS

This often involves scammers sending fraudulent messages containing suspicious links or attachments. Opening a phishing link can expose you to malicious software being downloaded onto your device or lead you to webpages, that may request action from you; for example, asking you to enter your personal information which may be used to hack your accounts.

ONLINE SHOPPING SCAMS

This usually involves scammers setting up fake online shopping sites or sending a bill requiring immediate payment to prevent losing a service (e.g. Internet or phone) or negatively affecting your credit score. It may also involve sending fake offers to get victims to make payments for goods that never arrive.

INVESTMENT SCAMS

Scammers will offer high and quick-return investments, including through cryptocurrency, or tax-free benefits, convincing victims to invest before stealing their money.

* App Store is a service mark of Apple Inc.
** Google Play is a trademark of Google LLC.

WE HAVE A SPECIALIST TEAM ON HAND TO HELP YOU

24 hours a day, 7 days a week

KEY FEATURES THAT HELP KEEP YOU PROTECTED

- **Automatic log out** – If you forget to log out, we time-out your session after 3 minutes in the ANZ App and 15 minutes in Internet Banking.
- **One-time passcodes** – To make some transactions, you will need to add a second passcode. We will send this passcode via email or SMS/text to you, so you can make this transaction.
- **Fraud protection** – We'll reimburse you for any unauthorised transactions on your account, provided you didn't contribute to the loss and you report any unauthorised transactions as soon as you suspect something suspicious or unusual has occurred.

REPORT ANY FRAUDULENT OR UNUSUAL ACTIVITY

Contact us if you've:

- Shared or updated your account details in response to a hoax phone call, email, or SMS.
- Accidentally clicked on any suspicious links or downloaded any attachments.
- Noticed any unusual transactions on your accounts.

Report suspicious messages: 13 33 50
+61 3 9683 8833 (if overseas)

If something doesn't look right, forward the email or send a screenshot of the SMS to hoax@cybersecurity.anz.com and delete it from your phone or inbox immediately.

IMPORTANT THINGS YOU NEED TO KNOW

1. This brochure is current as of May 2022. New scams are constantly emerging and this brochure isn't a full exhaustive list of all scams currently out there. Please visit anz.com and search 'latest security alerts' to help you protect your banking information.
2. This brochure provides general information only and doesn't take into account your personal objectives, needs and circumstances. So please consider if these tips are appropriate for you.
3. The ANZ App is provided by Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. Super, Shares and Insurance (if available) are not provided by ANZ but entities which are not banks. ANZ does not guarantee them. This information is general in nature only and does not take into account your personal objectives, financial situation or needs. ANZ recommends that you read the ANZ App Terms and Conditions available at www.anz.com and consider if this service is appropriate to you prior to making a decision to acquire or use the ANZ App.

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 06.2022 WZ116897

anz.com