Scam and Fraud Awareness

Your guide to helping protect yourself against scams and fraud.

Heritage Bank

People first.

STOP Before acting on an email, phone call or message, take a moment to stop and assess the request. Consider how the information was received and what information is being requested. Stopping before you act on any request is a vital step as most scams rely on a sense of urgency or panic.

THINK Think to yourself, does this request make sense? Could this be a scam? If there is an urgency to respond or provide information, think about what could happen if you comply. Could the information you share grant access to your accounts or personal devices?

CHALLENGE Challenging requests is the best way to protect yourself. Refusing to provide information or ignoring requests gives you an opportunity to follow up the request directly with the company in question to validate the query.

Don't open suspicious texts or emails – delete them

If you're not sure, check the identity of the contact through an independent source such as a phone book or online search. Don't use the contact details provided in the message sent to you.

Tip: If you **DON'T KNOW** who sent you the text or email don't open or click on any links. The safest option is to delete it.

Beware of any requests for your details or money

Never send money or give bank card numbers, online account details or copies of personal documents to anyone you don't know or trust. Don't agree to transfer money or goods for someone else; money laundering is a criminal offence.

Tip: **SEARCH ONLINE** to confirm the contact details before proceeding.

Beware of unusual payment methods

Scammers often ask for payment by wire transfers, preloaded cards and even Google Play, Steam, or Apple gift cards and cryptocurrency. These are nearly always a sign that it is part of a scam. Check your transactions often and let us know immediately if there is any activity you do not recognise on your account.

Tip: **DO YOUR RESEARCH** via an independent source before you part with any money.

Be careful when shopping online

Beware of offers that seem too good to be true and always use an online shopping service that you know and trust.

Tip: **LOOK FOR THE CLOSED PADLOCK** on the website, as this confirms the site is secure. Do your research before you shop with a site that doesn't have a secure padlock.

Know who you're dealing with

If you've only ever met someone online or are unsure if a business is real, take some time to do a bit more research. Search online for real business photos or for reviews from others who may have had dealings with them.

Beware scammers will try and tell you what to say and how to act to avoid detection. Don't be afraid to ask questions.

Protect your Passwords, PINs, Internet & Mobile Banking

- Help protect your Passwords and PIN by memorising - never write them down or share with anyone. Keep all receipts in a safe place, or destroy carefully. Always keep your card in sight during a transaction, and destroy all cards when they expire
- Choose passwords that would be difficult for others to guess and update them regularly
- Don't use the same password for every account/profile, and don't share your passwords with anyone
- Never share your One Time Password (OTP) with anyone - this is personal to you and your financial institution will never ask for it. If you share your OTP, you may fail to meet Heritage Bank's passcode requirements, which could result in you being liable for unauthorised transactions on your account. Liability for losses will be determined under the ePayments Code, rather than these guidelines.

Keep your identity and personal details safe

- Always use password protection
- Don't share access to your computer or phone with anyone, including allowing remote access. Never give someone else access to your device by downloading anything or visiting a website.
- Update security software
- Back up content regularly
- Protect your WiFi network with a password
- Avoid using public computers or WiFi hotspots to access online banking or provide personal information
- If you are not sure how to do this, ask a trusted individual for assistance.

Steps you can take if you are a victim of fraud:

- Call us on our **Priority line 13 14 22 (option 0)** immediately if you suspect that you have been involved in scam activity
- Advise us as soon as you possibly can so that we can act immediately to help prevent further loss on your accounts
- Report the theft/crime to your local police
- Report online scams/crime to the Cyber Issue Reporting System via https://www.cyber.gov.au/report-and-recover/report
- If identification documents have been lost or stolen, contact **Equifax (telephone 13 83 32 or refer to www.mycreditfile.com.au)** to advise the credit bureau and check for any new applications for credit in your name
- Make sure to check with the post office if you haven't received regular expected mail, as your mail may have been redirected.

No one is immune to scams, and it can be very hard to deal with if you become a victim. We can all play a part to help remove the shame and isolation victims of scams can feel, by sharing experiences and what you've learned with your friends, family and community.

Tips for keeping our communities safe:

- Keep an eye out for new scam advice in the media.
- Subscribe to Scamwatch and follow us on Facebook for alerts and tips
- Educate your family members on safe technology use and how to spot warning signs
- And finally – talk with us and seek support. We are here to support you, and if in doubt, calls us or pop into the branch to talk about what's on your mind.

Further support

This may be a difficult time. Help can be found from a number of places outside the Bank.

To access confidential counselling services contact:

- **Lifeline Australia: 13 11 14 or online crisis support chat**
- **Beyond Blue: 1300 22 4636 or online chat**
- **Moneysmart: Financial counselling - Moneysmart.gov.au**

The following are official Australian Government websites with more information about fraud:

Scamwatch

www.scamwatch.gov.au

Australian Cyber Security Centre

Website and email alert service
www.cyber.gov.au

What to do if you have concerns:

Contact us immediately on 13 14 22
or visit your nearest branch.

heritage.com.au

Heritage Bank
People first.

Heritage Bank a trading name of Heritage and People's Choice Limited
ABN 11 087 651 125 AFSL and Australian Credit Licence 244310.
FC001 Effective 03/24