
**The golden rules to
protect yourself from
scams and fraud.**



Heritage Bank
People first.

Be aware that scams exist

When dealing with unknown contacts from people or businesses always consider the possibility that the approach may be a scam.

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

Don't open suspicious texts or emails – delete them

If unsure, verify 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.

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 proceed with a site that doesn't have a secure padlock.

Beware of unusual payment methods

Scammers often ask for payment by wire transfers, preloaded cards and even Google Play, Steam, or iTunes gift cards and cryptocurrency. These are nearly always a sign that it is part of a scam.

Tip: **DO YOUR RESEARCH** via an independent source before you proceed.

Know who you're dealing with

If you've only ever met someone online or are unsure of the legitimacy of a business, 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.

Keep your personal details secure

Keep your passwords and PIN (personal identification number) in a safe place and never share them with anyone or write them down. Be very careful about how much personal information you share on social media sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.


Tip: NEVER SHARE codes sent to you as an SMS from the bank to anyone – not even the bank.

Keep your mobile devices and computers secure

Always use password protection, don't share access to your computer or phone with anyone (including remotely), update security software and back up content regularly. Protect your WiFi network with a password and 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.

Choose your passwords carefully

Choose passwords that would be difficult for others to guess and update them regularly. A strong password should include a mix of upper and lower case letters, numbers and symbols (try a phrase). Don't use the same password for every account/profile, and don't share your passwords with anyone.



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.

The content of this brochure has been derived from the Australian Consumer and Competition Commission's Little Black Book of Scams available at www.accc.gov.au. The materials have been used under a Creative Commons Attribution 3.0 Australia licence. For more information see <http://creativecommons.org/licenses/by/3.0/au/>.
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 03/23