People's Choice

Banking for life

Scam and Fraud Awareness

Your guide to helping protect yourself against scams and fraud.

Stop

Before acting on an email, phone call or message, take a moment to stop and assess the request. Consider how any provided information may have been obtained 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? Is there an urgency to respond or provide information? Think about what could happen next 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.

Avoid interacting with unusual messages.

If unsure, verify the identity of the contact through an independent source such as a phone book or online search. Do not use the contact details provided in the message sent to you. If you don't know the sender do not open or click on any links. The safest option is to delete the message. Please call us to verify all communications and transactions claiming to be from People's Choice.

Beware of requests for your details or money.

Never send money or provide bank card numbers, account details or copies of personal documents to anyone you don't know or trust. Do not agree to transfer funds or goods to someone else, this could be considered money laundering and is a criminal offence.

Be careful when shopping online.

Beware of retail offers that seem too good to be true and choose verified retailers that you know and trust. Look for the closed padlock in the search bar of the website, as this confirms the site is secure. Do your research before proceeding with a site that doesn't have a secure website certificate.

Beware of unusual payment methods

Scammers often ask for payment via wire transfers, preloaded cards, cryptocurrency or even Google Play, Steam or Apple gift cards. This request is a strong indicator that it may be a scam. Check your transactions often and let us know immediately if there is any activity you do not recognise on your account.

Know who you're talking to.

If you've only met someone online or are unsure of the legitimacy of a business take some time to do a bit of research before continuing the conversation. Independently search for confirmation of the business or legitimate customer reviews. Scammers will try to tell you what to say to avoid flagging their activity with others. Don't be afraid to ask questions.

Keep your bank details secure.

- Protect your passwords and PIN by memorising them, never write them down or share them with anyone
- Keep all receipts in a safe place or destroy appropriately
- Always keep your cards in sight during a transaction and destroy all cards as they expire
- Choose passwords that would be difficult for others to guess, update them regularly and avoid using the same passwords across different accounts
- Never share your One Time Password (OTP) or Secure Code with anyone, including family and friends

If you are expecting a new card, cheque book or statement and it doesn't arrive in a reasonable amount of time, make sure you contact us immediately.

If the guidelines above are not followed, you may be liable for any unauthorised transactions. Liability for losses resulting from unauthorised transactions will be governed by the ePayments Code.

Protect your personal devices.

Never allow anyone to access your computer, tablet or mobile device, even remotely. Ensure you password protect your home WiFi, back up your content and update your security software regularly. Avoid using public computers or WiFi hotspots to access online banking or provide personal information.

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

If you are concerned about fraudulent activity on your account, have been contacted by someone claiming to have your information or your personal device has been infected with malicious software, please call us immediately on 13 11 82.

- Advise us as soon as possible so that we can act immediately to safeguard your accounts.
- Report the crime to your local police.
- Report online scams to the Cyber Issuing 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.
- For after-hours reporting of lost or stolen cards call People's Choice on 13 11 82.

There are also many support services that can help you through this time. Visit https://www.peopleschoice.com.au/help-and-support/fraud-and-scams to learn how to access confidential counselling services.

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 11 82**
or visit your nearest branch.

People's Choice Credit Union (People's Choice), a trading name of Heritage and People's Choice Ltd ABN 11 087 651 125, Australian Financial Service Licence 244310 and Australian Credit Licence 244310. In this document, People's Choice Credit Union is referred to as People's Choice.

BRC 8.6.223 V2-0524