

Fraud Guide

People's
Choice

Banking for life

Fraud protection.

Your
guide to
protecting
yourself
against
fraud.



People's Choice has a strong commitment to providing secure products and services. In this guide we've prepared some simple tips to help you protect your finances from the most common types of financial fraud.

Tips for your security

Ensure that personal information is kept safe and secure

- Change passwords often and do not use the same password for different services – alpha-numeric passwords can be selected
- Do not tell anyone your PIN or password. You can ask for your PINs and passwords to be changed if you feel that they may have been compromised
- Check your transactions often and let us know immediately if there are any transactions you do not recognise on your account.
- If you are expecting a new card, cheque book or statement and it doesn't arrive in a reasonable time, make sure you contact us immediately

Steps you can take if you are a victim of fraud

- Advise us as soon as you possibly can on 13 11 82 so that we can act immediately to safeguard your accounts
- Report the theft/crime to your local police
- Report online scams/crime to the Cyber Issue Reporting System via www.cyber.gov.au/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.

Cards

- Memorise your PIN. Never keep it recorded with your card or on your phone or other devices. This is very important as experience has shown these are very quickly guessed or located
- Don't disclose your PIN to anyone. If you think that your PIN may have become known to another person, you can change it by using the mobile banking app, through internet banking or at a People's Choice ATM
- Protect your PIN by placing your other hand over the keypad when you are entering your PIN at an ATM or using EFTPOS
- Keep all receipts in a safe place or destroy them appropriately
- Always keep your card in sight during any transaction
- Sign any new card immediately in ink and never allow other people to use it
- Try to be as discreet as possible when withdrawing cash
- Once your transaction is completed, make sure you take your card, cash and receipt with you. If you do not need your receipt, make sure you place it in the secure bin at the ATM
- Destroy all cards as they expire
- If you are travelling overseas and can be contacted by phone, provide your number to People's Choice before you leave
- Update to a chip-enabled Visa card for additional security and support when travelling overseas

Cheques

- Don't pre-sign cheques
- Don't give your cheque book to anyone
- Always use a pen rather than a pencil to write cheques
- Always cross cheques with 'not negotiable'
- If sending cheques through the mail, use a plain envelope instead of one with a window

Home banking and online shopping

- Keep your log in websites in a favourites or bookmark folder to reduce the risk of mistakes or deception
- Always type 'peopleschoice.com.au' in your Internet browser address bar when accessing Internet Banking
- Change your Internet Banking password if the computer you use has been infected with a virus or malicious software
- Always take precautions in public to ensure that your personal details are protected and log off the computer at the end of each session
- Always use secure sites that have a padlock icon at the bottom of the web browser
- Don't supply any account or card details unless you have initiated the transaction
- Be wary of banners, ads and pop-ups while surfing the Internet. Don't click on them no matter how enticing they may appear
- Use email confirmation for transfers in Internet Banking as added security

Phishing emails

Phishing emails are seemingly genuine requests from your financial institution to reconfirm your account details and/or password.

Alternatively, they can sometimes also be emails that pose to be from any authoritative body. These emails can sometimes be easy to spot, as they often have typing errors or grammatical mistakes.

If you receive a phishing email, do not respond and delete it immediately. Never click on any links or attachments as this may download a virus or take you to a 'ghost' website designed to install malicious software on your device.

Never supply account or card details by email – no trustworthy company will request this information in this unsecure way.



Viruses and spyware

Viruses and spyware are generally downloaded via hoax emails, websites, pop-up banners or data downloads. A 'keylogger' virus is often used to record passwords used on your computer to forward them to an unknown third party. To protect yourself against these you can:

- Install security measures on your devices including firewall, anti-virus and anti-spyware software
- Ensure your protective software is updated often and patches installed
- Change your passwords if you have had a virus on any device and have since had it cleaned

Identity fraud

Identity fraud is when someone 'steals' your identity and uses it to access your accounts or take out credit in your name. To protect yourself against identity fraud, you can:

- Carry as little personal information as possible
- Place a padlock or similar security device on your letterbox
- Carefully discard any communication that contains personal information
- Keep a list of items carried in your wallet that has personal information. That way, if your wallet is lost or stolen, you can notify institutions and the police

Scams

There are a number of scams promising large amounts of money if you perform a series of tasks. Usually, these scams are from foreign countries and always sound too good to be true.

These scams can be sent to you via post, email, phone or door knocking. They include offers such as:

- Goods that are waiting collection upon payment of delivery charge
- Opportunity to be part of an exclusive lottery through payment of an upfront fee
- Opportunity to participate in a 'skills' competition after payment of an upfront fee
- A postage payment to receive how-to-make-money information, lottery or horse-betting prediction systems and personalised horoscopes

Sales agent scam

This type of scam is when a job is advertised by email or by an employment website, providing an opportunity to earn a commission simply by getting payments for sales of goods to your personal account. Once received, victims are instructed to retain the commission and remit the remaining funds overseas. These funds are almost always the proceeds of fraud.

Over-payment scam

If you are selling goods online you may receive either a cheque or direct credit payment that is more than what you are selling the goods for, with a request to send the additional money back. The funds received are either from a counterfeit cheque or have been stolen from another party.

Without your knowledge you may be involved in the criminal offence of participating in money laundering. It is possible that people who agree to participate in money laundering activities may be prosecuted.

Skimming

This involves capturing card details when the card is swiped either through a secondary terminal or through a tampered with ATM or EFTPOS terminal. If for any reason you believe an ATM appears to have been tampered with, you should retrieve your card and advise the financial institution involved.

Contact us

If you think you have been the victim of fraud or would like further information about what to do if fraud happens to you, refer to our Accounts & Access Facilities Terms and Conditions brochure, or call us on 13 11 82.

People's Choice is here for all your financial needs.

We offer:

- Home loans
- Personal loans
- Savings and investments
- Credit and debit cards
- Transaction accounts
- Insurance
- Business banking
- Internet and phone banking
- Smartphone apps
- Contactless payments
- Foreign currency
- Fast Payments



SAMSUNG Pay



The details in this brochure are correct as at March 2022 and are subject to change.

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

Apple, the Apple logo and Apple Pay are trademarks of Apple Inc., registered in the U.S. and other countries. Android, Google Pay, and the Google Logo are trademarks of Google LLC. Samsung Pay is a trademark or registered trademark of Samsung Electronics Co., Ltd.

BRC 8.6.16 V5.1-0323

Call us on 13 11 82
peopleschoice.com.au

Banking for life