Fraud Guide

people's choice CREDIT UNION

Fraud Protection

A simple guide on how to protect yourself against fraud.

A simple guide on how to protect yourself against fraud

It seems like every day there are new reports of different scams and the costs to society of crimes like identity fraud. However there are easy things you can do to protect yourself and your finances.

To begin with, you can have faith in People's Choice Credit Union's commitment to providing secure products and services.

For example, we have a thorough member verification process and our website and home banking services; Internet Banking, Phone Banking and SMS Banking, employ the latest security to ensure your transactions are safe.

We've also prepared this guide to give you an idea of things to be aware of and simple tips to protect you from the most common types of financial fraud.

General security guidelines

- Ensure that personal information is kept safe and secure
- Change passwords regularly and do not use the same password for different services – alpha-numeric passwords can be selected
- Do not tell anyone your PIN or password. PINs and passwords can be changed upon request if you feel that they may have been compromised
- Check your transactions regularly and notify People's Choice immediately if there are any transactions you do not recognise
- If you are expecting a new card, cheque book or statement and it doesn't arrive in a reasonable time, contact People's Choice immediately

What to do if you are a victim of fraud?

- Advise People's Choice as soon as possible 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 Australian Cybercrime Online Reporting Network (ACORN) www.acorn.gov.au
- 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
- If you haven't received regular expected mail, check with the post office to ensure your mail has not been redirected

For after hours reporting of lost or stolen cards call People's Choice on 13 11 82.

Card fraud

- Memorise your PIN. Never keep it recorded with your card or on your telephone or computer, even if disguised. This is very important as experience has shown these are very quickly guessed or located
- Do not disclose your PIN to anyone. If you feel 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 selected People's Choice branches
- 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, ensure 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 mobile phone, provide your number to People's Choice
- Use a Travelex Cash Passport and update to a chip-enabled Visa card for additional security and support when travelling overseas

Cheques

- Never pre-sign cheques
- Don't give your cheque book to others
- 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/shopping

- Keep official log in websites in a favourites or bookmark folder to reduce the risk of mistakes or deception
- Always type 'peopleschoicecu.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 Internet cafes 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. Do not click on them no matter how enticing they may appear
- Use email confirmation for transfers in Internet Banking as added security

Phishing emails

These are seemingly legitimate requests from your financial institution to reconfirm your account details and/or password.

Alternatively, they may purport to be from any authoritative body. Often they contain typing errors or grammatical mistakes. Do not respond to any unsolicited email and delete them immediately. Never click on any link or attachments as this may download a virus or take you to a 'ghost' website designed to install malicious software on your computer.

Never supply account or card details by email – no reputable company will request information in this manner.

Viruses and spyware

Computer viruses and spyware are generally downloaded via hoax emails, websites, pop-up banners or data downloads from the Internet. 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:

- Install adequate security measures on your computer including firewall, anti-virus and anti-spyware software
- Ensure your protective software are updated regularly and patches installed as advised
- Change your online passwords if you have had a virus on your computer and have since had it cleaned

Identity fraud

This is when someone 'steals' your identity and uses it to access your accounts or take out credit in your name.

- Carry as little personal information as possible in case of loss or theft
- Place a padlock or similar security device on your letterbox to guard against theft
- Carefully dispose of any correspondence that contains personal information
- Keep a list of items carried in your wallet that has personal information. If your wallet is lost or stolen, you can act quickly to notify institutions and the police

Scams

There are a number of fraudulent schemes promising large sums of money, mostly from foreign countries if you perform a series of tasks as requested. They always sound too good to be true, and they are.

These scams can be from postal mail, email, telephone 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

Jobs are advertised from email or legitimate employment websites providing opportunities to earn a commission simply by receiving payments for sales of goods to your personal account. Once received, you will then be instructed to retain your 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 in excess of what you are selling, 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 Credit Union is one of Australia's largest credit unions.

We offer:

Home Loans
Personal Loans
Savings & Investments
Credit & Debit Cards
Transaction Accounts
Insurance
Financial Planning
Superannuation
Business Banking
Internet, Phone & SMS Banking
Smartphone Apps
Contactless Payments
Foreign Currency

Call us on 13 11 82, visit any branch or peopleschoicecu.com.au

Connect with us.

BRC 8.6.16 V1.6-1118