People First Bank

Scam and fraud awareness

Your guide to helping protect yourself against scams and fraud.

Scams are becoming harder to recognise

Scams are becoming more sophisticated and can affect anyone. Messages, calls, and offers may appear legitimate and can be difficult to distinguish from genuine communications. Scammers often rely on urgency, pressure, or emotional manipulation to encourage quick decisions.

Being targeted by a scam does not mean you've done something wrong. Scammers use tactics designed to catch people off guard, often at busy or stressful moments. Taking time to pause and consider a situation can help reduce the risk of financial loss.

How scammers manipulate people

- They create a sense of urgency or pressure
- They impersonate trusted organisations or people
- They exploit emotions such as fear, trust, or excitement
- They encourage secrecy or discourage checking.

Know the warning signs

Understanding common warning signs can help you recognise a scam and decide what to do next.

Stop

Say no, hang up or delete suspicious messages. Remember, scammers rely on creating a sense of urgency to pressure you into acting quickly. Take your time, trust your instincts and avoid giving out any personal information or money if you're unsure.

Check

Ensure the person you are dealing with is real. Scammers often pose as trusted organisations and may have some of your details. Contact organisations directly using official contact details you find yourself, verify investment offers through ASIC and confirm with family, friends or a professional before acting.

Protect

Act quickly if you are concerned you have been in contact with a scammer. Contact us immediately on 13 11 82 or visit your nearest branch. You can also help others by reporting scams to Scamwatch (www.scamwatch.gov.au) or the police (www.cyber.gov.au).

High-risk scams to watch for

Scammers use many tricks, but five common scam types are responsible for most financial losses in Australia.

Investment scams

Promises of high returns with little or no risk

Investment scams often appear professional and credible. Scammers may pose as investment advisers or financial institutions and advertise opportunities through social media, websites, apps or messaging services.

Common signs include:

- Unsolicited investment offers or trading opportunities
- Claims of guaranteed or unusually high returns
- Pressure to act quickly or keep the opportunity confidential
- Requests to invest using cryptocurrency or overseas accounts

What to do

- Take time to consider any offer — legitimate investments do not rely on urgency
- Verify the investment through ASIC's Investor Alert List
- Seek independent advice before investing
- Contact us before making any payment if you're unsure

Remote access scams

Requests to install software or "fix" your device

In remote access scams, criminals claim there is a problem with your computer, phone, or bank account. They may contact you unexpectedly or use pop-up messages that appear urgent or alarming.

Common signs include:

- Requests to install software or allow remote access
- Claims your device or account has been compromised
- Instructions to act immediately to avoid loss

What to do

- Do not install software or allow remote access
- Close the message or hang up the call
- Turn off your device and contact us immediately if access has already been given

Scams that rely on trust and urgency

Impersonation and phishing scams

Messages pretending to be from a trusted organisation

Scammers impersonate banks, government agencies, delivery services, or well-known businesses. Messages may look genuine and use official logos, language, or caller IDs. They may even have some of your personal information from various data breaches.

Common signs include:

- Urgent requests to verify details or make a payment
- Links or attachments asking you to log in
- Requests for passwords, verification codes, or personal information

What to do

- Do not click links or open attachments
- Use official contact details to verify the request
- Contact us if you're unsure or have shared information

Dating and romance scams

Online relationships that lead to money requests

Romance scams begin with online relationships that build trust over time. Scammers may avoid meeting in person and gradually introduce financial requests.

Common signs include:

- A relationship moves quickly or feels intense
- Requests for money, gifts, or investment opportunities
- Stories involving emergencies, travel issues, or financial hardship

What to do

- Be cautious of financial requests from online contacts
- Pause and talk to someone you trust
- Contact us before sending money or making payments

Transaction-based scams

Buying and selling scams

Scams on online marketplaces, social media and fake websites

These scams often occur when buying or selling goods online. Scammers may pose as buyers or sellers and use deceptive payment tactics to mislead and confuse.

Common signs include:

- Requests to receive and forward money
- Over-payments followed by refund requests
- Pressure to use unusual or insecure payment methods

What to do

- Use secure and trusted payment methods
- Stop the transaction if something feels wrong
- Contact us immediately if money has been sent

Fraud and unauthorised transactions

When unauthorised access to your information of accounts occurs

Fraud is different from a scam. Fraud occurs when someone gains access to your account or payment details and uses them without your authorisation. This may happen through stolen card details, compromised devices, or other unauthorised access.

If you notice a transaction you don't recognise, it's important to act quickly.

Common types of fraud

Card-not-present: Criminals steal card details for unauthorised purchases/withdrawals

Skimming: Card details captured from tampered ATMs or EFTPOS machines

Account takeover: Someone gains access to your account without permission

Unauthorised online payments – payments made without your consent

What to do if you notice an unauthorised transaction

Act quickly

- Contact us immediately so we can help secure your account on 13 11 82
- Stop or block cards and access if possible

Check your accounts

- Review recent transactions carefully
- Continue to monitor your accounts for unusual activity

Report the issue

- We'll guide you through the next steps and investigate the transaction
- In some cases, you may also be asked to report the matter to police

Remember, you are not expected to manage fraud on your own. If you act promptly and follow the steps above, we can help investigate unauthorised transactions and work to help you.

Keeping your accounts and devices secure

You don't need to be a technology expert to keep your accounts secure. A few simple habits can help reduce the risk of scams and unauthorised access.

Protect your bank details

- Keep your passwords and PINs private and never share them
- Use strong, unique passwords and avoid reusing them across accounts
- Enable two factor authentication (2FA) on your accounts
- Never share one-time passcodes (OTP) with anyone
- Check your account transactions regularly and report anything unusual

Keep your devices secure

- Keep your phone, tablet and computer updated with the latest software
- Use security features such as passcodes, biometrics or screen locks
- Avoid using public computers or Wi-Fi to access online banking
- Do not allow remote access to your device

Be cautious online

- Only access online banking through official websites or apps
- Be wary of links, pop-ups or attachments you weren't expecting
- Avoid clicking on ads or messages that create urgency or pressure
- Take time to verify unexpected requests before acting

If something doesn't feel right

Trust your instincts. Pausing and checking can help prevent issues before they occur. Acting early can help reduce the impact of scams or fraud.

Contact us on **13 11 82** if you're unsure about a message, call or transaction.

Steps to take if you've experienced a scam fraud or fraud event

If you're concerned you've been targeted by a scam or notice an unfamiliar transaction, or you suspect your personal device has been compromised, support is available. Acting fast is critical. Please call us immediately on 13 11 82.

- Advise us as soon as possible so we can act immediately to safeguard your accounts.
- Report the crime to your local police.
- Report scams and cybercrime through the Cyber Issuing Reporting System at 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 https://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 First Bank on 13 11 82.
- There are also many support services that can help you through this time. Please visit https://www.peoplefirstbank.com.au/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 First Bank, a trading name of Heritage and People's Choice Ltd ABN 11 087 651 125, Australian Financial Services Licence 244310 and Australian Credit Licence 244310.

13 11 82
peoplefirstbank.com.au

BRC 8.6.223 V3.0-0526