Staying Safe From Scams

Trust and security is a top priority for us at CommBank. We're seeing growing instances of customers who are pressured or tricked by scammers into sending them money. These scams can be sophisticated and come in various forms. It's important to keep an eye out and let us know if something doesn't feel right. To learn more about how to protect yourself and report a scam, check out **commbank.com.au/safe**.

Authentication and Verification

- Complete the security check-up in the CommBank app.
- Enable multi-factor authentication, which adds an additional check to prove your identity.
- Use **CallerCheck** to verify the identity of callers claiming to be from the bank.
- Use **CustomerCheck** in branch to verify yourself to our staff.
- **NameCheck** will prompt you if the account details on a first-time payment don't look right.

Device and Payment Security

- Keep anti-virus software up to date and protect your computer from common threats.
- Use secure payment methods like tapping or inserting your card.
- Don't share devices that have access to your digital wallet.

Password & Personal Information

- Never share passwords or PINs, and be cautious when sharing personal information.
- Never provide your NetCode to anyone, including CommBank staff.
- You can change your password in NetBank and the CommBank app at any time.
- Create strong passwords and change them regularly. For our tips on password creation, visit commbank.com.au/password-security.

Email, SMS and Online

- Don't click on links in suspicious emails or SMS.
- If you're unsure about a message, discuss it with someone you trust or contact the organisation directly via official contact details.
- Hang up on automated, suspicious or threatening phone calls from third parties.
- Be cautious of unknown contacts on social media and online platforms.

Stop. Check. Reject.

Stop. Does something seem off? If in doubt, the best thing to do is stop. Take a breath.
Check. Ask someone you trust or contact the organisation directly, using their official details.
Reject. Hang up on the caller, delete the email, block the phone number. Change your passwords.

If you believe you're a victim of a scam, contact CommBank immediately on **13 22 21**, or **+61 2 9999 3283** from overseas.

If English isn't your first language, the government's free Translating and Interpreter Service can help you to communicate with us. This service is available in over 150 languages. We can arrange this service when you call us or visit us in branch.

Commonwealth Bank

Published 01/06/2024

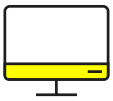
Important information about common scams

Investment (Including Crypto)

Scammers entice individuals with the promise of high returns, often involving crypto or other investment opportunities. Scammers may attempt to contact you via phone, email, or social media platforms.

Tips to protect yourself:

- If it sounds too good to be true, it probably is.
- Be cautious of unsolicited offers and pressure to invest or act quickly.
- Verify the legitimacy of the company or broker on the ASIC website first.



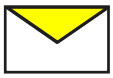
Remote Access

Where a scammer calls you and attempts to obtain access to your accounts or device, pretending to be from a trusted company or organisation.

Tips to protect yourself:

- Never download remote access software at the request or under pressure from a third-party caller.
- You can always call an organisation back on their legitimate contact details, found on their official website.
- If you receive a call claiming to be someone from CommBank, you can always ask us to verify the call via the in-app CallerCheck feature.

Business Email Compromise



Scammers can target businesses with emails from a compromised address, or emails made to look like they came from a trusted contact such as: your assistant, customer, lawyer, manager or supplier.

Tips to protect yourself:

- Before making first-time payments or a change of payment details, call the organisation on their official contact number to confirm the details first.
- Use the NameCheck feature when making payments, to see if the account name matches the BSB and account number given.
- Train employees to recognise and report phishing attempts.

Phishing and Smishing

Scammers use deceptive emails or text messages that might include a link directing you to a fraudulent website or ask for sensitive personal information.

Tips to protect yourself:

- Don’t click on links in suspicious emails or SMS.
- You can confirm the authenticity of a message by contacting the organisation directly, using their official contact methods available.
- Report any suspicious messages from CommBank to hoax@cba.com.au

Important information about common scams

Relationship

Scammers create fake profiles to form relationships and manipulate victims into sending money or personal information.

Tips to protect yourself:

- Never send money, or share passwords, credit card or account details with anyone you don't trust.
- Research your potential partner online via Google or social media apps. Try a reverse image search to identify if someone else owns the photos you've been sent.
- Speak to your family and friends about your online relationship. They may be able to offer perspective and identify warning signs that you may not have noticed.

Employment Opportunity

Where a job offer appears to require little to no effort for a high financial gain, or promises to make quick money.

Tips to protect yourself:

- Verify the company and offer through official channels, and do research on the company to ensure they are legitimate and currently trading.
- Be wary of job offers via social media, encrypted chat, email, phone or letter from people you haven't met or companies you don't know.
- A legitimate company would never require you to make an advance payment or use your personal banking information to facilitate company funds or trade.

Online Shopping

Scammers create online stores or ads to lure shoppers into purchasing non-existent or fake products.

Tips to protect yourself:

- Shop only on reputable and secure websites and be wary of any offer that seems too good to be true.
- Use secure payment methods and avoid direct transfers to sellers.
- Don't rush or be pressured by 'limited offers' or end of sale 'countdowns'.

Threat and Penalty

Scammers impersonate authorities or trusted organisations to extort money through threats of fines or legal action.

Tips to protect yourself:

- Hang up on threatening callers and contact the organisation directly.
- A legitimate organisation will never ask you to pay by unusual methods such as by gift or store cards, iTunes vouchers, wire transfers or Bitcoins.
- If you're concerned for your safety, contact the police assistance line.