Commonwealth Bank

Important information for customers about scams.

Dear Customer,

Trust and security is a priority for us.

From time to time, we see instances where a customer is under duress, coerced or manipulated by a third party into conducting a financial transaction. Occasionally perpetrators accompany a customer to a branch or provide instructions over the phone to ensure a financial transaction is completed.

These scams come in a number of forms and can be highly sophisticated. Customers should be vigilant and aware, and report any suspicious activity.

Warning signs and red flags.

Scammers often try to create a sense of urgency. They do this by pressuring customers with short deadlines, fake emergencies, threats of legal action or posing as a representative of the Police force, a bank or a Government department.

Types of scams.

Common scams include:

- information technology and remote access (to your computer, mobile or other electronic device)
- investment
- dating and romance
- unexpected money or winnings
- fake charities
- buying or selling
- jobs and employment
- threats and extortion
- other attempts to gain your personal information

We will never ask you for your PIN, password or NetBank SMS Code via telephone or email. If you receive any contact from someone claiming to be from CommBank asking for this information or anyone that you are not certain is genuine, do not proceed and call us to verify before taking any action.

Where to find out more.

There are a number of online resources with further education and information about current scams, including www.commbank.com.au/scams and www.scamwatch.gov.au

You can also search for 'Safe & Savvy' on the CommBank website for a copy of our guide designed to help older customers understand and avoid elder abuse, scams and fraud. If you need assistance in accessing any of the above resources, please visit any CommBank branch.

We're here to help.

If you identify unauthorised transactions or unusual conduct on your accounts, or need to confirm contact from CommBank is genuine you can call us anytime on **13 2221 (+61 2 9999 3283 from overseas)**, or **visit your local branch**.

You can also call the Bank's Scams Team on 1800 023 919. Select option 2, then option 1 (Monday to Friday 8am – 7pm, Saturday to Sunday 8am – 4pm Sydney time).

If you need emotional and psychological support please call our Customer Support Service on 1300 360 793 and make an appointment.
The Customer Support Service is a short term, confidential telephone counselling service which is available to Commonwealth Bank and Bankwest customers based in Australia.

Thanks
CommBank

For a summary of common scam types please see page 2.

Commonwealth Bank

Information Technology & Remote Access Scams.

You may:

- get a cold call from someone claiming to be from a financial institution, telecommunication company or IT helpdesk. They may already have your details.
- be asked to install a program or read out a specific code. This technique is often used to provide remote access so the scammer can see and control your device.
- be contacted to assist in catching criminals.

Investment & Job Scams.

You may:

- be offered investment products such as shares or cryptocurrency that guarantee a very good rate of return on your investment.
- be offered a work opportunity that sounds too good to be true. It may involve receiving funds from a business or their “customers” and transferring those funds onwards.
- be asked to recruit others into the job or investment.

Relationship Scams.

You may:

- have struck up a relationship with someone you met through online dating or social media who is now asking for money urgently.
- be asked to register for International Money Transfers (IMTs), and be instructed on how to send the money overseas. The IMT description may not match the intended recipient’s details.

Unexpected Money Scams.

You may:

- receive a letter, an email, call or pop-up on your computer about a lottery win, inheritance or similar.
- be told that you are entitled to money but that you must first pay to have the money released, e.g. legal fees.

Threat & Penalty Scams.

You may:

- be contacted by someone claiming to be Bank fraud staff, Police, Immigration, or the ATO.
- be told you have unpaid bills/fines or overdue taxes.
- be threatened with punishment such as gaol or deportation if you don’t make a payment.

False Invoice/Email Compromised Scams.

You may:

- receive a notice or invoice to pay an established supplier through a new account.
- receive notice from your supplier that they never received payment.

Buying/Selling.

You may:

- purchase goods online and but not receive the goods after paying.
- purchase a puppy/pet online but not receive the pet after paying.

Fake charities.

You may:

- be contacted by someone claiming to be from a charity or to need money to help a child who is ill.