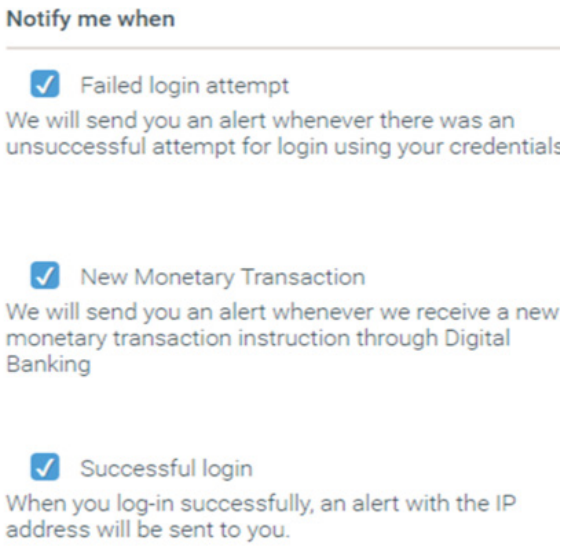
FAQ's CB - Online Banking Service

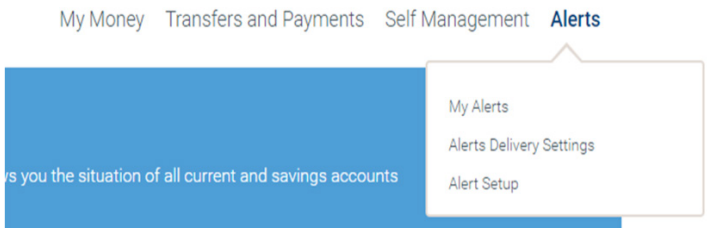
By working together we can keep your account safe and minimize financial services fraud.

Q1. What Security Does Commonwealth Bank Provide for online banking?

A1a. Security and Account Alert Set-Up on Online Banking



Customers have the ability to set up alerts once logged into their online banking to notify themselves via email or SMS text via cell phone when there is a failed login attempt, a new monetary transaction or a successful login.



An SMS is a Short Message Service that is the most widely used type of text messaging.

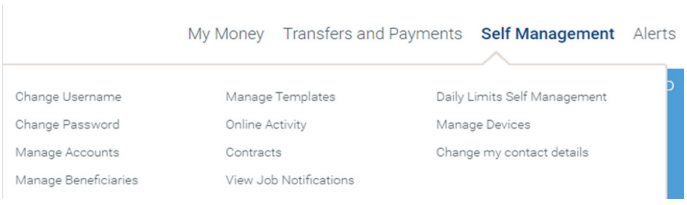
A1b. Multi-Factor Authentication functionality - One-time password sent via SMS

A one-time password (OTP), also known as one-time pin or dynamic password, is a password that is valid for only one login session or transaction, on a computer system or other digital device.

For every new monetary transaction, a new OTP will be sent to the cell phone on file via SMS. A customer that changes their cell number must visit a branch to update their account information to ensure that SMS texts via OTP are delivered to the account holder.

A1c. Self Management Feature on Online Banking

Customers have the ability to use our Self Management option once logged into their online banking to change username, password and many other features as shown below.



COMMONWEALTH BANK

FAQ's

CB - Online Banking Service

By working together we can keep your account safe and minimize financial services fraud.

Q1. What Security Does Commonwealth Bank Provide for online banking?

A1d. Challenge questions when calling Call Centre

A list of verification questions will be asked by the call service agent before proceeding with personal information.

Q2. Who do I contact if I feel that I have suspicious activity on my account or with my login credentials?

A2. Contact Commonwealth Bank Ltd by phone 5026159 option 2 or 4 or email **cbcyberfraud@combankltd.com**

Q3. Is it ok to send my personal and account information via email?

A3. No. Regular email is not secure. Never email personal information such as your account numbers, National identification numbers or passport information.

Q4. How can I avoid falling victim to a mystery shopping scam?

A4. Beware of Mystery Shopper Offers received from unknown parties.

DO YOUR RESEARCH. Most legitimate secret shopper jobs are posted online by reputable marketing research or merchandising companies.

NEVER WIRE MONEY TO SOMEONE YOU DON'T KNOW. Wiring money is the same as sending cash – once you send it, you can't get it back.

NEVER give your personal or financial information out online. Guard your personal information, and treat it as if it were cash.

COMMONWEALTH BANK

FAQ's CB - Online Banking Service

By working together we can keep your account safe and minimize financial services fraud.

Q5. What clues can I look out for in an email phishing message?

A5.
- General or missing greeting
- Suspicious links (URLs)
- Typos and grammar mistakes
- Incorrect or confusing message
- Messages that direct you to do something
- Email messages with missing recipient's address or aliased sender's address
- Logos inconsistent with authentic company logo

Q6. What measures can I take to further protect my personal information?

A6. Customers can choose to use the "Bookmark" feature for your frequently used secure websites to ensure authentic website launch and access.

Change your password periodically throughout the year.

Never share or write down your user name or password information.

Delete messages that: Ask for private information, Look suspicious. **Do not respond to any suspicious message or click on any links/attachments contained within one.**

If you have clicked on a link or opened an attachment, we advise you to go to your bank and change your account password/PIN immediately.

Q7. Who bares the liability if my account was hacked or compromised by cyber fraud?

A7. Subject to investigations, and further review/consultation with the relevant authorities (if necessary), customers can be held liable for initiating any transactions (i.e. Online Banking transfers, ABM withdrawals, Wire transfers, In-Branch transactions etc.), held responsible for repayment, and/or be subject to criminal prosecution.