Fact sheet: cyber security and protecting our customers

How we protect our customers

- Security of our customers' banking details is a top priority for the Commonwealth Bank.
- We invest in state of the art fraud prevention and detection technology and have a dedicated team who actively monitor unusual or suspicious activity.
- Another way we keep ahead of the curve is working closely with law enforcement agencies and other banks to share information and understand potential threats.
- We offer our customers the benefit of our 100% guarantee against fraud where they are not at fault.
- Where there is fraudulent activity, our process is to fully reimburse our customers.
- If a customer notices an unusual transaction on their account, they should contact us on 13 2221 immediately to report it.

Additional layers of protection

- NetCode SMS
  - Traditional authentication relies on 'something you know' such as a password or security questions.
  - Adding a second layer of security requiring 'something you have' such as a mobile phone protects customers from evolving online threats such as financial crimeware and identity theft.
  - As the NetCode SMS single-use password is sent directly to your mobile phone, cyber criminals are unable to authorise fraudulent transactions.
  - NetCode SMS is a highly effective yet convenient authentication system requiring single-use passwords to authorise certain NetBank activities and transactions.
  - The single-use password is sent to your mobile phone via an SMS message and only remains valid for 2 minutes.
  - A NetCode may be sent via CommBank app instead of SMS if you have installed and registered the CommBank app (on a compatible iOS or Android device) with notifications enabled.
- Spend alerts
  - Spend alerts are notifications customers receive on their phone instantly when they pay or are charged for something on their CommBank debit or credit card.
  - Spend alerts have helped our customers detect fraud 60% faster making it easier to recover lost funds.

How customers can protect themselves

- Customers should always be vigilant when it comes to protecting their banking details, but also interacting with people online that they do not know.
- Customers should never give their PIN, account details, or NetBank username and password to anyone.
- Likewise, they should only send money to people they know and trust.
- When we're made aware of a particular scam targeting Commonwealth Bank customers, we may post a warning on Facebook to help them stay vigilant.
- Scammers will often create a sense of urgency. They may try to test your better judgment by stating that something needs your immediate attention.
- Education is key. Read up on what to look out for, so you don't fall for it.

Tips to avoid potential security issues

- If you receive a telephone call from anyone claiming to be from your Bank be suspicious – banks do not contact customers asking for PIN, Password or confidential information.
- Banks do not email customers seeking personal information or account details. If customers receive these, contact your Bank.
- Do not click onto links in emails from people you don't know or trust.
- Regularly check statements for unauthorised and unusual transactions and report to your financial institution immediately.
- Always sign new cards upon receipt and destroy expired cards.
- Memorise your PIN and do not keep it with your card.
- Report lost and stolen cards, cheque and passbooks.
- Regularly check your PC's anti-virus and anti-spyware software to be sure it is on and up to date.
- Cover the PIN pad with your hand when using an ATM.
- You can find out more information, hints and advice on https://www.commbank.com.au/personal/support/security.html