Factsheet
Security Guidelines

Security Guidelines

We are committed to protecting our customers' money. This guide gives you a few ideas you can use to ensure your money remains as safe as possible.

Bank Australia will never

- send you unsolicited emails asking for information;
- ask you to tell us your PIN or personal banking details in an unsolicited email, SMS or telephone call;
- ask you to give us your full card number or security information; or
- ask you to click on a link in an email to log in to your account and verify your details.

It's your responsibility to

- ensure the security of your devices and passwords;
- update your personal details straight away if you've moved house or have a new number;
- contact us immediately if any payment options (card, cheque book, phone banking, internet banking, device) are compromised or there is a transaction you don't recognise on your account; and
- let us know of travel plans and if you will be contactable during your trip.

Online Safety

- use the information on Scam Watch and Stay Smart Online to stay informed about any online risks, such as phishing and scams;
- use social media with caution and be careful to not over-share your personal information; and
- don't click on links or enter any payment or personal details on an unsecured website.

Fraud prevention

- check your statements and contact us immediately if there is anything you don't recognise or understand;
- destroy statements and letters securely if you no longer need them;
- be aware of scams. Scammers may contact you via mail, email, SMS, telephone, online marketplaces like eBay, social media, or even door knocking;
- check your credit report at least once a year; and
- read any Terms and Conditions carefully before making any purchases.

Device security

- update devices regularly and run virus scans frequently;
- check the log-in information on the welcome page of internet banking – it contains the most recent activity completed with your log-in details;
- use websites and apps that you can trust;
- for security, turn on auto-lock (requiring a PIN/Password/Facial Recognition) and don't let others use your login credentials; and
- turn your auto-updates on to make sure you don't miss any security patches and bug-fixes.

Card security

- sign the signature panel as soon as you receive a new card and destroy your old card;
- use card controls to turn off any purchase options you don't need – you can use the Internet Banking and app controls to toggle these on and off as needed;
- don't let anyone else use your card or card details; and
- treat your card as if it were cash, and don't leave it unattended (e.g. in a car, at your workplace, or in a public place).

Password security

- don't choose a password that is easily identified with you, such as your name, date of birth or telephone number;
- never tell anyone else your PIN or access codes, including family, friends, police or Bank staff;
- make sure that no-one sees you enter your PIN or pass code;
- for personal security, avoid using dimly lit ATMs;
- notify Bank Australia immediately if you believe your PIN or codes become known to anyone else;
- don't provide banking details via open email, or via a link in an email – contact the merchant directly on their legitimate phone number if you are unsure;
- don't record details of your PIN or access codes on a hand-held device or computer;
- never use a terminal or ATM that doesn't look genuine, appears to have been modified or has a suspicious device attached;
- cover your hand when inputting your PIN; and
- if a merchant doesn't let you insert your chip card and enter your PIN, we encourage you to exercise caution.

Have any questions about the security of your account? Contact us on 132 888 or mail@bankaust.com.au. If you're overseas please call (03) 9854 4666. If you need to cancel your card after hours, use card controls or call 132 888 and follow the prompts.

Bank Australia Limited ABN 21 087 651 607 AFSL/Australian Credit Licence Number 238431.