

Personal Identification Number (PIN) Security

Protect your PIN as well as your card

- Keep your PIN secret from everyone – even family and friends.
- Never tell anyone else your PIN or let anyone see you enter your PIN when you use your card in an electronic terminal, such as an EFTPOS machine or ATM.
- Do not write your PIN on your card even if it is disguised.
- Memorise your PIN – if you must record your PIN, keep it separate from your card in a secure location and never keep it in a place where it is liable to be lost or stolen with your card, such as your wallet or handbag.
- Be suspicious if you receive a call from anyone requesting your PIN – bank staff will not call for this purpose.
- Never disclose your PIN to anyone over the phone and do not enter your PIN into a web page which has been accessed by a link from an email, even if the email appears to be from ME Bank.
- Destroy the letter provided by ME Bank containing your PIN after you have memorised it.

You should not disguise your PIN by recording it:

- as a phone number where no other phone numbers are recorded;
- as a four digit number, prefixed by a telephone or area code;
- as a date where no other dates are recorded;
- in reverse order; or
- as an easily understood code.

Call us on 1300 654 998 to report unauthorised use, loss or theft.

Notify us immediately if you discover that your card, customer ID, access code, password or PIN record has been lost, stolen or used by someone else, or that your access code, password or PIN may have become known to someone else.

If you do not notify us within a reasonable time you may be liable for losses which occur as a result of your delay.

Our Electronic Access Terms and Conditions set out in full the situations where you could be liable for unauthorised electronic transactions involving use of your card, customer ID, access code, password or PIN. Your liability for losses resulting from unauthorised electronic transactions will be determined under our Electronic Access Terms and Conditions (which reflect the liability under the EFT Code of Conduct) rather than these guidelines.

Our Electronic Access Terms and Conditions that apply to the use of your card and PIN, Internet Banking, Phone Banking and Operator Assisted Banking are available by calling us on **1300 654 998** or by visiting **mebank.com.au**

BE ALERT

Always report any unauthorised or suspicious transactions to **ME Bank** on **1300 654 998**

ME Bank Account Security

What you need to know...



Account Security

Transaction account usage

You should never:

- allow strangers to transact through your account for their own purposes;
- accept money in return for allowing others to transact through your account;
- sell your account to another person,

as you risk becoming involved in a criminal offence.

Internet, Phone and Operator Assisted Banking Security

Protect your security

- Safeguard your access code used for Internet and Phone Banking, as well as your password used for Operator Assisted Banking.
 - Choose an access code and password which is difficult to guess and not easily associated with you. Do not pick your date of birth, phone number or name.
- Do not share your customer ID, access code or password with anyone. Never disclose your customer ID, access code or password to anyone over the phone unless using Phone or Operator Assisted Banking. Do not enter your customer ID, access code or password into a web page which has been accessed by a link from an email, even if the email appears to be from ME Bank.
- Memorise your customer ID, access code and password. If you must record your customer ID, access code or password do not keep a record on the same document or on something liable to be lost or stolen.
- Change your access code regularly e.g. at least every 30 days.
- Never let anyone else see or hear you enter your customer ID, access code or password when using Internet, Phone or Operated Assisted Banking.
- Do not use Internet Banking on unfamiliar computers as they may not be protected with the latest anti-virus software.
- Check the time and date of your last log-in to Internet Banking are correct.
- When using Internet Banking, confirm that your data is encrypted by noting the lock symbol at the bottom

right-hand corner of the browser.

- Never leave your computer unattended while you are logged into Internet Banking and always log off as soon as you are finished.
- Close your internet browser after signing out at the end of each Internet Banking session.
- Make sure to hang up the phone when finished using Phone or Operator Assisted Banking.
- If you think someone has seen or heard your access code or password, you should change it as soon as possible.

Protect your computer

- Ensure you have the latest anti-virus and firewall protection on your computer and the software is updated regularly to keep it current.
- Download and install the most up-to-date security patches from your software vendor.
- Do not click on links or open email attachments from unknown sources.
- Scan your computer with anti-virus software at regular intervals.
- Delete spam and hoax emails.
- Clear cookies and old files on a regular basis and scan for viruses, worms, Trojans etc.
- When using independent sites over the internet ensure you are dealing with reputable companies.

The following companies provide online virus scanners, spyware protection, anti-virus software and/or firewalls:

- Spyware Doctor
- Trend Micro
- McAfee
- ZoneAlarm

Mobile Device Security

- Utilise the lock capability on your mobile device when it is not in use. This function helps to protect your device and details.
- Never disclose via email or text message your account number, customer ID, access code or password.
- Do not modify or hack into your mobile device as this can make your device susceptible to viruses, worms, Trojans etc. ME Bank recommends you install security software if available for your device.

Card Security

Help protect the security of your card

- Once you receive your card, immediately sign the signature strip on the back.
- When your card expires please destroy the card by cutting it in half diagonally.
- Do not record your card number or the Card Verification Value (CVV) code, which is the 3 or 4 digit code found on the back of your ME Bank MasterCard.
- Never let anyone else use your card.
- Protect your card from theft by keeping it in a safe place.
- Regularly check that you still have your card.
- Ensure that your card is handed back to you after use – not a different one.
- Treat your card like cash and keep it nearby.

Don't be a victim of card skimming!

Skimming is the unauthorised copying of information stored on the magnetic strip on the reverse of debit or credit cards, such as an ME Bank MasterCard. This information is transferred onto a cloned card, which is then used to make fraudulent transactions that are charged to the skimmed account. Industry experience has shown that skimming occurs more frequently when people are travelling overseas, however the incidence of skimming is increasing in Australia.

To safeguard yourself against card skimming, ME Bank recommends that you follow the simple steps listed below.

- Never leave your card unprotected from unauthorised access.
- If possible, don't let anyone walk out of your sight to process a transaction.
- Always watch your card being swiped through a card terminal – this should only occur once per transaction.
- If a transaction fails or is cancelled ask to see the cancellation receipt.
- Look out for unusual devices – an illegal device may be hand-held or stored near the legitimate card terminal at a retail counter.
- Keep all purchase receipts.
- Check all transactions on your statements.