Get the last laugh on the fraudsters.

Account security tips

Safety 101 – protecting your money.

Lock it down.

It's important to keep your account info secure. Anything that could give other people access to your account puts your hard earned money at risk. If you smell something fishy, get ME on the case. Report any unauthorised or suspicious transactions on **13 15 63**.

Keep it hands off.

Never let anyone else use your account. Along with possible theft, you risk your account being used for illegal purposes, which may implicate you in a criminal offence (imagine explaining that to your friends).

Visit ME regularly.

Get into the habit of checking your account regularly via internet or mobile banking – that way you'll catch any suspicious activity sooner rather than later.

Keep it between you and ME.

Your access code for internet and phone banking and password for operator assisted banking are like the keys to your digital bank vault – keep them safe.

- Keep your customer ID, access code and password to yourself. Don't share them with anyone. That includes close family or a friend – not even a really, really good friend.
- Choose a password that is hard to guess – that means birthdays are out. The same goes for addresses, phone numbers, names or an alphabetical password that is a recognisable part of your name.
- It's best to memorise your customer ID, access code and password. If you have to write these details down, don't keep a record on the same document or on something that could be lost or stolen.
- Never let anyone else see or hear you enter your customer ID, access code or password when using internet, phone or operator assisted banking.

See **mebank.com.au/security** for more information on password and access code security.

Play it safe around internet banking.

- Make sure the lock symbol is showing in your browser while you're using internet banking.
- Log out as soon as you're finished.
- Keep your anti-virus software up to date, and do virus scans regularly. Don't log in on public computers as they may not be protected with the latest anti-virus software.
- If you do decide to use a public computer, close your browser after you sign out. Don't click on links or open email attachments from unknown sources.
- Never enter your PIN, password, card details or personal details into a web page that you reached by either clicking on a link or a pop up window that has appeared on your screen.

Keep fraud off the cards.

A few simple steps will protect your card from fraud:

- When you get your card, autograph the signature strip on the back, pronto.
- Don't record your card number or the Card Verification Value (CVV) code (the 3 or 4 digit code found on the back of your card).
- Never let anyone else use your card.
- Keep your card in a safe place – the cookie jar is not a safe place.
- When your card expires, destroy it by cutting it in half diagonally a few times, making sure you cut through the chip.
- Check that you have your card regularly – the checkout is a good place to make sure you do.

Keep it private.

Your PIN is important – keep it to yourself:

- Keep your PIN secret from everyone. You guessed it. That means family and friends too.
- When you're entering your PIN into a keypad, make sure no one can see you enter it.
- Memorise your PIN – if you have to write it down, put it somewhere separate to your card, so they can't be stolen together.
- Don't write your PIN on your card, even if it is disguised.
- Don't reveal your PIN to anyone over the phone (bank staff will never ask you for your PIN).
- Never enter your PIN into a webpage that you reach using a link via email, no matter how legitimate the site looks.
- You shouldn't disclose 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. Fraudsters will spot those a mile away.

See **mebank.com.au/security** for more tips on PIN security.

Lock up your phones and tablets.

Smartphones and tablets can be easy for other people to get access to, so it's worth taking some extra precautions:

- Lock your devices when you're not using them – if criminals don't get into them, the kids will.
- Don't let your devices 'remember' user names and passwords for your banking accounts.
- Never disclose your customer ID, card details, personal details, PIN, access number or password via email or text message.

See **mebank.com.au/security** for more information on keeping your account secure while using internet banking.

Cheque your pockets.

Tips to keep them safe.

- Keep your cheque books in a safe place where no one can access them.
- Never pre-sign cheques.
- Always write your cheques with a pen – not a pencil.
- If posting a cheque use a plain envelope – not one with a window.

Get ME on the case.

Report unauthorised use, loss or theft ASAP – call ME on 13 15 63.

Contact 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. This includes if your mobile phone is lost or stolen (SMS is used for additional security).

If you don't 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 reflects liability under the ePayments Code) rather than these guidelines.

You can get a copy of our Electronic Access Terms and Conditions by calling us on **13 15 63** or by visiting **mebank.com.au**

ME Bank – a division of Bank of Queensland Limited ABN 32 009 656 740 AFSL and Australian Credit Licence Number 244616. ME0026.v16/202202/214059