MACQUARIE

Security measures

to help protect your online banking

macquarie.com

While the internet offers enormous advantages and opportunities, it also presents various risks. At Macquarie, we make every effort to assist in protecting your banking and personal information.

To help deliver secure online banking services, Active Banking password tokens are just one of the mechanisms that are used to help keep your accounts safe. An Active Banking password token provides an extra level of security when authorising transactions and/or accessing Active Banking. In addition to our Active Banking password tokens, secure login passwords are also issued to access online banking, which provides a high level of protection for your online accounts.

The more you know about potential risks, the better you can protect your online accounts from fraud.

Before you start using Active Banking, take a few minutes to familiarise yourself with the following.

Security tips

In addition to our security measures, you also have a role to play in ensuring your security is not compromised.

How to protect yourself when using Active Banking

- Always access Active Banking by typing the full web address **macquarie.com/activebanking** into your browser
- When using Active Banking check for the locked padlock symbol
- Never disclose your Macquarie Access Code (MAC) and/or password details to anyone. Disclosing your MAC and password details is in direct breach of the Active Banking Online Terms and Conditions.
- Regularly reconcile your account statements, checking for any transactions that look suspicious. If you suspect anything, report it to us immediately
- Always select ‘Log out’ from the Active Banking menu when you complete your session
- Close your internet browser after logging out at the end of each Active Banking session
- Avoid using public computers (eg internet cafés) as harmful spyware may be installed and anti-virus protection may be inadequate
- Beware of any windows that ‘pop up’ while you are using Active Banking, in particular those that direct you to another website, which then asks for your MAC and password.

Security tips

If you have an Active Banking password token:

- ensure your Active Banking password token is kept in a safe place
- never disclose your token PIN to anyone
- never store your MAC or token PIN with your Active Banking password token.

If you do not have a password token (for non transactional users of Active Banking):

- ensure you change your login password on a regular basis and ensure that it:
  1. contains at least one (1) numeric character
  2. contains at least two (2) alphabetic characters
  3. does not contain more than five (5) repeated characters
  4. does not contain any spaces, apostrophes or symbols
  5. is at least six (6) characters long
  6. is no longer than eight (8) characters long
  7. is not the same as any of your last six (6) passwords
- ensure your password is unique and is not related to your name, a birth date, telephone number or anything easily associated with you
- never disclose your login password to anyone.

Security tips

* How to treat suspicious emails

- Never click on a link in an email which re-directs you to the Active Banking login page
- Be wary of any emails you receive from people you don't know or trust
- Delete, preferably without opening, any emails you think are suspicious
- Delete the email from your 'Inbox' and then delete it again from your 'Deleted' and 'Sent' folders, if you have forwarded the email to anyone
- Macquarie will never ask you for personal information via email. If you receive an email claiming to be from Macquarie requesting your personal information, please do not respond to it. Forward the email to Macquarie at **report_scams@macquarie.com**.

* How to protect your PC

- Keep your computer secure by installing and regularly updating effective anti-spyware, anti-virus software and firewall protection.

Frequently asked questions

What is an Active Banking password token?

An Active Banking password token is an easy to use, numeric keypad device which can be used for authentication when logging in and must be used to authorise transactions in Active Banking.

What is a one-time password?

When the Active Banking token PIN is entered into the password token, a one-time password is generated. This numeric password is eight digits long and is different each time. The password will expire after a set amount of time. If this happens a new one-time password will need to be generated.

What if the one-time password is not accepted?

If the one-time password is not accepted, generate another one-time password by turning the Active Banking password token off, and back on again. If the one-time password is not accepted after three attempts, please contact us on 1800 620 673, Monday to Friday from 8.30am to 6.30pm (AEST/AEDT) or +61 2 8245 4177, if calling from overseas.

What will happen if I enter an incorrect token PIN into the Active Banking password token?

The Active Banking password token has been configured to lock itself after seven consecutive incorrect token PINs have been entered. The Active Banking password token will display a fail message when an incorrect token PIN has been entered.

If your Active Banking password token has been locked, please contact us.

Frequently asked questions

What is a login password?

A login password is issued to all Active Banking users. To access your accounts online, you will need your login password along with your MAC.
To keep your accounts safe, you should not disclose your password to others and you should change it regularly.

How do I change my login password?

You can change your login password in Active Banking using the 'Change Password' option under 'My Details and Preferences'.

Any problems?

If you experience difficulties with Active Banking, please contact us.

If you are calling from:
Australia: 1800 620 673 Monday to Friday
from 8.30am to 6.30pm (AEST/AEDT)
Overseas: +61 2 8245 4177

More information is available in the Help section of Active Banking. To access Help, login to Active Banking and select the link to Help. Alternatively navigate to macquarie.com/activebanking/help

For more information about internet security

To find out more about internet security and other useful information relating to online fraud, visit these websites:

- The Australian Securities and Investments Commission **moneysmart.gov.au**
- The Australian Bankers' Association **bankers.asn.au**
- The Australian Competition and Consumer Commission **accc.gov.au**
- SCAMwatch **scamwatch.gov.au**

Need help?

If you feel that the security of your computer or access to Active Banking has been compromised, or you have concerns or are suspicious about a transaction on your account, please contact Client Support immediately on **1800 620 673**.

macquarie.com/business

This material has been prepared by Macquarie Bank Limited ABN 46 008 583 542 AFSL & Australian Credit Licence 237502 (“Macquarie”) for general discussion purposes only, without taking into account your personal objectives, financial situation or needs. Before acting on this general information, you must consider its appropriateness having regard to your own objectives, financial situation and needs. The information provided is not intended to replace or serve as a substitute for any accounting, tax or other professional advice, consultation or service.