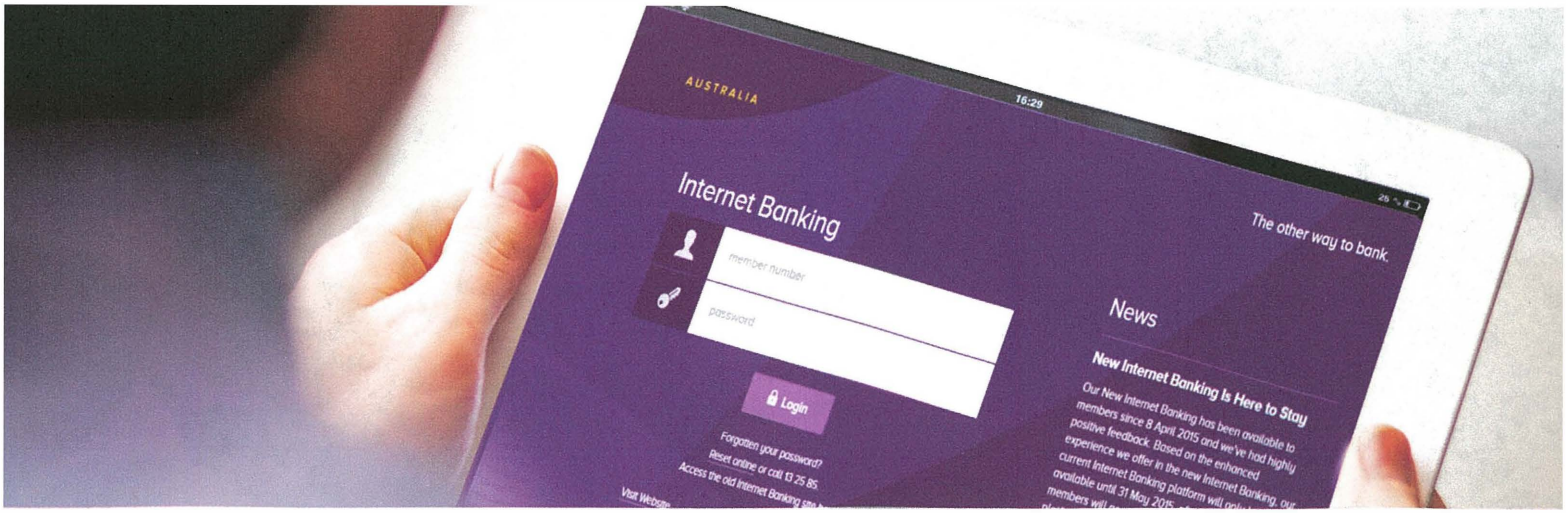

Smart ways to keep your money safe.

At Beyond Bank we use state-of-the-art technology and systems to keep your money safe. But there are a number of things you can do to keep your assets even more secure.

Card security.

- Always sign your card when you receive it.
- Never lend your cards to anyone else including family members or friends.
- Try to memorise your Personal Identification Number (PIN) and never write down and keep your PIN in obvious places such as your wallet or handbag, near your telephone, or on your computer terminal.
- When you change your PIN do not choose a PIN or code which is easily identified with you such as your birth date, telephone number, your account number, or an obvious combination of letters and numbers which can be easily guessed by someone else.
- Cover your PIN when entering it at any ATM.
- Be wary when using an ATM if it appears to have been tampered with or is unusual.
- Notify us immediately if you become aware that your card has been lost or stolen or used by someone else.
- Change PIN and passwords regularly.
- Check your EFTPOS receipts for any irregularities or inconsistencies.
- Check your account statements regularly and be aware of your balance.
- Destroy your card on the expiry date by cutting through the chip and magnetic strip, and disposing of it safely.

Online security.

Logging in online is an everyday occurrence and it's easy to become complacent. But when it comes to internet banking, here are some things you can do to keep aware.

- Maintain an adequate level of antivirus software on your computer.
- Delete any email or attachment if it seems suspect – it may be a virus!
- Beware of emails with 'friendly' headings from addresses you don't recognise.
- Set your spam email filter as high as possible.

We will never send you unsolicited emails requesting password or security information. If you ever receive an unsolicited email claiming to be from us or another financial institution requesting that you click on a link or provide personal information, it may be a scam so check with us before you respond.

Mobile and landline telephone security.

Fraudsters have developed a technique to intercept the one-time passcodes sent to mobile and occasionally landline numbers via SMS to authenticate transactions processed through internet banking and other channels.

This involves transferring your mobile phone or your landline to another provider without your knowledge ('porting') or creating a redirection. They can then intercept the SMS code we send you to authenticate a transaction to conduct fraudulent transactions on your account.

If you notice that your mobile or landline phone has unexpectedly stopped working, contact your provider immediately to confirm why your service has stopped. If you're mobile number or landline has been ported or redirected to another telephone number of which you are not associated with, contact us immediately so we can protect your account against fraud.