

Security

Protect your identity and financial details:

- Do not disclose personal or banking information to any unauthorised person.
- If you receive correspondence, email, SMS or a phone call from your financial provider that appears to be valid, and you are requested to take action, then be cautious. It could be a hoax. Contact your financial provider and confirm its validity first before responding.
- Ensure your loan provider has your current contact details.
- Record important contact and account details in a secure place - not in your wallet or purse.
- Notify your loan provider if you suspect missing mail and ensure your letterbox is locked at all times.
- Don't leave documents with your personal information lying around the home or office (such as invoices, tax file records, registration papers, licenses and the like).
- Always check your account and statements for suspicious transactions.
- Destroy personal documents before discarding in the rubbish.
- Do not give your credit card or credit card details to any unauthorised person.
- Maintain up-to-date anti-virus software and regular operating system updates on your computer.
- Never allow strangers to make transactions through your account for their own personal uses.

Protect your passwords / PINs:

- Do not record your passwords or PIN details on your computer.
- Do not give these details to any unauthorised person.
- Store your passwords and debit cards securely - and not together.
- Keep your card in sight when using it and report a stolen card immediately to 1300 530 466.
- Change your passwords and PINs regularly and do not use the same details for all your passwords.
- Do not use personal details for your passwords, such as phone numbers, birth dates, postcodes, or repeat / consecutive number sequences.



