Your security and you.

With security becoming more important than ever we've put together these simple guidelines to help you and your information stay safe. These tips don't just apply to banking but to any situation where your personal information could be at risk.

Keeping your card safe.

Always take steps to ensure your Visa Debit or rediCARD are secure to protect yourself from unauthorised card access.

- Never lend your card to anyone or disclose your PIN.
- Never give your card number to cold callers asking for card details over the phone.
- Never keep your PIN in an obvious place.
- Choose a unique PIN and don't reuse old or existing PINs.
- Make note of when new and replacement cards may arrive. Call us if they don't arrive on time.

We're monitoring your card 24 hours, seven days a week for data protection purposes. Our card monitoring system provides you with early detection of suspicious card activity, and in some cases may block cards until we can verify the detected activity with you.

Our top overseas travel security tip.

If travelling overseas let us know your travel details before leaving. Card fraud can happen anywhere, so be vigilant when transacting overseas and make sure we have your contact number(s).

Internet Banking securely

Use this guide to create stronger passwords and bank securely online:

- Create passwords using eight character or more upper and lower case letter, numbers and special characters.
- Never share passwords with anyone. Even close family or friends.
- Change your passwords at least every six months, or anytime you suspect your password has been compromised.
- Always access Internet Banking via our official website or mobile apps. We will never send you a link via email to access your accounts.
- Avoid accessing your Internet Banking on public computers or over public Wi-Fi networks.
- Always check login times and dates; if you see any inconsistencies tell us immediately.
- Install antivirus, anti-spyware and firewall software on your computer and mobile devices and keep them up-to-date.

Securing your smartphone

Follow these simple guidelines to protect your personal information on your mobile device:

- Always set your smartphone to auto-lock after inactivity, and use PIN, password or fingerprint protection.
- Don't use Internet Banking via unsecured and public Wi-Fi networks.
- Don't use the same PIN that you use for your card to access Internet Banking.
- Don't share your Internet Banking PIN.
- Ensure SMS codes are kept secret and secure.
- Ensure your operating systems and apps are up-to-date.
- If you lose your phone, block your SIM card immediately.

ROCK

Protecting your identity

As technology becomes more advanced, so do the techniques used by scammers and fraudsters. Take the steps below to make sure you are being as secure as possible.

- Never give your personal information to someone you don't know or trust.
- Your bin is a goldmine of personal information, shred or destroy personal or financial information such as bank statements or bills before binning. If filing personal documents, make sure they are kept in a secure place.
- Secure your letterbox with a lock, and follow up if you do not receive your regular expected mail.
- Keep your contact information with us current so we can contact you if we notice unusual activity.
- If you think you have come into contact with a scammer or believe you're a victim of fraud or a scam, call us as soon as possible.

Identifying scams at home

Email scams are now common. We'll never send you an email asking to confirm any personal or banking details or to reset your password. Never click links or attachments contained within our emails and always log onto Internet Banking manually through your browser.

- Be cautious when you receive unsolicited phone calls. Scams offering to 'fix' your computer and other scams are also on the rise.
- Never give your log on details or account access to another person.
- Never give a stranger remote access to your computer.
- Never provide your SMS verification code to another person, or verify an unknown Internet Banking transfer using an SMS code.
- Be wary of emails from email addresses that you don't know or trust.
- Never provide your personal or security details in response to an email or phone call. We never request this information from you via email or over the phone.

Secure social networking

Be aware of information you share online via social networking websites and wary of anyone asking for your personal information on these networks. Follow these simple rules and learn how your social media platforms handle your personal information:

- Don't use social networking sites without any privacy settings, or that allow anonymous user contact.
- Always protect social media accounts with strong passwords.
- Familiarise yourself with privacy settings to only share your information with people you want to share it with.
- Be selective when accepting friend requests. If you don't know the person, don't accept their request.
- Be wary of showing personal details (date of birth, phone number, contact details, etc.) on your social profiles and avoid posting pictures online that may give away personal information.
- Be careful if sending money overseas, particularly if its to someone new that you've just met online.

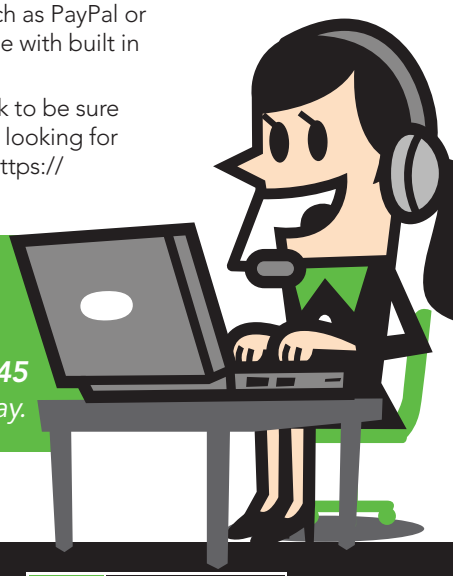
Shopping safely online

Be aware that every online purchase is an opportunity for people to access your information.

- If a website seems slightly suspicious don't make your purchase.
- Personal information is like money, value it and protect it when shopping online.
- Use safe payment options such as PayPal or your Visa Debit card that come with built in consumer protection.
- Protect your money and check to be sure the site is security enabled by looking for web addresses starting with https://

Need to change your details immediately?

Call us on 1800 806 645 *and we'll do it right away.*



ROCK