AUSTRALIAN BANKERS' ASSOCIATION INC.
Strong banks – strong Australia

Level 3, 56 Pitt Street
Sydney NSW 2000
Australia
+61 2 8298 0417
@austbankers
bankers.asn.au

Security and fraud prevention

Banks have sophisticated fraud prevention and detection systems in place to help protect customers. At the same time, there are some simple things you can do to help keep your personal and financial information secure.

Internet banking

Customers who bank online should be aware of methods used by criminals to trick people into revealing personal and confidential information.

'Phishing' emails claim to be from a bank or another legitimate business and ask for confidential information, but links within the email may take you to fake websites, which can attempt to capture your personal information.

One of the easiest ways to spot a phishing email is to see whether it uses your proper name. Most phishing emails are sent out en masse to thousands of recipients, so won't use your name. They'll also often contain typing errors and grammatical mistakes, even if they include the banks' registered logos.

Tips to prevent fraud

- Never provide personal details, including customer ID or passwords, in response to an email. A bank will never ask you for your password.
- Always access your bank's website by typing the address into the browser and not by clicking on a link in an email.
- Make sure your computer is up to date with anti-virus and firewall software.
- Avoid using passwords or PINs that relate to you personally (e.g your date of birth) and memorise it instead of writing it down.
- Always log out from the internet banking menu when you finish and close your browser after logging out.

Mobile banking

- Ensure your mobile is password protected and automatically locks when not in use.
- Clear your mobile of text messages from banks especially before sharing, discarding or selling your device.
- Be careful what you send via text – never use text messages to disclose account numbers, passwords or other personal information which could be used to steal your identity.
- Contact your bank if you lose your smartphone or tablet, especially if your bank uses an SMS message to authenticate transactions.

Using ATMs

- Check for attached devices on the ATM – if you encounter difficulty inserting your card this could be an indicator that the ATM has been tampered with.
- Check for any notable visible marks or changes on the ATM.
- Cover the key pad with your spare hand when entering your PIN.

Strong banks – strong Australia

Ongoing phone scam

We are aware of a telephone scam that uses the Australian Bankers' Association's name (or a variation of the name) in an attempt to defraud bank customers.

Scammers are calling households across the country asking about bank satisfaction to try and get people to reveal personal and financial information.

The ABA does not conduct customer satisfaction surveys. Do not provide any information to these callers. If you have provided details to these callers, such as who you bank with or your name and date of birth, alert your bank immediately. Your bank may be able to put a note on your account and monitor it for suspicious activity.

A similar scam involves callers claiming to be from the ABA and telling people they can visit a post office to pick up unclaimed money they are owed.

The scammers then try to talk people into sending 'refund service fees' via the post or money transfer outlets, and attempt to obtain victims' credit card details or drivers' licence numbers.

The ABA never calls members of the public about unclaimed monies. If you receive a call from someone that tries to perpetrate this scam, hang up immediately.