



Message

NAB-branded phishing messages

NAB is aware of current phishing messages sent by email and SMS which may appear to come from NAB.

The messages may state that your account has been suspended, ask you to verify your information, or offer you a reward for completing a survey. They then direct you to click on a link to provide personal and banking information. Please see two examples below.

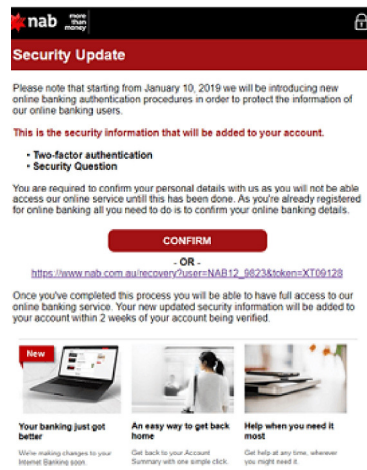
If you receive this type of message, forward it to hoax@nab.com.au, and then delete the message without clicking on any links. You can also report suspicious text messages by forwarding them to 0476 220 003 (047 NAB 0003) and then deleting.

NAB will never ask you to confirm, update or disclose personal or banking information via email or text message.

If you have received an email or text message of this type and have clicked on the link, please contact your local branch or call 13 22 65 immediately.

For more security advice, and to see the latest security alerts, please visit the NAB Cyber Safety Hub at nab.com.au/security.

From: Nab Bank <diglorevolution@xiamamymail.com>
Date: 10 January 2019 at 3:55:02 pm AEDT
To:
Subject: Account activity - #ELEL1154-AU



Your Nab account has been blocked for unusual activity. Please log on to: www.nablocked.com and follow the unlock procedure or visit our nearest branch.

Date: 25/01/19 08:48 Subject: NAB-branded phishing messages Reference: SB352036859

Delete Reply Return to list