GET ONE STEP AHEAD OF SCAMMERS



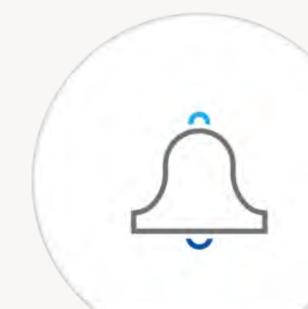


Be scam-savvy

Learn how to spot fraudulent activity and ways to protect yourself from common scams.

Scammers and fraudsters are advancing in ways to steal your personal information and access your banking details to make unauthorised transactions.

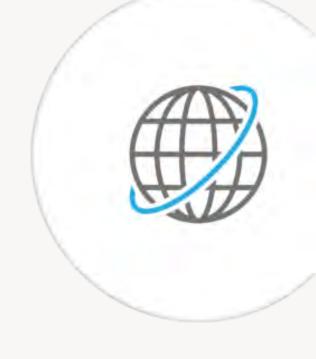
HOW TO LOOK OUT FOR SCAMS:



They can use fake email addresses and domains that look similar to official organisations to

Scammers can make messages appear legitimate and urgent.

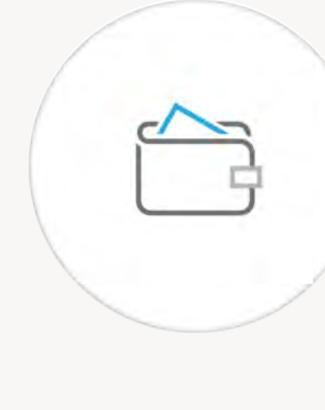
- convince you that they're real (e.g. impersonating your bank, courier, boss or IT department). Scammers are experts at faking urgent scenarios to rush you into responding. Stop for a
- moment to think before parting with any money or information.



If you can't confirm the sender, don't click on any links or attachments sent to your email

The message contains an unsecure website link or attachments.

or via text message. Verify the sender by contacting the organisation on their official number.



If the offer is too good to be true, it most likely is. Scams include the offers such as expensive

The offers are just too good to be true.

gifts, vouchers or unrealistic discounts to tempt you and drive impulsivity (e.g. free trials, flash sale, or out-of-the-blue lottery win).

The bank will never...

such as username, PIN or passwords.

personal or account information,

Call and ask you to provide

link to your online banking.

Email or text you with a direct login

reason.

Ask you to move funds to another

account to keep it safe from

hackers.

Ask to share remote access to your

devices or download software for any

Send you a direct message on social

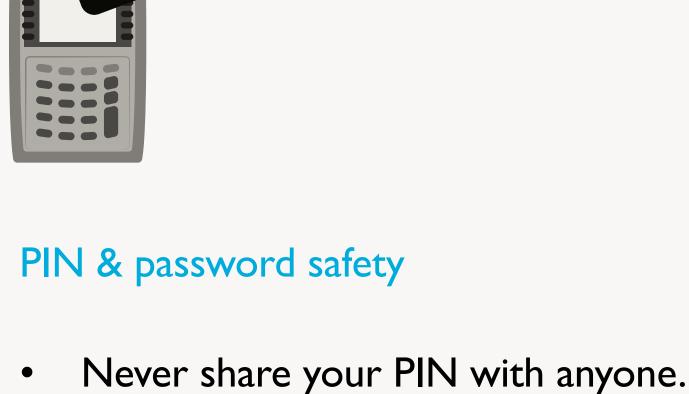
media or messaging apps.

pick up cards or cash.

Visit your house or send a courier to

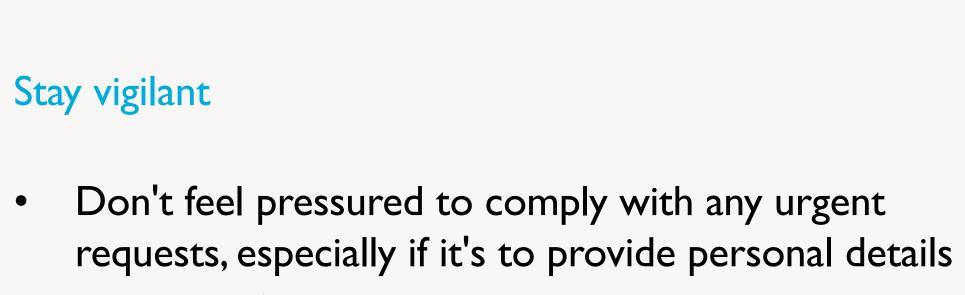
scams by using the tips below to secure your banking details and personal information. KEEP YOUR BANKING ACTIVITY SECURE

Protect yourself and your loved ones from fraudulent activity. Avoid



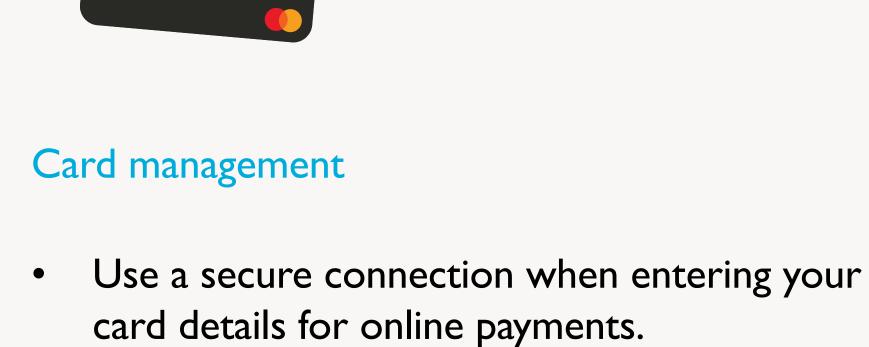
Use a unique password for each of your online accounts by including a combination of characters

- and symbols or a phrase.

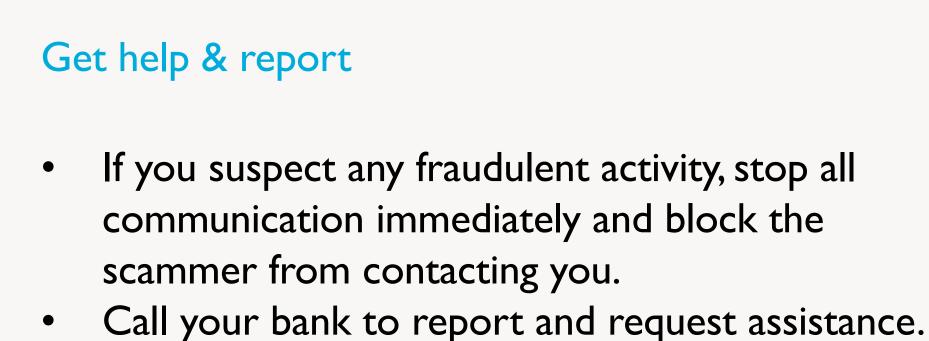


or payments. Bank staff will never ask you for your online password or PIN.

account information safe.



Never save your card or login details with an auto-fill setting on any browser.



- Safeguarding your banking information is a top priority. BRED Bank Fiji applies a number of security measures to keep your finances and

HOW BRED BANK FIJI PROTECTS YOU: Two-factor authentication (2FA)

BRED Bank Fiji uses two steps of authentication with security questions, images or phrases. This extra security layer ensures only authorised users can access your internet banking and make transactions.



Notifications or text alerts

payments. BRED Bank Fiji will send this code via SMS.

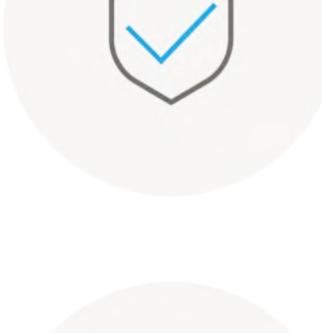
Enable notifications for your banking app or opt to use a digital security code for online



BRED Bank Fiji prevents your sensitive data from being intercepted by using end-to-end encryption. This can be identified in browsers with https://> and password-protected

Encryption

statements.



Firewalls are used to protect a bank's server from cyberattacks. In online banking, firewalls act as a barrier between your device and internet connection to protect your data from

Firewalls

unauthorised access.



Automatic time-outs After your internet banking session remains idle for a few minutes, this system will

automatically log out from your account to prevent unauthorised access.



Suspect fraudulent activity?

Call BRED Bank Fiji E-Channels 24/7 immediately at 323 0218 or

report to the authorities should you suspect any fraudulent activity.