Inconsistent Communication:
Scammers' stories may have inconsistencies or grammatical errors.

Verification with Official Source:
If contacted about suspicious activity on your mobile wallet account, contact your mobile money provider directly through their official customer service channels (phone number or website listed on their app or official communications) to verify the information.

ADDITIONAL TIPS:

Enable two-factor authentication (2FA):
This adds an extra layer of security to your accounts by requiring a second verification code in addition to your password.

Be cautious on social media:
Don't share personal information or financial details publicly on social media platforms.

Keep software updated:
Regularly update your mobile phone's operating system and mobile wallet apps to ensure you have the latest security patches.

Report suspicious activity:
If you suspect a scam attempt, report it to your mobile money provider and the relevant authorities.

Mobile money wallets and digital finance make shopping and managing finances incredibly easy, offering the convenience of transactions from anywhere, anytime. However, prioritizing your security is essential. By following key safety tips and staying informed about secure practices, you can protect your financial data while enjoying the quick and efficient benefits of online shopping and mobile finance.

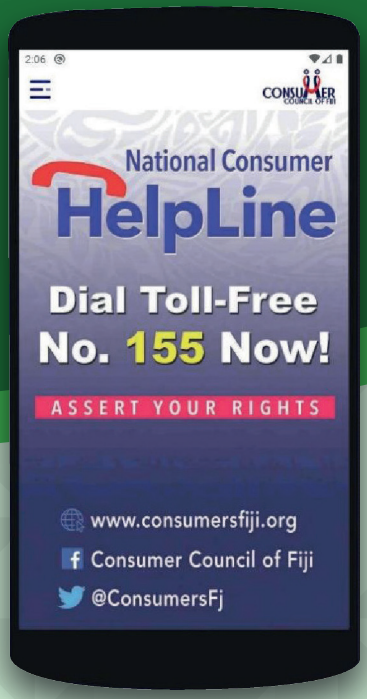
Embrace Convenience, but Prioritize Security
Mobile wallets revolutionize financial transactions, but security remains paramount. By following these tips and staying informed, you can keep your digital money protected. For more information and assistance, contact the Consumer Council of Fiji via toll free number 155!

CONSUMER COUNCIL OF FIJI

Suva Office
Level 5 Vanua House
Victoria Parade, Suva.
Phone: 3300792 | Mobile: 9716255
Email: complaints@consumersfiji.org

Lautoka Office
Suite 4 Popular Building
Vidilo Street, Lautoka
Phone: 6664987 | Mobile: 9262807
Email: RC.ltk@consumersfiji.org

Labasa Office
Shop 2 Mudaliar Investments
Sangam Avenue, Labasa
Phone: 8812559 | Mobile: 9736799
Email: RC.lbs@consumersfiji.org



CONSUMER COUNCIL OF FIJI

DIGITAL FINANCE SCAMS

The world of mobile wallets offers unparalleled convenience – pay for groceries, send money to friends, or top up your phone credit, all from the palm of your hand. But with this ease comes an unfortunate reality: mobile wallet scams are on the rise in Fiji. This brochure equips you with the knowledge to identify and avoid these scams, keeping your hard-earned money safe.

THE DECEPTIVE LANDSCAPE: POPULAR MOBILE WALLET SCAMS

Scammers are constantly adapting their tactics, but some common themes emerge:

Impersonation Scams:

Scammers use social media and messaging apps, such as Viber, to impersonate trusted individuals like friends or family, work colleagues, heads of organizations and other prominent people in the community. They request urgent money transfers citing some form of emergency, promising repayment later. Unfortunately, once users send the money, they discover the deception. Some scammers also hijack Viber accounts to solicit money from unsuspecting contacts.

Imagine receiving a frantic message from your cousin "Ana." She claims her phone is broken, and urgently needs a small loan via mobile wallet to pay a bill. Knowing you're close, she pleads for help. However, this could be a scammer impersonating Ana. Always verify requests, especially for money, through a trusted channel like a call to Ana's known phone number.

SMS Scam:

Scammers send messages that look real to random phone numbers, claiming they've received money through the mobile wallet. They then call those people and ask for the money back. Some unsuspecting users will send this money back, not knowing that there was no money received in the first place. Another variation of this scam occurs when individuals make purchases using their mobile wallet for payment. Instead of actually completing the transaction, they fabricate a message indicating that the payment has been made. Unbeknownst to the recipient, who may not verify their account, they fall victim to this deception.

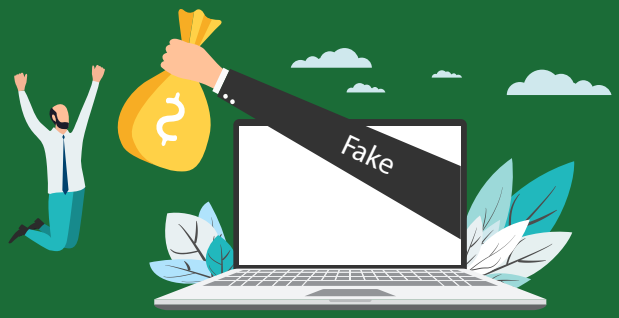
The Lottery Scam:

"Congratulations! You have won the lottery!" Users have reported receiving calls from an unknown/offshore phone number informing them that they have won a cash prize. To claim it, they're asked to fulfill certain requirements, like paying a fee or sharing personal details like OTPs or bank account information. Unfortunately, once these details are handed over, scammers swiftly drain the victim's bank account.

Imagine, an unexpected call informs you that you've won a national lottery! All you need to do is send a small "processing fee" via mobile wallet to claim your millions. This is a classic scam. Real lotteries won't ask you to pay upfront fees to claim winnings. Don't be fooled by such promises.

Unauthorized Transactions:

Some scammers also send users links that allow scammers to access the accounts and funds of users, and then use the OTP to drain the account of any money. Cases have also been reported of family members making unauthorized transactions with access to mobile wallet accounts.



RED FLAGS: HOW TO SPOT A MOBILE WALLET SCAM

Staying vigilant is key. Here are some warning signs to be on the lookout for, with additional details to help you identify scams:

The Urgency Trap:

Scammers create a sense of urgency, pressuring you to act quickly without thinking things through. Ask yourself: Why the rush? A legitimate request can wait for verification.

Impersonation:

If someone you don't know personally contacts you claiming to be a friend, family member, official, or authority figure, especially via social media or messaging apps, verify their identity through a trusted channel (e.g., call them directly at a known number).

Unbelievable Offers:

"Get Rich Quick" schemes or unbelievable lottery wins are too good to be true. They likely are scams in disguise. If something sounds too promising, it probably is.

Suspicious Contact:

Be wary of unknown or international phone numbers, unsolicited messages, or anyone pressuring you for personal information. Don't engage with unknown contacts, and never share personal details unless you're absolutely certain of the recipient's legitimacy.

Phishing Attempts:

Don't click on links or download attachments from unknown senders. These could be attempts to steal your login credentials. Be cautious of messages with grammatical errors or poor formatting, as these can be signs of a scam.

Verification Requests:

Never share personal information, like one-time passwords (OTPs) or bank account details, through unsolicited messages or phone calls. Legitimate institutions will not ask for this information via these channels.