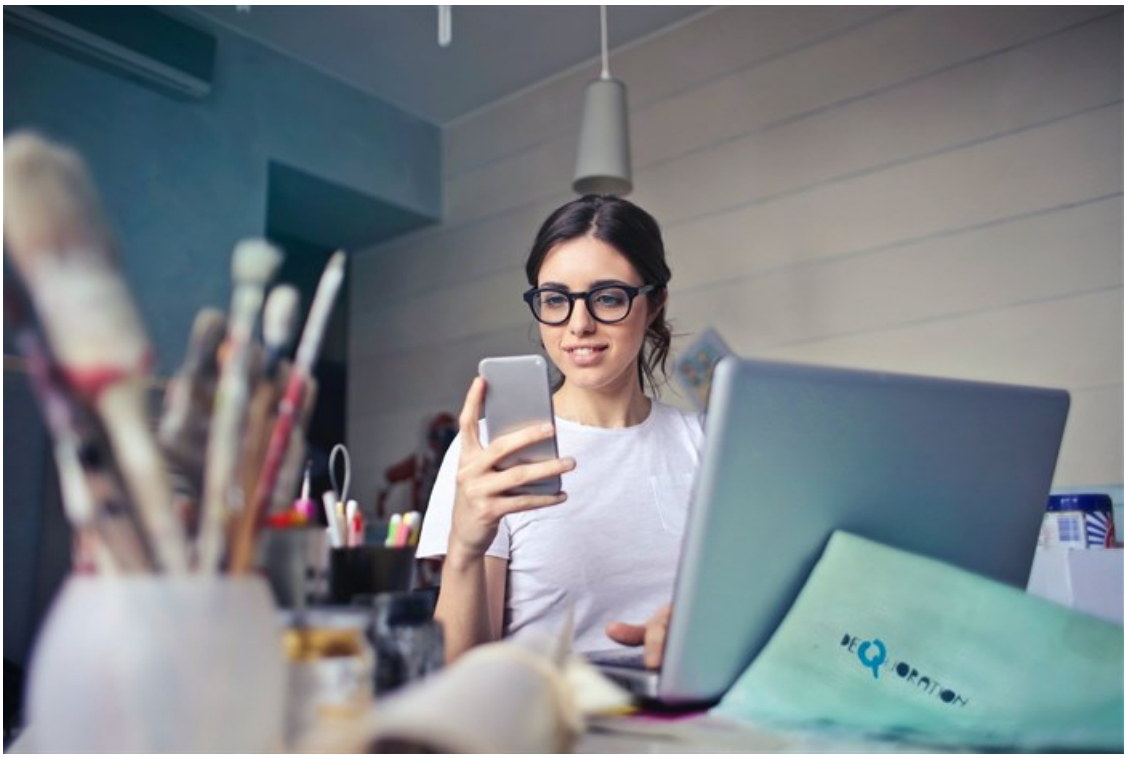
BIZCOMMUNITY

5 safety tips to consider when using your mobile money app

By Pardon Mujakachi

29 Nov 2021

The festive season is upon us, traditionally, it is time to send, receive and spend money. Many of us connect to the internet using mobile devices and peer-to-peer (P2P) money transfer platforms are becoming a favoured option for daily transactions. According to a Technoserve study, over R157bn moves between provinces every year and over 24 million South Africans use P2P platforms for domestic remittances.



Source: Unsplash

P2P platforms such as mobile money solutions offer a convenient and easy-to-use alternative to traditional financial platforms. They have made it easier to shop online, order services, buy essentials like airtime and data, pay bills and support friends and family members from afar with little to no lag time. Unfortunately, the convenience of P2P apps has attracted opportunistic scammers and fraudsters to target users.

Types of scams associated with P2P money transfer platforms

Here are the nine most common scams that fraudsters use to steal money and 5 tips people can follow to protect themselves.

1. **Application fraud (stolen identities):** This happens when strangers sign up for P2P apps pretending to be you and pulling money directly from your bank account. They create P2P accounts after obtaining bank account numbers and other sensitive information through data breaches.
2. **Smishing scams:** Stealing your password is a common goal of a phishing, vishing or smishing scheme. Be careful of emails, phone calls or text messages (even from people you know) that sounds like an emergency and ask you to open an attachment, click a link or send information. Banks or P2P platforms will never call, send an SMS or email asking for your pin.
3. **Authentication scams:** Fraudsters send out fake alert text messages, pretending to be from the P2P platform. If you

respond, the con artist will call asking you to verify your account and request passwords, secure access codes, verification codes, PIN, etc.

4. **Account takeovers:** Smishing or phishing can lead to hackers accessing your account and transferring funds to another account within seconds. Often, passwords and usernames will be changed so that it is more difficult to regain the account and file a report.
5. **Fake support:** Scammers comment on your social media post and ask for your number and your password so they can assist to set up your account.
6. **DM scammers:** Such scammers pretend to be from the P2P platform, and they usually direct message (DM) you promising to 'Add to' or multiple the funds that you send to them.

7. **Money flippers:** This happens when you receive a message about a quick tip to double or triple your money. The message will be time-sensitive forcing you into rushed decisions.
8. **Fake services:** Fraudsters make offers that are "too good to be true" and they also propose services that your P2P platform doesn't offer such as a loan service with high interests for the loanee.
9. **Fake agents:** These fraudsters contact people with fake, unverified accounts on social media posing as the official account from your P2P platform.

How to protect yourself from scams

- **Who and what to trust:** Be careful of anyone who calls or sends you an unsolicited message asking for payment first before providing you with a service or assistance. They are almost certainly a fraudster.
- **Take it slow:** Fraudsters often capitalise on the need to urgently receive a particular service. You must carefully review any offer you receive and consider whether it is genuine or not.
- **Confirm the facts:** Be suspicious of any messages sent to you without invitation. Take steps to confirm if the communication has been sent from an official source such as verified social media handles or in-app chat features.
- **Protect your information:** Never respond to any request to share your confidential information including your mobile number, account password or pin.
- **Do not accept offers of help or respond to requests for help:** Find official channels that your P2P platform uses to communicate such as in-app chat features. Unsolicited offers to help with a particular service outside of official channels is fraudulent.

Conclusion

Fraud and scams are a real threat to people's financial security and the convenience of using P2P payment platforms. People can avoid falling victim to financial loss and identity theft by exercising extreme caution to any unsolicited messages, staying updated on the latest schemes, staying wary and turning to trusted and official sources. If you suspect any fraudulent activities in your account, contact your P2P transfer service provider.

ABOUT THE AUTHOR

Pardon Mujakachi is vice president: strategy and partnerships, Africa at Chipper Cash.