African Bank Ltd press release

7 May 2021

Payment platforms remain a playground for criminals, be aware of what they're up to

Online transacting hit an all-time high worldwide due to Covid-19 lockdown restrictions, and many consumers now prefer this method despite being able to actually leave home to buy something.

And, why not transact online? It is simple, convenient and cheaper, banks are encouraging it and just about every store has an online shop today.

Piet Swanepoel, Chief Risk Officer at African Bank, says the reality is that this environment provides fraudsters with an easy and ever-growing range of targets.

"Just as the online transaction landscape has transformed, so have the methods criminals use to access your money," he says. "Strong identification and verification procedures remain a vital defence but digital attacks continue to pose challenges to the online payments ecosystem."

This is mainly due to the proliferation of payment platforms and channels and the growing list of Internet of Things devices.

According to African Bank, devices are now a significant vulnerability in the battle against 'Account Take Over' fraud. In fact, with merchants now commonly using mobile devices to facilitate transaction processing, the number of device takeovers reported has doubled every year since 2014.

Some common forms of fraud:

Card Not Present (CNP) fraud: A fraudulent transaction takes place but neither the card nor the cardholder is present. Only the card details are used. These transactions are usually performed by the merchant where the customer provided the card details in a non-secure manner.

This kind of fraud generally falls into two categories. "One is device theft whereby criminals manage to access your banking app through methods in which they break / breach the security features of the device. The other is what we term a Sim SWAP / TWIN/PORTING fraud. This is a big problem in the sector as effectively, if there are not controls in place detecting the aforementioned, the fraudster will receive either the OTP or USSD message from the user's bank and can easily steal funds from a customer's existing accounts," says Swanepoel.

He says the problem is we all tend to store large amounts of valuable information on our phones, including account numbers, passwords, phone numbers and email addresses. With phone hacking software easily available online, it does not take a genius to commit fraud and this is where an account takeover can be really serious.

Members of fraudster syndicates trick ordinary, often desperate, citizens to use their bank account or open new accounts for them to use in their syndicate operations.

"They can also use social engineering methods (no tech but persuasive psychology to break normal security procedures and practices) to gain access to the user's OTP to initiate the account take-over or Profile compromise. They have become so skilled that it is often difficult to realise you are being scammed. Once criminals have access to the profile, they will change the stored cell phone number to potentially receive all future OTP's or interactive accept messages."

Tips to avoid fraud:

- Subscribe to your bank's SMS notification services to stay informed of any transactions on your accounts.
- Review account statements regularly and immediately alert your bank to disputed transactions.
- When shopping online, only place orders with your card on a secure website.
- Do not click on hyperlinks found in emails or text messages from unknown or suspicious sources.
- Never share your PIN, password or any One-Time-Pin (OTP) with anyone.
- Do not send emails that quote your card number, card expiry date and/or CVV number.
- Report lost and stolen cards immediately.
- Destroy your credit card receipts before discarding them.
- Never let the card out of your sight when making payments.
- Your credit card is not transferable. Only the person whose name appears on the front of the card is authorised to use it. This is the same with your debit cards.
- Do not choose the same PIN for all your cards.
- Protect your cards (and the details printed on your card) as if they were cash.
- Always check transaction slips for correct purchase amounts and/or suspicious transactions.
- If your device is lost or stolen, report it immediately to your bank to ensure they can proactively prevent any possible fraud on your banking app.

“The best defence against falling victim to criminals is to take care with each and every online transaction, carefully ensuring the platform, prompts and payment method is legitimate,” Swanepoel says.

“If you suspect something is not right, stop or cancel the transaction immediately, and always report suspicious activity, emails or phone calls to your bank.”

ENDS

Visit the African Bank website or like them on Facebook , Twitter and LinkedIn

PREPARED ON BEHALF OF AFRICAN BANK BY CATHY FINDLEY PR. CONTACT JACQUI MOLOI ON JACQUI@FINDLEYPR.CO.ZA OR 071 7648233 WITH ANY CONSUMER PR QUERIES.