African Bank Ltd press release

March 2021

Don't let these ATM scams happen to you

Customer protection strategies are at the forefront of banks' efforts to curb ATM and related crimes, but to be effective they require customers to also do all they can to protect themselves, says Piet Swanepoel, Chief Risk Officer at African Bank.

ATMs are a favourite target for criminals simply due to their increased usage and accessibility to customers, day and night.

Their modus operandi, Swanepoel says, involves various scams, like shoulder surfing, card skimming, swopping of cards and the trapping of cards inside ATMs.

As part of its Customer Protection Programme, African Bank provides insight on how these scams work and how customers can avoid falling victim:

CARD SWOPPING:

- The perpetrators are groups of at least three criminals.
- The victim is distracted while the card is swopped, usually after inserting their PIN number. One of the criminals will have shoulder surfed the PIN prior to the card swop.
- The victim leaves with someone else's card and the criminals immediately use the stolen card to make purchases or withdraw money, before the victim realises and has a chance to block their card.

SKIMMING:

- Victims are coerced into swiping their cards through hand-held devices at ATMs.
- A person claiming to be a bank employee approaches the victim and requests they 'reactivate' their card by swiping it through the hand-held device (the skimming device). This can happen before or after the customer has withdrawn money. There is often a second or third person loitering around the ATM, shoulder surfing for the PIN.
- In some cases, the ATM card reader entry slot is damaged. While the victim struggles to insert their card, the criminal will approach the victim and take the ATM card from the victim, often escorting the victim to another ATM to attempt the withdrawal. While on their way to the second ATM, the criminal gets hold of the card and it is skimmed.
- The victim is handed back the original card only to discover much later that money was withdrawn from their account.

ATM-MOUNTED SKIMMING:

- Most ATM skimming devices do not interfere with the ATM when utilised. These devices are created to look like a card reader slot and fit seamlessly over the slot, making them difficult to detect.
- A skimming device can also be mounted over the ATM card slot. The false reader in the skimming device acquires the magnetic strip data and the PIN is compromised by means of a camera containing the skimming device which is installed in the mould.

TIPS

- Follow the instructions on the ATM screen carefully.
- Be alert to your surroundings and leave if you notice anyone loitering suspiciously.
- After successfully transacting at the ATM, leave immediately.
- If your card does not go in smoothly do not force it in. Rather leave the ATM.
- If your card is swallowed do not leave the ATM before you have cancelled your card.
- Memorise your PIN, never have it written down or share it with anyone.
- Key in your PIN yourself in such a way that no one else can see.
- Never let anyone stand close to you while using the ATM.
- Make sure you are not followed after withdrawing money from an ATM.

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.