African Bank Limited press release

17 November 2020

Make sure it is just the cost of your black Friday shopping that leaves the store

The internet is buzzing with black Friday specials already and retailers are busy stocking shelves in anticipation for the traditional hordes of bargain seekers.

It is an exciting time but also an opportunity for criminals to strike. “Black Friday and Cyber Monday is the time of the year that phishing grounds are the most lucrative for cybercriminals. Attacks increase by as much as 336% around this time,” says Neil Thompson, Head of Product and Customer Value Proposition at African Bank.

While retailers should go to great lengths to protect your data, as consumers it still remains your responsibility to keep your own information safe.

Here are 10 golden rules to staying safe this Friday and Monday:

- ✓ Always get your own card back after every purchase and always ask that the credit card machine is swiped in front of you.
- ✓ Never write down your pin or disclose it to anyone and use different pins for different cards.
- ✓ Be aware of scam URLs – mobile users are often susceptible to this scam as they often do not check the full URL on their device. This is an easy way to trick people into thinking they are buying the real thing.
- ✓ Keep your transaction slips and check them against your statement to spot any suspicious transactions and query them immediately.
- ✓ While transacting always keep an eye on the ATM card slot to ensure that your card is not taken out, skimmed and replaced without your knowledge. The South African Banking Risk Information Centre (SABRIC) also advise that if you are not familiar with the screen layout of the ATM or if it appears that the machine has been tampered with, do not insert your card.
- ✓ Should an ATM retain your card, contact your bank and block your card before you leave the ATM.
- ✓ Subscribe to your bank's SMS notification services; this will inform you of any transactional activity on your account.
- ✓ If you are shopping online be especially cautious of phishing scams. Internet

banking fraud now makes up 55% of all fraud occurring through banks. If an offer looks too good to be true it is probably fake. You need to watch out for emails promising these amazing bargains. Rather than click on a link in an email or SMS, go to the site itself. Hackers can even spoof websites, so make sure you're shopping on the actual site.

- ✓ Do not assume you are speaking to your bank. Unsuspecting customers honestly believe they are speaking to a credible source from their bank or another trusted institution and disclose sensitive information, often under the pretence of a 'security protocol'. Once a criminal has a mobile banking pin or password, a fraudulent sim swop is conducted on the cell phone number and that allows the criminals to transact as if they were the real account holder.
- ✓ Always use a secure and trusted WiFi

"Always let caution prevail and stay alert and aware to scams and fraudsters looking to take advantage of distracted shoppers," concludes Thompson.

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 RORKE ON JACQUI@FINDLEYPR.CO.ZA OR 071 764 8233 WITH ANY CONSUMER PR QUERIES.