African Bank Limited press release

December 2018

'Tis the season for online shopping – beware of phishing scams

'Tis the season for shopping and with it comes the threat of phishing, warns Penny Futter, Chief Information Officer at African Bank. She explains that phishing is when criminals use a form of electronic communication to try and extract sensitive information like usernames, passwords and credit card details. It is fast becoming one of the leading contributors of fraud.

"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'," says Futter. Once a criminal has your 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.

"The problem," she says, "is that although most people are aware of the scams and would not normally give out important information, these fraudsters are so clever and believable that many people still fall victim to their scheme and then are not even aware that they have been scammed until it is too late."

Online shopping is growing but, says Futter, we should continue to be cautious when shopping online. "Only use vendors who offer a second form of identification to avoid being scammed. You may want to even consider opening a second bank account for online transactions and keep only keep a minimum balance in the account topping it up when funds are needed."

So, while you are merrily spending your hard-earned cash this festive season take note of these important tips:

- Don't click on links or icons in unsolicited emails. Do not even reply to these emails. Delete them immediately.
- Type in the URL for your bank in the internet browser if you need to access your bank's website. Check that you are on the real site before using any personal information. If you think that you might have been compromised, contact your bank immediately. Create complicated passwords that are not easy to decipher and change them often.
- It may be worth considering protecting your passwords using any one of the public and freely available password managers.
- Never carry unnecessary personal information in your wallet or purse and never access your banking site on a public WiFi network.
- Don't give out any personal details if someone phones you. A bank will never phone you to ask for your pin.

"If you do get caught and believe your information has been compromised, change your internet banking credentials immediately and advise the bank accordingly," concludes

Futter. “Let’s all be more savvy this festive season and make sure we don’t take the phishing bait.”

Source: SABRIC

Visit the African Bank website or like them on Facebook

ENDS

PREPARED ON BEHALF OF AFRICAN BANK BY CATHY FINDLEY PR. CONTACT JACQUI RORKE ON JACQUI@FINDLEYPR.CO.ZA OR (011) 463-6372 WITH ANY CONSUMER PR QUERIES.