African Bank Limited press release

January 2019

Phishing scams in the spotlight again

The recent exposé on Carte Blanche has once again brought phishing and other online banking scams into the spotlight. Penny Futter, Chief Information Officer at African Bank, says it is a real issue facing financial institutions and the public. 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. “No financial institute or individual is immune. Phishing is one of the leading contributors of fraud,” she says.

Carte Blanche reported that, according to data collected over 8 months in 2018 by the South African Banking Risk Information Centre (SABRIC), internet banking fraud now makes up 55% of all fraud occurring through banks amounting to a R250 million loss over this period.

Futter says 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.

“Although most people are aware of the scams and would not normally give out important information, the problem is these fraudsters are so 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.”

She says it is vital to check bank statements regularly and to have limits on accounts. Futter also strongly recommends that all banking customers read the terms and conditions as well as the security protocols in place before agreeing to any online or mobile banking. “Speak to the bank and make sure you understand what security protocols are in place to protect your money.”

When shopping online she recommends using only reputable companies who have robust security and authentication policies in place to avoid being scammed. “You may want to even consider opening a second bank account for online transactions and keep only a minimum balance in the account topping it up when funds are needed.”

Keep these tips top of mind:

- 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. Always keep your online banking login details confidential.

“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.

Visit the African Bank website or like them on Facebook

For the Carte Blanche episode on online banking fraud click here:

https://m-net.dstv.com/show/carte-blanche/videos/online-banking-theft/video

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.