African Bank Limited press release

27 November 2017

Don't be a phishing victim this holiday season

Phishing, when criminals use a form of electronic communication to try and extract sensitive information like usernames, passwords and credit card details, is fast becoming one of the leading contributors of fraud. "And these fraudsters will be on the hunt this holiday season as people receive bonuses and do more online buying," says Hendus Venter, Chief Information Officer at African Bank. Kalyani Pillay, CEO of South African Banking Risk Information Centre (SABRIC), agrees saying criminals are always looking for opportunities to defraud their victims, particularly at this time of year when they know that people are winding down for the holidays, and spending their bonuses.

Clever social engineering tactics are regularly used by criminals to trick their victims into disclosing their cell phone or mobile device banking login credentials. "Unsuspecting customers honestly believe they are speaking to a credible source from their bank and disclose sensitive information, often under the pretence of a 'security protocol'," says Venter. 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," says Venter, "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."

Pillay says SABRIC is urging users not to click on links or icons in unsolicited e-mails. "Do not even reply to these e-mails. Delete them immediately. Do not believe the content of unsolicited e-mails blindly. If you are worried about what is alleged, use your own contact details to contact the sender to confirm."

She explains that you should type in the URL for your bank in the internet browser if you need to access your bank's webpage. "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."

Venter adds to that saying 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. Remember that you should never give out any personal details if someone phones you. A bank will never phone you to ask for your pin number."

While online shopping is becoming more and more popular, Venter says 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."

"Be aware and cautious. Fraudsters do know all the tricks so in the event that you do get caught and believe your information has been compromised, change your internet banking credentials immediately and advise the bank accordingly," concludes Venter.

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.