African Bank Ltd press release

June 2021

Beware being lured in by vishing criminals

Criminals use many avenues to access personal information and money from bank accounts. One such means is called Vishing, says African Bank Chief Risk Officer Piet Swanepoel.

He explains that vishing is the phone version of email phishing and it uses a live voice or automated voice message to access confidential information, such as banking or credit card details.

The perpetrators deliberately create perfect conditions to trap unsuspecting victims into willingly handing over personal information, such as their full names, ID numbers, addresses, phone numbers and your online banking or credit card details.

Their aim is to trick people into providing sensitive information over the phone with which they can access your financial accounts or steal your identity.

“The word ‘vishing’ is a combination of ‘voice’ and ‘phishing. Most people are familiar with phishing. This is when someone phones claiming to be from your bank, a credit card company, charity or even a debt collector.

“Vishing criminals use a spoofed caller ID, which can make the attack look as though it comes from either an unknown number or an 800 number, in the hopes the person targeted will answer the call,” says Swanepoel.

“Impersonating a person or legitimate business to scam people isn’t a new thing. Vishing is simply a new twist on an old routine and has been around for as long as the internet has.”

An example of vishing is receiving a phone call from someone who says they are from your bank or some other financial institution. They may say they are calling because there is a problem with your account or with a payment from your account and ask you to transfer money to a different account to solve the problem.

The attacker, posing as a bank official or service provider, uses social engineering skills to manipulate the person into disclosing confidential information because they believe they are speaking to a legitimate employee of the company.

Social engineering is where fraudsters use psychology rather than technology to gain access to sensitive information. It relies on persuasion, manipulation or deception to get a person to break normal security procedures and best practices.

Swanepoel says this is why many people do not even realise they are being conned.

“Victims are often totally oblivious to the fact that they have handed over valuable information to the ‘helpful’ person on the phone which will be used to steal their money or personal information – or both!

He points out that the biggest red flag with vishing schemes is an extreme sense of urgency for you to act on whatever the caller says the problem is – a breach of your bank account, a fraudulent transaction or having won a prize you need to redeem.

Tips from African Bank to avoid falling victim to vishing:

- Be aware that criminals mask telephone numbers to appear they are calling from legitimate businesses.
- Your bank will never ask you to confirm confidential information over the phone.
- Never give a stranger your personal information over the phone such as your Banking profile information or debit / credit card information.

- If you suspect the person you are speaking to is not truly a bank representative, drop the call and phone your bank on a known number obtained from their website.
- If you see an OTP on your phone without having transacted yourself, it is likely a fraudster has used your personal information. Do not give anyone this OTP over the phone and contact your bank immediately to alert them to the fact you believe there has been fraudulent activity on your account.
- If asked to share your OTP, consider it fraud.

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.**