African Bank Limited press release

24 February 2016

Don't take the phishing bait

Phishing is fast becoming one of the leading contributors of fraud today with 80% of malicious software attacks coming from phishing.

In the personal loan sector, impersonation or identity theft ranks top as the number one contributor to fraud, followed by credit card transaction dispute and then phishing comes in a close third.

Hendus Venter, Chief Information Officer at African Bank says phishing is when criminals use a form of electronic communication, either SMS (smishing) or email (phishing), to try and extract sensitive information like usernames, passwords and credit card details. "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.

And, SMS notifications on your cell phone will not even help you here. Venter explains that because the sim has been deactivated, no notifications will be received by the victim, making the fraud difficult to detect.

Venter says sim swops allow the criminal to receive Transaction Verification Codes (TVCs), Random Verification Codes (RVCs) or One Time Passwords (OTPs). "By using these together with compromised login credentials, criminals are able to change, add beneficiaries and transfer money out of a victim's account. They are even able to move to another cell phone network and still retain their cell phone number which means the criminal will continue to receive communication on the new sim card while the victim's sim card remains deactivated."

"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."

Venter offers the following useful advice to prevent becoming a victim of phishing:

- Use a clever pin: Always protect your cell phone and/or mobile device content and personal information by using a pin and ensuring that your phone and/or computer and mobile devices are password protected. This is your strongest protection against being scammed. Never use your birthday or that of a family member or part of your phone or cell phone number. It is just too easy for criminals to work out.

Rather choose an unusual pin that is hard to guess.

- Consider protecting your passwords using any one of the public and freely available password managers.
- Never carry unnecessary personal information in your wallet or purse.
- Never access your banking site on a public WiFi network.
- Never give out any personal details if someone phones you. A bank will never phone you to ask for your pin number.
- Ensure you have the latest antivirus and antispyware software installed on your cell phone and computers and other mobile devices.
- Regularly verify whether details received from your cell phone notifications are correct. Should any details appear suspicious, immediately make contact with your bank.
- Never log onto your bank's website from a link in an email or SMS. Rather type in the full web address yourself.
- Be cautious when shopping online. Only use vendors who offer a second form of identification to avoid being scammed. In fact, according to Gary Desilla, African Bank's Manager for Information Security, one may even consider opening a second bank account for online transactions. Desilla says a good tip is to only keep a minimum balance in the account and to then transfer funds to that account only when you need to complete an online transaction.

"Fraudsters do however 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.

ENDS

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