African Bank

Phishing: don't take the bait

Phishing is fast becoming one of the leading criminal activities of fraud in South Africa.

Phishing is a form of fraud in which a fraudster acts as a credible institution or person on either SMS, calls or email. Fraudsters will commonly use phishing emails which contains harmful links or attachments. Once you click on them, malware infects your system, giving these cyber-criminals access to your personal information. These criminals will then use that information to steal your identity to commit fraud or access your bank accounts.

"Although you may be aware of some phishing scams and would not normally give out important information, fraudsters are so believable that you may honestly believe you are speaking to a credible source from your bank or another trusted institution. By the time you realise you have been scammed, it is in most cases too late because you would have already disclosed personal information", said, African Bank's Group Chief Marketing Officer, Sbusiso Kumalo.

The good news is you can protect yourself against phishing. Criminals are always looking for new ways to get you to divulge your personal details but, by following these simple tips, you can keep them at bay and keep your money safe.

- Regularly check your bank statements and your credit score. They will reveal any discrepancies and unauthorised transactions, which could be indicators of fraud. You can get unlimited access to your credit score at www.africanbank.co.za
- When shopping online, use only reputable companies who have robust security and authentication policies in place to avoid being scammed. Look for the green verification tick that lets you know it's safe to click.
- Don't click on links or icons in unsolicited emails. Do not even reply to these emails. Delete them immediately.
- If an online deal seems too good to be true, it probably is. That's the bait scammers often use to get you to click.
- Type in the URL for your bank in your 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 complex passwords that aren't easy to decipher and change them often. The best passwords are a mix of upper- and lower-case letters, numbers, and symbols.
- Don't use the same password for multiple accounts. If you do, and a scammer cracks it, they will then have access to all your accounts.
- Do not write your PIN or password down, not even on the Notes app on your phone. If you have trouble remembering your passwords, consider using a freely available password manager to help you.
- Never access your banking site on a public Wi-Fi 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 your bank accordingly. You can also contact the South African Fraud Prevention Service on 011 867 2234.

ENDS