#425

Money Matters

Bank safely at all times

Johnny Truter
Manager of Forensic Services

The most popular benefit to digital banking is the convenience it gives the customer to manage their finances at any given time. Provided that customers have an internet connection and a mobile device or computer, they can access digital banking services 24 hours a day, seven days a week. While the environment for online banking is safe, criminals will take every opportunity to defraud customers.

More often, the weakest link in the fraud chain is human vulnerability, where fraudsters use techniques referred to as phishing, vishing and smishing. These techniques require the full cooperation of the account holder and a skilled fraudster who will convince customers that they are calling from their bank or send an email with the aim of getting personal information and banking details from the customer. To bank safely, customers should have a better awareness and understanding of the technology of the Bank's products and services.

For instance, the Bank Windhoek Mobile Application (App) has the functionality to activate and de-activate a card when it is not in use. The App allows a customer to decrease the card's daily limit, further protecting customers from losing large sums of money should their account be breached. When making a purchase that exceeds their daily limit, a customer can increase their daily limit on the Mobile App and, once the transaction is complete, decrease the limit again.

Another way to bank safely is for customers to subscribe to their bank's transaction notification service, such as Bank Windhoek's SMS AlertMe service notification. This service is free of charge, and notifies customers of transactions on their accounts, be it debit or credit transactions using Bank Windhoek debit and credit cards, or login and payments made on the Internet Banking (iBank) platform. Below are more safety tips when using online, mobile, and internet banking platforms:

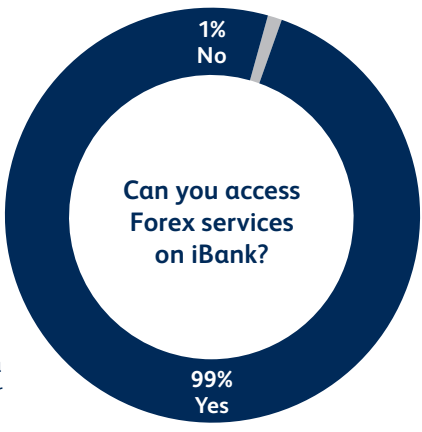
- Be cautious when using public Wi-Fi networks and do not use them for banking purposes.
- Keep your software, anti-virus and banking apps updated with the latest versions available on all your electronic devices. Change password and Personal Identity Number (PIN) frequently.
- Always type your bank's website Uniform Resource Locator (URL) directly in the browser instead of clicking on links and beware of fraudulent or imposter websites when shopping online.
- Be cautious when a caller says he or she is calling from your bank. No bank will ask you to update or confirm confidential details over the phone or by email.
- Never provide any personal and banking details to anyone for any reason, including account numbers, card numbers, Card Verification Value (CVV) numbers, usernames, passwords, and PINs, irrespective of the urgency stated. Should you get a call where these details are requested, contact your branch immediately and report the incident.
- Do not click on links provided in unsolicited emails. You may activate hidden malware embedded in the email.
- Use biometric identification and security if available.
- If you receive a transaction notification or One-Time-Pin (OTP) on your phone, do not provide it to anyone.
- Report unauthorised debit orders on your account to your bank immediately.
- Independently verify payment details by phone with a supplier before transacting Electronic Fund Transfer (EFT) payments to eliminate the risk of man-in-the-middle frauds.

Vigilance for fraudster tricks and scams remains one of our most robust defences to curb theft and fraud. For more information, contact Bank Windhoek's Customer Contact Centre on **061 299 1200.**

Win N$1000 in our Opinion Poll

Will a bank ask you to update or confirm confidential details over the phone or by email?

Email: **poll@bankwindhoek.com.na** with your full name, contact number and your "yes" or "no" answer.



Winner: Martha Heita is the lucky winner in the Money Matters Issue 424 poll draw.

Bank Windhoek
a member of **Capricorn Group**