FRAUD AWARENESS & CYBERSECURITY FAQS

1. **Why does the Kenyan banking system use a 4-digit PIN?**

   Banks use 4-digit PINs for simplicity and compatibility with global card systems. However, longer PINs or passwords offer stronger security. Always enable additional security features like Multi-Factor Authentication (MFA) where available. Multi-Factor Authentication is a multi-step account login process that requires users to enter more information than just a password.

2. **Is it safe to use public Wi-Fi for banking?**

   Avoid public Wi-Fi for financial transactions. If unavoidable, use a trusted Virtual Private Network (VPN) and never share sensitive details over unsecured networks.

3. **What should I do if I receive a phishing (suspicious) email?**

   Do not click any links or share personal details. Report the email to the bank immediately and delete it.

4. **Which details will NCBA never ask for?**

   We will never ask for your PIN, One Time Passwords (OTPs), full card number or passwords via phone, email or SMS.

5. **How do I handle a call from someone claiming to be from the bank?**

   If you receive a call from anyone claiming to be from NCBA, do not share any codes, passwords or personal details. Simply hang up and call the official NCBA Contact Centre on 0711 056 444 or 0732 156 444 to verify the request.

6. **What should I do if my account is compromised?**

   Call NCBA immediately on the official numbers [0711 056 444 or 0732 156 444]. We will block your account and guide you on next steps.

7. **Is it safe to use NCBA WhatsApp for support?**

   Yes, but only through the official verified NCBA WhatsApp number [+254717804444].

8. **Why do fraudsters mimic official phone numbers?**

   This is called "number spoofing." Always verify by calling back on the official NCBA number.

9. **Can fraudsters change my password if they have my phone number and ID?**

   Your accounts still require additional verification steps to make any changes. To stay safe, keep your SIM card protected and ensure you have enabled multi-factor authentication (MFA) on all your accounts.

10. **Is it safe to accept cookies online?**

    Only accept cookies from trusted websites. Decline cookies on unfamiliar or \suspicious sites.

11. **How do I know if an online purchase site is genuine?**

    A genuine and secure website will start with "https://" instead of "http://". HTTPS is a more secure version of HTTP. With HTTPS, the browser and server establish a secure, encrypted connection before transferring data. Additionally, verify the domain name and avoid deals that seem too good to be true.

12. **What is the best antivirus for mobile and laptop?**

    Use reputable options like Norton, Kaspersky or Bitdefender. For laptops, Windows Defender already provides solid built-in security but can be complemented with additional protection by adding one of the trusted antivirus solutions above

13. **Can I change my NCBA App login PIN?**

    Yes, you can update your PIN through the app 'Settings' then 'Change Pin'.

14. **What should I do if I have been "pwned" (data breach)?**

    If you discover that your personal information has been exposed in a data breach:

- Change all affected passwords immediately and use strong, unique passwords foreach account.
- Enable Multi-Factor Authentication (MFA) wherever available.
- To enable MFA:
    - Log into your account settings.
    - Navigate to the Security or Privacy section.
    - Select "Enable Multi-Factor Authentication" or "Two-Factor Authentication."
    - Choose your preferred verification method (Authenticator App, SMS, Email, or Security Key).
    - Complete the verification process and save your settings.
    - Monitor your accounts regularly for suspicious activity.
    - Report any unauthorized activity to the service provider or bank immediately.

15. **Is it safe to use tap-to-pay cards?**

    Yes. Tap-to-pay technology is designed with multiple security controls to protect cardholders. NCBA has set transaction limits per card type to reduce risk.

Card Type	Single Transaction Limit
Infinite	KES 15,000
Platinum	KES 5,000
Gold	KES 5,000
Prepaid	KES 5,000
Classic	KES 5,000

Additionally: The card must be extremely close to the payment terminal (usually within 1 centimeter or almost touching the device) for the transaction to be processed, and each transaction uses secure encryption to protect your payment information.

16. **What is the safest way to bank while traveling?**

    To stay secure while on the move, avoid using public Wi-Fi for any banking activity. Instead, use secure networks or a trusted Virtual Private Network (VPN). Always keep your card safe, and if you lose sight of it or receive an alert for a transaction you do not recognize, notify the Bank immediately.

17. **What should I do if someone asks me to read out a One Time Password (OTP) code?**

    Never share your OTP with anyone, not even with someone claiming to be from the Bank. Banks will never ask for your OTP. If someone requests it, it is a common fraud attempt. Simply decline and report the incident to the Bank immediately.

18. **Is it okay to use free Wi-Fi with Virtual Private Network (VPN)?**

    VPN adds a layer of security, but public Wi-Fi still carries risks. Use mobile data for sensitive transactions.

19. **Does NCBA share customer data with other banks?**

    NCBA does not share customer information without lawful authority, customer consent, or where required by regulation. We comply with the Kenya Data Protection Act and maintain strict controls to protect customer information.

20. **Can I share the webinar link with family and friends?**

    Yes, feel free to share the link so they can also benefit from the insights.

    Visit our new website for more information on NCBA products and services here.