Cyber Awareness

Frequently Asked Questions

Protect Yourself from Cyber Fraud

At **Development Bank of Kenya (DBK)**, protecting your money and personal information is a shared responsibility. Stay alert, know the warning signs, and never share your confidential banking information with anyone.

1. What is cyber fraud?

Cyber fraud is the use of technology, deception, or social engineering to steal money, personal information, banking credentials, or access to accounts.

2. What information should I never share?

Never share your:

- PIN
- Password
- One-Time Password (OTP)
- Mobile banking credentials
- Internet banking login details
- Account or personal identification information with unauthorized persons

DBK will never ask you to disclose your PIN, password or OTP.

3. What is phishing?

Phishing is a scam where criminals pretend to be a legitimate bank, company, or person to trick you into revealing confidential information.

Phishing may happen through:

- Emails
- SMS
- WhatsApp or other messaging platforms
- Social media

- Fake websites
- Phone calls

Always verify the source before clicking a link or providing information.

4. How can I identify a suspicious message?

Be cautious if a message:

- Creates a sense of urgency or panic
- Requests your PIN, password or OTP
- Contains suspicious links
- Promises unexpected rewards or money
- Threatens account closure or suspension
- Comes from an unknown or unusual number or email address
- Asks you to install an application or provide remote access to your device

5. Can I trust someone who claims to be calling from DBK?

Not automatically. Fraudsters can impersonate bank employees or use information obtained from social media and other sources.

If you receive a suspicious call, do not disclose confidential information. End the call and contact DBK using our official contact channels.

6. What should I do if I receive a suspicious SMS, email or WhatsApp message?

Do not click on links, reply to the message, or provide any confidential information.

Verify the communication through DBK's official channels and report any suspicious activity to the bank.

7. What should I do if I accidentally share my PIN, password or OTP?

Act immediately. Contact **Development Bank of Kenya** through our official customer service channels and report the incident.

If possible, change your affected passwords immediately and monitor your account for unusual transactions.

8. How can I protect my mobile banking?

- Keep your phone's operating system and banking applications updated.
- Download applications only from trusted official app stores.
- Use a strong screen lock.
- Never allow strangers to access your phone remotely.
- Avoid reusing the same PINs or passwords across multiple applications or accounts
- Do not save your banking PINs or passwords where others can easily access them.
- Avoid conducting banking transactions over unsecured public Wi-Fi.

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

Avoid accessing mobile or internet banking through unsecured public Wi-Fi networks. Use a trusted and secure connection whenever possible.

10. What should I do if I notice an unusual transaction?

Report it to **DBK immediately** through the bank's official channels. The faster you report suspicious activity, the sooner appropriate action can be taken.

11. How can I verify that I am visiting the genuine DBK website?

Always access the bank's website using the **official DBK web address**. Be cautious of websites with unusual domain names, spelling mistakes, suspicious pop-ups, or requests for confidential banking information.

12. Should I allow someone to remotely access my computer or phone?

- No, unless you have independently verified that the request is legitimate and authorized.
- Fraudsters may claim to be bank employees or technical support agents and ask you to install remote-access software. This can give them control of your device and access to sensitive information.

13. What is social engineering?

Social engineering is when criminals manipulate people into giving away confidential information or performing actions that compromise their security.

Common examples include impersonating bank employees, relatives, government officials, or service providers.

14. How can I protect my family from cyber fraud?

Talk to your family about online safety. Encourage them to:

- Keep passwords and PINs private.
- Avoid clicking suspicious links.
- Verify unexpected requests for money.
- Use strong passwords.
- Enable multi-factor authentication where available.
- Report suspicious activity immediately.

15. What is the most important rule to remember?

STOP. THINK. VERIFY.

Before sharing information, clicking a link, approving a transaction, or sending money, take a moment to verify that the request is genuine.

Stay Alert. Stay Secure.

Your security matters to us. If you suspect that your account or banking information has been compromised, contact **Development Bank of Kenya immediately through our official customer service channels.**

Never share your **PIN**, **password** or **OTP** with anyone — including someone claiming to be from DBK.

Official Website: www.devbank.com

Contacts: 0207904815 | 0207904819

Your solid financial partner