Customers who need help reading this screen may use the Kibo App on the Apple Play Store or InstaReader App on the Android Play Store

Online Banking Security Measures

- National Development Bank PLC has implemented multiple layers of security for online banking and is continuously upgrading it, to protect you from online frauds.

Secure sessions

- You will see that our URL address begins with https: which confirms that you have logged on to a secured site
- Padlock () symbol available in the right hand corner resembles the security certificate issued by a reputed company
- Be cautious about the last visited date and time shown in NDB Bank Online for your information

Encryption

- Secure Sockets Layer-SSL encryption technology is used within your Online banking session to encrypt your personal information before it leaves your computer in order to ensure no one else can read it.

Session time out

- If you are inactive for a certain period of time while logged in to NDB Bank Online, system will automatically log you out, to avoid unauthorized activities.

Automatic lock out

- Your user ID will be disabled or blocked by the system due to number of invalid log in attempts
- Unique user ID and password is given for proper identification
- You are identified by the user ID and the correct password keyed in by you. It is vital that you do not share your password with anyone
- As a customer you are playing a vital role, you are requested to be vigilant and exercise caution while you are online with the bank.

Please adhere to the following recommendations to reduce the chance of an unauthorized person accessing your account

Access NDB Bank Online the correct way

- Ensure you are accessing the authentic NDB Bank website by typing the correct website address (https://www.neosonline.ndbbank.com/) in to your browser
- Check for security indications
- Make sure that you are on the secure NDB Bank Online website before you enter sensitive information by verifying that;
- The website address begins with https: rather than http:

Safeguard your password

- Change the initial password issued to you by the bank immediately to something that is difficult for someone else to guess
- Create a strong password by adopting the following
- At least eight characters with a combination of letters, numbers, lower case, and upper case
- Easy for you to remember, but difficult for others to guess
- Unique and must not be used for accessing other online services as in e-mail or internet access
- Avoid using dictionary words or personal information as in your child's name, pet's name, your date of birth, etc. when choosing a password, as these can be easily guessed by someone else
- Do not create passwords using a combination of consecutive numbers or letters such as 12345678, abcdefgh or adjacent letters on your keyboard such as zxcvbnm
- Never disclose your password to anyone including bank staff and do not record them anywhere. Change the password immediately if you believe your password has been compromised
- Change your password regularly to minimize the risk of having your password being compromised
- Disable your browser's Auto Complete feature that remembers the data including your online password that you input Refer to your browser's Help function for details. Also avoid the option Remember my Password

Use a secure login

- Avoid accessing NDB Bank Online from shared computers or public computers as in internet cafés, free wireless access points etc....
- Never change sensitive details such as your password when using public computers
- Protect your computer
- Ensure that no one has unauthorized access to the computer you use for Online Banking
- Install a reliable anti-virus product and ensure it is updated regularly
- Configure your computer to obtain the latest security patches for your operating system
- Use a personal firewall to perform real time detection of malicious programs and intrusions
- Do not install free software from the internet or from unreliable sources

Precautions for emails

- Online identity fraud, often known as phishing, occurs when fraudsters impersonate trusted businesses and send emails to thousands of random email addresses, tricking you into downloading a virus or signing onto a bogus website and giving personal information. To defend yourself from such fraud.
- Do not react to e-mails requesting personal information such as your password, credit card details, account number, etc.
- If you receive such a request, refrain from responding, and notify the bank immediately.
- When contacting the bank, exclusively use the Message to Bank tool that is available in NDB Bank Online.
- Do not click on hyperlinks embedded in emails or third-party websites to access the NDB Bank Online website.
- Use caution when using the phone. It's easy for someone to pretend to be someone else while on the phone. Whether it's someone who wants personal information about a specific customer or someone who claims they need to authenticate one of your personal accounts, don't offer information over the phone unless you can positively validate the caller's identity.

Limit access to your computers

- Of course, your computer network must be password protected so that anyone wandering through your business cannot simply access it. However, you should also examine internal network access difficulties. Do all employees need access to applications or databases that may contain sensitive information? Passwords safeguard these as well, and access is granted only to those who need it, helping to reduce identity theft.

Disconnect ex-employees immediately

- When employees no longer work for your business, you need to be sure that their access to your computer network and company data is cut off immediately

Other safety measures

- Always keep track of the date and time you last signed into NDB Bank Online. If you detect any differences, reset your password immediately and notify the bank.
- Check your account statements and bank balance on a regular basis, and alert the bank promptly if you uncover any inaccuracies or unlawful activity.
- Avoid surfing to other websites while conducting online banking operations.
- Never leave your computer alone while doing online financial activities.
- After each session, clear your browser's cache and history to remove your account information, especially if you're using a shared computer.

General Safety Tips for ATM/CRM Usage

- Be mindful of shoulder surfers - people who may attempt to watch your PIN as you type it in.
- Once your transaction is complete, immediately retrieve your card and cash before leaving the ATM or CRM.
- In the event your card is lost, stolen, or stuck in the machine, notify the bank immediately to avoid any misuse.
- Memorize your ATM PIN; don’t write it down.
- Avoid easily guessed numbers like birthdays, anniversaries, or simple patterns like "1234" or "0000" as your Debit/Credit Card PIN.
- Regularly change your PIN to minimize risk.
- Never share your ATM PIN with anyone, including bank staff.
- Do not allow anyone else to handle your card or perform transactions on your behalf to prevent potential misuse.
- When you perform a cash deposit/ bill payment through a CRM, confirm that your account/ biller has been credited with the deposited amount by checking the on-screen confirmation and retaining the receipt.