LANDBANK eMDS ONLINE SECURITY POLICY

Security Systems

LANDBANK deploys intrusion detection systems, firewalls, encryption systems such as Transport Layer Security (TLS) 1.3 and other internal controls which are meant to safeguard, physically and logically, all our servers and information systems, including the data stored in these systems. Furthermore, it has an in-house Network Operations Department that secures the maintenance of the whole facility.

Website Authentication

The LANDBANK eMDS facility is secure, using GMO GlobalSign Certificate for you to verify the authenticity of the eMDS site. At times, it may be necessary for you to verify the authenticity of the eMDS site so you will not be a victim of internet scams (for example, clients will be directed to seemingly legitimate sites then mislead them into providing vital account information to entities not authorized by the Bank). The GlobalSign Logo attached on all our eMDS pages, when clicked, securely authenticates the eMDS site.

The best, safest and recommended way to access the eMDS website is by typing https://www.lbpemds.com at the browser address bar.

Third-Party Agreements

Certain transactions involving third parties – Notice of Transfer Allocation and List of Due and Demandable Accounts Payable (LDDAP), all require enrolment of accounts submitted to us for verification and the inclusion of Multifactor Authentication/One-Time-Password in the User Login and LDDAP Transactions. With this policy, you are assured that LANDBANK will honor requests for transfers or payments only to and from those that you have signed for.

E-mail

All financial transactions made through the LANDBANK eMDS will generate corresponding emails which will be sent to your registered e-mail address. We encourage you to continually check and verify your e-mails, especially the e-mail facility incorporated in the eMDS, in order to assure that all your transactions are in order.

The official e-mail address of LANDBANK eMDS is lbpemds@mail.landbank.com.

Password Protection

All clients visiting the eMDS website pass through the Log-in authentication process. Clients are advised to use a password that is easy to remember but hard for others to guess. Ensure to keep password confidential at all times by not writing or divulging it to anyone. Change password frequently, or change it immediately once password has been compromised.

How To Protect Yourself Online

LANDBANK encourages clients to take part in protecting their account while doing transactions online by ALWAYS doing the following:

1. **Ensure that the site is secured before using it:**

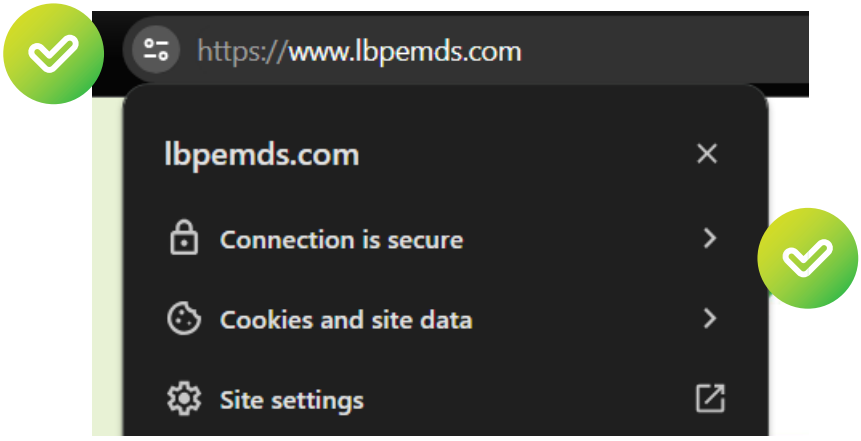
   a. Always type the complete web address into your browser instead of clicking links. By doing this, you are decreasing the risks of being deluded by a phishing* site.

   ***Phishing** is the practice of attempting to obtain information *(e.g., usernames, passwords, credit card details, Bank account numbers, ATM PIN, etc.)* by pretending to represent a legitimate company in an e-mail or websites.

   The e-mail usually claims that it is necessary for the recipient to update and provide the information in the link or form attached in the e-mail. The criminals then use the information entered on the phishing site or form for their own fraudulent intentions.

   Official URL of LANDBANK eMDS: https://www.lbpemds.com/
   Official e-mail Address of LANDBANK eMDS: lbpemds@mail.landbank.com

   b. Ensure that **'https'** and the **padlock symbol** are present in the website. These indicators signify that the site you are entering is genuine and secure. Double click the padlock symbol to verify if the certificate issued is still within its valid dates or if it has been issued to the website you are accessing.



2. **Secure your password.**
   a. Use a password consisting of alphanumeric combination with a minimum length of 6 characters.
   b. Keep the password confidential at all times.
   c. If prompted to change the password, please make it a point to change it at once.
   d. Disable the browser's password-saving feature.

3. **Protect your computer from online attacks from viruses, hackers, spywares and other malicious programs by doing the following:**
   a. Install and regularly update your Anti-virus and Anti-spyware Software.
   b. Activate the computer's firewall settings.
   c. Always update the operating system.
   d. Do not download files or software from websites which you are not familiar with or from hyperlinks sent by strangers.

4. **When accessing your account using a public computer or using a public WIFI network, please practice the following:**
   a. Never adjust the security details.
   b. Always log-out from the online session once finished with the transaction.
   c. Ensure that no one can see the transactions in public.

5. **Personal information** such as address, mother's maiden name, mobile/telephone numbers, social security number, Bank account number and e-mail address **should not be disclosed unless the one gathering the information is reliable and trustworthy.**

6. **Regular checking of transaction history details and statements should be done to ensure that no unauthorized transactions occur.**