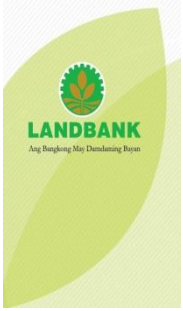


weAccess Online Security Policy

At LANDBANK, you are always assured that all your Internet Banking transactions are safe and secure. The LANDBANK Institutional Internet Banking facility, weAccess, takes great measures to ensure that our security practices conform to the best banking standards and adequately respond to all your institutional needs.

To ensure that the privacy of your account information and banking transactions are maintained, LANDBANK has set forth the following:

Security Systems

LANDBANK deploys intrusion detection systems, firewalls, encryption systems such as 128-bit Secure Sockets Layer (SSL) 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 weAccess facility is secure, using Verisign's Security Certificate for you to verify the authenticity of the weAccess site.

At times, it may be necessary for you to verify the authenticity of the weAccess site in order not to fall victim to email scams, for example, those that direct our clients to seemingly legitimate sites then mislead them into providing vital account information to entities not authorized by the Bank. The Verisign Logo attached on all our weAccess pages, when clicked, securely authenticates the weAccess site. The best, safest and recommended way to access the weAccess website is by typing https://www.lbpweaccess.com at the browser address bar.

Third-Party Agreements

Certain transactions involving third parties – Third-Party Fund Transfers, Auto Debiting and Bills Payment – all require enrollment of accounts and Memorandum of Agreement (for Auto Debiting) submitted to us for verification. With this policy, you are assured that LANDBANK will honor requests for transfers/payments only to and from those that the institution has signed for.

Email

All financial transactions made through the LANDBANK weAccess will generate corresponding emails which will be sent to the Maker/s and Authorizer/s. We encourage you to continually check and verify your emails, especially the email facility incorporated in the weAccess system, in order to assure that all your institutional transactions are in order.

Password Protection

All clients visiting the weAccess 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:

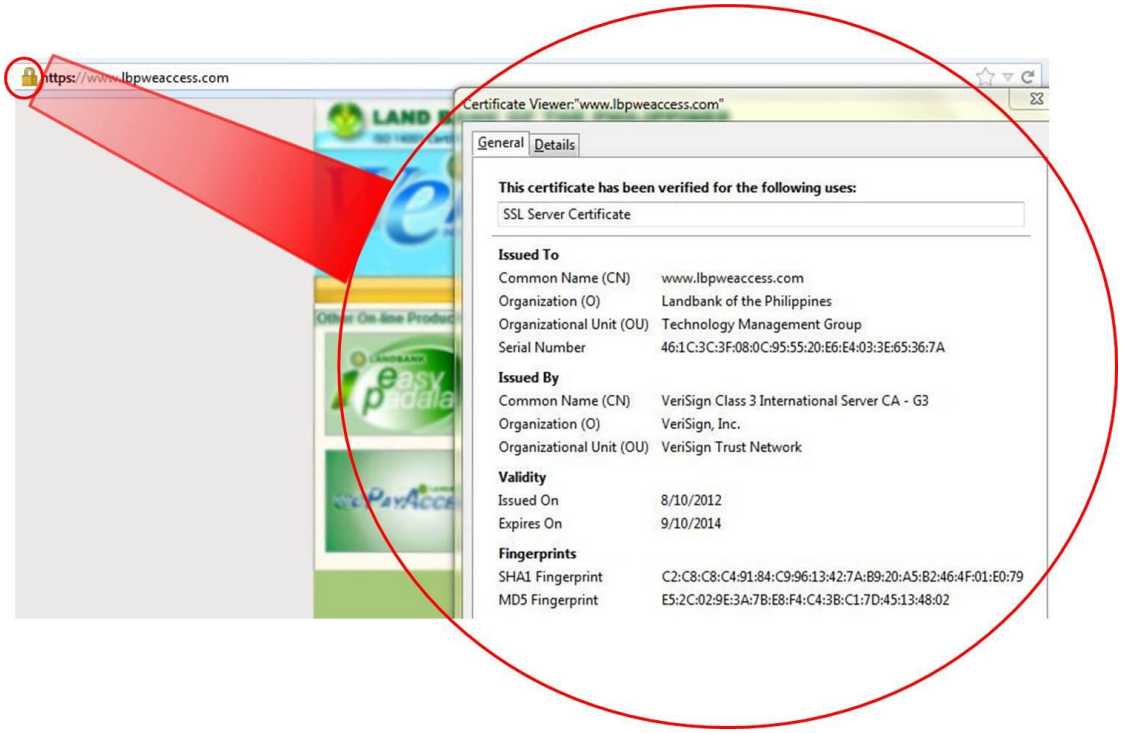
1. Ensure that the site is secured before using it.

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, etc.) by pretending to represent a legitimate company in an email. The email usually claims that it is necessary for the recipient to update and provide the information in the link or form attached in the email. The criminals then use the information entered on the phishing site or form for their own fraudulent intentions.

The official URL of LANDBANK *weAccess is* https://www.lbpweaccess.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 your password confidential at all times.
c. If prompted to change your password, kindly make it a point to change it at once.
d. Disable your 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 your computer's firewall settings.
c. Always update your 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, kindly practice the following:

a. Never adjust your security details.
b. Always log-out from your online session once you are finished with your transaction.
c. Ensure that no one can see your transactions in public.

---

5. Personal information such as address, mother's maiden name, telephone number, social security number, Bank account number and email 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.
