ONLINE BANK SECURITY POLICY

Effective March 2016

Table of Contents

1. Registration

To start using the Tonga Development Bank Online Banking services, you will need to complete an **Access Authority** form authorized by the Bank.

Access Authority forms are available from any of our offices, or you can download a copy from our Web site. Alternatively, you can fill out a form online and then submit it to us for further processing.

2. How safe is Online Banking?

Our Online Banking system is safely protected by various mechanisms, therefore it is very secure to use.

The Internet is merely a tool to provide convenient banking methods to you as a valuable customer of the Bank. There will always be the threat of cybercrime and computer criminals using things like phishing and spyware to try and get their hands on your money or personal information. However, we are very vigilant to ensure that you are protected from unauthorized users, fraud and theft.

Read our **Security Guarantee** statement to see why Online Banking is as safe as a bank.

3. Security Guarantee to Online Banking Users

When you use Online Banking, you can be **confident** that we employ sufficient **security** measures to protect your accounts and personal information.

This is why we **guarantee** that you will not be personally liable for any unauthorized transactions on your TDB accounts, provided that you are:

a. in no way responsible for the unauthorized transaction;

b. did not contribute to the loss; and

c. complied with **TDB's Online Banking Terms and Conditions.**

Two examples of **common internet scams that we are aware of and are particularly vigilant to prevent:**

- Stealing of customer's login details by sending emails which appear to be from the Bank requesting personal details like IDs and passwords; and

- Creating of 'ghost website' to capture customer details which may then be used to transact on customer's account.

The Bank is always implementing new measures to ensure the security of your account and personal information.

If you think you have been the subject of a scam, contact our Customer Service staff to find out how we can help – Phone 23-333 (ext 300) or email tdevbank@tdb.to.

For more information about TDB Online Banking security, read our **TDB Online Banking Terms and Conditions and Online Banking Security Policy.**

4. Features of TDB's Online Banking

With TDB's Online Banking you can:

View your accounts

- see a list of your accounts, current balances and available funds, last statement balance, year-to-date interest;
- view your last 10 debit and credit transactions;
- view and request statement information;
- view your account history for selected periods in various formats;

Transfer funds

- move money between your TDB accounts; and

Update details

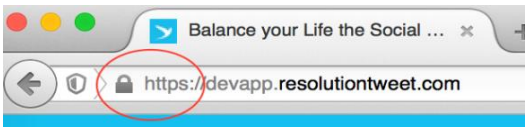
- change your password regularly (for example, every month).

5. Security Measures

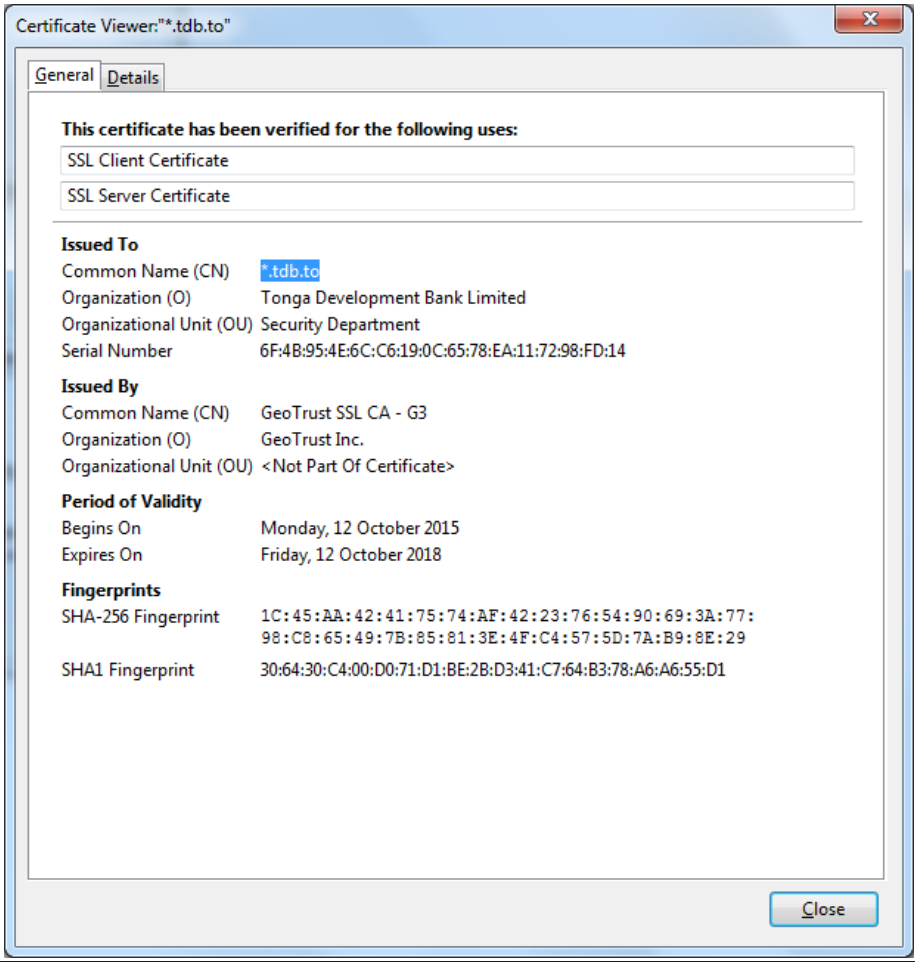
TDB is aware of the risks involved in Online Banking. Listed below are various security mechanisms to help protect your accounts and information:

(a) Check that you are connected to a legitimate TDB web site with data encrypted

- the lock ⇩ symbol should be displayed at the top left corner of our IB log in page;



- the browser (Internet Explorer) should connect with full **SSL 256 Bit** to the **www.tdb.to to encrypt your data;**
- check and confirm your **'digital certificate'** to ensure that you are connected to a legitimate tdb web site; and
- check and ensure that the digital certificate has an Issuer and still valid. Refer TDB digital certificate below.



(b) Use Hyper Text Transfer Protocol Secure (HTTPS)

Ensure that the secure version of **HTTP** is the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of **HTTPS** stands for 'Secure'. It means all communications between your browser and the website are encrypted.

(c) Check that the email request has come from TDB

- Be careful to ONLY ACT upon instructions and advice from legitimate TDB emails. TDB will use the same style, layout, terminology and language in its emails.
- TDB will never ask for personal and login details via email.
- You should never send your personal details via return email under any circumstance. NEVER PROVIDE PASSWORDS IN RESPONSE TO AN EMAIL REQUEST.
- Delete junk emails and do not open email attachments from strangers as they could contain malicious viruses.
- Familiarize yourself with standard TDB emails and how they should appear. Always keep a copy of a legitimate email to compare against any suspicious looking emails.
- Language and text used in emails from the Bank should be professional sounding, using correct terminology and grammar.

(d) Check the fields of the digital certificate

Check the fields of the certificate to ensure that the:

- fields of the digital certificate to ensure that it has been issued to a link ending in "…..tdb.to;"
- 'Issued by' section refers to Geotrust;
- 'date specified' is within a valid date range; and

- validity of the 'digital thumbprint' subject is to TDB….

6. Protection of your financial records

Use the following guidelines to ensure that your financial records are protected:

- always keep your personal details and Bank records and other financial documents in a secure place;
- when throwing out a document, make sure your tax identification number (TIN) is not printed on the document or visible;
- do not disclose your account information over the phone, unless you have made the call yourself;
- be wary of emails or websites which ask you to provide your personal or account information - they may be from a false company;
- keep photocopies of your financial records in a secure place, including the contact numbers of relevant financial institutions, so you can contact them immediately if you suspect fraud or theft; and
- it may be tedious, but ensure you check your bank statements for any transactions you didn't make.

7. Protection of your computer

Use the following guidelines to ensure that your computer is protected:

- install appropriate antivirus software on your computer, and keep it updated. We recommend that you do not use TDB Online Banking until you are sure your anti-virus protection is up to date;
- always sign out of Online Banking and close the browser window;
- try to avoid using public or shared computers (eg at an Internet cafe) as there may by increased exposure to viruses, and these public computers generally contain unauthorized software with minimal security options;

- change the web browser setting of the computer you use for Online Banking to ensure that the Online Banking pages you view are not saved to the computer's hard drive; and
- use recommended software requirements to ensure the highest level of security for your computer.

8. Protection of your password

Use the following guidelines to ensure that your password is protected:

- do not use your Online Banking password for other services (eg - video account, gmail password, mobile phone service);
- change your passwords regularly and never write them down – we recommend every 3 months;
- never disclose details to others. If you do, you may be liable to repay any losses to the Bank due to fraud;
- if you cannot memorise your password and you need to keep it written down, store the information where other people wouldn't think to look;
- keep photocopies of important contact numbers and your records, in a secure place, so you can quickly report suspected fraud or theft;
- destroy any notifications from the TDB containing this information; and
- do not use obvious passwords that others might be able to guess, such as names and phone numbers, birth dates, postcodes, or simple number sequences like 1234.

9. Protection of your privacy

Use the following guidelines to protect your privacy:

- ask what the privacy policy is for the companies you provide your personal/bank details to, and find out how they handle such information to ensure they respect your privacy; and
- ensure these companies protect your privacy by collecting only what is necessary and use this information only for reasons they disclose, i.e. they do not sell your personal details to marketing companies.

10. Protection from identity theft

Identify theft occurs when your personal information is obtained without your knowledge or consent and is used to commit fraud or theft. Thieves and fraudsters seek to use your personal and/or banking information to obtain credit and steal money in your name. If this occurs, it can be very difficult to prove your innocence and restore your credit rating. It is not possible to completely eliminate the risk of fraud or theft, but here are some ways to mitigate the risk.

Use the following guidelines to protect yourself from identity theft:

- do not disclose personal information or banking details to anyone over the phone, through the mail, or over the internet unless you have initiated the contact or are sure who you are talking to;
- always check your bank statements and accounts for any transactions that look suspicious;
- shred any receipts or documents that contain personal information;
- do not distribute personal information on social networking sites;
- ensure that the Bank always has your current contact details, including work and mobile phone number;
- update your anti-virus software and scan your PC regularly to reduce your risk becoming a victim of online fraud, phishing emails or ghost websites. Cyber viruses can capture your personal information, banking and business details; and
- if you suspect that your security or personal information has been compromised or your have noticed a transaction that you did not initiate, contact the Bank immediately.

11. Recommended Log-in Procedure

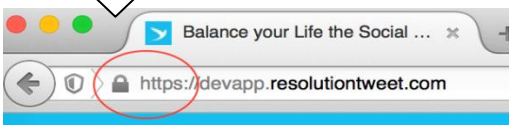
Outlined below is the recommended log in procedure for the Bank's Online Banking:

(a) Access Online Banking correctly

Always access the Bank's Online Banking system by typing www.tdb.to. Never access the Bank's Online Banking system through a link such as: http://www.tdb.to/2015-campaigns-new-home-loans-offer-just-5-in-the-first-2-years.

(b) Before enter your access number and password:

- check that the lock symbol is at the top left corner;



- position the mouse on the lock symbol to ensure you are connected on SSL Secured 256 Bit;
- double click on the lock and confirm the Bank's Digital Certificate and Fingerprint Certificate details.
- do not log into the Online Banking system if any of the details listed above is different to what the Bank has provided. Contact the Bank immediately to resolve any issues before continuing; and
- always sign out of Online Banking and close the browser window.

12. Other Security Tips

Listed below are additional security tips which are useful:

- As a precaution, cross-check all transactions in your Online Banking accounts against your paper account statements;
- If necessary, order up-to-date paper statements. This should help you spot any suspicious transactions;
- Consider setting up a separate accounts with a minimum monthly balance for Bill payments;
- Users should read and understand the Banks "Online Banking Term and Conditions;"
- Do not disclose any information relating to your financial identity over the phone. It is better to initiate communication when you wish to discuss your financial information or identity;
- Do not leave your PC unattended if you are online. Always complete your financial transactions and log out; and
- Contact a TDB Customer Service Staff immediately if you think someone is using our bank accounts.

13. Recommended browsers

In order to access the new TDB Online Banking system, please make sure that you are using the most recent version of your preferred browser. This will ensure the highest level of security for you and provide a better online experience.

Browser	**Internet Explorer**	**Firefox**	**Chrome**	**Safari**
Minimum Version	8	3.5	16	5
Operating System	Win8, Win7, Vista	Mac, Win8, Win7, Vista	Mac, Win8, Win7, Vista	Mac

If you are having problems using our site, please call us on **23-333** (9am - 4pm, Monday to Friday).

To ensure you have the latest browser update, please refer to:

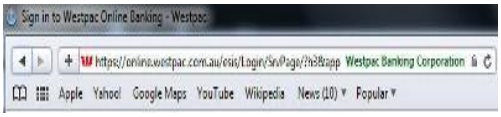
- Internet Explorer - www.microsoft.com/ie
- Firefox - www.firefox.com
- Chrome - www.google.com/chrome
- Safari - www.apple.com/safari

Internet Explorer

Firefox

Chrome

Safari



14. Support services

Online help

- We offer help and support between the hours of 9:00 a.m. and 4:00 p.m. Monday to Friday on business banking days.
- When you are using Online Banking, help is available at the click of a button. Simply select the help symbol pictured at the top of the screen, to display step-by-step instructions and information about the function you are using.

Phone us

- Call the TDB's Online Banking help desk on **23-333 ext 300** to speak directly with a Customer Service officer.
- Technical assistance is available 9:00 a.m. and 4:00 p.m. Monday to Friday on business banking days.

Go to a TDB branch

Our branch staff is able to answer any questions about Online Banking. Please feel free to visit any of our branches in Nuku'alofa, Vava'u, Ha'apai or 'Eua.

15. Mobile Banking Security

Our security guarantee

TDB Mobile Banking provides the same high level security as our Online Banking. And our security guarantee means we'll refund your money if your account is compromised due to internet fraud, as long as you comply with our Online Banking Terms and Condition. This includes keeping your access codes and passwords private.

Mobile security tips

Here are some simple things you can do to keep yourself secure online:

- ✓ Download and install reputable mobile anti-virus software to your device (if your operating system permits).
- ✓ Lock your phone when not in use. The password protects your device so that nobody else can use it or view information. Also, be sure to always store your device in a safe location.
- ✓ Lost or changed your mobile phone number? Call Customer Services **23-333 ext 300** in order to change your TDB Mobile Banking Details. We suggest this is one of the first things you do.
- ✓ Clear your mobile frequently by deleting text messages from financial institutions, especially before sharing, discarding, or selling your device.
- ✓ Watch what you send via your phone - never disclose via text message any personal information such as account numbers, passwords, or personal information that could be used in access codes theft.
- ✓ We recommend that you install mobile security software if available.
- ✓ Stick with a secure network by ensuring wherever possible that all internet connections are password protected.
- ✓ Use trusted applications and always download mobile applications from reputable sources. If you are suspicious about the authenticity of a mobile banking app, visit us at any of our branches or contact us on **23-333 ext 300**.

16. Additional things you should know

TDB Mobile Banking applications are only available for use by TDB customers. Internet connection is needed to access TDB Mobile Banking.

17. Fees and Charges

Conditions, fees and charges apply. These may change or we may introduce new ones in the future. Full details are available on request. Lending criteria apply to approval of credit products. This information does not take your personal objectives, circumstances or needs into account. Consider its appropriateness to these factors before acting on it. Read the disclosure documents for your selected product or service, including the **Terms and Conditions** before deciding.