Security Measures on TMB-Mobile Banking

On TMB M-Banking your information is protected by the following security measures:

- The Download of TMB - Mobile app is restricted after one successful download from a registered user.
- In any re-download scenario, the Customer will have to request the bank through any registered means of communication.
- TMB Mobile app cannot be used with a different sim card or different handset other than the registered one.
- TMB mobile app doesn't store personal account information on mobile devices, so your accounts are not exposed if your phone is lost or stolen
- When you use TMB mobile app, your information is protected by 128-bit encryption, just as when you bank online
- TMB mobile app always requires an activation code at the first login after download. The activation code can be generated only once by a registered user by sending SMS to 9282112225. No activation code can be used twice.

Secured Download

- When downloading the TMB Mobile app to your mobile device, be sure to go to a trusted source such as the App Store on the IPhone or Google's Android Market. You can alternately SMS to 9282112225 and click on the download URL in the response SMS and install the application. Do not download the app from any other third party source.

Information security – Do's and Don'ts

- Password-protect the mobile phone and set the maximum number of incorrect password submissions to no more than three.
- *Choose a complex password.* Do not use personal details like date of birth, names and common patterns (123, 111, 222 etc) while choosing your password. Make it totally non-guessable and change your PIN and login PASSWORD for your TMB M-Banking app periodically
- Do not store your bank account number or Transaction PIN or Login password on your mobile phone
- Don't Reveal or write down PINs or retain any email or paper communication from your bank with regard to the PIN or password
- Be careful when typing out your account number , MPIN or password details on the mobile phone, especially while using the phone in a public spot, to prevent shoulder surfing.
- Please report the loss of mobile phone to the bank so that we may disable the access to your account through TMB Mobile app.
- Never share your personal information (e.g. PAN, credit /debit card numbers, date of birth, mother's maiden name or any other personal information) over the phone, mail /SMS or on the internet unless you have a trusted business relationship with the company.
- Do not root or jailbreak your mobile device to get around limitations set by your carrier or device manufacturer. It may remove any protection built into the device to defend against mobile threats
- Beware of everything you download onto your Smartphone, especially applications. Only use reputed applications from the market/store.
- *Review account statements frequently to check for fraudulent transactions.*
- Never connect your mobile phone through an unsecured Wi-Fi connection available in public places such as airports etc.
- Don't open every SMS / MMS as it may contain viruses, especially from unknown sources.
- Never accept offers such as caller tunes or dialer tunes from unknown sources.
- Try and avoid using Bluetooth in public places, as someone can access your confidential data / information.
- Never open / download emails or attachments from unknown sources.
- Be careful about the websites you are browsing. If it does not sound authentic, do not download anything from it.
- Never forget to inform your bank about any changes in your mobile number, to ensure SMS notifications are delivered to the intended person only.
- Don't install third-party banking apps, without the bank's consent.
- Always take a backup of your Smartphone data.

- Always keep the bank's customer care number in reach for emergencies.
- Register for SMS alerts to keep track of your banking transactions.
- Delete junk message and chain messages regularly
- If you have to share your mobile with anyone else or send it for repair/maintenance
    - Clear the browsing history
    - Clear cache and temporary files stored in the memory as they may contain any sensitive information
    - Block your mobile banking applications by contacting your bank. You can unblock them when you get the mobile back
- Avoid giving verification details to banking officer in public place when you call the bank for a genuine reason.
- Once you have completed your mobile banking transactions, remember to log-off by clicking on the exit option.
- Carefully check the IFSC code of bank and account number of beneficiary before making any payment.
- If you have been victimized by cellular fraud, please file a complaint with your mobile phone service provider and the law enforcement agency

SMS (smishing) Alert

'SMiShing' is used to describe phishing attempts over text messages (SMS). This occurs when a fraudster sends you a SMS/text message asking you to provide sensitive, personal, and/or financial information via a web link and false website, or a telephone number.

- Don't respond to text messages or automated voice messages from unknown or blocked numbers on your mobile phone.
- Don't enable the feature in Android to install applications from 'Untrusted Sources'
- User awareness – don't download anything unless you trust the source.
- When buying online, use a legitimate payment service and always use a credit card because charges can be disputed if you don't receive what you ordered or find unauthorized charges on your card.
- Don't respond to unsolicited e-mails, texts or phone calls requesting personal information.
- Never click on links or attachments contained within unsolicited e-mails.
- While visiting a merchant's website, type the URL directly into your browser's address bar.

Mobile Security

Mobile Security effectively protects your mobile device from all common mobile threats. It guards against loss and theft, keeps your device free of malware and lets you browse the web/apps safely.

Mobile Security keeps you safe from malware and malicious apps.

- Install anti-virus/anti-malware software on your mobile phone.
- Configure the anti-virus software to automatically notify you when new updates are available for download
- Perform a complete scan of your mobile phone at least once a week
- Configure the anti-virus software to scan all in-coming and out-going sms/mms/emails.

Contact your mobile handset vendor for authorized Mobile security software's.

Some standard Mobile security softwares are listed below,

1. AVG Antivirus Security
2. McAfee Antivirus & Security
3. Avast Mobile Security
4. Symantec Mobile Security
5. Norton Security
6. Kaspersky Mobile Security Lite
7. NetQin mobile Guard – for Symbian OS S60 Devices