TELANGANA GRAMEENA BANK

INTERNET BANKING WITH TRANSACTION RIGHTS

Tips to protect against Online Fraud and Phishing Variations

- **Be suspicious** of any e-mail or text message containing urgent requests for personal or financial information. (TGB and most other financial institutions and credit card companies normally will not use e-mail to confirm an existing client's information).
- Contact the organization by using a **telephone number from a credible source** such as a phone book or a bill.
- If you receive an email claiming to be from TGB that appears to be suspicious, **do not click on any links** it provides or reply to it – simply delete it.
- **Avoid embedded links** in an e-mail claiming to bring you to a secure site.
- **Never disclose** via text message any personal information, including account numbers, passwords, or any combination of sensitive information that could be used fraudulently. Use caution if you receive a text message expressing an urgent need for you to update your information, activate an account, or verify your identity by calling a phone number or submitting information on a web site. These messages may be **part of a phishing scam** conducted by fraudsters to capture your confidential account information and commit fraud.
- Get in the habit of looking at a **website's address line** and verify if it displays something different from the address mentioned in the email.
- Regularly update your computer protection with **anti-virus** software, spyware filters, e-mail filters and firewall programs.
- As a general rule, **be suspicious** when receiving any unsolicited incoming communication/phone call asking your personal or financial information or asking to update them on a site. Contact your Bank directly through official channels available to verify authenticity of those calls.
- Do not share any confidential information through suspicious emails, websites, social media networks, text messages or phone calls.
- Always use latest web browser.
- Your online banking username or password should not be the same as other online accounts.
- Regularly check you bank debit card statements to ensure that all transactions are legitimate.

Report It

If you receive one of these suspicious e-mails:

Report it to inb_mb@tgbhyd.in or the institution that it appears to be from.

If you received one of these suspicious e-mails and you unwittingly provided personal information or financial information, follow these steps:

- **Step 1** - Contact your bank.
- **Step 2** - Contact your local police.
- **Step 3** - Always report phishing. If you have responded to one of these suspicious e-mails, report it to

Protecting You Online

At TGB we use the highest industry standard for security. And we constantly review it to counter any new security threats.

Here are some of the steps we take to protect you while you’re banking online.

When you login:

- Access to your accounts is controlled by your unique username and password.
- Your access is suspended after three invalid login attempts.
- We show you the date and time of your last login so you know that no one else has accessed your accounts.

While you're banking online:

- We have 128-bit SSL encryption to keep your information secure. This basically means your information travels over the internet as a sophisticated code that only we can unscramble.
- "Transaction OTP" provides you with an extra layer of protection when making payments online, adding third parties etc. This One Time based SMS password validates your identity and processes a transaction through.

When you're finished:

- You are automatically signed off from your account if it's inactive for a set period of time.
- All pages you visit in our online banking websites are automatically removed from your browsers cache after you have logged off. This removes the opportunity for later users of that computer to view your personal or account details by, for example, selecting the browser back button or searching the contents of the computer's hard-drive.

Security experts at TGB behind the scenes

- Our dedicated security team investigates new technologies, monitors activity and responds promptly to any emerging security issues.
- We regularly use reputable independent consultants to audit the security of all our systems.
- Regular intense security drilling carried out as part of our efforts to look into any possible security concern and immediately address them.

Safe Online Banking

Select a suitable password.

- Unique Characters: An acceptable password must have at least eight (8) different characters. Repeated characters can make for palindromes and make it easier to crack.
- Character Types: An acceptable password must have characters from at least three (3) different character types -- upper case, lower case, digits, punctuation, etc. A password that includes a sample from a rich character set is difficult to crack.
- Long Alpha Sequences: An acceptable password must not have an alphabetic sequence any longer than three (3) characters.
- Long Digit Sequences: An acceptable password must not have a digit sequence any longer than two (2) characters.
- Forbidden Characters: There are a few characters that will cause problems if used in a password - the "delete" character is one of the obvious ones.
- Passwords should not be any of the following:
    - Dictionary words (including foreign and technical dictionaries)
    - Name of a person or a thing, a place, a proper noun, a phone number or a vehicle number
    - Simple pattern of letters on keyboards
    - Any of the above reversed or concatenated
- One possible method for picking a good password is to make up your own acronym.

Always protect your password

- Sharing passwords is a security risk.
- Do not divulge your password to anyone.
- Enter your user-id and password only in the space provided for- that you are normally used to.
- Any changes from normal make sure there is no attempt to steal your personal information before providing it.
- Do not provide user-id and passwords on any page that appears as a popup when you click on a hyperlink received through email. Better practice would be to log on to the service by typing in the URL in the address bar after making sure the page opening up is from the genuine service provider.
- Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
- Change passwords at least once every 90 (ninety) days.
- Do not let your computer remember your password. Do not accept auto complete option provided by your computer/ browser.
- As far as possible do not use un-trusted system to access a sensitive service. If you must, change the password on the first occasion immediately thereafter from a trusted system

Remember to logout

- Ensure to log out when you are done with our online banking services by clicking on "logout". Then close the browser window.

Check that the website is secure

- Always visit the INB Site from through our Bank’s Website.
- On the login page, you will see a pad lock somewhere on the browser window (mostly in the end of the address bar or on the right hand down corner in a locked in position indicating that the website you are visiting is genuine and your communication with us (OnlineTGB) is high grade encrypted. Click on the padlock to view the security certificate.
- Look out for URL address on the address bar of your internet browser begins with "https"; the letter 's' at the end of "https" means 'secured'.

Be careful with emails

- Never download attachments or click on embedded links on emails from unknown sources. Be Suspicious of emails that seek your personal or financial information.
- Check the validity of the emails claiming to be purported from a financial institution by contacting the organization in person or by phone or through secured mail box.
- TGB never sends email /SMS or makes phone calls for getting customer information. Please report immediately if you receive any e-mail purported to be originated by TGB to gather your Username or Password or any other personal information.

Secure your computer

- Use a personal firewall.
- Install antivirus software and keep it updated with the latest signatures.
- Get antispyware software.
- Regularly update your OS
- Beware of public or shared computers.

Features for Safe Online Banking

OnlineTGB provides several inbuilt features for safe and secure banking. You can use the security options in the profile tab to:

Customize your Personal Profile

You can set your display name, mobile number and email ID in your personal profile. The display name is used in the Welcome message.

Manage Third Party

You can define your own trusted third parties to whom you wish to transfer funds. You can also add, delete or modify your list of trusted third parties.

Define Limits

You can set limits for fund transfers, in the profile section. It is advisable to set a lower limit. You can enhance the limit as and when required.

Types of Online Fraud and Phishing Variations

Phishing Email and Fraudulent websites

Phishing is a general term for e-mails, text messages and websites fabricated and sent by criminals and designed to look like they come from well-known and trusted businesses, financial institutions and government agencies in an attempt to collect personal, financial and sensitive information. It’s also known as brand spoofing. If you should ever receive an email that appears to be suspicious, do not reply to it or click on the link it provides. Simply delete it. To report a suspicious email that uses TGB’s name, you can report to us immediately at inb_mb@tgbhyd.in.

Popup windows/advertisements

Pop-ups are the advertisements that "pop up" in a separate browser window. When you click on some of these pop-ups, it's possible that you're also downloading "spyware" or "adware."

Vishing

Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private, personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing.

Scammers randomly dial phone numbers using an automated system or a real human being pretending they are calling on behalf of Bank/financial company asking you to update information regarding your, bank accounts, Card details etc. because there is a problem on your account or they may also say that they have made some upgrades into their system.

Smishing

Smishing is a form of criminal activity using social engineering techniques similar to phishing. Smishing victims receive SMS messages. Known as "smishing," these text messages might ask a recipient to register for an online service -- then try to sneak a virus onto the users' device. Some messages warn that the consumer will be charged unless he/she updates his/her personal or financial credentials in a Web site that then extracts such information and other private data.

Key logging

Unwanted Key-Logging software can record everything that is typed on a computer and send the information to an outside party. Key-Logging "Spyware" or "Adware" often infects a computer via a virus attached to an e-mail or other type of download.