



தமிழ்நாடு கிராம வங்கி
TAMIL NADU GRAMA BANK
(A Government owned Bank Sponsored by Indian Bank)

CYBER AWARENESS



Be safe in your Cyber Behavior

- ▶ **NEVER** respond to any popups, emails, SMS or phone calls, no matter how appealing or official looking, seeking your personal information such as username, password(s), PINs, mobile number, ATM Card details, Credit Card details etc. Such communications are sent or created by fraudsters to trick you into parting with your credentials.
- ▶ Beware of Malicious/ Illegal Loan App/Websites
- ▶ Tamil Nadu Grama Bank (TNGB) advises the customers to refrain from operating illegal Apps and not to fall prey to the illicit activities so that it ensures their better security and online safety.

Beware of Malicious/ Illegal Loan App/Websites

- ▶ Tamil Nadu Grama Bank advises the customers to refrain from operating illegal loan Apps and not to fall prey to the illicit activities of the illegal lending Apps curbing illegal acts of the unregistered lending Apps so that it ensures their better security and online safety.

Security Alert to the Customers and General Public

- ▶ Tamil Nadu Grama Bank never sends any such emails/ SMS asking for confidential/personal details of any customers. Please report immediately on headoffice@tngb.co.in if you receive any e-mail purported to be originated by Tamil Nadu Grama Bank to gather your Username, Password, Card Details, OTP or any other personal information. This may be a Phishing mail.
- ▶ User ID and password for Net Banking Web sites, ATM Card, Credit Card, Debit Card Numbers and their respective PINs and online financial information such as Bank account number etc. are highly confidential. Do not part with them.
- ▶ Do not click on any unknown link to access our web site. Always type <https://tamilnadugramabank.in/> [or] <https://netbanking.tngb.in> at the browser address field to access the web site/ net banking page of Tamil Nadu Grama Bank.

Beware of Phishing

- ▶ There has been increasing incidences of phishing recently which targets the customers of leading banks throughout the world including our Bank. Hence to alert the customers on such attacks which actually start through a spoofed e-mail purported to be sent by the Bank, we give below the modus operandi of the attacks, how they are perpetrated to get the personal credentials from unsuspecting customers and also how to avoid becoming victims to such attacks.

Beware of Phishing

- ▶ Phishing is a form of cyber-attack in which scammers/attackers make Internet users divulge with sensitive information about their bank accounts and personal details. A common online phishing scam starts with a spoofed e-mail message that looks like an official notice from a trusted source, such as a bank, credit card company, or reputable online merchant. Such spoofed mails would tell the recipients to validate or update their personal credentials failing which their accounts would become inactive and direct them to a website that looks like the genuine organisation's website. If unsuspecting customers follow the links in the mail and submit their personal credentials, those details would be actually going to the fraudsters who later use the credentials for placing the orders, services, transferring money from the accounts, etc, leading to identity theft.