J&K Grameen Bank
Head Office
Narwal Line
Pin-180006
P : 8899006461
P: 7051510171, 7051510172
E: it.hoj@jkgb.in
W: www.jkgb.in

Ref No : JKGB/IS CELL/2022-3357

February 18, 2022

Public Notice regarding Safe Digital Banking Practices

In view of defrauding and misleading techniques being used by unscrupulous elements to obtain confidential details like user id, login / transaction password, OTP (one time password), debit card details such as PIN, CVV, expiry date and other personal information, Bank cautions all its customers to be aware of fraudulent messages, spurious calls, unknown links, false notifications, unauthorized QR Codes, etc. promising help in securing concessions / expediting response from bank in any manner. All the customers are advised to follow safe Digital Banking practices by adopting measures:

- Never share your account details such as account number, login ID, password, PIN, UPI-PIN, OTP, ATM / Debit card details with anyone, not even with bank officials, howsoever genuine they might sound.
- Any phone call / email threatening the blocking of your account on the pretext of non-updation of KYC and suggestion to click link for updating the same is a common modus operandi of fraudsters. Do not respond to offers for getting KYC updated / expedited. Always access the official website of the bank (i.e. https://www.jkgb.in) or contact the branch.
- Do not download any unknown app on your phone / device. The app may access your confidential data secretly.
- Transactions involving receipt of money do not require scanning barcodes / QR codes or entering MPIN. Thus, exercise caution if asked to do so.
- Always access the official website of bank for contact details. Contact numbers on internet search engines may be fraudulent.
- Check URLs and domain names received in emails / SMSs for spelling errors. In case of suspicion, notify Bank/local police / cybercrime branch immediately.
- If you receive an OTP for debiting your account for a transaction not initiated by you, inform bank immediately. If you receive a debit SMS for a transaction not done by you, inform bank immediately and block all modes of debit, including UPI. If you suspect any fraudulent activity in your account, check for any addition to the beneficiary list enabled for digital banking.

- Do not share the password of your email linked to your bank account. Do not have common passwords for e-commerce / social media sites and your bank account / email linked to your bank account. Avoid banking through public, open or free Internet networks.

- Do not set your email password as the word “password” while registering in any website / application with your email as user-id. The password used for accessing your email, especially if linked with your account, should be unique and used only for email access and not for accessing any other website / application.

- Do not be misled by advices intimating deposit of money on your behalf with Bank for foreign remittances, receipt of commission, or wins of lottery.

- Regularly check your email and phone messages for alerts from your Bank. Report any un-authorized transaction observed to your bank immediately for blocking the card / account, so as to prevent any further losses.

- Secure your cards and set daily limit for transactions. You may also set limits and activate / deactivate for ATM/eCOM/POS use. This can limit loss due to fraud.

General Manager
J&K Grameen Bank