Safe Digital Banking Practices

Jana Small Finance Bank
A SCHEDULED COMMERCIAL BANK

- Never share your account details such as CRN, account number, internet banking login ID/password, or mobile banking MPIN, UPI-PIN, OTPs, debit card details/PIN with anyone, including Jana Small Finance Bank's (the "Bank") officials, no matter the however genuine they might sound.
- Any phone call/email threatening to block your account/debit card on the pretext of non-updation of KYC and any suggestion to click a link for updating the same is a common modus operandi of fraudsters. Do not respond to such offers for getting KYC updated/expedited. For any clarification/ details, kindly visit the official website of the Bank at https://www.janabank.com/ or contact the Bank branch or contact centre at 1800 2080.
- Do not download any unknown app on your phone/device. The app may access your confidential data secretly.
- In transactions involving receipt of money, you are not required to scan barcodes/QR codes or enter MPIN. Thus, exercise caution if you are asked to do so, since entering the UPI PIN/ MPIN may result in debit of account.
- Always access the official website of a bank/NBFC/financial provider for getting their contact details. Contact numbers on internet search engines may be fraudulent and might not be genuine.
- Check URLs and domain names received in emails/SMSs for spelling errors. Use only verified, secured, and trusted websites/apps for online banking, that is, websites starting with "https". Kindly notify the local police/cybercrime branch immediately if you come across any suspicious URL, domain name, website and/or app.
- If you receive an OTP to debit your account for a transaction not initiated by you, inform your bank/e-wallet provider immediately. If you receive a debit SMS for a transaction not done, inform the Bank immediately to 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 internet / mobile 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 networks.
- Secure your cards and set daily limits for transactions. You may also set limits and activate/deactivate for domestic/international use. This may limit the loss due to fraud.

Safe Practices for using Jana Bank Mobile Banking

- Do not share your MPIN/OTP with anyone.
- Keep your phone locked while not in use.
- Change your mobile banking PIN frequently.
- Inform the Bank immediately in case of any suspicious transactions.
- Avoid using unsecured Wi-Fi, public or shared networks.
- Do not use 'jail broken' or 'rooted' devices for online banking.
- You can lower the debit card transaction limit under 'Manage Limit' section, if your debit card usage is limited.
- Do not ignore Bank's alerts/communications sent to your registered mobile number/email ID.
- Never download and install apps from untrusted sources. Only use play store/app store for downloading and installing apps.
- In case you lose your mobile phone, please call the Bank's 24-hour customer care number 1800-2080 or email us at customercare@janabank.com to deregister from mobile banking.

Safe Practices of Jana Bank Internet Banking

- Do not share your internet banking login password/OTP with anyone.
- Change your internet banking password frequently.
- Inform the Bank immediately in case of any suspicious transactions.
- Avoid using unsecured Wi-Fi, public or shared networks.
- You can lower the debit card transactions limit under 'Manage Limit' section, if your debit card usage is limited.
- Do not ignore the Bank's alerts/communications sent to your registered mobile number/email ID.
- Never download and install apps from untrusted sources. Only use Play Store/App Store for downloading and installing apps.

****