प्रेस प्रकाशनी PRESS RELEASE

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

वेबसाइट : www.rbi.org.in/hindi
Website : www.rbi.org.in
ई-मेल/email : helpdoc@rbi.org.in

संचार विभाग, केंद्रीय कार्यालय, एस.बी.एस.मार्ग, फोर्ट, मुंबई-400001
Department of Communication, Central Office, S.B.S.Marg, Fort, Mumbai-400001
फोन/Phone: 022- 22660502

January 28, 2022

Consumer Awareness - Cyber Threats and Frauds

It has come to the notice of Reserve Bank of India that unscrupulous elements are defrauding and misleading members of public by using innovative modus operandi including social media techniques, mobile phone calls, etc. In view of this, the Reserve Bank cautions members of public to be aware of fraudulent messages, spurious calls, unknown links, false notifications, unauthorized QR Codes, etc. promising help in securing concessions / expediting response from banks and financial service providers in any manner.

Fraudsters attempt to get confidential details like user id, login / transaction password, OTP (one time password), debit / credit card details such as PIN, CVV, expiry date and other personal information. Some of the typical modus operandi being used by fraudsters are -

- Vishing - phone calls pretending to be from bank / non-bank e-wallet providers / telecom service providers in order to lure customers into sharing confidential details in the pretext of KYC-updation, unblocking of account / SIM-card, crediting debited amount, etc.

- Phishing - spoofed emails and / or SMSs designed to dupe customers into thinking that the communication has originated from their bank / e-wallet provider and contain links to extract confidential details.

- Remote Access - by luring customer to download an application on their mobile phone / computer which is able to access all the customers' data on that customer device.

- Misuse the 'collect request' feature of UPI by sending fake payment requests with messages like 'Enter your UPI PIN' to receive money.

- Fake numbers of banks / e-wallet providers on webpages / social media and displayed by search engines, etc.

RBI urges the members of public to practice safe digital banking by taking all due precautions, while carrying out any digital (online / mobile) banking / payment transactions. These will help in preventing financial and / or other loss to them.

Press Release: 2021-2022/1630

(Yogesh Dayal)
Chief General Manager

SAFE DIGITAL BANKING PRACTICES

- Never share your account details such as account number, login ID, password, PIN, UPI-PIN, OTP, ATM / Debit card / credit card details with anyone, not even with bank officials, however 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 your bank / NBFC / e-wallet provider 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 / NBFC / e-wallet provider for contact details. Contact numbers on internet search engines may be fraudulent.

- 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''. In case of suspicion, notify local police / cybercrime branch immediately.

- If you receive an OTP for debiting 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 your bank / e-wallet provider 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 internet / mobile banking.

- Do not share the password of your email linked to your bank / e-wallet 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.

- 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 RBI for foreign remittances, receipt of commission, or wins of lottery.

- Regularly check your email and phone messages for alerts from your financial service provider. Report any un-authorized transaction observed to your bank / NBFC / Service provider immediately for blocking the card / account / wallet, 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 domestic / international use. This can limit loss due to fraud.