Customer Awareness - Cyber Threats and Fraud

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 of India (RBI), 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 –

- Phishing /Vishing/ SMiSHing **-** Fraudulent techniques deployed via fake emails/phone calls/SMS respectively to deceive the customers into thinking that the communication is from their bank / trusted entity. Fake emails & SMS may contain harmful links which can extract confidential information or launch malware. Customers are lured into sharing confidential details in the pretext of KYC-update, job application, unblocking of account / SIM-card,filing Income Tax Returns, lapsing reward points, cashback offers, etc.

- Remote Access – Fraudster lures customer to download an application on their mobile phone / computer which can access all the customers' data via customer device.

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

- Fake helpline /customer care contact details - Fake numbers of banks / e-wallet providers on webpages / social media are 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.

Safe Digital Banking Practices

1. 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.
2. 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.
3. Transactions involving receipt of money do not require scanning barcodes / QR codes or entering MPIN. Thus, exercise caution if asked to do so.
4. Always access the official website of bank / NBFC / e-wallet provider for contact details. Contact numbers on internet search engines may be fraudulent.
5. 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.
6. 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.
7. 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.

For more info Visit: https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=5318.