Consumer Awareness - Cyber Threats and Frauds

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.

SAFE DIGITAL BANKING PRACTICES

1. DO NOT SHARE YOUR PERSONAL INFORMATION

- Never share your account details such as account number, login ID, password, PIN, UPI-PIN, OTP, CVV number, Expiry date, ATM / Debit card / credit card details, Mobile and Internet Banking Password, MPIN,TPIN and QPIN, Aadhar Card and PAN Card details with anyone, not even with bank officials, however genuine they might sound. Never share this information to anybody on phone/SMS/email.

2. DO NOT RESPOND TO ANY FAKE CALL OR ANY OFFER

- 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. DO NOT DOWNLOAD ANY UNKNOWN APP

- Do not download any unknown app on your phone / device. The app may access your

confidential data secretly.

4. DO NOT SCAN BARCODE OR QR CODE WHERE NOT REQUIRED

- Transactions involving receipt of money do not require scanning barcodes / QR codes or entering MPIN. Thus, exercise caution if asked to do so.

5. ALWAYS ACCESS OFFCIAL WEBSITES

- Always access the official website of bank / NBFC / e-wallet provider for contact details. Contact numbers on internet search engines may be fraudulent.

6.USE ONLY SECURED AND TRUSTED WEBSITES

- 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.

7.DON'T DO ANY SUSPIOUS TRANSACTIONS

- 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.

8.DO NOT SHARE YOUR PASSWORD

- 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.

9.DO NOT MISLED BY ANY ADVICES

- 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.

10.REPORT IMMEDIATELY FOR ANY UN-AUTHORIZED TRANSACTIONS

- 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.

11. SECURE YOUR TRANSACTIONS

- 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.

12. LOCK YOUR PRIVACY SETTINGS ON SOCIAL MEDIA

- Fraudsters can use social media profiles to figure out your passwords and answer security questions to reset your password. Lock your privacy setting on social media and avoid posting things like birthdays, address, mother name, etc. Do not answer to request from unknown person.

13.SECURE AND PROTECT YOUR INTERNET CONNECTIONS

- Always protect your home & Office wireless network with a strong password. Be cautious while using public Wi-Fi networks.

14.KEEP YOUR MOBILE DEVICES AND COMPUTERS UPDATED

- Always keep updated operating system, browsers, anti-virus software of computer/ laptops / tabs/ smart phone .

15. USE OF ANTI VIRUS SOFTWARE

- Always install a good quality paid Anti-Virus / malware software in your device.

16.SET STRONG PASSWORDS

- Always set strong passwords for your devices. A strong password is at least 8 characters in length and includes mix of capital & lower case letters, minimum one number and minimum one special character.