CYBER SECURITY AWARENESS

Some unethical and exploitative elements are defrauding and misleading members of public by using innovative modus operandi including social media techniques such as fraudulent messages, spurious calls, sending unknown links, false notifications and unauthorized QR codes. In view of this, the Reserve Bank of India cautions general public to practice safe digital banking by taking all due precautions while carrying out digital banking / payment transactions thereby preventing financial and/or other loss to them.

Steps for Safe Digital banking:

- Never ever 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 sound. Since banks never asks for such details.
- Do not respond to phone calls / emails threatening blocking of your account, getting KYC updated and never click suggested link for updating the same. Always access official website of your bank or contact the branch.
- Do not download any unknown app on your phone / device from untrusted / unfamiliar sites since it may access your data secretly. Always seek legitimate information from authentic government, university, hospital & news sites known to you.
- Never enter UPI PIN and / or scan barcodes / QR codes to receive money, if asked to do so.
- Strictly avoid clicking any links received via email to prevent phishing attacks. Check email or web address for spelling errors and delete immediately if there are any inconsistencies. Use only secured, verified and trusted web-sites / apps for online banking.
- Check validity of any email that asks you to submit / share personal or financial information.
- If you receive an OTP for debiting your account for a transaction not initiated by you and/or if you receive a debit SMS for a transaction not done, inform your bank immediately and block all modes of debit, including UPI.
- Do not share the password of your email linked to your bank / e-wallet account.
- Use virtual keyboard shown on the screen, to enter passwords.
- Do not have common passwords for e-commerce / social media sites and your bank account / email linked to your bank account.
- Use strong/unique passwords for login to your personal desktops, laptops. Use separate logins/passwords for systems and putting through financial transactions. Do not repeat/reuse passwords. Change passwords at regular intervals.
- Do not be misled by emails / SMSs intimating deposit of money, wins of lottery, freebies and / or redeeming of points earned etc.
- Do not click / forward social media messages on Covid pandemic, religious messages assuring good luck if forwarded to your contacts etc.
- Deny permissions to unknown utility apps asking for access to your media & other sensitive information such as your address book/contact details/photo gallery.

- Secure your plastic money (ATM Debit/credit cards) by setting daily limits and activate / deactivate features such as domestic / international use, card-less online transactions etc.
- Regularly check your email and phone messages for alerts related to your bank transactions received from your bank and other financial service providers to prevent/mitigate losses.

Report Fraud/Un-Authorized transaction

If you are a victim of Financial Cyber Fraud, Call customer support number 1800220199/ or alternatively reach out to the National Cyber Crime Portal cybercrime.gov.in or dial Helpline Number **1930.**