RBI Kehta hai....

Jaankar Baniye,
Satark Rahiye!”

RBI Kehta hai....

There cannot be a better custodian of customer rights than a well-informed customer! Customer protection through customer education is, therefore, one of the important functions.

- Don’t get cheated by SMS, phone, email in the name of Dhani
- Do not give details of your bank account by clicking on links received through SMS / Email.
- Beware of SMSs/Calls citing pending KYC updation /PAN card Verification etc. Such SMS are fake, do not respond.
- Don’t share your passwords, PIN, OTP, CVV, etc. with anyone online or through phone
- Never click on suspicious links that you receive via SMS, email or social media platforms
- Don’t get clean bowled by a fraudulent or an unauthorised transaction in your bank account. Notify the bank immediately.
- The longer you take to notify the bank, the higher will be the risk of loss
  If the fraudulent transaction is due to your negligence, you will bear the loss till you report to the bank
- When you notify the bank of a fraudulent transaction, ask for an acknowledgment. The bank should resolve your complaint within 90 days from the date of its receipt
- Always keep your bank’s contact details handy to report fraudulent transactions

Financial Literacy Material - FAME Booklet

The Reserve Bank of India has released the Third Edition of the FAME (Financial Awareness Messages) booklet that intends to provide basic financial literacy messages for the information of the general public. The booklet contains twenty institution/product neutral financial awareness messages, propagating relevant messages across the four themes of Financial Competencies, Basic Banking, Digital Financial Literacy and Consumer Protection.

The RBI has developed tailored financial literacy content for five target groups' viz. Farmers, Small entrepreneurs, School children, Self Help Groups and Senior Citizens that can be used by the trainers in financial literacy programmes.

Audio visuals have been designed for the benefit of general public on topics relating to Financial Literacy. These Audio visuals are on "Basic Financial Literacy", "Unified Payments Interface" and "Going Digital".

For more information please visit
https://www.rbi.org.in/FinancialEducation/fame.aspx

Consumer Awareness - Cyber Threats and Frauds

It has come to the notice 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 -

RBI has issued guidelines for customer awareness. For more information please visit https://rbikehtahai.rbi.org.in

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.

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
- Do not download any unknown app on your phone / device. The app may access your confidential data secretly
- Always access the official website of bank / NBFC / e-wallet provider for contact details. Contact numbers on internet search engines may be fraudulent.
- 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.
- Transactions involving receipt of money do not require scanning barcodes / QR codes or entering MPIN. Thus, exercise caution if asked to do so.
- 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.

SAFE DIGITAL BANKING PRACTICES

- 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.

RBI has issued guidelines for customer awareness. For more information please visit https://rbikehtahai.rbi.org.in

SAFE DIGITAL BANKING PRACTICES

- 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.

RBI has issued guidelines for customer awareness. For more information please visit https://rbikehtahai.rbi.org.in

Modus Operandi and Precautions to be taken against Fraudulent Transactions

SMS / Email / Instant Messaging / Call scams

Modus Operandi

➢ Fraudsters circulate fake messages in instant messaging apps / SMS / social media platforms on attractive loans and use the logo of any known NBFC as profile picture in the mobile number shared by them to induce credibility.

➢ The fraudsters may even share their Aadhaar card / Pan Card and fake NBFC ID card.

➢ After sending such bulk messages / SMS / emails, the fraudsters call random people and share fake sanction letters, copies of fake cheques, etc., and demand various charges. Once the borrowers pay these charges, the fraudsters abscond with the money.

Precautions

➢ Never believe loan offers made by people on their own through telephones / emails, etc.

➢ Never make any payment against such offers or share any personal / financial credentials against such offers without cross-checking that it is genuine through other sources.

➢ Never click on links sent through SMS / emails or reply to promotional SMS / emails.

➢ Never open / respond to emails from unknown sources containing suspicious attachment or phishing links.

Modus Operandi and Precautions to be taken against Fraudulent Transactions

OTP based Frauds

Modus Operandi

➢ Fraudsters impersonating as NBFCs, send SMS / messages offering loans or enhancement of credit limit on NBFC/bank customers' loan accounts, and ask the customers to contact them on a mobile number.

➢ When the customers call such numbers, fraudsters ask them to fill forms to collect their financial credentials. Fraudsters then induce / convince the customers to share the OTP or PIN details and carry out unauthorised transfers from the customers' accounts.

Precautions

➢ Never share OTP / PIN / personal details, etc., in any form with anyone, including your own friends and family members.

➢ Regularly check SMS / emails to ensure that no OTP is generated without your prior knowledge.

➢ Always access the official website of bank / NBFC / e-wallet provider or contact the branch to avail their services and / or seek product and services related information and clarifications

OTP based Frauds

Precautions

➢ Never share OTP / PIN / personal details, etc., in any form with anyone, including your own friends and family members.

➢ Regularly check SMS / emails to ensure that no OTP is generated without your prior knowledge.

➢ Always access the official website of bank / NBFC / e-wallet provider or contact the branch to avail their services and / or seek product and services related information and clarifications

Fake loan websites / App frauds

Modus Operandi

➢ Fraudsters create unscrupulous loan apps which offer instant and short-term loans. These apps dupe the borrowers and may also charge significantly higher interest rates.

➢ To attract gullible borrowers, the fraudsters advertise “limited period offers” and ask borrowers to make urgent decisions using pressure tactics.

Precautions

➢ Verify if the lender is registered with the Government / Regulator /authorised agencies

➢ Check whether the lender has provided a physical address or contact information to ensure it is not difficult to contact them later.

➢ Beware if the lender appears more interested in obtaining personal details rather than in checking credit scores.

➢ Remember that any reputed NBFC / bank will never ask for payment before processing the loan application.

➢ Genuine loan providers never offer money without verifying documents and other credentials of the borrowers.

➢ Verify if these NBFC-backed loan apps are genuine

Money circulation / Ponzi / Multi-Level Marketing (MLM) schemes fraud

Modus Operandi

➢ Fraudsters use MLM / Chain Marketing / Pyramid Structure schemes to promise easy or quick money upon enrolment / adding of members.

➢ The schemes not only assure high returns but also pay the first few instalments (EMIs) to gain confidence of gullible persons and attract more investors through word of mouth publicity.

➢ The schemes encourage addition of more people to the chain / group. Commission is paid to the enroller for the number of people joining the scheme, rather than for the sale of products.

➢ This model becomes unsustainable after some time when number of persons joining the scheme starts declining. Thereafter, the fraudsters close the scheme and disappear with the money invested by the people till then.

Precautions

➢ Returns are proportional to risks. Higher the return, higher is the risk.

➢ Any scheme offering abnormally high returns (40-50% p a) consistently, could be the first sign of a potential fraud and caution needs to be exercised.

➢ Always notice that any payment/ commission / bonus / percentage of profit without the actual sale of goods/ service is suspicious and may lead to a fraud.

➢ Do not be tempted by promises of high returns offered by entities running Multi-Level Marketing/ Chain Marketing/ Pyramid Structure schemes.

➢Acceptance of money under Money Circulation/ Multi-level Marketing / Pyramid structures is a cognizable offence under the Prize Chits and Money Circulation Schemes (Banning) Act, 1978.

➢ In case of such offers or information of such with the state police.

Fraudulent loans with forged documents

Modus Operandi

➢ Fraudsters use forged documents to avail services from financial institutions.

➢ Fraudsters commit identity thefts, steal personal information of customers such as identity cards, bank account details etc., and use this information or credentials to avail benefits from a financial institution.

➢ Fraudsters pose as NBFC employees and collect KYC related documents from customers.

Precautions

➢ Exercise due care and vigilance while providing KYC and other personal documents, including the National Automated Clearing House (NACH) form for loan sanction / availing of credit facility from any entity, especially individuals posing to be representatives of these entities.

➢ Such documents should be shared only with the entity's authorised personnel or on authorised email IDs of the entities.

➢ Follow up with the concerned entities to ensure that the documents shared by you are purged immediately by them in case of non-sanction of loan and/ or post closure of the loan account.

For more details please visit
(https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf)

General Precautions to be taken for financial transactions

Be wary of suspicious looking pop ups that appear during your browsing sessions on internet.

➢ Always check for a secure payment gateway (https:// - URL with a pad lock symbol) before making online payments / transactions.

➢ Keep the PIN (Personal Identification Number), password, and credit or debit card number, CVV, etc., private and do not share the confidential financial information with banks/ financial institutions, friends or even family members.

➢ Avoid saving card details on websites / devices / public laptop / desktops.

➢ Turn on two-factor authentication where such facility is available.

➢ Never open / respond to emails from unknown sources as these may contain suspicious attachment or phishing links.

➢ Do not share copies of chequebook, KYC documents with strangers

RBI has issued guidelines for customer awareness. For more information please visit https://rbikehtahai.rbi.org.in