ujjivan SMALL FINANCE BANK
Build a Better Life

FRAUDS & SAFE DIGITAL PRACTISES

Types of Frauds

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 or SMS designed to dupe customers into thinking that the communication has originated from their bank / e-wallet provide 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 Practises

- 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.
- 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 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
- Check URLs and domain names received in emails. 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.
- 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.

How to report alleged Transaction

- If someone has fraudulently withdrawn money from your bank account, inform the bank immediately. When you notify the bank, remember to take acknowledgement from the bank. The bank has to resolve your complaint within 90 days from the date of receipt.
- In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorised transaction to the bank. Any loss occurring after the reporting of the unauthorised transaction shall be borne by the bank. Hence ensure to report such instances immediately on occurrence.
- If some financial fraud happens you can complain **in National Cyber Crime Reporting Portal's website** https://cybercrime.gov.in/ **or** helpline number **1930** .
- This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complains online.