



# Customer Awareness – Cyber Threats and Frauds



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:**

**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

