

Cyber Fraud Awareness

Types of Frauds to Display

Fraud Type	Modus Operandi	Prevention
Phishing	Fake emails/SMS with malicious links mimicking bank websites	Verify sender; never click unsolicited links
Vishing	Fraudsters call posing as bank/RBI officials, seek OTP/credentials	Bank never calls for OTP; disconnect immediately
SIM Swap Fraud	Fraudster duplicates your SIM to receive OTPs	Immediately contact your telecom provider if SIM stops working
Investment/Part-time Job Scams	Lure victims with high returns; route funds through shell companies/UPI	No legitimate scheme guarantees doubling of money
KYC Fraud	Fake messages directing customers to update KYC on phishing sites	Always visit official bank branch or website
Money Mule	Victims used as conduit for laundering proceeds of fraud	Do not share or rent your account to others
ATM Skimming	Card reader devices installed on ATMs to clone card data	Cover keypad while entering PIN; use bank ATMs only
Juice Jacking	Malware installed through public USB charging ports	Use personal chargers or power banks ^[2]
Illegal Lending Apps	Unauthorised apps offering instant loans; misuse personal data	Check RBI's list of registered NBFCs before borrowing
Ponzi/Investment Fraud	Fraudulent platforms promising unrealistic returns	Report to cybercrime.gov.in or call 1930

Immediate Action: If you have been defrauded — report at <https://cybercrime.gov.in> or call 1930.^[8]

Suspicious communication: Report suspected fraud communication on the **Chakshu platform** at <https://sancharsaathi.gov.in/sfc/>.