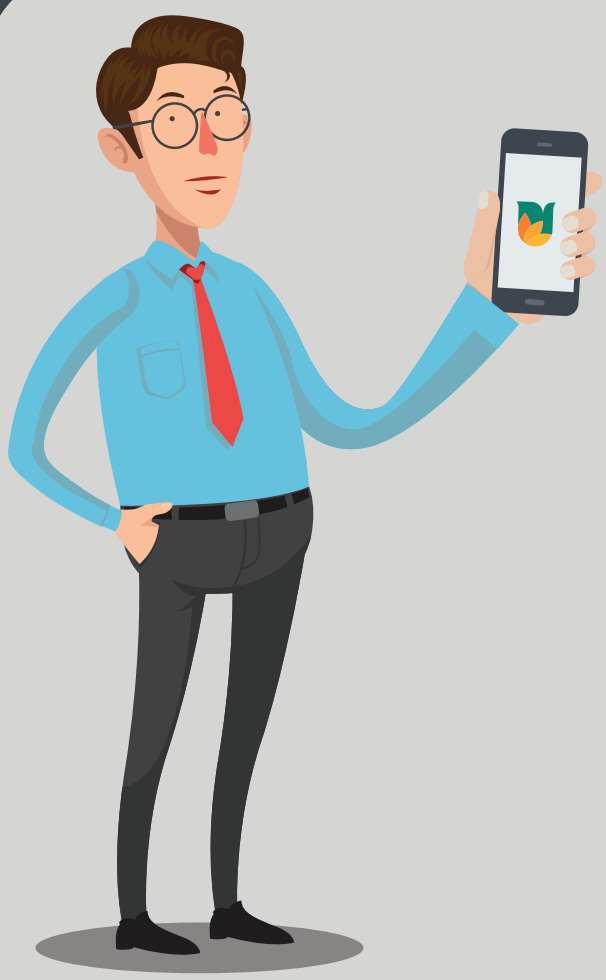
ujjivan SMALL FINANCE BANK

Better Banking. Better Living.



OPT FOR SIM SAFETY.

Beware of SIM card-related fraud.

A mobile phone is a convenient banking channel which people use for shopping, paying bills, and other financial transactions. With **SIM** swap, fraudsters manage to get a new **SIM** card for your registered mobile number through the mobile phone operator and gains access to information like OTP, banking details, etc.

Step 1: Fraudsters gather the customer's personal information through Phishing, Vishing, Smishing or any other means.

Step 2: They approach the mobile operator with fake **ID** proof posing as the customer, and get the **SIM** card blocked.

Step 3: The mobile operator deactivates the genuine SIM card and issues the fraudster a new SIM.

Step 4: The customer's handset will have no network. The customer will not receive any information such as alerts and **OTP** on the phone. Fraudsters then generate One Time Password **(OTP)** required to facilitate transactions using the stolen banking information. The **OTP** is received on the new SIM held by the fraudster who then carries out banking transactions.

SIM Swap Fraud – Safety measures

- If your mobile number has stopped working, enquire with the mobile operator as soon as possible.
- Register for **SMS** and Email alerts to stay informed about the activities in your bank account.
- You should also regularly check the bank statements and transaction history for any irregularities.
- Never share your bank account details over phone call/SMS/e-mails. The bank never asks for such information. Please report such cases to 1800-208-2121.