What is SIM SWAP FRAUD ?

- Fraudster collects victim's personal banking information
- Fraudster approaches victim's mobile operator with victim's fake identity proofs & obtains a duplicate SIM card
- Mobile operator deactivates the original SIM card post successful verifications & issues a replacement SIM
- Fraudster generates the One Time password (OTP) which come on the new SIM & carries out account transactions without victim's knowledge

Tips to safeguard yourself against SIM SWAP FRAUD :

- If your mobile stops working for unusual reasons, check with your mobile operator immediately
- Do not share your 20 digit SIM number mentioned on the back of your SIM with anyone
- Register for Instant bank alert with your bank
- Never disclose Internet banking password/ATM PIN/CVV/Expiry Date/OTP/Telephone PIN to anyone
- Do not disclose your mobile number on social media platforms
- Register for both SMS as well as e-mail alerts to stay informed about transactions on your account
- Never respond to unknown mails or calls asking your account details and registered mobile number