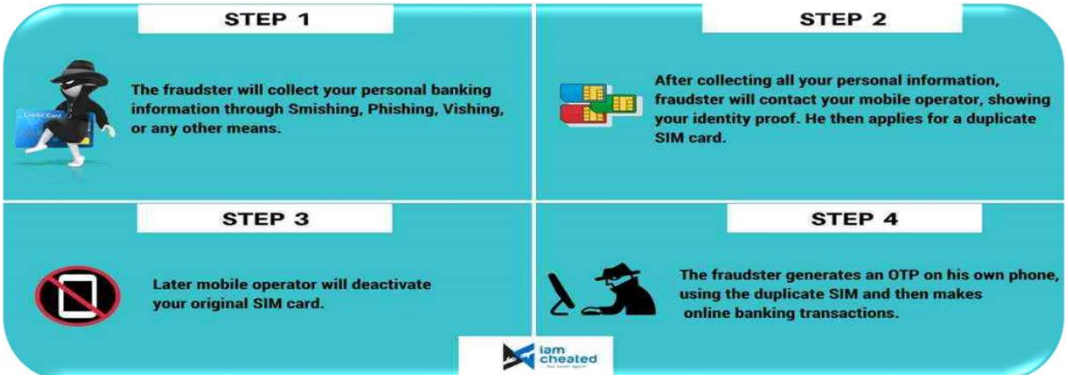
केनरा बैंक Canara Bank

सिंडिकेट Syndicate

Advisory

DATE: 07.08.2020

SIM SWAP FRAUDS



A SIM swap scam is a type of account takeover fraud that misuses personal information in getting duplicate SIM and committing frauds by getting OTP in fraudsters 's mobile device.

How the fraud happens?

- ❑ The fraudsters obtain victims confidential personal details through social engineering techniques or through some unscrupulous bank employees.
- ❑ Using the personal data, they impersonates genuine customers before telecom service providers to obtain and activate duplicate SIM cards and opening deposit accounts through e-KYC without personal verification at the time of opening the accounts.
- ❑ The deposit accounts thus opened are being used for collecting money through unauthorized fund transfers from others accounts, which are later siphoned off by way of cash withdrawals or online payments.
- ❑ Similar techniques are being used for opening credit card accounts and doing online purchases or obtaining personal loans and siphoning off funds through cash withdrawals or online payments.
- ❑ In a few cases, duplicate SIM cards were obtained against deceased customers or those who had moved abroad for work but had not updated their contact numbers and email IDs. This resulted in not getting alerts from their banks about debits in their accounts.

How to protect from SIM swap scams?

- ❖ **Beware of phishing emails and other social engineering attacks which try to access personal information.**
- ❖ **Change in mobile numbers and E-mail ids should be updated in Bank's account by visiting the branch immediately.**
- ❖ **Keep checking the SMS / E-mail alerts received from the Bank.**

INFORMATION SECURITY SECTION, RISK MANAGEMENT WING