Types of Fraud:

SOCIAL ENGINEERING FRAUD

Social Engineering Fraud encompasses a variety of deceptive techniques used by fraudsters to manipulate victims into divulging sensitive information. These tactics include phishing emails, phone calls, SMS, and other methods.

1. Phishing

Phishing is an act of attempting to acquire information such as usernames, passwords, and credit card details by disguised entities with malicious intent. It can be in the form of an email, SMS, website screen or pop-up that appears to be from your bank or card issuer.

2. Vishing

Vishing, short for voice phishing, uses fraudulent phone calls to trick victims into providing sensitive information, like login credentials, credit card numbers, or bank details.

3. Smishing

Smishing is a social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information, or sending money to cybercriminals. The term “smishing” is a combination of “SMS”—or “short message service,” the technology behind text messages—and “phishing.”

SKIMMING FRAUD

Skimming is the act of illegally copying data from the magnetic strip of a credit, debit, or ATM card. The card number and/or details are procured using a small electronic device called skimmer to swipe and store hundreds of such credit card numbers. Skimming can be done at restaurants, bars, gas stations and retail counters where the physical use of card is done.

IDENTITY TAKEOVER FRAUD/APPLICATION FRAUD

WHAT IS IT?

Identity takeover fraud or identity theft occurs when someone gains unauthorized access to your personal information, your identity and uses it for malicious purposes. This includes stealing the individual’s KYC information.

HOW IT WORKS?

- Scammers can exploit Unverified or incomplete KYC documents to fraudulently apply for loans or credit cards.
- The fraudster can steal your mail or personal information from the internet and then use it for fraudulent activities.

ACCOUNT TAKEOVER FRAUD

WHAT IS IT?

In Account Takeover Fraud, fraudsters contact the victims through calls, messages or emails, and influence victims to share their credentials. They gain access to the mobile app/website by creating a new user ID or re-setting password followed by demographic details change, unauthorized transactions or booking of cross-selling products like Encash /BT/BT EMI etc.

HOW IT WORKS?

- The Fraudster influences customers to share OTP (One Time Password).

- The fraudster uses the customer's credentials to initiate a login to their online account (Mobile/Email Change or set up New Device without change).

- As soon as the login credentials change, the account gets logged out from other signed-in devices.

- The Fraudster then uses the account to make unauthorized transactions or book cross-sell products.

CARD, MOBILE HANDOVER

WHAT IT IS?

It involves the unauthorized use of a physical credit or debit card or a mobile device. The fraudster first gain trust of the victims and then manipulates them to share the physical card or mobile. Fraudster gains access to a victim's card or mobile and uses it for fraudulent transactions.

HOW IT WORKS?

- **The fraudster physically steals the victim's credit card or debit card.**
- **They may also use a lost or stolen card that belongs to the victim.**
- **In some cases, the fraudster manipulates the victim through distraction or deception to hand over the physical card or mobile device.**

SOCIAL MEDIA FRAUD

WHAT IT IS?

Social media fraud encompasses deceptive or fraudulent activities that occur on social media platforms. These schemes aim to deceive individuals, steal personal information, manipulate users into specific actions, or achieve financial gain for malicious purposes.

HOW IT WORKS?

- Fraudsters create fake profiles: They often befriend innocent people and send spam messages or links. These links may lead to malicious websites or prompt users to reveal personal or financial details.
- Fake Advertisements and Store Approach: Create ads using social media tools. Target users based on age, interests, and past purchases.

JUICE JACKING FRAUD

WHAT IS IT?

The USB charging points at public charging stations provide an unauthorized access to cyber attackers to our mobile phone data during the charging process, leading to data theft. This is known as Juice Jacking.

The attack could be as simple as extracting all your contact details and private pictures or can be an invasive attack of injecting malicious code directly into your device which can then copy all your passwords or financial data.

A regular USB connector has five pins, where only one is needed to charge the device. Other pins are used for data transfer.

A hacker can easily tamper with a USB charging port at a public charging station to steal passwords and export data.

HOW IT WORKS?

- Fraud originates from USB charging ports installed at public places such as airports, cafes, bus stands, etc.
- Once the device is plugged-in and connection is established, it either installs malware or secretively copies sensitive data from your device.

SCREEN SHARING FRAUD

WHAT IT IS?

Screen Sharing or Mirroring App Fraud is a scam where Fraudsters ask users to install a third-party screen-sharing application to assist online or to update some documents. These apps may or may not be malware, but they do grant complete access of your device to the scammer.

There are hundreds of free screen-sharing applications available all over the internet. Engineers originally used these apps to fix issues on a phone/computer from a remote location. These apps allow full access and control to the user's device.

HOW IT WORKS?

- Fraudster approaches the user imposing to be from a financial institution/bank or an online service provider.
- They will ask the user to download a third-party screen-sharing application on their device to solve an issue immediately.
- Instead of asking users to share their card, bank details, UPI PIN or OTP, fraudsters will ask users to type in the details.
- While users think they are being helped, fraudsters use the opportunity to record the user's card number, CVV code and send an OTP for transferring funds into their own account through an SMS.
- Remember, screen-sharing apps allow access to your device. Fraudsters view the OTP received on the user's device and use it for transferring funds to their own account.

Always Remember: SBI Card will never ask you to install any third-party application on your device.

SIM SWAP FRAUD

WHAT IT IS?

SIM Swap Fraud involves an account takeover where a fraudster gains unauthorized access to your personal and financial details by obtaining a duplicate SIM card associated with your mobile number.

HOW IT WORKS?

- Manipulating the Mobile Operator: The fraudster tricks the mobile operator into initiating a request for a duplicate SIM card linked to the victim’s mobile number.
- Lost or stolen SIM- The fraudster may use victims lost or Stolen SIM to generate new SIM.