**Types of Cyber Frauds observed:**

I. Vishing :

Vishing (Voice Phishing) is a type of cyber fraud that involves fraudulent calls or voice messages to deceive individuals and extract sensitive information. It is form of social engineering where scammers pretend to be legitimate organizations or individuals to gain trust of the victim.

II. Investment Scam :

Fraudsters lure individuals into investment schemes that promise high returns but are actually Ponzi Schemes.

III. Online Job Scam :

Scammers offer fake job opportunities, requiring applicants to pay upfront fees or provide personal information for identity theft. These scams exploit job seekers desperation and willingness to find employment.

IV. Lottery or Prize Scams :

Victims receive notifications claiming they have won a lottery or prize, but to claim it they must pay a fee or provide personal information. These scams exploit people’s desire for easy money or valuable prizes.

V. Online Shopping Frauds :

Fraudulent online sellers may advertise products or services, collect payments, but never deliver the goods. Alternatively, they may send counterfeit or substandard products. These frauds exploit the trust of online shoppers.

VI. Fake Websites :

Fraudsters create fake websites of any institution e.g. Airlines, Financial Institution, Doctors Clinic, Social Media Channels etc. When a customer searches for authentic websites, he/she lands on these fake websites. These frauds exploit the need of the individuals.

VII.  Fake Calls :

Customer receives call from some unknown number where the fraudster impersonates as relatives or friend and lures customer into scam.

**Modus Operandi:**

There are various modus operandi adopted by fraudsters to scam customers. Some of them mostly are detailed hereunder:

1. A customer has put an advertisement to sell any of his items on online selling websites such as OLX. Where he is contacted by the scammer and the scammers pretend to buy the item & offers advance payment and instead of paying, scammer influence customer to pay instead.
2. A customer has put an advertisement to rent out his flat on Magic Bricks. Where he is contacted by the scammer and the scammer pretend to be from ARMY and is interested as tenant & offers advance payment and instead of paying, scammer influence customer to pay instead.
3. Customer has ordered some item online and didn’t receive the item or items received are defective. When he search the customer care no. of the that online store, he/she lands on fake website created by fraudster & under influence of fraudster, customer downloads Screen Sharing/Remote Access Applications which gives scammers full access of the customers mobile device, after which scammer carry out the fraudulent transactions.
4. Customers receives call from someone pretending to be from Courier and threatens customers that your courier will be cancelled if you do not pay upfront fees or GST amount and influence customer to download Screen Sharing/Remote Access Applications which gives scammers full access of the customers mobile device, after which scammer carry out the fraudulent transactions.
5. Customer searches the contact no. of the doctor on online search engine for appointment but lands on fake website created by fraudster & under influence of fraudster download Screen Sharing/Remote Access Applications which gives scammers full access of the customers’ mobile device, after which scammer carry out the fraudulent transactions.
6. Customer receives a whatsapp message to receive high returns if he invest or performs some task. Task involves, giving 5 star rating to some websites or some positive comments and then are lured to invest  initially very small amounts, such as, Rs 2000/- with return of Rs. 2800/- . At first he/she receives Rs 2800/- there after he is assigned task with higher investment, such as, Rs 15000/- & more and also high return. When customers invest for once, he is again advised to invest Rs 15000/- or more or else he will lose all amount & thus resulting in loss to customer.
7. Customer receives a call from someone impersonating to be customer relative and says that his/her father has asked him to send you (customer) money and instead of sending money, scammer influence customer to send the money to the scammer.
8. Customer receives a call from someone impersonating to be customer relative and says that his/her father has asked him to send you (customer) Rs 15,000/-. After sometime customer receives a SMS (sent by fraudster and SMS is formatted in such a way that it appears to be from some bank) that Rs. 50,000/ has been credited in your account (It’s only a fake message generated by scammer, no amount is credited to customers account). Immediately scammer again call the customer and inform him that by mistake he has send Rs. 50,000/- instead of Rs. 15,000/- and ask customer to send him back Rs. 35,000/- the difference amount, which customer sends by himself/herself.
9. Customer receives a call from someone impersonating to be from BSNL or any particular Bank and informs the customer that his KYC has expired & he has to pay some trivial amount as upfront fees for account activation and influence customer to download Screen Sharing/Remote Access Applications which gives scammers full access of the customers mobile device, after which scammer carry out the fraudulent transactions.