Awareness Series 5: (If that doesn't get your thinking, we don't know what will!)

(A CSR initiative)

Author: Advocate Raji Nathani,

Delhi High Court

www.relegal.in; 9818331659

relegal25@gmail.com

June 2024

I. Understanding types of Frauds and modus operandi hooks to lure into fraud

With an upsurge in Digital payments, the tricks and innovative ways of Fraudsters to hoodwink unsuspecting general public to defraud are also on the rise

When it is done with your knowledge (social engineering):

They exploit emotions such as fear, greed & need to manipulate unsuspecting victims into compromising their sensitive information by either clicking on a link or by downloading some "app".

Fear: Example being threats of electricity disconnection, blockage of bank accounts for non-compliance with KYC requirements, insurance policy renewal, contrived interception of courier packages allegedly containing illegal items (also known as FedEx phishing) to make you part with sensitive information or money.

Greed: Bait to transfer funds with a promise of better returns or a great deal. E.g spurious e-commerce websites offerering stupendous deals in the form of discounts or cash back on branded items without Cash On Delivery (COD) but only against pay first, delivery later. Another popular method involves lottery winnings e.g you getting selected as beneficiary in a "lucky draw", availing big pre-approved loans at low rate by clicking on link, option to purchase branded merchandise at cheaper rates by downloading the app and investment scams are also some of the baits used to entice innocents.

Need: Fake jobs, pay for likes, become movie critic etc to enrol and share bank details much like Home job or Telegram fraud: In this, the potential target will get a message on his or her WhatsApp number with a part-time job offer. The target is told to open an account in Telegram and an organiser then adds the number in a group. Another common trick on the house rentals is through tracking postings on platforms like Magic Bricks, NoBroker etc. and posing as military personnel on transfer seeking house on rental. The fraudsters request you to initiate digital payment to enable them to get your UPI handle for "transferring" initial deposit. Subsequently, instead of sending a payment they send a request for funds which if accepted leads to debit to your account instead of a credit. Similar modus operandi is used by way of requesting QR code scans for money transfers in cases of sale of goods on resale platforms like OLX etc.

Request: Fraudsters may transfer some amount to your account and then request for return on the pretext of mistaken transfer taking advantage of the trust**.**

When Fraud is done without your knowledge

Card-not-present fraud

(CNP) fraud happens when someone with malicious intent gets hold of crucial payment details, such as credit card numbers, personal information (e.g. names and addresses), or the three-digit security code on the card's back. Armed with this information, the fraudster can make fraudulent purchases including online shopping **Source:** fraudsters can easily purchase 'fullz' (Login,Password, https://github.com/igoshev/laravel-captcha. Captcha, Remember me, Register Login), where complete stolen profiles are uncovered through data breaches or phishing attacks and can be purchased via the dark web.

➡ the most common methods are phishing, skimming, hacking, data breaches and social engineering. Digital skimming, hacking and breaches are unavoidable but phishing and social engineering can be avoided if you are alert and vigilant.

Package Redirection Scams
Legitimate-looking purchases are made using stolen credentials. After the transaction is completed, the crook goes into the online account and edits the delivery address. They ship the order to themselves, or perhaps a location where the delivery could be easily intercepted.

Device fingerprinting
It collects data about a device, such as the IP address, device type, operating system, and browser type, to create a unique fingerprint'.

Phishing involves the use of fraudulent emails, texts, or other electronic communications to deceive people into sharing their personal and financial information.

Digital Skimming Also known as Magecart attacks, captures credit or debit card information. They install small devices, known as "skimmers", on card readers at ATMs or point-of-sale (POS) terminals. When someone uses the ATM and swipes their card, the skimmer captures payment card information entered by unsuspecting customers to carry out unauthorized transactions or sell it on the dark web.

Hacking and Data Breaches by getting unauthorized access and manipulating computer systems or networks to gain valuable information.

The rise of AI voice cloning- The voice clip is used to simulate a distress call from someone you know — son, daughter, friend, superior from your workplace — seeking urgent assistance with a promise to return the favour. The situation simulated is either a lost wallet at the airport or an accident requiring urgent money to be transferred for emergency medical assistance

FraudGPT- there is a product sold on the dark web called FraudGPT, which allows criminals to make content to facilitate a range of

frauds, including creating bank-related phishing emails, or to custom-make scam web pages designed to steal personal information.

II. Do's to Protect Yourself:

- Register your email and mobile number with your bank to receive instant alerts.
- Opt for chip-enabled cards and set transaction limits for online, ATM, international, and NFC transactions.
- Verify message headers for authenticity- Check URLs and domain names received in emails for spelling errors, especially wrt re-KYC, account blockage, or disconnection of services. In case of suspicion, notify local police/cybercrime branch immediately.
- Request official meetings or written communication when someone purports to be calling on behalf of law enforcement agencies or insurance companies.
- Evaluate deep discount deals sceptically, ensure to conduct background checks by simply asking around before engaging in deals and avoid prepayment-only transactions.
- Look before you use an ATM: At off-site ATMs without security guards, check for evidence of tampering. Don't use ATMs that have damaged or loose parts or look as if they have been tampered with. Cover the PIN pad when you enter your PIN or Another way is to opt for cardless transactions at ATMs.
- Positive Pay: For cheque payments, the positive pay feature enables you to pre-inform your bank about the details of the issued check and the intended beneficiary. This helps prevent misuse through alterations or duplication of checks by unscrupulous individuals.
- **Adopt Good Practices:** If you receive an OTP for debiting your account for a transaction not initiated by you, inform your bank/e-wallet immediately, Set strong passwords or PINs and regularly change them, immediately block lost or misplaced cards, Install antivirus software on desktop/laptop devices to protect against malware attacks.

- a product called Catch is an AI system that has been trained to spot scam emails. Currently compatible with Google's Gmail, Catch scans incoming emails, and highlights any deemed to be fraudulent, or potentially so.

III. Don'ts to safeguard against:

- Avoid using public, open, and free networks for banking transactions.
- Switch off your Bluetooth while travelling and at public places
- Do not accept any invitation that reads like "Mr/Ms X is trying to send you a photo"- just deny
- Refrain from downloading unknown/screen-sharing app on your phone/device. The app may access and share your confidential data secretly.
- Never share PINs, login credentials, or passwords with anyone.
- Don't answer calls from unknown numbers.
- If someone transfers some money to your account and claims that it was done mistakenly and wants you to return the same then **IN THAT CASE, PLEASE DONOT PAY DIGITALLY.** Please ask him to meet you personally at the nearest police station and then issue him a cheque of the same amount.
- Do not share Aadhar, Pan card copies without masking to avoid misuse.
- Do not handover self-attested copies of property papers, identity documents or income papers to middlemen without specifying the end purpose for which the attested documents have been handed over.
- Do not just sign application forms and leave it to the salesperson to fill up the details. Ensure to fill up entire application forms for opening an account, loan, card yourself ensuring the correct details are filled in especially when it comes to the contact number, email, etc.
- Avoid sharing bank account details for receiving rewards/lottery winnings.
- Receiving money does not require scanning of QR codes or entering MPIN Do not scan QR codes to receive payments
- Never respond to messages offering/promising prize money, Government aid. These may defraud your phone/device.
- DO NOT provide access to your device via AnyDesk or any other such remote access software

IV. In Case of Becoming a Victim

Act within the Golden Hour Immediately

1. Complete all the protocols viz reporting to your bank (number is always prominently displayed on all bank's websites), report online on cybercrime website (https://cybercrime.gov.in/) or call 1930 within the golden hour — less than 30 min of the incident. This can help the bank trace the money trail and seek a freeze on the beneficiary's accounts to prevent the money withdrawal.
2. File FIR at the earliest, at least within 24 hours. Take proactive steps to reach out to the bank's Nodal officers to facilitate immediate action.
3. Check for any systemic deficiency on the part of the bank vis-a-vis regulations or industry practice.
4. In case of any deficiency, bring it up to the senior / top management and the regulator, persist and pursue the matter to its logical conclusion.
5. As per RBI guidelines, if the loss is due to an error on your part, your liability is limited until you report the activity. If you haven't shared payment details and report within three days, you won't bear any loss. The bank is obligated to refund the lost amount if the fraud is confirmed.

V. How & Where to Report a Cyber Fraud?

- Take a clearly visible screenshot of the evidence.
- Magic number "1930" – make a call in the "Golden Hour" i.e. within one hour of the crime.
- Brief facts of the complaint explaining how you have come in contact with the alleged person/website and subsequent fraud.
- Visit the nearest Police Station/Cyber Cell immediately.
- To report cybercrime complaints online, visit the National Cyber Crime Reporting Portal. This portal can be accessed at https://cybercrime.gov.in. In this portal, there are two sections. One section is to report crimes related to Women and Children

(where reports can be filed anonymously as well). Another section is to report other types of cybercrimes. Complaint can also be filed via offline by dialing the helpline number **1930** which connects to the T4C i.e., Telangana Cyber Crimes Co-ordination Centre from which authorized personnel will guide the victim in freezing/ withholding the victim's amount in the bank account.

- **Chakshu facilitates** citizens to report the suspected fraud communications with the intention of defrauding telecom service users for cyber-crime, financial frauds, non-bonafide purpose like impersonation or any other misuse through Call, SMS or WhatsApp.

Few examples of suspected fraud communications are communication related to Bank Account / Payment Wallet / SIM / Gas connection / Electricity connection / KYC update / expiry / deactivation, impersonation as Government official / relative, sextortion related etc.

Note**: If you have already lost money due to financial fraud or are a victim of cyber-crime, then report as per above. Chakshu facility does not handle financial fraud or cyber-crime cases.**

VI. Who is liable for card-not-present fraud?

- In most cases it will fall on the merchant however depending on the security setup it can also cost the payment service provider or bank.

VII. Some Super Dupers:

1. the first reported case of such fraud at the Cyber Crime pol station in Noida. The perpetrators, posing as police officials implicated the victim in an imaginary money-laundering case referencing the names of an IPS officer in the CBI and the founder of a grounded airline. The criminals kept her online via Skype, urging her not to share information during the fraudulent arrest.
2. A postmaster tampered with the post office account and transferred Rs 21.75 lakh from the account of a city couple to their account in Kanpur.

3. Cyber crooks' con biz consultant into buying 'shares', loot Rs 6 cr - The cyber fraud victim said, he first received a message on WhatsApp to join an online business platform, which provides people with institutional accounts to block trade in shares and get preferential shares in IPOs, and also helps to invest in the stock market using institutional accounts for purchase of shares. After the business consultant transferred ₹5.98 crore into11 different accounts of various companies, the dashboard showed a value of ₹21 crore, indicating that it was the amount of profit he made from the investments. The woman instructed him to sell the holdings. But when he wanted to know the process of withdrawing his funds, she insisted on a payment of 20% of 'profit', amounting to₹2.88 crore in addition to the value of his money. He requested them to hold back 20% and release the balance, but they refused and insisted on a minimum payment of 10% of profits, which was ₹1.44 crore. He tried to contact the other group members, but they did not respond and later realised that he was duped and approached police.
4. Courier Scammers, Fake TRAI (Telecom Regulatory Authority of India) or FedEx (courier) company callers: A person from Vijayawada was duped by cyber fraudsters to the tune of 5 lakh. The miscreants posed as anti-narcotics cell personnel from Mumbai and threatened him with a false case of drugs smuggling through couriers. They even said they were in possession of his adhaar copy. He also advised the victim to speak with a Mumbai police officer through Skype call. The victim clicked on the link provided by the miscreants, following which a person posing as a police officer, with the background of a police station threatened the victim with dire consequences. The victim lodged a complaint with NTR district police in Vijayawada.
5. sextortion scammers on Instagram- the boy committed suicide- They pretended to be a pretty girl his age and flirted with him, sending sexual pictures to coax him into sharing explicit photos of himself. They then blackmailed him for hundreds of pounds to stop them sharing the pictures online to his friends. (BBC)

6. The Mumbai police have arrested two persons after it emerged that over 25 Indians were lured with "high-paying" jobs in Thailand but taken to Laos, where they were forced to commit cyber fraud,
7. Hyderabad Cyber Crime Police arrested five accused persons who were associated with a trading fraud case and cheated the complainant in the guise of getting high returns by investing in the stock market.
8. A 40-year-old woman software engineer from Bengaluru, Karnataka, has become the latest victim of the 'FedEx' scam, losing Rs 1 crore to cybercriminals in just two days. The scammers trapped her in a "digital arrest" by initially informing her of a parcel supposedly containing illegal substances sent in her name. Then, posing as law enforcement officers, they coerced her into making multiple money transfers.
9. Online friendships can sometimes prove to be quite costly. A Bengaluru woman learned this lesson after losing over Rs 12 lakh. The woman reported to the cops that she met the suspect two years ago in January 2022. The lady also told the police that she and her online friend used to talk over the phone and text each other regularly. As time passed, the man started to visit her residence when her husband went to work. She also revealed to the investigating officers that the man forced her to be intimate with him despite her disagreement and then blackmailed her.

Traumatising data which can't be ignored:

In their total analysis of frauds the Reserve Bank of India in their annual report for 2023-24 records that 'Frauds have occurred predominantly in the category of digital payments (card/internet), in terms of number."

Out of total number of fraud cases of 36075 in 2023-24 as many as 29082 relate to Card/Internet cases which is 80% cases. In terms of absolute value it amounted to 14.57 billion rupees ($175 million). This is more than double the allocation for cybersecurity projects by the Government of India for 2024-2025.

“Data is the heart of your digital life; keep it beating.”

Earlier Runs (Click to read):

- **Awareness Series 1 crimes against women**
- **Awareness Series 2 search**
- **Awareness Series 3 Senior Citizens**
- **Awareness Series 4 (Gold and Bank Locker facts)**