Common Types of Cyber Frauds and the Preventive Measures to be Adopted

1. Phishing Links

Modus Operandi:

- ➢ Fraudsters create a third-party phishing website which looks like an existing genuine website, such as a bank's website or an e-commerce website or a search engine etc.
- ➢ Links to these websites are circulated by fraudsters through Short Message Service (SMS)/ social media/email/Instant Messenger etc.
- ➢ Many customers click on the link without checking the detailed Uniform Resource Locator (URL) and enter secure credentials such as Personal Identification Number (PIN), One Time Password (OTP), Password etc., which are captured and used by the fraudsters.

Precautions:

- ➢ Do not click on unknown/unverified links and immediately delete such SMS/email sent by unknown sender to avoid accessing them by mistake in future.
- ➢ Unsubscribe the mails providing links to a bank/e-commerce/search engine website and block the sender's e-mail ID, before deleting such emails.
- ➢ Always go to the official website of your bank/service provider. Carefully verify the website details especially where it requires entering financial credentials. Check for the secure sign (https with a padlock symbol) on the website before entering secure credentials.
- ➢ Check URLs and domain names received in emails for spelling errors. In case of suspicion, do not open the mail.

2. Vishing calls

Modus Operandi:

- ➢ Imposters call or approach the customers through telephone call/social media posing as bankers/company executives/insurance agents/government officials. To gain confidence, imposters share a few customer details such as the customer's name or date of birth.
- ➢ In some cases, imposters pressurize/trick customers into sharing confidential details such as passwords/OTP/PIN/Card Verification Value (CVV) etc., by citing an urgency/emergency such as - need to block an unauthorized transaction, payment required to stop some penalty, an attractive discount etc. These credentials are then used to defraud the customers.

Some of the latest methods of cheating are furnished below:

Imposters trick customers by pretending as Government official enquiring about Covid Vaccination and whether interested in booster dose. If the customer says "yes", they will advise to do registration, share OTP and defraud the customer.

In some cases the fraudster calls and informs that your utility bill (like Electricity bill) is not paid and if you say that it is already paid, they will say that in their records it is not seen as paid and the amount might have accounted in some other's account. To test, they will ask for sending another Rs.10/- and still they will inform that it is also not seen as paid and will ask to share the OTP received on your mobile phone, through which they carry out online looting.

Precautions:

- ➢ Bank officials/financial institutions/RBI/any genuine entity never ask customers to share confidential information such as username/password/card details/CVV/OTP.
- ➢ Never share these confidential details with anyone, even your own family members, and friends.

3. <u>Frauds using online sales platforms</u>

Modus Operandi:

- ➢ Fraudsters pretend to be buyers on online sales platforms and show an interest in seller's product/s. Many fraudsters pretend to be defense personnel posted in remote locations to gain confidence.
- ➢ Instead of paying money to the seller, they use the "request money" option through the Unified Payments Interface (UPI) app and insist that the seller approve the request by entering UPI PIN. Once the seller enters the PIN, money is transferred to the fraudster's account.

Precautions:

- ➢ Always be careful when you are buying or selling products using online sales platforms.
- ➢ Always remember that there is no need to enter PIN/password anywhere to receive money.
- ➢ If UPI or any other app requires you to enter PIN to complete a transaction, it means you will be sending money instead of receiving it.

4. <u>Frauds due to the use of unknown/unverified mobile apps</u>

Modus Operandi:

- ➢ Fraudsters circulate through SMS/email/social media/Instant Messenger etc., certain app links, masked to appear similar to the existing apps of authorised entities.
- ➢ Fraudsters trick the customer to click on such links which results in downloading of unknown/unverified apps on the customer's mobile/laptop/desktop etc.

➢ Once the malicious application is downloaded, the fraudster gains complete access to the customer's device. These include confidential details stored on the device and messages/OTPs received before/after installation of such apps.

Precautions:

➢ Never download an application from any unverified/unknown sources or on being asked/ guided by an unknown person.

➢ As a prudent practice before downloading, check on the publishers/owners of the app being downloaded as well as its user ratings etc.

➢ While downloading an application, check the permission/s and the access to your data it seeks, such as contacts, photographs etc. Only give those permissions which are absolutely required to use the desired application.

5. <u>ATM card skimming</u>

Modus Operandi:

➢ Fraudsters install skimming devices in ATM machines and steal data from the customer's card.

➢ Fraudsters may also install a dummy keypad or a small/pinhole camera, well-hidden from plain sight to capture ATM PIN.

➢ Sometimes, fraudsters pretending to be other customer standing near-by gain access to the PIN when the customer enters it in an ATM machine.

➢ This data is then used to create a duplicate card and withdraw money from the customer's account.

Precautions:

➢ Always check that there is no extra device attached, near the card insertion slot or keypad of the ATM machine, before making a transaction.

➢ Cover the keypad with your other hand while entering the PIN.

➢ NEVER write the PIN on your ATM card.

➢ Do NOT enter the PIN in the presence of any other/unknown person standing close to you.

➢ Do NOT follow the instructions given by any unknown person or take assistance/guidance from strangers/unknown persons at the ATMs.

➢ If cash is not dispensed at the ATM, press the 'Cancel' button and wait for the home screen to appear before leaving the ATM.

6. <u>SIM swap/SIM cloning</u>

Modus Operandi:

- ➢ Fraudsters gain access to the customer's Subscriber Identity Module (SIM) card or may obtain a duplicate SIM card (including electronic-SIM) for the registered mobile number connected to the customer's bank account.
- ➢ Fraudsters use the OTP received on such duplicate SIM to carry out unauthorised transactions.
- ➢ Fraudsters generally collect the personal/identity details from the customer by posing as a telephone/mobile network staff and request the customer details in the name of offers such as - to provide free upgrade of SIM card from 3G to 4G or to provide additional benefits on the SIM card.

Precautions:

- ➢ Be watchful regarding mobile network access in your phone. If there is no mobile network in your phone for a considerable amount of time in a regular environment, immediately contact the mobile operator to ensure that no duplicate SIM is being/has been issued for your mobile number.

7. <u>Frauds by compromising credentials on results through search engines</u>

Modus Operandi:

- ➢ Customers use search engines to obtain contact details/customer care numbers of their bank, insurance company, Aadhaar updation centre etc. These contact details on search engines often do NOT belong to the respective entity but are made to appear as such by fraudsters.
- ➢ Customers may end up contacting unknown/unverified contact numbers of the fraudsters displayed as bank/company's contact numbers on search engine.
- ➢ Once the customers call on these contact numbers, the imposters ask the customers to share their card credentials/details for verification.
- ➢ Assuming the fraudster to be a genuine representative of the RE, customers share their secure details and thus fall prey to frauds.

Precautions:

- ➢ Always obtain the customer care contact details from the official websites of banks/companies.
- ➢ Do not call the numbers directly displayed on the search engine results page as these are often camouflaged by fraudsters.
- ➢ Please also note that customer care numbers are never in the form of mobile numbers.

8. <u>Scam through QR code scan</u>

Modus Operandi:

- ➢ Fraudsters often contact customers under various pretexts and trick them into scanning Quick Response (QR) codes using the apps on the customers' phone.

➢ By scanning such QR codes, customers may unknowingly authorise the fraudsters to withdraw money from their account.

Precautions:

➢ Be cautious while scanning QR code/s using any payment app. QR codes have account details embedded in them to transfer money to a particular account.

➢ Never scan any QR code to receive money. Transactions involving receipt of money do not require scanning barcodes/QR codes or entering mobile banking PIN (m-PIN), passwords etc.

9. Fake advertisements for extending loans by fraudsters

Modus Operandi:

➢ Fraudsters issue fake advertisements offering personal loans at very attractive and low rates of interest or easy repayment options or without any requirement of collateral/ security etc.

➢ Fraudsters send emails with such offers and ask the borrowers to contact them. To gain credibility with the gullible borrowers and to induce confidence, these email-ids are made to look-like the emails IDs of senior officials of well-known/genuine Non-Banking Financial Companies (NBFCs).

➢ When borrowers approach the fraudsters for loans, the fraudsters take money from the borrowers in the name of various upfront charges like processing fees, Goods and Services Tax (GST), intercity charge, advance Equated Monthly Instalment (EMI) etc., and abscond without disbursing the loans.

➢ Fraudsters also create fake website links to show up on search engines, when people search for information on loans.

Precautions:

➢ Loan processing fee charged by NBFCs/banks is deducted from the sanctioned loan amount and not demanded upfront in cash from the borrower.

➢ Never pay any processing fee in advance as NBFCs/banks will never ask for an advance fee before the processing of loan application.

➢ Do not make payments or enter secure credentials against online offer of loans at low interest rates etc., without checking/verifying the particulars through genuine sources.

10. SMS/ Email/Instant Messaging/Call scams

Modus Operandi:

- ➢ Fraudsters circulate fake messages in instant messaging apps/SMS/social media platforms on attractive loans and use the logo of any known NBFC as profile picture in the mobile number shared by them to induce credibility.
- ➢ The fraudsters may even share their Aadhaar card/Pan Card and fake NBFC ID card.
- ➢ After sending such bulk messages/SMS/emails, the fraudsters call random people and share fake sanction letters, copies of fake cheques etc., and demand various charges. Once the borrowers pay these charges, the fraudsters abscond with the money.

Precautions:

- ➢ Never believe loan offers made by people on their own through telephones/emails etc.
- ➢ Never make any payment against such offers or share any personal/financial credentials against such offers without cross-checking that it is genuine through other sources.
- ➢ Never click on links sent through SMS/emails or reply to promotional SMS/emails.
- ➢ Never open/respond to emails from unknown sources containing suspicious attachment or phishing links.

General precautions:

- ➢ Be wary of suspicious looking pop ups that appear during your browsing sessions on internet.
- ➢ Always check for a secure payment gateway (https:// - URL with a pad lock symbol) before making online payments/transactions.
- ➢ Keep the PIN (Personal Identification Number), password, and credit or debit card number, CVV etc. private and do not share the confidential financial information with banks/ financial institutions, friends or even family members.
- ➢ Avoid saving card details on websites/devices/public laptop/desktops.
- ➢ Turn on two-factor authentication where such facility is available.
- ➢ Never open/respond to emails from unknown sources as these may contain suspicious attachment or phishing links.
- ➢ Do not share copies of chequebook, KYC documents with strangers.

For device/computer security:

- ➢ Install antivirus on your devices and install updates whenever available.
- ➢ Always scan unknown Universal Serial Bus (USB) drives/devices before usage.
- ➢ Configure auto lock of the device after a specified time.
- ➢ Do not install any unknown applications or software on your phone/laptop.
- ➢ Do not store passwords or confidential information on devices.

For safe internet browsing:

- ➢ Avoid visiting unsecured/unsafe/unknown websites.

➢ Avoid using/saving passwords on public devices.

➢ Avoid entering secure credentials on unknown websites/ public devices.

➢ Do not share private information with anyone, particularly unknown persons on social media.

➢ Always verify security of any webpage (https:// - URL with a pad lock symbol), more so when an email or SMS link is redirected to such pages.

For safe internet banking:

➢ Always use virtual keyboard on public devices since the keystrokes can also be captured through compromised devices, keyboard, etc.

➢ Log out of the internet banking session immediately after usage.

➢ Update passwords on a periodic basis.

➢ Do not use same passwords for your email and internet banking.

➢ Avoid using public terminals (viz. cyber cafe etc.) for financial transactions.

1930 is the new help line number against Cyber Crimes.
Victims can register a complaint and Cyber police will take action as per requirement.

How the platform works:

Reporting and initial action

- Victim can call help line number 1930, if getting defrauded on Cyber Fraud.
- The call is attended by authorized personnel, who asks for minimum mandatory details of the financial transactions.
- A token is generated and the Beneficiary Bank, wallet or merchant is alerted to trace and 'HOLD' the amount if available.

Formal Complaint

- The complaint is notified through an SMS having the reference number and a link to www.cybercrime.gov.in.

- A formal and detailed complaint is required to be lodged by the victim, within the next 24 hours.

Trail and Freeze

- As soon as the Digital alert is sounded, the system hold the flow of defrauded money and report back to the platform.
- In case the money has been shifted to another financial intermediary, an alert is sent for freezing of the amount.
- The process is repeated till the amount has either been kept on temporary hold,

withdrawn or spent online.

Getting your money back

After following the due process, victim may receive the money back, if available.