Beware of frauds through fake Investment / Part-time Job / Ponzi Schemes

Recently there is a surge in the number of cybercrimes wherein the criminals and fraudsters are resorting to different kinds of modus operandi for perpetrating cybercrimes routed through the banking channels and payment gateways.

The **modus operandi** includes **"***Investment / Part Time Job / Ponzi Schemes*" etc. wherein the transactions are routed through the banking channels

Few among the scenarios involved are:

- Victims are lured through part-time job offers and other advertisements on Internet and/or messaging platforms, etc., and are promised high commissions or high returns such as doubling of money in short span of time. These advertisements / SMS messages usually contain a link, which directly prompts for a chat. Further, mobile applications, bulk SMS messages, SIM-box-based Virtual Private Network (VPNs), phishing websites, cloud services, virtual accounts in banks, Application Programming Interfaces (APIs), etc., are used to carry out such financial frauds.

- Words such as "Earn Online", "Part Time Job", etc. are being used by fraudsters and criminals to match their advertisements with the terms people are searching for. Such advertisements are mostly displayed from 10 AM to 7 PM, which is usually the peak time for internet use. Majority of these websites used by fraudsters have domains - 'xyz' and `wixsite' and most of these sites either redirect to a messaging platform or to a website which has embedded messaging platform link which, on clicking, again redirects to a chat.

- Multiple local numbers are being used for communication with victims. Upon analysis, it is found that mobile number holder was not aware about messaging platform being operated in his/her name. In some cases, the mobile number holder knowingly shares OTP in return for some money from the fraudsters.

- The fraudsters sends an investment link over chat with a referral code. Fraudsters in this case generally communicates in English and even Google Translate is also used to communicate with the victims.

  A screenshot is sent to the person over the messaging platform to activate the account. Once the account is activated, a task is given to the user to gain confidence of the person. Mandatory condition to do a task is to load money through Payment Gateways which are not authorized to operate in a particular jurisdiction. All the payments are made through UPI and some of the UPI addresses belong to even registered companies.

  A call centre is also usually used to interact with the victim for communication regarding tasks. For instance, upon failure to load funds on investment website, the call centre executive initiates a call prompting to initiate the payment. Once the task is completed, the victim is asked to withdraw the money and the withdrawal is done through various Payment Aggregators.

  On getting the first refund, the victim is now lured to do more tasks which involve loading of more money. The process continues and once a big amount is loaded by the victim, the person (fraudster) stops responding over chat.

  UPI details are updated daily on these fraudulent websites. While the Investment websites keep changing, the source code remains same with different domains.

- Bank accounts opened by money mules using real / fake identification are used to receive stolen funds from compromised bank accounts, through sharing of OTPs, etc.

- Layering of transactions is carried out by account to account transfers. From the intermediate account, money is diverted to multiple sources/assets like crypto currencies, bullion, pay out accounts (for gaining confidence and hiding laundering), foreign money transfer, person-to-person transfer, etc.

- Instances have been observed where Shell Companies or Paper Companies with dummy directors, rented companies with registration certificates, Fintech companies, Payment Gateways, SMS aggregators are noted to be involved in carrying out such financial frauds (mostly using UPI as payment mode). Main objective of opening these Shell Companies is to create a current account or a fintech company for accepting or paying out proceeds of frauds. Most of these Shell Companies appear to be Technology Companies created with 'Technology Private Limited' name

- UPI addresses are used to create layering behind Payment Aggregators thereby, facilitating end of day settlement.

- Aggregator on aggregator concept is used by these players (fraudsters) in order to conceal their identities. The network of fraudsters start creating Payment Aggregator business in collaboration with banks directly or with other fintech companies. The fraudsters would be sitting behind the payment aggregator as sub-aggregator or directly as a merchant. The money collected by the fraudsters as sub-aggregator and/or as merchant, is remitted to the Payment Aggregator wherefrom the API (app) based pay outs take place. After the aggregator network is set up, the accounts are operated for making the pay outs by the fraudsters overseas.

- Professionals, foreign nationals, payment aggregators, points of sale terminals for SIM cards, etc., are also reported to be involved in such frauds.

- Gold, crypto currencies, international money transfers are also observed by Law Enforcement Agencies (LEAs) to be the usual termination points of the fraud trails.

Thanks,
Team CSB Bank Ltd.