Frauds / Cybercrimes through investment/ part time job/ ponzi scheme scams

There are witnessing the incidence of several 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.

Modus operandi

Some of the modus operandi followed by the fraudsters and criminals through investment / part time job / ponzi schemes, wherein the transactions are routed through the banking channels are given hereunder.

(a) 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. The advertisements ISMS 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 financial frauds.

(b) Keywords such as "Earn Online", "Part Time Job", etc., are used by fraudsters and criminals to match their advertisements with the terms people are searching for. Further, such advertisements are mostly displayed from 10 AM to 7 PM, which is usually the peak time for internet use by Indian public. Majority of websites used by fraudsters have domains - 'xyz' and 'wixsite'. 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.

(c) Multiple Indian numbers were used for communication with victims. Upon analysis, it was 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.

(d) The fraudster sends an investment link over chat. Each person has a referral code. Fraudster generally communicates in English. Google Translate is also used to communicate with the victims.

(e) 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.

(f) UPI details are updated daily on the fraudulent websites. Investment websites keep changing. Source code remains same but domain changes.

(g) 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. Rented accounts are sourced by agents and account owners (Money mules) are given fixed rent or commission or lumpsum amount for the account.

(h) Layering of transactions is carried out by account-to-account transfers. Bulk payments/ APIs are also used for this.

(i) From the intermediate account, money is diverted to multiple sources/assets like crypto currencies, bullion, payout accounts (for gaining confidence and hiding laundering), foreign money transfer, person-to-person transfer, etc.

(j) Payment aggregators, points of sale terminals for SIM cards, etc., are also reported to be involved in such frauds.

(k) Gold, crypto currencies, international money transfers are observed to be the usual termination points of the fraud trails.