# Advisory on Frauds/Cybercrimes

RBI has issued an advisory on Frauds / Cybercrimes through investment/ part time job/ ponzi scheme scams/harvesting user credentials, OTP as below:

(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 / 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 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) A screenshot needs to be 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 India. All payments are made through UPI. Some of the UPI addresses belong to companies registered with Ministry of Corporate Affairs (MCA). A call centre is usually used to interact with the victim for communication regarding tasks. For instance, on failure to load funds on investment website, the call centre executive initiates a call.

(f) Once the task is completed, the victim is asked to withdraw the money. Money is withdrawn through various Payment Aggregators.

(g) 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.

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

(i) 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.

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

(k) 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.

(l) Instances have been observed where Shell Companies with dummy directors, rented companies with MCA registration certificates, fintech companies, payment gateways, SMS aggregators are reported to be involved in carrying out such financial frauds, mostly using UPI as payment mode. Main objective of opening 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 and mostly registered with Bengaluru RoC.

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

(n) Aggregator on aggregator concept is used by these players (fraudsters) in order to conceal their identities. The merchants onboarded on the fintech players (Eg. ABC company onboarded on Payment Aggregator) are frauds. 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 APl(app) based payouts take place. After the aggregator network is set up, the accounts are operated for making the payouts by the fraudsters based outside India.

(o) Chartered Accountants, foreign nationals (from Cambodia, China, Dubai, Nepal, Philippines, etc.), payment aggregators, points of sale terminals for SIM cards, etc., are also reported to be involved in such frauds.

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

(q) Cyber Criminals are using techniques to harvest user credentials, steal OTP etc .There have been several instances of cyber fraudsters using Malicious Android Applications sent through SMS and email. Multiple social engineering techniques in the name of cashback, KYC etc. are used to lure victims download the malicious mobile application. Same application is used with several banking customers by changing Logo /file/bank name.

- Fraudsters sends link to malicious apk file using bulk SMS to potential victims.
- Victim clicks on the short link which results in malicious APK getting downloaded on his/her mobile.
- Permissions are exploited by Android Application for stealing OTP and phone information including send, Receive, Read, Write and Broadcast SMS.