

ગ્રાહકો જોગ જાણવા લાયક અગત્યની સૂચના

પ્રિય ગ્રાહક મિત્રો.....

હાલમાં કેટલાક લેભાગુ વ્યક્તિઓ દ્વારા ગ્રાહકોને છેતરવા માટે લોભામણી સ્કીમ લાવવામાં આવે છે જેમાં ગ્રાહકોને ખુબજ ઓછા સમયમાં રોકાણ કરી ઉચ્ચ વળતર આપવું, પાર્ટ ટાઈમ જોબ ઓફર કરી તેમાં ઉચ્ચ વળતર આપવું વગેરે. આવી સ્કીમ ઈન્ટરનેટ ઉપર જાહેરાત આપી કે ગ્રાહકોના મોબાઈલ નંબર ઉપર SMS દ્વારા મોકલવામાં આવે છે. આવા SMS માં ઘણી વાર ભારતીય નંબરનો પણ ઉપયોગ કરવામાં આવે છે. આવા SMS માં એક લીન્ક મોકલવામાં આવે છે. ગ્રાહકો આવી લીન્ક ઉપર ક્લિક કરેતો એક ચેટ બોક્ષ ઓપન થાય છે અને ગ્રાહકોને ચેટ બોક્ષ દ્વારા વાતચીત કરી તેમને આવી સ્કીમમાં રૂપિયા રોકવા લલચાવવામાં આવે છે. વધુમાં તેઓ આવો ફોડ કરવા મોબાઈલ એપ્લિકેશન, બલ્ક એસ.એમ.એસ. સીમ બોક્ષ બેંક વરચ્યુઅલ પ્રાઈવેટ નેટવર્ક, ફ્રીશીંગ નેટવર્ક, એપ્લિકેશન પ્રોગ્રામીંગ ઈન્ટરફેસ, ક્લાઉડ બેંક સર્વિસ કે વરચ્યુઅલ ખાતા નંબરનો ઉપયોગ કરે છે.

આવા લેભાગુ લોકો તેમની જાહેરાત લોકો સુધી ઝડપથી પહોંચે તે માટે 'Earn Online', 'Part Time Job' વિગેરે જેવા શબ્દોનો ઉલ્લેખ કરતા હોય છે. આવી જાહેરાત ઈન્ટરનેટ ઉપર સામાન્ય સંજોગોમાં સવારે ૧૦:૦૦ થી સાંજનાં ૭:૦૦ વાગ્યા સુધી જોવા મળતી હોય છે, જે ભારતમાં વ્યસ્ત સમય કહેવાય છે. આવી જાહેરાતોમાં લીન્ક ઉપર ક્લિક કરતા ફોડયુલન્ટ વેબસાઈટ ઉપર રીડાયરેક્ટ થાય છે. અને ચેટ બોક્ષ ઓપન થાય છે. તેમાં ગ્રાહકોને આવી સ્કીમમાં રૂપિયા રોકવા લલચાવવામાં આવે છે અને ગ્રાહકોને ઈન્વેસ્ટમેન્ટ લીન્ક મોકલવામાં આવે છે. વધુમાં ગ્રાહકોને તેમનું એકાઉન્ટ એક્ટીવેટ કરવા સ્ક્રીન શોટ મોકલવાનું કહેવામાં આવે છે. એક વખત એકાઉન્ટ એક્ટીવેટ થયા બાદ તેમને ટાસ્ક આપવામાં આવે છે અને તેમને આવી સ્કીમમાં UPI થી રોકાણ કરવા જણાવવામાં આવે છે.

શરૂઆતમાં ગ્રાહક નાની રકમનું આવી સ્કીમમાં રોકાણ કરે છે અને તેમને ઉચ્ચ વળતર સાથે રૂપિયા પરત આપવામાં આવે છે. જ્યારે ગ્રાહક આવી સ્કીમમાં રૂપિયા પરત મેળવે છે ત્યારે ગ્રાહક વધુ વળતરનાં લોભમાં વધુ ઉંચી રકમનું રોકાણ કરે છે. ત્યાર બાદ આવા લોકો ગ્રાહકોને ચેટ બોક્ષમાં જવાબ આપવાનું બંધ કરીદે છે. જેથી ગ્રાહકોને રૂપિયા ગુમાવવાનો વારો આવે છે.

હાલમાં આવી પધ્ધતિથી ગ્રાહકોને છેતરવામાં આવે છે. તેથી ગ્રાહકોએ આવી છેતરામણી સ્કીમમાં રોકાણ કરવું નહીં અને જ્યારે ગ્રાહકો કોઈ સ્કીમમાં રોકાણ કરવા ઓનલાઈન પેમેન્ટ કરતા પહેલા આવી કંપની કે વેબસાઈટની સત્યતાની કાળજીપૂર્વકની ચકાસણી કરી લેવી. જેથી આવી છેતરામણી સ્કીમમાં રોકાણ કરી રૂપિયા ગુમાવવાથી બચી શકાય.

નોંધ: ગ્રાહકે તેમના ખાતાનાં OTP, ડેબીટ કાર્ડને લગતી કે ખાતાને લગતી સંવેદનશીલ માહિતી જેવી કે User Id, Password, CVV વિગેરે કોઈને આપવી નહીં. કોઈપણ અજાણી લીંક ઉપર ક્લિક કરવી નહીં. જ્યારે લીંક ઉપર ક્લિક કરી રૂપિયા ટ્રાન્સફર કરવાના થાય તો ટ્રાન્સફર કરતા પહેલાં તે મેસેજ, એપ્લિકેશન કે વેબસાઈટની સત્યતાની ખાતરી કરી લેવી. બેંક દ્વારા કે બેંકના કોઈપણ કર્મચારી દ્વારા આવી માહિતી ક્યારેય પણ માગવામાં આવતી નથી.

Frauds / Cybercrimes through Investment, Part-Time Job and Ponzi Scheme Scams

The following are some of the common modus operandi adopted by fraudsters and cybercriminals in relation to investment scams, part-time job frauds, and Ponzi schemes, wherein transactions are routed through banking channels:

- A. Victims are targeted through advertisements relating to part-time jobs, online earning opportunities, and investment schemes circulated via the internet, messaging platforms, social media channels, and similar digital mediums. Such advertisements generally promise unusually high commissions or unrealistic returns, such as doubling of money within a short period.

These advertisements or SMS messages typically contain links that redirect victims directly to chat platforms or fraudulent websites. Fraudsters also make use of mobile applications, bulk SMS services, SIM-box-based Virtual Private Networks (VPNs), phishing websites, cloud services, virtual bank accounts, and Application Programming Interfaces (APIs) to facilitate and execute financial frauds.

- B. Fraudsters commonly use keywords such as “Earn Online,” “Part-Time Job,” and similar search terms to ensure that their advertisements appear prominently in internet searches conducted by potential victims. Such advertisements are generally displayed during peak internet usage hours, typically between 10:00 AM and 7:00 PM.

It has also been observed that many fraudulent websites operate using domains such as “xyz” and “wixsite.” These websites often redirect users to messaging platforms or contain embedded chat links that further redirect victims to fraudulent communication channels.

- C. Multiple Indian mobile numbers are used to communicate with victims. Analysis has revealed that, in many instances, the registered holders of such mobile numbers are unaware that messaging platform accounts are being operated in their names. In certain cases, mobile number holders knowingly share One-Time Passwords (OTPs) with fraudsters in exchange for monetary consideration.
- D. Fraudsters generally share investment or task-related links with victims through chat applications. Each victim is assigned a referral code or user identification number. Communication is generally carried out in English, and in several cases, translation tools such as Google Translate are used to interact with victims.
- E. Victims are often instructed to share screenshots through messaging platforms for activation of their accounts. Once activated, victims are initially assigned small tasks in order to gain their confidence.

- F. A mandatory requirement for completing such tasks is the transfer or loading of funds through payment gateways, many of which are not authorised to operate in India. Most payments are routed through UPI channels. Certain UPI IDs are linked to entities registered with the Ministry of Corporate Affairs (MCA).
- G. Fraudsters also operate call centres to interact with victims and provide assistance regarding assigned tasks. For example, if a victim encounters difficulty while transferring funds to an investment website, a call centre executive may contact the victim to facilitate the transaction.
- H. Upon successful completion of the initial task, victims are permitted to withdraw a small amount of money in order to establish credibility and build confidence. Such withdrawals are generally processed through various payment aggregators.
- I. After receiving the first refund or payout, victims are persuaded to undertake additional tasks involving larger monetary transfers. This cycle continues until a substantial amount has been deposited by the victim, after which the fraudsters abruptly discontinue all communication.
- J. UPI details and payment credentials used on fraudulent websites are frequently changed on a daily basis. Although the source code and operating pattern of the websites often remain the same, the domain names are regularly modified to avoid detection.
- K. Bank accounts operated by money mules using genuine or fabricated identification documents are commonly utilised for receiving proceeds of fraud, including funds obtained through compromised bank accounts and misuse of OTPs.
- L. Such rented or mule accounts are generally sourced through agents, and the account holders are paid fixed commissions, rental amounts, or lump-sum compensation for permitting use of their accounts.
- M. Layering of transactions is commonly carried out through multiple account-to-account fund transfers in order to obscure the trail of fraudulent proceeds. Bulk payment mechanisms and API-based transaction systems are also used for this purpose.
- N. Funds routed through intermediate accounts are subsequently diverted into various assets and channels, including cryptocurrencies, bullion, payout accounts, foreign remittances, and person-to-person transfers, with the objective of concealing the origin of funds and laundering proceeds of crime.
- O. Instances have been observed where shell companies with dummy directors, rented companies holding MCA registration certificates, fintech entities, payment gateways, and SMS aggregators are involved in facilitating such fraudulent activities, primarily using UPI as the mode of payment.
- P. The primary objective behind establishing such shell companies is to create current accounts or fintech entities for accepting, routing, or disbursing proceeds of fraud. Many such entities present themselves as technology-based companies.

- Q. UPI IDs are also used to create additional transaction layering behind payment aggregators, thereby facilitating end-of-day settlement mechanisms and concealment of fund flows.
- R. Fraudsters commonly adopt an “Aggregator-on-Aggregator” model to conceal their identities and transaction trails.
- S. Under this arrangement, fraudulent merchants are onboarded onto fintech platforms or payment aggregators. Fraud networks establish payment aggregator businesses either directly in collaboration with banks or indirectly through fintech entities. Fraudsters may operate as sub-aggregators or merchants behind the payment aggregator structure.
- T. Funds collected through such fraudulent arrangements are remitted to payment aggregators, following which API or application-based payouts are executed. Once the aggregator network is operational, payouts are controlled and managed by fraudsters, including those operating from outside India.
- U. Reports indicate involvement of various intermediaries and facilitators, including Chartered Accountants, foreign nationals, payment aggregators, and point-of-sale entities associated with SIM card issuance, in the execution of such fraudulent activities.
- V. Law Enforcement Agencies (LEAs) have observed that gold purchases, cryptocurrency transactions, and international fund transfers are among the most common end-use destinations for proceeds generated through such frauds.