Vikas Arora, IPS

D. O. No. 21796/VA

Commissioner of Police,
Gurugram - 122 001, Haryana
पुलिस आयुक्त,
गुरुग्राम-122001, (हरियाणा)
Off. : 0124-2311200, 2312200
Fax : 0124-2314200

Date 5-11-2024

To,

Residents of Gurugram

I hope this message finds you in good health and high spirits. As the Commissioner of Police, Gurugram, I am reaching out to seek your esteemed collaboration in advancing cyber crime awareness within your neighbourhoods.

Five Major Types of Cyber Frauds

1. Investment Fraud:
   Victim clicks on some investment Ad on popular social media platform like Facebook, Instagram, etc. Fake investment opportunities like: stocks/ commodities trading, business ventures, real estate deals, etc. are being offered to him on fake WhatsApp group. Fraudster explains to the victims about the investment opportunity details and presents fake success stories of others. He also offers training course on trading etc. to victim. The victim is asked to download fake Stock Trading Apps like – VEPro, Anglebg, Anglone, vikinginvest, etc. Victim starts investing with a fake dashboard shows high returns. Victim is initially lured by receiving some petty profits which further encourages him to give away more money. When the victim wishes to withdraw the money, he isn't able to do so.

2. Custom/ Parcel Delivery Fraud (Digital Arrest):
   Victim receives a call from a person impersonating as official from Custom Department/ FedEx company claiming that he has allegedly sent a parcel which contains illegal material like drugs, foreign currency, arms and ammunition etc. The phone is redirected allegedly to Police department whereby the said person instructs the victim to download Skype App and remain on Video call till further directions. The cyber fraudster can be seen in a fake police uniform and impersonates a police station setup and claim that the victim is under 'Digital arrest'. The cyber fraudster further directs the victim to share details of all bank accounts and ask the victim to transfer the money into the accounts sent by them in lieu of verifying whether the money is not obtained from ill means. They promise to return back the entire amount upon proper verification. Once all the money is transferred, the fraudster disconnects the call and victim loses all his money.

3. Fake Call Fraud (Vishing):
   Victim receives a call from someone claiming to be a police officer, doctor, or relative. These callers often use fake caller ID information to appear legitimate like WhatsApp profile pic, AI generated voice etc. While impersonating as police official, the cyber fraudster warns that a relative of the victim has broken a law (Eg. molested a girl, violated traffic signal, kidnapped a colleague etc.) and demands money generally through UPI. While impersonating as a doctor

or relative, the cyber fraudster allegedly claims that relative of the victim is in distress and demands instant money generally through UPI.

4. Task Based Fraud:
   Victim receives a message for part time work with easy money on WhatsApp. Typical tasks, for instance, like or comment a YouTube video, Facebook / Instagram likes, google map reviews, etc. are being offered to him. Initially, fraudsters may send victim some money (Rs 150-500) to win his/her trust. The fraudster further asks personal information and convince victim to download Telegram app. Now, victim is asked to invest his money to play high value tasks to get high returns. Fake Dashboard shows high profits/gains to victim. Now, Victim wants to withdraw, but he cannot! Further, fraudsters try to convince to take last task (high value) to withdraw money. Else, entire amount invested will be forfeited.

5. Scams via Search Engine Searches:
   Victim search on search engines (google, etc) about hotels, ticket booking, customer care number etc. He may get fake results via sponsored ad's, links, leading to fake websites or contact numbers. He falls prey to look alike but fake phishing websites, numbers etc. On pretext of calling customer care of reputed brand store based on online searches, he actually is calling a cyber fraudster. The fraudster lures with offers, convenience at your door-step, easy/fast resolutions of your needs but actually dupes the victim robbing him of hard-earned money.

Precautions: Be cautious about fake online advertisements and do not click on unknown links/ engage with unknown suspicious person online. Be skeptical about free offers, high returns, easy money schemes. **Dial 1930** to report any cyber crime or lodge cyber complaint on **cybercrime.gov.in.** Immediate reporting of the cyber crime is of paramount importance as the earlier the intimation is done, higher is the probability of getting the defrauded money back.

I encourage you to organize informative sessions, distribute educational materials, and foster discussions that elevate awareness about cyber safety regarding the aforesaid modus operandi of cyber crime in your societies.

Furthermore, in instances where any society member falls victim to cyber fraud, kindly ensure that necessary precautions and reporting mechanism may be informed to him. Wherever possible, you may assist him to the nearest cyber police station. In nearer future, any person may be enquired whether such information was disseminated to him/ her through you or your representative. Moreover, police station wise meeting will be conducted of all the RWA presidents at the nearest police station shortly with representation from Cyber police station to aware you about all the modus operandi of cyber crime. Your presence is mandated in such meeting.

Together, let us empower our residents with the knowledge and tools necessary to navigate the digital landscape safely. Thank you for your unwavering commitment to the well-being of our community.

Warm regards,

(Vikas Arora, IPS)