BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Hyderabad Man Loses ₹2.43 Cr in Fake Investment App Scheme

Incident: A 56-year-old from Hyderabad was lured into an investment scam via social media ads promoting a trading app mimicking legitimate financial service providers.

Modus Operandi: After downloading the fake app, he was shown consistent profits, boosting his confidence. He kept depositing increasing amounts—believing he could withdraw at any time. Eventually, ₹2.43 crore had been invested. But when he attempted a withdrawal, all activity was blocked.

Action Taken: Police traced the bank accounts used and arrested a 22-year-old account supplier from Navi Mumbai who was allegedly facilitating the fraud.

Key Concern: Fraudsters are leveraging cloned apps and gamified interfaces to build trust over time before cutting off access entirely and disappearing with the victim's savings.

Mumbai Senior Duped of ₹2.21 Cr in Fake Provident Fund Verification

Incident: An elderly resident of Nana Chowk, Mumbai, lost ₹2.21 crore after falling prey to scammers posing as officials from the Provident Fund department.

Modus Operandi: The victim received a call from individuals claiming to be verification officers who insisted on validating her PF credentials. Trusting the legitimacy of the call, she began transferring money as instructed—believing it was for official processes. Within hours, her savings were siphoned off into numerous bank accounts.

Action Taken: A case has been registered with the South Cyber Cell. No arrests have been made yet, and the stolen funds remain untraced.

Key Concern: This case showcases the growing trend of fraudsters impersonating government officials to exploit senior citizens, using intricate laundering tactics involving cryptocurrency and cross-border accounts.

Chandigarh Man Scammed of ₹3.66 Cr in High-End Stock Market Trap

Incident: Surinder Kumar Thakur from Sector 49 joined a WhatsApp group promising premium stock tips and market predictions. Within months, he was conned into investing ₹3.66 crore.

Modus Operandi: Group admins claimed affiliation with top-tier financial advisory firms. They shared detailed trading analysis and daily returns, and offered private coaching. After a few small successful trades, Thakur was persuaded to invest crores into what turned out to be a fake trading dashboard. The entire ecosystem—from the group members to the trading portal—was fake.

Action Taken: Chandigarh Police arrested six accused, including one from Tihar Jail already involved in cybercrime. The scam has been linked to multiple other fraud cases across northern India.

Key Concern: Elaborate fake communities and convincing impersonators are being used to trap even seasoned investors.

₹60 Lakh Ransom Demanded in Bengaluru Ransomware Attack

Incident: A structural design firm in Bengaluru fell victim to a ransomware attack. Hackers encrypted critical business files and stole sensitive client information.

Modus Operandi: The attack occurred within a 40-minute window on March 31. After infiltrating the company's systems, the attackers demanded up to ₹60 lakh for data restoration and to avoid public leaks. Communication came through anonymous email and Telegram channels often linked to international cybercrime groups.

Action Taken: An FIR was filed under the Information Technology Act. Investigations are ongoing.

Key Concern: Ransomware is no longer targeting only large enterprises—SMBs are increasingly vulnerable and often underprepared.

Retired Mumbai Teacher Loses ₹1.72 Cr in Fake Crime Branch Scam

Incident: A 61-year-old retired schoolteacher from Mahim was duped of ₹1.72 crore by cybercriminals posing as courier agents, police officers, and financial investigators.

Modus Operandi: The fraud began with a WhatsApp call claiming a suspicious parcel in her name contained drugs and fake documents. The scammers, posing as law enforcement, told her she was linked to a criminal case and used fear of arrest to pressure her into transferring money over several weeks.

Action Taken: An FIR has been filed; police are tracing the transaction trail and digital leads.

Key Concern: Scammers are exploiting fear and impersonating multiple authorities to trap vulnerable individuals into high-value frauds.