BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Delhi man loses ₹25 lakh in 'digital arrest' fraud: three arrested

Incident
A resident was duped into transferring ₹25 lakh after receiving a video call from someone impersonating a crime branch officer. The caller falsely claimed that the victim's Aadhaar details had been misused to open fraudulent bank accounts linked to money laundering by a major airline company. The victim, under pressure and fear, complied with the instructions and transferred the money.

Modus Operandi
The fraudsters executed the scam from hotel rooms, using video calls to impersonate law enforcement officers and create a sense of urgency. They fabricated a scenario involving identity misuse and financial crimes. To facilitate transactions, they collaborated with account holders (referred to as 'mules') who were brought in person to enable the money transfers.

Action Taken
Upon receiving the complaint, law enforcement authorities traced the accused to a hotel in the Paharganj area. Three individuals were arrested in connection with the case. Investigations confirmed their roles in orchestrating the fraud and using mule accounts for laundering the stolen money.

Key Concern
The incident highlights the growing threat of impersonation scams and 'digital arrest' tactics, where individuals are psychologically manipulated into believing they are under investigation. The misuse of official identities and fear tactics underscores the urgent need for public awareness and stronger safeguards against cyber-enabled financial frauds.

Cyber thugs trapped seven people, cheated them and defrauded them of ₹ 3.7 crore

Incident
In a rising wave of cyber fraud, several individuals were duped under different pretexts, amounting to a reported loss of over ₹5 crore this month. Notably, one case involved a digital arrest scam. Multiple victims across different regions fell prey to cybercriminals using tactics such as impersonation, fake investment offers, fraudulent customer service numbers, and phishing links.

Modus Operandi
Cybercriminals employed a variety of deceptive tactics to defraud victims. In one case, the victim was threatened with arrest after being falsely linked to a money laundering investigation, a typical example of a "digital arrest" scam. In another, fraudsters used the lure of high earnings through a gaming app investment scheme to siphon off ₹1.7 crore. Some victims became targets after searching for services online; one individual looking for AC repair found a fake customer care number on Google and lost ₹5.7 lakh after transferring a nominal amount. In another instance, a man was offered a cement dealership and lost ₹14 lakh after clicking on a fraudulent WhatsApp link. Similarly, another victim clicked a link sent via WhatsApp, which resulted in his phone being hacked and ₹15 lakh withdrawn from his bank account. These scams relied heavily on social engineering, impersonation, and malicious digital content to exploit user trust and trigger financial transactions.

Action Taken
The cases have been reported to the police, with at least seven formal complaints received in the current month. Authorities are investigating the incidents, but specific outcomes such as arrests or recoveries were not detailed in the report.

Key Concern
The cases underscore a disturbing trend: cybercriminals are diversifying their techniques—ranging from impersonation and social engineering to phishing and fake online services. Public unawareness, especially regarding fraudulent digital touchpoints like fake numbers or links, continues to enable large-scale financial losses. The scale and variety of these scams emphasize the urgent need for continuous cyber hygiene education and robust digital literacy among citizens.

Coimbatore entrepreneur duped of ₹64 lakh online in overseas job

Incident
A woman entrepreneur from Coimbatore lost approximately ₹64 lakh in an elaborate online scam related to overseas job placements. She was lured by a Facebook advertisement offering affordable international job opportunities. Trusting the legitimacy of the offer, she proceeded to make payments over several transactions in exchange for work-related documentation for her clients.

Modus Operandi
The scam was orchestrated through a fake Facebook advertisement that promised low-cost overseas job placements. The victim, who runs a company that facilitates foreign placements, responded to the ad and entered into an agreement with a purported firm. Believing the company to be genuine, she made multiple payments totalling ₹64 lakh to a bank account, allegedly for visa invitations, work permits, and other job-related documents for her clients. It was later revealed that the company was fictitious, and the entire operation was a fraudulent setup.

Action Taken
The Cyber Crime Police arrested a 25-year-old man from Gujarat in connection with the case. He is alleged to have posted the fraudulent advertisement and received the funds. Investigations are ongoing to trace further links and identify any additional accomplices involved in the scam.

Key Concern
This case highlights the increasing sophistication of cyber scams that exploit the aspirations of individuals and businesses alike. The use of fake corporate identities, online advertisements, and believable service offerings makes such frauds harder to detect. It underscores the importance of verifying digital entities and exercising caution when engaging in high-value online transactions, especially in sectors involving international employment and migration services.

Gurugram cops bust ₹72-cr cyber fraud syndicate

Incident
A major cyber fraud racket has been uncovered involving 55 individuals who allegedly defrauded people across India of a staggering ₹72.49 crore. These individuals were linked to 18,228 complaints and 597 FIRs registered nationwide, including 48 in Haryana alone. The scale and geographic spread of the operation indicate a deeply rooted and coordinated cybercrime network.

Modus Operandi
The fraudsters operated a complex web of scams that included fake social media profiles, sextortion schemes, investment frauds, and impersonation-based FedEx scams. They posed as fake officials or representatives to deceive victims and extract money through threats, emotional manipulation, or false promises. These tactics exploited both fear and greed, relying heavily on digital platforms to reach and manipulate their targets.

Action Taken
Between January and May 2025, 55 cybercriminals were arrested from various parts of the country, including Maharashtra, Rajasthan, Delhi, Punjab, Jharkhand, Madhya Pradesh, Uttar Pradesh, and Chandigarh. The arrests were carried out by cyber-crime police teams under Gurugram's Cyber East, Cyber West, and Cyber South police stations. During the operation, authorities recovered 21 mobile phones and 11 SIM cards, which have been sent to the Indian Cyber Crime Coordination Centre (I4C) for forensic analysis to aid further investigation.

Key Concern
This case underscores the scale and sophistication of modern cybercrime, with fraudsters exploiting digital channels to target victims across the country. The variety of scams—ranging from sextortion to investment fraud—demonstrates the adaptability of these networks. It highlights the urgent need for enhanced digital vigilance, stronger law enforcement collaboration across states, and ongoing public education to recognize and avoid such cyber threats.