BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Cyber fraud accused nabbed by Hyderabad police at Mumbai airport

Incident
A man involved in a major digital arrest fraud case was detained by immigration authorities at Mumbai International Airport and subsequently arrested by the Hyderabad Cyber Crime Police. The case relates to a deceptive operation that targeted a woman under the guise of a legal investigation.

Modus Operandi
The fraud was executed by a network posing as legal authorities to intimidate and extract sensitive information and money from the victim. The accused were part of an organized racket, where certain members acted as account suppliers or holders to facilitate the transfer and laundering of illicit funds. The scam was sophisticated in its approach, simulating authentic legal proceedings to manipulate the victim into compliance.

Action Taken
The arrest was made based on a Look Out Circular issued by law enforcement. Several individuals connected to the same racket had been apprehended in an earlier phase of the investigation. Charges have been filed under relevant provisions of the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita.

Key Concern
This case highlights the growing threat of impersonation and psychological manipulation in digital frauds. The use of fabricated legal pressure tactics not only undermines public trust in official communication but also exposes the vulnerabilities of unsuspecting individuals to highly coordinated cybercrime networks.

CBI conducts raids in 7 states, arrests 3 over cybercrimes, digital arrests

Incident
The Central Bureau of Investigation (CBI) conducted coordinated raids across seven states—Delhi, Bihar, Madhya Pradesh, Kerala, Punjab, Rajasthan, and Andhra Pradesh—as part of an ongoing investigation into cybercrime, specifically digital arrest scams. Three individuals were arrested in connection with the probe, which had previously uncovered over 850,000 mule bank accounts spread across 700 branches nationwide.

Modus Operandi
Cybercriminals employed a widespread network of mule accounts to facilitate the laundering of fraudulent proceeds. These accounts were allegedly opened and operated with the assistance of middlemen, agents, and in some cases, complicit bank employees. The network enabled seamless receipt, transfer, and withdrawal of illicit funds generated through scams, including those involving fabricated digital arrest narratives.

Action Taken
As part of Operation Chakra-V, CBI executed search operations at multiple premises, leading to the recovery of critical evidence such as mobile phones, KYC documents, transaction records, and account opening forms. A formal case was registered on June 25 against 37 individuals, comprising suspected mule account holders, intermediaries, and bank personnel believed to have collaborated with cyber fraudsters.

Key Concern
The scale of the mule account network reveals a deeply entrenched infrastructure supporting cybercrime in India. The collusion of financial intermediaries, including bank insiders, significantly amplifies the threat landscape, calling for stringent verification mechanisms and real-time fraud monitoring within banking institutions.

UP cyber fraudsters brought to Chennai for duping locals of Rs 48 lakh via fake trading app

Incident
Four individuals from Uttar Pradesh were arrested for defrauding Chennai residents of ₹48 lakh through an online trading scam. The arrests were made based on warrants issued by a Chennai court while the accused were already in custody for a separate cybercrime.

Modus Operandi
The group created 153 mule bank accounts linked to mobile numbers to collect and move stolen funds. These funds were routed through multiple accounts, converted into cryptocurrency and US dollars, then withdrawn in Indian rupees. They used a mobile app called ‘Chinese Dragon’ to give international associates real-time access and control over transactions via API tools.

Action Taken
With court approval, the suspects were brought to Chennai by the Cyber Crime Police. One additional accused, believed to be the coordinator with international ties, is currently in custody in Telangana. The case is connected to multiple complaints filed through the National Cyber Crime Reporting Portal.

Key Concern
This case highlights the increasing use of advanced tools and cross-border networks in cyber frauds. The combination of remote access apps, digital currencies, and foreign collaboration makes detection and enforcement more complex.

50-Year-Old Chembur Businessman Duped of ₹90,000 Via Hacked WhatsApp Account of Sister-In-Law; Case Registered

Incident
A 50-year-old businessman from Chembur was defrauded of ₹90,000 after receiving a WhatsApp message from a number impersonating his sister-in-law. The fraud occurred on July 5 and was later reported to the Cybercrime Helpline and local police.

Modus Operandi
The fraudster used a U.S.-based WhatsApp number with the victim’s relative’s profile photo and claimed it was her new contact. Under the pretence of an emergency, they requested a money transfer via Google Pay to an Indian number. The victim, unaware of the hack, transferred the amount promptly.

Action Taken
The victim contacted the 1930 cybercrime helpline and filed a complaint at the Chembur Police Station. A case was registered under relevant sections of the Bharatiya Nyay Sanhita and the Information Technology Act.

Key Concern
This incident illustrates how easily trust can be exploited through hacked social media accounts. The use of familiar identities adds urgency and credibility, making it harder for victims to detect fraud in time.