BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Navi Mumbai Cyber Police Bust ₹4.71 Crore Investment Scam, 2 Held

Incident
A 70-year-old retired government officer was defrauded of ₹4.71 crore in a large-scale online investment scam. The fraud occurred between late November 2024 and early March 2025, during which the victim was lured with promises of high returns through IPO and Index Trading investments. Over several months, the individual was systematically manipulated into transferring funds to multiple bank accounts under the pretense of legitimate financial opportunities.

Modus Operandi
The scammers approached the victim with convincing offers of high-return investments in IPOs and Index Trading. Using persuasive communication and financial jargon, they gained the victim's trust and encouraged multiple transfers of large sums to different accounts. The fraudulent scheme was carefully orchestrated to appear credible and professional, reducing suspicion and prolonging the deception.

Action Taken
After the complaint was registered, the cyber investigation team conducted a thorough analysis of the digital footprint and banking transactions associated with the fraud. Based on this technical evidence, two individuals involved in the scheme were identified and taken into custody. The case has been registered under relevant sections of the Indian Penal Code and the Information Technology Act, and further investigation is underway.

Key Concern
This incident highlights the growing threat of cyber fraud targeting elderly individuals through financial schemes that appear legitimate. With the increasing use of digital platforms to execute such crimes, it has become essential to strengthen awareness around online investment fraud, particularly among vulnerable populations who may not be familiar with the warning signs of digital deception.

Rajasthan Police warn people of cyber fraudsters impersonating SEBI officials:

Incident
A new cyber fraud trend has emerged where scammers are impersonating regulatory officials to deceive investors. Using the names and symbols of financial regulatory bodies, cybercriminals are sending out forged documents to trick individuals into believing they are dealing with legitimate recovery and compliance communications. This sophisticated scam is designed to exploit the trust that people place in official institutions.

Modus Operandi
Fraudsters are generating fake letters on forged letterheads, using fabricated seals and bogus recovery certificates that appear authentic. These documents closely resemble formal communication typically issued by regulatory authorities. By posing as officials, the scammers aim to mislead victims into believing they are entitled to financial recoveries or need to act on regulatory instructions. The appearance of authenticity in these documents makes them particularly convincing and dangerous.

Action Taken
The cybercrime unit has issued a formal public warning, alerting citizens to this emerging scam. Authorities have urged the public to remain cautious and not fall prey to communications that appear to be from regulatory bodies without proper verification. They are also advising citizens to cross-check any such documents or recovery claims through official digital platforms and recommended verification mechanisms.

Key Concern
This case reflects the growing sophistication of impersonation-based cyber frauds, especially those that leverage the credibility of official institutions. With documents that closely mimic regulatory correspondence, unsuspecting individuals—particularly investors—are at heightened risk of falling victim. The incident underscores the urgent need for greater public awareness about how to verify financial communications and identify red flags in digital interactions.

₹11.55 Crore Fraud After Server of Himachal Pradesh State Cooperative Bank Hacked

Incident
An elaborate cyber fraud amounting to ₹11.55 crore has targeted a cooperative bank, leading to a multi-state investigation. The case involves a sophisticated server breach that enabled unauthorized access and fraudulent transactions, highlighting a significant breach in financial cybersecurity infrastructure.

Modus Operandi
The fraud was executed through a complex hacking operation involving unauthorized access to the bank's internal systems. Funds were diverted into multiple beneficiary accounts, some of which recorded transactions ranging from ₹16 lakh to ₹48 lakh. The technical nature of the breach suggests the involvement of skilled actors using advanced methods to exploit backend vulnerabilities in the bank's systems.

Action Taken
In a coordinated enforcement effort across multiple states—including Maharashtra, Rajasthan, Delhi, and Uttar Pradesh—four individuals were apprehended. Two of them, whose accounts reflected substantial transaction volumes, have been remanded to judicial custody. The other two were released on notice due to lower-value transactions and limited cooperation with investigators. Bank accounts connected to the fraud have been frozen, and further analysis is underway to identify additional suspects involved in the financial trail.

Key Concern
This case underscores the growing threat of targeted cyberattacks on banking infrastructure. The ability of threat actors to infiltrate core systems and execute high-value fraud reflects vulnerabilities in server-level security protocols. It also highlights the urgent need for enhanced digital forensics, better incident response coordination across jurisdictions, and proactive cyber hygiene practices within critical financial institutions.

Elderly couple duped of ₹4.79 crore in ‘digital arrest’ scam, 2 arrested

Incident
An elderly couple fell victim to a cyber extortion scam, resulting in a financial loss of ₹4.79 crore. The fraud took place over nearly three months, from mid-March to mid-May, during which the couple was manipulated into believing they were under a so-called “digital arrest” by national law enforcement agencies. The victims, isolated and vulnerable, complied with the instructions of the fraudsters, leading to repeated high-value fund transfers.

Modus Operandi
The fraudsters contacted the couple posing as bank officials, initially claiming that there were discrepancies and overdue bills linked to their credit card. They escalated the deception by alleging that the couple's bank accounts were involved in money laundering activities. Fake arrest warrants were sent, purportedly issued by national investigative agencies. To intensify the psychological pressure, the scammers conducted video calls while impersonating officials, thereby convincing the victims of the urgency and severity of the situation. This led the couple to transfer large sums of money over multiple transactions.

Action Taken
The cybercrime unit initiated a financial tracking operation after the complaint was filed. By analysing the bank accounts that had received the funds, the investigation team identified and apprehended two suspects involved in the scam. Both individuals were traced using digital footprints and financial transaction records. Their accounts, which received transfers amounting to several crores, have been flagged and are part of the ongoing investigation.

Key Concern
This incident sheds light on the alarming trend of psychological manipulation in cybercrime, where fear and authority are used as tools to extort money. The concept of a "digital arrest" and impersonation of law enforcement not only induces panic among victims but also creates a false sense of legitimacy. It also highlights the vulnerability of elderly citizens, especially those living in isolation, to scams that exploit trust, fear, and lack of digital awareness. Strengthening public education around such tactics is critical to prevent further incidents.

Three arrested in ₹2.5-cr digital arrest scam busted by Chandigarh Police

Incident
A high-value cyber fraud amounting to ₹2.5 crore has come to light, involving the manipulation and intimidation of an individual through impersonation of regulatory and law enforcement authorities. The incident occurred in early May, when the victim was coerced into transferring her entire life savings under the pretense of legal scrutiny and arrest. The matter was formally registered in early June under multiple sections of the updated legal framework.

Modus Operandi
The scam began with a phone call falsely attributed to a telecom regulatory body, alleging that the victim’s SIM card was linked to unlawful activities. This was followed by WhatsApp video calls from individuals posing as high-ranking law enforcement officers, including senior officials and even a judge. The fraudsters used forged documents such as fake arrest warrants and employed psychological tactics to instil fear. Under intense pressure and manipulation, the victim was persuaded to transfer funds into various accounts for "verification" to supposedly clear her name from fabricated charges.

Action Taken
Following the complaint, cybercrime investigators launched a multi-pronged digital investigation involving call data records, IP tracking, and Know Your Customer (KYC) analysis. These efforts led to the identification and arrest of three individuals across multiple states. The accused are currently under custody, and further analysis of digital and financial trails is ongoing to uncover the full network behind the scam.

Key Concern
This case demonstrates a disturbing evolution in cyber fraud, where impersonation of high-level legal and government authorities is used to create panic and extract money from unsuspecting citizens. The emotional and psychological stress imposed on victims through such scams often leads to hurried decisions and massive financial losses. It underlines the urgent need for public sensitization on how to verify official communications and recognize red flags in high-pressure digital interactions.