BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

CBI Traces ₹7.67 Crore Cyber Extortion Trail

Incident
A resident of Rajasthan became the victim of a sophisticated digital arrest scam. The individual was coerced into transferring a substantial amount of money under the pretence of avoiding legal consequences, ultimately losing ₹7.67 crore.

Modus Operandi
Cybercriminals executed the scam by impersonating law enforcement officials. They used fake identities and manipulated digital platforms to establish credibility. The victim was threatened with severe legal repercussions, which pressured them into transferring the funds to the fraudsters.

Action Taken
In response to the incident, the Central Bureau of Investigation (CBI) launched a detailed investigation under Operation Chakra-V. As a result, two more individuals were arrested, bringing the total number of arrests to six. The operation also led to nationwide raids, including locations in Mumbai and other major cities.

Key Concern
This case underscores the growing threat of digital arrest scams and the alarming ease with which cybercriminals can exploit fear and impersonate authorities. It highlights the need for greater public awareness and stronger verification mechanisms to prevent such high-value frauds in the future.

Private Employee Loses ₹1.16 Crore in Online Trading Scam

Incident:
A 33-year-old private employee from Madhapur, Hyderabad, fell victim to a sophisticated investment scam. The individual was lured into making substantial financial transfers totalling ₹1.16 crore, believing them to be legitimate investments based on trading advice.

Modus Operandi:
The scam began when the victim was added to a Telegram group by unknown fraudsters posing as financial experts. They provided fake trading tips and initially showed false profits to gain trust. Over time, the victim was manipulated into investing large sums of money through both bank and e-wallet transfers, under the illusion of guaranteed returns.

Action Taken:
After the victim requested to withdraw the supposed profits, the scammers blocked all communication. A complaint was subsequently registered with the Cyberabad police (Commissionerate area of Hyderabad), who have initiated an investigation into the matter.

Key Concern:
This case highlights the growing prevalence of online investment scams on social media platforms and messaging apps. It emphasizes the need for heightened vigilance, financial literacy, and public education on recognizing fraudulent schemes before significant losses occur.

MBA Students Lost ₹43 Lakh to Fake CBI Threat in Mumbai

Incident:
A student became the target of a fear-driven digital scam, resulting in a financial loss of ₹43 lakh. The scam unfolded through a series of threats and manipulative tactics used by cybercriminals posing as government officials.

Modus Operandi:
The attackers impersonated officials from the Central Bureau of Investigation (CBI) and falsely accused the student of being involved in 50 criminal cases. They further escalated fear by threatening jail time and the arrest of the student's father, creating intense psychological pressure.

Action Taken:
The scam led the student to make multiple fund transfers totalling ₹43 lakh. Although the exact steps taken by law enforcement have not been detailed, the nature of the scam indicates that an official complaint was likely filed, and investigative efforts initiated.

Key Concern:
This case underlines the severe impact of fear-based manipulation in cyber fraud, especially when targeting vulnerable individuals like students. It also highlights the urgent need for awareness around impersonation scams and better safeguards against psychological coercion tactics.

Cuttack Cyber Police Bust ₹78 Lakh Online Trading Fraud

Incident:
Victims were defrauded through a fake online trading scheme, leading to a financial loss of ₹78,00,000. The scam was conducted in a staged manner, with victims making multiple transfers to different bank accounts based on false promises of high returns.

Modus Operandi:
The fraudsters created a fake trading company and lured victims through Telegram groups. They assured high profits to build trust and persuaded victims to make repeated bank transfers. The scam exploited digital communication platforms and fabricated investment opportunities to deceive individuals.

Action Taken:
Law enforcement authorities arrested six individuals involved in the scam. During the investigation, crucial evidence was seized, including Telegram chat logs and bank transaction records from DBS, IDFC, and Bandhan Bank accounts used to receive the fraudulent funds.

Key Concern:
This case highlights the increasing use of encrypted messaging platforms like Telegram for financial frauds. It emphasizes the need for tighter monitoring of digital financial activities and greater public education on recognizing and avoiding high-return scams.

Faridabad Cyber Police Nail ₹1 Crore Stock-Trading Racket

Incident:
A victim was defrauded of over ₹1.10 crore in a honey-trap scam that began through a dating app. The scam escalated when the victim was directed to a fraudulent trading platform and manipulated into making large financial transfers.

Modus Operandi:
The accused used a honey-trap tactic by initiating contact through a dating app and then moving the conversation to WhatsApp. There, they shared a link to a fake trading application. Once the victim logged in and began investing, the fraudsters disabled withdrawal options and demanded an additional ₹24 lakh, further exploiting the victim's trust and desperation.

Action Taken:
Two individuals, Satyam and Raj Kapur from Kanpur, were arrested in connection with the case. A formal complaint was filed at the Central Cyber Police Station, and the arrested accused were placed in four-day custody for further interrogation and investigation.

Key Concern:
This case underscores the blending of social engineering and financial fraud, where emotional manipulation is used to trap victims into high-stakes scams. It also points to the growing misuse of dating platforms and messaging apps in cybercrime, calling for enhanced user vigilance and regulatory oversight.