BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Three arrested for cyber fraud, duping man of Rs 70 lakh in Odisha

Incident
A cyber fraud case was reported in which an individual was duped of ₹70 lakh after being lured into a fraudulent investment scheme. The individual had been seeking part-time employment and came across an offer promising high returns from stock market investments.

Modus Operandi
The victim received a message via WhatsApp containing a link to a part-time job opportunity. Upon clicking the link, they were redirected to a Telegram group. Initially, small tasks such as rating business establishments on Google were assigned, for which the victim received minor payments—creating a false sense of legitimacy. Gradually, the fraudsters convinced the victim to invest substantial amounts of money, under the pretext of stock market trading with guaranteed high returns. Investigations revealed that the fraud network utilized mule bank accounts to route the funds, with operatives located across multiple regions in the country.

Action Taken
Law enforcement authorities arrested three individuals linked to the fraud. It was determined that a portion of the defrauded amount had been transferred to one of their bank accounts. Two of the individuals were found to be responsible for sourcing mule accounts used in the scam. During the operation, mobile phones and an ATM card were seized as evidence.

Key Concern
This case underscores the growing threat of organized cyber fraud operations leveraging digital communication platforms and deceptive employment offers. The use of mule accounts and cross-regional collaboration by fraudsters highlights the urgent need for increased public awareness, digital vigilance, and coordinated enforcement efforts to combat such schemes.

45-year-old doctor duped of Rs. 1.23 crores by cyber fraudsters in a ‘Digital Arrest’

Incident
An individual from the city was defrauded of ₹1.23 crore in a sophisticated cyber scam known as a 'Digital Arrest.' The victim, a 45-year-old professional, was coerced into transferring the amount over multiple transactions under the false pretense of being involved in a criminal investigation.

Modus Operandi
The scam began with a phone call from an unknown number, during which the caller falsely claimed that a parcel addressed to the victim contained illegal items such as police uniforms, banned medical substances, and identification cards of law enforcement officials. This was followed by video calls from individuals posing as police officers, who threatened the victim with arrest. Exploiting fear and urgency, the fraudsters conducted several video conference calls, during which they demanded financial verification. Under this guise, the victim was manipulated into transferring over ₹1.23 crore through multiple transactions.

Action Taken
Upon realizing the deception, the victim reported the matter to the authorities. A formal case has been registered, and investigations are underway to identify and apprehend those involved in the scam.

Key Concern
This case highlights the alarming rise of 'Digital Arrest' scams, where cybercriminals impersonate law enforcement to exploit victims through psychological intimidation and social engineering. The use of video conferencing adds a layer of perceived authenticity, making it difficult for individuals to discern the fraud. There is a critical need for public awareness regarding such tactics and stronger mechanisms to trace and curb these evolving cyber threats

Negligence in ₹1.38 Cr Fraud Probe: Three Cybercrime Cops Suspended

Incident
A cyber fraud case involving a financial loss of ₹1.38 crore was reported by a city resident who fell victim to an elaborate investment scam. Despite the severity of the case, procedural lapses in the investigation led to disciplinary action against three personnel from the cybercrime unit.

Modus Operandi
The victim was targeted through a sophisticated scam that promised high returns from investments in stock market trading and IPO subscriptions. Cyber criminals used deceptive tactics to gain the victim’s trust and orchestrated the fraud through multiple transactions, gradually siphoning off the amount.

Action Taken
Following a routine review of the case, serious lapses in investigative diligence were identified. A report submitted by a senior officer highlighted the failure of the investigating team to act promptly and follow established protocols. As a result, three members of the cybercrime unit were suspended for negligence, marking a rare instance of internal accountability in handling cybercrime cases.

Key Concern
This case underscores the dual threat posed by both external cybercriminals and internal procedural failures. While public awareness of cyber threats is essential, timely and effective law enforcement response is equally critical. The incident reveals gaps in investigative accountability and the urgent need to reinforce capacity-building and oversight within cybercrime units.

In 15 months, Gujarat Police recovered over Rs 147 crore lost to cyber fraud. Reporting within 8 hours the key, say officers.

Incident
Over the last 15 months, a significant rise in cyber fraud incidents has been observed, resulting in financial losses totalling Rs 1,761.73 crore. These cases form a substantial portion of the overall Rs 2,941 crore lost to cyber frauds since 2020, coinciding with increased digital activity following the onset of the COVID-19 pandemic.

Modus Operandi
Cyber fraudsters exploited digital platforms, often executing scams that required swift reporting for successful intervention. A crucial factor in mitigating these losses was the prompt reporting of incidents within an eight-hour window from the time of the crime. This early window proved essential in facilitating recovery efforts through active coordination mechanisms.

Action Taken
Between January 1, 2024, and April 30, 2025, law enforcement agencies successfully recovered Rs 147.74 crore, more than half of the Rs 218.16 crore recovered since 2020. This achievement is attributed to the effective functioning of a dedicated cybercrime helpline and proactive collaboration with financial institutions. In 2024 alone, Rs 113.33 crore was returned to victims, with an additional Rs 34.41 crore recovered in 2025 thus far. Additionally, Rs 672.55 crore worth of fraudulent transactions have been traced and frozen, pending judicial orders for disbursement.

Key Concern
Despite notable recovery efforts, the volume of financial loss due to cyber fraud remains alarmingly high. A major concern is the disparity between the total losses and the amount recovered or frozen. The sustained vulnerability of individuals and organizations to digital fraud highlights the urgent need for enhanced cyber hygiene, broader public awareness, and more robust preventive frameworks.

Two online fraud cases lodged where citizens lost ₹49 lakh

Incident
Two separate cyber fraud cases have been reported, resulting in combined financial losses of approximately ₹48.85 lakh. In the first case, a resident was defrauded of ₹40.26 lakh under the pretense of high returns in online trading. In the second incident, another individual lost ₹8.59 lakh through a deceptive link that compromised their bank deposit.

Modus Operandi
In the first case, the fraudsters lured the victim by promising substantial profits through online gold trading and share investments. The victim was persuaded to make multiple transfers totalling ₹40.26 lakh before realizing the scam in October 2024.
In the second case, the perpetrators used a phishing technique by sending a fraudulent link. Upon clicking, the victim's fixed deposit was illicitly accessed and siphoned off.

Action Taken
Following the complaints, the Baner police have registered formal cases in both instances. For the investment fraud, the police have begun analyzing the beneficiary accounts where the funds were transferred, and an investigation is underway. In the second case involving a bank fraud, a First Information Report (FIR) was lodged on May 14, 2025, for an incident that occurred on April 20. Further inquiries are ongoing.

Key Concern
These cases reflect the persistent vulnerability of individuals to investment and phishing scams, particularly those involving enticing financial returns or deceptive digital communication. Delayed reporting further complicates recovery efforts. The incidents underscore the pressing need for increased awareness, real-time fraud detection systems, and prompt response mechanisms.

From Dropout to B.Tech. Graduate, 12 held as Bengaluru Cops Bust Cybercrime Ring Run from UP, Bihar

Incident
A cybercrime racket operating under the guise of work-from-home job offers was dismantled by law enforcement in southeastern Bengaluru. The case came to light after a homemaker reported a loss of Rs 5 lakh on January 22, 2025, after being deceived by false employment promises.

Modus Operandi
The perpetrators approached victims with seemingly lucrative work-from-home opportunities. Once interest was shown, they fabricated reasons—such as a "low credit score"—to justify upfront payments. Victims were then manipulated into transferring funds in multiple instalments under the belief that these payments were necessary to receive their promised earnings.

Action Taken
A total of 12 individuals were arrested in connection with the scam. The group, primarily from Uttar Pradesh and Bihar, was led by two individuals with contrasting backgrounds—one a technically skilled but unemployed engineering graduate, the other a former labourer with an extensive local network. Police have identified all suspects and are continuing their investigation into the extent and operations of the racket.

Key Concern
This case highlights the growing trend of cybercriminals exploiting remote work opportunities to target unsuspecting victims. The ease with which such scams are orchestrated, coupled with the victims' financial vulnerability and lack of awareness, remains a serious concern. Enhanced public education and proactive cyber monitoring are critical to preventing similar frauds.