BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Ghaziabad Cops Uncover ₹109 Crore Cyber Scam

Incident
A large-scale cyber fraud operation has been unveiled, resulting in financial losses exceeding ₹109 crore across more than 450 reported cases. The case emerged from an investigation led by cybercrime authorities in a specific district, revealing a widespread inter-state cybercrime network.

Modus Operandi
The perpetrators employed various digital deception methods, including fake calls, phishing attacks, and fraudulent online schemes. Victims were tricked through impersonation tactics involving banks and government agencies or redirected to malicious websites to steal sensitive data and funds. A total of 97 mobile numbers, traced to a particular eastern state, were found to be involved, suggesting a coordinated and systematic approach.

Action Taken
The findings were presented during a two-day strategic workshop that included law enforcement officials from multiple regions. Cybercrime investigators traced the source of fraudulent communications and confirmed the use of numerous SIM cards registered in another state. This intelligence has been shared with relevant authorities to drive inter-agency collaboration and further action.

Key Concern
The investigation highlights the scale and reaches of organized cybercrime networks operating across state and national borders. The recurring use of regional mobile numbers to perpetrate widespread scams emphasizes the urgent need for enhanced inter-state surveillance, intelligence sharing, and a coordinated law enforcement response.

International Cyber Fraud Ring busted; Mohali police nab 7 foreigners.

Incident
A group of foreign nationals was arrested in a major cyber fraud case involving financial deception totaling nearly ₹15 crore. The suspects were operating out of a residential area in Uttar Pradesh and had allegedly defrauded over 350 individuals using online scam techniques.

Modus Operandi
The accused operated a fake call center from a rented location and used social media platforms to befriend married men and women. Once trust was established, they claimed to have sent valuable gifts that were supposedly held by customs authorities. Victims were then persuaded to transfer money online to release the gifts. These funds were routed to bank accounts controlled by the group. The operation also involved the use of numerous SIM cards and digital devices to carry out the scam.

Action Taken
Law enforcement agencies conducted a raid on the hideout and arrested the suspects. A significant quantity of evidence was seized, including 79 smartphones, multiple laptops and MacBooks, 99 Indian and foreign SIM cards, and approximately ₹30 lakh in cash. The arrests took place in mid-May as part of an ongoing crackdown on cyber-enabled fraud.

Key Concern
This case highlights the growing misuse of social engineering via social media to exploit emotional vulnerabilities. The scale of digital infrastructure recovered, including SIM cards and multiple devices, underscores the sophistication and reach of such operations. It also reflects the need for increased vigilance on cross-border fraud and the misuse of residential spaces for cybercrime activities.

Two held in Telangana for trafficking Indians into cyber slavery racket in Southeast Asia

Incident
A significant breakthrough was achieved with the arrest of two key individuals involved in a transnational cyber slavery racket. This operation trafficked thousands of Indian citizens to Southeast Asian countries under false pretenses of job opportunities. Victims were allegedly coerced into engaging in illegal cyber activities abroad.

Modus Operandi
Victims were deceived with offers of high-paying jobs and transported to a foreign country. Upon arrival, they were handed over to international criminal syndicates operating out of neighboring nations. The trafficked individuals were then detained and forced to participate in illegal cyber operations against their will.

Action Taken
Following a formal complaint from one of the victims, authorities initiated an investigation that led to the arrest of two primary suspects. The complaint also prompted diplomatic coordination efforts, resulting in a large-scale rescue mission. Approximately 2,000 individuals were successfully extracted from detention in the foreign country and repatriated to their home country with the assistance of embassy officials and local military forces.

Key Concern
The case highlights a disturbing evolution of cybercrime into human trafficking networks, where victims are exploited as digital labor under duress. It raises serious concerns about job scam-related trafficking, international syndicate operations, and the urgent need for cross-border cooperation in combating such hybrid threats.

A 26-year-old man from West Bengal has been apprehended for allegedly duping an Odisha man of more than Rs 73 lakh in a ‘digital arrest’ fraud.

Incident
An individual from Odisha was defrauded of Rs 73.62 lakh in a sophisticated cyber scam involving impersonation and psychological coercion. The case was formally registered at a cybercrime police station on May 15.

Modus Operandi
The fraudsters contacted the victim, falsely claiming to be officials from central investigative and law enforcement agencies. They alleged that a parcel booked in the victim's name had been seized by customs authorities. Under the threat of legal consequences, the victim was coerced into paying Rs 73.62 lakh to "prove his innocence." The technique used in this case is known as a 'digital arrest', wherein victims are mentally manipulated into believing they are under investigation or custody without any physical detention.

Action Taken
Following the complaint, a team from the Odisha Police Crime Branch traced and arrested a 26-year-old suspect from Howrah district in West Bengal on May 15. Investigations are ongoing to identify other potentially involved individuals and recover the defrauded amount.

Key Concern
This incident highlights the growing threat of 'digital arrest' frauds that exploit fear and authority impersonation to extort large sums from unsuspecting individuals. The psychological manipulation employed in such scams makes them particularly dangerous, emphasizing the urgent need for public education on cyber fraud tactics and verification protocols when approached by alleged officials.

A company from Navi Mumbai lost Rs. 75 Lakhs in cyber-Fraud

Incident
An employee of a Navi Mumbai-based farmers producer company was deceived into transferring ₹75 lakh to cyber fraudsters. The fraud occurred over two days, between May 18 and 19, 2025, following receipt of a WhatsApp message impersonating the company’s managing director.

Modus Operandi
The perpetrators used social engineering and impersonation tactics, sending a fraudulent WhatsApp message to an accounts department employee. The message, which appeared to be from the company's MD, urgently instructed the transfer of ₹75 lakh to a specified bank account. Trusting the message's authenticity, the employee completed the transaction without verifying its legitimacy.

Action Taken
Upon discovery of the fraud, the company filed a complaint with the Cyber Police Station in Navi Mumbai. An FIR was registered on May 21 under relevant sections of the Bharatiya Nyaya Sanhita (criminal breach of trust, cheating, and personation) and applicable provisions of the Information Technology Act. An investigation is currently underway to identify and apprehend the perpetrators.

Key Concern
This incident highlights a growing trend of executive impersonation frauds leveraging popular messaging platforms like WhatsApp. The lack of internal verification protocols in financial workflows poses a serious risk, emphasizing the need for multi-level authentication, employee training, and stringent communication validation practices within organizations.