गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

Indian Cyber Crime Coordination Centre
सहवीर्यं करवावहै • Working Together With Vigour

CYBER DIGEST

22.09.2025

CD-710

PREPARED BY

INDIAN CYBER CRIME COORDINATION CENTRE

MINISTRY OF HOME AFFAIRS

GOVERNMENT OF INDIA

NATIONAL

S. No.	News
1.	Cybercrime police bust trading and parcel fraud rackets **(The Hindu)**
2.	Punjab man held in Rs 86.65 lakh cyber fraud case in Hyderabad **(Telangana Today)**
3.	Cyber fraud racket busted in Phagwara, 36 arrested **(The Tribune)**
4.	Retired Banker Loses Rs 23 Crore To Fraudsters Posing As Mumbai Police **(Delhi Now)**
5.	UIDAI Deactivates Crores of Aadhaar Numbers of Deceased to Prevent Welfare Fraud **(The 420)**
6.	Bengaluru director duped into buying ₹7.5 lakh in vouchers by scammer impersonating CEO **(Hindustan Times)**
7.	Telangana Youths Fall Prey To Global Cybercrime Job Rackets **(Deccan Chronicle)**

INTERNATIONAL

S. No.	News
1	Disruption continues at Heathrow, Brussels and Berlin airports after cyber-attack **(The Guardian)**
2	Rising threats push industrial supply chains to adopt real-time monitoring, proactive cybersecurity practices **(Industrial Cyber)**

National

Cybercrime police bust trading and parcel fraud rackets

The cyber crimes wing of the Hyderabad police have cracked down on a series of criminal networks that duped victims in trading and parcel scam cases, arresting accused persons from Gujarat, Punjab, and Haryana. Investigators said the cases involved use of fake trading apps, WhatsApp groups and intimidation tactics, with victims losing crores of rupees.

In one case, two men from Vadodara, Gujarat, were arrested for luring investors through fake stock market platforms disguised under the name of reputed companies. The accused, Inamdar Vinayaka Rajendar, 25, and Rishi Thushar Arothe, 30, tricked a Hyderabad resident into investing ₹32 lakh.

Victims were shown fake profits through fraudulent apps and asked to pay additional charges to withdraw funds. Once large sums were collected, the platforms were shut down. Police said the two had provided bank accounts and cryptocurrency wallets to fraudsters and were involved in 12 cases across India. Arothe, a former Ranji cricket player, had a past criminal record for diverting fraud money.

Punjab man held in Rs 86.65 lakh cyber fraud case in Hyderabad

A 27-year-old man from Punjab was arrested by the Hyderabad Cyber Crime police for providing his bank account to cyber fraudsters. The bank account was used to dupe several persons, including a city-based man of Rs 86.65 lakh.

The arrested, Gurdit Singh (28), a resident of Jantanagar in Punjab, had provided his account to cyber fraudsters who conned a city-based freelancer into transferring Rs 86,65,563 on the pretext of stock trading into that bank account.

In April 2025, the victim had received a message on WhatsApp about daily trading in institutional stocks, OTC trades and IPOs and was assured huge returns. The conmen cheated him after he transferred the huge amount over a period of time.

A case was registered and the account holder, Gurdit Singh, was traced and arrested. The police are investigating.

Cyber fraud racket busted in Phagwara, 36 arrested

The Kapurthala district police, headed by Phagwara DSP Phagwara Bharat Bhushan and Inspector Amandeep Kaur of Cyber Cell, Kapurthala, busted a large-scale cyber fraud racket operating out of a rented premises on Palahi Road, Phagwara, late on Thursday night. The operation, carried out jointly by the Cyber Crime Police Station, Kapurthala, and Phagwara City Police, led to the arrest of 36 persons and the recovery of 40 laptops, 67 mobile phones, and ₹10 lakh in cash. Senior Superintendent of Police (SSP) Gaurav Toora said the accused were booked under FIR No. 14, dated September 19, 2025, at PS Cyber

Crime Kapurthala. They face charges under sections 111, 318(4), 61(2) of the Bharatiya Nyaya Sanhita, along with sections 66C and 66D of the IT Act. Investigations are under way to trace the wider network and financial channels involved.

Preliminary inquiries revealed that the racket was being run by Amrinder Singh, alias Sabhi Tohri, a resident of Mohalla Gujratian in Phagwara, who had leased the premises to set up the illegal operation. The call centre was being managed by Jaspreet Singh, a resident of New Ranjit Nagar, and Sajan Madan of South Avenue, New Delhi. Both were found to have direct links with a Delhi-based individual identified as Suraj, who in turn is connected to a suspect named Shen from Kolkata.

Retired Banker Loses Rs 23 Crore To Fraudsters Posing As Mumbai Police

In another case of digital arrest, a retired banker from South Delhi lost nearly Rs 23 crore in a cyber fraud after scammers posing as Mumbai police officials allegedly held him under virtual confinement for over a month. The 78-year-old banker was threatened not to disclose this to anyone or face consequences.

The police, after being aware of the incident, said that the cybercriminals impersonated as Mumbai police officials and terrorised the victim, Naresh Malhotra, by alleging that his Aadhar details were linked to bank accounts used in terror funding and the Pulwama terror attack.

Malhotra said that on August 1, he received a call on his landline from an unidentified person who posed as a Mumbai Police official. The fraudster said that Malhotra's Aadhar number and all his communication lines would be disabled. They then forced him to share details of his bank accounts, assets, demat accounts, lockers and personal information about his family members.

He was then told to liquidate his equity holdings and transfer Rs 22.93 crore to their accounts, saying that it would be held with the RBI, and the RBI would return the money after verification.

Malhotra lives alone at his Gulmohar Park home near Hauz Khas. The scammers further warned him to kill his daughters, their husbands and his grandchildren if he takes the matter to anyone.

However, based on Malhotra's complaint, an FIR was registered by the Intelligence Fusion and Strategic Operations (IFSO) unit of Delhi Police. The IFSO team launched a probe into the matter.

UIDAI Deactivates Crores of Aadhaar Numbers of Deceased to Prevent Welfare Fraud

The Unique Identification Authority of India (UIDAI) has begun deactivating Aadhaar numbers linked to deceased individuals, in one of the largest clean-up operations in India’s welfare system. The move is aimed at curbing misuse of government schemes, where benefits were often issued in the names of the dead. In an effort to tighten India’s welfare delivery system, the Unique Identification Authority of India (UIDAI) has deactivated more than 1.4 crore Aadhaar numbers belonging to deceased citizens. The measure,

officials say, is part of the government's broader campaign to ensure that subsidies, pensions, and other welfare benefits are delivered only to living, eligible beneficiaries.

With Aadhaar linked to over 3,300 government schemes, the implications are vast. For years, reports surfaced of ghost beneficiaries drawing funds under the names of the dead. UIDAI's intervention, backed by the Modi government's 2047 vision of a fraud-free welfare state, is intended to stem these losses.

Bengaluru director duped into buying ₹7.5 lakh in vouchers by scammer impersonating CEO

In yet another incident of cyber fraud in Bengaluru, a director at a multinational company fell victim to an online scam and lost ₹7.5 lakh after being tricked into buying gift vouchers by someone posing as his company's CEO. The incident came to light after Abhishek Mitra, the victim, filed a formal complaint with the Whitefield Division Cyber Crime Police, who registered a case on Friday, as per a report by The Hindu. The FIR invokes relevant sections of the Information Technology Act, 2000, as well as Sections 318 and 319 of the Bharatiya Nyaya Sanhita (BNS), 2023, which pertain to cheating and impersonation.

According to Mitra's statement, he received a WhatsApp message from an unknown number, with the sender claiming to be the CEO of his firm. The imposter, pretending to be stuck in a meeting in the United States, urgently requested Mitra to buy Apple Store gift vouchers and share the codes.

Trusting the message and without verifying the identity of the sender, Mitra proceeded to purchase 80 Apple Store vouchers online and sent the codes to the number. The scam unravelled shortly afterward when he contacted the actual CEO, who denied sending any such request or receiving any codes.

Telangana Youths Fall Prey To Global Cybercrime Job Rackets

Unemployed youths from Telangana are increasingly falling prey to international cybercrime gangs. While many traditionally preferred Gulf countries for employment, a growing number are now being lured to Malaysia, Thailand, Indonesia, and Bangkok with promises of high-paying jobs. Once abroad, these youths are trapped and forced into cybercrime operations. Officials said several youths, including some from Hyderabad, are now playing key roles in international cybercrime networks. Victims are confined in so called "cybercrime dens," where they are made to place fraudulent calls in Telugu to cheat people. Lakhs of rupees have been misappropriated in this manner. Cyber gangs based in the "Golden Triangle" region are particularly active in trapping Telangana youths.

For the first time, Nizamabad Commissionerate police arrested a prime accused, Kolanati Nagashiva (36) of Suchitra Circle, Jeedimetla, Hyderabad, and booked him under the Prevention of Detention (PD) Act, 1986. He allegedly cheated youths in Nizamabad, Rajanna Sircilla, and other districts by offering them jobs abroad and later forcing them into cybercrimes. He has been remanded to Chanchalguda jail in Hyderabad.

International

Disruption continues at Heathrow, Brussels and Berlin airports after cyber-attack

Hundreds of thousands of passengers at Heathrow and Berlin airports faced flight delays on Sunday after a cyber-attack hit check-in desk software, while cancellations at Brussels airport suggested that disruption of Europe's air travel would continue into Monday.

Airlines were forced to revert to slower manual check-ins from Friday night after the attack hit Collins Aerospace, which provides check-in desk technology to various airlines.

Brussels airport asked airlines on Sunday afternoon to cancel half of the departing flights scheduled for Monday. The airport said Collins was "not yet able to deliver a new secure version of the check-in system", and confirmed a cyber-attack had taken place.

Airports urged passengers to check the status of their flights before travelling and asked them to arrive no earlier than three hours before long-haul flights and two hours before shorter journeys.

Collins said on Saturday it was dealing with a "cyber-related incident". The hack joins a long line of attacks that have hit big companies in recent months. The UK's largest automotive employer, Jaguar Land Rover, has been unable to produce any cars for three weeks because of a hack, while the British retailers Marks & Spencer and the Co-op were also hit by separate attacks earlier this year.

Rising threats push industrial supply chains to adopt real-time monitoring, proactive cybersecurity practices

Supply chain cybersecurity in industrial settings mirrors the increasing complexity and interdependence of today's operations. Industrial supply chains are now subject to dynamic cyber threats at software, hardware, and service layers, prompting businesses to adopt a new age of continuous assurance. As opposed to traditional single-point safety checks, continuous assurance involves regular verification and monitoring processes that keep software and components safe throughout their lifespan. This strategy hardens security and makes it more difficult for attackers to target vulnerabilities.

Across the global system of manufacturers, distributors, and consumers, supply chains face the challenge of ensuring that operations remain resilient against cyberattacks. Digital technologies are already making supply chains more transparent, efficient, and agile, and will be central to future initiatives aimed at improving industrial productivity. However, as digital capabilities expand across ERP solutions, advanced planning, customer and supplier integration, and shopfloor automation using cloud services and SaaS platforms, systemic reliance on specific platforms, vendors, or service providers also increases.

News / Feeds References

NATIONAL

1. https://www.thehindu.com/news/cities/Hyderabad/cybercrime-police-bust-trading-and-parcel-fraud-rackets/article70070555.ece
2. https://telanganatoday.com/punjab-man-held-in-rs-86-65-lakh-cyber-fraud-case-in-hyderabad
3. https://www.tribuneindia.com/news/jalandhar/cyber-fraud-racket-busted-in-phagwara-36-arrested/
4. https://www.timesnownews.com/delhi/delhi-cyber-scam-shocker-retired-banker-loses-rs-23-crore-to-fraudsters-posing-as-mumbai-police-delhi-news-article-152866612
5. https://the420.in/uidai-deactivates-aadhaar-numbers-deceased-welfare-fraud/
6. https://www.hindustantimes.com/cities/bengaluru-news/bengaluru-director-duped-into-buying-rs-7-5-lakh-in-vouchers-by-scammer-impersonating-ceo-report-101758429867563.html
7. https://www.deccanchronicle.com/southern-states/telangana/telangana-youths-fall-prey-to-global-cybercrime-job-rackets-1904999

INTERNATIONAL

1. https://www.theguardian.com/business/2025/sep/21/delays-continue-at-heathrow-brussels-and-berlin-airports-after-alleged-cyber-attack
2. https://industrialcyber.co/features/rising-threats-push-industrial-supply-chains-to-adopt-real-time-monitoring-proactive-cybersecurity-practices/

CYBER DOST

In Case of Online Financial Fraud

Dial 1930

FOR ANY CYBER CRIME COMPLAINT REPORT ON
https://cybercrime.gov.in

FOR FULL VERSION OF DAILY DIGEST, VISIT:
https://i4c.mha.gov.in/cyber-digest.aspx