गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

सत्यमेव जयते

Indian
Cyber
Crime
Coordination
Centre

सहवीर्यं करवावहै • Working Together With Vigour

CYBER DIGEST

26.09.2025

CD-714

PREPARED BY

INDIAN CYBER CRIME COORDINATION CENTRE

MINISTRY OF HOME AFFAIRS

GOVERNMENT OF INDIA

NATIONAL

S. No.	News
1.	Cops bust Rs 892cr cyber scam in Surat **(Ahmedabad Mirror)**
2.	Two men working for Malaysia-based cyber fraudsters nabbed in Chennai **(The Hindu)**
3.	DoT, FIU-IND join hands to curb cyber crimes and financial frauds **(DD News)**
4.	Lawyer Defrauded Of ₹1.80 Crore By Cyber Impersonators Posing As CBI Officers **(Free Press Journal)**
5.	Telangana Police to Open History Sheets to Contain Cybercrooks Activities Telangana **(Deccan Chronicle)**
6.	Cyber Fraudster Posing as IIT-B Professor Dupe Engineering College of Rs 2.46 Crore in Pune **(Pune Mirror)**
7.	78-year-old duped of Rs 48 lakh in 13-day digital arrest scam **(The New Indian Express)**

INTERNATIONAL

S. No.	News
1	Hackers reportedly steal pictures of 8,000 children from Kido nursery chain **(The Guardian)**
2	Netherlands establishes cyber resilience network to strengthen public-private digital defence **(Computer Weekly)**

National

Cops bust Rs 892cr cyber scam in Surat

In one of the largest crackdowns on cyber fraud in recent years, the Gandhinagar State Cyber Crime cell has unearthed a Rs 892 crore racket, arresting 10 men from Surat district who allegedly served as the backbone of a nationwide scam syndicate. Cops said the accused acted as "facility providers" – supplying bogus bank accounts, SIM cards, PoS (point-of-sale) machines and other digital tools that enabled cyber fraudsters to fleece victims across the country.

Police said the gang created 482 "mule" accounts through which fraudsters executed 1,549 cybercrimes nationwide, including 141 cases in Gujarat alone, worth Rs 17.75 crore. Cybercrime officials told Mirror this is among the biggest busts in recent years.

The State Cyber Cell has seized 529 bank account kits, 447 ATM cards, 686 pre-activated SIM cards, 16 PoS machines, 60 mobile phones, two laptops, 11 sound boxes, 17 QR codes and one router from the accused.

Two men working for Malaysia-based cyber fraudsters nabbed in Chennai

The Cyber Crime Wing of the Central Crime Branch, Chennai, has arrested two men from Tirupur and Thoothukudi who were operating as mule accounts for an alleged Malaysia-based cyber fraudster and reportedly swindled ₹2.49 crore from an elderly woman in an online trading scam.

The police said that a 70-year-old woman from Chennai was cheated out of ₹2.49 crore by fraudsters operating through a fake investment platform named HEMSecurities. The victim was enticed via WhatsApp to install a fraudulent trading application, where fabricated profits were displayed. She was then persuaded to transfer large sums of money to unlock these supposed profits. Between December 2024 and January 2025, she transferred a total of ₹2.49 crore in nine transactions to eight different bank accounts. When she attempted to withdraw the money, her requests were blocked, and she was asked to make further deposits. Based on her complaint, a case was registered at the Cyber Crime Police Station, Central Crime Branch, Greater Chennai Police.

DoT, FIU-IND join hands to curb cyber crimes and financial frauds

In a major move to curb cyber-crimes and financial frauds, the Department of Telecommunications (DoT) and the Financial Intelligence Unit-India (FIU-IND) on Thursday signed a comprehensive Memorandum of Understanding (MoU) to enhance data sharing and inter-agency coordination.

The MoU was signed by Sanjeev Kumar Sharma, Deputy Director General of the AI & Digital Intelligence Unit (DIU) at DoT, and Amit Mohan Govil, Director of FIU-IND, in the presence of Dr. Neeraj Mittal, Secretary

(Telecom), and Arvind Shrivastava, Secretary (Revenue).

Speaking on the occasion, Dr. Neeraj Mittal highlighted the growing importance of technology in governance. "Departments have leveraged technology to achieve their respective goals. While this is an essential first step, true progress lies in transcending departmental boundaries to address existing gaps. Developing synergies by learning from each other is crucial," he said.

Under the MoU, both agencies will exchange critical information in real-time to strengthen fraud detection. FIU-IND will share mobile numbers linked to accounts involved in suspicious transactions, while DoT will provide details of mobile numbers disconnected due to fraudulent activity. The exchange of information will be facilitated through advanced technology platforms such as DoT's Digital Intelligence Platform (DIP) and FIU-IND's Finnex 2.0 portal, ensuring secure, system-based transmission of data.

Lawyer Defrauded Of ₹1.80 Crore By Cyber Impersonators Posing As CBI Officers

A senior citizen lawyer was cheated out of ₹1.80 crore by fraudsters posing as CBI officers. A case was registered regarding this on Wednesday. The accused used the victim's Aadhaar card and told him money was being laundered in his name, threatening him with a bogus money laundering case.

Police said that, fearing arrest, the victim lawyer transferred a total of ₹1,80,37,000 to various bank accounts. The online fraud took place between September 4 and September 19 in Udyam Nagar, Pimpri.

Ganpat Balaji Kakade (73, Udyam Nagar, Pimpri) has complained to the Cyber Police Station. The suspects include three mobile number holders and four different bank account holders.

According to the police, the fraudsters threatened to arrest the complainant and his wife in a fraud case. They also warned the couple that if they told anyone about the situation, those people would also be arrested. They gained the lawyer's trust by sending him fake PDF documents with the names of senior police officers.

Telangana Police to Open History Sheets to Contain Cybercrooks Activities Telangana

Cyber fraudsters can no longer strike as per their whims and fancies as Telangana police decided to open suspect or history sheets against them to contain their activities. The Director-General of Police Jitender has issued instructions to all the Inspectors and Sub-Inspectors (SIs) of cybercrime stations to open suspect or history sheets on all the habitual and repeated offenders persons, who were involved in social media offences and financial frauds ensuring close surveillance over their activates to curb their nefarious conduct. A memo in this regard was issued to all the Inspectors and SIs of the cybercrime stations. The move assumed significance as most of the offenders involved in cybercrimes were found to be committing repeatedly. It will also act as deterrence on the cyber fraudsters, who are targeting innocent people and swindling their hard-earned money. Instructions were issued to identify such accused persons, open and maintain suspect and history sheets in cybercrime police station (CCPS) records, and ensure close surveillance over their activities to curb their nefarious conduct and manage the activities of habitual or potentially repeat offenders effectively. The suspect and history sheets must be opened under provisions of Bharatiya Nyaya Sanhita (BNS) even if they are not yet convicted, fall under the category of "suspects", one of the classifications of history sheeters and submit compliance reports to the cybercrime station in Hyderabad within the stipulated time.

Cyber Fraudster Posing as IIT-B Professor Dupe Engineering College of Rs 2.46 Crore in Pune

When a young and smart glib-talking man visited an engineering college and introduced himself as an IIT-B professor, the faculty and administration were impressed. The 'professor' offered to help them join a research project and assured that the college would also get access to government-funded artificial intelligence and drone initiatives. He also pointed out that substantial research funding would come the college's way, if it joined the project. What unfolded was a scam that has sent shockwaves through the academic community, exposing vulnerabilities in higher education institutions.

The 'professor' said he would get all the paper work done. All the college had to do was to pay for the technical requirements, which could be viewed as investment for the funding to take place. He guided the college step-by-step through emails and WhatsApp messages, urging them to make the payments on time, so that they do not miss the golden opportunity to join the research project.

The college paid various amounts from time to time, totalling Rs2.46 crore, after which the 'professor' vanished. The college then realised they had been duped and approached the cyber police, which registered FIR No. 96/2025.

78-year-old duped of Rs 48 lakh in 13-day digital arrest scam

A 78-year-old retired Singareni Collieries employee lost Rs 48 lakh after being kept under "digital arrest" for 13 days by fraudsters posing as officials from the police, CBI and Enforcement Directorate.

According to the victim, his ordeal began on September 2 when he received a call from someone claiming to be from the Department of Telecommunications, Secunderabad, who said his number was under scrutiny by the Bengaluru police.

The call was transferred to another person who alleged his Aadhaar had been misused to obtain a SIM card used for harassing women. He was then told that a man arrested in Mumbai for human trafficking had named him, alleging he sold his Aadhaar for Rs 30 lakh. The fraudsters, introducing themselves as CBI and ED officials, threatened him with an arrest warrant from the Supreme Court. During video calls, they showed him fabricated documents and claimed his assets had to be audited in the interest of national security.

Fearing arrest, the victim was pressured to disclose details of his finances, including his retirement savings, fixed deposits and valuables.

International

Hackers reportedly steal pictures of 8,000 children from Kido nursery chain

The names, pictures and addresses of about 8,000 children have reportedly been stolen from the Kido nursery chain by a gang of cybercriminals.

The criminals have demanded a ransom from the company – which has 18 sites around London, with more in the US, India and China – according to the BBC.

The hackers have claimed they also possess information about the children's parents and carers, as well as safeguarding notes, and have contacted some by phone as part of their extortion tactics.

Kido was contacted for comment. The company has yet to confirm the hackers' claims. The company has not released a public statement nor confirmed the hackers' claims.

An employee at one of the nurseries told the BBC they had been notified of a data breach.

The Metropolitan police said they had received a referral on Thursday "following reports of a ransomware attack on a London-based organisation". They added: "Enquiries are ongoing and remain in the early stages within the Met's cyber crime unit. No arrests have been made."

Netherlands establishes cyber resilience network to strengthen public-private digital defence

The Netherlands has launched a Cyber Resilience Network, a public-private partnership aimed at fundamentally overhauling the nation's approach to digital defence.

The initiative, detailed in a comprehensive building plan from the National Cyber Security Centre (NCSC-NL), aims to connect over 1,152 organisations in a collaborative framework that extends far beyond simple information sharing to include coordinated incident response, training and threat intelligence.

The move comes at a critical time, as a stark government report reveals just how close the country came to a debilitating IT crisis that could have brought essential public services to a standstill.

The urgency for this new approach becomes clear when examining the statistics. The chance of an organisation being hit by a cyber incident is now one in eight, yet preparation for such a crisis remains alarmingly low, according to the NCSC building plan. This isn't merely a private sector problem.

A recently published Dutch government report, titled *From vulnerable to resilient*, paints a sobering picture of the Dutch government's own digital dependencies, revealing that the near-collapse of a major IT supplier in early 2024 could have triggered a national crisis.

News / Feeds References

NATIONAL

1. https://www.ahmedabadmirror.com/cops-bust-rs-892cr-cyber-scam-in-surat/81899734.html
2. https://www.thehindu.com/news/cities/chennai/two-men-working-for-malaysia-based-cyber-fraudsters-nabbed-in-chennai/article70092767.ece
3. https://ddnews.gov.in/en/dot-fiu-ind-join-hands-to-curb-cyber-crimes-and-financial-frauds/
4. https://www.freepressjournal.in/pune/pimpri-chinchwad-crime-lawyer-defrauded-of-180-crore-by-cyber-impersonators-posing-as-cbi-officers
5. https://www.deccanchronicle.com/southern-states/telangana/telangana-police-to-open-history-sheets-to-contain-cybercrooks-activities-1906056
6. https://punemirror.com/city/crime/cyber-fraudster-posing-as-iit-b-professor-dupe-engineering-college-of-rs-2-46-crore-in-pune/
7. https://www.newindianexpress.com/states/telangana/2025/Sep/25/78-year-old-duped-of-rs-48-lakh-in-13-day-digital-arrest-scam

INTERNATIONAL

1. https://www.theguardian.com/technology/2025/sep/25/cybercriminals-steal-pictures-and-details-of-8000-children-from-nursery-chain
2. https://www.computerweekly.com/news/366631894/Netherlands-establishes-cyber-resilience-network-to-strengthen-public-private-digital-defence

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