गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

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

CYBER DIGEST

08.10.2025

CD-721

PREPARED BY

INDIAN CYBER CRIME COORDINATION CENTRE

MINISTRY OF HOME AFFAIRS

GOVERNMENT OF INDIA

NATIONAL

S. No.	News
1.	CBI Joins Interpol's Operation HAECHI-VI; 8 Key Operatives Arrested **(Free Press Journal)**
2.	Cyber police Jammu busts ₹4.44 cr fraud; 3 nabbed from Gujarat **(Hindustan Times)**
3.	Rs 66.23 crore lost in nine months; Kochi sees surge in cyber fraud cases **(The New Indian Express)**
4.	ED Freezes ₹2.85 Crore in Alleged Cyber-Fraud Linked to Foreign Nationals **(The 420)**
5.	Cyber fraudsters dupe Hyderabad man through 'fake' BigBasket site **(Telangana Today)**
6.	Kerala cyber security summit to focus on MSMEs, start-ups **(Business Line)**
7.	Doctor Duped of ₹45.16 Lakh, Case Registered in Nagpur **(The Live Nagpur)**

INTERNATIONAL

S. No.	News
1	OpenAI bans suspected Chinese accounts using ChatGPT to plan surveillance **(The Register)**
2	North Korean hackers increasingly targeting wealthy crypto holders **(BBC)**

National

CBI Joins Interpol's Operation HAECHI-VI; 8 Key Operatives Arrested

The Central Bureau of Investigation (CBI) has actively participated in Operation HAECHI-VI launched by Interpol targeting seven specific types of crimes, namely, cyber-enabled financial crime, voice phishing, love/romance scam, online sextortion, investment fraud, money laundering associated with illegal online gambling, business email compromise and e-commerce fraud.

During Operation HAECHI-VI, International Operations Division of CBI closely coordinated with FBI US Department of Justice and the German authorities and arrested 08 offenders and identified 45 suspects who were indulging in the transnational cyber enabled financial crimes and subjecting the minor girls to sexual offences online. Cash amount of USD 66,340 was recovered from the offenders and 30 bank accounts involved in the crime were blocked.

CBI acting upon operational inputs received from FBI, US Department of Justice apprehended two offenders who were targeting minor US girls online through social media platforms inducing and intimidating those minor girls to share their obscene images/videos.

Cyber police Jammu busts ₹4.44 cr fraud; 3 nabbed from Gujarat

In a major breakthrough against cybercrime, the Jammu cyber police has successfully unearthed a high-value cyber fraud involving ₹4.44 crore, resulting in the arrest of three accused from Surat in Gujarat, said officials. Jammu SSP Joginder Singh said that on September 2, a written complaint was received from a victim at the cyber police station, Jammu, alleging that he had been defrauded of ₹4.44 crore by people impersonating as law enforcement officials. They coerced the victim into transferring ₹4.44 across multiple bank accounts through a series of fraudulent transactions, he added.

Taking cognisance of the matter, a case under Section 66 D of the Information Technology Act, 2000, was registered at cyber police station, Jammu, and a detailed investigation was launched.

The Jammu cyber police has, so far, successfully frozen ₹55,88,256.74 across various bank accounts linked to the accused. Efforts are actively underway to reverse and refund the defrauded amounts to the complainant, out of which ₹6 lakh has already been credited back to the victim's account, he said.

Rs 66.23 crore lost in nine months; Kochi sees surge in cyber fraud cases

While Kochi recently made headlines after a pharma company owner lost Rs 25 crore to a single cyber fraud case, the broader picture is even more alarming. As of September 15, city residents have lost a total of Rs 66.23 crore to

cyber frauds and the authorities have managed to recover only Rs 4.18 crore!

While the gap remains huge, it is a stroke of fortune that even a small portion of the money lost has been recovered, said a source with Kochi city police.

"In a typical cyber fraud case, scammers operate systematically, taking their time and executing multiple transactions to drain the victim's account. By the time the victim realises they've been duped and lodge a complaint, a major share of the money is already gone. And we're often able to recover only the last few traced transactions," the source said.

In the recent `25-crore cyber fraud case, the complainant initially hoped the scammers would return the money and hence delayed filing a formal complaint, a source said.

South Range IG S Syamsundar, a former Kochi City police commissioner, noted that while the number of cases registered may have declined, the quantum of financial loss from such crimes has been increasing.

ED Freezes ₹2.85 Crore in Alleged Cyber-Fraud Linked to Foreign Nationals

The Enforcement Directorate (ED) has attached assets worth **₹285 crore** in connection with an alleged cyber-fraud involving foreign nationals — one of the largest such seizures this year. Officials say the assets, spread across real estate, bank deposits and company holdings, represent proceeds of an international laundering operation. The move underscores India's growing use of financial enforcement tools to tackle cross-border cybercrime, even as questions linger about due process and evidence.

The ED's order, issued under the Prevention of Money Laundering Act (PMLA), follows months of investigation into what officials describe as a sophisticated digital fraud network. According to the agency, the group targeted victims abroad and funneled illicit earnings into Indian accounts through remittances, shell firms, and cryptocurrency channels.

The attachment is provisional — not a finding of guilt — but it freezes assets pending further inquiry. "Freezing funds before trial gives the agency leverage but tests the limits of procedural fairness," said a Delhi-based lawyer familiar with similar cases.

Officials suggest the ₹285 crore figure may grow as new links emerge between overseas victims and domestic assets. For investigators, the action aims to preserve value before funds can vanish into a global web of accounts.

Cyber fraudsters dupe Hyderabad man through 'fake' BigBasket site

A 36-year-old man from Yousufguda became the latest victim of cyber fraud while reportedly trying to buy groceries through a fake website impersonating the popular grocery platform BigBasket.

As per available information, the victim placed an order on September 30 after finding a site offering groceries at unusually low prices. On October 2, he received a call from a person posing as a BigBasket customer care executive, who asked him to clear a pending payment. The fraudster sent an APK file

through WhatsApp, which the victim installed and paid Rs 360 through an e-wallet. Soon after, he received an SMS showing a large unauthorised debit from his credit card, amounting to Rs 1.9 lakh.

Based on his complaint, the Hyderabad Cybercrime police booked a case. Investigations revealed that the fraudsters had remotely activated call forwarding on his phone without his knowledge, allowing them to intercept banking messages.

Kerala cyber security summit to focus on MSMEs, start-ups

The Kerala Cyber Security Summit (KCSS), with a special emphasis on strengthening the cyber resilience of(MSMEs and start-ups, will be held at the Kochi Marriott on October 11.

The summit is being organised by F9 Infotech, a global multi-cloud and cyber security firm, in association with the State Government and the Kerala Start-up Mission.

P. Rajeeve, the State Industries Minister will inaugurate the event. Start-up Mission CEO Anoop Ambika will deliver the keynote address.

The organisers said the summit aims to position Kerala's cyber security ecosystem on par with global standards through innovative collaborations and knowledge exchange.

A highlight of the event will be a 'Live Attack Simulation & Resilience Workshop' (From Breach to Defense) designed to demonstrate real-time defence strategies against cyber breaches. Panel discussions will address themes such as 'How cyber security can aid the growth of MSMEs' and 'Technical leadership in the age of artificial intelligence'.

F9 Infotech, with operations spanning six countries, will conduct free cyber security assessments and awareness workshops for small businesses.

Doctor Duped of ₹45.16 Lakh, Case Registered in Nagpur

A shocking case of cyber fraud has been reported in Nagpur where a local doctor was duped of ₹45.16 lakh on the pretext of investing in the share market. The victim, a 60-year-old resident of Friends Colony, was lured by online scammers promising high returns through stock investments. According to police reports, the incident occurred between September 26 and October 1. The doctor was added to a WhatsApp group that claimed to offer expert guidance on stock trading. The group members posed as financial advisors and persuaded him to invest in various stocks through fake trading platforms.

Tempted by the assurance of profit, the doctor transferred ₹45.16 lakh to the fraudsters' accounts. However, when he tried to withdraw his supposed earnings, the scammers stopped responding and deleted the WhatsApp group. Realizing he had been cheated, the doctor filed a complaint with the Cyber Police.

A case has been registered, and an investigation is underway to trace the culprits and recover the amount. Police have also urged citizens to remain alert and verify the authenticity of online investment platforms before transferring money.

International

OpenAI bans suspected Chinese accounts using ChatGPT to plan surveillance

OpenAI has banned ChatGPT accounts believed to be linked to Chinese government entities attempting to use AI models to surveil individuals and social media accounts.

In its most recent threat report [PDF] published today, the GenAI giant said that these users usually asked ChatGPT to help design tools for large-scale monitoring and analysis - but stopped short of asking the model to perform the surveillance activities.

"What we saw and banned in those cases was typically threat actors asking ChatGPT to help put together plans or documentation for AI-powered tools, but not then to implement them," Ben Nimmo, principal investigator on OpenAI's Intelligence and Investigations team, told reporters.

One now-banned user, suspected to be using a VPN to access the AI service from China, asked ChatGPT to design promotional materials and project plans for a social media listening tool, described as a "probe," that could scan X, Facebook, Instagram, Reddit, TikTok, and YouTube for what the user described as extremist speech, and ethnic, religious, and political content.

This user claimed a government client wanted this scanning tool, but stopped short of using the model to monitor social media. OpenAI said it's unable to verify if the Chinese government ended up using any such tool.

North Korean hackers increasingly targeting wealthy crypto holders

Targeting high net worth crypto holders has helped North Korean hackers steal more than $2bn (£1.49bn) so far this year according to researchers.

The thefts are a record for the regime-linked hackers who now account for around 13% of North Korea's gross domestic product (GDP), according to United Nations' estimates.

For the last few years operatives from hacking teams like Lazarus Group have focussed on attacking cryptocurrency companies for large thefts of digital tokens.

Western security agencies say stolen funds are used to finance North Korea's nuclear weapons and missile development programs.

Dr Tom Robinson, chief scientist at Elliptic, says the targeting of individuals - which is less likely to be disclosed - means the true figure for hacks carried out by North Korea could be even higher.

North Korea's UK embassy was approached for comment but did not immediately respond. Previously the regime has denied any involvement in hacks.

Elliptic and other companies like Chainalysis are able to track the movement of stolen funds like Bitcoin and Ethereum by following the public list of transactions on the blockchain.

News / Feeds References

NATIONAL

1. https://www.freepressjournal.in/india/cbi-joins-interpols-operation-haechi-vi-busts-global-cyber-crime-networks-targeting-us-german-nationals-8-key-operatives-arrested
2. https://www.hindustantimes.com/cities/chandigarh-news/cyber-police-jammu-busts-4-44-cr-fraud-3-nabbed-from-gujarat-101759864383658.html
3. https://www.newindianexpress.com/cities/kochi/2025/Oct/08/rs-6623-crore-lost-in-nine-months-kochi-sees-surge-in-cyber-fraud-cases
4. https://the420.in/ed-2-85-crore-cyber-fraud-asset-attachment-india/
5. https://telanganatoday.com/cyber-fraudsters-dupe-hyderabad-man-through-fake-bigbasket-site
6. https://www.thehindubusinessline.com/info-tech/kerala-cyber-security-summit-to-focus-on-msmes-start-ups/article70134473.ece
7. https://thelivenagpur.com/2025/10/08/cyber-fraud-doctor-duped-of-%E2%82%B945-16-lakh-case-registered-in-nagpur/

INTERNATIONAL

1. https://www.theregister.com/2025/10/07/openai_bans_suspected_china_accounts/
2. https://www.bbc.com/news/articles/cwy8z7wxe03o

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