गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

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

CYBER DIGEST

15.09.2025

CD-705

PREPARED BY

INDIAN CYBER CRIME COORDINATION CENTRE

MINISTRY OF HOME AFFAIRS

GOVERNMENT OF INDIA

NATIONAL

S. No.	News
1.	Surat Cyber Crime Cell Arrests Key Mastermind Alfaz Memon in International Cyber Slaves Human Trafficking Racket **(Desh Gujarat)**
2.	India Blocks Over 100,000 SIM Cards in Crackdown on Cyber Fraud **(The 420)**
3.	Lucknow Police Exposed Gang Supplying Fake SIM Cards to Cyber Criminals **(The 420)**
4.	Telangana facilitates ₹40.8 crore refunds for cybercrime victims through latest Lok Adalat **(The Hindu)**
5.	Cybercrime Costs India Rs 31,000 Crore: Parliamentary Panel Tells Central Govt To Act Fast **(ETV Bharat)**
6.	UP man held in Rs 98 lakh cyber fraud case **(Hans India)**
7.	Kerala police to host annual cyber security conference c0c0n in Kochi **(The New Indian Express)**

INTERNATIONAL

S. No.	News
1	Cyber-scam camp operators shift operations to vulnerable countries as sanctions strike **(The Register)**
2	Shiny Hunters Attack National Credit Information Center of Vietnam **(Security Affairs)**

National

Surat Cyber Crime Cell Arrests Key Mastermind Alfaz Memon in International Cyber Slaves Human Trafficking Racket

The Surat Cyber Crime Cell has achieved a major breakthrough in an international human trafficking and cyber fraud case by arresting Alfaz Hanifbhai Aziz Memon (27), a key operative accused of luring Indian youth into cyber slavery in Myanmar.

According to officials, Memon played a central role in sending job-seeking youth from India to Thailand under the pretext of lucrative employment, before pushing them illegally across the border into Myanmar. There, they were forced to work for Chinese cyber fraud syndicates engaged in large-scale online scams targeting Indian citizens.

Memon, originally from Bhalej Road in Anand and residing in Sarkhej, Ahmedabad, was nabbed from Anand after being on the run. He had earlier worked for a Chinese cyber fraud company in Myanmar's KK Park area, where he learned various online fraud techniques. After returning to India, he allegedly began acting as an agent, recruiting Indian youth and sending them abroad through fake promises for commission from Chinese gangs operating cyber fraud business.

India Blocks Over 100,000 SIM Cards in Crackdown on Cyber Fraud

In one of its most sweeping actions against digital fraud, India's Department of Telecommunications (DoT) has shut down more than 100,000 SIM cards this year that were being used by organized cybercrime networks. Officials say that since 2023, nearly 8.2 million fraudulent connections have been deactivated nationwide.

Authorities found that criminal groups routinely acquired SIM cards with forged or stolen identity documents. In many cases, a single identity was used to activate hundreds of connections, which were then deployed for banking scams, phishing calls and online fraud.

Investigations revealed that cybercriminals exploited weak verification processes to obtain SIM cards in bulk. Some identities were linked to as many as 200 active numbers. These numbers were later used to deceive unsuspecting customers through fraudulent call centers, fake loan offers and OTP theft.

Lucknow Police Exposed Gang Supplying Fake SIM Cards to Cyber Criminals

Lucknow Police uncovered a gang involved in supplying fake and forged SIM cards to cybercriminals. The racket came to light after the Indian Cyber Crime Coordination Centre (I4C) flagged suspicious mobile numbers and alerted the police.

Investigations revealed that these SIM cards were not only fueling cyber fraud within India

but were also being misused across South and East Asian networks for financial scams.

Police officials said the SIM cards were issued during the post-sale process using forged identity documents. The mastermind of the racket has been identified as Farhan, who allegedly supplied these SIM cards to fraudsters and organized cyber gangs.

According to the cyber cell, these SIMs were being used for OTP fraud, online banking scams, phishing attempts, and other financial crimes, making them the backbone of various digital fraud operations.

Considering the seriousness of the case, the cyber cell lodged an FIR at Gomtinagar police station. The Department of Telecommunications (DoT) has also been roped into the investigation to examine how retailers and agents facilitated the fake SIM issuance.

Police are now tracing the chain of vendors and middlemen involved in the racket, aiming to dismantle the larger network that enables cybercriminals to exploit loopholes in telecom services.

Telangana facilitates ₹40.8 crore refunds for cybercrime victims through latest Lok Adalat

Telangana has secured refunds worth ₹40.86 crore for 7,040 cybercrime victims during the third National Lok Adalat of the year. Of this, ₹12.94 crore was ordered for refund in a single day to 4,539 victims, while a further ₹27.91 crore had already been settled in pre-Lok Adalat disposals for 2,501 victims.

The Cyberabad Commissionerate led the performance with 1,937 cases amounting to ₹11.51 crore in refunds, followed by Hyderabad with 941 cases and ₹9.29 crore, and Rachakonda with 1,061 cases totalling ₹6.41 crore. The Telangana Cyber Security Bureau headquarters recorded ₹4.21 crore with od refunds in 197 cases, while the Sangareddy police ₹1.04 crore in 266 cases.

With this round, total refunds through Lok Adalat in Telangana have risen to ₹138.04 crore in 2025, benefitting 18,872 victims. Since the mechanism was adopted for cybercrime restitution in March 2024, ₹321 crore has been returned to 36,786 victims across the State.

The TGCSB stressed the importance of timely reporting and urged citizens to exercise caution by avoiding suspicious links, not sharing sensitive banking information, and verifying customer care contacts only through official sources.

Cybercrime Costs India Rs 31,000 Crore: Parliamentary Panel Tells Central Govt To Act Fast

The Parliamentary Committee on Home Affairs has vehemently criticised the central government for its failure in tackling cybercrime despite the fact that several steps have been initiated to fight against the menace. The panel, in its latest report, has found that while victims may report to helplines such as 1930 or portals like cybercrime.gov.in, follow-ups are often delayed due to inter-jurisdictional challenges or a lack of real-time investigation frameworks.

"As a result, citizens feel that justice in cybercrime cases is slow and uncertain. The online grievance mechanism is often slow and difficult to access. Women and youth, key drivers of digital uptake, are especially impacted by safety concerns," the Committee on Home Affairs, chaired by Rajya Sabha MP Radha Mohad Das Agrawal, has highlighted in its latest report.

UP man held in Rs 98 lakh cyber fraud case

The Commissionerate Police arrested a cyber criminal from Uttar Pradesh for allegedly duping a person of over Rs 98 lakh on the pretext of investment in shares and securities, said Jagmohan Meena, the Deputy Commissioner of Police, Bhubaneswar, on Friday. The accused, identified as Mohd Shadab (33), is a resident of Rahimpur village in Bijnor district of Uttar Pradesh. During a media briefing, DCP Meena said the victim in June this year received a WhatsApp link with the invitation to join the WhatsApp Group namely "X05-IIFL SECURITIES LTD".

Later, the accused cyber fraudsters contacted the victim impersonating as officials of IIFL Securities Limited by using the company's logo. They lured the complainant into investing by promising huge trading benefits through misleading and biased communication in the said WhatsApp group. "The complainant was duped and deceived by the lucrative offers of the cyber fraudsters with a false promise of high returns. The complainant has deposited his hard-earned money to the tune of Rs 98.10 lakh in various bank accounts supplied by the fraudsters during the period from June 17 to July 1, 2025," informed the Commissionerate Police sources.

Kerala police to host annual cyber security conference c0c0n in Kochi

The annual cyber conference 'c0c0n' organised by the state police and Information Security and Research Association (ISRA) will be held in Kochi on October 10 and 11. The 2025 edition will unveil new innovations in cyber security domain.

In the run-up to the conference, training programmes organised by cyber security experts will be held from October 7 to 9. At the conference, deliberations will be held on challenges arising out of proliferation of AI technology and organised cyber crimes.

Another key area of attention will be on countering child sexual abuse. A comprehensive action plan will be formulated with an objective of purging the menace. In connection with this, cyber investigators from all the states will be provided a 10-day training camp on victim identification exercise. Domain experts from international organisations, including the Interpol, will lead the training at Kerala Police Academy in Thrissur from September 29 to October 9. A digital tool will be unveiled to counter circulation of Child Sexual Abuse Materials (CSAM) via the dark web and other encrypted platforms. A month-long hackathon involving developers from the country's top technical institutions will be organised in connection with the conference.

International

Cyber-scam camp operators shift operations to vulnerable countries as sanctions strike

The United Nations Office on Drugs and Crime (UNDOC) last week warned it had found "indications of scam center activity, including SIM cards and satellite internet devices" at a hotel in Timor-Leste, a nation founded in 2002 and whose gross domestic product is under $2 billion.

UNDOC believes "entities associated with convicted cybercriminals, offshore gambling operators, and triad-linked networks" are responsible for the material found in the hotel, and that they are evidence of shifting behavior by scammers.

"With growing awareness and understanding of scam centers and related criminal activity, law enforcement pressure has intensified across Southeast Asia, making it more difficult for organized crime groups to operate in traditional hotspot areas," the agency advised. "As a result, syndicates actively create avenues for expanding operations to new jurisdictions with limited experience in scam center responses, including Timor-Leste."

UNDOC's warning came just three days after the USA's Department of the Treasury announced fresh sanctions on cyber-scam centers in Myanmar and Cambodia.

ShinyHunters Attack National Credit Information Center of Vietnam

Authorities are investigating a cyber-attack against National Credit Information Center (CIC) of Vietnam by ShinyHunters. As confirmed by the Vietnam Cyber Emergency Response Team (VNCERT), signs of unauthorised access aimed at stealing personal data have been identified.

Resecurity's HUNTER team was able to acquire samples of leaked data. Notably, multiple records include references to the leading financial institutions in Vietnam including but not limited to VietCredit, MB Bank, Ocean Bank, VPBank, Sacombank (Saigon Thuong Tin Commercial Joint Stock Bank), Agribank (Vietnam Bank for Agriculture and Rural Development).

ShinyHunters claimed to exploit an "n-day" vulnerability (a known but unpatched flaw) in end-of-life software used by the CIC. Because the software was no longer supported, no security patches were available, leaving the system especially vulnerable. Unlike many ransomware attacks, ShinyHunters did not attempt to extort the CIC. Instead, they listed the data for sale on a hacking forum on the Dark Web, providing a large sample as proof.

ShinyHunters is one of the most prolific and notorious cybercriminal groups of the past five years, responsible for a series of high-profile data breaches that have impacted hundreds of millions of users and some of the world's largest organizations—including the compromise of Microsoft's GitHub account, AT&T, Ticketmaster, Santander, MathWay, Tokopedia, Wishbone, Wattpad, Pluto TV, Bonobos, Aditya Birla Fashion and Retail, Mashable, and the Legal Aid Agency.

News / Feeds References

NATIONAL

1. https://deshgujarat.com/2025/09/13/surat-cyber-crime-cell-arrests-key-mastermind-alfaz-memon-in-international-cyber-slaves-human-trafficking-racket/
2. https://the420.in/india-sim-card-block-cyber-fraud-2025/
3. https://the420.in/lucknow-fake-sim-card-gang-busted/
4. https://www.thehindu.com/news/cities/Hyderabad/telangana-facilitates-408-crore-refunds-for-cybercrime-victims-through-latest-lok-adalat/article70049027.ece
5. https://www.etvbharat.com/en/!bharat/cybercrime-costs-india-rs-31000-crore-parliamentary-panel-tells-central-govt-to-act-fast-enn25091309849
6. https://www.thehansindia.com/news/national/up-man-held-in-rs-98-lakh-cyber-fraud-case-1006208
7. https://www.newindianexpress.com/cities/kochi/2025/Sep/15/kerala-police-to-host-annual-cyber-security-conference-c0c0n-in-kochi

INTERNATIONAL

1. https://www.theregister.com/2025/09/15/asia_tech_news_roundup/
2. https://securityaffairs.com/182189/cyber-crime/shinyhunters-attack-national-credit-information-center-of-vietnam.html

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