अति उत्तम
(NABET ACCREDITATION)

NEWS LETTER

JUNE 2026

CALL FOR APPOINTMENT

0141-2823100

BPR&D JAIPUR

CENTRAL DETECTIVE TRAINING INSTITUTE
BUREAU OF POLICE RESEARCH & DEVELOPMENT

तेजस्वि नावधीतमस्तु

BPR&D JAIPUR

Promoting Good Practices and standards for the Indian Police

Accomplished Course

(1)Wildlife Crime Investigation and Enforcement From (04-08 May 2026)

(2)Juvenile Justice and Investigation of Crime Against Children From (04-08 May 2026)

(3)Crime against weaker section remedial action & Establishing the role of law From (11-13 May 2026)

(4)Counter Terrorism - Changing Contest and emerging contours From (11-15 May 2026)

(5)NATGRID- Role in Changing Policing From (18-20 May 2026)

NEWS PAPER

DELHI POLICE NABS 89 INDIVIDUALS IN MONTH-LONG CRACKDOWN ON CYBERCRIME

Published – May 21, 2026 05:51 am IST – New Delhi

The Delhi Police has busted multiple interstate cyber fraud syndicates and brought 89 offenders to justice during a month-long crackdown in April in west Delhi, officials said on Wednesday.

According to police, 35 accused were arrested, 54 persons were brought in to issue warnings and investigation in 34 major cyber fraud cases was completed during the operations conducted across several states, including Jharkhand, Punjab, Haryana, Uttar Pradesh, Rajasthan, Gujarat and Delhi.

The syndicates were involved in digital arrest scams, investment frauds, APK file scams, fake dating membership frauds and mule account operations, they said.

Officials said the operations exposed cyber fraud networks involving transactions worth nearly Rs 40 crore.

During the drive, police recovered Rs 14.18 lakh in cash, 359 SIM cards, 218 ATM cards, 88 mobile phones, 78 cheque books, five passbooks, three credit cards, two laptops, a pen drive and a car allegedly used in cyber fraud activities.

Police said against a total cheated amount of Rs 3.36 crore reported during the month, teams managed to secure Rs 1.11 crore through immediate lien marking and coordination with banks. Additionally, Rs 51.95 lakh were reverted to victims through court orders.

In one of the major operations, police busted a highly organised mule account and OTP-sharing syndicate allegedly operating from Karampura in west Delhi.

Police said the accused used a social media group titled "DL Office" to share OTPs and illegally operate mule bank accounts used in cyber frauds across India.

The accused – identified as Bittoo Chaudhary, Lavish Chugh, Rishi, Arun Singh, Ashish and Deepak Bhatt – allegedly tried to escape by jumping from the fourth floor of a building during the raid but were apprehended after a chase.

Technical analysis through the Samanvaya portal revealed that the syndicate was linked to 35 NCRP complaints involving cheated amounts of around Rs 40 crore, police said.

FBI links First VPN Service to ransomware gangs, botnets, criminal dark web activity; calls for layered defensive controls 27 May 2026

The Federal Bureau of Investigation (FBI) disclosed that about 25 ransomware groups used a criminal VPN service known as 'First VPN Service' to conduct network intrusions, scanning operations, botnets, denial-of-service attacks, and scams. The service has been active since around 2014 across 32 exit nodes in 27 countries. It affects organizations by enabling ransomware groups and other cybercriminal actors to conduct network intrusions, reconnaissance, credential abuse, denial-of-service attacks, and broader malicious operations.

At least 25 ransomware groups, such as Avaddon Ransomware, have used First VPN Service infrastructure to perform network reconnaissance and intrusions," the FBI wrote in a recent FLASH advisory. "First VPN Service IP addresses have been used for scanning activity, botnets, denial of service attacks, scams, and hacking. First VPN Service was almost exclusively advertised in known criminal dark web forums such as Exploit in and XSS is, two of the most prominent Russian-language online forums which provide marketplaces for cyber criminals to buy and sell unauthorized access to computer systems, stolen personal identifying information, hacking tools, and contraband. This reporting applies solely to the First VPN Service and does not extend to other VPN providers with similar naming."

The revelation came alongside a coordinated international takedown of the service, led by French and Dutch cybercrime units with support from Ukraine, the U.K., Switzerland, and Luxembourg. It follows from the findings that the VPN was marketed almost exclusively on prominent Russian-language dark web forums used by cybercriminals to trade stolen data, hacking tools, and unauthorized access to systems.

MUMBAI OFFICIALS FALL VICTIM TO PHISHING SCAM VIA COLLECTOR'S WHATSAPP ACCOUNT

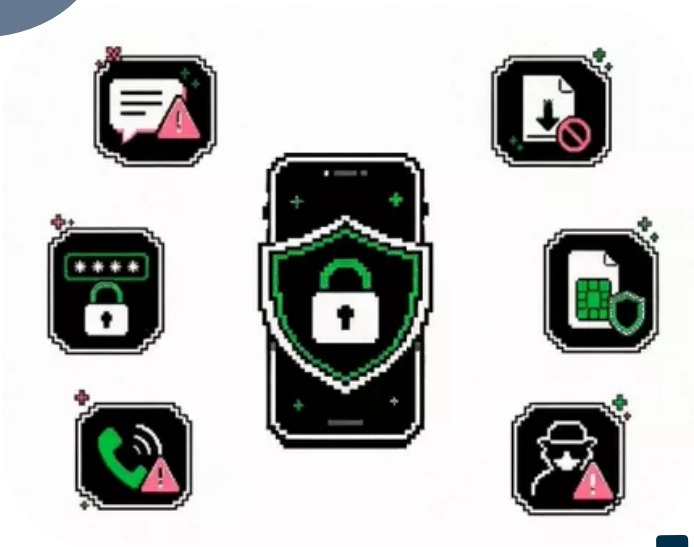
DATE: MAY 27, 2026

A serious and well-planned cyber fraud attempt has surfaced in the city, where unknown scammers impersonated the Mumbai City Collector and District Magistrate and sent WhatsApp messages to senior revenue officials, attempting to extract money under the pretext of an "urgent government project." However, alert officials detected the fraud in time, preventing any financial loss.

78-YEAR-OLD WOMAN'S PHONE HACKED; ₹25 LAKH STOLEN:LEARN FROM EXPERTS HOW TO AVOID FALLING PREY TO SUCH SCAMS

Recently, a case of fraud worth ₹25 lakh with a 78-year-old elderly woman in Mumbai came to light. Cyber criminals executed this scam by hacking the woman's phone.

The scammers contacted the woman through WhatsApp and claimed to be an official from the electricity department. After gaining trust through conversation, they asked her to download an APK file and make a payment to update the name in the connection. As soon as the woman made the payment, her phone got hacked and ₹25 lakh were deducted from her account. In such a situation, it is extremely important to find out how scammers con people.



NIA FILES CHARGESHEET AGAINST FIVE FOR TRAFFICKING OF INDIANS TO 'CYBER SLAVERY' FIRMS IN CAMBODIA

The agency named Anand Kumar Singh as the alleged 'kingpin', accusing him of charging between $2,000 and $3,000 for each person sent to fraudulent companies.

The National Investigation Agency on Friday filed a chargesheet against five persons in connection with a Cambodia-linked human trafficking and cyber slavery case that involved luring young persons from India with fake job offers.

In a statement on Tuesday, the agency said the chargesheet was filed before a special NIA court in Patna under sections of the Indian Penal Code.