

**GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS**

**RAJYA SABHA
STARRED QUESTION NO. *113**

TO BE ANSWERED ON THE 29TH JULY, 2026/ SHRAVANA 7, 1948 (SAKA)

CYBER CRIME AND ONLINE FINANCIAL SCAMS

***113. SHRI JOSE K. MANI:**

Will the Minister of HOME AFFAIRS be pleased to state:

- (a) whether Government has data regarding cyber crime and online financial scams reported during the last five years;**
- (b) if so, year-wise and State-wise details thereof, including the amount of money lost and recovered;**
- (c) the number of complaints resolved through the National Cyber Crime Reporting Portal; and**
- (d) the measures taken to strengthen cyber policing and public awareness against cyber crime?**

ANSWER

**MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI BANDI SANJAY KUMAR)**

(a) to (d) A Statement is laid on the Table of the House.

STATEMENT IN REPLY TO THE RAJYA SABHA STARRED QUESTION NO. *113 FOR 29th JULY 2026 BY SHRI JOSE K. MANI REGARDING CYBER CRIME AND ONLINE FINANCIAL SCAMS

The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication “Crime in India”. The latest published report is for the year 2024. As per the data published by the NCRB, State/UT wise details of cases registered under Fraud under Cyber Crimes during the period from the year 2020 to 2024 are at the Annexure-I. As per the data published by the NCRB, Crime Head-wise details of cases registered under fraud under cyber crimes during the period from 2020 to 2024 is as under:

Sl. No.	Crime Heads	2020	2021	2022	2023	2024
1.	Credit Card/Debit Card	1194	1624	1665	2098	3829
2.	ATMs	2160	1899	1690	1783	1659
3.	Online Banking Fraud	4047	4823	6491	4435	4659
4.	OTP Frauds	1093	2028	2910	5116	965
5.	Gaming App or Website	-	-	-	-	1019
6.	Marketing or Investment	-	-	-	-	3044
7.	Fraud Call/Vishing	-	-	-	-	1264
8.	E-wallet or UPI	-	-	-	-	723
9.	Others	1901	3633	4714	6034	12596
Fraud (Total) (1 to 9)		10395	14007	17470	19466	29758

***Data under the heads Gaming App or Website, Marketing or Investment, Fraud Call/Vishing, E-wallet or UPI is being maintained from 2024.**

Data on amount of money lost and recovered is not maintained by NCRB.

The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cyber crimes in the country, in a coordinated and comprehensive manner.

The 'National Cyber Crime Reporting Portal' (NCRP) (<https://cybercrime.gov.in>) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children.

The 'Citizen Financial Cyber Fraud Reporting and Management System' (CFCFRMS), under I4C, has been launched in year 2021 for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. As per CFCFRMS operated by I4C, till 30.06.2026, financial amount of more than Rs. 11,158 Crore has been saved in more than 32.80 lakh complaints.

Cyber crime incidents reported on National Cyber Crime Reporting Portal, their conversion into FIRs and subsequent action i.e. filing of chargesheets, arrest and resolution of complaints, thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.

‘Police’ and ‘Public Order’ are State subjects under the Seventh Schedule to the Constitution of India. Accordingly, the States and Union Territories (UTs) are primarily responsible for the prevention, detection, investigation, and prosecution of cybercrime. The Central Government, through the Ministry of Home Affairs (MHA), supplements the efforts of States and UTs by providing policy guidance, technological support, capacity-building assistance, and financial resources to strengthen cybercrime management and enforcement capabilities.

The Central Government has taken the following steps to strengthen cyber policing and public awareness :

- i. Samanvaya Platform has been made operational to serve as an Management Information System (MIS) platform, data repository and a coordination platform for LEAs for cybercrime data sharing and analytics. It provides analytics based interstate linkages of crimes and criminals, involved in cybercrime complaints in various States/UTs. The module ‘Pratibimb’ maps locations of criminals and crime infrastructure on a map to give visibility to jurisdictional officers. The module also facilitates seeking and receiving of techno-legal assistance by Law Enforcement Agencies from I4C and other SMEs. It has lead to arrest of more than 29,837 accused and more than 2,33,593 Cyber Investigation assistance request.**

- ii. **A State of the Art, Cyber Fraud Mitigation Centre (CFMC) has been established at I4C where representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and representatives of States/UTs Law Enforcement Agency are working together for immediate action and seamless cooperation to tackle cybercrime.**
- iii. **‘Sahyog’ Portal has been launched to expedite the process of sending notices to IT intermediaries by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the IT Act, 2000 to facilitate the removal or disabling of access to any information, data or communication link being used to commit an unlawful act.**
- iv. **Seven Joint Cyber Coordination Teams (JCCTs) have been constituted for Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati under I4C covering the whole country based upon cyber crime hotspots/ areas having multi jurisdictional issues by onboarding States/UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs.**
- v. **A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions. Till 30.06.2026, more than 30.48 lakh suspect identifier data received from**

Banks and 32.08 lakh Layer 1 mule accounts have been shared with the participating entities of Suspect Registry and declined transactions worth Rs. 25,698 crores.

- vi. Cyber Commando programme was launched by the Hon'ble Home Minister on 10.09.2024 to establish a Special Wing of Cyber Commandos equipped with specialized training to counter cybersecurity threats in the country. The programme envisions the creation of a dedicated, skilled workforce capable of securing critical information infrastructure and supporting national cybersecurity efforts. So far, 281 cyber commandos successfully completed their training at premier institutions including IITs, IIITs, Rashtriya Raksha University (RRU), National Forensic Sciences University (NFSU) Gandhinagar & New Delhi, etc.**
- vii. The state of the art National-Digital Investigation Support Centre (previously known as National Cyber Forensic Laboratory (Investigation) {NCFL(I)}) has been established, as a part of the I4C, at New Delhi (on 18.02.2019) and at Assam (on 29.08.2025) to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police. Till 30.06.2026, National-Digital Investigation Support Centre, New Delhi has provided its services to State/UT LEAs in more than 14,064 cases pertaining to cyber crimes.**

- viii. **To further strengthen operational efficiency and ensure uniformity in handling cybercrime complaints, the Ministry has issued a comprehensive Standard Operating Procedure (SOP) for NCRP-CFCFRMS. The SOP lays down a standardized framework for complaint processing, bank coordination, grievance redressal, removal of lien markings, and restoration of defrauded funds to rightful claimants based on complaints received through the NCRP. Money Restoration Module for expeditious restoration of defrauded money to the victims and Grievance Redressal Module for timely attending to the grievances relating to freezing of the bank accounts and lien marking of the amount, have been made functional from April, 2026.**
- ix. **To further spread awareness on cyber crime, the Central Government has taken steps which, inter-alia, include; caller tune campaigns, dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@CyberDost), Facebook (CyberDostI4C), Instagram (CyberDostI4C), Telegram (cyberdosti4c), SMS campaign, TV campaign, Radio campaign, School Campaign, advertisement in cinema halls, celebrity endorsement, IPL campaign, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, digital displays on metro stations, railway stations and airports across the country, etc.**

ANNEXURE-I
R.S.S.Q. NO. *113 FOR 29.07.2026

State/UT-wise Cases Registered, under Fraud for Cyber Crimes from the Year 2020 to 2024.

SL	State/UT	2020	2021	2022	2023	2024
1	Andhra Pradesh	764	952	984	909	593
2	Arunachal Pradesh	3	2	0	0	0
3	Assam	58	82	16	0	1
4	Bihar	1294	1373	1441	2611	4020
5	Chhattisgarh	71	67	42	29	74
6	Goa	1	1	11	0	0
7	Gujarat	205	208	108	112	80
8	Haryana	36	52	44	11	215
9	Himachal Pradesh	1	6	9	7	2
10	Jharkhand	83	79	98	43	57
11	Karnataka	0	6	0	0	0
12	Kerala	6	16	26	117	86
13	Madhya Pradesh	69	89	180	91	96
14	Maharashtra	2032	1678	2202	2075	2827
15	Manipur	0	0	0	0	0
16	Meghalaya	10	0	0	0	0
17	Mizoram	0	0	0	0	0
18	Nagaland	0	0	0	0	0
19	Odisha	1079	1205	957	1362	1546
20	Punjab	16	29	61	25	95
21	Rajasthan	332	371	292	84	78
22	Sikkim	0	0	0	0	0
23	Tamil Nadu	5	107	251	887	684
24	Telangana	3316	7003	9581	10626	18922
25	Tripura	0	0	0	0	0
26	Uttar Pradesh	837	614	766	287	165
27	Uttarakhand	1	0	31	18	2
28	West Bengal	145	40	30	7	29
	TOTAL STATE(S)	10364	13980	17130	19301	29572
29	A&N Islands	0	0	0	0	0
30	Chandigarh	0	0	2	0	76
31	D&N Haveli and Daman & Diu	0	0	0	0	0
32	Delhi	31	19	331	163	110
33	Jammu & Kashmir	0	8	7	2	0
34	Ladakh	0	0	0	0	0
35	Lakshadweep	0	0	0	0	0
36	Puducherry	0	0	0	0	0
	TOTAL UT(S)	31	27	340	165	186
	TOTAL (ALL INDIA)	10395	14007	17470	19466	29758

Source: 'Crime in India' published by NCRB.