GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 2645

TO BE ANSWERED ON THE 16TH DECEMBER, 2025/ AGRAHAYANA 25, 1947 (SAKA)

CYBER FRAUD CASES IN KARNATAKA AND BENGALURU

2645. SHRI P C MOHAN:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) the number of cyber fraud cases reported in the country during the last three years, along with the figures for Karnataka and Bengaluru separately;

(b) the major types of cyber frauds being reported, such as UPI scams, online shopping frauds and identity theft;

(c) the steps taken by the Government to prevent and track cyber crimes, including the role of the Indian Cyber Crime Coordination Centre (I4C) and the cyber helpline 1930;

(d) the awareness campaigns and training programmes being carried out to educate citizens in the country and specifically in Karnataka and Bengaluru about online safety; and

(e) the punishments and legal actions prescribed under the Information Technology Act and related laws against those involved in cyber frauds?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS

(SHRI BANDI SANJAY KUMAR)

(a) to (e): 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 2023. As per the data published by the NCRB, State/UT-wise (including Karnataka) cases registered under

Fraud for Cyber Crimes (involving communication devices as medium/target) and Crime Head-wise cases registered under Cyber Crimes (involving communication devices as medium/target) in Bengaluru during the period from 2021 to 2023 are at the Annexure-I& II respectively. Crime Head-wise cases registered under Cyber Crimes (involving communication devices as medium/target) during 2023 is at Annexure-III.

'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. The States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cyber crime through their Law Enforcement Agencies (LEAs). The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their LEAs.

To strengthen the mechanism to deal with cyber crimes in a comprehensive and coordinated manner, the Central Government has taken steps which, inter-alia, include the following:

i. **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.

ii. 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. Cyber crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.

iii. 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. Till 31.10.2025, financial amount of more than Rs. 7,130 Crore has been saved in more than 23.02 lakh complaints. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints.

iv. 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.

v. Till 31.10.2025, more than 11.14 lakhs SIM cards and 2.96 lakhs IMEIs as reported by Police authorities have been blocked by Government of India.

vi. 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 on boarding States/UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs.

vii. I4C, MHA is regularly organising 'State Connect', 'Thana Connect' and Peer learning session to share best practices, enhance capacity building, etc.

viii. The state of the art 'National Cyber Forensic Laboratory (Investigation)' 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. So far, National Cyber Forensics Laboratory (Investigation), New Delhi has provided its services to State/UT LEAs in around 12,952 cases pertaining to cyber crimes.

ix. '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.

x. A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions. Till 31.10.2025, more than 18.43 lakh suspect identifier data received from Banks and 24.67 lakh Layer 1 mule accounts have been shared with the participating entities of Suspect Registry and declined transactions worth Rs. 8031.56 crores.

xi. 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 16,840 accused and 1,05,129 Cyber Investigation assistance request.

xii. The Central Government has taken various initiatives to create cyber crime awareness which, inter-alia, include:-

1) The Hon'ble Prime Minister spoke about digital arrests during the episode "Mann Ki Baat" on 27.10.2024 and apprised the citizens of India.
2) A special programme was organized by Aakashvani, New Delhi on Digital Arrest on 28.10.2024.
3) Caller Tune Campaign: I4C is collaboration with the Department of Telecommunications (DoT) has launched a caller tune campaign with effect from 19.12.2024 for raising awareness about cybercrime and promoting the Cybercrime Helpline Number 1930 & NCRP portal. The caller tunes were also being broadcast in English, Hindi and 10 regional languages by Telecom Service Providers (TSPs). Six versions of caller tunes were played which cover various modus-operandi, namely, Digital Arrest, Investment Scam, Malware, Fake Loan App, Fake Social Media Advertisements.
4) The Central Government has launched a comprehensive awareness programme on digital arrest scams which, inter-alia,

include; newspaper advertisement, announcement in Delhi Metros, use of social media influencers to create special posts, campaign through Prasar Bharti and electronic media, special programme on Aakashvani.

5) In partnership with DD News, I4C conducted a cybercrime awareness campaign running through Weekly Show Cyber-Alert starting from 19th July 2025 for 52 Weeks.

6) To further spread awareness on cyber crime, the Central Government has taken steps which, inter-alia, include; 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, campaign during Kumbh Mela 2025& Suraj Kund Mela 2025, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, digital displays on railway stations and airports across, etc.

There are 18 sections under the Information Technology Act, 2000 ("IT Act") which cover various forms of cyber offences, out of which 6 offences are non-bailable and 12 offences are bailable. Details of all the offences under the IT Act along with their penal consequences are at Annexure-IV.

*****

L.S.US.Q.NO. 2645 FOR 16.12.2025

ANNEXURE-I

State/UT-wise Cases Registered under Fraud for Cyber Crimes during 2021-2023

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

Source: 'Crime in India' published by NCRB.

L.S.US.Q.NO. 2645 FOR 16.12.2025

ANNEXURE-II

Crime Head-wise Cases Registered under Cyber Crimes in Bengaluru During 2021-2023

SL	Crime Heads	2021	2022	2023
1	Tampering computer source documents	4	4	4
2	Computer Related Offences	6247	9501	17122
3	Cyber Terrorism	1	1	1
4	Publication/transmission of obscene / sexually explicit act in electronic form	170	422	471
5	Interception or Monitoring or decryption of Information	0	0	0
6	Un-authorized access/attempt to access to protected computer system	0	0	0
7	Abetment to Commit Offences	1	0	0
8	Attempt to Commit Offences	0	3	1
9	Other Sections of IT Act	0	9	32
A	**Total Offences under I.T. Act**	6423	9940	17631
10	Abetment of Suicide (Online)	0	0	0
11	Cyber Stalking/Bullying of Women/Children	0	0	0
12	Data theft	0	0	0
13	Fraud	0	0	0
14	Cheating	0	0	0
15	Forgery	0	0	0
16	Defamation/Morphing	0	0	0
17	Fake Profile	0	0	0
18	Counterfeiting	0	0	0
19	Cyber Blackmailing/Threatening	0	0	0
20	Fake News on Social Media	0	0	0
21	Other Offences	0	0	0
B	**Total Offences under IPC**	0	0	0
22	Gambling Act (Online Gambling)	0	0	0
23	Lotteries Act (Online Lotteries)	0	0	0
24	Copy Right Act	0	0	0
25	Trade Marks Act	0	0	0
26	Other SLL Crimes	0	0	0
C	**Total Offences under SLL**	0	0	0
	Total Cyber Crimes	**6423**	**9940**	**17631**

Source: 'Crime in India' published by NCRB.

L.S.US.Q.NO. 2645 FOR 16.12.2025

ANNEXURE-III

Crimeheads-wise Cases Registered under Cyber Crimes (Involving Communication Devices as Medium/Target) during 2023

SL	Crime heads	Cases Registered
1	Tampering computer source documents	71
2	Computer Related Offences	35329
2.1	Computer Related Offences	4154
2.1A	Ransom-ware	795
2.1B	Offences other than Ransom-ware	3359
2.2	Dishonestly receiving stolen computer resource or communication device	395
2.3	Identity Theft	4978
2.4	Cheating by personation by using computer resource	25334
2.5	Violation of Privacy	468
3	Cyber Terrorism	11
4	Publication/transmission of obscene / sexually explicit act in electronic form	7893
4.1	Publishing or transmitting obscene material in Electronic Form	3110
4.2	Publishing or transmitting of material containing Sexually explicit act in electronic form	2168
4.3	Publishing or transmitting of material depicting children in Sexually explicit act in electronic form	1472
4.4	Preservation and retention of information by intermediaries	23
4.5	Other Sections 67 IT Act	1120
5	Interception or Monitoring or decryption of Information	1
6	Un-authorized access/attempt to access to protected computer system	1
7	Abetment to Commit Offences	0
8	Attempt to Commit Offences	11
9	Other Sections of IT Act	920
A	Total Offences under I.T. Act	44237
10	Abetment of Suicide (Online)	30
11	Cyber Stalking/Bullying of Women/Children	1305
12	Data theft	113
13	Fraud	19466
13.1	Credit Card/Debit Card	2098
13.2	ATMs	1783
13.3	Online Banking Fraud	4435
13.4	OTP Frauds	5116
13.5	Others	6034
14	Cheating	16943
15	Forgery	444
16	Defamation/Morphing	36
17	Fake Profile	225
18	Counterfeiting	0
18.1	Currency	0
18.2	Stamps	0
19	Cyber Blackmailing/Threatening	689
20	Fake News on Social Media	209
21	Other Offences	2389
B	Total Offences under IPC	41849
22	Gambling Act (Online Gambling)	87
23	Lotteries Act (Online Lotteries)	0
24	Copy Right Act	23
25	Trade Marks Act	1
26	Other SLL Crimes	223
C	Total Offences under SLL	334
	Total Cyber Crimes (A+B+C)	**86420**

Source: 'Crime in India' published by NCRB.

L.S.US.Q.NO. 2645 FOR 16.12.2025

ANNEXURE-IV

Offences under the IT Act along with their penal actions

S. No.	Section No.	Offence	Punishment	Bailable/Cognizable
1	65	Tampering with computer source documents.	Imprisonment up to 3 years or fine up to 2 lakhs or both	Bailable, Cognizable
2	66	Computer related offences: Punishment for doing dishonestly or fraudulently any act cited in section 43 directly or causing any person to do so, such as unauthorised access to or use of, introducing virus to, damages to, disruption of, denial of access to, assistance to access to, wrongful charges to another person's account by tampering with, destroying, deletion or alteration of any information in, computer resource or stealing/ concealing/ destroying any computer source code.	Imprisonment up to 3 years or fine up to 5 lakh or both.	Bailable, Cognizable
3	66B	Punishment for dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years or fine up to 1 lakh or both.	Bailable, Cognizable
4	66C	Punishment for identity theft, i.e., making use of	Imprisonment up to 3 years or fine up to 1 lakh or both.	Bailable, Cognizable
5	66D	Punishment for cheating by personation by using computer resource	Imprisonment up to 3 years and fine up to 1 lakh.	Bailable, Cognizable
6	66E	Punishment for violation of privacy.	Imprisonment up to 3 years or fine up to 2 lakh or both	Bailable, Cognizable
7	66F	Punishment for cyber terrorism	Imprisonment which may extend to life.	Non-Bailable, Cognizable
8	67	Punishment for publishing or transmitting obscene material in electronic form	1st Conviction – Imprisonment up to 3 years and fine up to 5 lakh. 2nd Conviction – Imprisonment up to 5 years and fine up to 10 lakh	Bailable, Cognizable
9	67A	Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form	1st Conviction – Imprisonment up to 5 years and fine up to 10 lakh. 2nd Conviction – Imprisonment up to 7 years and fine up to 10 lakh.	Non-Bailable, Cognizable

L.S.US.Q.NO. 2645 FOR 16.12.2025

ANNEXURE-IV

S. No.	Section No.	Offence	Punishment	Bailable/Cognizable
10	67B	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form	1st Conviction – Imprisonment up to 5 years and fine up to 10 lakh. 2nd Conviction – Imprisonment up to 7 years and fine up to 10 lakh.	Non-Bailable, Cognizable
11	69	Power to issue directions for interception or monitoring or decryption of any information through any computer resource (*punishment to intermediary who fails to assist the agency*)	Imprisonment up to 7 years and fine	Non-Bailable, Cognizable
12	69A	Power to issue directions for blocking for public access of any information through any computer resource. (*punishment to intermediary who fails to comply with such Government direction*)	Imprisonment up to 7 years and fine	Non-Bailable, Cognizable
13	69B	Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security. (*punishment to intermediary who intentionally or knowingly contravenes by not providing technical assistance*)	Imprisonment up to 1 year or fine up to 1 crore or both	Bailable, Cognizable
14	70	Critical Information Infrastructure (CII)/ Protected system: *Punishment to any person who secures access or attempts to secure access to any computer resources relating to CII and declared as protected system*	Imprisonment up to 10 years and fine	Non-Bailable, Cognizable
15	70B	CERT-In: Indian Computer Emergency Response Team (CERT-In) to serve as national agency for incident response. (*punishment to any service provider, intermediaries, datacentres, etc., who fails to provide the information called for or comply with the direction issued by the CERT-In*)	Imprisonment up to 1 year or fine up to 1 crore or both	Bailable, Non-Cognizable
16	71	Punishment for misrepresentation to Controller of Certifying Authorities (CCA) or Certifying Authorities	Imprisonment up to 2 years or fine up to 1 lakh or both	Bailable, Non-Cognizable
17	73	Punishment for publishing electronic signature Certificate false in certain particulars	Imprisonment up to 2 years or fine up to 1 lakh or both	Bailable, Non-Cognizable
18	74	Punishment for publication of electronic signature certificate for fraudulent purpose	Imprisonment up to 2 years or fine up to 1 lakh or both	Bailable, Non-Cognizable

******