GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

RAJYA SABHA
UNSTARRED QUESTION NO. 1998

TO BE ANSWERED ON THE 17TH DECEMBER, 2025/ AGRAHAYANA 26, 1947 (SAKA)

RISING INCIDENTS OF CYBER CRIMES AND FINANCIAL FRAUDS

1998 SHRI HARSH MAHAJAN:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether Government is aware of the increasing incidents of cyber crimes across the country, particularly those related to online financial frauds and phishing;

(b) the number of such cyber crime cases registered during the last three years, along with the State-wise details, including Himachal Pradesh;

(c) the steps taken by Government to strengthen cyber security infrastructure and enhance coordination between law enforcement agencies and financial institutions; and

(d) whether Government proposes to launch any new public awareness campaigns or digital literacy initiatives to protect citizens from falling victim to cyber frauds?

ANSWER

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

(a) to (d): 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, Crime Head-wise & State/UT wise details of cases registered under cyber crimes (involving communication devices as

medium/target) during the period from 2021 to 2023 are at the Annexure-I& II respectively.

'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. The Ministry of Home Affairs has formed CyMAC (Cyber Multi Agency Centre) under the MAC (Multi Agency Centre) platform on 22.01.2025 with the objective to effectively address cybersecurity threats, cyber espionage, misuse of emerging technologies and similar concerns against national security.

vii. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.

viii. National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.

ix. CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.

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

xi. 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.

xii. 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. Till 31.10.2025, National Cyber Forensics Laboratory (Investigation), New Delhi has provided its services to State/UT LEAs in around 12,952 cases pertaining to cyber crimes.

xiii. ‘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.

xiv. 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.

xv. 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.

xvi. 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 in 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.**

*****

ANNEXURE-I
R.S.US. Q. NO. 1998 FOR 17.12.2025

Crime Heads-wise Cases Registered under Cyber Crimes during 2021-2023

SL	Crime Heads	2021	2022	2023
1	Tampering computer source documents	55	65	71
2	Computer Related Offences	19915	23894	35329
3	Cyber Terrorism	15	12	11
4	Publication/transmission of obscene / sexually explicit act in electronic form	6598	6896	7893
5	Interception or Monitoring or decryption of Information	2	1	1
6	Un-authorized access/attempt to access to protected computer system	3	1	1
7	Abetment to Commit Offences	7	4	0
8	Attempt to Commit Offences	5	18	11
9	Other Sections of IT Act	827	1017	920
A	**Total Offences under I.T. Act**	27427	31908	44237
10	Abetment of Suicide (Online)	10	24	30
11	Cyber Stalking/Bullying of Women/Children	1176	1471	1305
12	Data theft	170	97	113
13	Fraud	14007	17470	19466
14	Cheating	6343	10509	16943
15	Forgery	198	224	444
16	Defamation/Morphing	31	61	36
17	Fake Profile	123	157	225
18	Counterfeiting	2	2	0
19	Cyber Blackmailing/Threatening	689	696	689
20	Fake News on Social Media	179	230	209
21	Other Offences	2456	2857	2389
B	**Total Offences under IPC**	25384	33798	41849
22	Gambling Act (Online Gambling)	27	37	87
23	Lotteries Act (Online Lotteries)	4	6	0
24	Copy Right Act	32	27	23
25	Trade Marks Act	1	14	1
26	Other SLL Crimes	99	103	223
C	**Total Offences under SLL**	163	187	334
	Total Cyber Crimes	**52974**	**65893**	**86420**

Source: ‘Crime in India’ published by NCRB.

ANNEXURE-II
R.S.US. Q. NO. 1998 FOR 17.12.2025

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

SL	State/UT	2021	2022	2023
1	Andhra Pradesh	1875	2341	2341
2	Arunachal Pradesh	47	14	24
3	Assam	4846	1733	909
4	Bihar	1413	1621	4450
5	Chhattisgarh	352	439	473
6	Goa	36	90	86
7	Gujarat	1536	1417	1995
8	Haryana	622	681	751
9	Himachal Pradesh	70	77	127
10	Jharkhand	953	967	1079
11	Karnataka	8136	12556	21889
12	Kerala	626	773	3295
13	Madhya Pradesh	589	826	685
14	Maharashtra	5562	8249	8103
15	Manipur	67	18	3
16	Meghalaya	107	75	64
17	Mizoram	30	1	31
18	Nagaland	8	4	2
19	Odisha	2037	1983	2348
20	Punjab	551	697	511
21	Rajasthan	1504	1833	2435
22	Sikkim	0	26	12
23	Tamil Nadu	1076	2082	4121
24	Telangana	10303	15297	18236
25	Tripura	24	30	36
26	Uttar Pradesh	8829	10117	10794
27	Uttarakhand	718	559	494
28	West Bengal	513	401	309
	TOTAL STATE(S)	**52430**	**64907**	**85603**
29	A&N Islands	8	28	47
30	Chandigarh	15	27	23
31	D&N Haveli and Daman & Diu	5	5	6
32	Delhi	356	685	407
33	Jammu & Kashmir	154	173	185
34	Ladakh	5	3	1
35	Lakshadweep	1	1	1
36	Puducherry	0	64	147
	TOTAL UT(S)	**544**	**986**	**817**
	TOTAL (ALL INDIA)	**52974**	**65893**	**86420**

Source: ‘Crime in India’ published by NCRB

*****