GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 2687

TO BE ANSWERED ON THE 19TH DECEMBER, 2023/ AGRAHAYANA 28, 1945 (SAKA)

CYBER FRAUDS

2687. SHRI L.S. TEJASVI SURYA:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) the number of cyber complaints received on the 1905 helpline on a monthly basis for the year 2023;

(b) whether the number of cyber frauds are increasing day by day and if so, the comparison indicating the increase in cyber frauds over the last few years;

(c) the measures taken by the Government to equip policemen to tackle cyber crimes effectively;

(d) whether the convictions in cyber crimes are low in the country and if so, the details of such convictions during the last two years; and

(e) whether there is a need to amend provisions of the Information Technology Act, 2000 to help policemen get more convictions for cyber crimes and if so, the measures taken by the Government towards the same?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI AJAY KUMAR MISHRA)

(a) :Ministry of Home Affairs has operationalized National Cyber Crime Reporting Portal (https://cybercrime.gov.in) on 30th August 2019 to provide a centralized mechanism to the citizens for online reporting of all types of cyber crime incidents, with a special focus on cyber crimes against

women and children. Incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agency (LEA) concerned as per the provisions of the law.

Citizen Financial Cyber Frauds Reporting and Management System (CFCFRMS) has been developed as a part of "National Cybercrime Reporting Portal". This module provides an integrated platform, where all stakeholders including LEAs of States/UTs, all major Banks and financial intermediaries, payment wallets, crypto exchanges and e-commerce companies work in tandem to ensure that quick, decisive, and system-based effective action is taken to prevent the flow of money from victim's account to cyber fraudster's account. The money thus seized is then restored to the victim following due legal process. The platform enables identification of the various financial channels being misused by the fraudsters for routing the fraud proceeds. A toll-free Helpline number '1930' (not 1905, as mentioned in part a) has been operationalized to get assistance in lodging online cyber incidents. More than 10.10 lakh incidents for financial fraud have been registered on CFCFRMS from 01.01.2023 to 30.11.2023. Since inception (01.04.2021)of CFCFRMS, an amount of more than Rs. 1000 Crore have been saved in more than 4 lakh incidents.

(b): 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 2022. As per the data published by the NCRB, year wise details of cases registered under fraud for cyber crimes (involving communication devices as medium/target) during the period from 2020 to 2022 are as under:

Fraud for Cyber Crimes	Year		
	2020	2021	2022
Cases registered	10,395	14,007	17,470

(c): '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 LEAs. The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for their 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) to deal with all types of cyber crime in the country, in a coordinated and comprehensive manner.**

ii. 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. Seven workshops were organized for JCCTs at Hyderabad, Ahmedabad, Guwahati, Vishakhapatnam, Lucknow, Ranchi and Chandigarh in 2023.

iii. The state of the art 'National Cyber Forensic Laboratory (Investigation)' has been established, as a part of the I4C, at New Delhi to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police. So far, National Cyber Forensics Laboratory (Investigation) have provided its services to State LEAs in around 8,840 cyber forensics like mobile forensics, memory forensics, CDR Analysis, etc. to help them in investigation of cases pertaining to cyber crimes.

iv. The Massive Open Online Courses (MOOC) platform, namely 'CyTrain' portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cyber crime investigation, forensics, prosecution etc.

along with certification. More than 72,800 Police Officers from States/UTs are registered and more than 50,000 Certificates issued through the portal.

v. The Ministry of Home Affairs has provided financial assistance to the tune of Rs. 122.24 crores under the 'Cyber Crime Prevention against Women and Children (CCPWC)' Scheme, to the States/UTs for their capacity building such as setting up of cyber forensic-cum-training laboratories, hiring of junior cyber consultants and training of LEAs' personnel, public prosecutors and judicial officers. So far, cyber forensic-cum-training laboratories have been commissioned in 33 States/UTs. So far, more than 24,600 LEA personnel, judicial officers and prosecutors have been provided training on cyber crime awareness, investigation, forensics etc.

vi. National Cyber Forensic Laboratory (Evidence) has been set up at Hyderabad. Establishment of this laboratory provides the necessary forensic support in cases of evidence related to cyber crime, preserving the evidence and its analysis in line with the provisions of IT Act and Evidence Act; and reduced turnaround time.

(d): As per the data published by the NCRB, year wise details of persons convicted under cyber crimes (involving communication devices as medium/target) during the period from 2021 to 2022 are as under:

Details of persons convicted under cyber crimes	Year	
	2021	2022
	736	1407

(e): Ministry of Electronics and Information Technology has recently amended the provisions relating to punishment for contraventions under the IT Act under the Jan Vishwas (Amendment of Provisions) Act, 2023 (18 of 2023)" enacted on 11th August 2023.While one of the objectives of the Jan Vishwas Act was to decriminalise the imprisonment clauses wherever possible, or reduce the quantum of punishment or/and make the offence compoundable for advancing Ease of Doing business, however, the Ministry had retained the criminal punishment for more serious offences. In doing so, the punishment across similar offences under sections 69B and 70B of the Information Technology Act, 2000 relating to enhancing the cyber security measures and cyber incidents response mechanism were aligned under these sections and to make the offences relating to cyber security more deterrent the corresponding fines were also enhanced up to Rs. one crore from the earlier fine of Rs. one lakh only. The said amendments to the IT Act, 2000 are in force from 30th November, 2023.

*****