GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

RAJYA SABHA
UNSTARRED QUESTION NO. 235

TO BE ANSWERED ON THE 24TH JULY, 2024/ SRAVANA 2, 1946 (SAKA)

CYBER CRIMES THROUGH FAKE SITES

235 SHRI C. VE. SHANMUGAM:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether large scale crimes are being committed by cyber criminals through fake sites such as online shopping and applying for Government documents etc. in the country;

(b) if so, the number of cases of crimes through fake sites that have been reported in the country during the last three years, year-wise;

(c) the details of the action taken in said cases, State-wise;

(d) whether Government proposes to set up any monitoring mechanism for fake sites; and

(e) if so, the details thereof and if not, the reasons therefor?

ANSWER

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

(a) to (e): '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 cyber crimes including frauds through fake websites through their Law Enforcement Agencies (LEAs).

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, cases registered under Fraud for Cyber Crime during the year 2020, 2021 and 2022 are 10395, 14007 and 17470 respectively. Specific data regarding frauds through fake websites is not maintained separately by NCRB.

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 for spreading awareness about cyber crimes, issuance of alerts/ advisories, capacity building/training of law enforcement personnel/ prosecutors/judicial officers, improving cyber forensic facilities, etc. The Government has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cyber crime 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. 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.

"Report Suspect" feature has been added with effect from 31.01.2024 on NCRP, for quick reporting of attempts made to commit cybercrime, using suspicious Website URLs. 5252 suspect URLs have been reported so far. I4C analyses and issues necessary advisories to concerned stakeholders from time to time. Facility has been added on NCRP for public to check the authenticity of any website under "Suspect Data" category.

I4C has collaborated with National Internet Exchange of India (NIXI) to prevent abuse of 'dot in' Domains. Between October 2023 and May 2024, 310 'malicious/phishing' domains have been made non functional with the help of NIXI. I4C has also collaborated with Industry for proactive detection of phishing websites on internet through technology-based solution. Further, 91 phishing/ fake websites and 379 illegal loan/ scam apps hosting websites have been made non functional by I4C with the help of stakeholders concerned.

The 'Citizen Financial Cyber Fraud Reporting and Management System', under I4C, has been launched for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. So far, financial amount of more than Rs. 2400 Crore has been saved in more than 7.6 lakh complaints. A toll-free Helpline number '1930' has been operationalized to provide assistance in lodging online cyber complaints.

*****