GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO. *192
TO BE ANSWERED ON: 02.08.2023

CYBER SECURITY GUIDELINES

***192†. SHRI GAJENDRA SINGH PATEL:**

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) the details of the efforts being made by the Government to prevent cyber crime;

(b) whether the Government has issued cyber security guidelines to the States and if so, the details thereof;

(c) whether any scheme is being implemented by the Government to prevent fake calls and online fraud and if so, the details thereof;

(d) whether any workshop is being conducted for cyber security and awareness in rural areas; and

(e) if so, the details thereof along with the steps taken by the Government in this regard during the last three years?

ANSWER

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (e) : A Statement is laid on the Table of the House

STATEMENT REFERRED TO IN REPLY TO LOK SABHA STARRED QUESTION NO. *192 FOR 02.08.2023 REGARDING CYBER SECURITY GUIDELINES

.....

(a) and (c): The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users. With the expansion of the Internet and more and more Indians coming online, instances of cyber crimes have also increased. Government is fully cognizant and aware of various cyber security threats and has undertaken following initiatives for curbing cybercrimes:

i. The Government has established the Indian Cyber Crime Coordination Centre (I4C) to provide a framework and eco-system for Law Enforcement Agencies (LEAs) to deal with cyber crimes in a comprehensive and coordinated manner.

ii. The Government has launched the National Cyber Crime Reporting Portal (https://cybercrime.gov.in) to enable the public to report all types of cyber crimes. Cyber Crimes incidents reported on this portal are routed automatically to respective State/UT LEAs for further handling as per the provisions of law. Also, a toll-free number 1930 has been made operational for citizens to get assistance in lodging online complaints in their own language.

iii. The Information Technology Act, 2000 ("IT Act") and rules made thereunder contain several provisions for safeguarding users in the cyberspace. The Act penalises various offences relating to computer resources, including tampering with computer source documents (section 65), dishonestly or fraudulently damaging computer system (section 66), identity theft (section 66C), cheating by impersonation (section 66D), etc. In addition to such general provisions regarding cyber offences, it also provides for various offences that serve to secure the digital space for women, e.g., violation of bodily privacy (section 66E), transmitting of obscene material (section 67), and publishing or transmission of material containing sexually explicit act in electronic form (section 67A and 67B). These offences are in addition to various penal provisions under the Indian Penal Code, such as the offence of stalking using electronic communication (section 354D).

As per the Seventh Schedule to the Constitution, 'Police' is a State subject. As such, States are primarily responsible for the prevention, investigation etc. of such cybercrimes through the State police departments, which take preventive and penal action as per law.

iv. The Government has launched Sanchar Saathi portal (https://sancharsaathi.gov.in/ to empower mobile subscribers, strengthen their security and increase awareness about citizen centric initiatives of the government.

v. Telecom Regulatory Authorities of India (TRAI) issued a regulation "Telecom Commercial Communication Customers Preference Regulation (TCCCPR), 2018" with an aim to prevent the incidence of Unsolicited Commercial Communications (UCC), which may include Spam and phishing calls.

vi. Department of Telecommunication (DoT) blocks access of Apps used for making fake calls with Calling Line Identification (CLI) of someone else. For example, DoT blocked the access of IndyCall, Booster IndyCall etc.

vii. The Government has set up a call centre with number 1963 / 1800110420 for reporting by the citizens on receiving any incoming international call displaying Indian mobile/ landline numbers. This helps in busting illegal exchanges cum telecom setups in the country. Till date 87 operations of illegal telecom setups have been unearthed.

(b): The Government has issued number of cyber security guidelines to the States/UTs Government which inter alia include the following:

i. The Indian Computer Emergency Response Team (CERT-In) has issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.
ii. The Government has formulated Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors. In addition, guideline documents and templates have been published to assist development and implementation of sectoral Cyber Crisis Management Plans. CCMP provides strategic framework to coordinate recovery from cyber-crisis.

(d) and (e):A number of activities for increasing public awareness regarding cyber security have been carried out, across the country including in rural areas, under the aegis of the Ministry of Electronics and Information Technology. These include the following:

i. 1,519 awareness workshops on information security have been organised in both direct and virtual mode for school and college students, teachers, faculty, government personnel, law enforcement agencies, general users, parents, women, Common Service Centres, etc., covering 3,18,767 participants across 33 States and Union territories. 1,24,909 school teachers have been trained as master trainers in 43 training programme.
ii. 5.75 crore beneficiaries are estimated to have been covered so far through multiple modes including 15 Cyber Safety and Cyber Security Awareness Weeks, 116 mass awareness programme broadcast through Doordarshan/All India Radio; 26 editions of bimonthly newsletter and multilingual awareness materials in the form of handbooks (16), multimedia short videos (75), multi-lingual posters (121), cartoon stories for children (65), etc. which have been disseminated through the print, electronics and social media, besides being made available through the ISEA awareness website (www.infosecawareness.in).
iii. A self-paced three module e-learning course on 'Cyber Hygiene Practices' has been made available through ISEA awareness portal www.infosecawareness.in under which 85,767 participants have been registered and 30,849 participants have been certified. In addition, online quiz competitions on cyber hygiene/cyber security aspects have been organized regularly for various users, in which, 7.37 lakh candidates have participated and 3.90 lakh candidates have cleared the same.
iv. The CSC Academy, a society set up by CSC e-Governance Services India Limited, has partnered with a number of corporate partners to implement cyber security and safety projects in the rural areas covering more than five lakh direct and indirect beneficiaries, including women.
v. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis through its official social media handles and websites, which benefits all citizens, including those in rural areas.
vi. CERT-In organised various events and activities for citizens during Safer Internet Day on 07.02.2023 and Cyber Security Awareness Month in October 2022, by posting security tips using posters and videos on social

media platforms and websites. CERT-In, in association with Centre for Development of Advanced Computing, conducted an online awareness campaign for citizens, covering topics such as general online safety, social media risks and

safety, mobile related frauds and safety, secure digital payment practices, etc., through videos and quizzes on the MyGov platform.

vii. Cyber Swachtta Kendra conducted "Cyber Swachhta Campaign" during the month of October 2022, and around 69 crore one-time SMS were sent out through Internet Service Providers to citizens including in rural areas to create cyber security awareness.

viii. The Ministry of Home Affairs (MHA) has taken steps to spread awareness on cyber crime that inter-alia include; issuance of alerts/advisories, dissemination of messages through SMS, 14C social media account i.e. Twitter handle (@Cyberdost), Facebook(CyberDostI4C), Instagram (cyberdosti4c), Telegram (cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple media, publishing of Handbook for Adolescents/Students, organizing of Cyber Safety and Security Awareness week, in association with police department in different States/UTs etc.

ix. MHA has issued advisory to all the State/UT Governments to carry out publicity of National Cyber Crime Reporting Portal https://cybercrime.gov.in and toll-free helpline number '1930' to create mass awareness.

****