GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1625
TO BE ANSWERED ON:**21.09.2020**

THREAT OF CYBER ATTACK

1625. SHRI TALARI RANGAIAH:

Will the Minister of Electronics & Information Technology be pleased to state:-

(a) whether the Government has made any efforts to protect the public against the possibility of cyber attacks during lockdown;
(b) if so, the details thereof;
(c) the steps taken by the Government to check cyber attacks completely and if so, the details thereof;
(d) whether the Government has any statistics regarding the number of citizens who are vulnerable to cyber crimes amid Coronavirus pandemic; and
(e) if so, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a) and (b): During the COVID-19 pandemic situation, the Indian Computer Emergency Response Team (CERT-In) has worked proactively and tracked various cyber threats in the Indian cyber space. CERT-In issued 23 advisories on various topics such as secure use of web conferencing software, securing mobile devices and apps, secure use of Virtual Private Network (VPN), security best practices for Work From Home (WFH), security measures for healthcare sector, online safety of children, various phishing attack campaigns pretending to be from popular Apps and services and securely managing business continuity during crisis situation due to COVID- 19 pandemic. etc.In addition, CERT-In has conducted 3 cyber crisis exercises for organizations to train and guide them to respond to COVID-19 pandemic related cyber-attacks. 72 organisations including key stakeholders participated in these exercises.

Cyber security incidents such as phishing, Distributed Denial of Service (DDoS) attacks, website intrusions, malware infections and vulnerable services were handledbyCERT-In through coordinated measures with concernedorganisations and stakeholders.

(c): Government has taken following measures to enhance the cyber security posture and prevent cyber attacks:

(i) 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 regular basis.

(ii) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
(iii) All the government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications will be conducted on a regular basis after hosting also.
(iv) Government has empanelled 90 security auditing organisations to support and audit implementation of Information Security Best Practices.
(v) Government has formulated Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.
(vi) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 49 such drills have so far been conducted by CERT-In where 434 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.
(vii) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks.
(viii) Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.
(ix) Government has initiated setting up of National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. Phase-I of NCCC has been made operational.

(d) and (e): Due to increase in online transactions, citizens are vulnerable to cyber crimes amid Coronavirus pandemic due to phishing and spamming.

'Police' and 'Public order' are State subjects as per the Constitution of India and States/UTs are primarily responsible for prevention, detection, investigation and prosecution of crimes through their law enforcement machinery. The Law Enforcement Agencies take legal action as per provisions of law against the cyber crime offenders.

Government of India helps States in combating cyber crimes by assisting them through advisories and funds under various schemes.

The Government has launched the online National Cyber Crime Reporting Portal, www.cybercrime.gov.in to enable citizens to report complaints pertaining to all types of cyber crimes with special focus on cyber crimes against women and children. A toll-free helpline no. 155260 has been made operational in all States/UTs to assist citizens.

Government is implementing a scheme 'India Cyber Crime Coordination Centre'(I4C) to deal with cyber crimes in a coordinated & comprehensive manner.

Further, to spread awareness on cyber crime, several steps have been taken that include dissemination of messages on cyber crime through MHA Twitter handle @CyberDost, Radio campaign, publishing of Handbook for Adolescents / Students, publishing of 'Information Security Best practices' for the benefit of Govt. Officials, organizing of Cyber Safety and Security Awareness week, in association with police department in different States/UTs etc.

******