GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO.1693
TO BE ANSWERED ON: 09.03.2018

CRITICAL INFRASTRUCTURE TO PREVENT CYBER CRIMES

1693. DR. T. SUBBARAMI REDDY:

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

(a) the number of cyber crimes like phishing, scanning or probing, site intrusions, defacements, virus or malicious code and ransomware reported during the last three years;

(b) whether, in view of online transactions, the Ministry has adequate mechanism and technology to deal with the rising cyber crimes; and

(c) the steps taken to put in place critical infrastructure to predict and prevent cyber crimes?

ANSWER

MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(a): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total no. of 49455, 50362 and 53081 cyber security incidents were observed during the year 2015, 2016 and 2017 respectively. The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, ransomware, Denial of Service attacks, etc.

(a) and (c)**:** Government has taken a number of legal, technical and administrative measures to prevent incidents of cyber crimes. These *inter alia,* include:

(i) Enactment of the Information Technology (IT) Act, 2000 which has adequate provisions for dealing with prevalent cyber crimes.

(ii) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the Information Technology (IT) Act, 2000 for protection of critical information infrastructure in the country. NCIIPC has been regularly advising the critical information infrastructure sector organisation to reduce vulnerabilities to all kinds of threats and attacks, by sharing threat intelligence, guidelines, best practices and frameworks for protection and guiding them with policies and protection strategies. In addition, training and awareness programs are regularly conducted to improve the cyber hygiene in CII organisations

(iii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers on regular basis. Security tips have been published to enable users to secure their Desktops and mobile/smart phones. Tailored alerts are sent to key organisations to enable them to detect and prevent cyber attacks.

(iv) Government has initiated setting up of National Cyber Coordination Centre (NCCC) in CERT-In 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.

(v) 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 for banks as well as common users.

(vi) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of cyber crime cases.

(vii) Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of law enforcement personnel and Judiciary in these States.

(viii) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 15 such drills have so far been conducted by CERT-In where 148 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated. In addition 3 drills were conducted in coordination with The Reserve Bank of India and The Institute for Development and Research in Banking Technology.

(ix) A number of Cyber forensics tools for collection, analysis and presentation of the digital evidence have been developed indigenously and such tools are being used by law enforcement Agencies.

(x) 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.

(xi) 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. 22 training programs covering 610 participants were conducted during the year 2017.

*****