GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION. NO. *27
TO BE ANSWERED ON: 21.07.2023

INCREASE IN CYBER ATTACKS IN NON-METROPOLITAN AREAS

***27 SHRI V. VIJAYASAI REDDY:**

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

(a) whether cyber attacks have increased in non-metropolitan areas, strategically targeting rural population with lower digital awareness;

(b) if so, the steps taken by Government to create awareness about such cyber attacks among rural population;

(c) whether it is a fact that 25 per cent of cases are closed due to insufficient evidence, only 4 per cent are chargesheeted and majority of cases are still pending for investigation;

(d) if so, the reasons therefor and steps taken to address these issues; and

(e) the details of any other steps taken by Government to ensure that people are equipped to identify and deal with cyber attacks?

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 RAJYA SABHA STARRED QUESTION NO. *27 FOR 21.07.2023 REGARDING INCREASE IN CYBER ATTACKS IN NON-METROPOLITAN AREAS

……..

(a) and (b): 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, the possibility that Digital Nagrik or citizens being exposed to user harms and criminality has also increased. Government is fully cognizant and aware of various cyber security threats and it is necessary to create awareness among digital nagrik on issues of cyber security.

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) 1,509 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 3,14,115 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 the ISEA awareness website, under which 74,495 participants have been registered and 27,764 participants certified; also Online quiz competitions on cyber hygiene and cyber security aspects have been organised for various users, in which 6.22 lakh persons have participated, of which 3.21 lakh 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) In addition, 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, which benefits all citizens, including those in rural areas.

(c) to (e): As per the provisions of the Code of Criminal Procedure, 1973, prevention and investigation of cognizable offences is to be done by the police, and 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, including in respect of training their police personnel for upgrading technical knowhow to investigate and solve such crimes.

Further, the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs has been designated as the nodal point in the fight against cybercrime. A toll-free number 1930 has been made operational for citizens to get assistance in lodging online complaints in their own language. To spread awareness on cybercrime, the Ministry of Home Affairs has taken several steps that include dissemination of messages on cybercrime through the Twitter handle @cyberDost and radio campaigns.

A Massive Open Online Courses (MOOC) platform, named 'CyTrain' portal, was developed under the Indian Cyber Crime Coordination Centre set up by the Ministry of Home Affairs, for capacity building of police officers and judicial officers through online courses on critical aspects of cybercrime investigation, forensics, prosecution etc., along with certification. In addition, training curriculum was prepared for police personnel, public prosecutors and judicial officers for better handling of investigation and prosecution. States and Union Territories have been requested to organise training programmes accordingly.

Cyber Swachhta Kendra (CSK) - Botnet Cleaning and Malware Analysis Centre, operated by CERT-In, has been established for detection of compromised systems in India and to notify, enable cleaning and securing systems of end users to prevent further malware infections. The centre works in close coordination and collaboration with Internet Service Providers, Academia and Industry. The centre provides detection of malicious programs and free tools to remove the same for common users.

******