GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 262
TO BE ANSWERED ON: 03.02.2023

SECURITY MEASURES TO AVOID CYBER ATTACKS

262. SHRI K.C. VENUGOPAL:

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

(a) whether it is a fact that ransomware incidents and cyber attacks grew significantly last year;
(b) if so, the details thereof;
(c) whether Government has taken necessary security measures to avoid cyber attacks, particularly in the light of Government offices going digital; and
(d) if so, the details thereof, and if not, the reasons therefor?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a) and (b):The Government is committed to an Open, Safe and Trusted and Accountable Internet for its users. With a borderless cyberspace coupled with the anonymity, along with rapid growth of Internet, rise in cyber attacks, cyber security incidents and user harm area global phenomenon and hence the focus of Government on policies and rules forthe Open, Safe and Trusted and Accountable Internet for all Indian users

Ransomware incidents have grown over time with attacks across multiple sectors, including commercial and critical infrastructure. Threat actors have sophisticated attack methodologies and tactics and adopted a wide range of strategies.Ransomware actors exploit known vulnerabilities, compromised credentials of remote access services and phishing campaigns for gaining access into the infrastructure of organisations.

The Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India.It is continuously focused on expanding its capacity and capabilities to deal with these newly emerging sophisticated cyber threats.CERT-In has reported a total number of 1402809 and 1391457 cyber security incidents including 132 and 202 ransomware incidents during the year 2021 and 2022 respectively

(c) and (d):The following measures have been taken to enhance the cyber security posture and curb such incidents:

(i) A Cyber Crisis Management Plan for countering cyber-attacks and cyber-terrorism, has been formulated by CERT-In, for implementation by all Ministries and Departments of the Central Government, State Governments and their organisations and critical sectors.
(ii) On observing a ransomware incident, CERT-In notifies the affected organisations along with remedial actions to be taken, and coordinates incident response measures with affected organisations, service providers, respective sector regulators and law enforcement agencies.
(i) Regular training programmes for network and system administrators and the Chief Information Security Officers of government and critical sector organisations are conducted by CERT-In, for securing the information technology infrastructure and

mitigating cyber-attacks. A total of 42 training programmes were conducted, covering 11,486 participants, during the years 2021 and 2022.

(iv) CERT-In has been issuing alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks, on an ongoing basis.

(ii) Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) is operated by CERT-In to detect malicious programs and free tools to remove the same, and to provide cyber security tips and best practices for citizens and organisations.

(iii) CERT-In operates an automated cyber-threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

(vii) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

(viii) Cyber security mock drills are conducted to enable assessment of cyber security posture and preparedness of organisations in the government and critical sectors. 74 such drills have so far been conducted by CERT-In, in which 990 organisations from different States and sectors participated.

(ix) The National Cyber Coordination Centre has been set up to generate situational awareness regarding existing and potential cyber security threats.

(x) CERT-In and the Reserve Bank of India (RBI) jointly carried out a cyber security awareness campaign on ‘beware and be aware of financial frauds’ through the Digital India Platform.

******