GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1061
TO BE ANSWERED ON: 10.02.2023

GOVERNMENT ORGANIZATIONS AFFECTED BY RANSOMWARE/ SMISHING/PHISHING/CYBER HACKING ATTEMPT

1061. SHRI SUJEET KUMAR:

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

(a) the details of Government Organizations affected by ransomware/ smishing/ phishing/ cyber hacking attempt in the last three years; and
(b) the steps been taken by the Ministry to address these issues?

ANSWER

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

(a): The Government is committed to ensure that the Internet in India is Open, Safe and Trusted and Accountable for all its users. With the expansion of the Internet and more and more Indians coming online, the possibility of cyber-attacks has also increased.

As per the information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), a total of 9, 7 and 19 ransomware incidents pertaining to government organisations were observed during the years 2020, 2021 and 2022 respectively. Further, a total of 77, 159 and 246 phishing and smishing incidents of government organisations and 59, 42 and 50 incidents of hacking of website of Ministries/Departments of the Central Government and of State Governments were observed during the years 2020, 2021 and 2022 respectively.

(b): Government is fully cognizant and aware of various cyber security incidents and has taken following measures to enhance the cyber security posture and curb such incidents:

(i) CERT-In coordinates incident response measures with affected organisations, service providers, respective sector regulators as well as law enforcement agencies. CERT-In notifies the affected organisations along with remedial actions to be taken.
(ii) CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations for proactive threat mitigation actions by them.
(iii) CERT-In operates the Cyber Swachhta Kendra (Botnet cleaning and malware analysis centre) to detect malicious programs and free tools to remove the same, and to provide cyber security tips and best practices for organisations.
(iv) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.
(v) CERT-In issues alerts and advisories on latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis.
(vi) Security tips are published for users to secure desktops and mobile phones and to prevent phishing attacks.
(vii) Cyber Crisis Management Plan formulated by CERT-In for implementation by all Ministries and Departments of the Central and State Governments and their organisations and critical sectors to help counter cyber-attacks and cyber terrorism.
(viii) CERT-In conducts regular training programmes for network and system administrators and Chief Information Security Officers of government organisations regarding securing information technology infrastructure and mitigating cyber-

attacks. Forty-two training programmes have been conducted, covering 11,486 participants, during the years 2021 and 2022.

(ix) All government websites and applications are audited with respect to cyber security and compliance with the Government of India Guidelines for Websites prior to their hosting. The auditing of the websites and applications is conducted on a regular basis after hosting also.

(x) Cyber security mock drills are conducted to enable assessment of cyber security posture and preparedness of organisations in the Government and critical sectors. Seventy-four such drills have been conducted by CERT-In, covering 990 organisations from different States and sectors.

(xi) CERT-In and the Reserve Bank of India jointly carry out a cyber security awareness campaign on 'beware and be aware of financial frauds' through the Digital India Platform.

(xii) CERT-In has set up the National Cyber Coordination Centre to generate situational awareness regarding existing and potential cyber security threats.

(xiii) The Ministry of Electronics and Information Technology conducts programmes to generate information security awareness. Specific books, videos and online materials are developed about information security which are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

(xiv) The analytics centre at National Critical Information Infrastructure Protection Centre provides near-real-time threat intelligence and situation awareness, based on which regular alerts and advisories are sent to critical information infrastructure / protected system entities of the government to mitigate cyber security threats.

****