**GOVERNMENT OF INDIA**
**MINISTRY OF HOME AFFAIRS**

**LOK SABHA**
**STARRED QUESTION NO. *393**

**TO BE ANSWERED ON THE 23RD MARCH, 2021/ CHAITRA 2, 1943 (SAKA)**

**CYBER ATTACKS**

***393. MS. PRATIMA BHOUMIK:**

**Will the Minister of HOME AFFAIRS be pleased to state:**

**(a) whether there has been an increase in cyber attacks in the country;**

**(b) if so, the details of cyber attacks reported during the last two years;**

**(c) whether there are reports of cyber attack into systems of the companies which manage power supply and also into the system of a company which is supplying COVID-19 Vaccine across the country; and**

**(d) if so, the details thereof along with the action taken by the Government in this regard?**

**ANSWER**

**MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS**
**(SHRI G. KISHAN REDDY)**

**(a) to (d): A Statement is laid on the Table of the House.**

**STATEMENT REFERED TO IN REPLY TO LOK SABHA STARRED QUESTION *393 FOR 23.03.2021 REGARDING CYBER ATTACKS**

**(a) & (b): As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), 3,94,499 and 11,58,208 cyber security incidents have been observed during the years 2019 and 2020 respectively.**

**(c) & (d): The Indian Computer Emergency Response Team (CERT-In) is serving as national agency for responding to cyber security incidents as per provisions of Section 70B of Information Technology Act, 2000. CERT-In receives inputs from its situational awareness systems and threat intelligence sources about malware infections in networks of entities across sectors. Whenever any incident comes to the notice of CERT-In, it issues alerts and advisories to the entities concerned and sectoral Computer Emergency Response Teams (CERTs) for remedial measures.**

**Government has taken following measures to enhance the cyber security posture and prevent cyber attacks:**

i. **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 audited with respect to cyber security prior to their hosting. The auditing of the websites and applications are conducted on a regular basis after hosting also.

iv. Government has empanelled security auditing organisations to support and audit implementation of Information Security Best Practices.

v. Government has formulated Cyber Crisis Management Plan (CCMP) for countering cyber attacks for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

vi. Government is operating 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.

vii. Government has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.

********