GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 656
TO BE ANSWERED ON: 16.09.2020

SECURITY BREACH IN USER DATA

656. SHRI PRATHAP SIMHA:
SHRI L.S. TEJASVI SURYA:

Will the Minister of Electronics & Information Technology be pleased to state:-

(a) whether the Government is aware of any security breach in the user data stored with the BHIM app, and if so, the details thereof.

(b) whether there have been any previous instances of security breaches of Government websites, apps and services and if so, the details thereof and the data of occurrence of such a breach.

(c) whether the Government is taking steps to further strengthen its existing security patches and if so, the details thereof; and

(d) whether the Government proposes to take steps in order to prevent any future relapses in data security, and if so, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a): No such security breach in BHIM app has been reported to Ministry of Electronics and Information Technology.

(b): As per the information reported to and tracked by Computer Emergency Response Team(CERT-In), a total number of 54 and 37 websites of Central Ministries/Departments and State Governments were hacked during the year 2019 and 2020 (till August)respectively. Further, a total number of 15 instances of insecure data hosting of government website based services were reported in 2020 (till August).Remedial measures were suggested to owners of affected websites and services.

(c) and (d): In tune with the dynamic nature of Information Technology and emerging cyber threats, continuous efforts are required to be made by owners and users to protect networks and data by way of hardening and deploying appropriate security controls.
Government has taken following measures to enhance the cyber security posture and prevent cyber attacks:

i. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data 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 to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications are to be conducted on a regular basis after hosting also.

iv. Government has empanelled 90 security auditing organisations to support and audit implementation of Information Security Best Practices.

v. 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/UTs and their organizations and critical sectors.

vi. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 49 such drills have so far been conducted by CERT-In where 434 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated.

vii. 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.

viii. 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.

ix. Government has initiated setting up of National Cyber Coordination Centre (NCCC) 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.

******