GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2335
TO BE ANSWERED ON: 05.08.2022

DATA BREACHES

2335. DR. SANTANU SEN :
SHRI ABIR RANJAN BISWAS:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:
(a) the details of the data breaches reported in the country in the last five years, year-wise;
(b) the details of the action taken by Government against the breaches;
(c) the details of the number of banking fraud- online/UPI related reported in the last five years in the country; and
(d) the details of the unrecovered money involved in banking fraud- online/UPI, year-wise?

ANSWER

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

(a): Indian Computer Emergency Response Team (CERT-In) is mandated to track and monitor cyber security incidents in India. CERT-In has reported that a total number of 2, 5, 11, 36, 39 and 13 data breach incidents are observed during the year 2017, 2018, 2019, 2020, 2021 and 2022 (upto June) respectively.

(b): The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users. Government has taken the following measures to enhance the cyber security posture and prevent data leaks:

i. On observing the data breaches, CERT-In notifies the affected organisations along with remedial actions to be taken. CERT-In coordinates incident response measures with affected organisations, service providers, respective sector regulators as well as Law Enforcement Agencies (LEA).

ii. CERT-In issues advisories to organisations regarding prevention of data breaches, data leaks and also issues best practices forthe users for mitigating risk due to data breaches and securing online credentials. CERT-In has issued 70 advisories for data security and mitigating fraudulent activities.
Further, CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.

iii. CERT-In operates an automated cyber threat exchange platform to proactively collect, analyse and share tailored alerts with organizations across sectors for proactive threat mitigation actions by them.

iv. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

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

vi. CERT-In has empanelled 97 security auditing organisations to support and audit implementation of Information Security Best Practices.

vii. CERT-In has formulated a Cyber Crisis Management Plan to counter cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

viii. Cyber security mock drills and cyber security exercises are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 67 such drills have so far been conducted by CERT-In where 886 organizationsfrom different States and sectors participated.

ix. 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. 19 and 5 training programs were conducted covering 5169 and 449 participants during the year 2021 and 2022 (upto June) respectively.

x. CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre provides detection of malicious programs and free tools to remove the same alongwith cyber security tips and best practices for citizens and organisations.

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

xii. CERT-In also co-operates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as Law Enforcement Agencies.

xiii. Ministry of Home Affairs (MHA) has issued National Information Security Policy and Guidelines (NISPG) to the Central Ministries/Departments as well as the State Governments/Union Territories in order to prevent information security breaches/Cyber intrusions in ICT infrastructure.

(c): Activities of fraudulent emails, SMS messages and phishing websites pretending to be from legitimate services, lure users to divulge credentials to conduct financial frauds. As per the information reported and tracked by CERT-In, a total number of 552, 454, 472, 280, 523 and 1217 phishing incidents were observed during the year 2017, 2018, 2019, 2020, 2021 and 2022 (upto June) respectively. CERT-In has also reported that a number of 14, 6, 4, 4, 13 and 9 financial fraud incidents affecting ATMs, Cards, Point of Sale (PoS) systems and Unified Payment Interface (UPI) have been reported during the year 2017, 2018, 2019, 2020, 2021 and 2022 (upto June) respectively.

As per the National Payments Corporation of India (NPCI), the number of UPI fraud cases reported by member banks to NPCI were 172, 1967, 17759, 77299 and 84274 during the financial years2017-18, 2018-19, 2019-20, 2020-21 and 2021-22 respectively.

(d): There is no such information available with Ministry of Electronics and Information Technology (MeitY).

****