

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION. NO. 2327
TO BE ANSWERED ON: 17.12.2021

DATA BREACHES

2327. DR. SANTANU SEN:

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 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 and 33 data breach incidents are observed during the year 2017, 2018, 2019, 2020 and 2021 (upto October) respectively.

(b): The Government has taken several measures to enhance the cyber security posture and prevent cyber-attacks:

- 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.
- ii. The Indian Computer Emergency Response Team (CERT-In) issues advisories to organisations regarding prevention of data breaches, data leaks and best practices to be followed by users for mitigating risks due to data breaches and securing online credentials. CERT-In has issued 68 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. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

- iv. 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.
- v. CERT-In has empanelled security auditing organisations to support and audit implementation of Information Security Best Practices.
- vi. The Government has formulated a Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State /UT Governments and their organizations and critical sectors.
- vii. Cyber security mock drills are conducted regularly in Government and critical sectors. So far 61 such drills have been conducted by CERT-In where 600 organisations from different States and sectors have participated.

- viii. 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. 15 and 17 training programs were conducted covering 708 and 4801 participants during the year 2020 and 2021 (till October) respectively.
- ix. CERT-In 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.
- x. CERT-In 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.

(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 to and tracked by CERT-In, a total number of 552, 454, 472, 280 and 379 phishing incidents were observed during the year 2017, 2018, 2019, 2020 and 2021 (upto October) 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 67230 during the financial years 2017-18, 2018-19, 2019-20, 2020-21 and 2021-22 (upto November 2021) respectively.

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