GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION. NO. 2137
TO BE ANSWERED ON: 09.08.2024

ACTION AGAINST DATA BREACHES

2137. DR. FAUZIA KHAN:

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 actions taken by Government against these breaches;
(c) The details of banking frauds- online/UPI related, reported in the last five years in the country;
(d) The details of the unrecovered money involved in banking fraud- online/UPI, year-wise and State/Union Territory-wise; and
(e) The details of the measures being adopted by Government to counter the said situation?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (e): The Government is fully cognizant and aware of various cyber security threats and challenges and has taken following measures against data breaches:

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

(ii) CERT-In has issued an advisory to various Ministries outlining the measures to be taken for strengthening the cyber security by all entities that are processing the digital personal data or information including sensitive personal data or information.

(iii) The Digital Personal Data Protection Act, 2023 (The DPDP Act) provides for the processing of digital personal data in a manner that recognizes the need to process personal data for lawful purposes by the data fiduciaries.

(iv) MeitY has issued Guidelines for Cybersecurity Audit that cover both comprehensive and limited audit on periodic basis by competent auditors with clear responsibilities for ensuring such audit regularly, inclusive of vulnerability assessment and penetration testing.

(v) CERT-In regularly carries out various activities for development of cyber security capacities, skill building, awareness and citizen sensitization with respect to cyberattacks and cyber frauds. In order to create security awareness within the Government, Public and Private Sector organizations, CERT-In regularly conducts trainings / workshops to train officials of Government, Public and Private sector organizations across all sectors on focused topics of Cyber Security.

(vi) National Informatics Centre (NIC) provides IT support to user ministries, departments and agencies of the Central Government, State Governments and

district administrations for various e-governance solutions and, as part of this, helps maintain various government databases that contain data of citizens. NIC follows information security policies and practices in line with industry standards and practices, aimed at preventing cyber-attacks and safeguarding data.

(vii) CERT-In has empanelled 176 security auditing organisations to support and audit implementation of Information Security Best Practices.

(viii) CERT-In has issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.

(ix) Cybersecurity mock drills are conducted to enable assessment of cyber security posture and preparedness of organisations in the Government and critical sectors. 92 such drills have been conducted by CERT-In where around 1400 organizations from different States and sectors participated.

(x) National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.

(xi) Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.

Further measures adopted by Government are as follows:

(i) To deal with cybercrimes in a coordinated & comprehensive manner, Ministry of Home Affairs operates a National Cyber Crime Reporting Portal (www.cybercrime.gov.in) to enable citizens to report complaints pertaining to all types ofcybercrimes.

(ii) The Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs is designated as the nodal point in the fight against cybercrime. A toll-free number 1930 is operational for citizens to get assistance in lodging online complaints in their own language. To spread awareness on cybercrime, the Ministry has taken several steps, which include dissemination of messages on cybercrime through the Twitter handle @cyberDost and radio campaigns.

(iii) RBI through “RBI Kehta Hai” has issued guidelines on aspects such as different types of frauds, modus operandi, and measures to be taken during digital payment transactions and through advertising (through prominent personalities) for creating awareness amongst public, etc.

(iv) RBI has issued the booklet BE(A)WARE on modus operandi of financial frauds in the public domain to educate the public.

(v) CERT-In and the RBI jointly carry out a cyber security awareness campaign on ‘beware and be aware of financial frauds’ through the Digital India Platform.

****