GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2418
TO BE ANSWERED ON: 15.03.2023

BREACHING OF USER DATA

2418. SHRI PRADYUT BORDOLOI:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether the Government is aware of the reported leaks and breaches of user data during the last five years;
(b) if so, the details thereof along with the action taken by the Government thereto;
(c) the details of data hacked from the RailYatri app which is authorised by IRCTC;
(d) whether any civil/criminal action has been initiated against any company for breach of data and if so, the details thereof and if not, the reasons therefor; and
(e) the details of the Government websites which leaked the data and the action taken by the Government for such breach?

ANSWER

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

(a) and (b): The policies of the Government are aimed at ensuring an Open, Safe, Trusted and Accountable Internet for its users. With the expansion of the Internet, more and more Indians coming online and increase in the volume of data generated, stored and processed, instances of data breaches have also grown. As per information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), a total of47 incidents of data leak and 142incidents of data breach were reported during the last five calendar years.

To achieve the Government's aim, enhance the cybersecurity posture and thereby secure data against leak and breach, Government has acted on several fronts. Some of the key actions taken are as under:

(i) CERT-In, in April 2022, issued directions under section 70B for mandatory reporting of cyber incidents to CERT-In within six hours of such incidents being noticed or being brought to notice.
(ii) CERT-In, in December 2022, issued a special advisory on best practices to enhance the resilience of health sector entities, and has requested the Ministry of Health and Family Welfare to disseminate the same to all authorised medical care entities and service providers in the country.
(iii) Cyber security best practices have been issued in September 2022 for adherence by all government employees, including outsourced, contractual and temporary employees who work for Central Government's Ministries and Departments.
(iv) CERT-In coordinates incident response measures with affected organisations, service providers, respective sector regulators as well as Law Enforcement Agencies. CERT-In notifies the affected organisations along with remedial actions to be taken.
(v) Cyber Crisis Management Plan formulated by CERT-In for implementation by all Ministries and Departments of the Central / State Governments and their organisations and critical sectors help to counter cyber-attacks and cyber terrorism.
(vi) CERT-In conducts regular training programmes for network and system administrators and Chief Information Security Officers of government and critical sector organisations regarding securing information technology infrastructure and mitigating cyber-attacks. A total of 42 training programmes have been conducted, covering 11,486 participants, during the years 2021 and 2022.

(vii) All government websites and applications are audited with respect to cyber security and compliance with the Government of India Guidelines for Websites prior to their hosting.
(viii) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.
(ix) CERT-In issues alerts and advisories on latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis.
(x) CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.
(xi) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and free tools to remove the same, and to provide cyber security tips and best practices for citizens and organisations.
(xii) Security tips are published for users to secure desktops and mobile phones and to prevent phishing attacks.
(xiii) Cybersecurity mock drills are being conducted to enable assessment of cyber security posture and preparedness of organisations in the Government and critical sectors. Seventy-four such drills have been conducted by CERT-In, covering 990 organisations from different States and sectors.
(xiv) CERT-In organised various events and activities for citizens during Safe Internet Day on 8.2.2022 and Cyber Security Awareness Month in October 2022 by posting security tips using posters and videos on social media platforms and websites. CERT-In, in association with C-DAC, conducted an online awareness campaign for citizens, covering topics such as general online safety, social media risks and safety, mobile related frauds and safety, secure digital payment practices etc. through videos and quizzes on MyGov platform.
(xv) CERT-In and the Reserve Bank of India jointly carry out a cyber security awareness campaign on 'beware and be aware of financial frauds' through the Digital India Platform.
(xvi) The Ministry of Electronics and Information Technology conducts programmes to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security, which are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

(c) and (d): As per information furnished by the Indian Railway Catering and Tourism Corporation (IRCTC), upon receipt of information from CERT-In in December 2022 regarding leakage of data acquired and maintained by RailYatri app, the ticket-booking facility on RailYatri app was stopped, penalty was imposed on the company which is the custodian of the RailYatri app, and the app was restored after taking necessary security measures.

(e): As per the information reported to and tracked by CERT-In, a total of 10, 5 and 7 incidents of data leak related to government organisations were reported for the years 2020, 2021 and 2022 respectively. On observing 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 and law enforcement agencies.

****