GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO. *97
TO BE ANSWERED ON: 26.7.2023

LEAKING OF COWIN APP DATA

***97. SHRI RAVIKUMAR D.:**
SHRI ASADUDDIN OWAISI:

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

(a) the total number of people affected by the alleged leak of their personal and sensitive information including vaccination details by a Telegram Bot in the country;

(b) whether the Government was able to identify the threat actors behind this latest leak and if so, the details thereof along with the details of any enquiry conducted in this regard;

(c) whether any steps are being taken by the Government to strengthen the safety of the personal and biometric data of the citizens on the CoWin App/ portal; and

(d) if so, the details thereof and if not, the reasons therefor?

ANSWER

MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (d): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO LOK SABHA STARRED QUESTION NO. *97 FOR 26-7-2023 REGARDING LEAKING OF COWIN APP DATA

…….

(a) and (b): The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all users. With the expansion of the Internet and more and more Indians coming online, the possibility that citizens being exposed to user harms and criminality has also increased. Government is fully cognizant and aware of various cyber security threats.

Taking cognizance of the cyber incident regarding CoWIN data in June 2023, CERT-In coordinated incident response measures with Ministry of Health & Family Welfare (MoHFW). The MoHFW has lodged a complaint and F.I.R has been registered by a Law Enforcement Agency. CERT-In has provided inputs to facilitate investigation.

(c) and (d): As per the information provided by MoHFW, Co-WIN portal of Ministry of Health & Family Welfare has complete security measures and adequate safeguards for data privacy with Web Application Firewall (WAF), Anti- Distributed Denial-of-Service (DDoS), Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Identity & Access Management and regular vulnerability assessment.

To ensure safety of the personal and biometric data of the citizens on the Co-WIN App / Portal, MoHFW has taken following measures :

(i) Beneficiary can access vaccination details by registered mobile number through OTP authentication only.
(ii) Mobile Numbers, Aadhaar Number & other Photo ID Card numbers of beneficiary are masked. Only last 4 characters are visible to users (service providers) of Co-WIN.
(iii) Complete Co-WIN database is encrypted using “Encryption Algorithm” key toprotect citizen data and data integrity is maintained for all vital information.
(iv) Two factor authentication feature (Password & OTP) while login by the users (service providers) is put in place restricting unauthorised access to Co-WIN.

Government has taken following measures to enhance the cyber security posture and prevent data breaches:

(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) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.
(iii) A special advisory on security practices to enhance resilience of health sector entities has been communicated by CERT-In to the Ministry of Health and Family Welfare, for sensitising health sector entities regarding latest cyber security threats in December 2022. The Ministry has been requested to disseminate the advisory among all authorised medical care entities / service providers in the country.
(iv) 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.
(v) 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.

(vi) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

(vii) 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 Governments and their organizations and critical sectors.

(viii) Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 80 such drills have so far been conducted by CERT-In where 1062 organizations from different States and sectors participated.

(ix) 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

(x) Security tips have been published for users to secure their desktops and mobile phones and to prevent phishing attacks.

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

****