

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2521
TO BE ANSWERED ON: 21.12.2022

RISING INCIDENCE OF DATA BREACHES

2521. SHRI BHARTRUHARI MAHTAB:

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

- (a) whether any step has been taken by the Government to combat the rising incidence of data breaches in the country and if so, the details thereof;
- (b) whether the Government is contemplating any changes to the Information Technology Act, 2000;
- (c) if so, the details thereof including the current status of the National Cyber Security Policy; and
- (d) the reasons for the delay in the new cyber security policy?

ANSWER

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

(a) to (d): 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.

To achieve the Government's aim and to secure such data, the Government has published the National Cyber Security Policy. In line with vision and mission of the policy, Government has taken the following measures:

- (i) The Indian Computer Emergency Response Team (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.
- (ii) 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.
- (iii) 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.
- (iv) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.
- (v) CERT-In issues alerts and advisories on latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis.
- (vi) Security tips are published for users to secure desktops and mobile phones and to prevent phishing attacks.
- (vii) 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.

- (viii) 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. Forty one training programmes have been conducted, covering 11,377 participants, during the years 2021 and 2022 (up to November).
- (ix) 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.
- (x) Cyber security 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.
- (xi) 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.
- (xii) 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.
- (xiii) 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.

Further, the National Security Council Secretariat has formulated a draft National Cyber Security Strategy, which holistically looks at addressing the security issues in the national cyberspace.

Government, from time to time, receives suggestions from various quarters regarding changes to various enactments. Such suggestions also include those related to various provisions of the Information Technology Act, 2000. Examination of such suggestions is an ongoing activity.
