GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *78
TO BE ANSWERED ON: 09.02.2024

CYBER SECURITY AND HACKING OF SOCIAL MEDIA

***78. SHRI K.R.N. RAJESHKUMAR:**

Will the Minister of Electronics and Information Technology be pleased to state:

(a) whether the Ministry discusses cyber security and hacking of social media accounts (like Facebook) of individual users with leading social media platforms;
(b) if so, whether social media platforms assured Government of its security features to prevent hacking;
(c) the number of hacking / digital impersonations of public persons complaints received by Government; and
(d) the security measures and commitments of social media platforms and Government's direction to the social media platforms to ensure cyber security of citizens.

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 THE REPLY TO RAJYA SABHA STARRED QUESTION NO. *78 FOR 09.02.2024 REGARDING CYBER SECURITY AND HACKING OF SOCIAL MEDIA

.....

(a) to (d): The policies of the Government are aimed at ensuring that internet in India is open, safe &trusted and accountable to all our users. Specifically, to deal with cyber security, Indian Computer Emergency Response Team ("CERT-In") is established under Section 70B of the Information Technology Act, 2000 ("IT Act"). CERT-In is the national nodal agency for responding to computer security incidents and has power to prescribe and implement reasonable security best practices. CERT-In may also call for information and give direction to the service providers, intermediaries (including social media intermediaries), data centres, body corporate and any other person for carrying out the provisions of functions under section 70B(4) of the IT Act.

CERT-In issued a direction on 28th April, 2022 mentioning types of cyber security incidents, including identity theft, spoofing and phishing attacks, to be mandatorily reported by service providers, intermediaries (including social media intermediaries), data centres, body corporate and Government organisations to CERT-In.

Additionally, CERT-In has also taken following measures to enhance awareness among organisations and users for safe usage of digital technologies and prevent cyber frauds:

a. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis. CERT-In has issued 72 advisories for organisations and users for data security, securing social media accounts and mitigating fraudulent activities.
b. On observing hacking of social media accounts, CERT-In coordinates incident response measures with affected entities and service providers.
c. CERT-In is working in coordination with service providers to track and disable phishing websites and facilitate investigation of fraudulent activities.
d. CERT-In has empanelled 177 security auditing organisations to support and audit implementation of Information Security Best Practices.
e. CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) 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.
f. CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats.
g. CERT-In is regularly carrying out various activities for development of cyber security capacities, skill building, awareness and citizen sensitization with respect to cyber-attacks 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 and citizens on focused topics of Cyber Security. A total of 10074 officials from Government, critical sectors, public and private sector have been trained in 26 training programs in the area of cyber security during 2023.

CERT-In regularly disseminates information and shares security tips on cyber safety and security through its official social media handles and websites. CERT-In organised various events and activities for citizens during Safer Internet Day on 7.2.2023 and Cyber Security Awareness Month in October 2023, by posting security tips using posters and videos on social media platforms and websites. CERT-In, in association with Centre for Development

of Advanced Computing, 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 the MyGov platform.

Rule 3(1)(b)(v) and (vi) of the IT Rules 2021 prohibits misinformation and patently false information on the Indian Internet or that impersonates another person. MeitY has, from time-to-time, issued advisories to the intermediaries for ensuring compliance with the prescribed due diligence and grievance reporting mechanism under the IT Rules, 2021.The failure to observe these rules will amount to non-compliance with the IT Rules, 2021 and result in the concerned intermediary automatically losing exemption from liability under section 79 of the IT Act. Government has also established Grievance Appellate Committees ("GAC") under the IT Rules, 2021 to allow users and victims to appeal online on www.gac.gov.in against decisions taken by the Grievance Officers of intermediaries.

As per information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), there were 6, 32 and 15 instances of hacking of social media accounts of users and organizations during the years 2021, 2022 and 2023 respectively. Further, 13,506 cases have been registered for cheating by personation by using computer resource (Section 66D IT Act) during year 2022.

Additionally, GAC has also received 205 appeals related of hacking/digital impersonation and 181 appeals have been disposed.

****