GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 260
TO BE ANSWERED ON: 03.02.2023

NATIONAL CYBER SECURITY POLICY

260. SHRI ELAMARAM KAREEM:
SHRI VIJAY PAL SINGH TOMAR:

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

(a) whether Government has introduced a new National Cyber Security Policy in light of recent cyber attacks on Government websites;
(b) if so, the details thereof along with the proposed timelines for its implementation and if not, the reasons therefor;
(c) whether Government has taken any steps to mitigate citizens' vulnerability to cyber attacks;
(d) if so, the details thereof:
(e) if not, the reasons therefor;
(f) whether Government intends to coordinate with other countries to develop a global legal framework on cyber terrorism; and
(g) if so, the details thereof?

ANSWER

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

(a) and (b): The National Security Council Secretariat (NSCS) has formulated a draft National Cyber Security Strategy, which holistically looks at addressing the issues of security of national cyberspace.

(c) to (e):The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users. Government is fully cognizant and aware of various cyber security threats, and has taken the following measures to mitigate citizens vulnerability to cyber-attacks:

(i) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis.
(ii) Security tips have been published for users to secure their desktops and mobile phones and to prevent phishing attacks.
(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 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 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 the MyGov platform.
(v) CERT-In and the Reserve Bank of India (RBI) jointly carry out a cyber security awareness campaign on 'beware and be aware of financial frauds' through the Digital India Platform.

(vi) 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.

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

(viii) RBI has organised Financial Literacy Week activities every year since 2016 to propagate financial education messages on various themes among members of the public across the country. The theme selected for the current year's Financial Literacy Week was "Go Digital, Go Secure", and the same was observed between February 14 to 18, 2022 with afocus on creating awareness about convenience of digital transactions, security of digital transactions and protection of customers. Banks were advised to disseminate the information and create awareness among their customers and the general public. Further, RBI ran a mass media campaign during the month of February 2022 to disseminate essential financial awareness messages to the general public.

(ix) RBI has issued various instructions in respect of security and risk mitigation measures related to electronic/digital transactions. These cover securing card transactions, securing payments through Internet banking / electronic payments, ATM transactions, prepaid payment instruments (PPIs), limiting customer liability on unauthorized electronic banking transactions, including PPIs issued by authorised non-banks, safeguarding against email spoofing attacks, etc.

(f) and (g): Pursuant to United Nations General Assembly resolution 75/282, adopted in May 2021, an Ad Hoc Committee to elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes was established with all member states of the United Nations. As a member of the Ad Hoc Committee, India has proposed criminalisation of cyber terrorism under the said Convention.

******