GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 3439
TO BE ANSWERED ON: 01.04.2022

NATIONAL CYBER SECURITY POLICY

3439. SHRI VISHAMBHAR PRASAD NISHAD:
DR. L. HANUMANTHAIAH:
SHRI RAM NATH THAKUR:
SHRI G.C. CHANDRASHEKHAR:
CH. SUKHRAM SINGH YADAV:
SMT. CHHAYA VERMA:
SMT. PHULO DEVI NETAM:

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

(a) whether Government is planning to introduce a new National Cyber Security Policy in light of recent cyber attacks which have jeopardised national security;

(b) if so, the details thereof, including the proposed timelines for implementation of the same 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 and if not, the reasons therefor;

(e) whether Government intends to coordinate with other countries to develop a global legal framework on cyber terrorism; and

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

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 2021 (NCSS2021) which holistically looks at addressing the issues of security of national cyberspace.

(c) and (d):The Government is committed to ensure that the Internet in India is Open, Safe & Trusted and Accountable for all 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.   Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies. CERT-In has issued 68 advisories for data security and mitigating fraudulent activities.

ii. Security tips are published by CERT-In for users to secure their desktops, mobile/smart phones and preventing phishing attacks.

iii. CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

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. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

vi. CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. Total 15 and 19 training programs were conducted covering 708 and 5169 participants during the year 2020 and 2021 respectively.

vii. Table Top Exercises are conducted by CERT-In regularly for senior management and Chief Information Security Officers (CISOs) to build awareness on threat landscape and best practices to counter cyber threats. 24 such table top exercises involving Government and public sector organisations for building awareness were conducted by CERT-In till February, 2022.

viii. CERT-In observed the Cyber Security Awareness Month during October 2021 through conduction of various events and activities for citizens as well as the technical cyber community in the country in collaboration with Industry and Academia. The activities including awareness campaigns, publishing videos & posters and cyber security quizzes are conducted thorough online training platforms and social media channels.

ix. CERT-In observed 'Safer Internet Day' on 8th February 2022 by carrying out cyber security awareness campaign through its official social media handles and websites.

x. Ministry of Electronics & Information Technology (MeitY) conducts programs 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 like "www.infosecawareness.in", and "www.csk.gov.in".

xi. Reserve Bank of India (RBI) has issued various instructions in respect of security and risk mitigation measures related to electronic/digital transactions which includes Securing Card Transactions, Securing Payments through Internet Banking / Electronic Payments, ATM Transactions, Prepaid Payment Instruments (PPIs), Limiting Customer Liability on Unauthorized Electronic Banking Transactions, Limiting Customer Liability in Unauthorized Electronic Banking Transactions in PPIs issued by Authorised Non-banks, , safeguarding against email spoofing attacks etc.

(e) and (f):There is no such information available with this Ministry.

****