GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2986
TO BE ANSWERED ON: 06.08.2025

CYBER AWARENESS CAMPS

2986. DR. C N MANJUNATH:

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

(a) whether the Government is providing any support to prevent online frauds, phishing attacks and financial scams affecting rural internet users including those in the Bengaluru Rural Parliamentary Constituency and if so, the details thereof;
(b) whether any cyber awareness camps or grievance redressal training has been conducted in partnership with the State police or the district administration, if so, the details thereof; and
(c) whether the Government proposes to launch a localised public awareness campaign on cyber hygiene in regional languages?

ANSWER
MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (c): The Government has taken several initiatives for prevention of cyber frauds and promotion of cyber security awareness, with the objective of ensuring an Open, Safe, Trusted, and Accountable Internet for all users. Government remains cognizant and aware of cyber threats and challenges. The Government has taken the following key initiatives:

- Ministry of Electronics and Information Technology (MeitY) is implementing a project on 'Information Security Education and Awareness (ISEA)' for generating human resources in the area of Information Security and creating general awareness on various aspects of cyber hygiene/cyber security among the masses. Under the awareness component, 24 awareness workshops have been organized in Bengaluru Rural constituency covering 1,644 participants. Multilingual Awareness material in the form of handbooks, short videos, posters, brochures, cartoon stories for children, advisories, etc. on various aspects of cyber hygiene & cyber security are disseminated through these awareness workshops and portals such as www.staysafeonline.in, and www.csk.gov.in.
- Ministry of Electronics and Information Technology observes the Cyber Security Awareness Month (NCSAM) during October every year, Safer Internet Day on 2nd Tuesday of February every year, Swachhta Pakhwada from 1st to 15th February of every year and Cyber Jagrookta Diwas (CJD) on 1st Wednesday of every month by organising various events and activities for citizens as well as the technical cyber community in India.
- CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities including social engineering, phishing and vishing campaigns and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis.
- CERT-In publishes Security tips for users to secure their desktops and mobile phones and to prevent phishing attacks.

- CERT-In is working in coordination with service providers, regulators and Law Enforcement Agencies (LEAs) to track and disable phishing websites and facilitate investigation of fraudulent activities.
- Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In, which extends the vision of Swachh Bharat to the cyber space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre and helps 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.
- CERT-In has organized awareness programs to educate the users on cyber security best practices and measures that can be taken against the phishing and cyber fraud campaigns.
- CERT-In is regularly sharing safety and security tips, awareness posters, info-graphics, booklets and videos through its official websites and social media handles such as Facebook, X(Twitter), Instagram, YouTube and LinkedIn for sensitizing internet users on cyber security attacks and frauds and prevention measures
- Ministry of Home Affairs (MHA) has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cybercrimes in the country, in a coordinated and comprehensive manner.
- To spread awareness on cybercrime, the MHA has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@CyberDost), Facebook (CyberDostI4C), Instagram (CyberDostI4C), Telegram(cyberdosti4c), SMS campaign, TV campaign, Radio campaign, School Campaign, advertisement in cinema halls, celebrity endorsement, IPL campaign, campaign during Kumbh Mela 2025, Mann Ki Baat, caller tune, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, newspaper advertisement on digital arrest scam, announcement in Delhi metros on digital arrest and other modus operandi of cyber criminals, use of social media influencers to create special posts on digital arrest, digital displays on railway stations and airports across, etc.
- I4C is collaboration with the Department of Telecommunications (DoT) has launched a caller tune campaign with effect from 19.12.2024 for raising awareness about cybercrime and promoting the Cybercrime Helpline Number 1930 & NCRP portal.
- Department of Telecommunications (DoT) through its AI and Facial Recognition powered Solution for Telecom SIM Subscriber Verification (ASTR) tool detects mobile connections that were acquired through forged documents.
- DoT has developed an online secure Digital Intelligence Platform (DIP) for sharing of information related to misuse of telecom resources among the stakeholders. DoT and Telecom Service Providers (TSPs) have devised a system called Centralised International Outroamer Register (CIOR) to identify and block incoming international spoofed calls displaying Indian mobile numbers.
- DoT has also evolved the ecosystem for curbing misuse of telecom resources through enhanced capacity building of human resource skill set and by development of AI & big data analytics tools, inter-alia, including ASTR, CIOR and DIP. Further, Sanchar Saathi, a citizen centric initiative has been launched which is accessible through web portal & mobile App and facilitates citizens to report suspected fraud communications, to know mobile connections in their name, to report lost/ stolen mobile handsets etc. In addition, Financial Fraud Risk Indicator (FRI) has been developed which is a risk-based metric that classifies a mobile number to have been associated with Medium, High, or Very Highrisk of financial fraud. FRI empowers stakeholders-especially banks, Non-Banking Financial Companies (NBFC), and Unified

Payments Interface (UPI) service providers to prioritize enforcement and take additional customer protection measures in case a mobile number has high risk.

- RBI and banks have also been taking up awareness campaigns through short SMS, radio campaign, publicity on prevention of 'cyber-crime' etc. RBI has further launched an Artificial Intelligence (AI) based tool 'Mule Hunter' for identification of money mule and advised the banks and financial institutions for its uses.
- Additionally, NPCI provides a fraud monitoring solution to all the banks to generate alerts and decline transactions by using AI/ ML based models.

*****