GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1458
TO BE ANSWERED ON: 31.07.2024.

PERSONAL DATA MINING AND PHISHING

1458. SHRI MANISH JAISWAL:

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

(a) whether the Government is aware of the increasing incidents of personal data mining and phishing activities being undertaken by anti-social elements;
(b) if so, the measures taken by the Government to curb these activities and protect citizens' personal data in the country including in Jharkhand;
(c) the steps taken to raise public awareness about the risks of data mining and phishing to avoid falling victim to such activities;
(d) whether any recent cases of data mining and phishing has been reported in Jharkhand;
(e) if so, the details thereof and the actions taken against the perpetrators; and
(f) the future plans proposed by the Government to enhance cyber-security measures and to prevent personal data mining and phishing activities across the country?

ANSWER

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

(a) to (f): The policies of the Government are aimed at ensuring an open, safe, trusted and accountable internet for all users. The Government has taken several measures to safeguard against threats and protect citizens' personal data across the country, including in Jharkhand. These measures include:

i. The Ministry of Home Affairs has set up the Indian Cyber Crime Coordination Centre(I4C) to deal with all types of cybercrime, including cybercrime against children, in a coordinated and comprehensive manner. A toll-free number 1930 has been made operational for citizens to get assistance in lodging online complaints in their own language. The Ministry of Home Affairs has also taken several steps to spread awareness on cybercrime, including through dissemination of messages on cybercrime through the Twitter handle @CyberDost and radio campaigns.

ii. The Indian Computer Emergency Response Team (CERT-In) works in coordination with service providers, regulators and law enforcement agencies to track and disable phishing websites and facilitate investigation of fraudulent activities.

iii. 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.

iv. CERT-In has issued an advisory to various Ministries outlining the measures to be taken for strengthening the cyber security by all entities that are processing the digital personal data or information including sensitive personal data or information.

v. CERT-In, through RBI, has advised all authorised entities and banks issuing pre-paid payment instruments (wallets) in the country to carry out special audit by CERT-In-empanelled auditors, close the non-compliances identified in the audit report and ensure implementation of security best practices.

vi. CERT-In has issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.

vii. 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.

viii. On observing hacking of social media accounts, CERT-In coordinates incident response measures with affected entities and service providers.

ix. CERT-In works in coordination with service providers to track and disable phishing websites and facilitate investigation of fraudulent activities.

x. CERT-In has empanelled 176 security auditing organisations to support and audit implementation of Information Security Best Practices.

xi. 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.

xii. CERT-In provides leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to and containing and mitigating cyber security incidents reported from the financial sector.

xiii. CERT-In regularly carries out various activities for development of cyber security capacities, skill building, awareness and citizen sensitization with respect to cyberattacks 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 on focused topics of Cyber Security.

xiv. 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.

xv. The Ministry of Electronics and Information Technology conducts programmes to generate information security awareness. Books, videos and online materials about information security are developed for general users, children and parents, and are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

****