GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1351
TO BE ANSWERED ON: 06.12.2024

INITIATIVES TO IMPROVE DETECTION OF AI-GENERATED PHISHING EMAILS

1351. SHRI S NIRANJAN REDDY:

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

(a) whether there are any specific initiatives to improve detection of AI-generated phishing emails that are personalized to bypass traditional security systems;
(b) whether Government is working with telecom and tech companies to ensure better security practices, especially in light of SIM swapping and other social engineering-based attacks;
(c) the steps being taken to foster better collaboration between Government and private sector in combating new cyber threats like AI-powered malware and IoT vulnerabilities; and
(d) the steps being taken to strengthen cloud security standards in the country, particularly to prevent incidents like cloud jacking and data breaches?

ANSWER

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

(a) to (d): The Government is fully cognizant and aware of various cyber security threat including AI-generated phishing emails, SIM swapping, social engineering-based attacks, cloud jacking. Government has taken following measures to strengthen cyber security posture of the country:

i. Ministry of Electronics and Information Technology (MeitY) conducts joint cyber security training programs in collaboration with Industry partners to upskill the cyber security workforce in Government, PSU and private organizations. Technical training sessions in the area of AI-powered cybersecurity threats and Internet of Things (IoT) security were conducted by Indian Computer Emergency Response Team (CERT-In) with experts from Industry to help the participants understand the latest threat landscape and best practices.
ii. Department of Telecommunication (DoT) and Telecom Service Providers (TSP's) have devised a system to identify and block incoming international spoofed calls displaying Indian Mobile numbers which appear to be originating within India. Such international spoofed calls were made by cyber-criminals in recent cases of fake digital arrests, FedEX scams, impersonation as government and police officials, disconnections of mobile numbers by DoT/Telecom Regulatory Authority of India officials, etc. Directions were issued to the TSPs for blocking of such incoming international spoofed calls.
iii. DoT has launched an online Digital Intelligence Platform (DIP) for sharing of information related to misuse of telecom resources and list of disconnected numbers with the stakeholders for prevention of cyber-crime and financial frauds.
iv. MeitY has funded various Research and Development projects in thrust areas of IoT security and Malware detection and mitigation to institutes and Academia.
v. CERT-In regularly coordinates with leading service providers and product vendors within and outside the country to obtain advance information on latest cyber threats and devise appropriate proactive and preventive measures.
vi. CERT-In has issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security,

Cloud Security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.

vii. CERT-In has issued Guidelines for Secure Application Design, Development, and Implementation & Operations in September 2023. CERT-In has also released the Software Bill of Materials (SBOM) guidelines for entities, particularly those in the public sector, government, essential services, organizations involved in software export and software services industry in October 2024. SBOM helps organizations know exactly what components are in their software or assets, making it easier to identify and fix vulnerabilities.

viii. CERT-In issued alerts and advisories regarding latest cyber threats/vulnerabilities including malicious attacks using Artificial Intelligence and countermeasures to protect computers, networks and data on an ongoing basis. In this context, an advisory on safety measures to be taken to minimize the adversarial threats arising from Artificial Intelligence (AI) based applications was published in May 2023.

ix. 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.

x. CERT-In has released awareness posters on AI and IoT security through its social media handles to educate the users on the best practices that can be followed to stay protected against AI and IoT related threats.

xi. On observing data breach / data leak incidents, CERT-In notifies the affected organisations along with remedial actions to be taken and coordinates incident response measures with affected organisations, service providers, respective sector regulators as well as Law Enforcement Agencies.

xii. MeitY has empanelled both domestic and global Cloud Service Providers (CSPs) that guarantee data residency within India and adhere to Indian legal frameworks. These CSPs undergo rigorous audits by the Standardisation Testing and Quality Certification Directorate and comply with international security standards (ISO) such as ISO 27001, ISO 27017, ISO 27018, and ISO 20000. Additionally, CSPs go through periodic security audits to ensure that they meet the ever-evolving security guidelines and compliances mandated by the Government of India.

****