GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3775
TO BE ANSWERED ON: 18.12.2024

IMPACT OF DIGITAL BANKING BUSINESS ON CYBER SECURITY

†3775. SMT. DELKAR KALABEN MOHANBHAI:

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

(a) whether there has been any impact on cyber security due to increase in digital banking business keeping in view the dynamic nature of information technology; and
(b) if so, the number of cyber threats cases including phishing, network scanning and probing, viruses and website hacking registered during each of the last three years?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY

(SHRI JITIN PRASADA)

(a): Government is fully cognizant and aware of cyber threats and challenges including those due to increase in digital banking business keeping in view the dynamic nature of information technology. Government is committed to ensure an open, safe, trusted and accountable internet for its users and has taken several key initiatives aimed at safeguarding digital banking business which, inter alia, includes:

i. The Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology Act, 2000.
ii. The Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) has been setup for responding to and containing and mitigating cyber security incidents reported from the financial sector under the umbrella and guidance of CERT-In.
iii. To ensure that the technology deployed by the authorized Payment System Operators (PSOs) to operate the payment system/sin a safe secure, sound, and efficient manner, Reserve Bank of India (RBI) had directed all PSOs to get Audit of their payment system done by CERT-In empanelled auditors on an annual basis and submit the report to RBI within two months of close of their respective financial year.
iv. CERT-In has empanelled 155 security auditing organisations to support and audit implementation of Information Security Best Practices.
v. CERT-In has periodically issued advisories on awareness of security aspects of digital payments, that aim at creating cyber security know-how by analysing the threat vectors and suggesting best practices for the specific area in cyber security for organisations and users.
vi. CERT-In and RBI jointly carry out a cyber security awareness campaign on ‘Beware and be aware of Financial Frauds’ through the Digital India Platform.
vii. RBI has issued a comprehensive circular on the Cyber Security Framework for banks, which sets standards and guidelines for implementing robust cyber security controls. This circular serves as a benchmark for banks to follow, covering various aspects of cyber security, including risk management, threat

detection, data protection, and incident response, ensuring a uniform and effective approach to safeguarding digital banking systems.

(b): As per information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), the total number of cyber security incidents in Indian banking sector, including phishing, Network Scanning & Probing, virus, and website hacking incidents during the last three years, are as follows:

Year	**Phishing Incidents**	**Network Scanning & Probing**	**Virus /Malware Incidents**	**Website Hacking Incidents**	**Cyber Security Incidents**
2021	215	86,585	9,203	18	1,22,764
2022	1,145	10,220	2,559	57	27,482
2023	401	12,330	1,185	39	23,158

****