GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF FINANCIAL SERVICES

LOK SABHA
UNSTARRED QUESTION No. 1120
TO BE ANSWERED ON MONDAY, JULY 26, 2021/SRAVANA 4,1943 (SAKA)

CYBER RISKS

1120. SHRI SHANMUGA SUNDARAM K.:

Will the Minister of FINANCE be pleased to state:

(a) whether the Government is aware of the increasing cyber risks involving unknown developments through the debit and credit cards, mobile banking, and online deals;

(b) if so, the details thereof along with the steps taken by the Government to prevent such kind of frauds where the hard-earned money of the people has suffered financial loss;

(c) whether the Government has instructed Insurance Regulatory Development Authority, the nodal agency for insurance, to submit any proposal to cover such risks;

(d) if so, the details thereof and if not, the reasons therefor; and

(e) whether the Government proposes to instruct all insurance providers of private and Government companies to incorporate cyber risk claim and if so, the details thereof?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF FINANCE

(DR. BHAGWAT KARAD)

(a) and (b): As per the information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), a total of 454, 472, 280 and 138 phishing incidents were observed during the years 2018, 2019, 2020 and 2021 (up to June) respectively. Further, the number of financial fraud incidents affecting automated teller machines(ATMs), cards, point of sale (PoS) systems and the Unified Payment Interface (UPI) have been reported as six, four, four and four during the years 2018, 2019, 2020 and 2021 (up to June) respectively.

'Police' and 'public order' are State subjects as per the Seventh Schedule to the Constitution. States are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cybercrime through their respective law enforcement agencies (LEAs) which take action as per law against offenders. The Central Government supplements the efforts of State Governments through advisories and financial assistance under various schemes for capacity building.

A number of measures have been taken to prevent cyber risks involving unknown developments through the debit and credit cards, mobile banking and online deals, details in respect of which are at Annex.

(c), (d) and (e): The Insurance Regulatory and Development Authority of India (IRDAI) has informed that it has issued guiding principles for product design and rating of general insurance products, which are equally applicable for products covering cyber risks. The Authority has further apprised that general insurers can design and rate the insurance products keeping in view the basic guiding principles and follow the laid down procedure for filing of product before its launch. A number of such products are already being offered by general insurers covering cyber risks such as cyber protect digital business and data protection insurance, cyber security insurance, cyber risk protector, Internet security insurance policy, electronic and computer crime insurance policy, information and network technology errors or omissions liability insurance, electronic and computer crime policy, errors and omission policy for software development / technology-based services, computer services and software developers professional liability, electronic and computer crime policy, etc.

Annex

REPLY TO UNSTARRED QUESTION No. 1120 FOR ANSWER ON 26.07.2021 IN LOK SABHA

Measures taken to prevent cyber risks involving unknown developments throughthe debit and credit cards, mobile banking and online deals

(a) An Indian Cyber Crime Coordination Centre (I4C) has been established to provide a framework and ecosystem for LEAs for dealing with cybercrimes in a comprehensive and coordinated manner.

(b) A National Cyber Crime Reporting Portal has been launched to enable the public to report cybercrime incidents and a Financial Cyber Fraud Reporting and Management System module has been launched for immediate reporting of financial frauds and to check such frauds.

(c) CERT-In is working in coordination with service providers, regulators and LEAs to track and disable phishing websites and facilitate investigation of fraudulent activities.

(d) CERT-In issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies.

(e) Security tips have been published for users to secure their Desktops, mobile/smart phones and preventing phishing attacks.

(f) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government.

(g) CERT-In conducts regular training programmes for Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber-attacks.

(h) CERT-In is providing the requisite leadership for the CSIRT-Fin (Computer Security Incident Response Team-Finance Sector) operations under its umbrella for responding to, containment and mitigation of cyber security incidents reported from the financial sector.

(i) For better customer protection, card networks have been advised by RBI to ensure the following, for all face-to-face / card present (CP) transactions performed using cards issued and acquired by banks in India:

a. Mandatory personal identification number (PIN) authentication for all transactions performed using credit, debit and prepaid cards – magnetic stripe or Europay, MasterCard and Visa(EMV)chip and PIN based. Issuer banks to accordingly comply with this requirement.
b. While processing an EMV chip and PIN card, fall back to magnetic stripe option will be enabled only if the transaction cannot be completed as a Chip based transaction, i.e. ab initio processing of EMV chip and PIN based cards, on the basis of magnetic stripe data

will not be done. Further, specific code for all such fall back transactions will be indicated in the transaction message sent to the issuer.

c. Acquirer banks will be liable for any loss to customers in case of failure to ensure adherence to contents of point (b) above.
d. RBI has asked banks to put in place a system of online alerts for all types of transactions irrespective of the amount, involving usage of cards at various channels.

(j) RBI has instructed banks to frame rules based on the transaction pattern of the usage of cards by the customers, in coordination with the authorised card payment networks for arresting fraud. Banks are also instructed to build in a system of call referral in co-ordination with the card payment networks based on these rules. Further, all new debit and credit cards to be issued only for domestic usage unless international use is specifically sought by the customer.

(k) All new cards issued(both debit and credit and domestic as well as international) by banks are EMV chip and PIN based cards.

(l) RBI has issued instructions to limit the liability of customers, in case of unauthorised electronic transactions. Additionally, a customer may lodge his / her grievance under the Banking Ombudsman (BO) Scheme / Ombudsman Scheme for Digital Transactions of RBI.