GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO.1511
TO BE ANSWERED ON: 19.12.2018

RISK OF CYBER FRAUD

1511. SHRI OM PRAKASH YADAV:

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

(a) whether the Government has formulated any plan to check the risks of Cyber fraud in the economy and if so, the details thereof;
(b) the details of number of complaints received related to Cyber security; and
(c) the details of the complaints received from the State of Bihar in this regard ?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI S.S. AHLUWALIA)

(a): Government has taken several measures to check the cyber fraud in the economy. These, *inter alia*, include :

(i) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis to ensure safe usage of digital technologies. Regarding securing digital payments, 28 advisories have been issued for users and institutions.

(ii) All authorised entities/ banks issuing PPIs in the country have been advised by CERT-In through Reserve bank of India to carry out special audit by empanelled auditors of CERT-In on a priority basis and to take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices.

(iii) All the new government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is to be conducted on a regular basis after hosting.

(iv) Government has empanelled 76 security auditing organisations to support and audit implementation of Information Security Best Practices.

(v) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

(vi) All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.

(vii) Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

(viii) Cyber security mock drills and exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 38such exercises have so far been conducted by CERT-In where organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS etc. participated. 3 exercises were conducted in coordination with Reserve bank of India in November 2018 for senior management and Chief Information Security Officers (CISOs) of banks.

(ix) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. 22 trainings covering 746 participants conducted in the year 2018 (till November).

(x) Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

(b): As per information reported to Indian Computer Emergency response Team (CERT-In), a total of 3, 14 and 6 financial fraud incidents affecting ATMs, cards, Point of sale (PoS) systems and Unified Payment Interface (UPI) have been reported during the year 2016, 2017 and 2018 (upto November) respectively. Further, Reserve Bank of India (RBI) has registered a total of 1191, 1372, 2059 and 921 cases of frauds involving ATM/Debit Cards, Credit Cards and Internet Banking Frauds reported (amount involved Rs 1 lakh and above) during the year 2015-16, 2016-17, 2017-18 and 2018-19 (Upto 30 Sept 2018) respectively.

(c): "Crime", "Police" and "Public order" are State subject and data pertaining to complaints of cyber fraud at States are not maintained by MeitY.

****