GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2495
TO BE ANSWERED ON: 16.03.2018

CYBER CRISIS MANAGEMENT PLAN FOR CURBING CYBER FRAUD

2495. SHRI BHUBANESWAR KALITA:

Will the Minister of Electronics & Information Technology be pleased to state:-
  (a)   whether it is a fact that several cases of internet frauds have come to the notice of Government;
  (b)   if so, the details thereof during the last three years;
  (c)   whether it is also a fact that the Government has drawn a Cyber Crisis Management Plan to check cyber frauds in the country; and
  (d)   if so, the details thereof along with the achievements of the plan, so far?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI K. J. ALPHONS))

(a) and (b): As per incidents reported to the Indian Computer Emergency Response Team (CERT-In), a total of 71, 63 and 77 phishing incidents affecting customers of financial organisations were reported in 2015, 2016 and 2017 respectively. In addition 14 incidents affecting ATMs, cards, Point of Sales (POS) systems and Unified Payment Interface (UPI) have been reported during the year 2017.

(c) and (d):   (i) Ministry of Electronics & IT (MeitY) has formulated Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber terrorism for implementation by all key Ministries/Departments of Central Government, State Governments and Union Territories.

(ii)   The Indian Computer Emergency Response Team (CERT-In) along with Reserve Bank of India is enabling implementation of CCMP in banks by means of cyber security framework, minimum baseline resiliency requirements and best practices/guidelines.

(iii)   Regular workshops are conducted for Ministries/Departments, States & UTs and critical organizations to sensitize them about the cyber security threat landscape and enabling them to prepare and implement the CCMP. Till date 54 such workshops have been conducted.

(iv)   CERT-In is providing support to Central Government Ministries/Departments and State Governments in preparing their CCMP document. Till date, CERT-In has enabled 19 Central Ministries/Departments to develop their own CCMP and interacted with 21 Central Ministries/Departments for CCMP development. 11 states/UTs have been enabled to develop the CCMP and interaction is in process with 14 other states/UTs.

(v)   In order to assess effectiveness of CCMP implementation, Cyber security exercises are being conducted regularly by CERT-In for Government and critical sectors. Till date, CERT-In has conducted 25 such Exercises with the participation of   organizations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT / ITeS etc.

*****