GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2960
TO BE ANSWERED ON: 11.08.2017

SURGE IN MOBILE FRAUDS

2960 SHRI. SANJAY RAUT:

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

(a) whether it is a fact that mobile frauds is an area of great concern for companies as 40-45 per cent of financial transactions are done via mobile devices and this threat is expected to grow to 60-65 per cent, if so, the details in this regard and Government's response thereto; and
(b) the details of the steps taken or proposed to be taken by Government for implementing robust cyber security law to prevent the surge in mobile frauds?

ANSWER
MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI P.P. CHAUDHARY)

(a): There have been some media reports based on the joint study by 'The Associated Chambers of Commerce and Industry of India' (ASSOCHAM) and research firm 'Ernst & Young' (EY), titled "Strategic National Measures to Combat Cybercrime" indicating mobile frauds is an area of great concern for companies, as 40-45 per cent of financial transactions are done via mobile devices and this threat is expected to grow to 60-65 per cent.

(b): Government has taken a number of legal, technical and administrative measures for addressing cyber security. These include the following, namely:-

(i) Enactment of the Information Technology (IT) Act, 2000 which has adequate provisions for dealing with prevalent cyber crimes including frauds.
(ii) The Indian Computer Emergency Response Team (CERT-In) created under section 70B of IT Act, 2000, issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.certin.org.in).
(iii) Government has initiated setting up of National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. Phase-I of NCCC has been made operational.
(iv) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of Cyber Crime cases.
(v) Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of law enforcement personnel and Judiciary in these States.
(vi) A number of Cyber forensics tools for collection, analysis and presentation of the digital evidence have been developed indigenously and such tools are being used by law enforcement Agencies.
(vii) Reserve Bank of India (RBI) issues Circulars/advisories to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks. RBI also issues advisories relating to fictitious offers of funds transfer, remittance towards participation in lottery, money circulation schemes and other fictitious offers of cheap funds.

(viii) All banks have been mandated to report cyber security incidents to CERT-In expeditiously.

(ix) All authorised entities/banks issuing Prepaid Payment Instruments (PPIs) in the country have been advised to carry out audit by the empanelled auditors of CERT-In on a priority basis and take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices. Government has empanelled 54 security auditing organisations to support and audit implementation of Information Security Best Practices.

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

****