

**GOVERNMENT OF INDIA
HOME AFFAIRS
LOK SABHA**

UNSTARRED QUESTION NO:3846

ANSWERED ON:04.09.2012

INTERNET FRAUD CASES

Bundela Shri Jeetendra Singh;Meghwal Shri Arjun Ram ;Naik Shri Shripad Yesso;Panda Shri Prabodh;Patel Shri Devji;Wankhede Shri Subhash Bapurao

Will the Minister of HOME AFFAIRS be pleased to state:

- (a) whether cases of cyber crimes and frauds on internet are on the rise in the country;
- (b) if so, the details of such cases registered during each of the last three years and the current year, State-wise;
- (c) the conviction rate achieved and the number of cases pending in this regard;
- (d) whether there is a lack of advanced technology and trained manpower with the security agencies to deal with the said crimes effectively; and
- (e) if so, the details thereof and the remedial measures taken by the Government in this regard along with the other steps to check the said crimes?

Answer

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS (SHRI JITENDRA SINGH)

(a) & (b): The States /UTs-wise details of cases registered and person arrested under IT Act and Cyber related cases of criminal breach of trust/fraud reported during 2009-2011 are attached at Annexure-I.

(c): The data on conviction under IT Act is not maintained.

(d) to (e): The remedial measures taken by the Government of India are attached at Annexure-II The remedial measures taken by the Government of India are as under:-

(i) The Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 has been enforced on 27.10.2009. The Act provides legal framework to address various types of cyber crimes and prescribes punishment also for such crimes.

(ii) Indian Computer Emergency Response Team (CERT-In) issues alerts, advisories and guidelines regarding cyber security threats and measures to be taken to prevent cyber incidents and enhance security of Information Technology systems.

(iii) A major programme has been initiated on development of cyber forensics specifically cyber forensic tools, setting up of infrastructure for investigation and training of the users, particularly police and judicial officers in use of this tool to collect and analyse the digital evidence and present them in Court.

(iv) Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training of Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.

(v) Cyber forensic training lab has been set up at Training Academy of Central Bureau of Investigation (CBI) to impart basic and advanced training in Cyber Forensics and Investigation of Cyber Crimes to Police Officers associated with CBI. In addition, 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.

(vi) In collaboration with Data Security Council of India (DSCI), NASSCOM. Cyber Forensic Labs have been set up at Mumbai, Bangluru, Pune and Kolkata. DSCI has organized 112 training programmes on Cyber Crime Investigation and awareness and a total of 3680 Police officials, judiciary and Public prosecutors have been trained through these programmes. National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.

(vii) Government has formulated a set of investigation manuals with procedures for Search, Seizure Analysis and Presentation of digital evidence in courts. The manuals have been circulated to Law Enforcement Agencies in all States. Ministry of Home Affairs has issued an Advisory to the State Governments and Union Territory Administrations on Cyber Crime. State Governments have been

advised to build adequate technical capacity in handling cyber crime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of cyber crimes.