GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:575
ANSWERED ON:14.07.2014
CHECK ON INCIDENTS OF CYBER CRIME
Nayak Shri B.V.;Singh Shri Sunil Kumar

Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

-

(a) whether there has been a continuous rise in the number of cyber crimes in the country;

(b) if so, the details thereof and the number of such incidents which took place during the last three years and the current year;

(c) whether the Government has adopted any strategy to check such cyber crimes and if so, the details thereof; and

(d) the steps taken/being taken by the Government in this regard?

Answer

MINISTER FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI RAVI SHANKAR PRASAD)

(a) and (b): With the increase in the proliferation of Information Technology and related services there is a rise in number of cyber crime and cyber security incidents. The trend in increase in cyber incidents is similar to that worldwide. As per the cyber crime data maintained by National Crime Records Bureau, a total of 1791, 2876 and 4356 Cyber Crime cases were registered under Information Technology Act during the year 2011, 2012 and 2013 respectively, thereby showing an increasing trend. A total of 422, 601 and 1337 cases were registered under Cyber Crime related Sections of Indian Penal Code (IPC) during the year 2011, 2012 and 2013 respectively. In addition, a total no. of 13301, 22060, 71780 and 62189 security incidents including phishing, scanning, spam, malicious code, website intrusions etc. were reported to the Indian Computer Emergency Response Team (CERT-In) during the year 2011, 2012, 2013 and 2014 (till May) respectively.

(c): The Government has taken several measures and policy decisions to check cyber crimes/ incidents in the country. The details are:

i) In order to address the issues of cyber security in a holistic manner, the Government has released the "National Cyber Security Policy-2013" on 02.07.2013, for public use and implementation by all relevant stakeholders. This policy aims at facilitating creation of secure computing environment and enabling adequate trust and confidence in electronic transactions and also guiding stakeholders' actions for protection of cyber space.

ii) 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 prevalent cyber crimes and security breaches of information technology infrastructure.

iii) 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. Action also has been taken to set up a National Centre of Excellence exclusively devoted to render Cyber Forensic services and to act as National Research and Training Centre on Cyber Forensics

iv) A major programme has been initiated on development of cyber forensics 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 Courts.

v) 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.

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

vii) Cyber forensics 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 for training of Law Enforcement and Judiciary in these States.

viii) In collaboration with Data Security Council of India (DSCI), NASSCOM. Cyber Forensic Labs have been set up at Mumbai, Bengaluru, Pune and Kolkata for awareness creation and training programmes on Cyber Crime investigation. 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.

ix) Reserve Bank of India (RBI) has issued a Circular to all Commercial Banks on phishing attacks and preventive / detective measures to tackle phishing attacks. RBI has also advised Banks to leverage technology to support Business processes and implement all stipulations outlined by RBI from time to time. Banks are also advised to ensure implementation of basic Organizational framework and put in place policy and procedure to prevent financial frauds through Internet. RBI has mandated the banks to put in place additional authentication/validation for all on-line transactions based on information available on the credit/debit/prepaid cards. RBI has also suggested that chip based Cards may be used as an alternative to magnetic strip cards based as a measure to counter the risks of skimming of ATM cards.

x) Reserve Bank of India (RBI) had issued Circular dated 1st July, 2011 on Credit Card operations by Banks. The Banks have been advised to set up internal control system to combat frauds and to take proactive fraud control and enforcement measures. The Banks are required to fulfill 'Know Your Customer (KYC)' requirements. RBI has also issued advisories relating to fictitious offers of funds transfer, remittance towards participation in lottery, money circulation schemes and other fictitious offers of cheap funds. RBI also has cautioned public through Notification against fictitious offers of remitting cheap funds from aboard.

xi) Information Sharing and Analysis Centres (ISACs) for financial services has been set up at Institute for Development and Research in Banking Technology (IDRBT). Such a centre exchange information on cyber incidents in financial sector and advises them for appropriate mitigation. Action has been initiated to set up similar ISACs in power and petroleum sector.

xii) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing the websites, which are available on its website (www.cert-in.org.in). CERT-In also conducts regular training programme to make the system administrators aware about secure hosting of the websites and mitigating cyber attacks.

xiii) The Government is encouraging development of indigenous technology by carrying out Research and Development (R&D) in the area of cyber security.

xiv) A website (secureyourpc.in) for children, home users and elderly is available for safeguarding their computer systems and learning the risks on internet.

(d): The area of cyber crime/ incidents is very technology intensive and new techniques in the cyber crime emerge with the technological innovations. The Government takes necessary steps to review the policy and measures as deemed necessary to check the cyber crimes.