GOVERNMENT OF INDIA
ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:127
ANSWERED ON:16.11.2016
Cyber Crime
Bhaleram Shri Dharambir;Chaudhury Shri Jitendra;Hegde Shri Anant Kumar Dattatreya;Singh Shri Uday Pratap

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

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

(a) whether the Government has taken note of cybercrime especially on social media increasing all over the country;
(b) if so, the details thereof along with percentage increase in cyber crimes in the last three years;
(c) the action taken by the Government in this regard along with the steps taken to protect women from increasing harassment on social sites?

Answer

(a) and (b): With the proliferation of Information Technology and related services there is a rise in instances of cyber crimes including that on social media in the country like elsewhere in the world. As per the data maintained by NCRB, A total of 5693, 9622 and 11592 cyber crime cases were registered during the years 2013, 2014 and 2015 respectively, showing a rise of 69% during 2013 to 2014 and 20% during 2014 to 2015. Further, CBI has registered 11, 20 and 25 cases in the year 2013, 2014 and 2015 respectively related to cyber crimes.

(c): Government has taken various steps in the form of legal framework, emergency response, awareness, training, legal framework and implementation of best practices to prevent occurrence of cyber breaches and cyber crime threats. Such steps include:

i) The Information Technology Act, 2000 provides a comprehensive legal framework to address the issues connected with cyber crime, cyber attacks and security breaches of information technology infrastructure.
ii) Government is implementing a Framework for Enhancing Cyber Security, with a multi-layered approach for ensuring defence-in-depth and clear demarcation of responsibilities among the stakeholder organizations in the country.
iii) Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the Information Technology Act, 2000 for protection of Critical Information Infrastructure in the country.
iv) 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 IT infrastructure, which are available on its website (www.certin.org.in). In order to detect variety of threats and imminent cyber attacks from outside the country, periodic scanning of cyber space is carried out.
v) 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.

vi) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.
vii) 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.
viii) CERT-In, Ministry of Electronics & Information Technology is setting up a Botnet Cleaning and Malware Analysis centre for detection of computer systems infected by malware and to notify, enable cleaning and securing systems of end users to prevent further malware infections.
ix) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of Cyber Crime cases.
x) 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.
xi) Industry associations such as Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs, set up in certain States, have taken up tasks of awareness creation and training programmes on Cyber Crime investigation. Academia like 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.
xii) A number of Cyber forensics tools for collection, analysis, presentation of the digital evidence have been developed indigenously and such tools are being used by Law Enforcement Agencies.
xiii) 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.
xiv) 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.
xv) 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.

xvi) The Information Technology Act, 2000 together with the Indian Penal Code (IPC) and Protection of Children from Sexual Offences Act (POCSO) provides legal framework for dealing with online obscene material including child sexual abuse.

xvii) Government has notified the Information Technology (Intermediary Guidelines) Rules 2011 under Section 79 of the Information Technology Act. These rules require that the Intermediaries, including national and international social networking sites and matrimonial sites, shall observe due diligence while discharging their duties and shall inform the users of Computer resources not to host, display, upload, modify, publish, transmit, update or share any information that is harmful, objectionable, affect minors and unlawful in any way. The said rules also require the intermediaries to appoint Grievance Officers to address the grievances received from users and affected individuals / organizations as and when received by them.

xviii) Ministry of Electronics and Information Technology has issued an Advisory for Online Matrimonial Websites service providers. The Advisory aims to protect women from fraudsters after getting introduced through fake profiles on matrimonial portal. Through the advisory the Online Matrimonial Websites have been advised to adopt a framework which includes verification of users, privacy policy, user agreement (Terms and Conditions) etc.

****