GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

STARRED QUESTION NO:233
ANSWERED ON:05.08.2015
Cyber Frauds
Chavan Shri Harishchandra Deoram

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

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

(a) whether the cases of cyber crime and frauds have been reported by various networking websites including electronic mail account websites during the last three years and the current year and if so, the details thereof;

(b) whether there are large number of fake accounts on various e-mail and social networking sites which are being used for committing cyber fraud / crime;

(c) if so, the details thereof along with the action taken by the Government against the concerned websites and individuals; and

(d) the action formulated to safeguard the interest of the users of Digital India against leakage of sensitive data through cyber attacks?

Answer

ANSWER

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

(a) and (d): A Statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO LOK SABHA STARRED
QUESTION NO *233 FOR 05-08-2015 REGARDING CYBER FRAUDS
â€¦â€¦â€¦

(a): As per the Cyber Crime data maintained by National Crime Records Bureau (NCRB), a total of 2876, 4356 and 7201 Cyber Crime cases were registered under Information Technology Act, 2000 during 2012, 2013 and 2014 respectively. A total of 601, 1337 and 2695 cyber crime cases were registered under Cyber Crime related sections of Indian Penal Code (IPC) during 2012, 2013 and 2014 respectively. 784 cases of identity theft and 428 cases of cheating by personation by using computer resource were registered in 2014.

(b) and (c): Any user on the Internet may create an email account with any name including fake names on the web portal of free email service providers like Gmail, Hotmail, Yahoo etc. and further may register on a networking / matrimonial websites with fake credentials. No background information check is usually performed by the free email service providers or social networking sites, which leads to creation of fake accounts by miscreants for committing Crimes / frauds. Most of the free email service providers and social networking sites are located abroad. The servers of these social networking sites are also located abroad.

A total number of 11, 14, 19 and 11 incidents of fake email accounts and a total number of 37, 37, 57 and 16 fake Social Networking profiles were reported to Indian Computer Emergency Response Team (CERT-In) during 2012, 2013, 2014 and 2015 (till June) respectively. CERT-In contacted respective Social Networking and Email Service Providers for disabling of fake accounts and for getting user access details of these fake accounts / profiles. In most of the cases, such fake accounts were successfully disabled in association with Social Networking sites and Email Service Providers having offices in India. However, success rate is low in disabling accounts and getting information from Service Providers having offices abroad.

(d): In tune with the dynamic nature of Information Technology, continuous efforts are required to be made to prevent and recover from cyber attacks. Government of India under the flagship programme of "Digital India" has a vision of providing digital infrastructure as a utility to every citizen in safe and secure cyberspace. Security of cyberspace is identified as one of the key components envisaged for the success of 'Digital India' programme. As part of this, key initiatives of the Government are:

(i) Digital Locker system has been implemented, which envisages provision of private space on a public cloud to each citizen where he/she can keep public records and can even exchange it for availing various services. Digital Locker implements secure authentication mechanism to prevent leakage of data through Cyber attacks. Further, eSign framework enables citizens to digitally sign a document online using Aadhaar authentication.
(ii) National Cyber Coordination Centre (NCCC) to generate near real time macroscopic views of the cyber security breaches and cyber security threats in the country. The centre will provide a structured mechanism and facilitate coordination of efforts of all

stakeholder agencies in the country. NCCC will be a multi stakeholder body and will be implemented by Indian Computer Emergency Response Team (CERT-In) at Department of Electronics and Information Technology (DeitY).

(iii) "Botnet Cleaning and Malware Analysis Centre" to provide for detection of malware infected computer systems and enable cleaning and securing the systems of end-users to prevent further malware infections. The project is being implemented in coordination and collaboration with Internet Service Providers (ISPs) and Industry. This would help in enhancing the security of computer systems across the country.

(iv) Government has also taken steps to put in place a Framework for Enhancing Cyber Security, which envisages a multi-layered approach for ensuring defence-in-depth with clear demarcation of responsibilities among the stakeholder organizations in the country.

(v) 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.

(vi) 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.

****