GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:314
ANSWERED ON:14.03.2012
CYBER CRIMES/FINANCIAL FRAUDS
Agarwal Shri Jai Prakash;Bajwa Shri Partap Singh;Mahendrasinh Shri Chauhan ;Panda Shri Baijayant;Pradhan Shri Nityananda;Premajibhai Dr. Solanki Kiritbhai;Rajendran Shri C.;Singh Shri Ravneet

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

(a) whether the cases of cyber attack on the Government websites including the website of Bharat Sanchar Nigam Limited have been reported recently;

(b) if so, the details thereof alongwith the names of the Government agencies whose websites have been hacked; Â¦.

(c) whether the cases of financial fraud through internet and mobile phones have been on rise in the country;

(d) if so, the details of cases reported during the last three years and the current year till date and the total amount involved therein, State-wise and year-wise; and

(e) the action taken/likely to be taken by the Government for prevention of cyber attacks and financial frauds through internet and mobile phones in the country?

Answer

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI SACHIN PILOT)

(a) and (b): The website of Bharat Sanchar Nigam Limited (www.bsnl.co.in) was hacked on 4th December, 2011 by the `H4tr!ck` hacker group. In addition, during the period December, 2011 to February, 2012 a total no. of 112 Government websites were hacked. These hacked websites belonged to the agencies in the Government of Andhra Pradesh, Madhya Pradesh, Rajasthan, Tamil Nadu, Maharashtra, Gujarat, Kerala, Orissa, Uttar Pradesh, Sikkim, Manipur: Agencies of Ministry of Finance, Health, Planning Commission and Human Resource Development.

(c) and (d): According to Reserve Bank of India (RBI) the numbers of internet frauds involving Rs 1 lakh and above have declined over the last three years from 269 cases in the calendar year 2009 to 125 cases in the calendar year 2011. However, after taking into account the internet frauds wherein the amount involved in individual cases is less than Rs. 1.00 lakh, the total number of internet frauds were 864 numbers involving Rs. 824.05 lakh, 2232 cases involving Rs 1234.94 lakh and 1798 cases involving Rs.787.39 lakh for the calendar year 2009, 2010 and 2011 respectively. The state wise and year wise data is available only in respect of those internet fraud cases where amount involved in individual case is Rs. 1.00 lakh or more. The details are as per annexure -I.

Central Bureau of Investigation has also registered cases pertaining to Financial frauds under the provisions of Information Technology Act, 2000 along with other acts. These are:-

Year	No. of cases
2009	2
2010	2
2011	3
2012(upto 29/02/2012)	2

The details are at Annexure-II.

(e): The Government has taken several steps for prevention of Cyber attacks and financial frauds through internet and mobile phones in the country. These are:

i. Legal Framework in the form of Information Technology Act, 2000. The Act provides legal framework to address the issues connected with phishing, hacking and security breaches of information technology infrastructure.

ii. Reserve Bank of India (RBI) has issued a circular to all commercial banks on phishing attacks and minimum set of preventive /detective measures to tackle phishing attacks.

iii. Reserve Bank of India (RBI) has 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 frame work and put in place, policy and procedure to prevent financial frauds through Internet. These guidelines are expected to enhance safety,

security, efficiency in banking processes leading to benefits for the bank and the customers.

iv. 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 pro-active fraud control and enforcement measures. The banks are required to fulfill `Know Your Customer (KYC)` requirements.

v. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis.

vi. CERT-In is providing incident response service for handling of phishing attacks affecting the banks in the country.