

**GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA**

UNSTARRED QUESTION NO:1969
ANSWERED ON:05.12.2012
INDIVIDUAL DATA PRIVACY
Rai Shri Prem Das;Tagore Shri Manicka

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

- (a) whether there has been significant increase in the fraudulent practice of inducing individuals to reveal personal information such as password, credit card details etc. through phishing attacks;
- (b) if so, the details thereof;
- (c) the steps taken by the Computer Emergency Response Team India (CERT-In) to curb this practice;
- (d) whether the Government propose to introduce relevant law/rules for unauthorized sharing of personal information and its disclosure and made it a cognizable offence; and
- (e) if so, the details thereof and the action taken by the Government in this regard so far?

Answer

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI MILIND DEORA)

(a) and (b): There have been increase in the incidents involving revealing of personal information such as passwords, credit card details etc. through phishing attacks in the past few years. According to Reserve Bank of India and Indian Computer Emergency Response Team (CERT-In) a total number of 1618, 2124 and 2853 phishing incidents were reported to them in the year 2010, 2011 and 2012 (till October) respectively.

(c): CERT-In is taken several steps to handle phishing cases which include:

i. Providing incident response service on 24x7 basis for handling of phishing attacks affecting the banks and other institutions in the country.

ii. Regular training programmes are conducted by CERT-In for the Banks and other institutions for enhancing awareness on mitigating the phishing attacks.

iii. CERT-In issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis for safeguarding computer systems from phishing attempts and unauthorized information disclosure. CERT-In is working very closely with the Reserve Bank of India and other Banks in the country towards taking immediate steps to curb phishing attacks, adopting multi-factor authentication, technological solutions for early detection and take-down of phishing attempts and creating user awareness to deal with the phishing attacks.

(d) and (e): Section 43A of the Information Technology Act, 2000 and Rules notified there under establishes a legal framework for data privacy protection in India. It mandates body corporates to implement reasonable security practices, framework for mode of collection, transfer and disclosure of sensitive personal data or information. Further, section 66C and 72A of the Information Technology Act, 2000 provides for punishment and penalty for identity theft and breach of confidentiality & privacy respectively.