

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

UNSTARRED QUESTION NO:4313

ANSWERED ON:19.12.2012

DEVELOPMENT OF SECURITY SOFTWARE

Deo Shri Kalikesh Narayan Singh;Pradhan Shri Nityananda;Reddy Shri Magunta Srinivasulu

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

- (a) whether the Government has developed any indigenous security software for prevention of hacking and controlling internet fraud and cheating;
- (b) if so, the details thereof along with its efficacy in prevention of cyber crime and cheating and if not, the efforts being made by the Government in this regard;
- (c) the measures taken by the Government to conduct awareness programme for internet users of potential hacking and cyber cheats;
- (d) whether any software has also been developed to detect the fake currency in the country; and
- (e) if so, the details thereof?

**Answer**

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

(a) and (b): Cyber Security is dynamic that changes with the threat environment and advanced technology developments. To prevent cyber security incidents of hacking and Internet frauds, a comprehensive security strategy needs to be adopted by individual organizations. The holistic approach should include a combination of people, processes and technology. Further organization need to deploy different technology based solutions for protection of information, systems and networks. In order to prevent hacking and enhancing cyber security of information technology infrastructure, Government has taken a series of legal, policy and technology development measures. Due to the dynamic nature of threat landscape and continuous technology changes, these actions need to be continued, refined and strengthened on an ongoing basis.

Government has been promoting indigenous development of security solutions at academic and research organizations in identified thrust areas of cyber security. The initiative is a continuing process. As a result of these efforts, indigenous Cyber Forensics tools, intrusion prevention system, malware detection and prevention systems, tools for securing devices and web based tools for enterprise security management have been developed.

The tools developed by the government efforts are used by the Government agencies, industry and Academia. Based on the feedback received from users, changing threat landscape and technological advancements, these tools / solutions are continuously upgraded.

(c): Government has initiated a major programme to disseminate awareness on threats arising out of the new technologies on a mass scale to the Internet users focusing on threats from Personal Computers, USB Device, Mobile and Smart Phones, Modems, Credit Cards etc. In addition, Department has implemented Information Security Education and Awareness (ISEA) programme to create nationwide awareness on Cyber Security. Also various skill based training programmes have been organized to Information Security Officers and other relevant stakeholders from various Government organizations and Enterprises. In addition, basic and advanced level training programmes are organized regularly on Cyber Forensics to Law Enforcement Agencies across the country to train them on seizure, acquisition, analysis and presentation of digital evidence. In this regard, Cyber Forensics Training Labs, have been set up in various states to assist Law Enforcement and Judiciary. A web portal for Internet users has also been set up by Indian Computer Emergency Response Team (CERT-In) for disseminating Cyber Security awareness. CERT-In also issues security alerts and advisories on latest threats and vulnerabilities for securing the systems from hacking.

(d) and (e): Commercial solutions to detect certain features of fake currency are available and being used. Such solutions, however, are customised with respect to currencies. The technology is also upgraded regularly.