GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3785
TO BE ANSWERED ON: 11.12.2019

HACKING OF E-SERVICES

3785. MS. MIMI CHAKRABORTY :

Will the Minister of Electronics & Information Technology be pleased to state:-

(a) whether the Government has failed to check hacking of e-services in the country and if so, the details thereof and the reaction of the Government thereto along with the reasons therefor;

(b) whether hackers are now able to compromise the safety and security of Whatsapp services and if so, the details thereof; and

(c) the action taken/being taken along with the details of technology/software developed, if any, by the Government to deal with such issue?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a): Cyber space is a complex environment of people, software, hardware and services on the Internet. With a borderless cyberspace coupled with the possibility of instant communication and anonymity, the potential for misuse of cyberspace including hacking of websites and services is a global issue. As per information provided by National Informatics Centre (NIC), 12 websites hosted on its network (NICNET) have been defaced this year till-date**.**

(b): Government had been informed by WhatsApp of a vulnerability affecting some WhatsApp mobile users' devices through a spyware namely Pegasus. According to WhatsApp, this spyware was developed by an Israel based company NSO Group and that it had developed and used Pegasus spyware to attempt to reach mobile phones.

(c): NIC provides IT/E-Governance related services to Government departments and protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies that are put in place.

NIC has deployed state-of-the-art security solutions including firewalls, intrusion prevention systems, anti-virus solution for safe-guarding of hosted websites. Additionally, periodic security audits of resources are performed followed by subsequent hardenings. These are complemented by round-the-clock monitoring of security events. At NIC, Cyber Security is a continuous process and the protection elements are updated on a regular basis. A 24x7 security monitoring centre is in place at NIC, for detecting and responding to security

incidents and countering to exigencies with remedial measures, including NIC-CERT and Centres of Excellence for Application Security.

****