GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO.1601
TO BE ANSWERED ON: 19.12.2018

DATA HACKING

1601. SHRI DIBYENDU ADHIKARI:

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

(a) whether it is a fact that data hacking is a regular feature in Indian IT system;
(b) if so, whether in spite of Government security support, over 150 Government portals have been hacked since 2017;
(c) whether it is also a fact that siphoning of bank account has become common phenomena and has increased over 3% in last six months;
(d) if so, the details of year-wise complaints received and action taken thereon since 2016 till date; and
(e) the plan of action of the Government to stop data breaches or hacking in future?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI S.S. AHLUWALIA)

(a) and (b): With the innovation of technology and rise in usage of cyber space for businesses, the cyber attacks are also on the rise worldwide as well as in the country. Defacement / hacking attempts do occur on Internet facing servers by malicious actors like elsewhere in the world. As per information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), 172 and 105 Government websites, which includes 74 and 31 websites hosted on NICNET managed by National Informatics Centre (NIC), were hacked during the year 2017 and 2018 (upto November) respectively.

(c) and (d): As per information reported to Indian Computer Emergency response Team (CERT-In), a total of 3, 14 and 6 financial fraud incidents affecting ATMs, cards, Point of sale (PoS) systems and Unified Payment Interface (UPI) have been reported during the years 2016, 2017 and 2018 (upto November) respectively. Further, Reserve Bank of India (RBI) has registered a total of 1191, 1372, 2059 and 921 cases of frauds involving ATM/Debit Cards, Credit Cards and Internet Banking Frauds reported (amount involved Rs 1 lakh and above) during the year 2015-16, 2016-17, 2017-18 and 2018-19 (Upto 30 Sept 2018) respectively.

(e): In tune with the dynamic nature of Information Technology and emerging cyber threats, continuous efforts are required to be made by owners to protect networks by way of hardening and deploying appropriate security controls. Government has taken several measures to enhance the cyber security posture and prevent cyber attacks including breaches and hacking. These *inter alia*, include:

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

safe usage of digital technologies. Regarding securing digital payments, 28 advisories have been issued for users and institutions.

(ii) All authorised entities/ banks issuing PPIs in the country have been advised by CERT-In through Reserve bank of India to carry out special audit by empanelled auditors of CERT-In on a priority basis and to take immediate steps thereafter to comply with the findings of the audit report and ensure implementation of security best practices.

(iii) All the new government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is to be conducted on a regular basis after hosting.

(iv) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

(v) Government has empanelled 76 security auditing organisations to support and audit implementation of Information Security Best Practices.

(vi) All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.

(vii) Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

(viii) Cyber security mock drills and exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 38 such exercises have so far been conducted by CERT-In where organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeSetc participated.

(ix) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. 22 trainings covering 746 participants conducted in the year 2018 (till November).

(x) Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

(xi) Government has initiated setting up of National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. Phase-I of NCCC has been made operational.

(xii) National Informatics Centre (NIC), which provides IT/E-Governance related services to Government departments, 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. Additionally, periodic security audits of resources are performed followed by subsequent hardenings. These are complemented by round-the-clock monitoring of security events and remedial measures are carried out for solving the problems subsequently.

****