GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
**LOK SABHA**
**UNSTARRED QUESTION NO. 761**
TO BE ANSWERED ON: 07.02.2018

**UNCTAD REPORT ON CYBER SECURITY**

**761.    SHRIMATI  K. MARAGATHAM:**

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

(a)    whether it is a fact that India saw the highest number of people going online for the first time during 2012-15 period among all countries and if so, the details thereof;

(b)    whether it is also true that the UNCTAD report has raised concern about protection of online data and devices as more economic activities go digital and if so, the details thereof;

(c)    whether it is also true that the Government is taking all steps to prevent the growing cyber crime in the country as digital  payment  system  needs  more protection; and

(d)    if so, the details thereof?

**ANSWER**

MINISTER OF  ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(a) and (b): There have been some media news items based on the UN Conference on Trade and Development (UNCTAD) "INFORMATION ECONOMY REPORT 2017" which indicate that India saw the highest number of people going  online for the first time during 2012-15 period among all countries. The news items further highlight that the UNCTAD report has raised concern about protection of online data with digitization of more economic activities.

(c) and (d): Government has taken a number of legal, technical and administrative policy measures for addressing cyber attacks leading to cyber crime and enhance security of digital payment systems. This includes National Cyber Security policy 2013, enactment of Information Technology (IT) Act, 2000, setting up of Indian Computer Emergency Response Team (CERT-In) and National Critical Information Infrastructure Protection Centre (NCIIPC) under the provisions of IT Act, 2000, etc. Some major activities are:

(i)    CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities alongwith countermeasures to create awareness among stakeholders to take appropriate measures to ensure safe usage of digital technologies. Regarding securing digital payments, 27 advisories have been issued for users and institutions.

(ii)   All authorised entities/banks issuing Prepaid Payment Instruments (PPIs) in the country have been advised by CERT-In through the Reserve Bank of India to carry out security audit by the 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 organizations providing digital payment services have been mandated to report cyber security incidents to CERT-In expeditiously.

(iv)    CERT-In has empanelled 54 security auditing organizations to support and audit implementation of Information Security Best Practices.

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

(vi)    CERT-In is regularly conducting cyber security trainings for IT / cyber security professionals including CISOs of Government and critical sector organisations to give an exposure on current threat landscape and countermeasures. In addition, CERT-In has also conducted a workshop on security of digital payments systems for stakeholder organisations covering 110 participants.

(vii)    Government has established Botnet Cleaning and Malware Analysis Centre to detect and clean infected systems in the country.

(viii)    MeitY has organised 2 workshops for banks, Internet Service Providers (ISPs) and Prepaid Payment Instruments (PPIs) issuing entities regarding security of digital payments systems.

(ix)    Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 15 such drills have so far been conducted by CERT-In where 148 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated. In addition 3 drills were conducted in coordination with The Reserve Bank of India and The Institute for Development and Research in Banking Technology.

(x)    RBI has issued a comprehensive circular on Cyber Security Framework in Banks on June 2, 2016 covering best practices pertaining to various aspects of cyber security.

(xi)    RBI has issued Master Directions on Issuance and Operation of Prepaid Payment Instruments on October 11, 2017.

*******