GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2633
TO BE ANSWERED ON: 04.12.2019

ONLINE FRAUDS AND SCAMS

2633. SHRI NALIN KUMAR KATEEL:

Will the Minister of Electronics & Information Technology be pleased to state:-
(a) whether the Government has taken note of the fact that fraudsters leverage technology to mask identity and create fake e-mails and websites and if so, the details thereof and the reaction of the Government thereto;
(b) whether the Government has received any complaints over online fraud and online scams in the country and if so, the details thereof and the number of such complaints received by the Government during each of the last three years; and
(c) whether the Government proposes to introduce any mechanism to regulate the websites and resolve aforesaid complaints and if so, the details thereof?

ANSWER
MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(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 identity theft, creation of fake-emails and websites is a global issue.

(b): 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 year 2016, 2017 and 2018 respectively. Further, Reserve Bank of India (RBI) has registered a total of 1372, 2059 and 1866 cases of frauds involving ATM/Debit Cards, Credit Cards and Internet Banking Frauds reported (amount involved Rs. 1 lakh and above) during the year 2016-17, 2017-18 and 2018-19 respectively.

(c): 'Police' and 'Public Order' are State subjects as per the Constitution of India. States/UTs are primarily responsible for prevention, detection, investigation and prosecution of crimes through their law enforcement machinery. Ministry of Home Affairs (MHA) supports State Government initiatives through the various schemes and advisories.
Government has taken a number of legal, technical and administrative measures to prevent cyber crimes. These *inter alia*, include:
(i) Enactment of the Information Technology Act 2000 which has provisions to deal with prevalent cyber crimes. The Act has specific provisions for stringent punishment and fine for identity theft (section 66C) and cheating by personation using computer resource (section 66D).
(ii) To spread awareness on cyber crime, several steps have been taken that include dissemination of messages on cyber crime through MHA Twitter handle @cyberDost, radio campaign, publishing of Handbook for Adolescents / Students, publishing of 'Information Security Best practices' for the benefit of Govt. Officials/ Officers. Organizing of cyber Safety and Security Awareness weeks, in association with police department in different States/Uts etc.
(iii) To prevent such crimes and to speed up investigation, MHA has taken several steps to spread awareness about cyber crimes issue through alerts/ advisories, capacity building/training of law enforcement personnel/ prosecutors/ judicial officers, improving cyber forensics facilities etc. MHA has also launched an online national cyber crime reporting portal, (www.cybercrime.gov.in) to enable complainants to report complaints pertaining to all types of cyber crimes with special focus on cyber crimes against women and children.

(iv) Ministry of Electronics and Information Technology through a program, namely, Information Security Education & Awareness (ISEA), has been creating awareness among users highlighting the importance of following the ethics while using Internet and advising them not to share rumors/fake news. A dedicated website for information security awareness (https://www.infosecawareness.in) provides all the relevant awareness material.

(v) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of cyber crime cases.

****