

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 568
TO BE ANSWERED ON 16.09.2020

ONLINE FRAUDS AND SCAMS

568. SHRI SUMEDHANAND SARASWATI:

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

- (a) whether the Government has taken note of the fact that fraudsters use technology to hid their identity and create fake emails and websites and if so, the details thereof and the reaction of the Government thereto;
- (b) whether the Government has received a number of complaints regarding online frauds and scams in the country;
- (c) if so, the details thereof and the action taken by the Government thereon; and
- (d) whether the Government has put in place any mechanism to protect the common man from such frauds and if so, the details thereof?

ANSWER

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

(a) to (c) : 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. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In) a total of 454, 472 and 194 phishing incidents were observed during the year 2018, 2019 and 2020 (till August) respectively. Further, a total of 6, 4 and 2 financial fraud incidents affecting ATMs, Cards, Point-of- Sale (PoS) systems and Unified Payment Interface (UPI) have been reported during the year 2018, 2019 and 2020 (till August) respectively.

(d): '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 several steps to prevent such cyber security incidents and improving cyber safety in the country. These, *inter alia*, include :

- i) CERT-In is working in coordination with Reserve Bank of India (RBI) and Banks to track and disable phishing websites.
- ii) 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, 37 advisories have been issued for users and institutions.
- iii) Security tips have been published for users to secure their Desktops, mobile/smart phones and preventing phishing attacks.

- iv) All authorised entities/banks issuing Prepaid Payment Instruments (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.
- v) Government has empanelled 90 security auditing organisations to support and audit implementation of Information Security Best Practices.
- vi) 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.
- vii) Ministry of Electronics & Information Technology is conducting programs to generate information security awareness. Specific books, videos and online materials are developed for children, parents and general users about information security which are disseminated through Portals like “www.infosecawareness.in”, and “www.cyberswachhtakendra.gov.in”.
