

GOVERNMENT OF INDIA  
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY  
**LOK SABHA**  
**UNSTARRED QUESTION NO.3498**  
TO BE ANSWERED ON: 02.01.2019

**INCREASE IN ONLINE FRAUD**

**3498. SHRI D.K. SURESH:**  
**SHRI NALIN KUMAR KATEEL:**

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

- (a) whether it is true that consumers from India are less aware about online frauds when compared to other APAC (Asia Pacific) countries and if so, the details thereof and the reasons therefor;
- (b) whether it is also true that the opportunity for online fraud is escalating as consumers are looking for easier ways to buy products online;
- (c) if so, whether the Government is aware that there is more that needs to be done to build awareness to fight online fraud and if so, the steps taken in this regard; and
- (d) the other measures taken by the Government to protect the consumers from digital frauds?

**ANSWER**

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

(a): There are media reports indicating that that consumers from India are less aware about online frauds when compared to other APAC (Asia Pacific) countries.

(b): Cyberspace has distinct and unique characteristics as compared to physical space. With widespread proliferation of new technologies like online shopping, there are some miscreants who are misusing these technologies to commit online frauds. Thus misuse of cyberspace including online shopping related frauds is on rise in the country as elsewhere in the world.

(c) and (d): Cyber security is a challenging field because of ever changing threat scenario. Continuous efforts are required to be made to protect ICT infrastructure from cyber attacks by way of hardening of servers and networks and deploying appropriate security controls. Further, the Government has taken several measures to protect the consumers from digital frauds. 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) Government has empanelled 76 security auditing organisations to support and audit implementation of Information Security Best Practices.
- (iii) 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.
- (iv) 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.
- (v) Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.
- (vi) All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.

- (vii) 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).
- (viii) 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.

\*\*\*\*\*