GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3367
TO BE ANSWERED ON 09.08.2023

CYBER CRIMES IN CYBER WORLD

3367. SHRI MALOOK NAGAR:

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

(a) whether the Government is taking steps towards developing technology to prevent and monitor cyber crimes in view of the increasing number of these crimes;
(b) if so, the details thereof including the increase in cyber crimes during the last three years; and
(c) the mechanism available for compensating bank account holders who have been victims of economic frauds through cyber crimes?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a) and (b):The policies of the Government are aimed at ensuring an Open, Safe &Trusted and Accountable Internet for its all users, keeping in view emerging challenges of cybercrimes. The Information Technology Act, 2000 ("IT Act") and rules made thereunder contain provisions for safeguarding Digital Nagriks from cyber crimes. The IT Act penalises various offences relating to computer resources, including tampering with computer source documents (section 65), dishonestly or fraudulently damaging computer system (section 66), identity theft (section 66C), cheating by impersonation (section 66D), cyber terrorism (section 66F), securing unauthorised access to protected system (section 70), etc.

In addition to such general provisions regarding cyber offences, it also provides for various offences that serve to secure the digital space for women, e.g., violation of bodily privacy (section 66E), transmitting of obscene material (section 67), and publishing or transmission of material containing sexually explicit act in electronic form including depicting children in sexually explicit act (sections 67A and 67B). These offences are in addition to various penal provisions under the Indian Penal Code, such as the offence of stalking using electronic communication (section 354D).

As per the data maintained by National Crime Records Bureau, cases registered under the under Total Cyber Crimes, are 44735, 50035 and 52974 for the year 2019, 2020 and 2021, respectively.

As per the provisions of the Code of Criminal Procedure, 1973, prevention and investigation of cognizable offences is to be done by the police, and as per the Seventh Schedule to the Constitution, 'Police' is a State subject. As such, States are primarily responsible for the prevention, investigation etc. of such cybercrimes through the State police departments, including in respect of training their police personnel for upgrading technical knowhow to investigate and solve such crimes.

The Central Government supplements the initiatives of the State Governments through various advisories and schemes for the capacity building of their police personnel. Steps taken by it in this direction which include the following:

(i) The Ministry of Electronics and Information Technology has initiated many projects such as Setting up of a Collaborative and Comprehensive Live Cyber Operations Specific Exercise Training Facility (Cyber Closet) for Indian Cyber Space,

Development of Cyber Forensic Training cum Investigation Labs in North-Eastern States, and Cloud based centralized Cyber Forensics Lab Infrastructures and Capacity Development on Smart Device Forensics Investigations and Creation of Resource Centre for the North Eastern Police Forces.

(ii) The Ministry of Home Affairs has set up the Indian Cyber Crime Coordination Centre (I4C) to deal with all types of cybercrime in the country in a coordinated and comprehensive manner.

(iii) Under the Cybercrime Prevention against Women and Children (CCPWC) Scheme, financial assistance to the tune of Rs. 99.88 crore has been provided to all States and Union territories for setting up of cyber forensic cum training laboratories, hiring of junior cyber consultants and capacity building of Police personnels, public prosecutors and judicial officers. So far, cyber forensic-cum-training laboratories have been commissioned in 33 States and Union territories.

(iv) Training curriculum has been prepared for law enforcement agency personnel, prosecutors and judicial officers for better handling of investigation and prosecution. States and Union territories have been mandated to organise training programmes. So far, more than 20,300 police personnel, judicial officers and prosecutors have been provided training on crime awareness, investigation, forensics, etc.

(v) The Online Capacity Building Programme on Cyber Law, Cybercrime Investigations and Digital Forensics, of the Ministry of Electronics and Information technology, offers a post graduate diploma of nine month duration in a phased manner to 1,000 officials of police, State Cyber Cells, prosecutors and judicial officers through Learning Management System.

(vi) The 'CyTrain' portal has been developed under the I4C, for capacity building of police and judicial officers through online course on critical aspects of cybercrime investigation, forensics, prosecution etc. along with certification. More than 28,700 police officers from States and Union territories are registered and more than 7,800 certificates have been issued through the portal.

(vii) The Ministry of Home Affairs has provided financial assistance under the Assistance to States for Modernization of Police Scheme to State Governments for acquisition of latest weaponry, training gadgets, advanced communication and forensic equipment, cyber policing equipment etc. The State Governments formulate State Action Plans as per their strategic priorities and requirements including combating cybercrimes.

(c):With the increased thrust on financial inclusion and customer protection and considering the recent surge in customer grievances relating to unauthorised transactions resulting in debits to their accounts/ cards, the criteria for determining the customer liability in these circumstances have been reviewed by the Reserve Bank of India (RBI). In this direction, RBI has issued a revised Direction on 06.07.2017 to all Scheduled Commercial Banks including Regional Rural Banks (RRBs) and Small Finance Banks and Payments Banks with regard to the strengthening of systems and procedures, reporting of unauthorised transactions by customers to banks andzero liability/ limited liability of customer along with prescribed reversal timeline, etc. On being notified by the customer, the bank shall credit (shadow reversal) the amount involved in the unauthorised electronic transaction to the customer's account within 10 working days from the date of such notification by the customer (without waiting for settlement of insurance claim, if any). The bank has to resolve customer's complaint within 90 days from the date of receipt of customer's notification after establishing the customer's liability. This Direction is available in RBI's website – https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=2336.

******