Annexure – I
WRITE UP

Government of India
Ministry of Home Affairs
Indian Cyber Crime Coordination Centre (I4C)
(CIS Division)
***

Sub: -Commencement of 'CyberJaagrooktaDiwas' on First Wednesday of every month commencing from 6thOctober, 2021 (Wednesday)

Introduction

1. Cyber space is a complex and dynamic environment of interactions among people, software and services supported by world-wide distribution of Information and Communication Technology (ICT) devices and networks. On the one hand, cyber space, which cuts across global boundaries has brought in latest innovative technologies and modern gadgets, while on the other hand, it has inevitably led to increased dependencies on computer resources and internet-based professional, business and social networking.

2. The exponential increase in the number of internet users in Indiaand the rapidly evolving technologies have also brought in its own unique challenges, besides aggravating the existing problems of cybercrimes, which is one of the fastest growing forms of transnational and insidious crimes.

3. These technological developments have also led to the proliferation of cybercrimes, which is one of the fastest growing forms of transnational and invisible crimes. The borderless nature of cybercrimes poses challenges in responding effectively due to the limits of cross-border investigation, legal and jurisdictional challenges and diversity in the technological capabilities to combat this virtual crime space spread across the globe.

4. Cybercrimesare generally understood as malware attack (use of malicious software like ransom ware, viruses, trojans, spyware, bots etc.), phishing (capturing sensitive information like username, password, credit/debit card details using fake websites, emails etc.), attacks on critical infrastructure, unauthorized data access (data breach), online financial frauds, crimes against women and children like cyber stalking, child pornography etc.

5. There is a need to increase 'cyber hygiene' for prevention of cyber crimes by inculcating habits of taking basic care of ICT devices at regular intervals, such as, properly shutting down the computer, changing passwords at regular intervals, being cautious against opening of phishing websites along with other websites, precautions to be taken while handling social media platforms, protection against data theft,collection and disposable of E-waste etc.

6. Further, continuous efforts are required on frequent basis to remind the citizens about the cardinal principles of cyber hygiene to ensure safety against cyber

crimes. Cyber hygiene becomes more important on account of ever changing scenarios in cyber space clubbed with technological advancements.

7. Any lapse in cyber security and/or cyber hygiene has the potential to lead to a cybercrime and both these facets are interlinkedand require concurrent action of various stakeholders for the protection of Nation's cyber space and ensuring citizen safety in a holistic manner.

8. With evolving technology, cyber criminals use loopholes to conduct cybercrimes. Digital space will see rapid adoption of Cloud, Drones, Robotics, Digital Currency, Internet of Things (Connected Devices), 3D printing, Machine Learning, Virtual & Augmented Reality etc. These technologies can instigate significant risks to Nation's internal security, if these are allowed to be exploited by deviant characters.

Indian Cyber Crime Coordination Centre (I4C) – A Scheme of CIS Division

9. Cyber space makes geographical boundaries irrelevant and handling cyber-crime requires, besides latest technologies, coordination amongst different stakeholders and different jurisdictions at all levels (district/state/national/global).

10. To address this problem, MHA had constituted an Expert Group in 2014 to study the gaps and challenges and prepare a roadmap for effectively tackling cybercrimes in the country. Post identification of gaps, the Expert Group recommended for setting up of an Indian Cyber Crime Coordination Centre (I4C) in 2018 for strengthening the overall security apparatus to support States/UTs by providing a common framework to fight against cybercrimes, as enumerated below: -

- National Cyber Crime Reporting Portal for centralized reporting of complaints related to CPRGR & any other cyber-crimes.
- National Cyber Crime Threat Analytical Unit for bringing together Law Enforcement Agencies to share threat intelligence reports.
- National Cyber Forensic Laboratory with state of art forensic tools.
- Platform for Joint Cybercrime Coordination for intelligence led coordinated efforts against cyber-crimes.
- National Cybercrime Training Centre for advance simulation and training of LEAs on cyber-attacks.
- National Cybercrime Ecosystem for coordination with academia, institutions, Ministries etc.
- National Cyber Research and Innovation Centre to partner with various Institutes for Research and Development in field of cyber-crimes.

11. Due to penetration of high-end technologies like artificial intelligence, block-chain, machine learning etc. in conjunction with an ever growing number of users 'going online', newer patterns of cyber-threats are emerging. Several of these threats are prejudicial to national security, public order and are exposing nation's critical infrastructure to a complex risk matrix.Thus, there is a need for

extensively collaborative and coordinated efforts by various stakeholders to plug in the gaps in a structural and systematic manner.

12. Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes through their Law Enforcement Agencies (LEAS).

Mass Awareness Campaign in all the Schools, Colleges, Panchayati Raj Institutions (PRI) and Municipalities in the country

13. I4C proposes to observe'**Cyber Jaagrookta (Awareness)Diwas'** every month in all Schools/Colleges/Universities/ Panchayati Raj Institutions (PRI), Municipalities by involvingDistrict Magistrates, Police authorities, Officers of Education Department, PRIs etc. In this regard, it is informed that in the review meeting held on 23.6.2021 under the chairmanship of JS (CIS) with M/o Education, NCERT, CBSE, UGC, it was also mentioned that *M/o Education may commence 'Cyber Jaagrookta Diwas' to create awareness for prevention of cybercrimes and to organize various workshop, seminars etc in all schools every month.*

14. The main purpose of this initiative is to create awareness for prevention of cybercrimes amongst students of schools (6th standard onwards for all classes) and Colleges (all streams) through workshops, seminars, interactive sessions, quiz competitions, best practices, case studies, creative sessions like poster making/ slogan writing/ short stories/ essay writing etc by involvement of students every month on the same day and at the same time in all schools (around1.5 lakh) and Colleges/Universities of UGC (around 40,000) in the country covering approx.24.7 crore school students and approx. 2.45 crores College/University students. Further, the objective of this initiative is that each student should act as 'Cyber Warrior / Brand Ambassador' for prevention of cybercrimes. Also, the initiative may also be taken in various PRIs and Municipalities.

15. Basic protocols of Cyber Hygiene may also be highlighted during the 'Cyber Jaagrookta Diwas', some of which are mentioned here to name a few:*shut down the computer, Install and maintain up to date anti-virus software on your computer or device, keep your internet browser up-to-date, be alert to unusual computer activity or problems, use a modern browser with features such as a pop-up blocker, change your passwords often, beware of links sent via instant messaging and e-mail attachments, don't open emails or attachments from people you don't know, don't become online 'friends' with people you don't know, be very careful about sharing content online, use the strongest privacy setting when you set up your profile, avoid joining unknown Wi-Fi networks and using unsecured Wi-Fi hotspots, do not share any information related to sensitive and financial aspects in social networks.*

16. It is further informed that the necessary budgetary provisions will have to be made by the concerned States/UTs from their respective budgets.States/UTs may explore acknowledging every year five teachers of schools and colleges each, five representatives of PRIs and Municipalities each who have made exceptional contribution in generating awareness against cybercrime at their own level, so as to motivate them and inspire their tireless efforts of educating youngsters for cyber safe environment. States/UTs may also explore recognizing schools/colleges/PRIs/ Municipalities as "Cyber Star" of the month. States/UTs may like to consider forwarding the names of such persons to MHA, so that MHA may also suitably acknowledge the work done by them.

Topics to be covered in Cyber Jaagrookta Diwas:-

17. The suggestive topics for creating awareness are highlighted below:-

For Primary students of class 6th to 10th Standards

- Introduction to cybercrimes
- Kinds of cybercrimes: phishing, identify theft, cyber stalking, cyber obscenity, computer vandalism, ransomware, identity theft
- Spotting fake apps and fake news on social media and internet (fake email messages, fake post, fake whatsapp messages, fake customer care/toll free numbers, fake jobs)
- Internet Ethics, internet addiction, ATM scams, online shopping threats, lottery emails/SMS, Debit/Credit card fraud, Email security, mobile phone security
- Mobile apps security, USB Storage Device security,
- Mobile connectivity Security Attacks (Bluetooth, Wi-Fi, Mobile as USB)
- Preventive measures to be taken in Cyber space, reporting of cyber crime

For students of Class 11thStandard and above

Unit – I: Cyber Crimes and safety

- Introduction to cybercrimes
- Kinds of cybercrimes: phishing, identify theft, cyber stalking, cyber obscenity, computer vandalism, Ransomware, Identity Theft
- Forgery and fraud from Mobile Devices
- Cyber risk associated with varied online activities and protection therefrom.
- Work on different digital platforms safely
- Online cybercrimes against women and impersonation scams
- Safety in Online Financial transactions

Unit – II: Concept and use of Cyber Hygiene in daily life

- Browser Security, Desktop security, UPI Security, Juice Jacking, Google Map Security, OTP fraud

- IOT Security, Wi-Fi Security, Spotting fake apps on Social media and Internet (fake email messages, fake post, fake whatsapp messages, fake customer care/toll free numbers, fake jobs)
- Internet ethics, internet addiction, ATM scams, online shopping threats, lottery emails/SMS, loan frauds,
- How to avoid Social Engineering Attacks, debit/credit card fraud, e-mail security, mobile phone security, mobile apps security, USB storage device security, data security
- Mobile connectivity security attacks (Bluetooth, Wi-Fi) ,mobile as USB, broadband internet security
- Preventive measures to be taken in cyber space, reporting of Cyber crime

Unit – III: Introduction to Social Networks

- Social Network and its contents, blogs
- Safe and proper use of social networks inappropriate content on social networks
- Flagging and reporting of inappropriate content

Unit – IV: Electronic Payments and Safeguard therein

- Concept of E payments, ATM and Tele Banking
- Immediate Payment Systems Mobile Money Transfer and E-Wallets
- Unified Payment Interface (UPI)
- Cybercrimes in Electronic Payments
- KYC: Concept, cases, and safeguards

18. In addition to above, the students may also be informed about National Cybercrime Reporting Portal(https://www.cybercrime.gov.in) and a toll free helpline 155260 to assist citizens for registration of complaints on the portal. Further, students may be informed about @cyberdost twitter handle, (https://www.instagram.com/cyberdosti4c) instagram handle, (https://www.facebook.com/CyberDostI4C) facebook handle and (https://www.linkedin.com/company/cyberdosti4c) LinkedIn handle, which provide regular safety tips relating to prevention of cybercrimes. Every State/UT is requested to prepare an Action Planfor 12 months online/offline program in consultation with D/o Education, D/o Higher Education, MeitY and Police Department, commencing from **6th October, 2021**,wherein the States/UTs will be free to choose the topics forCyber awareness and Cyber Hygiene, as per the age group of students and may also dovetail schemes/projects of other Ministries, so as to have synergetic efforts in prevention of cybercrime.

Stakeholders

19. States/UTs may like to involve the following stakeholders for'**Cyber JaagrooktaDiwas**':-

- Collectorate (DM, ADM, SDMs)
- Police Department, especially Police officers handling cybercrimes
- Department of Education
- Department of Higher Education
- School teachers to cover all schools in the State
- College faculties to cover all Colleges
- MeitY
- Department of Social Welfare
- Department of Panchayati Raj
- Department of Women and Children
- Department of Labor
- Municipalities
- Citizen Service Centres
- Asha Workers
- Any other Departments/ Stakeholders in the States.

DGPs/CPs of all the States/UTs; Secretary (D/o Higher Education), Ministry of Education; Government of India and Secretary (D/o School Education), Government of India will also be requested to issue instructions to the concerned officers to kindly collaborate in this regard for creating awareness in prevention of cybercrimes.

Annual Action Plan

20. All the States/UTs may kindly prepare an "Action Plan" on **Cyber Jaagrookta Diwas** to involve above said stakeholders on every firstWednesday of the month online (during COVID) and offline there on commencing from6thOctober, 2021 (Wednesday) during the period 11am to 12 noon (tentatively). The draft action plan may kindly be provided to I4C by 27th September, 2021.