"हर काम देश के नाम"

रक्षा लेखा विभाग(र.ले.वि.) मुख्यालय

उलान बटाररोड, पालम, दिल्ली छावनी-110010

DEFENCE ACCOUNTS DEPARTMENT (DAD) HEADQUARTERS

Ulan Batar Road, Palam, Delhi Cantt.- 110010

Phone: 011-25665586, 2566589, 25665763 Fax: 011-25675030 email: cgdanewdelhi@nic.in

आज़ादी का अमृत महोत्सव

CIRCULAR

No. Mech/IT&S/810/CyberSecurity Dated:24.05.2022

To,

All the PCsDA/PIFAs/CsDA/IFAs

(As per standard list)

Subject: Observation of 'Cyber Jaagrookta Diwas' on first Wednesday of every month

The technological developments have led to the proliferation of cyber-crimes. Ministry of Home Affairs has taken initiative for prevention of cyber-crimes and to create awareness among people on "cyber hygiene". To address the problem, MHA has issued guidelines regarding the need to increase cyber-hygiene to remind citizens about the safety against cyber-crimes and to inculcate habits of taking care of ICT devices at regular intervals.

2. Accordingly, MHA has requested all the Ministries to observe "Cyber Jaagrookta (Awareness) Diwas" on first Wednesday of every month during the period 11-00 am to 12-00 am.

3. The main purpose of this initiative is to create awareness for prevention of cyber-crimes through various ways including organising workshops, seminars, interactive sessions, quiz competitions, case studies, and creative sessions every month on the same day and at the same time.

4. Basic protocols of **'Cyber Hygiene'** to be highlighted during the 'Cyber Jaagrookta Diwas' are mentioned below:

a) Shut down the computer

b) Install and maintain up-to-date anti-virus software on computer

c) Keep internet browser up-to-date

d) Be alert to unusual computer activity or problems

e) Use modern browser with features such as pop-up blocker

f) Change passwords regularly

g) Beware of links sent via instant messaging and e-mail attachments

h) Don't open e-mails and attachments from unknown people

i) Be careful about sharing content online

j) Use strong privacy settings

k) Avoid joining unknown Wi-Fi networks and using unsecured Wi-Fi hotspots

l) Do not share any information related to sensitive and financial aspects on social networks.

5. It is further informed that the necessary budgetary provisions will be made through the IT budget (Codehead 0/094/94). Every Controller Office may explore acknowledging every 5-10 employees who have made exceptional contribution in generating awareness against cyber-crimes at their own level to motivate and inspire them. It may also recognize sections/officials, etc as **"Cyber Star"** of the month.

6. A writeup on the Cyber Jaagrookta Diwas is enclosed herewith as Annexure-A1.Topics to be covered in Cyber Jaagrookta Diwas are enclosed as Annexure-A2.

7. Every Controller Office is requested to submit a Compliance Report with regard to activities performed and actions taken for Cyber Jaagrookta Diwas to this office on monthly basis for appraisal of CGDA.

It CGDA has seen.

Encls: Annexure A1& A2

(Sandeep Bansal)

Sr. ACGDA (IT&S)

Annexure – I
WRITE UP

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

Sub: - Observing 'Cyber Jaagrookta (Awareness) Diwas' on first Wednesday of every month.

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 India and 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. Cyber crimes are generally understood as malware attack (use of malicious software like ransomware, 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. It is also seen that around 60% of the cyber crimes reported on National Cyber Crime Reporting Portal (https://www.cybercrime.gov.in) relate to online financial frauds.

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 interlinked and 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, MHA

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 has set up 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 cyber crimes, as enumerated below: -

- National Cybercrime Reporting Portal (NCRP) for centralized reporting of complaints related to CPRGR & any other cyber-crimes.
- National Cybercrime Threat Analytical Unit (NCTAU) for bringing together Law Enforcement Agencies to share threat intelligence reports.
- National Cyber Forensic Laboratory (NCFL) with state of art forensic tools.
- Platform for Joint Cybercrime Coordination (JCCT) for intelligence led coordinated efforts against cyber-crimes.
- National Cybercrime Training Centre (NCTC) for advance simulation and training of LEAs on cyber-attacks.
- National Cybercrime Ecosystem Management Unit (NCEMU) for coordination with Academia, Institutions, Ministries etc.
- National Cyber Research and Innovation Centre (NCR&IC) 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.

Mass Awareness Campaign in all the Ministries

12. It is requested to observe **'Cyber Jaagrookta (Awareness) Diwas'** every month in all the offices, branches / sections, PSUs, etc in the Ministry. The main purpose of this initiative is to create awareness for prevention of cyber crimes through

workshops, seminars, interactive sessions, quiz competitions, best practices, case studies, creative sessions every month on the same day and at the same time.

13. 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.*

14. It is further informed that the necessary budgetary provisions will have to be made by the concerned Ministry from its respective budget. The Ministry may explore acknowledging every year 5-10 employees who have made exceptional contribution in generating awareness against cyber crime at their own level, so as to motivate them and inspire their tireless efforts for cyber safe environment. The Ministries may also explore recognizing sections / officials, etc as "Cyber Star" of the month.

Topics to be covered in Cyber Jaagrookta Diwas: -

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

Unit – I: Cyber Crimes and safety

- Introduction to cyber crimes
- Kinds of cyber crimes: 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
- 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 th... 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)
- Cyber crimes in Electronic Payments
- KYC: Concept, cases, and safeguards

16. In addition to above, the officials may also be informed about National Cybercrime Reporting Portal(https://www.cybercrime.gov.in) and a toll free helpline number 1930 (earlier helpline number was 155260) to assist citizens for registration of complaints pertaining to cyber crimes on the portal. Further, officials may be informed to follow **@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 cyber crimes.

17. All the Ministries are requested to prepare an "Annual Action Plan" online/offline program on Cyber Jaagrookta Diwas. The Ministries are free to choose the topics for Cyber awareness and Cyber Hygiene, as per the location of the institutions / offices (village, smaller towns, major cities etc) and may also dovetail schemes/projects of other Ministries, so as to have synergetic efforts in prevention of cyber crimes to citizens.

Annual Action Plan

18. All the Ministries may kindly prepare an "Annual Action Plan" for celebrating **Cyber Jaagrookta Diwas** on every first Wednesday of the month during the period 11am to 12 noon (tentatively) commencing from **6th April, 2022 (Wednesday) onwards**.

*****

ANNEXURE A2

Topics to be covered in Cyber Jaagrookta Diwas are as given below:

a) **Unit-I: Cyber-crimes and safety**

- Introduction to cyber-crimes
- Kinds of cyber-crimes: phishing, identity theft, cyber-stalking, cyber-obscenity, computer vandalism, ransomware
- Spotting fake apps and fake news on social media and internet
- Internet ethics, internet addiction, ATM scams, online shopping threats, lottery emails/SMS, Debit/Credit cards frauds, Email security, mobile phone security
- Mobile apps security, USB Storage Device security
- Mobile connectivity security attacks(Bluetooth, Wi-Fi, USB)
- Preventive measures to be taken in cyber-space, reporting of cyber-crime
- Forgery and fraud from mobile devices
- Cyber risk associated with varied online activities and protection therefrom.
- Online cyber-crimes against women and impersonation scams
- Safety in online financial transactions

b) **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

c) **Unit-III: Introduction to Social Networks**

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

d) **Unit-IV: Electronic payments and safeguards therein**

- Concept of e-payments, ATM and Tele-banking
- Immediate payments systems, mobile transfer and e-wallets
- Unified payment interface(UPI)
- Cyber-crimes in E-payments
- KYC: Concept, cases and safeguards