स्वातंत्र्याचा अमृत महोत्सव

डॉ. प्रभाकर देसाई
एम्.ए., पीएच् डी.
संचालक

सावित्रीबाई फुले पुणे विद्यापीठ
(पूर्वीचे पुणे विद्यापीठ)
राष्ट्रीय सेवा योजना
गणेशखिंड, पुणे – ४११ ००७

कार्यालय क्र. : ०२०-२५६२२६८८/८९
: ०२०-२५६२२६९०/९१
: ०२०-२५६२२६९२
: ०२०-२५६९७३४१

संदर्भ : रासेयो/२०२२—२३/५८६ दि. २३/०४/२०२२

प्रति,
मा.प्राचार्य/संचालक,
रासेयो संलग्नित संबधीत महाविद्यालये परिसंस्था,
पुणे, अहमदनगर व नाशिक जिल्हा,
सावित्रीबाई फुले पुणे विद्यापीठ.

विषय : सायबर जागरूकता दिवस साजरा करण्याबाबत

महोदय,

मा. क्षेत्रीय संचालक, रासेयो क्षेत्रीय संचलनालय, भारत सरकार, पुणे यांच्या पत्रानुसार आणि सहायक कार्यक्रम सल्लागार, युवा व क्रीडा मंत्रालय, नवी दिल्ली, भारत सरकार, यांच्या निर्देशानुसार प्रत्येक महिन्याच्या पहिल्या बुधवारी "सायबर जागरूकता दिवस" साजरा करण्याबाबत कळविण्यात आले आहे.

तरी आपण आपल्या महाविद्यालयामध्ये रासेयो एककाद्वारे सायबर जागरूकता उपक्रम राबविण्यात यावेत. अधिक माहितीकरिता सोबतच्या पत्राचे अवलोकन करावे. तसेच या उपक्रमाबाबत फेसबुक, व्हाट्सअॅप व इतर सोशल मिडीयाच्या माध्यमातून जास्तीत जास्त प्रसिध्दी द्यावी. सदर उपक्रम संपन्न झाल्यानंतर उपक्रमाचे फोटो व अहवाल त्वरीत nss_student_list@pun.unipune.ac.in या मेलवर "**सायबर जागरूकता दिवस २०२२**" या विषयासह पाठवण्यात यावा. कळावे, ही विंनती.

संचालक
राष्ट्रीय सेवा योजना

अधिक माहितीकरिता : सहायक कार्यक्रम सल्लागार, युवा व क्रीडा मंत्रालय, नवी दिल्ली, भारत सरकार, यांचे पत्र

भारत सरकार,
युवा कार्यक्रम और खेल मंत्रालय,
रा.से.यो.के क्षेत्रीय निदेशालय,
पहली मंजिल, 'ए' ब्लॉक हॉस्टल, कृषि महाविद्यालय परिसर,
शिवाजी नगर, पुणे - ४११ ००५

मी. सं. - २१/१५ / क्षे.नि./ रा.से.यो./ २०२२-२३ /63-102 दिनाँक- २२/०४/२०२२

प्रति,

सभी एनएसएस कार्यक्रम समन्वयक
महाराष्ट्र और गोवा राज्य

विषय: साइबर जागरुकता दिवस (सीजेडी) संबंध में

सर/मैडम,

विषय के संदर्भ में, कृपया महीने के प्रत्येक पहले बुधवार को साइबर जागरूकता दिवस मनाने के संबंध में गृह मंत्रालय से संलग्न पत्र प्राप्त करें।

इस संबंध में आपसे अनुरोध है कि कृपया अपने अधिकार क्षेत्र की सभी एनएसएस इकाइयों को हर महीने के पहले बुधवार को साइबर जागरूकता दिवस मनाने के लिए गतिविधियों का आयोजन करने और गतिविधियों पर एक समेकित रिपोर्ट इस कार्यालय को प्रस्तुत करने के लिए सूचित करें।

यह भी अनुरोध किया जाता है कि समुदाय के बीच जागरूकता पैदा करने वाले आधिकारिक सोशल मीडिया हैंडल पर लघु वीडियो क्लिप और तस्वीरें अपलोड करें

आपका आभारी,

संलग्नक: ऊपर के रूप में

(अजय शिंदे)
युवा अधिकारी
कृते क्षेत्रीय निदेशक

प्रति : 1) राज्य एन.एस.एस.अधिकारी, महाराष्ट्र सरकार, मुंबई
2) खेल एवं युवा कार्यक्रम निदेशक-राज्य एन.एस.एस अधिकारी, गोवा सरकार, पंजिम

Scanned by TapScanner

अ.शा.पी.24-1/रासेयो/निदेशा/2022/289-305

भारत सरकार
युवा कार्यक्रम और खेल मंत्रालय
राष्ट्रीय सेवा योजना निदेशालय
शिवाजी स्टेडियम, नई दिल्ली

दिनांक: 21 अप्रैल ,2022

सेवा में,

समस्त क्षेत्रीय निदेशक
राष्ट्रीय सेवा योजना

विषय : साइबर जागरूकता दिवस सबंधी

महोदया/महोदय,

उपरोक्त सन्दर्भ में मंत्रालय के मेल दिनांक 2 अप्रैल 2022 के सन्दर्भ में गृह मंत्रालय के पत्र (संलग्न) में दिए गए दिशा निर्देशों के अनुसार आप अपने अधिकार क्षेत्र में आने वाली समस्त राष्ट्रीय सेवा योजना इकाइयों में हर महीने के प्रथम बुधवार को **साइबर जागरूकता दिवस** के रूप में आयोजित करना सुनिश्चित करें व गतिविधियों की रिपोर्ट उसी दिन सांयकाल 4:00 बजे तक अविलम्ब निदेशालय को भेजें। साथ ही आयोजित कार्यक्रमों को राष्ट्रीय सेवा योजना के सभी सोशल मीडिया माध्यमों पर अधिक से अधिक अपलोड करें।

भवदीय

करिश्मा राव 21/04/2022
कृते, (सहायक कार्यक्रम सलाहकार)

संलग्नक: यथोक्त

प्रतिलिपि-

निदेशक, राष्ट्रीय सेवा योजना, युवा कार्यक्रम और खेल मंत्रालय , नई दिल्ली

D.O. of Union Home Secretary addressed to Secretaries to Government of India for "Cyber Jaagrookta Diwas (CJD)"

From : Anu Krishnan <anu.krishnan@mha.gov.in> Sat, Apr 02, 2022 01:59 PM

Subject : D.O. of Union Home Secretary addressed to Secretaries to Government of India for "Cyber Jaagrookta Diwas (CJD)" 1 attachment

To : Sanjay Agarwal <secy-agri@nic.in>, Trilochan Mohapatra <dg.icar@nic.in>, Jatindranath Swain <secy-fisheries@nic.in>, Secretary Textiles <secy-textiles@nic.in>, secytour@nic.in, Lakshmi Naryain <secy-tribal@nic.in>, Mr Indevar Pandey <secy.wcd@nic.in>, SUJATA CHATURVEDI <secy-sports@nic.in>, SUJATA CHATURVEDI <secy-sports@nic.in>, Secretary Youth Affairs <secy-ya@nic.in>, Mr R Subrahmanyam <secywel@nic.in>, Ms. Anjali Bhawra <secretaryda-msje@nic.in>, Secretary NCSC <secretary-ncsc@nic.in>, chairman@isro.gov.in, Dr(Mr) G P Samanta <secretary@mospi.gov.in>, Shri V. Srinivas <secy-arpg@nic.in>, Secy PNG <sec.png@nic.in>, Office of Secretary Ports Shipping and Waterways <secyship@nic.in>, Shri Alok Kumar <secy-power@nic.in>, Mr Nagendra Nath Sinha <secyrd@nic.in>, Mr Ajay Tirkey <secy-dolr@nic.in>, tirkeyaj@iac.nic.in, SECRETARY DST <dstsec@nic.in>, Dr Rajesh S Gokhale <secy@dbt.nic.in>, DG CSIR <dg@csir.res.in>, Rajesh Aggarwal <secy-msde@nic.in>, Alok Tandon <secy-mines@nic.in>, Secretary(Minority Affairs) <secy-mma@nic.in>, Mr. Indu Shekhar Chaturvedi <secy-mnre@nic.in>, Mr Sunil Kumar <secy-mopr@nic.in>, Gyanesh Kumar <secympa@nic.in>, Ms. Vini Mahajan <secydws@nic.in>, O/o Secy Labour Employment <secy-labour@nic.in>, Pankaj Kumar <secy-jus@gov.in>, Sh. Anoop Kumar Mendiratta <secylaw-dla@nic.in>, secyoffice-dla@nic.in, Secretary LD <secyoffice-ld@gov.in>, Bidyut Behari Swain <secretary-msme@nic.in>, Manoj Joshi <secyurban@nic.in>, Apurva Chandra <secy.inb@nic.in>, Secretary DIPAM <secydivest@nic.in>, Shri Pankaj Kumar <secy-mowr@nic.in>, Mr Rajesh Bhushan <secyhfw@nic.in>, Prof. Balram Bhargava <balram.bhargava@gov.in>, Arun Goel <shioff@nic.in>, Shri Ali R. Rizvi <secy-dpe@nic.in>, Dr. Ausaf Sayeed <secycpv@mea.gov.in>, Shri Ajay Seth <secy-dea@nic.in>, T.V. Somanathan <secyexp@nic.in>, Shri Tarun Bajaj Secretary DOR <rsecy@nic.in>, Sanjay Malhotra <secy-fs@nic.in>, Secretary MoFPI <secy.mofpi@nic.in>, K. Sanjay Murthy <secy.dhe@nic.in>, Shri K. Rajaraman <secretary@meity.gov.in>, Ms Leena Nandan <secy-moef@nic.in>, SAURABH KUMAR <secyeast@mea.gov.in>, Dammu Ravi <secyer@mea.gov.in>, Sanjay Verma <secywest@mea.gov.in>, Shri B. Anand <secyesw@nic.in>, DEFENCE SECRETARY <defsecy@nic.in>, Mr Lok Ranjan <secydoner@nic.in>, Dr M Ravichandran <secretary@moes.gov.in>, Ms Anita Karwal <secy.sel@nic.in>, ROHIT KUMAR SINGH <secy-ca@nic.in>, Mr Sudhanshu Pandey <secy-food@nic.in>, Raj Kumar <sdpns@nic.in>, secy moca <secy.moca@nic.in>, Anil Kumar Jain <secy.moc@nic.in>, Commerce Secretary Office <csoffice@nic.in>, Secy DPIIT <secy-ipp@nic.in>, K Rajaraman <secy-dot@nic.in>, secretary-posts@indiapost.gov.in, chairman@dae.gov.in, RAJESH KOTECHA <secy-ayush@nic.in>, Office of Secretary (C&PC) <sec.cpc@nic.in>, Ms S. Aparna <secy-pharma@nic.in>, Secretary MCA <secy.mca@nic.in>, Govind Mohan <secy-culture@nic.in>

Cc : Ashok Kumar <diri4c@mha.gov.in>, Deepak Virmani

Secy (YA)
DTS No. 132935
Date... 5-4-22

DS (CDN)
05/4/22
US (CDN)
Pl. circulate.

JS (YA)
4/4/22
SUJATA CHATURVEDI IAS
Secretary (Youth Affairs)

126/CDN-YA/2022
6/4/2022

Sh Prakash
6/4

<deepak.virmani@gov.in>, HIMANSHU PANDE
<dgmi4c@mha.gov.in>, DEEPAK KUMAR
<deepakkumar7459@crpf.gov.in>

Sir/ Madam

Kindly find enclosed herewith the D.O. of Union Home Secretary addressed to Secretaries to Government of India for observing **"Cyber Jaagrookta (Awareness) Diwas (CJD)"** for necessary action by the Ministries concerned please. For any query / clarification, Ministries may kindly contact at **deepak.virmani@gov.in** Deputy Secretary (I4C).

Regards
Indian Cyber Crime Coordination Centre (I4C),
Ministry of Home Affairs,
5th Floor, NDCC-II Building, Jai Singh Road,
New Delhi
Phone No: - 011- 23438207/ 08

DO 02.04.2022 (1).pdf
9 MB

अजय भल्ला, भा.प्र.से.
AJAY BHALLA, IAS

सत्यमेव जयते

आज़ादी का अमृत महोत्सव

गृह सचिव
Home Secretary
भारत सरकार
Government of India
नॉर्थ ब्लॉक/North Block
नई दिल्ली/New Delhi

Secy (YA)
FTS No. 132935
Date 5-4-22
7-4-22

D.O.No. 22003/15/2019-I4C

30th March, 2022

Dear Secretary,

As you may be aware, the Ministry of Home Affairs has launched the Indian Cyber Crime Coordination Centre (I4C) to strengthen the capabilities of Law Enforcement Agencies (LEAs) and improve coordination among the LEAs and other agencies. The MHA has also launched the National Cyber Crime Reporting Portal (NCRP) to facilitate online reporting of cyber crime incidents. The analysis has revealed that 60% of the complaints are related to online financial frauds. Hence, the MHA has also rolled out the Citizen Financial Cyber Fraud Reporting & Management System (CFCFRMS), as a part of the NCRP for immediate reporting of financial frauds and also for stopping the siphoning off of the funds by fraudsters.

2. One of the key actions for preventing cyber crimes is to generate sustained awareness among public, especially among the vulnerable sections and groups on 'cyber hygiene'. The MHA has already requested all the States/UTs to observe the" **Cyber Jaagrookta (Awareness) Diwas (CJD)**"on the first Wednesday of every month in all the Schools/Colleges/Universities/Panchayati Raj Institutions (PRIs) and Municipalities.

3. I request you to issue instructions to all the offices, branches / sections, PSUs, etc., under your Ministry for celebrating the "Cyber Jaagrookta Diwas (CJD)" on the first Wednesday of every month, commencing April, 2022 onwards, and also to prepare an **"Annual Action Plan"** in this regard. It may be added that special emphasis may be given on capacity building of the employees to deal with the challenges of cyber crimes. Training Institutes under the aegis of your Ministry may be instructed to design "Course Curriculum", along with Hands-On-Training for all the trainees/officials/employees.

4. Budgetary provisions to carry out the CJD have to be met from the budget of the respective Ministry concerned. A write-up on the CJD is enclosed herewith as **Annexure I**. This initiative may be supplemented by mass awareness program through multiple media. The publicity material, prepared by the I4C, is enclosed herewith as **Annexure-II,** which may be utilized. The list of suggested topics to be taken up for imparting training by Institutions/Academies for employees is also enclosed as **Annexure-III.**

Already Sent

US (CDN)

..contd..p/2..

5. I would be grateful if suitable instructions are issued to the stakeholders concerned on organizing the CJD every month, commencing April, 2022 onwards.

With regards

Yours sincerely,

30/03/22

(Ajay Bhalla)

Encl.: as above

All Secretaries to the Government of India.
(as per Standard List)

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 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)
- 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.

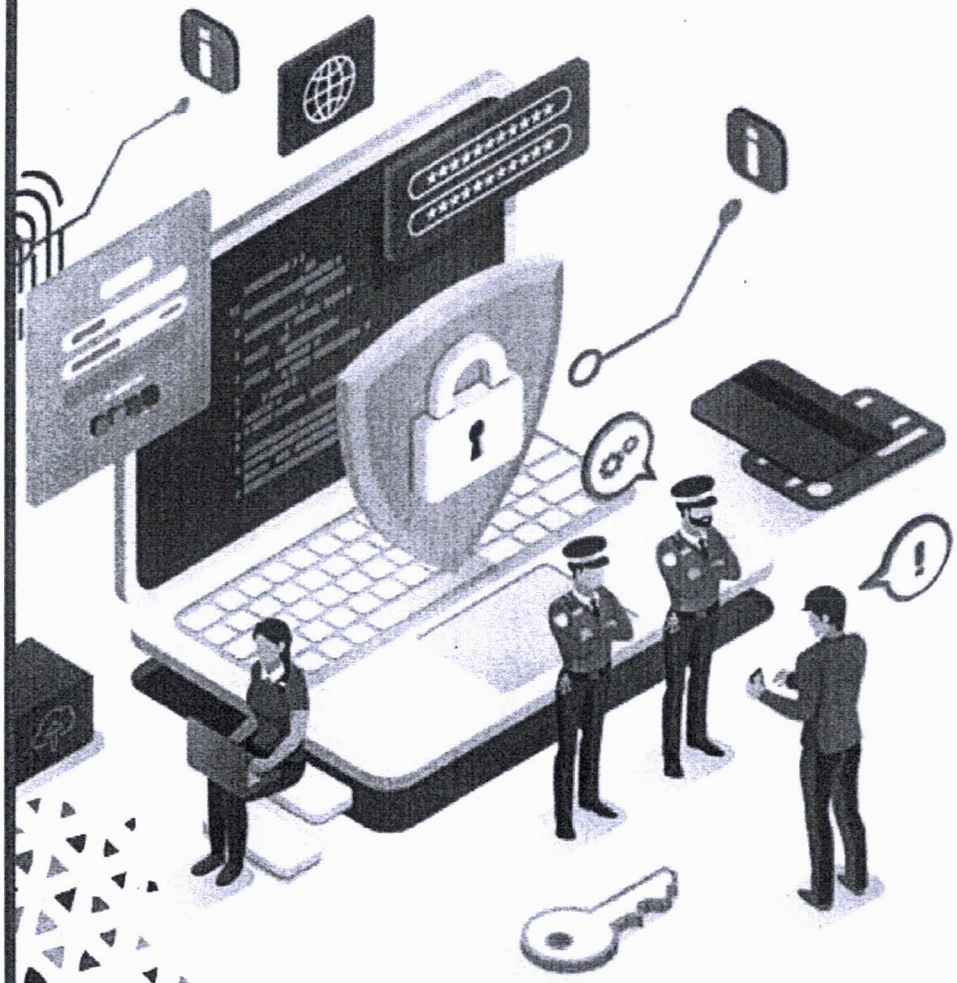
Annual Action Plan

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 II

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS



Report Cybercrimes at

cybercrime.gov.in

or

Call

1930

(Earlier 155260)

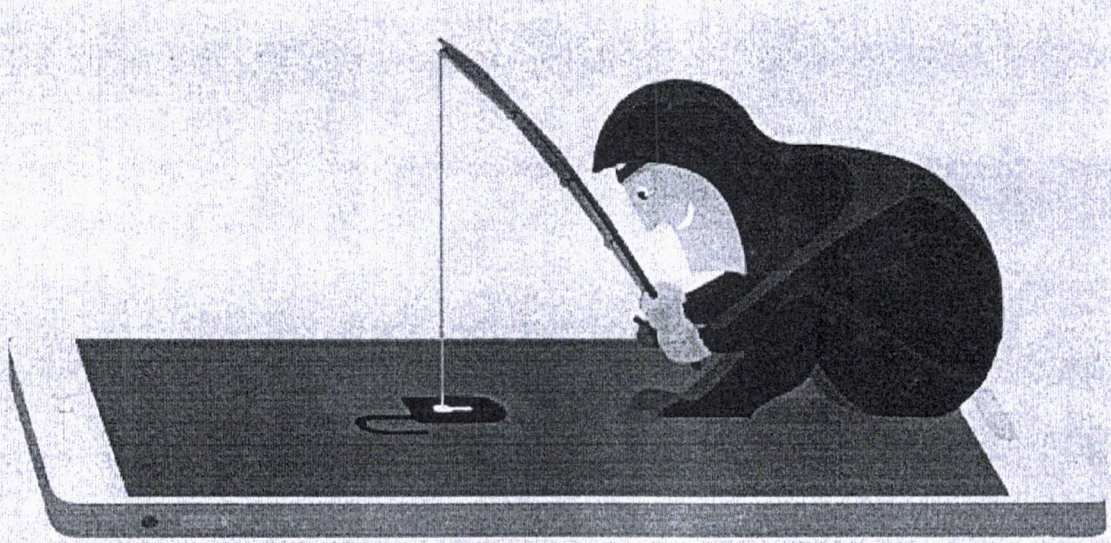
For Assistance

@CyberDostI4C @cyberdosti4c @cyberdost @cyberdosti4c @cyberdost.i4c @cyberdosti4c

Note: All the complaints are handled by respective State/UT Police, as per their jurisdiction

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

ARE YOU A VICTIM OF CYBER CRIME



REPORT ANY CYBERCRIME AT CYBERCRIME.GOV.IN OR DIAL 1930 (EARLIER 155260) FOR ASSISTANCE

Follow us on:

@CyberDost14C . @cyberdosti4c @cyberdost @cyberdosti4c @cyberdost.i4c @cyberdosti4c

Note: All the complaints are handled by respective State/UT Police, as per their jurisdiction

MINISTRY OF HOME AFFAIRS | I4C

ARE YOU A VICTIM OF CYBER CRIME ?

REPORT ANY CYBERCRIME AT CYBERCRIME.GOV.IN

OR

DIAL 1930 (EARLIER 155260) FOR ASSISTANCE

Follow us on:

@CyberDostI4C @cyberdosti4c @cyberdost @cyberdosti4c @cyberdost.i4c @cyberdosti4c

Note: All the complaints are handled by respective State/UT Police, as per their jurisdiction

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

सत्यमेव जयते

Report Cybercrimes at

cybercrime.gov.in

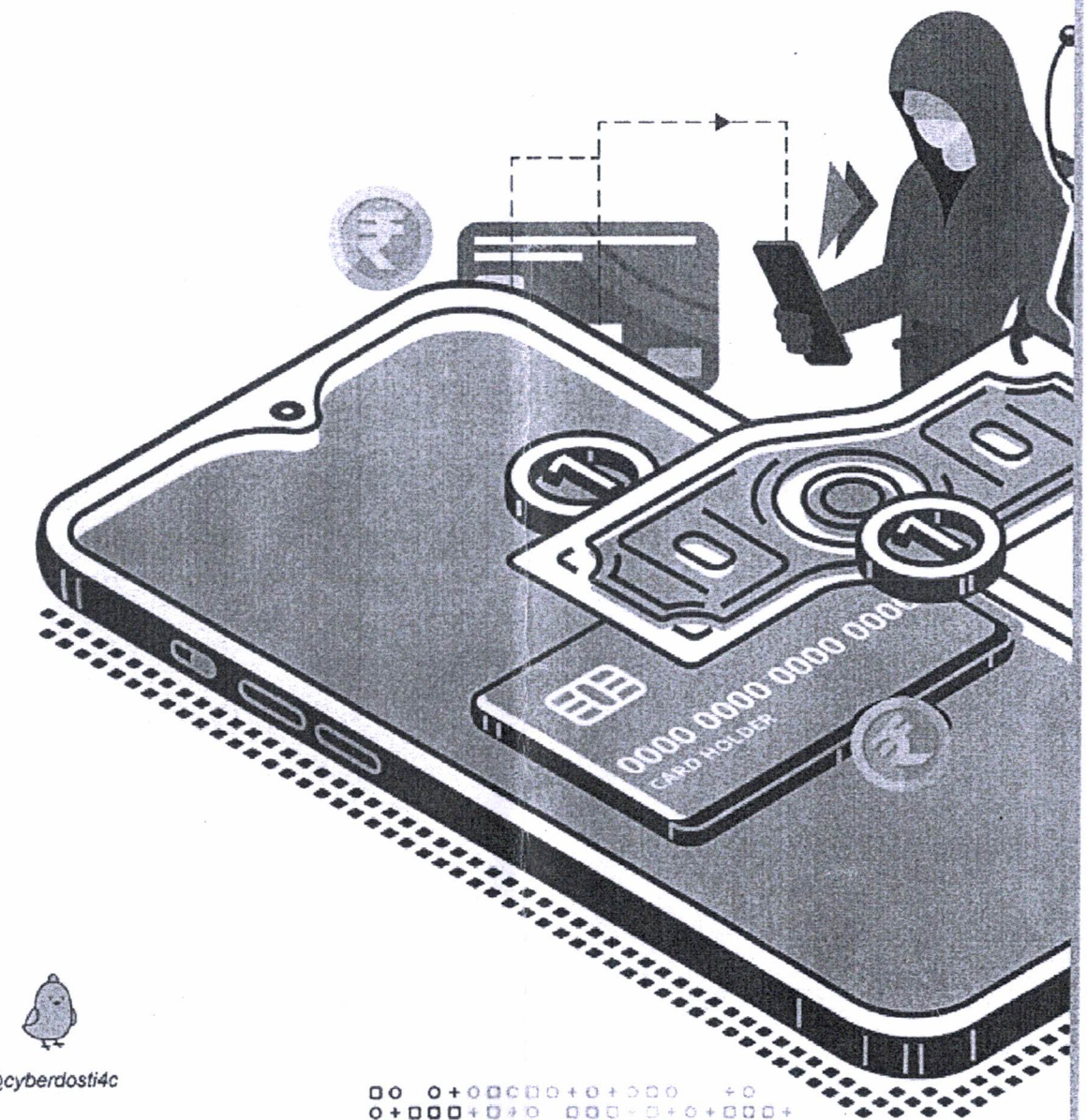
or

Call

1930

(Earlier 155260)

For Assistance



@CyberDostI4C @cyberdosti4c @cyberdost @cyberdosti4c @cyberdost.i4c @cyberdosti4c

Note: All the complaints are handled by respective State/UT Police, as per their jurisdiction

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Report any Cybercrime at

cybercrime.gov.in

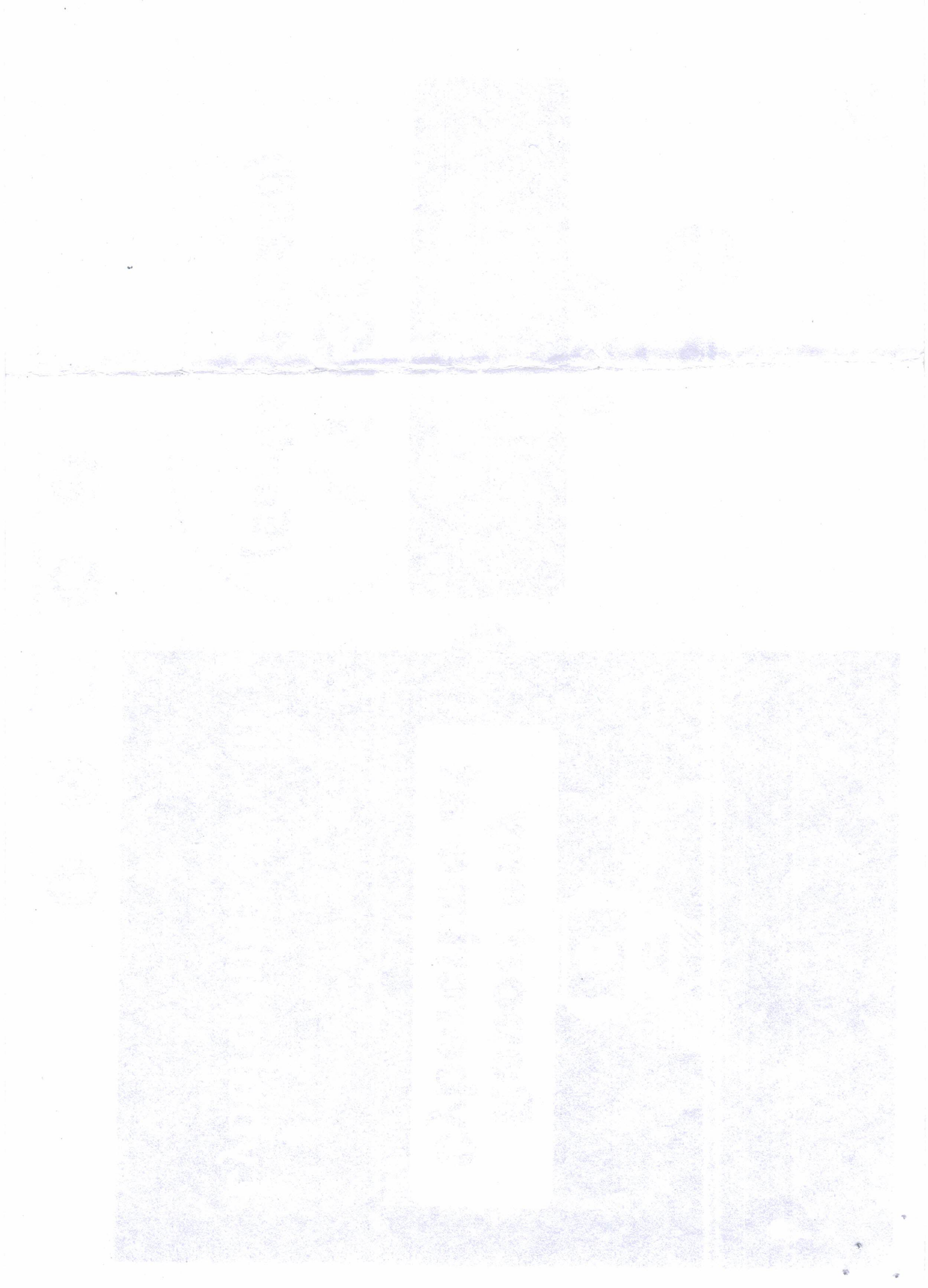
or

For any Assistance

1930
(Earlier 155260)

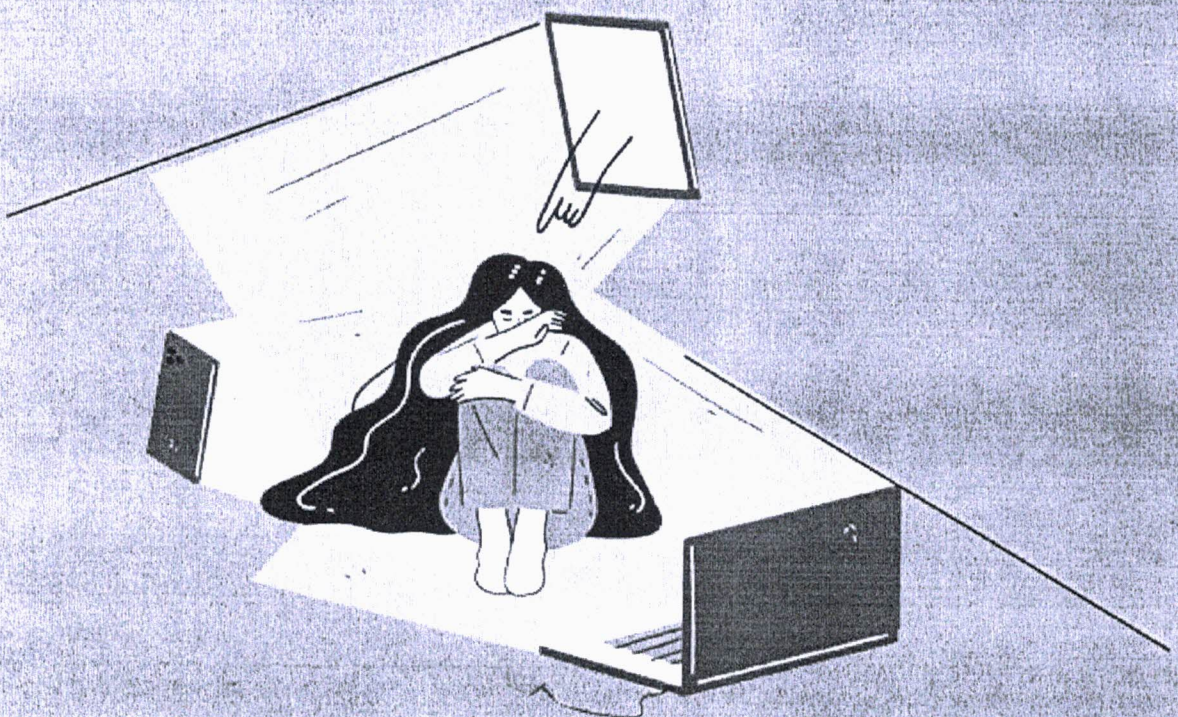
@CyberDostI4C @cyberdosti4c @cyberdost @cyberdosti4c @cyberdost.i4c @cyberdosti4c

Note: All the complaints are handled by respective State/UT Police, as per their jurisdiction



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

ARE YOU A VICTIM OF CYBER CRIME



REPORT ANY CYBERCRIME AT
CYBERCRIME.GOV.IN
OR
DIAL 1930 (EARLIER 155260)
FOR ASSISTANCE

Follow us on:

@CyberDostI4C @cyberdosti4c @cyberdost @cyberdosti4c @cyberdost.i4c @cyberdosti4c

Note: All the complaints are handled by respective State/UT Police, as per their jurisdiction

Annexure-III

LIST OF SUGGESTED TOPICS TO BE COVERED BY VARIOUS INSTITUTIONS/ ACADEMIES FOR TRAINEE OFFICERS/OFFICIALS

UNIT I: Electronics Payments and safeguards therein

i. Concept of E payments
ii. ATM and Tele Banking
iii. Immediate Payment Systems
iv. Mobile Money Transfer and E-Wallets
v. Unified Payment Interface
vi. Cybercrimes in Electronic Payments
vii. Precautions in Electronics Money Transfer
viii. RBI Guidelines of Customer Protection in Unauthorized Banking Transactions
ix. KYC: Concept, cases, and safeguards

UNIT II: Cyber Crimes and safety

i. Introduction to cybercrimes
i. Kinds of cybercrimes: phishing, identify theft, cyber stalking, cyber terrorism, cyber obscenity, computer vandalism, Ransomware, Identity Theft
ii. Forgery and fraud from Mobile Devices
iii. Cyber risk associated with varied online activities and protection therefrom.
iv. Work on different digital platforms safely
v. Online cybercrimes against women and impersonation scams
vi. Security awareness on Wearable gadgets
vii. Safety in Online Financial transactions
viii. Concept and use of Cyber Hygiene in daily life, Browser Security, Wi-Fi Security, UPI Security, Juice Jacking, Google Map Security, OTP fraud, IOT Security, E-mails.
ix. Reporting of Cyber crime

UNIT III: Introduction to Social Networks

i. Social Network and its contents, blogs
ii. Safe and Proper use of Social Networks
iii. Inappropriate Content on Social Networks
iv. Flagging and reporting of inappropriate content
v. Laws regarding posting of inappropriate content

UNIT IV: Introduction to Information and Technology Act, 2000(IT Act), The Indian Wireless Telegraphy Act and their use in Cyber Space

i. Concepts as defined in IT Act and The Indian Wireless Telegraphy Act
ii. Communication Device
iii. Computer, Cyber Security, Data Security
iv. Secure System
v. Basic concepts of Block Chain, 5G, IoT, Drones, AI etc.