

TRIFED, Ministry of Tribal Affairs, Govt. of India
Celebrating
Cyber Jaagrookta Diwas



Cyber Jaagrookta (Awareness) Diwas

An Initiative by The Ministry of Home Affairs

(D.O.No. 22003/15/2019-14C, Date- 30th March 2022)

www.kratikal.com



“आज का संकल्प, कल की सुरक्षा ”

- ❖ TRIFED Annual Action Plan on Cyber Jaagrookta Awareness 2022-23
- ❖ Ministry of Home Affairs , Govt. of India's Guidelines issued on Cyber Jaagrookta Awareness
- ❖ Cyber Security Guidelines for Government Servant

Cyber awareness

(Internet has become one of the integral part of our daily life. It has transformed the way we communicate, make friends, share updates, play games , and shop. They are impacting most aspects of our day-to-day life. Cyberspace connects us virtually with crores of online users across the globe. With increasing use of cyberspace, cybercrimes are also increasing rapidly. To stay safe in the online world, it is important to follow some cyber safe practices which may help in making our online experience productive

- ✓ **Do not click on unverified links**
- ✓ **Cautious while accepting friend requests from strangers online**
- ✓ **Do not share your OTP/ATM/UPI PIN with anyone**
- ✓ **Be vigilant of tempting offers on social media**
- ✓ **Report cybercrime at :-**
<https://cybercrime.gov.in/>

Business Email Compromise(BEC)

(BEC is when a fraudster hacks into an e-mail account and impersonates the real owner to defraud the company, its customers, partners, and /or employees. This may be used to send sensitive data, forged payment invoices or malicious documents.

Safety Tips.....

- ✓ **Enable multi-factor authentication for all email accounts.**
- ✓ **Flag differences in “reply” and “from” email addresses.**
- ✓ **Enable security features that block malicious emails.**
- ✓ **Do not share personal information**

How to prevent ONLINE FINANCIAL FRAUDS

- ✓ **Never disclose your net banking password, One-Time Password(OTP), ATM or phone banking PIN, CVV number, expiry date to anyone.**
- ✓ **Do not make financial transactions over shared public computers or while using public Wi-Fi networks.**
- ✓ **Use strong password for your online banking accounts and change them periodically.**

- ✓ **Always use virtual keyboards while logging into online banking services**
- ✓ **Always delete the browsing data of your web browser after completing your online banking activity**
- ✓ **Always review transaction alerts received on your registered mobile number and reconcile them with the amount of your purchase.**

“Be Vigilant, Be Cyber Safe”

APPENDIX

“आज का संकल्प, कल की सुरक्षा ”

**Annual Action Plan – 2022-23
for Celebration of ‘Cyber Jaagrookata (Awareness) Diwas
(on every 1st Wednesday of the month)**

Sr.No.	Month	Activity	Participation/ Involvement
1.	October,2022	Creating a webpage on Cyber Jaagrookta Diwas – Cyber Awareness on TRIFED website (www.trifed.tribal.gov.in) by Consultant	
2.	November,2022	“Pledge Ceremony” the pledge taking ceremony against cyber crime (By Digitization Div)	All employees of TRIFED (HO, RO, Tribes India Showrooms) (on-line mode)
3.	December,2022	Webinar on “Cyber Awareness” (Experts from relevant Govt. agencies will be invited)	All employees of TRIFED (HO, RO, Tribes India Showrooms) (on-line mode)
4.	January,2023	Quiz competition on Cyber Jaagrookta Diwas (By Digitization Div)	All employees of TRIFED (HO, RO, Tribes India Showrooms)
5.	February,2023	Session on Electronic Payments through Credit Card, Debit Card, Cowin App etc.and Safegaurd therein (IFD Officials of HO will lead the session)	All employees of TRIFED (HO, RO, Tribes India Showrooms)
6.	March,2023	Session on Security of personal computer and emails, whatsapp, mobile etc. (Experts from relevant Govt. agencies will be invited)	All employees of TRIFED (HO, RO, Tribes India Showrooms)

CYBER SECURITY GUIDELINES FOR GOVERNMENT EMPLOYEES

LIST

1. SCOPE AND TARGET AUDIENCE	2
2. DESKTOP/LAPTOP AND PRINTER SECURITY AT OFFICE	2
3. PASSWORD MANAGEMENT	3
4. INTERNET BROWSING SECURITY	3
5. MOBILE SECURITY	4
6. EMAIL SECURITY	5
7. REMOVABLE MEDIA SECURITY	6
8. SOCIAL MEDIA SECURITY	6
9. SECURITY ADVISORY AND INCIDENT REPORTING	7
10. CYBER SECURITY RESOURCES	7
11. COMPLIANCE	8

1. Scope and Target Audience

The following guidelines are to be adhered to by all government employees, including outsourced/contractual/temporary employees, who work for government Ministry/Department.

2. Desktop/Laptop and Printer Security at Office

- a. Use only Standard User (non-administrator) account for accessing the computer/laptops for regular work. Admin access to be given to users with approval of CISO only.
- b. Set BIOS Password for booting.
- c. Ensure that the Operating System and BIOS firmware are updated with the latest updates/patches.
- d. Set Operating System updates to auto-updated from a trusted source.
- e. Ensure that the Antivirus client installed on your systems are updated with the latest virus definitions, signatures and patches.
- f. Only Applications/software's, which are part of the allowed list authorized by CISO, shall be used; any application/software which is not part of the authorized list approved by CISO, shall not be used.
- g. Always lock/log off from the desktop when not in use.
- h. Shutdown the desktop before leaving the office.
- i. Keep printer's software updated with the latest updates/patches.
- j. Setup unique pass codes for shared printers.
- k. Internet access to the printer should not be allowed.
- l. Printer to be configured to disallow storing of print history.
- m. Enable Desktop Firewall for controlling information access.
- n. Keep the GPS, Bluetooth, NFC and other sensors disabled on the desktops /laptops and mobile phones. They may be enabled only when required.

- o. Use a Hardware VPN Token for connecting to any IT Assets located in Data Centre.

3. Password Management

- a. Use complex passwords with a minimum length of 8 characters, using a combination of capital letters, small letters, numbers and special characters.
- b. Change passwords at least once in 30 days.
- c. Use Multi-Factor Authentication, wherever available.
- d. Don't use the same password in multiple services/websites/apps.
- e. Don't save passwords in the browser or in any unprotected documents.
- f. Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on your table).
- g. Don't share system passwords or printer pass code or Wi-Fi passwords with any unauthorized persons.

4. Internet Browsing Security

- a. While accessing Government applications/services, email services or banking/payment related services or any other important application/services, always use Private Browsing/Incognito Mode in your browser.
- b. While accessing sites where user login is required, always type the site's domain name/URL, manually on the browser's address bar, rather than clicking on any link.
- c. Use the latest version of the internet browser and ensure that the browser is updated with the latest updates/patches.
- d. Don't store any usernames and passwords on the internet browser.

- e. Don't store any payment related information on the internet browser.
- f. Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies etc).
- g. Don't use any 3rd party toolbars (ex: download manager, weather tool bar, ask me tool bar etc.) in your internet browser.
- h. Don't download any unauthorized or pirated content /software from the internet (ex: pirated - movies, songs, e-books, software's).
- i. Don't use your official systems for installing or playing any Games.
- j. Observe caution while opening any shortened URLs (ex: tinyurl.com/ab534/). Many Malwares and phishing sites abuse URL shortener services. Such links may lead to a Phishing/malware webpage, which could compromise your device.

5. Mobile Security

- a. Ensure that the mobile operating system is updated with the latest available updates/patches.
- b. Don't root or jailbreak your mobile device. Rooting or Jail breaking process disables many in-built security protections and could leave your device vulnerable to security threats.
- c. Keep the Wi-Fi, GPS, Bluetooth, NFC and other sensors disabled on the mobile phones. They may be enabled only when required.
- d. Download Apps from official app stores of Google (for android) and apple (for iOS).
- e. Before downloading an App, check the popularity of the app and read the user reviews.
- f. Observe caution before downloading any apps which has a bad reputation or less user base etc.
- g. While participating in any sensitive discussions, switch-off the mobile phone or leave the mobile in a secured area outside the discussion room.

- h. Don't accept any unknown request for Bluetooth pairing or file sharing.
- i. Before installing an App, to carefully read and understand the device permissions required by the App along with the purpose of each permission.
- j. In case of any disparity between the permissions requested and the functionality provided by an app, users to be advised not to install the App (Ex: A calculator app requesting GPS and Bluetooth permission).
- k. Note down the unique 15-digit IMEI number of the mobile device and keep it offline. It can be useful for reporting in case of physical loss of mobile device.
- l. Use auto lock to automatically lock the phone or keypad lock protected by pass code/ security patterns to restrict access to your mobile phone.
- m. Use the feature of Mobile Tracking which automatically sends messages to two preselected phone numbers of your choice which could help if the mobile phone is lost/ stolen.
- n. Take regular offline backup of your phone and external/internal memory card.
- o. Before transferring the data to Mobile from computer, the data should be scanned with Antivirus having the latest updates.

6. Email Security

- a. Ensure that Kavach Multi-Factor Authentication is configured on the NIC Email Account.
- b. Download Kavach app from valid mobile app stores only. Do not download from any website.
- c. Do not share the email password or Kavach OTP with any unauthorized persons.
- d. Don't use any unauthorized/external email services for official communication.

- e. Don't click/open any link or attachment contained in mails sent by unknown sender.
- f. Regularly review the past login activities on NIC's Email service by clicking on the "login history" tab. If any discrepancy is observed in the login history, then the same should be immediately reported to NIC-CERT.
- g. Use Pretty Good Privacy (PGP) or digital certificate to encrypt e-mails that contains important information.
- h. Observe caution with documents containing macros while downloading attachments, always select the "disable macros" option and ensure that protected mode is enabled on your office productivity applications like MS Office.

7. Removable Media Security

- a. Perform a low format of the removable media before the first-time usage.
- b. Perform a secure wipe to delete the contents of the removable media.
- c. Scan the removable media with Antivirus software before accessing it.
- d. Encrypt the files /folders on the removable media.
- e. Always protect your documents with strong password.
- f. Don't plug-in the removable media on any unauthorized devices.

8. Social Media Security

- a. Limit and control the use/exposure of personal information while accessing social media and networking sites.
- b. Always check the authenticity of the person before accepting a request as friend/contact.
- c. Use Multi-Factor authentication to secure the social media accounts.
- d. Do not click on the links or files sent by any unknown contact/user.
- e. Do not publish or post or share any internal government documents or information on social media.

- f. Do not publish or post or share any unverified information through social media.
- g. Do not give share the @gov.in /@nic.in email address on any social media platform.
- h. It is recommended to use NIC's Sandes App instead of any 3rd party messaging app for official communication.

9. Security Advisory and Incident Reporting

- a. Adhere to the Security Advisories published by NIC-CERT (<https://niccert.nic.in>) and CERT-In (<https://www.cert-in.org.in>).
- b. Report any cyber security incident, including suspicious mails and phishing mails to NIC-CERT (incident@nic-cert.nic.in) and CERT-In (incident@cert.org.in).

10. Cyber Security Resources

The following resources may be referred for more details regarding the cyber security related notifications/information published by Government of India:

Sl. No.	Resource URL	Description
1.	https://www.meity.gov.in/cybersecuritydivision	Laws, Policies & Guidelines
2.	https://www.cert-in.org.in	Security Advisories, Guidelines & Alerts
3.	https://nic-cert.nic.in	Security Advisories, Guidelines & Alerts
4.	https://www.csk.gov.in	Security Tools & Best Practices
5.	https://infosecawareness.in	Security Awareness materials
6.	http://cybercrime.gov.in	Report Cyber Crime, Cyber Safety Tips

11. Compliance

All government employees, including temporary, contractual/outsourced resources are required to strictly adhere to the guidelines mentioned in this document.

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



सत्यमेव जयते

75
आज़ादी का
अमृत महोत्सव

54
गृह सचिव
Home Secretary
भारत सरकार
Government of India
गॉर्थ ब्लॉक/North Block
नई दिल्ली/New Delhi

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**.

..contd..p/2..

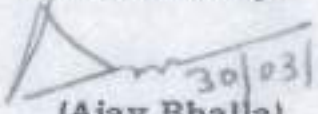
::2::

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

Encl.: as above

Yours sincerely,


30/03/22
(Ajay Bhalla)

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

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 disposal 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. 51

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

- 50
- 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)

- 49
- 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.



ARE YOU A VICTIM OF CYBER CRIME



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

Follow us on:



@CyberDost4C



@cyberdost4c



@cyberdost



@cyberdost4c



@cyberdost_4c



@cyberdost4c

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

ARE YOU A VICTIM OF CYBER CRIME



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

Follow us on:



@CyberDost4C



@cyberdost4c



@cyberdost



@cyberdost4c



@cyberdost4c



@cyberdost4c

ARE YOU A VICTIM OF CYBER CRIME



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

Follow us on:



@CyberDost4C



@cyberdost4c



@cyberdost



@cyberdost4c



@cyberdost4c



@cyberdost4c

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

1/6



45



**Report any
Cybercrime at**

cybercrime.gov.in

or



**For any
Assistance**

**1930
(Earlier 155260)**



@CyberDrama



@cyberdrama



@cyberdram



@cyberdram



@cyberdram



@cyberdram

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



**Report
Cybercrimes at
cybercrime.gov.in**

**or
Call
1930
(Earlier 155260)
For Assistance**



Note: All the complaints are handled by respective States/T. Police, as per their jurisdiction

43



**Report
Cybercrimes at**
cybercrime.gov.in

**or
Call
1930
(Earlier 155260)
For Assistance**



@CyberDust4C @cyberdust4c @cyberdust @cyberdust4c @cyberdust4c @cyberdust4c

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



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
- ii. Kinds of cybercrimes: phishing, identify theft, cyber stalking, cyber terrorism, cyber obscenity, computer vandalism, Ransomware, Identity Theft
- iii. Forgery and fraud from Mobile Devices
- iv. Cyber risk associated with varied online activities and protection therefrom.
- v. Work on different digital platforms safely
- vi. Online cybercrimes against women and impersonation scams
- vii. Security awareness on Wearable gadgets
- viii. Safety in Online Financial transactions
- ix. 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.
- x. 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.