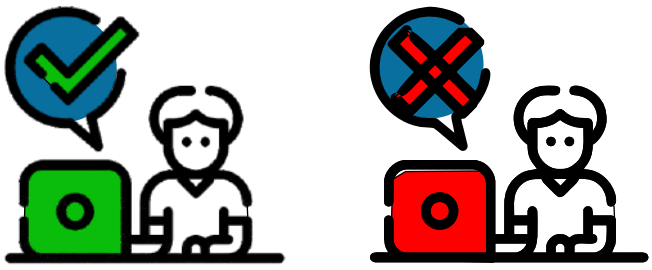
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

CYBER HYGIENE

FOR CYBER SPACE

Dos & Don'ts



ADVANCED

Published by:
Indian Cyber Crime Coordination Centre (I4C)
Cyber and Information Security (CIS) Division
Ministry of Home Affairs
Government of India
North Block
New Delhi – 110001

Introduction

Cyber space is a complex and dynamic environment of interactions among people, software and services supported by worldwide distribution of Information and Communications Technology (ICT) devices and networks. The exponential increase in the number of internet users in India clubbed with rapidly evolving technologies has brought in its own unique challenges.

Indian Cyber Crime Coordination Centre (I4C) under Cyber & Information Security (CIS) Division of the Ministry of Home Affairs, has prepared this manual to disseminate Cyber Hygiene Best Practices for the benefit of Industrial Bodies/General Public/Government Officials. This should not be considered as an exhaustive list of precautions for Cyber Hygiene but baseline precautions that are to be taken.

CONTENTS

1. General Computer Usage---------- 5

2. General Internet Safety Precautions----------10

3. USB Device Security----------14

4. Password Security Management----------17

5. Social Engineering-Trust but Verify----------23

6. Mobile Phones /Tabs----------27

7. Incident Response----------34

8. Organizational Level Security Controls----------36

9. Malware Defence----------40

10. Email Security Practices----------45

INTRODUCTION

Information Technology has made a significant contribution and impact on socio-economic scenarios. Rapid adoption of digital technology has led to employment generation, ease of living, ease of doing business and access to information.

Adoption of digital technology and internet have also led to increase in cyber crime incidents. It can be controlled or minimized with care, precaution, awareness and with the use of appropriate tools to secure the information. The tips and recommendations provided in this document may help the user to keep the information/data & device secure.

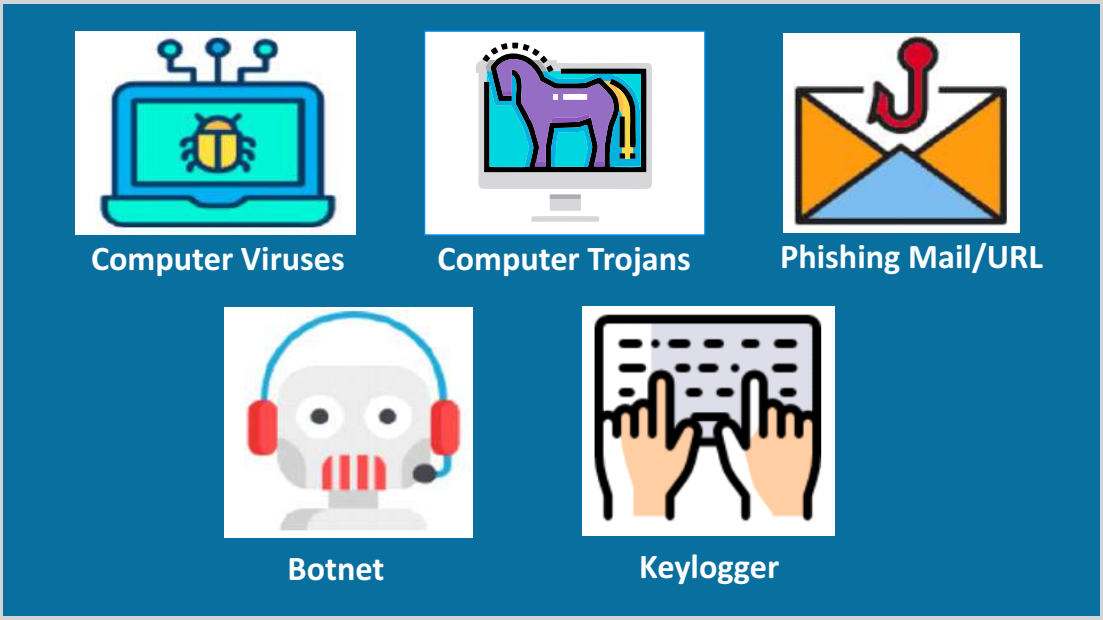
GENERAL COMPUTER USAGE

What is computer security?

Computer security is the protection of computer systems and information from theft and unauthorized access. It is the process of prevention and detection of unauthorized use of the computer systems.

Computer security threats

Computer security threats are possible dangers that can cause impediment to the normal functioning of the computer. Some of the common and harmful computer threats are depicted below:-



Dos

GENERAL COMPUTER USAGE

Always download applications/ software from trusted sources

Regularly update Operating System, Application and Anti-Virus software of the system

Ensure backup of important data/files/ documents at regular intervals

Lock the computer screen when not in use

Always keep the computer firewall “ON”

Dos

GENERAL COMPUTER USAGE

- Use account with limited privileges on systems
- Always insist on using genuine/ licensed software applications
- Scan all the files/contents downloaded from websites, e-mails or USBs
- Uninstall unnecessary programs or software

Dos

GENERAL COMPUTER USAGE

- Use “Task Manager” to identify any unwanted programs running on computer system
- Access to servers should be allowed via Multi-Factor Authentication (MFA)
- Disable Remote Desktop Connection and network file sharing , when not in use
- Set operating system update settings to “Auto-Download” option for regular updates

Don'ts

GENERAL COMPUTER USAGE

- Do not install or use pirated copies of software /applications under any circumstances. These may contain malware
- Do not use guessable/weak passwords like “password@123", etc.
- Do not click on untrusted/unexpected Pop-Up advertisements/ programs
- Do not dispose computer or hard drive without wiping and deletion of data

GENERAL INTERNET SAFETY PRECAUTIONS

Invention of internet has revolutionized the way of communication and information sharing. However, unsecured usage of internet may pose risks to an organization. Internet security includes browser security, website security, network security, software applications, etc. Its objective is to enforce rules and measures against attacks over the internet.

Unsafe internet practices may lead to risks from phishing, online viruses, trojans, worms, ransomware, business email compromise, financial loss, etc.

Dos

GENERAL INTERNET SAFETY PRECAUTIONS

Be vigilant while clicking/ downloading from suspicious links/ URLs

Make it a habit of clearing browser history after confidential activities/ transactions

Cloud storage to be used with appropriate security/ privacy settings

Verify the Authenticity and Identity of social media profiles before getting involved in any correspondence

Judiciously use services that require location information. Also, avoid posting photos with GPS-coordinates

Dos

GENERAL INTERNET SAFETY PRECAUTIONS

Be vigilant and verify the advertisements/ sponsored contents on search results or websites

Use File Sharing with appropriate security settings

Use strong or secure internet/ wireless protocols inside the organization

Don'ts

GENERAL INTERNET SAFETY PRECAUTIONS

Do not use any public computer or Wi-Fi for carrying out financial transactions like online shopping, internet banking, UPI transaction, etc.

Do not use e-mail address, phone number and details of payment cards on untrusted and unsecured websites

Do not trust and share unverified content on social media and messaging apps.

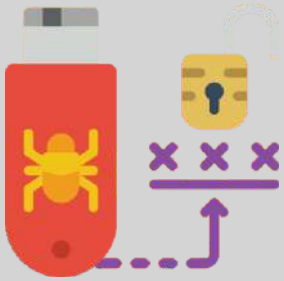
Always verify the source and authenticity of content before sharing

USB DEVICE SECURITY

USB devices are very convenient to transfer data between different computers. One can plug it into a USB port, transfer important data, remove and use it appropriately as desired. However, this portability, convenience and popularity also bring different threats to the information system.

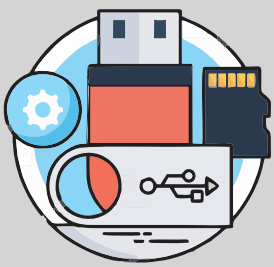
Threats

Unsecured use of USB drive can lead to data thefts, data leakages and malware infection. USB security can be ensured with care, awareness and by using appropriate scanning tools to secure the information.



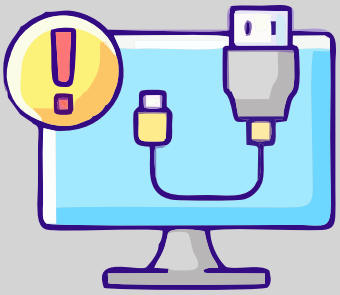
Types of devices which support USB

- Flash Drive/ Pendrive
- Portable Hard Drive/ SSD
- Mobile Phone



- Digital Camera
- Card Reader
- USB Keyboard/ Mouse

Dos



USB DEVICE SECURITY

Scan USB device with Antivirus/ Endpoint Protection before its use

All media must be stored in a safe and secure environment

Maintain records/ inventory of USB storage devices

Use only official USB storage devices for official work.

Ensure USB drive is encrypted and password protected

Autorun/ Autoplay feature shall be disabled in all the computers, while using USB

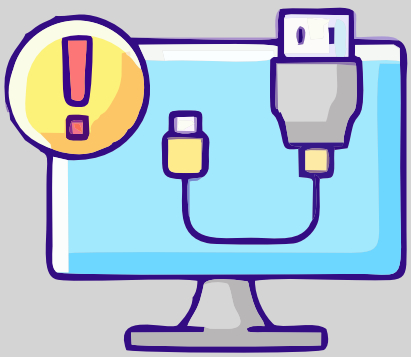
Don'ts

USB DEVICE SECURITY

Do not plug rogue USB devices

(Someone gives a USB drive or other electronic media that is preloaded with a malware in the hope of its use in the device which enable hackers to hack the computer)

Do not allow USB storage/ removable media devices in organization, unless it is essential



PASSWORD SECURITY MANAGEMENT

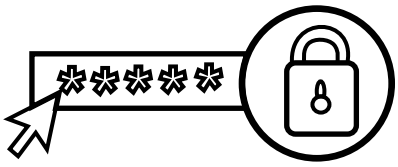
Password helps in protection of information accessible via computers. It allows access to information only to authorised users. Strong multi character passwords must be enforced in all the systems.

Password attack

Cyber criminals use many methods to access accounts, including dictionary brute-force attack (attacks made to guess passwords), as well as comparing various word combinations against a dictionary file.

Cyber criminals may also use password capturing tools like “Keyloggers” on victim’s computer.

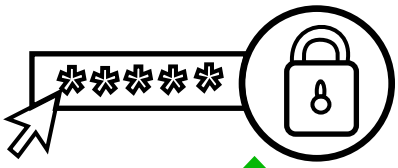
Dos



PASSWORD SECURITY MANAGEMENT

- Always use different passwords for different accounts. Ensure password is strong
- Strong passwords should contain combination of upper case, lower case, numbers,"Special" characters (e.g., @#$%^&*()_+|~-=\'{}[]: ";<>/, etc.)
- Immediately, change any password which might have been shared or revealed by mistake
- Passwords must be changed at regular intervals

Dos



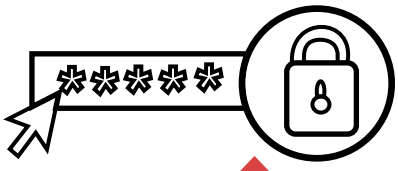
PASSWORD SECURITY MANAGEMENT

- Organization must store passwords in hash format rather than plain text
- Use Multi-Factor Authentication (MFA) for access to critical systems, accounts, etc.
- Password history settings should be enforced, wherever possible

A PASSWORD SHOULD NOT CONTAIN

- Birth dates, names, ID proofs and other personal information such as addresses and phone numbers
- Commonly used words such as names of family members, pets, friends, colleagues, movie/novel/comics characters, etc.
- Password recovery answers should not be guessable
- Password should not be less than eight characters

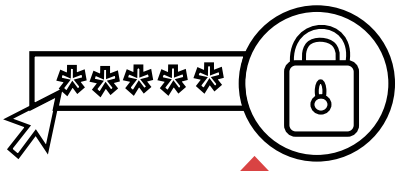
Don'ts



PASSWORD SECURITY MANAGEMENT

- Do not use public systems to access banking/ sensitive sites
- Do not share password, OTP through e-mail, chat or any other electronic communication
- Do not reveal password on questionnaires or security forms

Don'ts



PASSWORD SECURITY MANAGEMENT

- Do not choose/ select "remember my password" option for banking/ sensitive sites
- Never write down your password anywhere, especially as a 'note stick' to the computer
- Don't use your biometrics (finger print, etc.) at untrusted terminals/ places

SOCIAL ENGINEERING-TRUST BUT VERIFY

Social engineering, in the context of information and cyber security, is a broad range of malicious activities through human interactions. Psychological manipulation are used to trick users to obtain sensitive information or for making security mistakes.

Malicious social engineering activities and techniques may be used to gain access to information through misrepresentation. It is conscious manipulation of people for obtaining information without realizing that a security breach is occurring. It may take the form of impersonation via telephone or in person and through email.

Social Engineering attacks can lead to :-

- Financial Frauds
- Malware Attacks
- Phishing Attacks
- Account take over
- Critical infrastructure attacks,etc.

Dos

SOCIAL ENGINEERING-TRUST BUT VERIFY

Social Engineering tactics usually tend to create a sense of urgency.
If you are unsure about the legitimacy of an e-mail/SMS, verify it by contacting the company/ source directly

Dos

SOCIAL ENGINEERING-TRUST BUT VERIFY

Periodically carry out the phishing simulation exercise in the organization

Pay attention to the URL of a website.

Malicious website may look identical to a legitimate site but the URL may use a variation in spelling or a different domain

e.g:-
Correct- email.gov.in
Incorrect- email-gov.in

Use Anti-phishing feature offered by email security solution

Don'ts

SOCIAL ENGINEERING-TRUST BUT VERIFY

Do not open an attachment in an email from unknown senders, as these may contain malicious virus to harm the computer

Do not respond to unsolicited phone calls/SMS, visits or e-mail message from unknown individuals asking about employees or other internal information

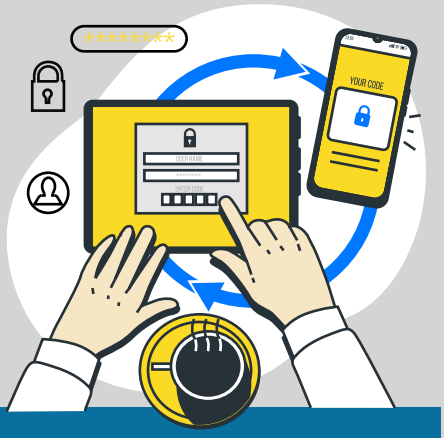
Do not share confidential information on social media platforms/ public forums

MOBILE PHONE/TABS

Mobile phones are integral part of any organization. Secure usage of phone is essential for personal and organizational data protection.

Data theft, financial loss, unauthorized access, malware infection, etc., may be a result of mobile phone compromise.

Dos



MOBILE PHONE/TABS

Be cautious with public Wi-Fi

Information shared over public network may be misused

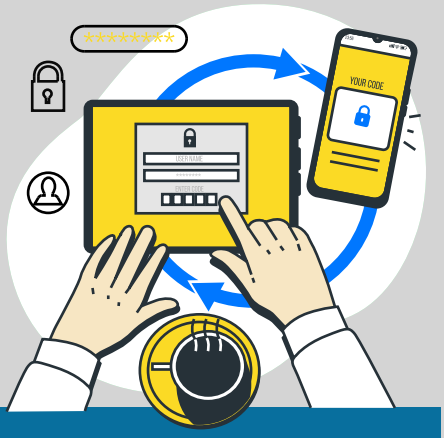
Review the default privacy settings of the smartphone, mobile applications and social media accounts

Personal photos posted on social media with public visibility may be misused

Before downloading any App, same should be checked for its reputation/ authenticity

Read vendor privacy policies and verify app permission before downloading apps

Dos



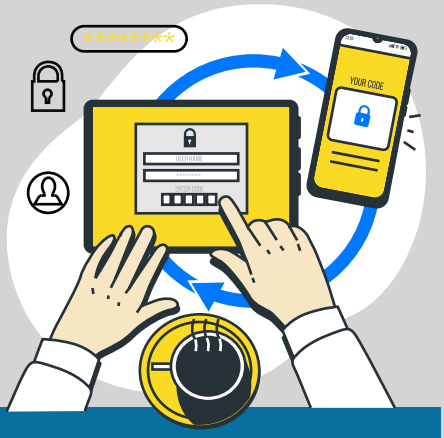
MOBILE PHONE/TABS

Turn off GPS/ Bluetooth location services when not needed

Turn off / remove unnecessary apps

Use Mobile Device Management (MDM) Solutions for official phones to ensure sensitive data protection

Dos

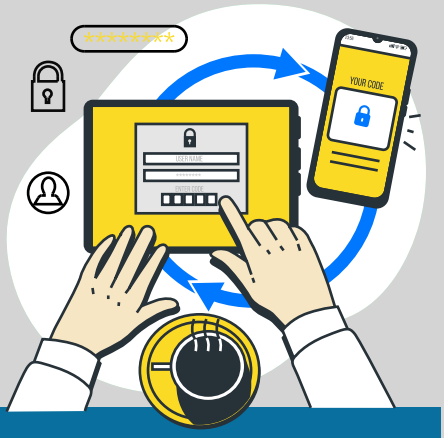


MOBILE PHONE/TABS

Prefer downloading mobile apps from genuine sources

Register for Do Not Disturb (DND) service with Telecom Operators

Dos

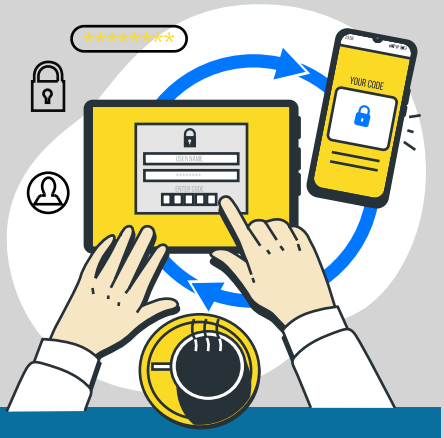


MOBILE PHONE/TABS

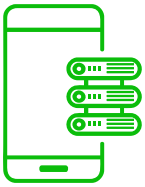
Use Parental control mode, while handing over mobile phones to kids or minors

Use device / SD card encryption to safeguard confidential data

Dos



MOBILE PHONE/TABS

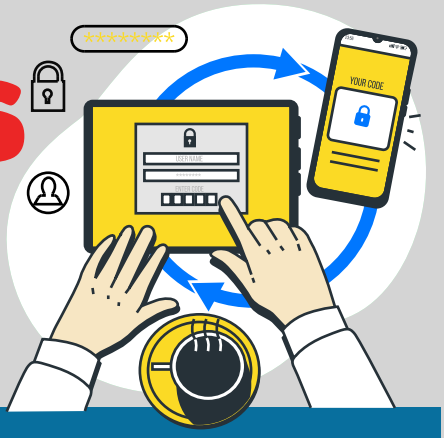


Auto-start, data usage for each App and App permission should be controlled

Protect your device with a strong PIN/Password or Biometrics and enable auto lock setting in mobile phone

Always take back-up of data (contacts, personal photos, etc.)

Don'ts



MOBILE PHONE/TABS

Do not reply or click on link sent through SMS, e-mails or chat messenger by strangers

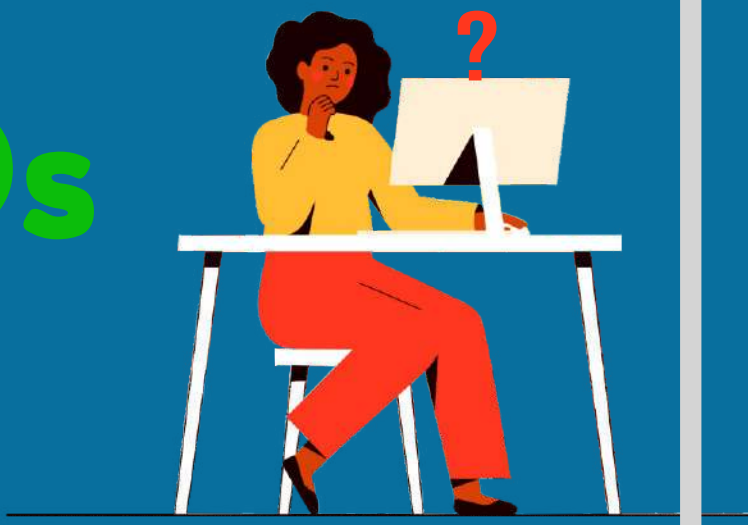
Do not store any classified/ sensitive data (text /video / photograph) in the device

Do not log into accounts, especially the financial accounts, when using public wireless networks

INCIDENT RESPONSE

Effective incident response helps an organization to identify and mitigate cyber incidents like data breach, malware attack, phishing, etc.

Dos



INCIDENT RESPONSE

- Disconnect the infected computers from LAN/ Internet immediately
- Remove unnecessary or unpatched software from computers particularly, remote desktop software, if any
- Change passwords of all e-mails and online services with another secure computer
- Re-install Operating Systems and applications from genuine source
- Scan backed-up data for virus/malware threat, etc., before restoring it

ORGANIZATIONAL LEVEL SECURITY CONTROLS

Dos

ORGANIZATIONAL LEVEL SECURITY CONTROLS

- Maintain up-to-date inventory of IT assets
- Regularly install patches on all digital assets, Operating System and software applications
- Ensure antivirus solution is present on all the systems

Dos

ORGANIZATIONAL LEVEL SECURITY CONTROLS

- Use Access Control Lists (ACL) to restrict direct network access to user machines, so that only approved IP addresses are allowed to connect to them
- Perform regular backups to allow quick restoration of impacted devices. Ensure backups are kept offline and make sure that Recovery Plan is in place
- Enable network segregation (partitioning of the network to keep critical parts of infrastructure away from the internet and internal networks) to curb malicious activity

Dos

ORGANIZATIONAL LEVEL SECURITY CONTROLS

- Enforce Multi-Factor Authentication (MFA) to prevent phishing attacks which may steal e-mail credentials
- Legacy computers (particularly internet facing servers) may be upgraded, so as to reduce Attack Surface
- Awareness sessions on IT security Best Practices to be periodically conducted
- Enforce Password Policy in the Organization to ensure that a minimum strength of password is complied with, across the network

MALWARE DEFENCE

Malware is a combination of ‘Malicious’ and ‘Software’. It is intentionally developed to perform unauthorized and destructive tasks on the victim's system without the knowledge of the victim.

It performs various activities like locking of important files, stealing sensitive information from the system, gaining unauthorized remote access, monitoring on the user activity, consuming computer memory, internet bandwidth, corrupting important files, etc.

The different types of malwares are ransomware, spyware, viruses, worms, rootkits, trojans, botnet, etc.

How to protect against malware?

- Keep all software up to date, including the Operating System and applications.
- Do not click on untrusted URL links.
- Use anti-Malware solutions.
- Patch Management to be ensured to overcome vulnerabilities.

DOs

MALWARE DEFENCE

Scan USBs, files on your computer regularly or before use. Disable USB devices if not needed

Use Licensed Version of Operating Systems and Application Software

Keep Operating System and Antivirus up-to-date with regular patches

DoS

MALWARE DEFENCE

PowerShell activities should be monitored for unusual activities

Deploy security solutions like Firewall, End Point Protection, E-mail Security, Web Filtering, Security Information and Event Management (SIEM), Anti-Advanced Threat Persistent (APT) in the organization

Periodically monitor and analyze network traffic for any suspicious or malicious activities

DOs

MALWARE DEFENCE

Ensure that Security and Event logs are monitored and preserved on periodic basis

Use Security Incident and Event Monitoring (SIEM) tools on 24x7 basis to identify any unwanted malware activity or suspicious events inside the organization

Browse only secure websites with “https”

Don'ts

MALWARE DEFENCE

Do not use your official e-mail address on websites to avail luring offers on unknown sites

Do not ignore security warnings from Operating System or Anti-virus program

E-MAIL SECURITY PRACTICES

Dos

EMAIL SECURITY PRACTICES

If any suspicious activity like e-mail access from suspicious IP addresses, etc., is noticed, report to Admin, do not click on any URL, do not download any file attached to it and do not pass any personal information over the e-mail

Monitor the e-mail protection system to check any suspected intrusion attempts

Don'ts

EMAIL SECURITY PRACTICES

Don't open/reply to e-mail links (hyperlinks/ web-links/ URLs mentioned in the body of such mails) giving any luring offer. It may result in compromising your personal and financial details.

Do not access to any spam e-mails, until the sender is properly verified

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

Indian Cyber crime Coordination Centre

CYBER DOST

Follow us on:

@CyberDostI4C

@cyberdosti4c

@CyberDost

@cyberdosti4c

December, 2021