Indian Cyber Crime Coordination Centre

सहवीर्यं करवावहै • Working Together With Vigour

Responding To Cyber Incidents In Schools

Why This Matters ?

Schools Are Increasingly Digital

Digital classrooms and smart boards

School management systems

Online examinations and assessments

Email and messaging platforms

Cloud storage and digital documents

Student and staff databases

Websites and social media

Online payments and fee systems

A cyber incident can affect:

Cybersecurity in schools is not only an IT responsibility it is a whole-school responsibility.

WHAT IS A CYBER INCIDENT?

A Cyber Incident is any event that threatens the **confidentiality**, **integrity** and **availability** of digital systems, information or services.

EXAMPLES

- Phishing or fraudulent emails
- Malware infection
- Ransomware
- Account compromise
- Password theft
- Data breach or data leak
- Website defacement
- DDoS attack
- Unauthorised access
- Cyberbullying or online harassment
- Fake social-media accounts
- Online financial fraud
- Exposure of children's personal information

REMEMBER:
Not every incident starts with a sophisticated hacker.

Sometimes it starts with:

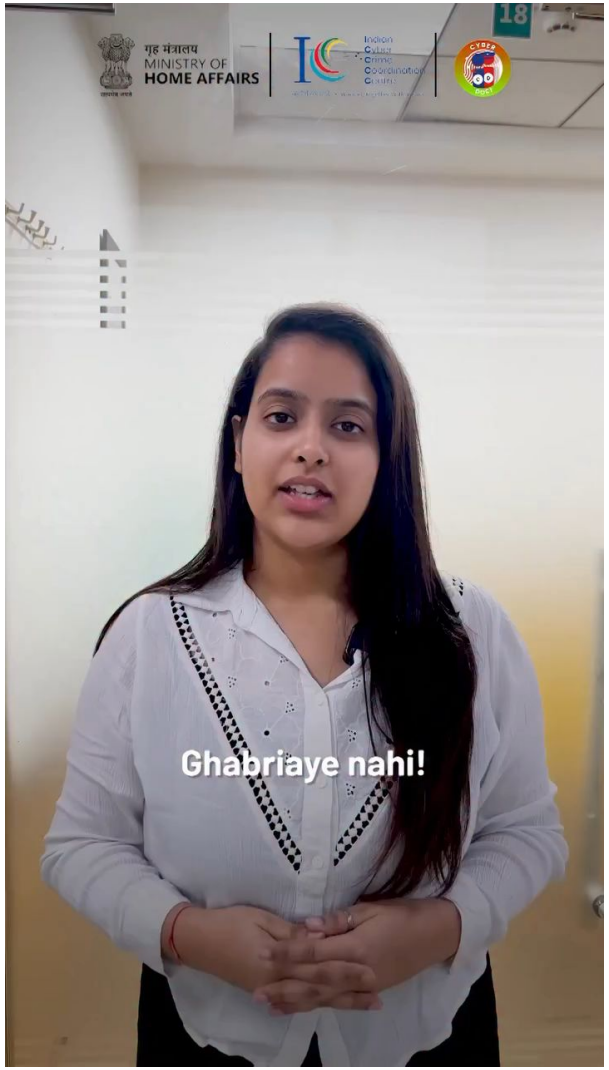
One click → One compromised account → One larger incident

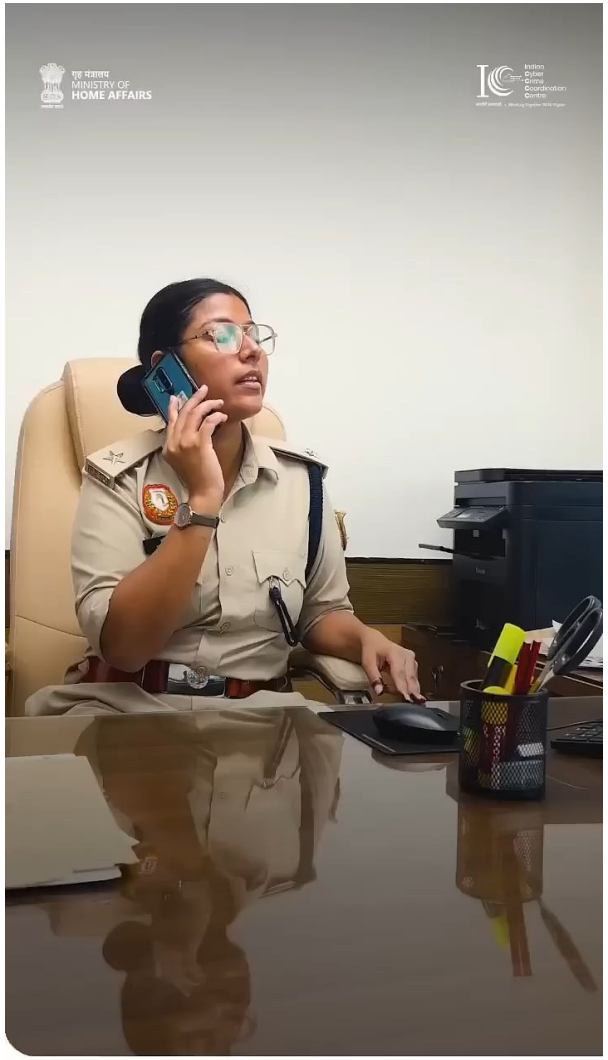
COMMON ONLINE RISKS TO CHILDREN

What Can Go Wrong?

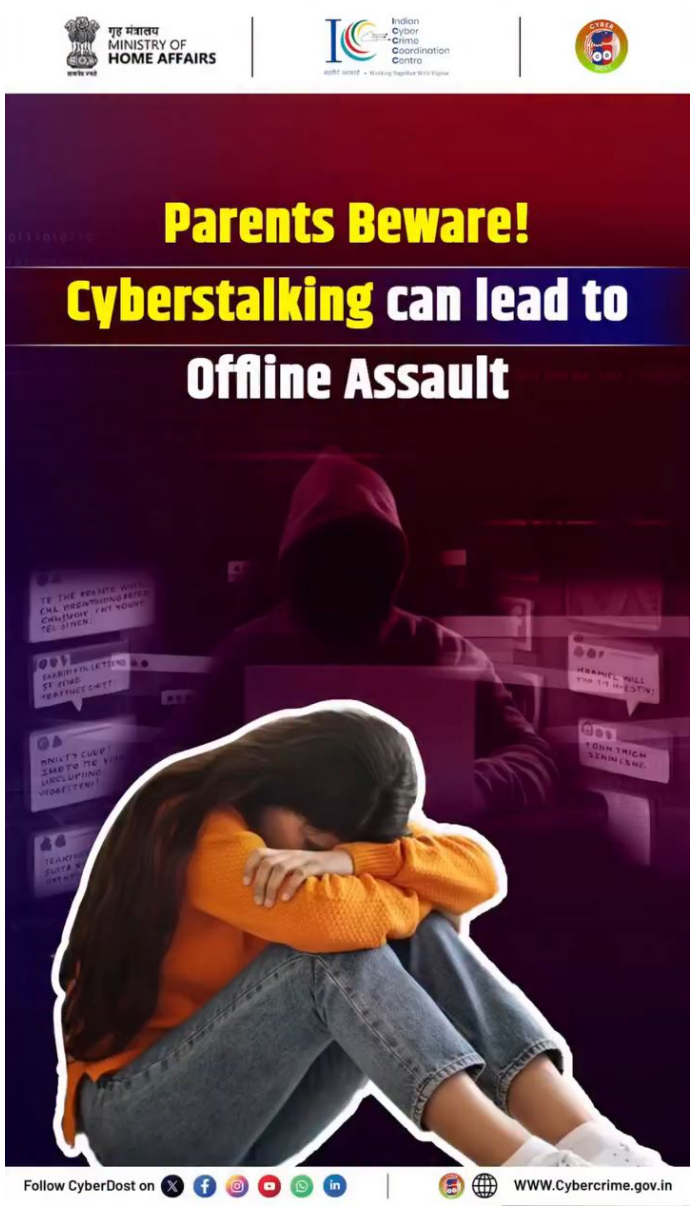
Risk	What It May Look Like
Cyberbullying	Insults, humiliation, threats, repeated harassment
Online Grooming	An adult builds trust with a child for harmful purposes
Sextortion / Blackmail	Threats to share private images or information
Fake Profiles	Someone pretends to be the child or another person
Gaming Risks	Unknown contacts, scams, inappropriate communication
Privacy Exposure	Sharing school, location, phone or personal details
Online Fraud	Fake prizes, links, offers or payment requests
Harmful Content	Exposure to violent, sexual or otherwise inappropriate material

REPORTING CYBERCRIME AGAINST WOMEN AND CHILDREN





अधिक जानकारी के लिए **CYBERDOST** को पर फॉलो करें


गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
Indian
Cyber
Crime
Coordination
Centre
Parents Beware!
Cyberstalking can lead to
Offline Assault
Follow CyberDost on
WWW.Cybercrime.gov.in

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

RECOGNISING WHEN TO SEEK HELP

1.

URGENCY

“Act now”, “account will be blocked”, “pay immediately”

2.

AUTHORITY IMPERSONATION

Police, government, bank, courier, employer or platform impersonation

3.

MONEY PRESSURE

Unexpected payment request, investment promise or recovery fee

4.

CREDENTIAL REQUEST

Requests for OTP, PIN, password, card details or remote access

WHY CYBERCRIME REPORTING MATTERS

STOP FURTHER LOSS

In financial fraud, immediate reporting through **1930** can support timely intervention.

ENABLE ACTION

Complete and accurate information helps law-enforcement agencies examine the complaint.

PROTECT OTHERS

Reporting suspicious identifiers can help strengthen repositories and monitoring.

Remember: Do not feel embarrassed or blame yourself. Cyber fraudsters often use urgency, fear, authority and attractive offers to manipulate victims.

Right response:

PAUSE → VERIFY → REPORT → PRESERVE

WHY VICTIMS MAY DELAY REPORTING

SHAME & STIGMA

Fear of being judged after making a mistake.

FEAR & INTIMIDATION

Threats, blackmail or impersonation can create panic.

LOW AWARENESS

The victim may not know that 1930 or the NCRP exists.

CONFUSION

Uncertainty about whether an incident is **“serious enough”** to report.

HOPE OF RECOVERY

The victim may continue negotiating with the fraudster instead of reporting.

EVIDENCE CONCERNS

The victim may think deleted chats or screenshots make reporting impossible.

Reporting helps you and protects others.

THE GOLDEN RESPONSE: ACT FAST

1. **STOP**

Do not send more money or share more credentials.

2. **CALL 1930**

For cyber financial fraud, report immediately through the 24×7 helpline.

3. **REPORT ONLINE**

Use the National Cyber Crime Reporting Portal:cybercrime .gov.in

4. **PRESERVE**

Keep transaction details, messages, emails, URLs, numbers and screenshots.

5. **TRACK & COOPERATE**

Keep acknowledgement/complaint details and provide further information if requested.

In a financial cyber fraud, speed matters. Report immediately.

WHERE TO REPORT CYBERCRIME IN INDIA

Use the official channels rather than responding to the fraudster.

1930 — CYBER CRIME HELPLINE

24×7 national helpline for reporting cyber financial fraud.

NATIONAL CYBERCRIME REPORTING PORTAL

Report cybercrime online at **cybercrime.gov.in**.

The portal provides complaint registration and tracking facilities.

LOCAL POLICE / CYBER POLICE

For emergencies or matters requiring immediate local police assistance, contact the police.

National police emergency number: 112

REPORT SUSPECT IDENTIFIERS

Suspicious URLs, phone numbers, WhatsApp/Telegram handles, email IDs, SMS headers and social-media URLs can be reported through the NCRP.

NATIONAL CYBERCRIME REPORTING PORTAL: BASIC WORKFLOW

1. **INCIDENT** — Identify the cyber incident and secure your accounts.
2. **COLLECT** — Keep transaction details and supporting evidence.
3. **REGISTER** — Open the official NCRP and select the relevant reporting category.
4. **SUBMIT** — Provide accurate incident details and evidence.
5. **ACKNOWLEDGEMENT** — Save the acknowledgement / complaint reference.
6. **FOLLOW-UP** — Track the complaint and cooperate with the investigating agency.

WHAT EVIDENCE SHOULD YOU PRESERVE?

Do not delete the conversation or reset the device before preserving useful information.

- Date and time of the incident
- Bank / wallet / merchant name
- Transaction ID / UTR and transaction date
- Fraud amount and account/payment details
- Phone numbers, email IDs, URLs and social-media handles
- Screenshots, emails, chats and call details
- Other relevant files
- Suspect details, if available

ACCURACY MATTERS

Provide correct and complete information so that the complaint can be examined effectively.

DO NOT PAY A "RECOVERY AGENT"

Use official channels.

MAKING HELP-SEEKING EASIER

LISTEN

Stay calm.
Avoid blaming the victim.
Let them explain what happened.
Focus on immediate safety and loss prevention.

STOP

ACT

Help contact 1930 where relevant.
Help access the NCRP.
Secure bank, email and social accounts.
Preserve evidence.

THINK

FOLLOW UP

Save acknowledgement details.
Cooperate with police/bank.
Be alert to repeat targeting.
Share verified awareness information.

TAKE ACTION

A victim who reports is helping investigators and potentially protecting other citizens.

DO'S & DON'TS FOR CYBERCRIME REPORTING

DO

- Report quickly
- Use **1930** for cyber financial fraud
- Use **cybercrime.gov.in** for online reporting
- Preserve evidence
- Provide accurate details
- Save your acknowledgement / complaint number
- Cooperate with the investigating agency

DON'T

- Don't feel ashamed or blame yourself
- Don't pay more to "recover" the money
- Don't share OTP/PIN/passwords
- Don't delete useful evidence
- Don't trust unofficial recovery agents
- Don't delay reporting a financial fraud

CYBERDOST: TURNING AWARENESS INTO ACTION

CyberDost is I4C's public-facing cyber-awareness handle, sharing practical safety messages and reporting guidance.

AWARENESS

Short, accessible messages on emerging scams, cyber hygiene and safe digital behaviour.

ALERTS

Timely awareness helps citizens recognise impersonation, phishing, fraud and other cybercrime patterns.

ACTION

The goal is not only awareness:

Know what happened →
Know what to do →
Know where to report →
Know how to seek help

- Follow official I4C/CyberDost channels.
- Do not rely on forwarded messages or unverified "cyber help" accounts.
- For reporting, use official government channels.

i4c.mha.gov.in

All | Gmail | YouTube | Maps | NCERT Solutions for... | yoga&meditation | India Communicatio... | Full Horoscope Rep... | Oscar Winner ~ Sho... | Green, Gold, Diamo... | New Tab | All Bookmarks

Contribute towards Cyber Hygiene. Become a Cyber Volunteer. **Click here.**

Awareness

Report a Cybercrime

Take a Pledge for Cyber Safety

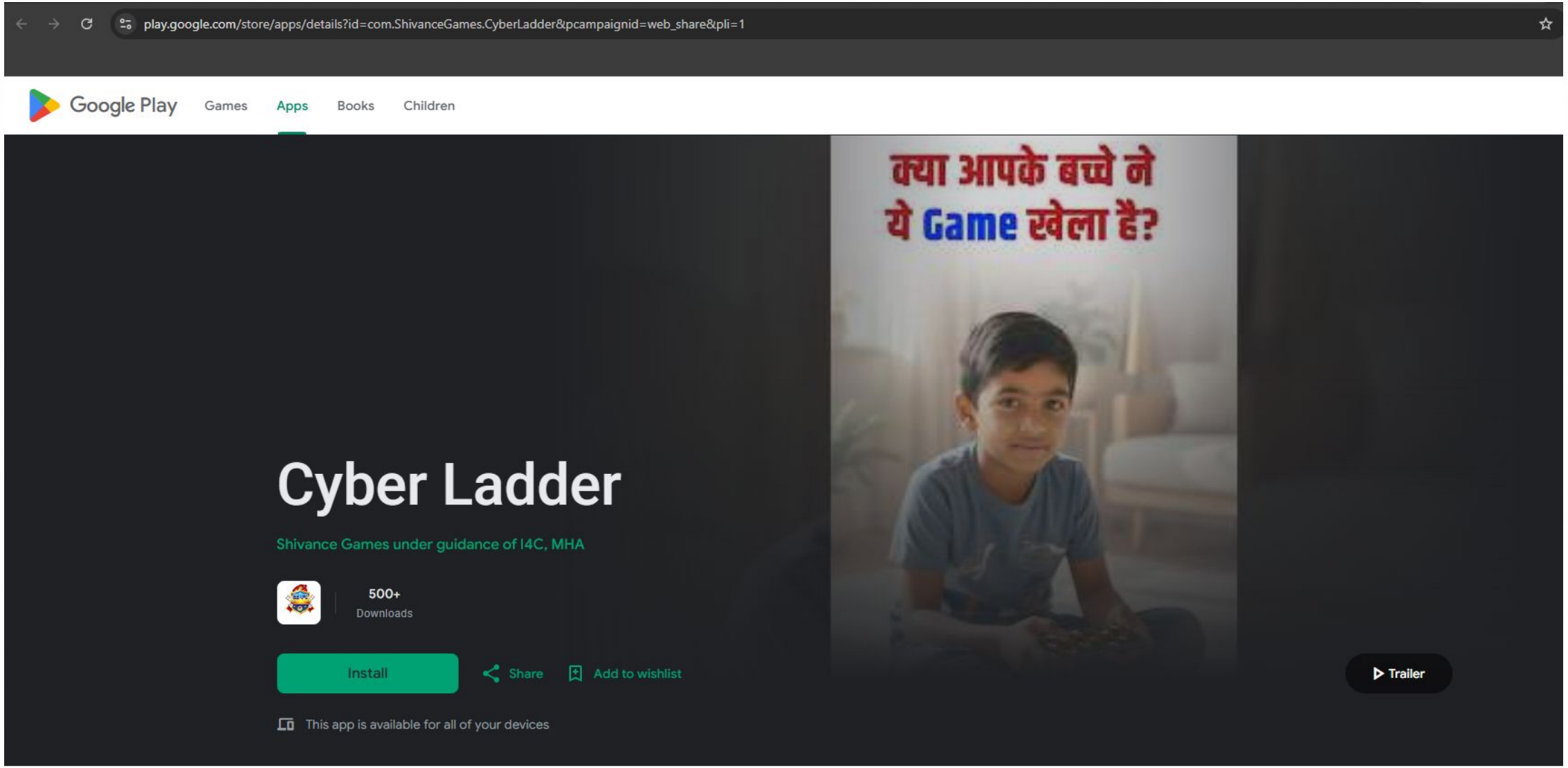
Download Cyber Hygiene Game

Indian Cybercrime Coordination Centre

What's new

View All

CYBER LADDER GAME



CYBER HYGIENE COURSE

learning.cte-i4c.live

English (en) | Log in | User Registration

गृह मंत्रालय MINISTRY OF HOME AFFAIRS | Indian Cyber Crime Coordination Centre

Home

Be "Cyber Smart"

Become a C3
Cyber Conscious Citizen

Join The Course

Welcome To "Cyber Smart" E-learning Course

Welcome to the crisp, smart and practical e-learning course on Cyber Hygiene by I4C — designed especially for common citizens. In just 4–5 hours, this interactive program will empower you to stay safe from today's fastest-growing online threats. Through simple videos, real-life examples, and easy-to-understand modules, you'll learn how to protect your money, identity, devices, and personal data.
From digital payments and social media safety to spotting fraud calls, fake links, investment traps, and cyber scams — this course covers everything you need to be a smart and secure digital citizen.

Anyone

- Student
- Working Professionals
- Govt. Employees
- Senior Citizens

Cyber Hygiene

Go To Course

pledge.cte-i4c.live

All Gmail YouTube Maps NCERT Solutions for... yoga&meditation India Communicatio... Full Horoscope Rep... Oscar Winner All Bookmarks

English Hindi

Google Translate

CYBER SAFETY PLEDGE

A SHARED RESPONSIBILITY FOR A SECURE DIGITAL FUTURE

JOIN THE MOVEMENT. TAKE THE PLEDGE.

Today's Pledge: 37

शपथ / Oath

(शपथ हिंदी में)

मैं शपथ लेता/लेती हूँ कि :

- मैं मोबाइल ऐप हमेशा ऑफिसियल वेबसाइट या प्ले स्टोर से ही इंस्टॉल करूँगा/करूँगी।
- मैं सोशल मीडिया ग्रुप्स या विज्ञापनों पर बिना सोचे भरोसा नहीं करूँगा/करूँगी।
- मैं अनजाने नंबरों से आने वाले कॉल्स पर आँख बंद करके भरोसा नहीं करूँगा/करूँगी।
- मैं डिजिटल सुरक्षा के लिए **"Stop. Think. Then Take Action."** इस सिद्धांत का हमेशा पालन करूँगा।
- मैं गृह मंत्रालय के सोशल मीडिया हैंडल **@Cyberdost** को आज और अभी फॉलो करूँगा/करूँगी।
- साइबर-अपराध का शिकार होने पर बिना देर किए **1930** पर कॉल करूँगा/करूँगी।

जय हिन्द !

(Pledge in English)

Cyber Awareness

Hon’ble Prime Minister cautioned citizens about "Digital Arrest" tactics being adopted by cyber criminals through the "Mann Ki Baat" programs on 27 Oct 2024 and 24 Nov 2024 and gave the *Mantra* of

STOP-THINK-TAKE ACTION

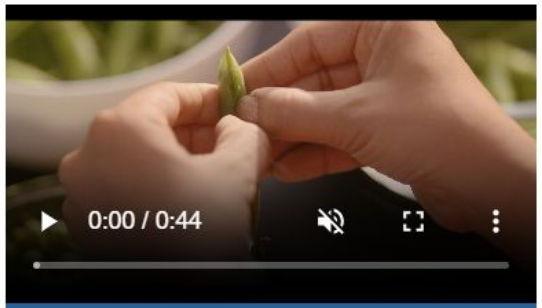
"Content available on the page are free

POSTS

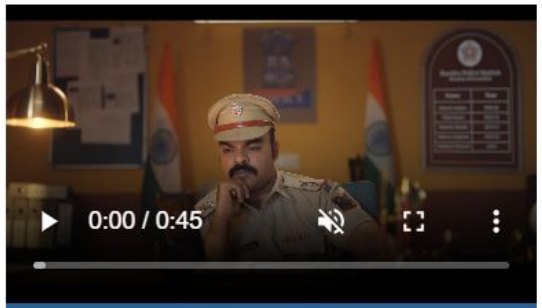
i4c.mha.gov.in/awareness.aspx

All Gmail YouTube Maps NCERT Solutions for... yoga&meditation India Communicatio... Full Horoscope Rep... Oscar Winner ~ Sho... Green, Gold, Diamo... New Tab All Bookmar

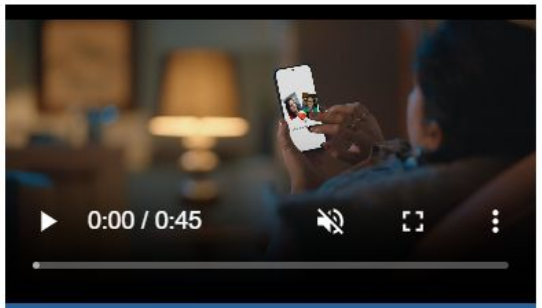
LATEST CYBER AWARENESS VIDEOS



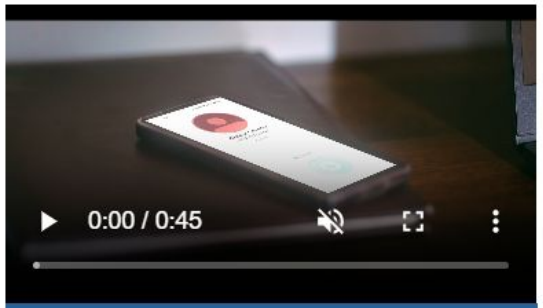
Money Transferred By Mistake



Fake Police



Dating Scan



Cyber Slavery

VIEW MORE →

CYBER AWARENESS AUDIOS

Digital Arrest

Urgency Based Scams

Investment Scam

Greed Based Scams

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian Cyber Crime Coordination Centre

CYBER CRIME PREVENTION HANDBOOK

ESSENTIAL
DOS AND DON'TS
FOR LATEST CYBER CRIMES

STOP. THINK. TAKE ACTION

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian Cyber Crime Coordination Centre

साइबर अपराधों से बचाव हेतु मार्गदर्शिका हैंडबुक

साइबर अपराधों से बचाव के लिए ज़रूरी
क्या करें और क्या ना करें

रुको. सोचो. एक्शन लो.

INDEX
SCAM ALERTS

SCAMS	Page No.
KYC Scam	4
Online Job Scam	5
Online Shopping Fraud	6
Digital Arrest	7
Investment Scam	8
Online Gaming	9
Lottery Fraud	10
Phishing	11
Vishing	12
Quishing	13
Search Engine Fraud	14
Social Media Impersonation	15

KYC Scam

✓ Dos:

- **Verify Requests:** Contact your bank or financial institution directly to confirm any KYC update requests.
- **Use Official Contacts:** Obtain contact numbers or customer care details only from the official website or trusted sources.
- **Report Incidents:** Inform your bank or financial institution immediately if you suspect any cyber fraud.
- **Check KYC Update Methods:** Enquire with your bank about the available methods for updating KYC details.

× Don'ts:

- **Protect Credentials:** Never share your account login details, card information, PINs, passwords, or OTPs with anyone or on unauthorised websites/apps.
- **Secure Documents:** Do not share KYC documents or their copies with unknown or unidentified individuals or organisations.
- **Avoid Suspicious Links:** Do not click on suspicious or unverified links received via mobile or email.

Online Jo

Online Job Scams [illegible] on websites, social media [illegible] Their goal is to steal the [illegible]

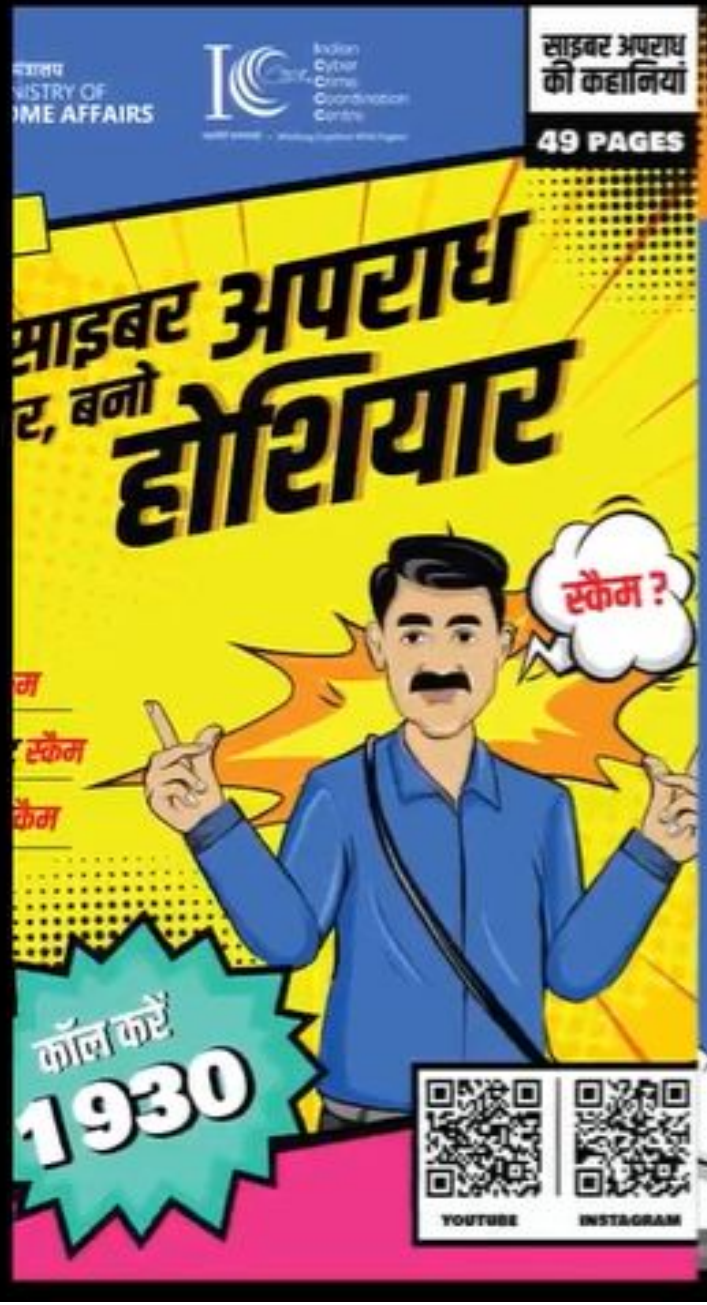
✓ Dos:

- **Use Trusted Sources:** Refer to news[illegible] job portals, or government portals [illegible] authentic private and government [illegible]
- **Check Credentials:** For international [illegible] offers, verify the company's credentials [illegible] ensure you have the correct work [illegible]
- **Ask Questions:** During online interviews [illegible] detailed questions about the company [illegible] interviewer.
- **Verify Emails:** Look out for email addresses [illegible] that mimic genuine companies. For example, info@company.net in place of info@company.com.

Digital Arrest

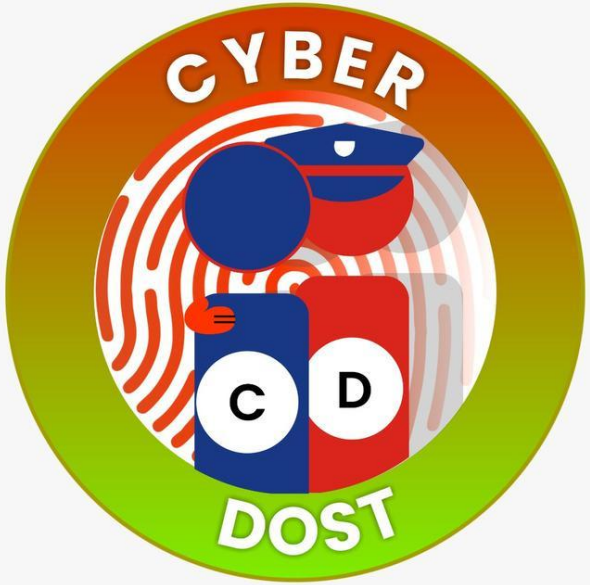
✓ Dos:

× Don'ts:



विषय सूची

संख्या	शीर्षक	पृष्ठ संख्या
1	भोला जी और डिजिटल अरेस्ट का जाल!	03
2	मिस्टर वेंकट और इन्वेस्टमेंट स्कैम की माया	07
3	गुरप्रीत और प्यार का जंजाल!	10
4	घोष बाबू और फ़र्ज़ी नोटिस	13
5	पटेल भाई और फ़र्ज़ी सरकारी अफ़सर का खेल	15
6	दीप्ति और सोशल मीडिया के ठग	18
7	भोलाराम और 2 मिनट में लोन का खेल	23
8	अर्जुन और अश्लील वीडियो का झांसा	26
9	बापू जी और APK फाइल का धोखा	29
10	नादान नोटियाल और QR कोड का स्कैम	32
11	जागरूकता देवी और ऑनलाइन शॉपिंग स्कैम	35
12	मासूम नकसूद और ऑनलाइन नौकरी का धोखा	38
13	होशियार सिंह और पैसे वापिसी का स्कैम	41
14	विदेश में नौकरी, पड़ गई भारी	44
15	करण और खेल-खेल में स्कैम	47



CYBERDOST
I4C

Thanks