Indian Cyber Crime Coordination Centre

सहवीर्यं करवावहै • Working Together With Vigour

विद्यालयों में साइबर घटनाओं पर प्रतिक्रियाएं

यह क्यों महत्वपूर्ण है?

स्कूल तेजी से डिजिटल हो रहे हैं

डिजिटल कक्षाएँ और स्मार्ट बोर्ड

स्कूल प्रबंधन प्रणालियाँ

ऑनलाइन परीक्षाएँ और आकलन

ईमेल और मैसेजिंग प्लेटफ़ॉर्म

क्लाउड स्टोरेज और डिजिटल दस्तावेज़

छात्र और स्टाफ डेटाबेस

वेबसाइट और सोशल मीडिया

ऑनलाइन भुगतान और शुल्क प्रणालियाँ

एक साइबर घटना प्रभावित कर सकती है:

स्कूलों में साइबर सुरक्षा केवल आईटी विभाग की जिम्मेदारी नहीं है, बल्कि पूरे स्कूल की जिम्मेदारी है।

साइबर घटना क्या है?

साइबर घटना कोई भी ऐसी घटना है जो डिजिटल प्रणालियों, सूचना या सेवाओं की **गोपनीयता**, **अखंडता** और **उपलब्धता** के लिए खतरा उत्पन्न करती है।

उदाहरण

- फिशिंग या धोखाधड़ी वाले ईमेल
- मैलवेयर संक्रमण
- रैनसमवेयर
- अकाउंट का समझौता
- पासबर्ड की चोरी
- डेटा ब्रीच या डेटा लीक
- वेबसाइट का विकृत (डिफेस) किया जाना
- DDoS हमला
- अनधिकृत पहुँच
- साइबर बुलिंग या ऑनलाइन उत्पीड़न
- फर्जी सोशल मीडिया अकाउंट्स
- ऑनलाइन वित्तीय धोखाधड़ी
- बच्चों की व्यक्तिगत जानकारी का अनधिकृत खुलासा

याद रखें:
हर घटना एक परिष्कृत हैकर से शुरू नहीं होती है।

कभी-कभी यह इस तरह शुरू होता है:

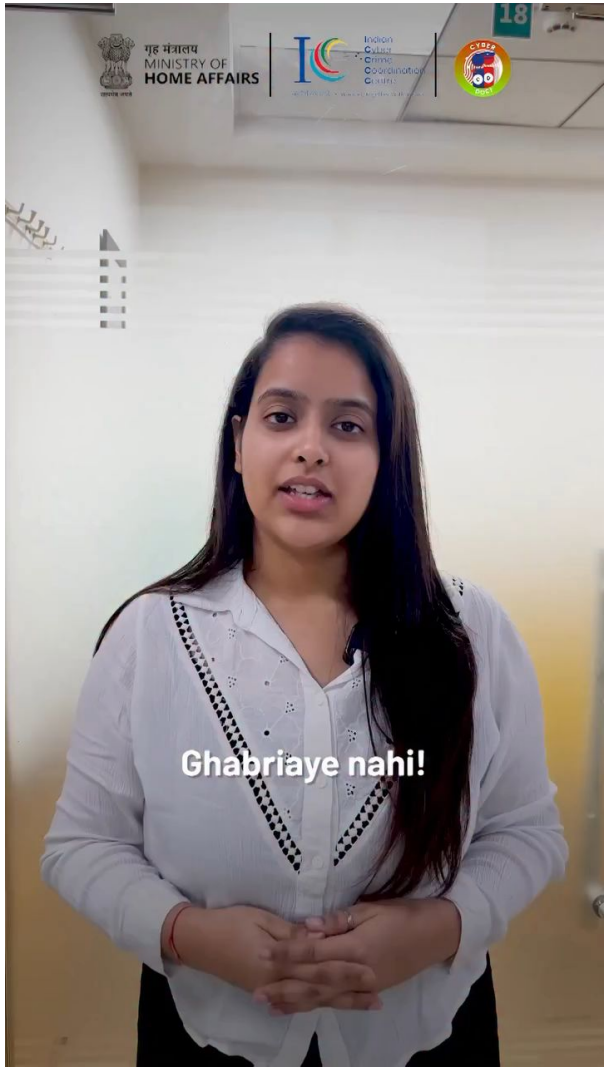
एक क्लिक से → एक समझौता किए गए अकाउंट से → और फिर एक बड़ी घटना में बदल जाता है

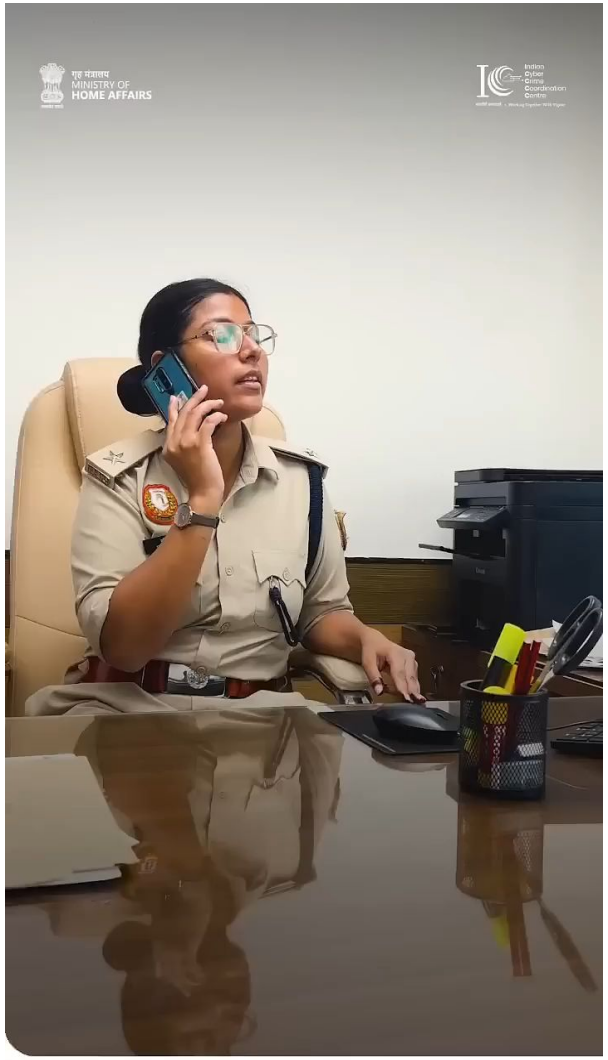
बच्चों के लिए सामान्य ऑनलाइन जोखिम

क्या गलत हो सकता है?

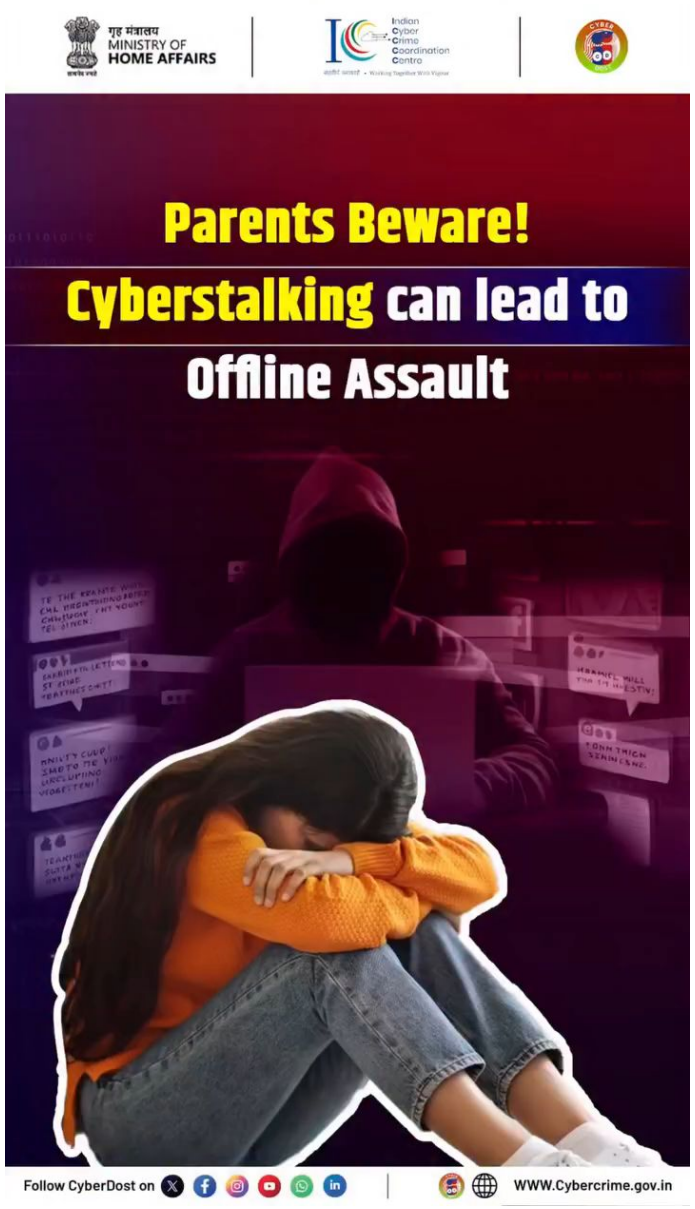
जोखिम	यह कैसा दिख सकता है
साइबर बुलिंग	अपमानजनक बातें, शर्मिंदा करना, धमकी देना, या बार-बार उत्पीड़न करना
ऑनलाइन ग्रूमिंग	कोई वयस्क गलत उद्देश्य से बच्चे के साथ विश्वास का रिश्ता बनाता है
सेक्सटॉर्शन / ब्लैकमेल	निजी तस्वीरें या जानकारी साझा करने के लिए धमकी देना
फर्जी प्रोफाइल	कोई व्यक्ति बच्चे या किसी और का बनकर पहचान छिपाता है
ऑनलाइन गेमिंग संबंधी जोखिम	अज्ञात लोगों से संपर्क, धोखाधड़ी, या अनुचित संवाद
गोपनीयता का उल्लंघन	स्कूल, स्थान, फोन नंबर या व्यक्तिगत जानकारी साझा होना
ऑनलाइन धोखाधड़ी	नकली पुरस्कार, लिंक, ऑफर या भुगतान अनुरोध
हानिकारक सामग्री	हिंसक, यौन या अन्य अनुचित सामग्री के संपर्क में आना

महिलाओं और बच्चों के विरुद्ध साइबर अपराध की रिपोर्टिंग





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

मदद लेने का सही समय पहचानना

1.

तात्कालिकता

“अभी कार्रवाई करें”, “खाता ब्लॉक कर दिया जाएगा”, “तुरंत भुगतान करें”

2.

अधिकारियों के नाम पर धोखाधड़ी

पुलिस, सरकार, बैंक, कूरियर, नियोक्ता या किसी ऑनलाइन प्लेटफ़ॉर्म के अधिकारी बनकर धोखा देना

3.

पैसों का दबाव

अप्रत्याशित भुगतान का अनुरोध, निवेश का वादा या पैसे वापस दिलाने के नाम पर शुल्क

4.

लॉगिन जानकारी माँगना

OTP, PIN, पासवर्ड, कार्ड विवरण या रिमोट एक्सेस माँगना

साइबर अपराध की रिपोर्टिंग क्यों महत्वपूर्ण है

आगे होने वाले नुकसान को रोकें
वित्तीय धोखाधड़ी के मामले में, 1930 के माध्यम से तुरंत रिपोर्ट करने से समय पर कार्रवाई में सहायता मिल सकती है।

कार्रवाई को सक्षम बनाएं
पूरी और सटीक जानकारी कानून प्रवर्तन एजेंसियों को शिकायत की प्रभावी जाँच करने में मदद करती है।

दूसरों की सुरक्षा करें
संदिग्ध पहचान संबंधी जानकारी की रिपोर्ट करने से डेटाबेस और निगरानी तंत्र को मजबूत करने में मदद मिल सकती है।

याद रखें: शर्मिंदा महसूस न करें और स्वयं को दोष न दें। साइबर ठग अक्सर पीड़ितों को गुमराह करने के लिए जल्दबाजी , डर, अधिकार का दिखावा और आकर्षक प्रस्तावों का इस्तेमाल करते हैं।

Right response:

रुकें → सत्यापित करें → रिपोर्ट करें → सुरक्षित रखें

पीड़ित रिपोर्ट करने में देरी क्यों कर सकते हैं?

शर्म और सामाजिक कलंक
गलती करने के बाद लोगों द्वारा आलोचना किए जाने का डर।

डर और धमकी

धमकी, ब्लैकमेल या किसी की पहचान का गलत इस्तेमाल होने से घबराहट पैदा हो सकती है।.

कम जागरूकता

पीड़ित को यह जानकारी नहीं हो सकती कि 1930 हेल्पलाइन या NCRP उपलब्ध है।

भ्रम और असमंजसयह

समझ न होना कि कोई घटना रिपोर्ट करने के लिए “पर्याप्त गंभीर” है या नहीं।

ठीक होने की उम्मीद

पीड़ित रिपोर्ट करने के बजाय ठग के साथ बातचीत करके अपनी राशि वापस पाने की कोशिश करता रह सकता है।

साक्ष्य से जुड़ी चिंताएँ

पीड़ित को लग सकता है कि डिलीट की गई चैट या स्क्रीनशॉट उपलब्ध न होने के कारण रिपोर्ट करना संभव नहीं है।

रिपोर्ट करने से आपकी मदद होती है और दूसरों की सुरक्षा होती है।

सुनहरा नियम: तुरंत कार्रवाई करें

1.

रुकें

और पैसे न भेजें या अपनी अन्य लॉगिन जानकारी साझा न करें।

2.

1930 पर कॉल करें

साइबर वित्तीय धोखाधड़ी के लिए 24×7 हेल्पलाइन के माध्यम से तुरंत रिपोर्ट करें।

3.

ऑनलाइन रिपोर्ट करें

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल का उपयोग करें:
cybercrime.gov.in

4.

सुरक्षित रखें

लेन-देन का विवरण, संदेश, ईमेल, यूआरएल, नंबर और स्क्रीनशॉट सुरक्षित रखें।

5.

नज़र रखें और सहयोग करें

स्वीकृति /शिकायत का विवरण सुरक्षित रखें और माँगे जाने पर अतिरिक्त जानकारी प्रदान करें।

वित्तीय साइबर धोखाधड़ी में समय बहुत महत्वपूर्ण है। तुरंत रिपोर्ट करें।

भारत में साइबर अपराध की रिपोर्ट कहां करें

धोखाधड़ी करने वाले को जवाब देने के बजाय, आधिकारिक चैनलों का उपयोग करें।

1930 — साइबर अपराध हेल्पलाइन

साइबर वित्तीय धोखाधड़ी की रिपोर्ट करने के लिए 24×7 राष्ट्रीय हेल्पलाइन।

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल

साइबर अपराध की ऑनलाइन रिपोर्ट **cybercrime.gov.in** पर करें।
इस पोर्टल पर शिकायत दर्ज करने और उसकी प्रगति को ट्रैक करने की सुविधा उपलब्ध है।

स्थानीय पुलिस / साइबर पुलिस

आपात स्थिति या ऐसी किसी भी मामले के लिए जिसमें तत्काल स्थानीय पुलिस सहायता की आवश्यकता हो, पुलिस से संपर्क करें।
राष्ट्रीय पुलिस आपातकालीन नंबर: 112

संदिग्ध पहचान संबंधी जानकारी की रिपोर्ट करें

संदिग्ध URL, फोन नंबर, WhatsApp/Telegram हैंडल, ईमेल आईडी,
SMS हेडर और सोशल मीडिया URL की रिपोर्ट NCRP के माध्यम से की जा सकती है।

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल: मूल कार्यप्रवाह

1 घटना

साइबर घटना की पहचान करें और
अपने खातों को सुरक्षित करें।

2 जानकारी एकत्र करें

लेन-देन का विवरण और
समर्थक साक्ष्य (सबूत) सुरक्षित रखें।

3 पंजीकरण करें

आधिकारिक NCRP पोर्टल खोलें और
उपयुक्त रिपोर्टिंग श्रेणी का चयन करें।

4 रिपोर्ट दर्ज करें

घटना से संबंधित सटीक विवरण और
साक्ष्य प्रदान करें।

5 स्वीकृति प्राप्त करें

स्वीकृति / शिकायत संदर्भ संख्या
सुरक्षित रखें।

6 अनुवर्ती कार्रवाई करें

अपनी शिकायत की स्थिति पर नज़र रखें
और जांच एजेंसी के साथ सहयोग करें।

कौन-से साक्ष्य सुरक्षित रखने चाहिए?

उपयोगी जानकारी सुरक्षित रखने से पहले बातचीत को डिलीट न करें और न ही डिवाइस को रीसेट करें।

- घटना की तारीख और समय
- बैंक / वॉलेट / व्यापारी का नाम
- लेन-देन आईडी / UTR और लेन-देन की तारीख
- धोखाधड़ी की राशि और खाता/भुगतान संबंधी विवरण
- फोन नंबर, ईमेल आईडी, यूआरएल और सोशल मीडिया हैंडल
- स्क्रीनशॉट, ईमेल, चैट और कॉल का विवरण
- अन्य प्रासंगिक फाइलें
- संदिग्ध व्यक्ति का विवरण, यदि उपलब्ध हो

सटीकता महत्वपूर्ण है

शिकायत की प्रभावी जाँच के लिए सही और पूरी जानकारी प्रदान करें।

"पैसे वापस दिलाने वाले एजेंट" को भुगतान न करें

आधिकारिक माध्यमों का उपयोग करें।

मदद लेने को आसान बनाना

सुनें

सुनें, शांत रहें।
पीड़ित को दोष देने से बचें।
उन्हें यह बताने दें कि क्या हुआ।
तत्काल सुरक्षा और नुकसान को रोकने पर ध्यान दें।

रुकें

कार्रवाई करें

रुकें जहाँ आवश्यक हो, 1930 पर संपर्क करने में सहायता करें।
NCRP तक पहुँचने में सहायता करें ।बैंक, ईमेल और सोशल मीडिया अकाउंट सुरक्षित करें।
साक्ष्य सुरक्षित रखें।

सो चें

अनुवर्ती कार्रवाई करें

स्वीकृति विवरण सुरक्षित रखें।
पुलिस/बैंक के साथ सहयोग करें।
बार-बार निशाना बनाए जाने के प्रति सतर्क रहें।सत्यापित जागरूकता संबंधी जानकारी साझा करें।

एक्शन लो

जो पीड़ित रिपोर्ट करता है, वह जांचकर्ताओं की मदद करता है और संभावित रूप से अन्य नागरिकों की सुरक्षा करता है।

साइबर अपराध की रिपोर्टिंग के लिए क्या करें और क्या न करें

करें

- जल्दी रिपोर्ट करें
- साइबर वित्तीय धोखाधड़ी के लिए **1930** पर कॉल करें
- ऑनलाइन रिपोर्टिंग के लिए **cybercrime.gov.in** का उपयोग करें
- साक्ष्य सुरक्षित रखें
- सटीक जानकारी प्रदान करें
- अपनी स्वीकारोक्ति / शिकायत संख्या सुरक्षित रखे
- जाँच करने वाली एजेंसी के साथ सहयोग करें

न करें

- शर्मिंदा महसूस न करें और स्वयं को दोष न दें
- “पैसा वापस पाने” के लिए अतिरिक्त भुगतान न करें
- OTP/PIN/पासवर्ड किसी के साथ साझा न करें
- उपयोगी साक्ष्य को न हटाएँ
- अनौपचारिक रिकवरी एजेंटों पर भरोसा न करें
- वित्तीय धोखाधड़ी की रिपोर्ट करने में देरी न करें

साइबरदोस्त: जागरूकता को कार्रवाई में बदलना

साइबरदोस्त (CyberDost) I4C का जन-जागरूकता संबंधी पहल है,
जो व्यावहारिक सुरक्षा संदेशों और रिपोर्टिंग संबंधी मार्गदर्शन को साझा करता है।

जागरूकता

उभरते घोटालों, साइबर स्वच्छता और सुरक्षित डिजिटल व्यवहार पर छोटे, सरल और सहज संदेश प्रदान करना।

चेतावनियाँ

समय पर दी गई जागरूकता नागरिकों को भेषधारी अपराध (इमरसनेशन), फिशिंग, धोखाधड़ी और अन्य साइबर अपराध के पैटर्न को पहचानने में मदद करती है।

कार्रवाई

लक्ष्य केवल जागरूकता नहीं, बल्कि:

- जानें क्या हुआ →
- जानें क्या करना है →
- जानें कहाँ रिपोर्ट करना है →
- जानें मदद कैसे प्राप्त करें →

- I4C/साइबरदोस्त के आधिकारिक चैनलों को फॉलो करें।
- फॉरवर्ड किए गए संदेशों या अनपुष्ट “साइबर सहायता” खातों पर भरोसा न करें।
- रिपोर्टिंग के लिए, आधिकारिक सरकारी चैनलों का उपयोग करें।

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

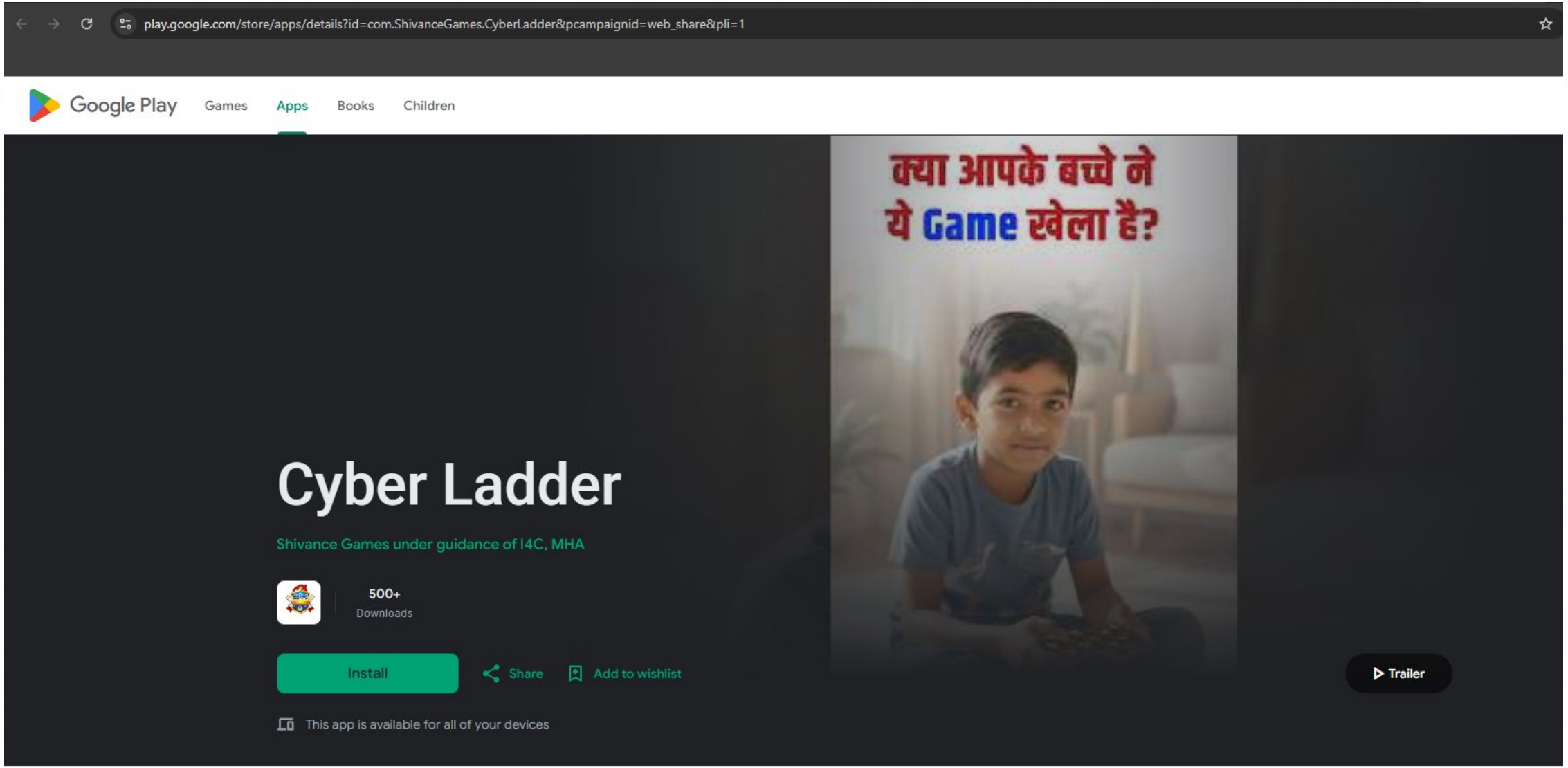
Download Cyber Hygiene Game

Indian Cybercrime Coordination Centre

What's new

View All

साइबर सीढ़ी खेल


play.google.com/store/apps/details?id=com.ShivanceGames.CyberLadder&pcampaignid=web_share&pli=1
Google Play
Games
Apps
Books
Children
क्या आपके बच्चे ने
ये Game खेला है?
Cyber Ladder
Shivance Games under guidance of I4C, MHA
500+
Downloads
Install
Share
Add to wishlist
This app is available for all of your devices
Trailer

साइबर स्वच्छता पाठ्यक्रम

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)

साइबर जागरूकता

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

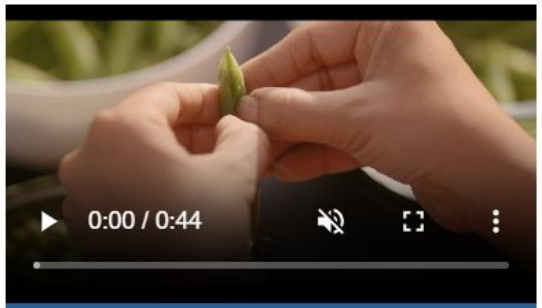
"Content available on the page are free

POSTS

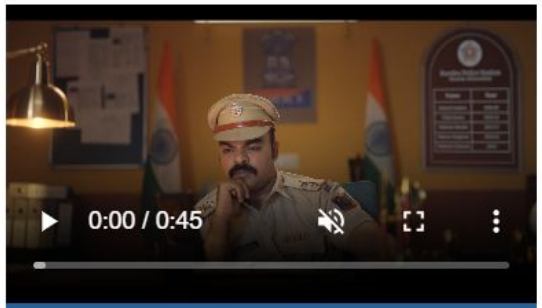
i4c.mha.gov.in/awareness.aspx

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

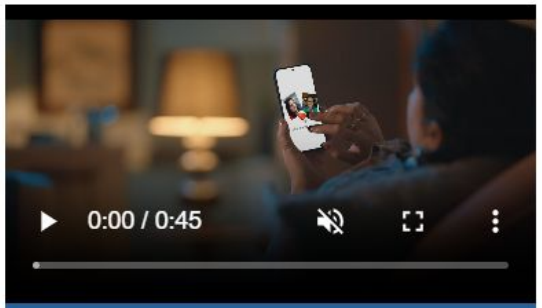
LATEST CYBER AWARENESS VIDEOS



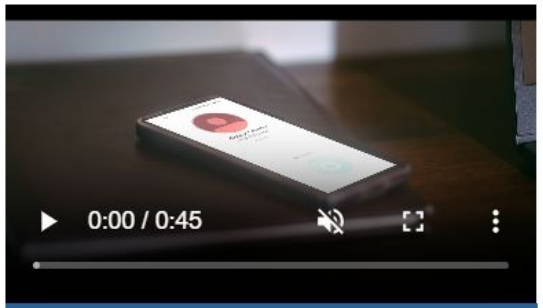
Money Transferred By Mistake



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]

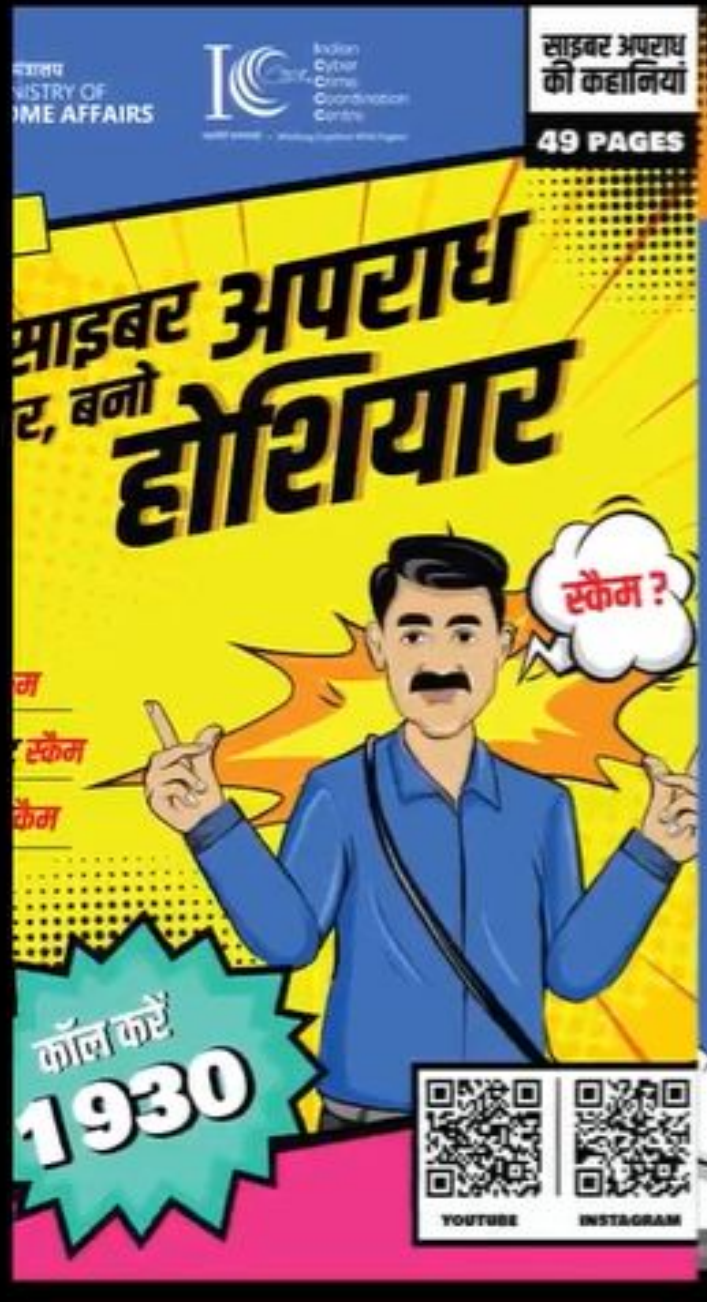
✓ Dos:

- **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

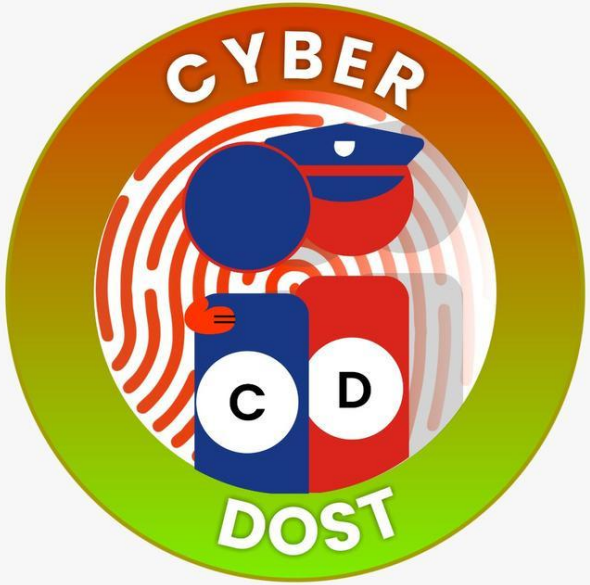
✓ Dos:

× 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

धन्यवाद