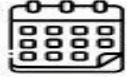


ऑनलाइन प्रशिक्षण “साइबर अपराध”

CIET-NCERT द्वारा गृह मंत्रालय (MHA) के भारतीय साइबर अपराध समन्वय केंद्र (I4C) के सहयोग से आयोजित



08 जुलाई 2025



4:00 -5:00 अपराह्न

दिन 2: साइबर अपराध के प्रकार

सुश्री निशा पांडे

प्रोफेशनल इकोसिस्टम एक्सपर्ट

भारतीय साइबर अपराध समन्वय केंद्र (I4C)

गृह मंत्रालय (MHA), नई दिल्ली

लाइव देखें

एनसीईआरटी आधिकारिक यूट्यूब चैनल

<https://www.youtube.com/@NCERTOFFICIAL>



You can
watch at:



DD Free Dish Channel
Dish TV Channel #2027-2033



PM eVidya Channel #6-12



Jio TV

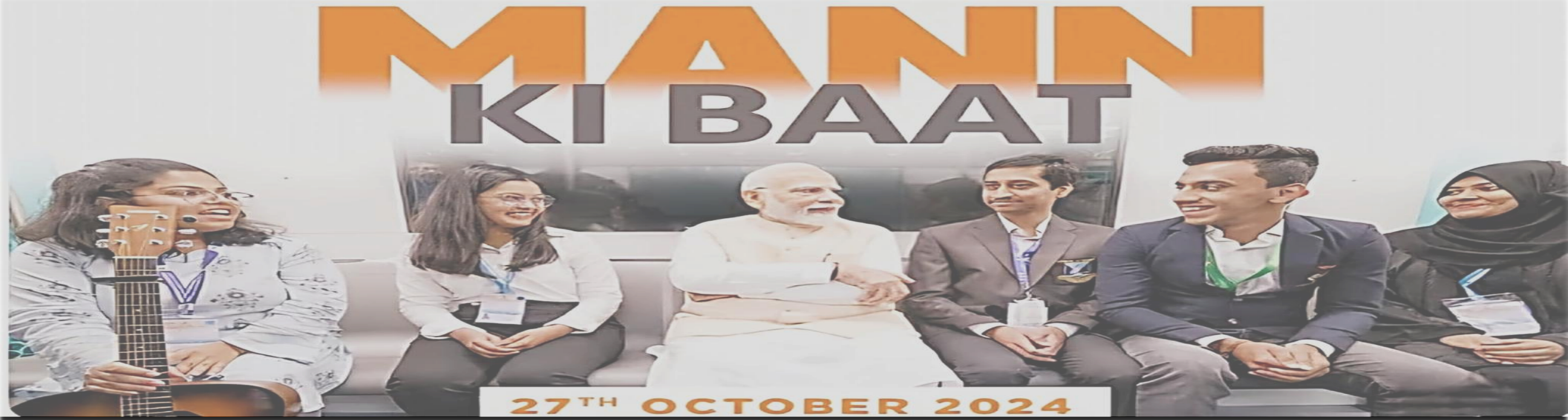
किसी भी अन्य प्रश्न के लिए, यहां मेल करें: training.helpdesk@ciet.nic.in या कॉल करें: 8800440559

बाचतीत के बिंदू

- 1 माननीय प्रधानमंत्री का आह्वान
- 2 साइबर अपराध जागरूकता में स्कूल की भूमिका
- 3 साइबर अपराध के प्रकार
- 4 अबाउट I4C
- 5 ऑफिसियल सोशल मीडिया हैंडल : CyberDost

माननीय प्रधानमंत्री का आह्वान

माननीय प्रधानमंत्री ने 27 अक्टूबर 2024 और 24 नवंबर 2024 को "मन की बात" कार्यक्रमों के माध्यम से नागरिकों को साइबर अपराधियों द्वारा अपनाई जा रही "डिजिटल गिरफ्तारी" रणनीति के बारे में आगाह किया और मंत्र दिया।
रोको-सोचो-एक्शन लो



साइबर अपराध जागरूकता में स्कूल की भूमिका

बचपन में बनी आदतें जीवन भर बनी रहती हैं।

स्कूलों के लिए यह आवश्यक है कि वे डिजिटल दुनिया में भी अनुशासन और जिम्मेदार व्यवहार को बढ़ावा दें, जैसा कि वे वास्तविक दुनिया में करते हैं।

भारत में स्कूलों को बहुत भरोसे और सम्मान की स्थिति प्राप्त है। जब वे बोलते हैं, तो छात्र, अभिभावक और परिवार सुनते हैं।

युवा छात्र साइबर खतरों के प्रति विशेष रूप से संवेदनशील होते हैं, इसलिए स्कूलों के लिए यह आवश्यक हो जाता है कि वे उनकी ऑनलाइन सुरक्षा सुनिश्चित करने में सक्रिय भूमिका निभाएं।



साइबर अपराध के प्रकार

साइबर स्पेस में बच्चों का शोषण



थ्रेट वेक्टर

साइबर स्टॉकिंग

साइबर बुलीइंग

ऑनलाइन ग्रूमिंग



सोशल मीडिया
प्लेटफॉर्म

इम्पेर्सोनेशन

आइडेंटिटी थ्रेफ्ट



फ़िशिंग



ऑनलाइन
गेमिंग

सेक्सटॉरशन

ऑनलाइन गेमिंग



मैसेजिंग ऐप

ऑनलाइन जॉब
स्कैम



वेबकैम



ईमेल



वीडियो चैट
प्लेटफॉर्म

यौन शोषण और बाल दुर्व्यवहार

वित्तीय धोखाधड़ी और घोटाले

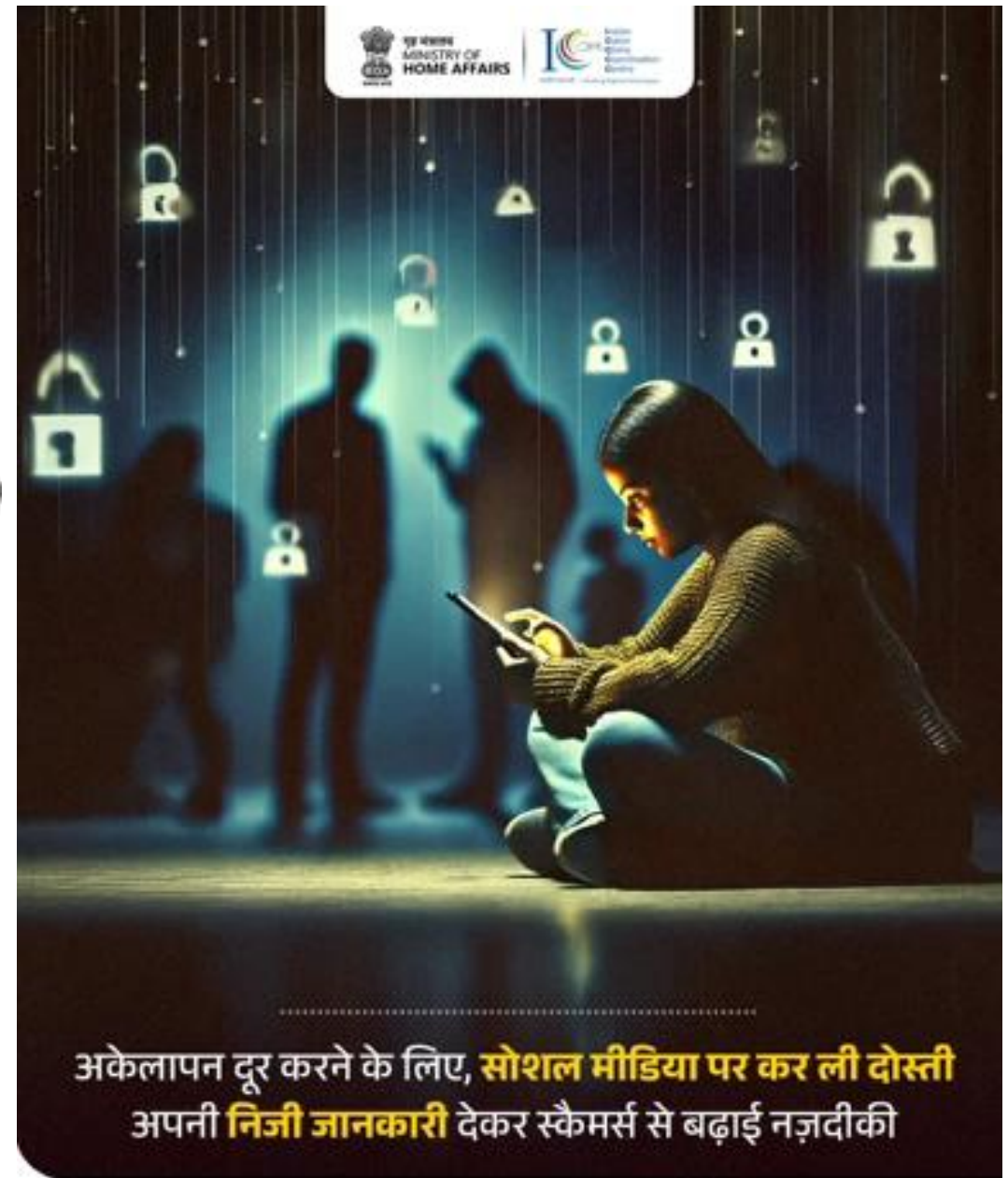
साइबर स्टॉकिंग और बुलीइंग



≡ INDIA TODAY

Delhi Police nabs cyber stalker for harassing, issuing death threats to woman

Rizwan Ansari, a 30-year-old man from Delhi, was arrested by the police for cyberstalking and for threatening a woman on Facebook. He allegedly used abusive language and threatened the woman that he would kill her if she did not talk to him and love him.



अकेलापन दूर करने के लिए, सोशल मीडिया पर कर ली दोस्ती
अपनी निजी जानकारी देकर स्कैमर्स से बढ़ाई नज़दीकी

अधिक जानकारी के लिए CYBERDOST को  पर फॉलो करें



CHILDREN'S DAY
SPECIAL

**CHAPTER
02**



ऑनलाइन ग्रूमिंग



Pedophiles 'cyber grooming' children for pornography

Soumitra Bose / TNN / May 28, 2020, 04:56 IST



Nagpur: Maharashtra cyber intelligence and analytical cell has issued an advisory, warning parents regarding paedophiles 'cyber grooming' children for pornographic posts by luring them with various incentives and offers. The government of Maharashtra has launched 'Operation Blackface' to tackle such child [pornography](#).

A steep rise in browsing of pornographic posts during lockdown following Covid outbreak has brought with it the peril of vulnerable children falling prey to paedophiles.



अनजान प्रोफ़ाइल से आई फ्रेंड रिक्वेस्ट,
15 साल की शीला ने बिना सोचे-समझे कर ली एक्सेप्ट

अधिक जानकारी के लिए CYBERDOST को पर फॉलो करें

Gets a friend request....



STOP. THINK. ACT

 **Beware of unknown/shady profiles**

 **Feel uncomfortable? Talk to someone trusted**

 **Need help? Call ☎ 1930 or visit cybercrime.gov.in**

 **Child Helpline number: ☎ 1098**

 **Share your issues with confidants.**



Think before you connect



Not every request is a 'friend' request



Share with someone you trust



FOR MORE INFO, FOLLOW **CYBERDOST**  ON     

FOR MORE INFO, FOLLOW **CYBERDOST**  ON     

ऑनलाइन गेमिंग



Shady Bets: How to Protect Yourself from Gambling Fraud Online

Scammers are using fake betting game advertisements on social media to target users, with over 500 deceptive advertisements and 1,377 malicious websites identified by Group-IB CERT. These scams promise quick money but are designed to steal personal data and funds, and this blog aims to educate users on how to recognize and protect themselves from such threats.



Int'l gang involving Rs 190cr gaming apps scam busted; 11 held



Varanasi: Busting an international gang of cyber fraudsters, who duped people of over Rs 190 crore through various gaming apps, Azamgarh police arrested 11 of its members and recovered Rs 35 lakh cash from their possession.

The police also ensured freezing of over Rs 2 crore deposited in 169 bank accounts belonging to the gang. A total of 71 cases have been lodged against the gang across the country.



ऑनलाइन जॉब स्कैम

Online Task के बदले दिया कमाई का लालच, स्कैमर्स ने ठग लिए 51 लाख रुपये, Scam से खुद को ऐसे रखें सेफ

Cyber Crime की बढ़ती घटनाओं के बीच नोएडा से एक नया मामला सामने आया है. यहाँ ऑनलाइन टास्क पूरा करने के बदले कमाई का लालच देकर ठगों ने युवक से 51 लाख रुपये की ठगी कर ली.

By : एबीपी टैक डेस्क | Edited By: Pramod Kumar | Updated at : 03 Feb 2025 04:00 PM (IST)



नोएडा में स्कैमर्स ने युवक से 51 लाख रुपये की ठगी की है



साइबर स्लेवरी : मानव तस्करी

MINISTRY OF HOME AFFAIRS
IC
NATIONAL CYBER CRIME CENTER
NCC

???

**GOT A JOB IN
CAMBODIA
MYANMAR, Lao PDR?**

**FAKE JOB
OFFER**

MYANMAR
LAO PDR
CAMBODIA

**YOU MAY END UP AS
CYBER SLAVE**

AND BE FORCED TO COMMIT CYBERCRIMES

- ✓ TRUST VERIFIED/GOVERNMENT AGENTS.
- ✓ PLEASE VERIFY THE OFFER CAREFULLY.
- ✓ CHECK DETAILS OF WORK VISA.
- ✓ RESEARCH THE ORGANIZATION OFFERING THE JOB.

DIAL CYBER HELPLINE 1930 OR VISIT WWW.CYBERCRIME.GOV.IN

FOLLOW CYBERDOST ON:



Operation Cyber Slaves: Stories of 'Golden Triangle', network of fake job offers

India Today's special Investigation Team managed to track down some of the survivors of the cyber slave camps in Southeast Asia, and recorded their stories. These are cautionary tales for all those tempted by dubious job offers from the 'Golden Triangle'.

स्टॉक निवेश घोटाला

Senior citizen from Bangalore joins training session online to learn stock investment, ends up losing Rs 6 crore

A senior citizen from Bangalore was duped into losing Rs 6.41 crore through an elaborate online investment scam. The fraudsters, posing as investment trainers, lured the victim via WhatsApp with promises of high returns and professional stock market insights.



वैवाहिक / डेटिंग धोखाधड़ी

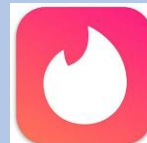
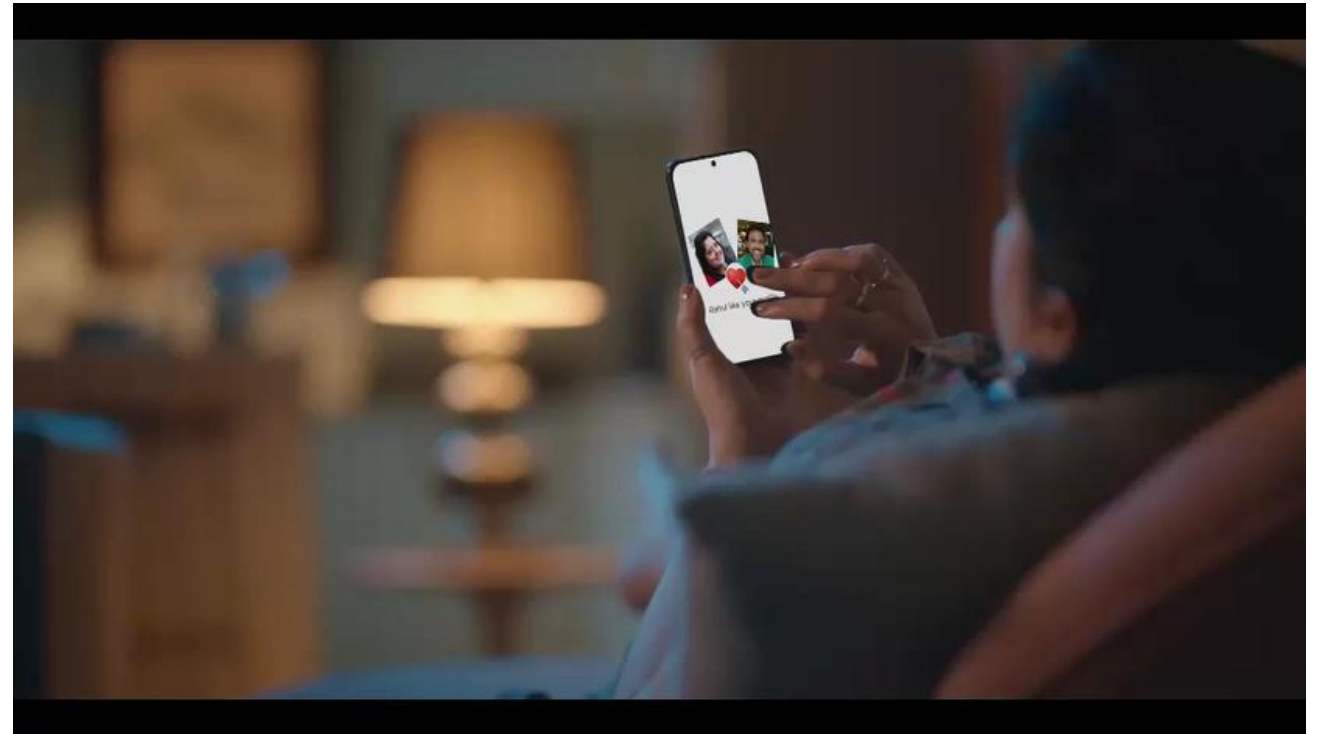
Pune

Online Matrimonial Fraud: Pune Woman Loses Rs 27 Lakh to Fake Groom

Kondhwa, 14th February 2025: A case of financial fraud through a matrimonial website has surfaced in Kondhwa, where a woman was allegedly deceived of ₹27 lakh by a man she met online. The victim has filed a complaint against the accused, Amit Chavan, at the Kondhwa Police Station.

Man cheats 500 single people using fake matrimonial sites: Modus operandi revealed

The fake matrimonial websites were promoted on social media platforms such as Facebook and Instagram, using photos of women downloaded from the internet to fabricate enticing profiles.



डिजिटल अरेस्ट : डिम्पेर्सॉनेशन स्कैम

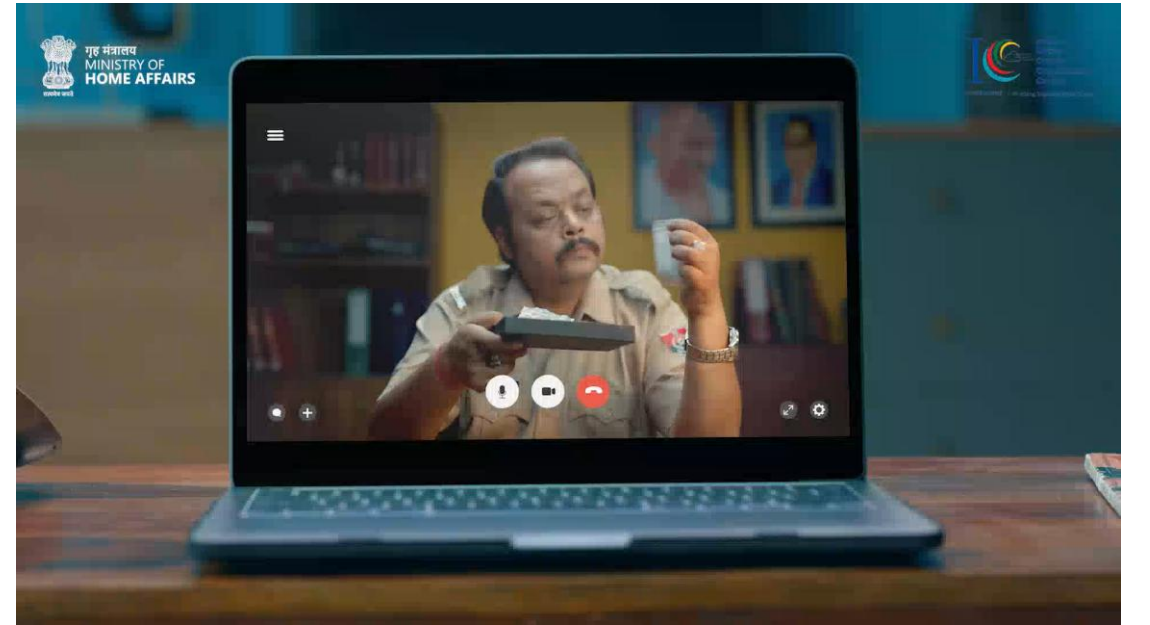
Elderly woman loses ₹20 crore to 'digital arrest' fraud; 3 held

One of the fraudsters posed as a 'CBI officer' to extort money from the woman adding three persons have been arrested in connection with the crime which took place between December 26, 2024 and March 3 this year

Published - March 20, 2025 05:38 pm IST - Mumbai

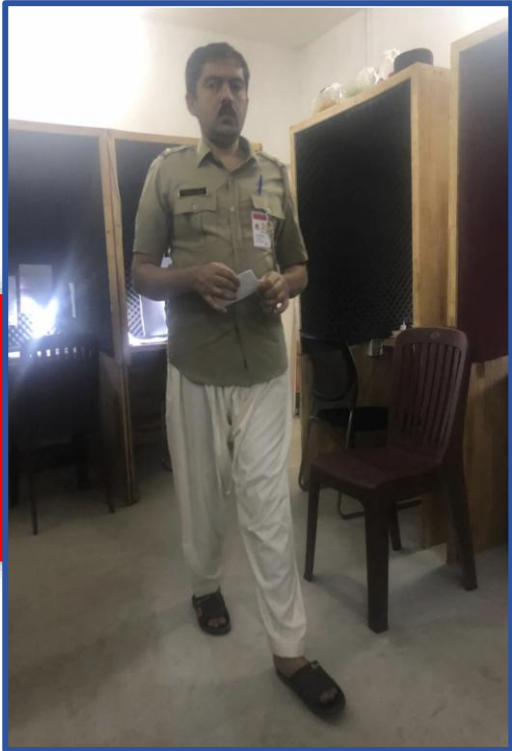
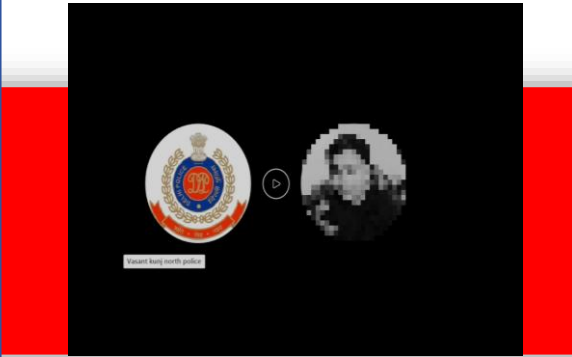
82-Year-Old Woman Falls Prey To 'Digital Arrest Scam' In Ghaziabad; Gets Duped Of Rs 9 Lakh By Fraudsters Posing As Mumbai Police

An 82-year-old woman from Indirapuram, Ghaziabad, was digitally arrested by some fraudsters posing as Mumbai Police officers, who defrauded her of Rs 9 lakh.



नकली पुलिस (इम्पेर्सोनेशन स्केम)

Fraudster posing as Fake Police Officers



धोखाधड़ी में डीपफेक का उपयोग

डीपफेक स्कैम से डरो नहीं रिपोर्ट करो

संकेत

- मशहूर हस्तियों द्वारा निवेश सलाह
- वीडियो और चेहरे के हाव-भाव में मेल न हो
- असामान्य पृष्ठभूमि या चेहरा
- अनवैरिफाइड टिप्स और ऐप्स

सुरक्षित रहें

- संदिग्ध वीडियो की पुष्टि करें
- ऐसी वीडियो से सोशल मीडिया पर सावधान रहें
- अगर किसी डीपफेक ने आपको धोखा दिया है तो तुरंत 1930 या cybercrime.gov.in पर रिपोर्ट करें

Bengaluru Residents Duped Of Rs 95 Lakh By Deepfake Videos Of Narayana Murthy And Mukesh Ambani

Recently, Bengaluru witnessed a concerning instance of cyber fraud involving deepfake videos of two prominent Indian businessmen: Infosys co-founder N. R. Narayana Murthy and Reliance Industries Chairman Mukesh Ambani. As per reports, these fraudulent videos were used as bait to deceive two individuals, leading to collective financial losses amounting to approximately Rs 95 lakh.

25 arrested in global hit against AI-generated child sexual abuse material

Europol has supported authorities from 19 countries in a large-scale hit against child sexual exploitation that has led to 25 arrests worldwide. The suspects were part of a criminal group whose members were engaged in the distribution of images of minors fully generated by artificial intelligence (AI).

Instagram

Jayla Kirk
Sponsored



Put in Rs 21,000 in February, you can earn Rs 1,700,000 in 28 days

Learn more

927 34

77,871 views

Learn more

View all comments

cyberdosti4c
GOOD NEWS · Political News

साइबर अपराध-मानसिक स्वास्थ्य पर असर

VIDEO: Agra Teacher Dies Due To Heart Attack Following 'Digital Arrest' Scam; Gets Fake Call Claiming Daughter Caught In Sex Racket

The woman could not bear the news and suffered heart attack and died. The incident was caught on the CCTV camera installed inside in her house and the video of the incident is going viral on social media.

Scientist Duped Of ₹ 71 Lakh After "Digital Arrest" By Fraudsters In Madhya Pradesh: Cops

Digital arrests are a new method of cyber fraud in which fraudsters make audio or video calls, pose as law enforcement officers and confine victims to their homes to scam them.

India News | Press Trust of India | Updated: October 05, 2024 12:15 am IST

Threatened by sextortionists, teen kills self

TNN / Updated: Jan 22, 2024, 11:43 IST

SHARE PRINT AA FOLLOW US

AHMEDABAD: A 15-year-old boy from Saraspur

Student dies by suicide after falling victim to cyberfraud

TNN / Jun 18, 2024, 04:22 IST

SHARE PRINT AA FOLLOW US



Bengaluru: A 20-year-old college student allegedly died by suicide in her hostel room Sunday night. She is suspected to have taken the step after losing a few thousand rupees to a cyberfraud.

The deceased, Pavana from KGF in Kolar district, was a first-year BSc student at Maharani Cluster University. Citing preliminary investigation, police said the hostel staff found Pavana hanging in her room at midnight.

News / Cities / Pune / After 'sextortion' calls demanding Rs 51 lakh, man commits suicide; probe on

After 'sextortion' calls demanding Rs 51 lakh, man commits suicide; probe on

आधार रेखा (शून्य विश्वास दृष्टिकोण)

सावधान रहें यदि
ऑफर:

इतना अच्छा है की
लगता नहीं की सच
है

उर्जेन्सी

आप में लालच पैदा
करना

धमकी देना या डर
पैदा करना

कैसे पहचानें कि
कॉल/ऑनलाइन जानकारी
वास्तविक है या जालसाजी?

सावधान रहो

अज्ञात कॉल/वीडियो
कॉल

कॉल/टेक्स्ट संदेश, जो
देखने में परिचित लगते हैं,
लेकिन अज्ञात नंबरों से
आते हैं

भारतीय साइबर अपराध समन्वय केन्द्र (I4C)



सहवीर्य करवावहै • Working Together With Vigour

Overview of I4C



सहवीर्य करवावहै • Working Together With Vigour

दृष्टि

भारत के नागरिकों के लिए एक सुरक्षित साइबरस्पेस बनाना

उद्देश्य

देश में साइबर अपराध की रोकथाम, पता लगाने, जांच और अभियोजन के लिए एक प्रभावी ढांचा और पारिस्थितिकी तंत्र बनाना.

Report Suspect Data on NCRP Portal



<https://cybercrime.gov.in/>

- REGISTER A COMPLAINT +
- TRACK YOUR COMPLAINT
- SUSPECT DATA +**
- CYBER VOLUNTEERS +
- LEARNING CORNER +
- CONTACT US

- ▶ SUSPECT SEARCH (MOBILE, EMAIL, ETC.)
- ▶ SUSPECT SEARCH (WEBSITE/APP)
- ▶ REPORT SUSPECT**








This facility has been created for quick reporting of Attempts made to access Confidential Website URLs, Whatsapp Numbers/ Telegram Handles, Phone Numbers, Email-IDs, SMS Headers/ Numbers and Social Media URLs etc. This will be used to build up a repository for analysis and monitoring of cybercrime.

If you have become a victim of Cybercrime, please report immediately at <https://www.cybercrime.gov.in/> or 1930 National Helpline Number.

State of Incident*

---Select---

What do you want to report ?

 Website URL	 Whatsapp Number / Telegram Handle	 Phone number	 Email Id	 SMS Header/ Number	 Social Media URL	 Deepfake
--	---	--	---	---	---	---

Reporting of Content on Social Media

भारत सरकार
GOVERNMENT OF INDIA

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

Indian
Cyber
Crime
Coordination
Centre
राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
Working Together With Vigor

Register a Complaint + Track your Complaint Report & Check Suspect + Cyber Volunteers + Learning Corner + Citizen Survey Contact Us

Suspect Data > Suspect Repository > Report Abuse to social Media

- Suspect Repository +
- Report Suspect +
- File an Appeal with GAC

- Report Suspect to I4C
- Report Abuse to Social Media
- Report Abuse to NCMEC
- Know your Mobile connections - TAF COP

Report Abuse to Social Media Intermediary

Citizens can report any online illegal activity directly to social media Intermediaries by using the links provided below.



Facebook



Twitter (now X)



Google



Instagram



Telegram



WhatsApp



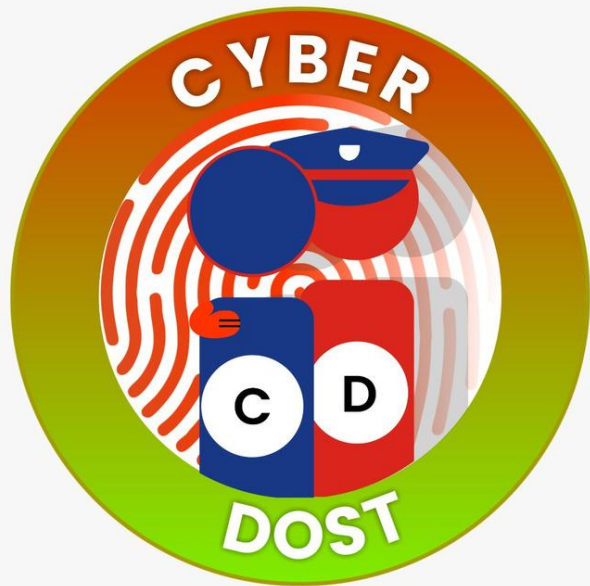
YouTube



Public



Koo



CYBERDOST

I4C



X: <https://x.com/Cyberdost>

FB: <https://www.facebook.com/CyberDostI4C/>

Insta: <https://www.instagram.com/cyberdosti4c/?hl=en>

WhatsApp: <https://whatsapp.com/channel/0029Va3VAOY8fewrOtXqMw1V>

Public: <https://public.app/user/profile/1ZCQuF5wrRbR9lcsrtcZgsPkYfC2>

ShareChat: <https://sharechat.com/cyberdost?referer=bottomNav>

Telegram: <https://t.me/cyberdosti4c>

YouTube: <https://www.youtube.com/@cyberdosti4c/featured>

LinkedIn: <https://www.linkedin.com/company/cyberdosti4c>



ABOUT CYBERDOST

साइबरदोस्त भारतीय साइबर अपराध समन्वय केंद्र (I4C) का आधिकारिक सोशल मीडिया है।

9 विभिन्न प्लेटफॉर्म पर साइबरदोस्त की सामग्री और पहलों से 18 लाख से अधिक अनुयायी जुड़े हुए हैं

साइबरदोस्त इंस्टाग्राम पर ट्रेंडिंग मीम्स और रील्स का उपयोग करता है जो युवाओं को पसंद आते हैं.

CYBER DOST CyberDost I4C
2,603 posts 232K followers 98 following

Official handle of Indian Cybercrime Coordination Centre (I4C), Ministry of Home Affairs, GoI | Raising awareness against Cybercrimes | 📞 1930
www.cybercrime.gov.in and 1 more

Followed by [gulatayyye](#), [venubatra_17](#) and 8 others

Following Message

Cyber Safe... Report Link Amitabh Ba... ₹GawaneKe... StopThin

WhatsApp OTP Scam Alert
साइबर अपराध का अंत कैसे करें?
जानिए SP Jamtara से



STOP THINK TAKE ACTION STAY CYBERSAFE

REPORT ANY CYBERCRIME AT **1930** OR REGISTER ONLINE COMPLAINT ON **CYBERCRIME.GOV.IN**

CYBER DOST

CyberDost I4C ✓

@cyberdosti4c

49.5K subscribers · 896 videos

Official handle of the Indian Cybercrime Coordination Centre (I4C), MHA, Gol ...more

cybercrime.gov.in and 8 more links

Manage videos

Home Videos Shorts Live Playlists

Shorts

WhatsApp Safe with CyberDost

आपके सवाल, हमारे जवाब #CyberSafeLive

155 views

WhatsApp OTP Scam Alert

2.5K views

CYBER CRIME BREAKING NEWS

602 views



ABOUT CYBERDOST

महत्वपूर्ण साइबर जागरूकता संदेशों को प्रसारित करने के लिए सूचनात्मक कैरोसेल और GIF का उपयोग करता है.

यूट्यूब जैसे प्लेटफॉर्म पर विशेष लाइव सत्र आयोजित करता है जिसमें विशेषज्ञ सुरक्षा संबंधी सुझाव देते हैं.

इसका उद्देश्य नागरिकों को ऑनलाइन सुरक्षा के लिए सशक्त बनाना, जागरूकता और सतर्कता को बढ़ावा देना है.

आकर्षक पुरस्कारों के साथ रोचक प्रतियोगिताएं

CYBER CRIME PREVENTION

HANDBOOK

ESSENTIAL
DOS AND DON'TS
FOR LATEST CYBER CRIMES

STOP. THINK. TAKE ACTION



साइबर अपराधों से बचाव हेतु मार्गदर्शिका

साइबर अपराधों से बचाव के लिए जरूरी
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
Wasting	12
Quitting	13
Search Engine Fraud	14
Social Media Impersonation	15



KYC Scam

KYC (Know Your Customer) is a process of identifying and verifying the identity of a customer. It is a mandatory requirement for all financial institutions, banks, and other entities. Scammers use this process to steal your personal information, identity, and assets. They use various methods to trick you into providing your details. This handbook provides detailed information on how to identify and avoid such scams. It also provides a checklist of Do's and Don'ts to help you stay safe.

- | ✓ Do's: | ✗ Don'ts: |
|--|---|
| <ul style="list-style-type: none"> Verify Requests: Contact your bank or financial institution directly to confirm any KYC update requests. Use Official Channels: Only 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: Compare with your bank about the available methods for updating KYC details. | <ul style="list-style-type: none"> Protect Credentials: Never share your account log-in details, card information, PIN, passwords, or OTPs with anyone or on untrusted websites/apps. Secure Documents: Do not share KYC documents or their copies with unknown or untrusted individuals or organizations. Avoid Suspicious Links: Do not click on suspicious or untrusted links received via mobile or email. |

Online Job

Online Job Scams trick you on websites, social media. Their goal is to steal the

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



Digital Arrest

- ✓ **Do's:**
- Secure Devices: Always use secure devices and avoid using public Wi-Fi networks.
 - Back Up Data: Regularly back up your data to a secure location.
 - Use Strong Passwords: Use strong, unique passwords for all accounts.
 - Report Incidents: Report any suspicious activity to the relevant authorities.
 - Stay Informed: Keep yourself updated on the latest cyber threats and prevention methods.
- ✗ **Don'ts:**
- Don't Click: Do not click on suspicious links or download files from untrusted sources.
 - Don't Share: Do not share your personal information or sensitive data on untrusted websites or apps.
 - Don't Ignore: Do not ignore any suspicious activity or warnings from your devices.
 - Don't Panic: Stay calm and report any incidents to the relevant authorities.



सत्यमेव जयते

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS



Thanks