इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Digital India
Power To Empower

NIC एन आई सी
National Informatics Centre

ISEA
www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

AI IMPACT SUMMIT

सुरक्षित इंटरनेट दिवस

स्मार्ट तकनीक,सुरक्षित विकल्प, एआई के सुरक्षित और जिम्मेदार उपयोग

SAFER INTERNET DAY

Smart tech, safe choices, exploring the safe and responsible use of AI

Date : 10th February 2026

Social Media Presence

www.isea.gov.in

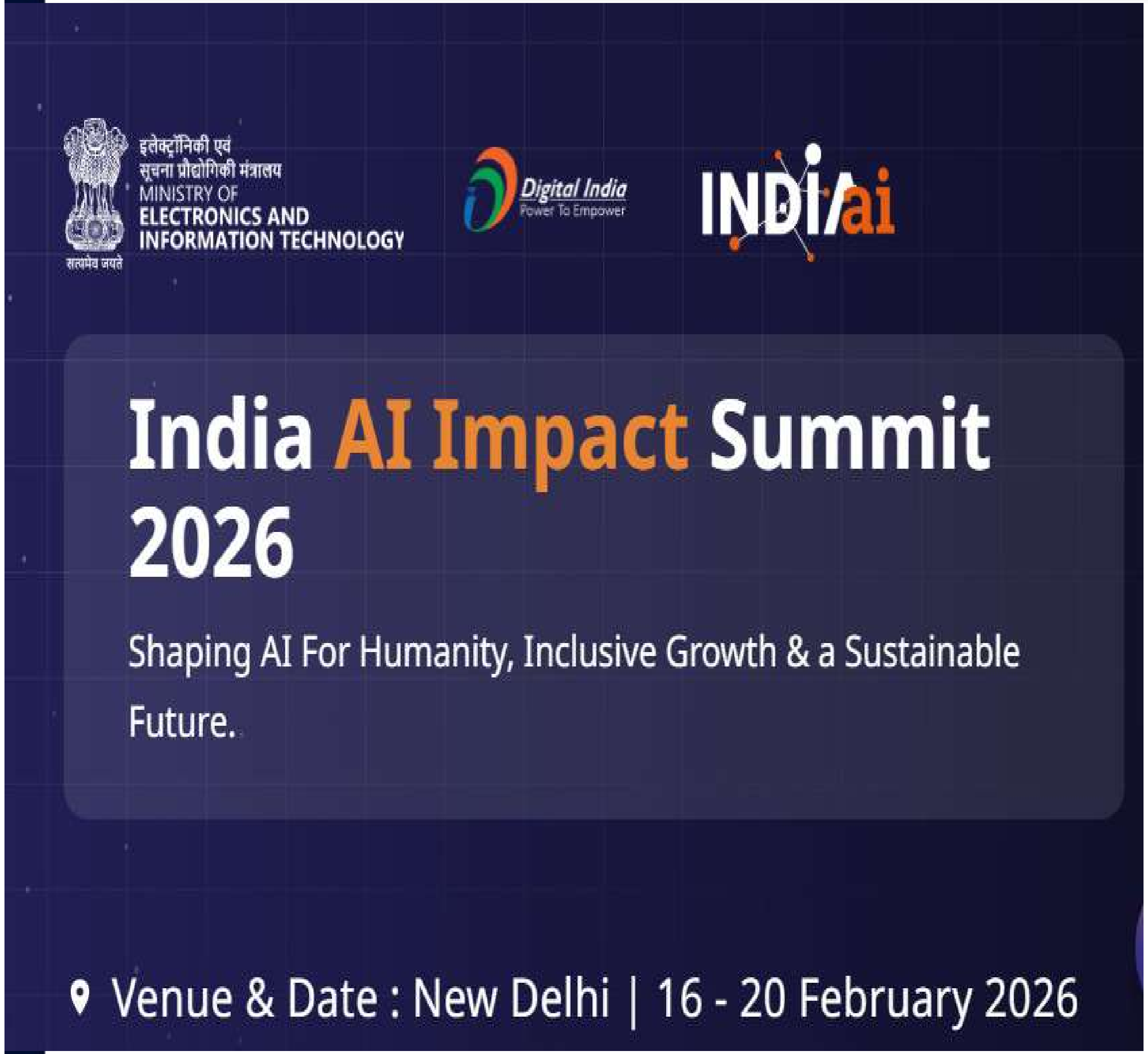
Information Security Education and Awareness (ISEA) Project

staysafeonline.in

Celebrating “ Safer Internet Day”

Smart tech, safe choices, exploring the safe and responsible use of AI

- Safer Internet Day is observed worldwide on the second Tuesday of every February to
  - Sensitize users about safe and responsible use of internet and AI
  - Promote best practices for cyber hygiene
  - Educate users about major cyber threats and mitigation techniques
- Ministry of Electronics and Information Technology (MeitY) is celebrating a nationwide awareness campaign on 10th February, 2026 under the aegis ISEA Project in collaboration with NIC and



इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Digital India
Power To Empower

INDIAai

India AI Impact Summit 2026

Shaping AI For Humanity, Inclusive Growth & a Sustainable Future.

Venue & Date : New Delhi | 16 - 20 February 2026

Core Focus

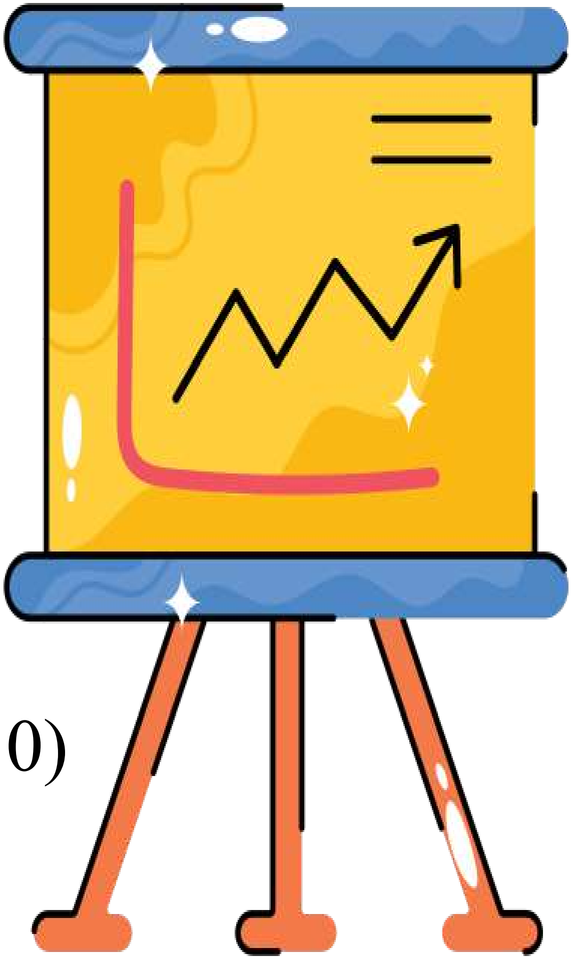
- **Democratizing AI** access and addressing the *AI divide* among nations and communities.

- Emphasis on **responsible, inclusive, and people-centric AI** for economic and social development.

- Promoting AI use in key sectors like **healthcare, agriculture, education, and governance**.

Outline of the presentation:

- About the Internet
- Use of Internet in our Day-to-Day life
- Safe Use of Internet (Internet Safety)
- Safe and Responsible use of AI
- Common Cyber Threats of AI
- Cyber Hygiene Practices
- Mechanism to report cybercrimes (1930)
- Awareness Resources for Staying Safe Online (www.staysafeonline.in)



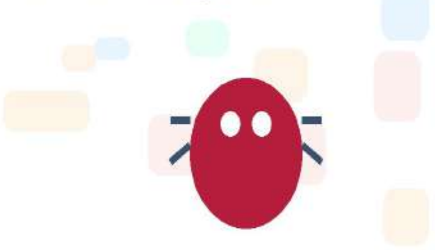
Common Cyber Threats

Phishing

OTP / UPI Fraud

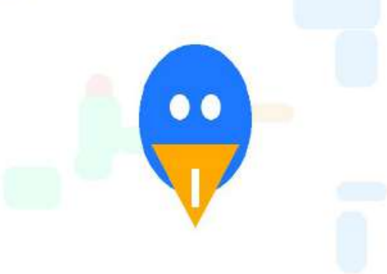
Fake Customer Care

Malware / Spyware



Remote Access Scam

Deepfake / AI Voice Scam



OTP / UPI Fraud

- Scammers trick victims into sharing OTP or UPI PIN.
- May ask to 'accept' request for refund or prize.
- Never share OTP/UPI PIN with anyone.
- For receiving money: you NEVER need to enter UPI PIN.

staysafeonline.in

Investment Frauds

Investment frauds deceive individuals into investing in fake or misleading opportunities, promising high returns with little to no risk.

- Scammers use money from new investors to pay earlier investors, creating an illusion of profits. Eventually, the scheme collapses.

- Fake crypto projects promise huge returns but disappear with investors’ money.

- Fake Real Estate Investments – Fraudsters sell non-existent properties or promise unrealistic rental income.

Fake Customer Care Scam

- **Fake helpline numbers** posted on Google/social media.
- They ask you to **install apps** or share screen.
- **Never install remote apps** for support.
- Use numbers only from **official website/app**.

Social Media Account Hacking

- Accounts **hacked via weak/reused passwords** or fake login pages.
- Hackers send **scam messages** to contacts.
- **Enable 2FA and use unique passwords**.
- **Avoid clicking 'login' links from unknown** messages.

HACKED
Send Payment Request
Hey, can you urgently send a ₹5000?
Hey, can you urgently send a ₹5000?

Online Shopping Scam

- **Fake websites/Instagram pages** offer heavy discounts.
- Payment taken but **no product delivered**.
- Check reviews, GST details, return policy.
- Prefer **COD or trusted marketplaces**.

Digital Arrest Scam

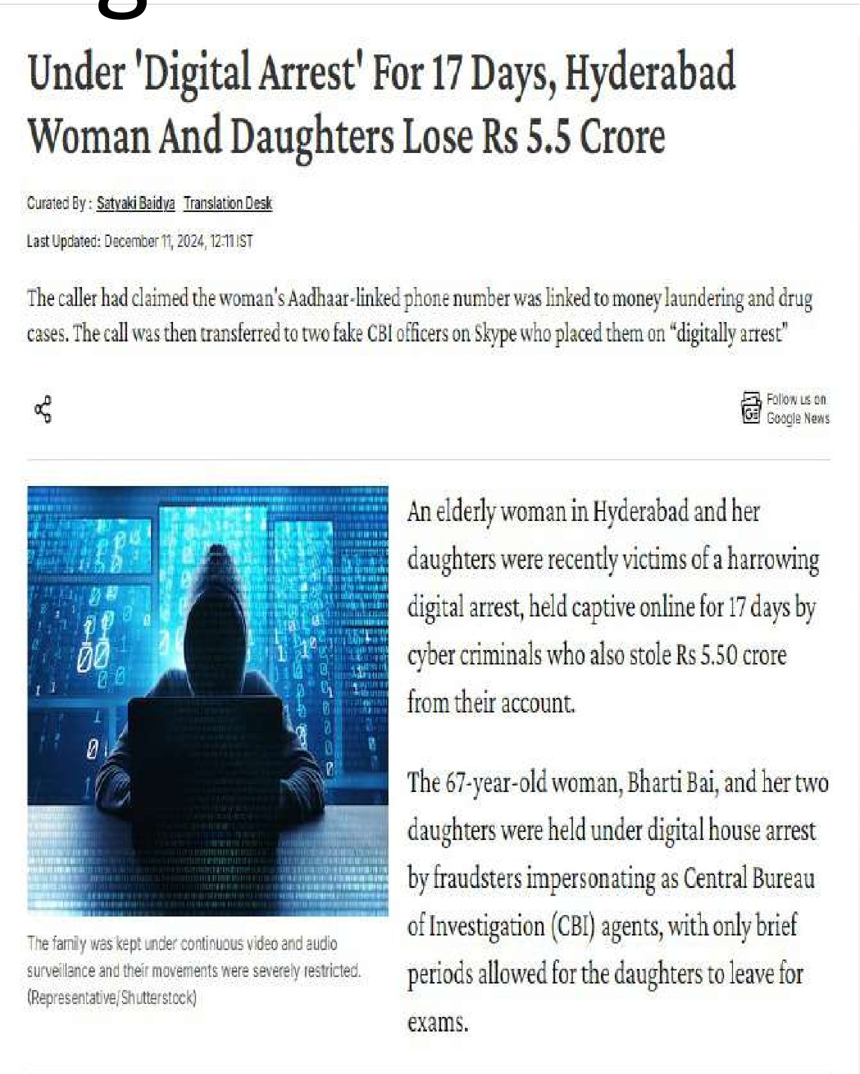
- Fraudsters **pose as police/CBI/customs/RBI officers**

- Threaten **arrest and demand money** immediately

- **No agency arrests via video call** or demands payment

- **Cut call and report** to cybercrime portal/ 1930

Digital Arrest is Fraud



Under 'Digital Arrest' For 17 Days, Hyderabad Woman And Daughters Lose Rs 5.5 Crore

Curated By : Satyaki Baidya Translation Desk

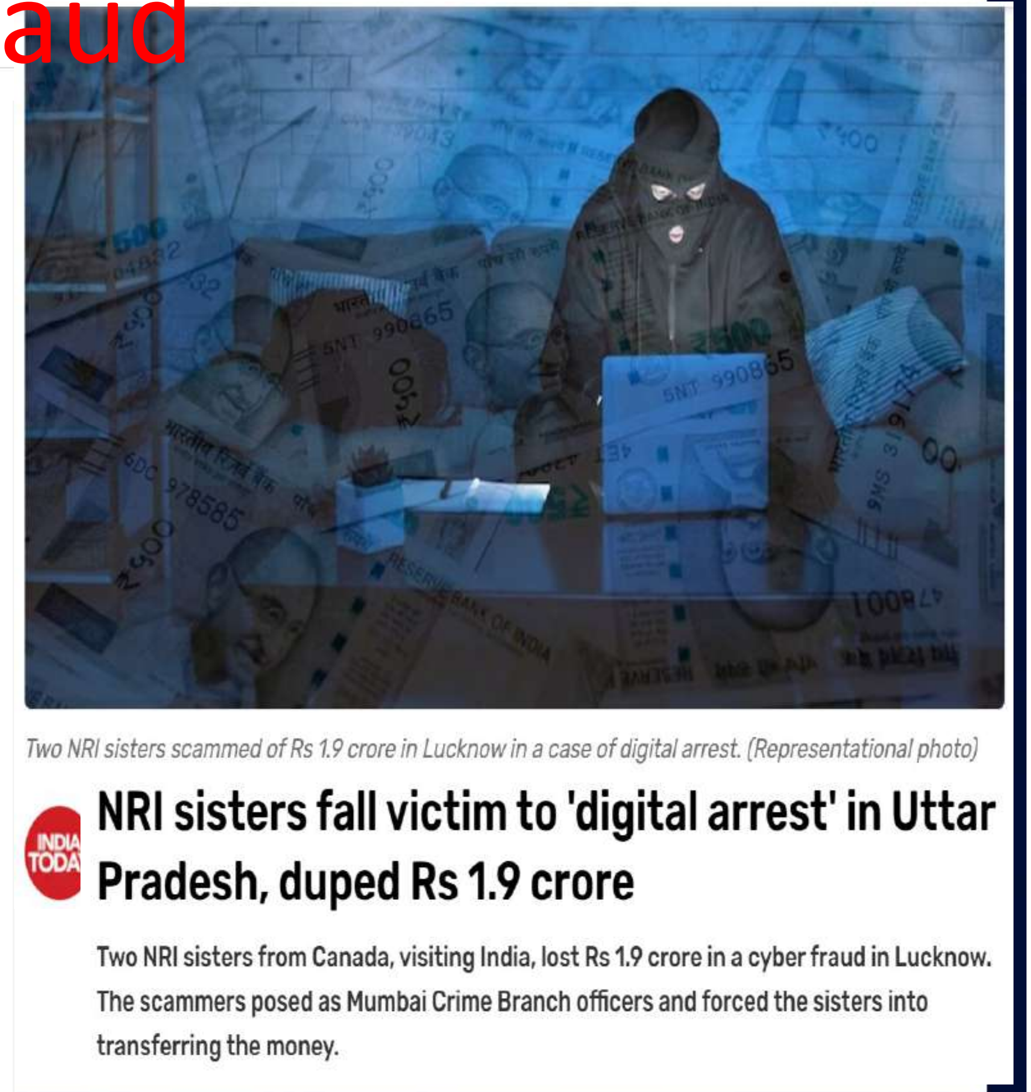
Last Updated: December 11, 2024, 12:11 IST

The caller had claimed the woman's Aadhaar-linked phone number was linked to money laundering and drug cases. The call was then transferred to two fake CBI officers on Skype who placed them on "digitally arrest"

The family was kept under continuous video and audio surveillance and their movements were severely restricted. (Representative/Shutterstock)

An elderly woman in Hyderabad and her daughters were recently victims of a harrowing digital arrest, held captive online for 17 days by cyber criminals who also stole Rs 5.50 crore from their account.

The 67-year-old woman, Bharti Bai, and her two daughters were held under digital house arrest by fraudsters impersonating as Central Bureau of Investigation (CBI) agents, with only brief periods allowed for the daughters to leave for exams.



Two NRI sisters scammed of Rs 1.9 crore in Lucknow in a case of digital arrest. (Representational photo)

NRI sisters fall victim to 'digital arrest' in Uttar Pradesh, duped Rs 1.9 crore

Two NRI sisters from Canada, visiting India, lost Rs 1.9 crore in a cyber fraud in Lucknow. The scammers posed as Mumbai Crime Branch officers and forced the sisters into transferring the money.

<< Scan to know mre about Digital Arrest

DIGITAL ARREST IS A FRAUD

- No Government agency (Police, CBI, ED) can investigate or arrest you over video or voice calls.
- Don’t Panic! Do not share any personal information over calls
- Before acting, check and confirm with concerned authority.
- Preserve evidence.

- कोई भी सरकारी एजेंसी (पुलिस, सीबीआई, ईडी) वीडियो या वॉयस कॉल पर आपकी जांच या गिरफ्तारी नहीं कर सकती।
- घबराये नहीं! कोई भी निजी जानकारी कॉल पर साझा न करें।
- कुछ भी करने से पहले, परिवार या संबंधित अधिकारी से पुष्टि करें।
- सबूत सुरक्षित रखें

What To Do If You Become a Victim

- Immediately **inform your bank and block cards/UPI** if needed

- **Change passwords** for email, banking, social media

- **Save evidence: screenshots**, call recordings, transaction IDs

- Report quickly on National Cyber Crime Reporting Portal (cybercrime.gov.in)

To Do If You Become a V
Report the Crime
Call the police and cybercrime helpline 1930
Inform Your Bank
Immediately freeze your accounts/cards
Contact Authorities
File a complaint on cybercrime.gov.in
Secure Your Accounts
Change passwords, secure accounts
1930
cybercrime.gov.in

staysafeonline.in

Key Safety Rules

- **Never share** OTP / UPI PIN / passwords.
- **Do not click** unknown links.
- Verify customer care numbers from official sources only.
- Use **strong passwords + 2FA**.
- **Install apps** only from trusted stores.
- If unsure: **STOP, THINK, VERIFY.**

Don't share OTP, PIN, passwords

Be wary of trusted links or apps

Avoid phone calls from unknown numbers

If scammed, inform police and bank

Use anti-virus software

Regularly update PIN, passwords

staysafeonline.in