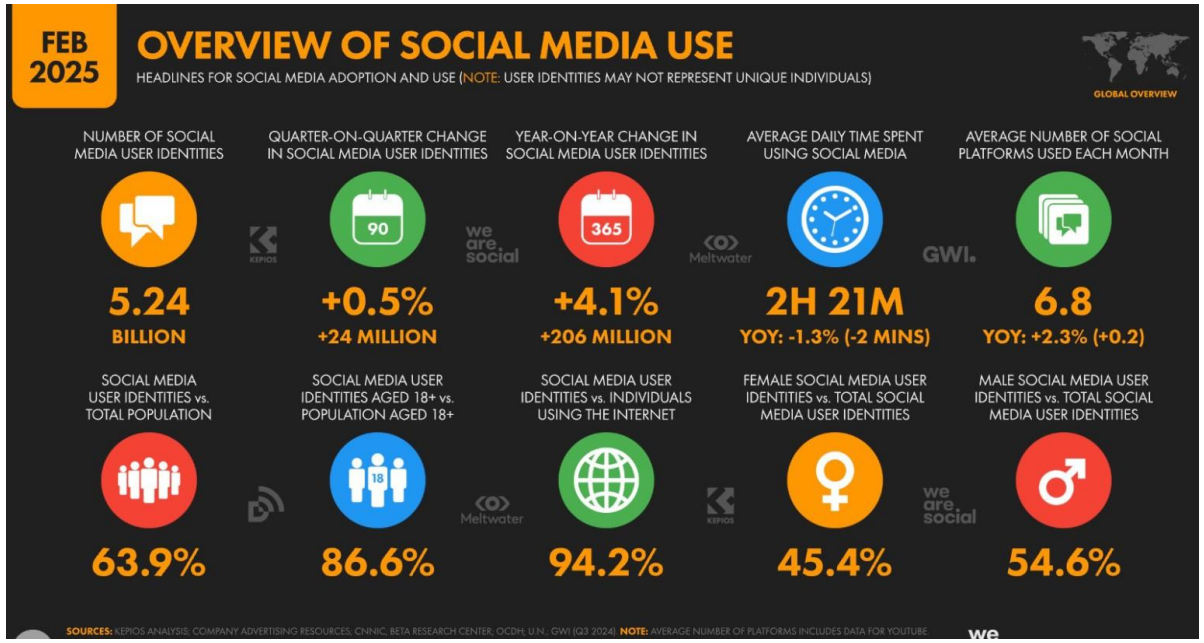
SESSION TWO · 60 MINUTES · PRACTITIONER WORKSHOP

सूचना लचीलापन और प्रतिक्रिया का निर्माण

खतरे को समझने से लेकर उसके बारे में कुछ करने तक — हेरफेर को पहचानने, दावे की जाँच करने और बिना स्थिति बिगाड़े प्रतिक्रिया देने के व्यावहारिक कौशल।

शिक्षा मंत्रालय · NCERT · CyberPeace Foundation



Internet Users in the world

Total number of Websites

Emails sent today

3,530,059,080

Google searches today

3,406,180

Blog posts written today

363,326,622

Tweets sent today

परिभाषा

सूचना लचीलापन का वास्तव में क्या अर्थ है

यह नहीं है

- कौन से दावे सच हैं यह जानना। आप इंटरनेट को याद नहीं कर सकते।
- हर चीज़ पर अविश्वास करना। पूर्ण संशयवाद वही हार है जो पूर्ण भोलापन।
- फैक्ट-चेक का इंतज़ार करना। जब तक यह आता है, नुकसान भावनात्मक होता है, तथ्यात्मक नहीं।
- एक तकनीक जो कोई और आपके लिए स्थापित करता है।

यह है

- उस पल को पहचानना जब आप सोचना बंद करते हैं और प्रतिक्रिया करना शुरू करते हैं।
- फॉरवर्ड करने से पहले एक प्रक्रिया चलाना — हर बार वही एक।
- वास्तविक रिपोर्टिंग चैनल कहाँ हैं, यह ज़रूरत पड़ने से पहले जानना।
- एक ऐसा नोड होना जो अफवाह को तेज़ करने की बजाय धीमा करे।

इसे प्रतिरक्षा समझें, कवच नहीं। प्रतिरक्षा संपर्क नहीं रोकती — यह संपर्क को संक्रमण बनने से रोकती है।

60 मिनट की योजना

यह घंटा कैसे बना है

ध्यान दो — 12 min

1

अपहरण को पकड़ो जब वह हो रहा हो — अपने शरीर में, इससे पहले कि आपकी राय बने।

जाँच करो — 16 min

2

90 सेकंड की सत्यापन प्रक्रिया। चित्र, वीडियो, स्रोत, और डीपफेक ने क्या तोड़ा।

प्रतिक्रिया दो — 16 min

3

बिना बढ़ाए सुधारो। पारिवारिक ग्रुप को संभालो।

वास्तविक चैनलों से रिपोर्ट करो।

निर्माण करो — 10 min

4

ऐसी आदतें जो सप्ताह भर टिकें, साथ ही भारत का अपना ज्ञानमीमांसा टूलकिट।

अंतिम 6 मिनट: खुले प्रश्न — वह फॉरवर्ड लाएँ जिसे आप हल नहीं कर पाए।

01

ध्यान दो

अपहरण को पकड़ो जब वह अभी हो रहा हो। राय बनने से पहले, अंगूठा चलने से पहले।

आपके पास सबसे विश्वसनीय हेरफेर डिटेक्टर आपका ज्ञान नहीं है। यह आपकी नब्ज़ है।

01 · ध्यान दो

आपका शरीर आपके दिमाग से पहले चेतावनी देता है

हेरफेर की गई सामग्री एक शारीरिक अवस्था पैदा करने के लिए इंजीनियर की जाती है। वह अवस्था अलार्म है — इसे अलार्म के रूप में सुनना सीखें।

गर्मी

पढ़ने के दो सेकंड के भीतर गुस्से, घृणा या डर की लहर। आपने अभी कुछ भी मूल्यांकन नहीं किया है — आपको खुराक दी गई है।

तात्कालिकता

“I have to send this NOW.” Real information is almost never time-critical to forward. तात्कालिकता एक निर्मित सामग्री है।

नैतिक श्रेष्ठता

सही साबित होने वाली भावना। यह सबसे खतरनाक है, क्योंकि यह स्पष्टता जैसी लगती है।

निश्चितता

कोई सवाल मन में नहीं आता। वास्तविक जटिल समाचार प्रश्न पैदा करता है। अपहरण निष्कर्ष पैदा करता है।

नियम: तेज़ भावना साझा करने का कारण नहीं है। यह रुकने का कारण है।

1 UNREAD MESSAGE

There is a part-time job, you can use your mobile phone to operate at home, you can earn 200-3000 rupees a day, 10-30 minutes a day, new users join to get you 50 rupees, waiting for you to join.

Reply 1 and long click the link to join us asap.

http://wame.wp-e.com/api/tg/wa/8w36ceh

This sender is not in your contac

Block

Report

🔒 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

🤡Can't you want to make money with only one mobile phone?🤡

😎Join us and earn 5000rs per day.😎

👀Whatsapp: 👇

➡ht ://wa.me/+918902404707?t o

16:48

This sender is not in your contacts

Block

Report

SCAM

Google

digital arrest

All | Images | News | Videos | Short videos | Forums | Web

Top stories

The Hindu

71-year-old ‘digital arrest’ victim in Hyderabad gets back ₹36.5 lakh of ₹43 lakh lost i…

4 hours ago

Lexology

From Clicks to Cuffs: Understanding Digital Arrest in the Indian Legal Landscapes

4 weeks ago

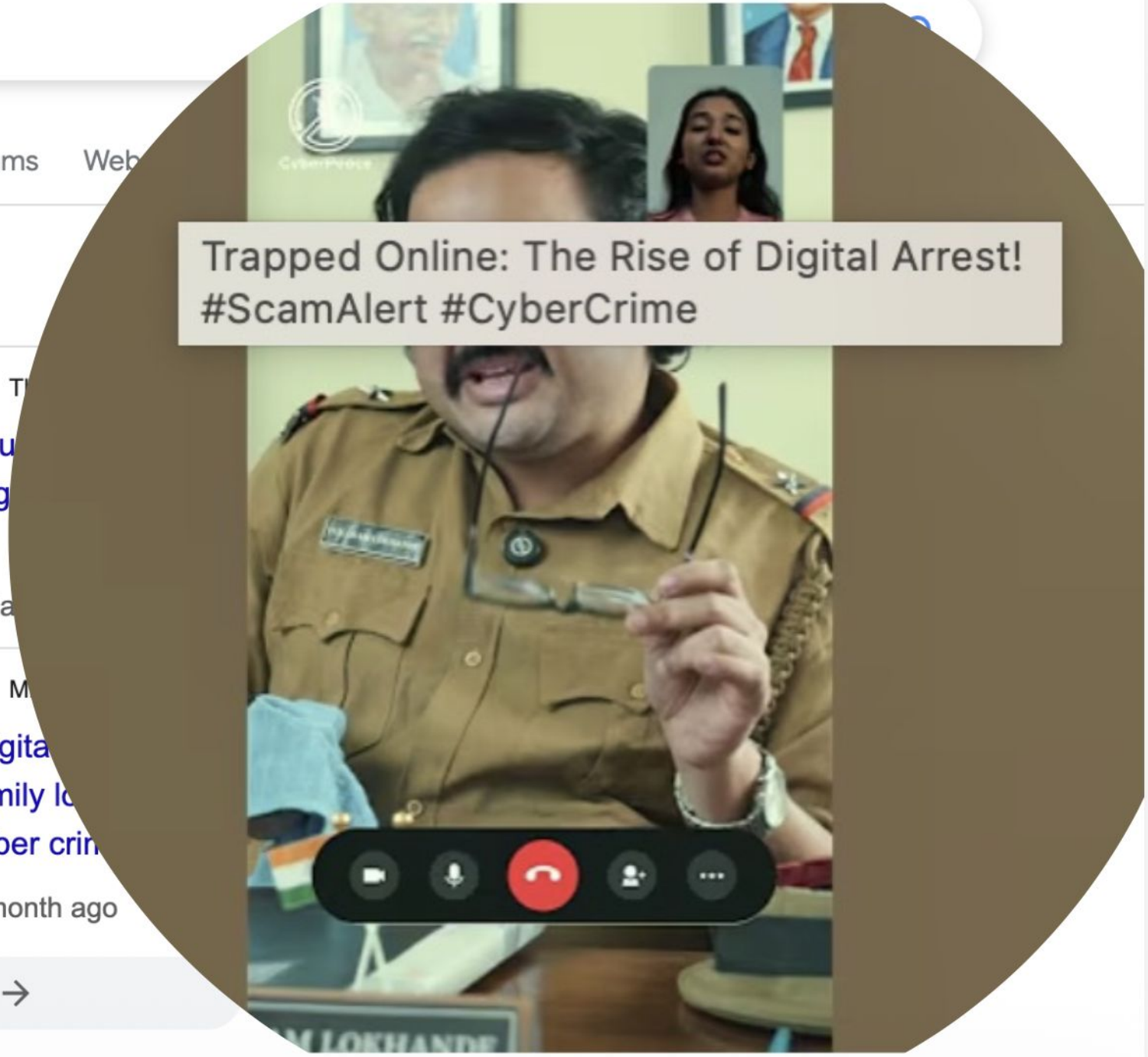
Fou
‘dig

1 da

‘Digita
family l
cyber crin

1 month ago

More news →

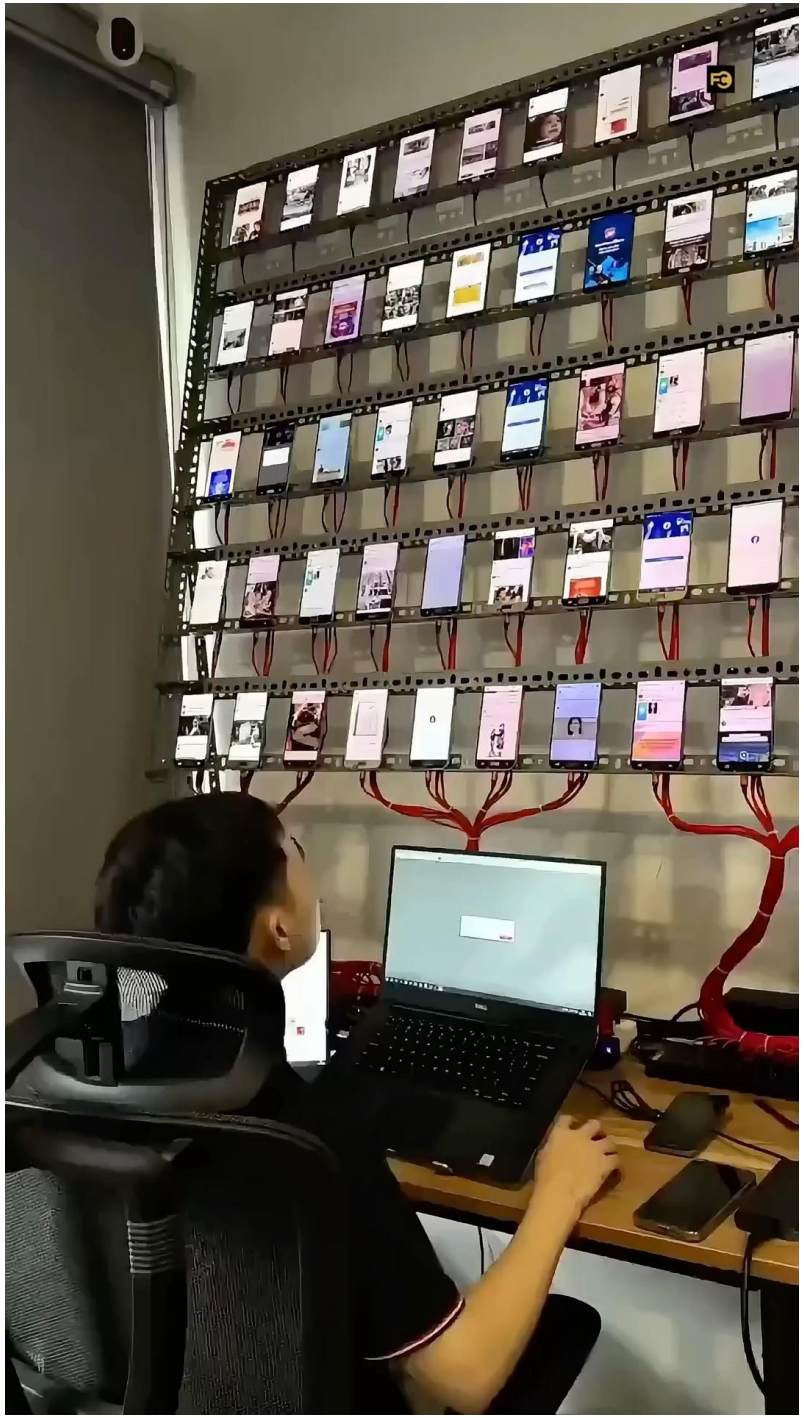


REPORTS

Digital blackmail and endless threats: scammy loan apps soar across India

Nearly half of the digital lending apps available in India between January and February 2021 were illegal, as per the central bank.

भारत में, हाल के राष्ट्रीय आँकड़ों से पता चलता है कि साइबर धोखाधड़ी और डिजिटल स्कैम चिंताजनक पैमाने पर पहुँच गए हैं, सबसे हाल के ट्रैक किए गए वर्ष में कम से कम 28.15 लाख साइबर अपराध के मामले दर्ज हुए और ₹22,845 करोड़ का नुकसान हुआ। जबकि कुल शारीरिक अपराध में गिरावट आई है, साइबर-संबंधित धोखाधड़ी लगभग 18% बढ़ी है



नफ़रत भरे भाषण का प्रसार

सोशल मीडिया प्लेटफॉर्म का नफ़रत भरे भाषण फैलाने के लिए शोषण किया गया है, जिससे सामाजिक तनाव पैदा हुआ और सख्त सामग्री मॉडरेशन की आवश्यकता हुई।

roby aja Follow
@roby_aja3

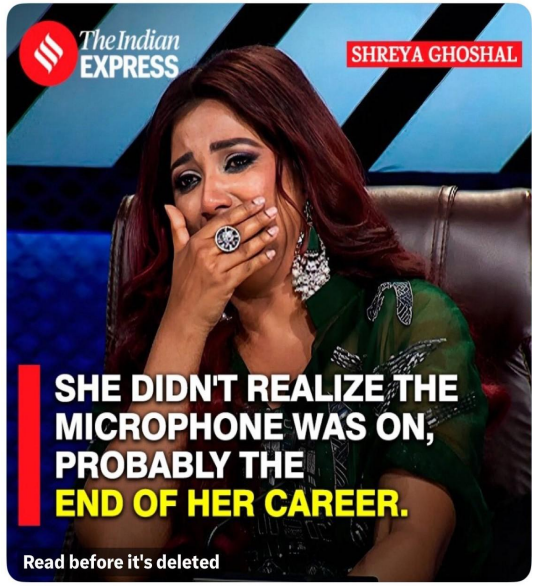
The Whole Nation Is Talking

From indianexpress.com

14:53 · 28/02/25 · 6.8K Views

Evelio socop Follow
@socop_10

Attention! New information!



From lacywrappedvalet.mom

15:03 · 28/02/25 · 2.7K Views

Home / Research / Long-Form / Occasional Papers

Countering Disinformation and Hate Speech Online: Regulation and User Behavioural Change

AUTHOR : ARCHIT LOHANI

Beyond likes and shares, millions of reasons to worry

The total number of social media users in South Asia as of October is around 961 million. What is the role of governments and civil society organisations in holding social media platforms accountable for the harmful content they host?

BEWARE LADIES!

Trending 'Saree Challenge'

This challenge might just be a playground for the **cyber criminals** to make **porn, catfish and blackmail people**. They are using Deep Nude for **creating morphed pictures** of clothed people as nude.

Be Smart, Stay Safe!

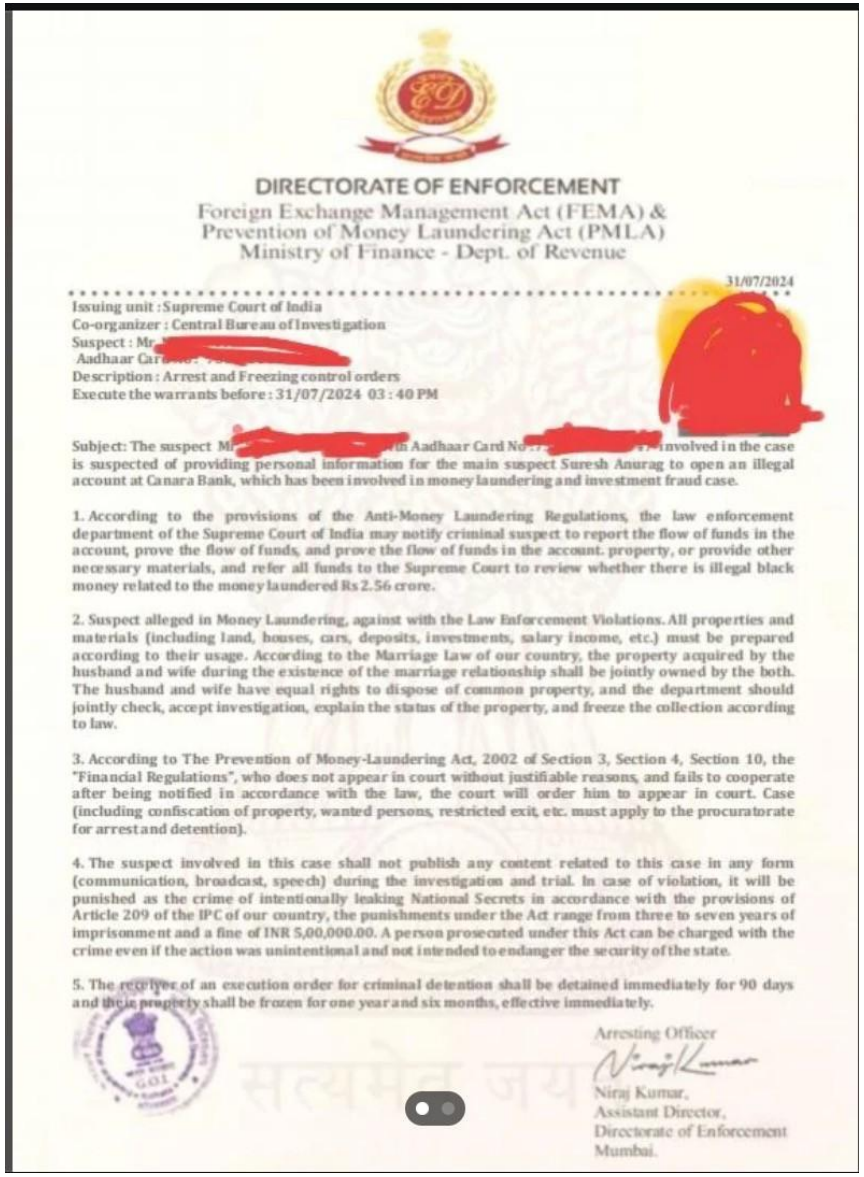
Follow **@CyberPeaceCorps** for More Online Safety Tips

Sextortion via WhatsApp Video Calls

How WhatsApp Messenger is becoming home to cyber crime and extortion:

Nowadays, many people are receiving video calls from unknown numbers. As soon as the receiver takes the call, a video of a nude girl is played on the screen. After some time, the call is abruptly disconnected. Shortly afterwards, the scamsters send Whatsapp text with **screen recording of the video call** from the same unknown number.

465 | 19



DIRECTORATE OF ENFORCEMENT
Foreign Exchange Management Act (FEMA) &
Prevention of Money Laundering Act (PMLA)
Ministry of Finance - Dept. of Revenue

31/07/2024

Issuing unit : Supreme Court of India
Co-organizer : Central Bureau of Investigation
Suspect : Mr. [redacted]
Aadhaar Card [redacted]
Description : Arrest and Freezing control orders
Execute the warrants before : 31/07/2024 03 : 40 PM

Subject: The suspect Mr [redacted] with Aadhaar Card No [redacted] involved in the case is suspected of providing personal information for the main suspect Suresh Anurag to open an illegal account at Canara Bank, which has been involved in money laundering and investment fraud case.

1. According to the provisions of the Anti-Money Laundering Regulations, the law enforcement department of the Supreme Court of India may notify criminal suspect to report the flow of funds in the account, prove the flow of funds, and prove the flow of funds in the account. property, or provide other necessary materials, and refer all funds to the Supreme Court to review whether there is illegal black money related to the money laundered Rs 2.56 crore.

2. Suspect alleged in Money Laundering, against with the Law Enforcement Violations. All properties and materials (including land, houses, cars, deposits, investments, salary income, etc.) must be prepared according to their usage. According to the Marriage Law of our country, the property acquired by the husband and wife during the existence of the marriage relationship shall be jointly owned by the both. The husband and wife have equal rights to dispose of common property, and the department should jointly check, accept investigation, explain the status of the property, and freeze the collection according to law.

3. According to The Prevention of Money-Laundering Act, 2002 of Section 3, Section 4, Section 10, the "Financial Regulations", who does not appear in court without justifiable reasons, and fails to cooperate after being notified in accordance with the law, the court will order him to appear in court. Case (including confiscation of property, wanted persons, restricted exit, etc. must apply to the procuratorate for arrest and detention).

4. The suspect involved in this case shall not publish any content related to this case in any form (communication, broadcast, speech) during the investigation and trial. In case of violation, it will be punished as the crime of intentionally leaking National Secrets in accordance with the provisions of Article 209 of the IPC of our country, the punishments under the Act range from three to seven years of imprisonment and a fine of INR 5,00,000.00. A person prosecuted under this Act can be charged with the crime even if the action was unintentional and not intended to endanger the security of the state.

5. The recipient of an execution order for criminal detention shall be detained immediately for 90 days and their property shall be frozen for one year and six months, effective immediately.

Arresting Officer
Niraj Kumar
Niraj Kumar,
Assistant Director,
Directorate of Enforcement
Mumbai.

01 · ध्यान दो

तकनीक सीखें, विषय नहीं

हज़ारों झूठे दावे हैं लेकिन केवल मुट्ठी भर हेरफेर तकनीकें हैं। पाँच सीखें और आप उन दावों के लिए तैयार हैं जो आपने कभी नहीं देखे।

1

भावनात्मक लोडिंग

भाषा उत्तेजना के लिए चुनी गई, सटीकता के लिए नहीं।

“SHOCKING” · “before they delete this” · ALL CAPS

2

झूठी दुविधा

जहाँ कई विकल्प हैं वहाँ दो प्रस्तुत किए गए।

“Either you support this or you are anti-national.”

3

बलि का बकरा बनाना

एक जटिल समस्या का दोष एक समूह पर।

“The shortage is because of those people.”

4

संदेशवाहक पर हमला

स्रोत को बदनाम करो ताकि सबूत कभी जाँचा ही न जाए।

“She only said that because of who she works for.”

5

नकली अधिकार

Borrowed credibility — a logo, a uniform, a forwarded “official” label.

“Forwarded from Cyber Cell” on an unsigned message.

इसीलिए प्रीबंकिंग डिबंकिंग से बेहतर है: आपको एक तकनीक के खिलाफ टीका लगाया जा सकता है इससे पहले कि विशिष्ट झूठ लिखा भी जाए।

CODE, ALGOS, LIKES, BOTS, DRONES, AND LIES:
WEAPONS TO TAKE DOWN COUNTRIES,
COMPANIES, OR CITIZENS.
युद्ध बदल गया है। गोलियाँ नहीं। सीमाएँ नहीं। बस कोड।
CODE
ALGOS
TARGET:
CITIZENS /
INFRASTRUCTURE
LIKES
BOTS
LIES

यह युद्ध कौन लड़ रहा है?

स्पॉइलर: यह सिर्फ सरकारें नहीं हैं

राष्ट्र - राज्य

Russia · China · USA · Iran · North Korea

बुनियादी ढाँचे पर हमले, चुनाव ऑपरेशन, आर्थिक जासूसी

निगम

NSO Group · Cambridge Analytica · विज्ञापन नेटवर्क

निगरानी पूँजीवाद, राज्य-स्तरीय स्पाइवेयर किसी को भी बेचना

अपराधी गिरोह

LockBit · REvil · रैनसमवेयर समूह

अस्पताल रैनसमवेयर, महत्वपूर्ण बुनियादी ढाँचे की ब्लैकमेल

आपका दोस्त (शायद)

हर लाइक, शेयर और क्लिक सिस्टम को बढ़ाता है

आपकी सहभागिता ईंधन है। आपका डेटा उत्पाद है।

आप

हैं निशाना

आपका ध्यान · आपकी आस्थाएँ · आपके वोट · आपके उपकरण

01

देखना अब विश्वास करना नहीं है

चार भारतीय मामले। चार राष्ट्रीय सदमे। उनमें से एक भी वास्तविक नहीं था।

छह सेकंड की क्लिप

क्या हुआ

A six-second video of actress Rashmika Mandanna stepping into a lift swept Instagram and X. It was a British influencer's body with the actress's face seamlessly swapped on. Millions had watched before the first fact-check appeared.

यह क्यों काम किया

It looked completely ordinary — no scandal, just a celebrity in a lift. That is what made it terrifying: if this could be faked invisibly, anything could. It triggered FIRs, MeitY advisories and India's deepfake reckoning.

6 sec

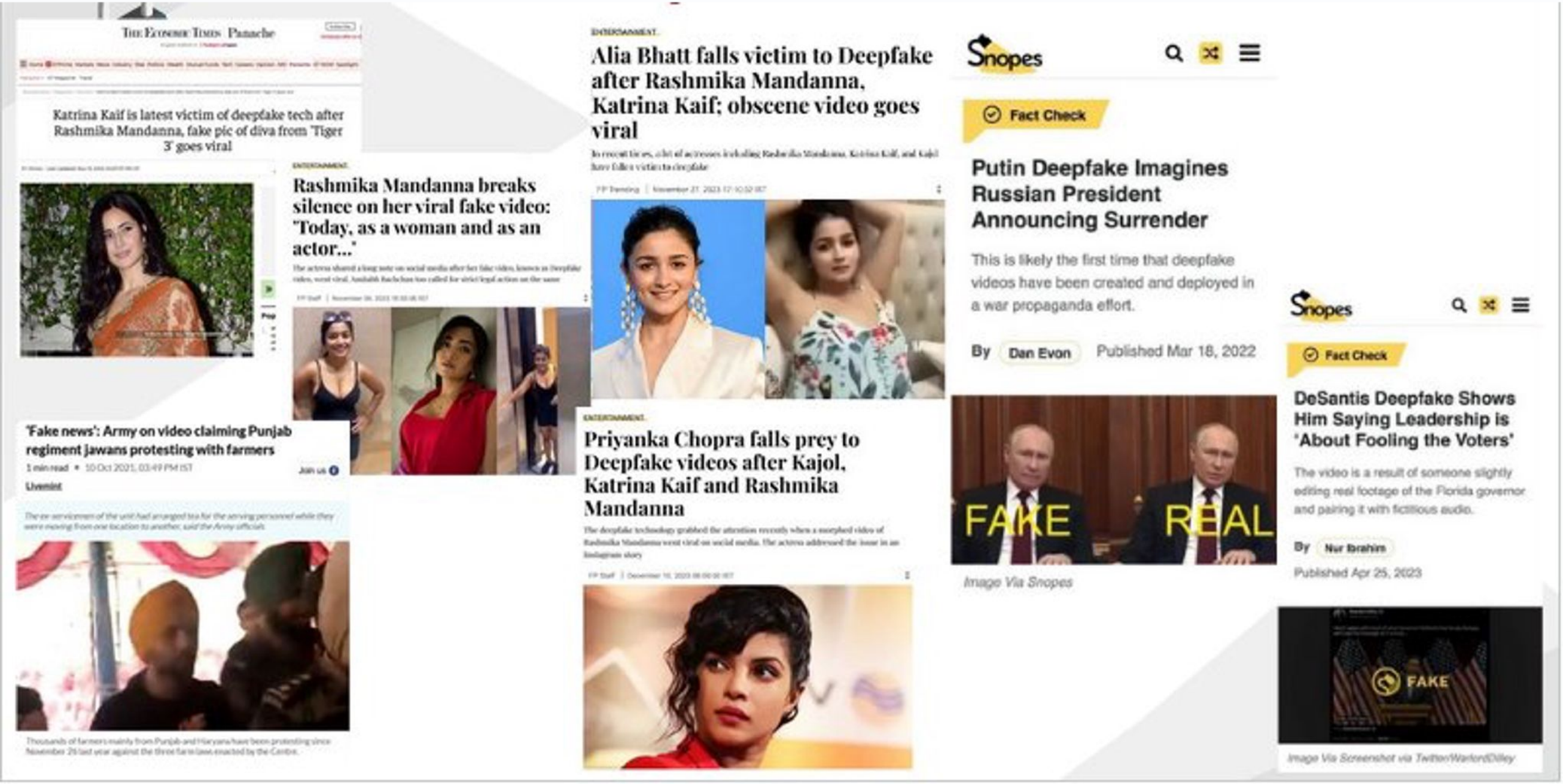
सिंथेटिक वीडियो जिसने राष्ट्रीय नीतिगत प्रतिक्रिया को मजबूर किया

उपकरण
फेस-स्वैप डीपफेक

माध्यम
Instagram → X → हर जगह

परिणाम
FIR + राष्ट्रीय परामर्श

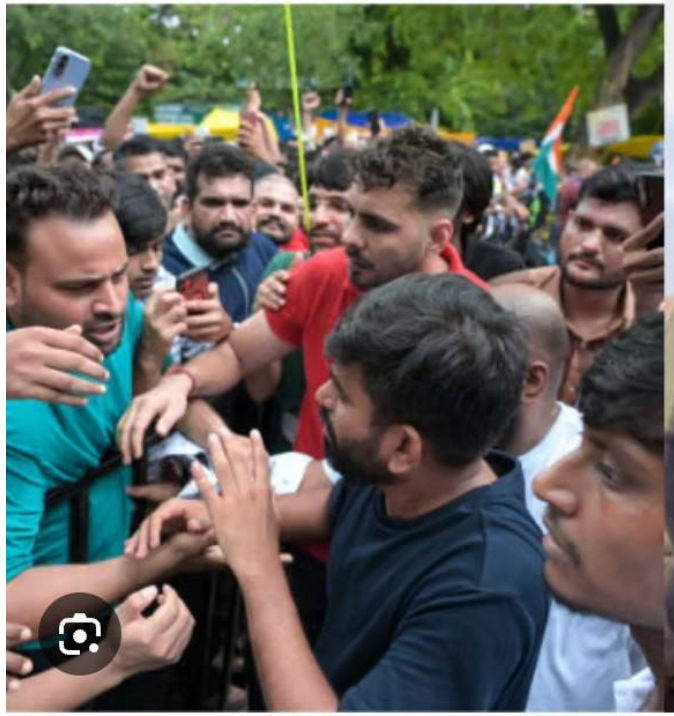
डीपफेक - वास्तविक दुनिया के उदाहरण



Delhi Police says 400 Pakistan-linked social media handles blocked over fake posts on CJP protest

Police said some of these accounts had also been active in spreading fake news during Operation Sindoor.

Advertisement



केस फाइल 003 // 2018

वह फॉरवर्ड जिसने जान ली

क्या हुआ

Grainy videos and voice notes warning of “child-lifting gangs” spread village to village on WhatsApp. Mobs formed around strangers — migrant workers, an engineer, travellers. More than thirty people were beaten to death.

यह क्यों काम किया

कोई AI नहीं। कोई हैकर नहीं। बस डर, पारिवारिक ग्रुप पर भरोसा, और एक फॉरवर्ड बटन। हमने सीखा कि गलत सूचना डीपफेक के आने से पहले ही मारती है — और तकनीक तब से केवल मज़बूत हुई है।

30+

एक ऐसी अफवाह में गई जानें जो कभी सच नहीं थी

उपकरण

एक टेक्स्ट फॉरवर्ड

माध्यम

पारिवारिक WhatsApp ग्रुप

प्रतिक्रिया

फॉरवर्ड सीमाएँ, राष्ट्रव्यापी

The ₹7 crore “digital arrest”

क्या हुआ

The chairman of a major Indian textile group spent two days on a video call under “digital arrest” by fake CBI officers — complete with a staged virtual courtroom and a deepfaked Chief Justice. He transferred ₹7 crore before anyone realised no such procedure exists.

यह क्यों काम किया

Uniforms, seals, case numbers, procedure — the scam wore the full costume of the Indian state. Authority plus fear plus isolation beats intelligence: the victim was one of India’s most accomplished industrialists.

₹7 Cr

एक ऐसे थाने को भुगतान जो कभी था ही नहीं

उपकरण
डीपफेक + नकली अदालत

माध्यम
एक वीडियो कॉल

पैमाना
हर साल हज़ारों मामले

$25 मिलियन की वीडियो कॉल

क्या हुआ

इंजीनियरिंग दिग्गज Arup के एक वित्त कर्मचारी ने CFO और कई सहकर्मियों के साथ वीडियो कॉन्फ्रेंस में शामिल हुआ। उस कॉल पर हर एक व्यक्ति डीपफेक था।

उसने कुल US$25.6 मिलियन के 15 ट्रांसफर अधिकृत किए।

यह क्यों काम किया

उसे पहले ईमेल पर शक था — इसलिए उसने कॉल माँगी। कॉल ही जाल थी। कई परिचित चेहरों और आवाज़ों ने एक सावधान, सक्षम पेशेवर को मात दे दी।

$25.6M

एक मीटिंग में खोए जहाँ कोई असली व्यक्ति मौजूद नहीं था

उपकरण

रियल-टाइम डीपफेक

माध्यम

नियमित वीडियो कॉल

हानि

"देखना ही विश्वास करना है"

02 जाँच करो

One routine, ninety seconds, every time. Short enough that you will actually use it.

You are not verifying the claim. You are verifying where it came from — that is a much faster job.

02 · जाँच करो

90 सेकंड की जाँच

चार चरण, क्रम में। आपको लगभग कभी चारों की ज़रूरत नहीं होती — अधिकांश दावे चरण 2 पर हल हो जाते हैं।

1 ~5 sec

रुको

आगे मत पढ़ो, प्रतिक्रिया मत करो। ध्यान दो कि आप इस स्रोत को नहीं जानते। चार सेकंड के लिए फोन नीचे रखो।

2 ~30 sec

स्रोत की जाँच करो

Who is publishing this? Not what the page says about itself — what others say about it. New tab, search the name.

3 ~30 sec

बेहतर कवरेज खोजो

इस संस्करण को अनदेखा करो। दावे को ही खोजो और देखो कौन और रिपोर्ट करता है। अगर कोई विश्वसनीय नहीं करता, तो यही आपका जवाब है।

4 ~25 sec

मूल तक पहुँचो

स्क्रीनशॉट, उद्धरण और क्लिप संपादित होते हैं। मूल पोस्ट, पूरा वीडियो, या वास्तविक दस्तावेज़ खोजो।

ध्यान दो क्या गायब है: इस प्रक्रिया में कहीं भी आप बहस नहीं करते, और कहीं भी आपको विषय में विशेषज्ञता की ज़रूरत नहीं।

02 · जाँच करो

पेज को आँकने के लिए पेज छोड़ो

संदिग्ध पेज को अधिक ध्यान से पढ़ने की प्रवृत्ति होती है। यह बिल्कुल उलटा है — आप एक ऐसा दस्तावेज़ पढ़ रहे हैं जो आपको समझाने के लिए लिखा गया है।

ज़्यादातर लोग क्या करते हैं

- लेख को ऊपर से नीचे तक पढ़ना
- Study the layout — “it looks professional”
- साइट का अपना About पेज पढ़ना
- यह कितना विश्वासपूर्ण लगता है उसके आधार पर तय करना

उस सूची की हर चीज़ लेखक के नियंत्रण में है।

इसके बजाय क्या करें

- तुरंत एक नया टैब खोलो
- Search the publisher's name + “who owns” or “criticism”
- डोमेन जाँचो — पिछले महीने रजिस्टर हुआ? करीबी ग़लत स्पेलिंग?
- लेखक का नाम अलग से खोजो

उसमें से कुछ भी लेखक के नियंत्रण में नहीं है। यही पूरा मुद्दा है।

पेशेवर फैक्ट-चेकर पेज पर 30 सेकंड से कम बिताते हैं। शौकिया लोग दस मिनट बिताते हैं और ग़लत जवाब पर पहुँचते हैं।

02 · जाँच करो

चार चरणों में तस्वीर या वीडियो की जाँच

Most viral “evidence” is a real photograph from the wrong place, the wrong year, or the wrong event.

1	**रिवर्स सर्च करो**	स्क्रीनशॉट लो, फिर रिवर्स इमेज सर्च से गुज़ारो। फोन पर, ब्राउज़र या कैमरा ऐप का बिल्ट-इन इमेज सर्च काम करता है।
2	**सबसे पुरानी कॉपी खोजो**	Sort results by date. If a “breaking” image existed three years ago, you are done — no further analysis needed.
3	**पृष्ठभूमि पढ़ो**	साइनबोर्ड की भाषा, वाहन नंबर प्लेट, वर्दियाँ, दुकानों के नाम, मौसम, ऋतु । इन्हें नकली बनाना बहुत मुश्किल है और जाँचना आसान।
4	**दावे को फ्रेम से मिलाओ**	क्या कैप्शन वही बताता है जो तस्वीर वास्तव में दिखाती है? अक्सर तस्वीर असली होती है और केवल कैप्शन झूठ होता है।

80% का नियम

अधिकांश भ्रामक तस्वीरें बिल्कुल भी गढ़ी हुई नहीं हैं। वे असली तस्वीरें हैं जो किसी और देश, किसी और दशक, या किसी और घटना से ली गई हैं, और उन्हें एक नया कैप्शन दिया गया है।

So the question is almost never “is this fake?” It is “where is this actually from?”

इसे एक बार करो तो दो मिनट लगते हैं। दस बार करो तो बीस सेकंड लगते हैं।

02 · जाँच करो

डीपफेक : क्या अभी भी काम करता है

तीन साल पहले दी गई सलाह अब सक्रिय रूप से खतरनाक है, क्योंकि यह झूठा आत्मविश्वास सिखाती है।

✕ काम करना बंद

- उंगलियाँ गिनना, दाँत और कान जाँचना
- जबड़े या बालों की रेखा पर धुंधलापन खोजना
- व्यक्ति के पलक झपकने का इंतज़ार करना
- “The voice sounds slightly robotic”
- अपनी आँखों और कानों पर बिल्कुल भरोसा करना

✓ अभी भी काम करता है

- फोन काटो और उस नंबर पर वापस कॉल करो जो आपके पास पहले से था
- कुछ ऐसा पूछो जिसका जवाब केवल असली व्यक्ति दे सके
- जाँचो कि क्या दावा कहीं और भी दिखाई देता है
- चैनल सत्यापित करो, चेहरा नहीं — क्या यह वहाँ आया जहाँ यह व्यक्ति सामान्यतः बोलता है?
- तात्कालिकता पर कार्य करने से इनकार करो, चाहे आवाज़ कितनी भी विश्वसनीय हो

चेहरा प्रमाणित करना बंद करो। चैनल प्रमाणित करो।

गतिविधि 2 · 6 मिनट

तीन मिनट का सत्यापन

फोन निकालो। आपसे दावे को सच या झूठ साबित करने के लिए नहीं कहा जा रहा — आपसे यह पता लगाने के लिए कहा जा रहा है कि यह कहाँ से आया।

दावा

एक न्यूज़ कार्ड का स्क्रीनशॉट आपके क्लास ग्रुप में घूम रहा है, जो कल से एक बड़े बदलाव का दावा करता है। कोई लिंक नहीं। कोई न्यूज़ आउटलेट का नाम दिखाई नहीं।

मिनट 1 मूल किसने प्रकाशित किया? एक नाम खोजो, स्क्रीनशॉट नहीं।

मिनट 2 क्या कोई और इसकी रिपोर्ट करता है? दावा खोजो, तस्वीर नहीं।

मिनट 3 सबसे पुराने संस्करण पर तारीख क्या है जो आप पा सकते हैं?

इस पर रिपोर्ट करो

- किस चरण ने आपको जवाब दिया?
- वास्तव में कितना समय लगा?
- आपने क्या पाया जो फॉरवर्ड ने आपको नहीं बताया?
- क्या आपने यह करने से पहले इसे साझा किया होता?

आखिरी सवाल असली है।

03 प्रतिक्रिया दो

यह जानना कि यह झूठ है आसान आधा है। बिना बिगाड़े इसके बारे में कुछ करना कौशल है।

अधिकांश सुधार इसलिए विफल नहीं होते कि तथ्य ग़लत हैं, बल्कि इसलिए कि जिस व्यक्ति को सुधारा जा रहा है उसे मूर्ख महसूस कराया गया है।

03 · प्रतिक्रिया दो

सबसे कठिन कमरा आपका अपना पारिवारिक ग्रुप है

एक अजनबी को सुधारने में कुछ नहीं लगता। एक बड़े को सुधारना जिसने नेक इरादे से कुछ फॉरवर्ड किया, रिश्ते की कीमत लगती है — यही कारण है कि कोई नहीं करता।

यहाँ सुधार क्यों विफल होते हैं

- सार्वजनिक में, सुधारा जाना अपमान जैसा लगता है
- फॉरवर्ड करने वाले का इरादा आमतौर पर सुरक्षात्मक था, दुर्भावनापूर्ण नहीं
- उम्र और अधिकार असहमति को सामाजिक रूप से महँगा बनाते हैं
- बहस जीतकर भी व्यक्ति को खो सकते हैं

1. उन्हें सीधे जवाब दो, कभी ग्रुप में नहीं। हमेशा।
2. **पूछो, घोषणा मत करो** — एक सवाल सोच को आमंत्रित करता है। एक सुधार बचाव को आमंत्रित करता है।
3. "I know you sent it because you were worried" costs you nothing and changes everything.
4. उन्हें दिखाओ आपने कैसे जाँचा। अगली बार वे आपके बिना कर सकते हैं।

आपका लक्ष्य बहस जीतना नहीं है। यह है कि अगले हफ्ते उन्हें बेवकूफ बनाना थोड़ा कठिन हो जाए।

03 · प्रतिक्रिया दो

चार वाक्य जो आप वास्तव में उपयोग कर सकते हैं

इन्हें कॉपी करो। अपनी भाषा और शैली में ढालो — ढाँचा मायने रखता है, शब्द नहीं।

जब आप अभी निश्चित नहीं हैं

“This one looks worrying — let me check where it came from before we send it on.”

बिना किसी पर आरोप लगाए समय खरीदता है।

जब आप जानते हैं कि यह झूठ है

“I looked this up — it is an old photo from a different incident. Sending you what I found.”

सबूत से शुरू करता है, सुधार से नहीं।

जब किसी बड़े ने फॉरवर्ड किया

“I know you shared it because you were concerned. Turns out it is not accurate — here is the actual news.”

इरादे की रक्षा करता है, सामग्री बदलता है।

जब आप पैटर्न को रोकना चाहते हैं

“Can I show you the thirty-second way I check these? It works on all of them.”

फैसले के बजाय कौशल हस्तांतरित करता है।

Notice that not one of these contains the word “fake”, and not one of them tells the other person they were wrong.

03 · प्रतिक्रिया दो

बिना बढ़ाए सुधारो

एक खराब तरीके से बना सुधार झूठ को दोहराता है, आपकी विश्वसनीयता जोड़ता है, और मूल से भी आगे फैलाता है। इसके बजाय इस क्रम में बनाओ।

1. **सच्चाई से शुरू करो** — वास्तव में क्या है बताओ। पहले, सीधे, एक वाक्य में।
2. **दावे को एक बार नाम दो** — झूठे दावे का संक्षेप में उल्लेख करो — एक बार, बिना विस्तृत विवरण, बिना तस्वीर।
3. **तकनीक समझाओ** — बताओ यह कैसे बना: पुरानी तस्वीर, संपादित क्लिप, नकली अधिकार। चाल का नाम बताना अगली के खिलाफ टीका लगाता है।
4. **सच्चाई से समाप्त करो** — जहाँ शुरू किया वहीं समाप्त करो। लोग पहली और आखिरी बात याद रखते हैं।

जाल

इंटरनेट पर सबसे आम सुधार ऐसा दिखता है:

“This is FAKE!”
— पूरे झूठ, मूल तस्वीर के साथ, और कोई स्पष्टीकरण नहीं।

वह सुधार नहीं है। वह मुफ्त वितरण है।

झूठ का खंडन करने के लिए कभी स्क्रीनशॉट मत लो। आपने अभी उसे एक नया, अधिक विश्वसनीय वाहक दिया है — आप।

03 · प्रतिक्रिया दो

कहाँ रिपोर्ट करें — भारत के वास्तविक चैनल

ज़रूरत पड़ने से पहले इन्हें जान लो। वित्तीय धोखाधड़ी में पहला घंटा तय करता है कि पैसा वापस मिल सकता है या नहीं।

1930	राष्ट्रीय साइबर अपराध हेल्पलाइन। टोल-फ्री, 24×7। चल रही या हालिया वित्तीय धोखाधड़ी के लिए — पहले कॉल करो, बाद में दर्ज करो।
cybercrime.gov.in	राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (I4C, गृह मंत्रालय)। सभी साइबर अपराध प्रकार। महिलाओं और बच्चों के खिलाफ अपराधों के लिए गुमनाम रिपोर्टिंग उपलब्ध।
1098	चाइल्डलाइन। बच्चे की ऑनलाइन सुरक्षा से जुड़ा कोई भी मामला।
181 · 112	महिला हेल्पलाइन और राष्ट्रीय आपातकालीन नंबर।

इसके अलावा, हमेशा

- ऐप के अंदर रिपोर्ट करो — प्लेटफॉर्म रिपोर्टिंग हटाने के लिए किसी भी कानूनी मार्ग से तेज़ है
- अगर कोई नाबालिग शामिल है तो शिक्षक, वार्डन, या माता-पिता को बताओ
- वित्तीय धोखाधड़ी के लिए: समानांतर में अपने बैंक को सूचित करो, इंतज़ार मत करो
- फॉरवर्ड की बजाय आधिकारिक परामर्श के लिए @CyberDost फॉलो करो

रिपोर्टिंग बढ़ाना नहीं है। यह एकमात्र तरीका है जिससे सिस्टम जानता है कि क्या हो रहा है।

Report inappropriate videos, channels & other content on YouTube

We rely on YouTube community members to report or flag content that they find inappropriate. Reporting content is anonymous, so other users can't tell who made the report.

What happens after I report content?

When content is reported, it's not automatically taken down. Reported content is reviewed along these guidelines:

- Content that violates our Community Guidelines is removed from YouTube.
- Content that may not be appropriate for younger audiences may be age-restricted.

To check if a video that you reported has been removed, you can view your Report history.

Report content

- Report inappropriate videos, channels & other content on YouTube
- Report a YouTube search prediction
- Report policy-violative ads
- About the YouTube Priority Flagger program
- View your Reporting History
- Other reporting options
- Australian Online Safety Act and how to report online harm
- Report NCII Content on YouTube

gac.gov.in

Finish update

English

Digital India

GRIEVANCE APPELLATE COMMITTEE

To Ensure Accountability for Digital Nagriks

Appellant Login (File appeal / View status)

☐ I have read and agree to the Privacy Policy and Terms of Service of the Grievance Appellate Committee platform.

Enter Mobile Number*

Ten Digit Mobile Number

Captcha*

CQpyQs

Enter Captcha

Send OTP

Change Your Registered Mobile Number

6080	5889
Appeals Received	Appeals Disposed

cybercrime.gov.in

Finish update

भारत सरकार
GOVERNMENT OF INDIA

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

Language

Indian Cyber Crime Coordination Centre
सहयोगी करावावे • Working Together With Vigour

सत्यमेव जयते

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal

आज़ादी का अमृत महोत्सव

WOMEN/CHILDREN RELATED CRIME

Register Anonymously

Register & Track

FINANCIAL FRAUD

Register a Complaint

OTHER CYBER CRIME

Register a Complaint

What's new

and other identifiers for their possible linkages with the cyber criminals at:

https://cybercrime.gov.in/Webform/suspect_search_repository.aspx

https://cybercrime.gov.in/Webform/suspect_search_websites.aspx

Through the **'Report Suspect'** facility at NCRP, citizens can report various types of suspect identifiers, viz; Website URLs WhatsApp

Learning Corner

MANUAL

CITIZEN MANUAL

CYBER SAFETY TIPS

CYBER AWARENESS

DAILY DIGEST

Instagram Help Centre

help.instagram.com/contact/552695131608132

Instagram

How can we help?

Help Centre

- Instagram Features
- Login, Recovery and Security
- Manage Your Account
- Staying Safe
- Privacy and Reporting
- Terms and Policies
- Instagram for Businesses
- Threads

Copyright Report Form

Copyright is a legal right that protects original works of authorship, such as film, music, books and art. This form is only to be used for reporting alleged infringements of your copyright on Instagram or Threads. Please note that any other types of claims will not be addressed through this form. Abuse of this form may result in the termination of your account or profile.

Describe your relationship to the rights owner.

- I am the rights owner
- I am reporting on behalf of my organisation or client
- I am reporting on behalf of someone else

Send

03 · प्रतिक्रिया दो

रिपोर्ट करने से पहले: सुरक्षित करो, हटाओ मत

कुछ कष्टकारी हटाने की प्रवृत्ति होती है। वह प्रवृत्ति जो हुआ उसका एकमात्र रिकॉर्ड नष्ट करती है।

1	**पूरा फ्रेम कैप्चर करो**	भेजने वाले का नाम, टाइमस्टैम्प, और URL शामिल स्क्रीनशॉट। क्रॉप की गई तस्वीर कुछ साबित नहीं करती।
2	**मूल संदेश रखो**	चैट या पोस्ट हटाओ मत। म्यूट करो, आर्काइव करो, आगे बढ़ो — लेकिन रखो।
3	**नंबर नोट करो**	भेजने वाले का फोन नंबर, प्रोफाइल हैंडल, ट्रांजैक्शन ID, UPI रेफरेंस। ऐप के बाहर कहीं लिखो।
4	**कब देखा यह रिकॉर्ड करो**	जब आपने प्राप्त किया तारीख और समय, और किस ग्रुप से आया।

ऐसा मत करो

- Do not forward it “as proof” — that is still spreading it
- भेजने वाले को जवाब मत दो या खाते से न जुड़ो
- Do not pay, click, or “just check” the link
- रिपोर्ट करने से पहले सबूत मत हटाओ

सुरक्षित रखने के दो मिनट जाँच के लिए दो सप्ताह के गुस्से से अधिक मूल्यवान हैं।

पीब

FACT CHECK

जो कथा नियंत्रित करता है वो
वास्तविकता नियंत्रित करता है।

AI सब कुछ बदल देता है

05

जो कुछ आपने अभी देखा उसके लिए टीमें और बजट चाहिए थे। अब बस एक लैपटॉप चाहिए।

नया शस्त्रागार

जो क्षमताएँ स्टूडियो चाहिए थीं अब सेकंड लेती हैं

भाषा मॉडल

ChatGPT, Claude, Gemini — मानव स्तरीय प्रवाह में प्रेरक टेक्स्ट, किसी भी आवाज़ में, किसी भी भाषा में

वॉइस क्लोनिंग

ऑडियो के तीन सेकंड कमरे में किसी को भी क्लोन करने के लिए काफी हैं — आप सहित

वीडियो जनरेशन

फोटो-रियल डीपफेक और पूर्ण सिंथेटिक दृश्य, वीडियो कॉल पर लाइव

इमेज जनरेशन

ऐसी घटनाओं की "तस्वीरें" जो कभी हुई ही नहीं, फीड स्पीड पर पहचानना असंभव

स्वायत्त एजेंट

AI that researches, targets, writes and posts — without a human in the loop

मूर्त AI

रोबोट और IoT: जब सिंथेटिक दिमागों को हाथ, सेंसर और पहुँच मिलती है

अंक 06 // 15 स्लाइड // टेबल चैलेंज

THE सत्यापन प्रयोगशाला

06

आपने काफी देर देख लिया। अब हर टेबल काम पर लगती है।

आपके उपकरण

सत्यापन टूलकिट

Google Lens
यह तस्वीर और कहाँ है?

InVID
वीडियो को सत्यापन योग्य कीफ्रेम में तोड़ो

VirusTotal
क्या यह फाइल या लिंक खतरनाक है?

URLScan
क्लिक करने से पहले वेबसाइट का X-ray करो

Wayback Machine
इस पेज ने पिछले हफ्ते क्या दावा किया?

Fact Check Explorer
क्या किसी ने पहले से इसका खंडन किया है?

Metadata viewer
फाइल अपने बारे में क्या छिपा रही है?

आपका संशयवाद
एकमात्र उपकरण जिसे पैच नहीं किया जा सकता

समापन से पहले // रक्षा किट

अब हम पलटवार करते हैं

दस मिनट के उपाय जो आपने अभी जो देखा उसका नब्बे प्रतिशत हरा देते हैं।

रक्षा 01 // व्यक्तिगत

व्यक्ति को सुरक्षित करो

पासवर्ड मैनेजर

One unique password per site — the manager remembers so you don't

हर चीज़ पर 2FA

SMS पर Authenticator ऐप — यह चुराए गए पासवर्ड को रोक देता है

उल्लंघन जाँच, तिमाही

हर तिमाही haveibeenpwned.com; जो भी उजागर हो उसे बदलो

गोपनीयता ऑडिट

सोशल मीडिया को प्राइवेट करो; हर बायो से अपना नंबर और जन्मदिन हटाओ

लोकेशन ट्रेल बंद करो

टाइमलाइन हिस्ट्री बंद करो; हर महीने ऐप अनुमतियों की समीक्षा करो

बेरहमी से अपडेट करो

पैच उन्हीं दरवाज़ों को बंद करते हैं जिनसे हमलावर आते हैं

बाद में पोस्ट करो, कम पोस्ट करो

Share the holiday after you're home
— जब घर खाली हो तब नहीं

सार्वजनिक Wi-Fi पर भरोसा मत करो

एयरपोर्ट Wi-Fi पर बैंकिंग नहीं — आपका अपना हॉटस्पॉट सुरक्षित है

रक्षा 02 // परिवार

परिवार को धोखाधड़ी -प्रूफ बनाओ

डिजिटल अरेस्ट नियम

कोई पुलिस, CBI, ED या अदालत किसी को वीडियो कॉल पर गिरफ्तार नहीं करती। कभी नहीं। फोन काटो — यही पूरी रक्षा है।

एक पारिवारिक कोड शब्द

Agree one secret word today. Any emergency call asking for money must say it — voice clones can't.

कॉलबैक नियम

पैसे या OTP की कोई भी माँग: फोन काटो, जो नंबर पहले से सेव है उस पर वापस कॉल करो।

OTP पवित्र है

No bank, officer or "official" ever needs your OTP. The moment someone asks, they are the scam.

QR का मतलब भुगतान

You never scan a code to receive money. If someone sends a QR so they can "pay you" — that scan is the theft.

धीमा सुरक्षित है

तात्कालिकता is the weapon: arrest, expiry, "your son is in trouble." Every "act now" deserves ten minutes of doubt.

अगर ऐसा हो: गोल्डन ऑवर में 1930 पर कॉल करो · cybercrime.gov.in पर रिपोर्ट करो · अपने बैंक से खाता फ्रीज़ कराओ · स्क्रीनशॉट सबूत हैं

संगठन को मज़बूत बनाओ

दो-व्यक्ति नियम

No payment or credential change on one person's say-so — a familiar face on video is no longer identity.

पूर्व-सत्यापित चैनल

अभी तय करो सच कहाँ रहता है — आधिकारिक साइट, सत्यापित हैंडल — ताकि दर्शक जानें कि नकली आने पर कहाँ जाँचें।

Prebunk, don't just debunk

नकली आने से पहले अपने दर्शकों को चेतावनी देना बाद में पीछा करने से बेहतर है। टीकाकरण ही एकमात्र रक्षा है जो बड़े पैमाने पर काम करती है।

एक डीपफेक प्लेबुक

संकट से पहले तय करो: कौन सत्यापित करता है, कौन बोलता है, क्या हटाने के लिए बढ़ाया जाता है — और कितनी तेज़ी से।

अपने ट्विन पर नज़र रखो

Your brand and leaders have digital twins too. Track impersonations; know each platform's takedown route.

मनुष्यों को प्रशिक्षित करो

Run today's Verification Lab with your own team every quarter — trained instinct is the real firewall.

सत्यापन एक टीम खेल है। विश्वास एक संस्थागत संपत्ति है — उसके अनुसार बजट बनाओ।

सर्वोत्तम प्रथाएँ

AI उपकरणों का सुरक्षित उपयोग

- डेटा लीकेज रोकने के लिए AI उपकरणों में संवेदनशील या गोपनीय डेटा दर्ज करने से बचें।
- ज़िम्मेदार उपयोग सुनिश्चित करने के लिए अपने संस्थान की AI उपयोग नीतियों और दिशानिर्देशों का सख्ती से पालन करें।
- डेटा और गोपनीयता पर नियंत्रण बनाए रखने के लिए निजी या ऑन-प्रिमाइसेस AI मॉडल का उपयोग करें।
- बदलते सुरक्षा मानकों के अनुरूप AI उपकरण उपयोग प्रथाओं की नियमित समीक्षा और अपडेट करें।

Amazon Alexa के लिए आवश्यक सुरक्षा सेटिंग्स

1. Amazon खाते पर Two-Factor Authentication सक्षम करें
2. Drop-In अक्षम करें (या विश्वसनीय संपर्कों तक सीमित करें)
3. **Voice History की समीक्षा करें और नियमित रूप से हटाएँ**
4. **Turn OFF 'Use Voice Recordings to Improve Alexa'**
5. Disable Skills you don't trust or no longer use
6. Smart Home डिवाइस अनुमतियाँ जाँचें और सीमित करें
7. आवाज़ से खरीदारी बंद करें या PIN जोड़ें
8. Echo डिवाइसों को स्वचालित रूप से अपडेट रखें
9. **Alexa App के माइक्रोफ़ोन , लोकेशन और Bluetooth एक्सेस को सीमित करें**
10. मज़बूत Wi-Fi एन्क्रिप्शन (WPA3/WPA) का उपयोग करें
    2) and guest network

04 निर्माण करो

कौशल दो सप्ताह में क्षय होते हैं जब तक कि वे आदतें न बन जाएँ। यह खंड इस बारे में है कि सप्ताह में क्या बचता है।

और इस तथ्य के बारे में कि भारत को अपनी ज्ञानमीमांसा आयात करने की ज़रूरत नहीं — उसने इसकी कुछ सबसे पुरानी लिखी थीं।

सात दिन की चुनौती

एक दिन में एक कार्य। इतना छोटा कि आप वास्तव में करेंगे, और सातवें दिन तक दिनचर्या अब निर्णय नहीं रहती।

दिन 1

अपने फोन में 1930 सेव करो। अभी, बाद में नहीं।

दिन 2

आपको मिलने वाले किसी भी फॉरवर्ड पर एक रिवर्स इमेज सर्च करो।

दिन 3

जिस न्यूज़ सोर्स का आप नियमित रूप से उपयोग करते हैं उसके मालिक को खोजो।

दिन 4

अपने आप को गर्मी महसूस करते पकड़ो
— और स्क्रॉल करने से पहले चार सेकंड रुको।

दिन 5

अपने से बड़े एक व्यक्ति को नब्बे-सेकंड की जाँच सिखाओ।

दिन 6

चार स्क्रिप्ट में से एक का उपयोग करके निजी संदेश में कुछ सुधारो।

दिन 7

एक चीज़ रिपोर्ट करो — ऐप में, या पोर्टल के माध्यम से। लूप एक बार पूरा करो।

दिन 8

कुछ नहीं। अब तक यह आदत है, कार्य नहीं — और यही पूरा मुद्दा था।

दिन 1 अभी करो, इस कमरे में। जाने से पहले 1930 सेव करो — बाकी सप्ताह तभी होगा जब आज होगा।

भरोसा दुनिया की सबसे कीमती मुद्रा बन जाएगा।

और इस कमरे के लोग तय करते हैं कि उनके संस्थान इसमें अमीर हैं या दिवालिया।