साइबर अपराध की रिपोर्टिंग एवं सहायता-प्राप्ति व्यवहार

Kajal Kashyap
Cybercrime Researcher, I4C, MHA

आज हम क्या-क्या समझेंगे

भारत में साइबर अपराध की स्थिति

बढ़ते मामले, कारण एवं प्रवृत्तियाँ

साइबर अपराध के प्रमुख प्रकार

वित्तीय धोखाधड़ी से लेकर साइबरबुलिंग तक

रिपोर्टिंग एवं सहायता-प्राप्ति व्यवहार

अवधारणा, महत्व एवं बाधाएँ

I4C — भारतीय साइबर अपराध समन्वय केंद्र

गठन, उद्देश्य एवं संरचना

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल

cybercrime.gov.in — शिकायत दर्ज करने की पूरी प्रक्रिया

1930 हेल्पलाइन एवं "गोल्डन ऑवर"

तुरंत सहायता व धनराशि रोकने की प्रक्रिया

साइबर अपराध क्या है?

इंटरनेट या डिजिटल उपकरणों के माध्यम से की जाने वाली अवैध गतिविधियाँ (जैसे- ऑनलाइन फ्रॉड, हैकिंग, साइबर बुलिंग)।

रिपोर्टिंग क्यों जरूरी है?अपराधियों को पकड़ने और न्याय पाने के लिए।

आगे होने वाले वित्तीय या मानसिक नुकसान को रोकने के लिए।

भारत में साइबर अपराध की स्थिति

Indian Cyber Crime Coordination Centre
सहवीर्य करवावहे • Working Together With Vigour

भारत आज विश्व के सबसे बड़े डिजिटल बाज़ारों में से एक है — 80 करोड़ से अधिक इंटरनेट उपयोगकर्ता, जिनमें से बड़ी संख्या पहली बार इंटरनेट का उपयोग कर रहे हैं। UPI, ऑनलाइन बैंकिंग एवं सोशल मीडिया के तीव्र विस्तार के साथ-साथ वित्तीय धोखाधड़ी, फ़िशिंग, पहचान की चोरी और महिलाओं-बच्चों के विरुद्ध साइबर अपराध भी तेज़ी से बढ़े हैं। डिजिटल साक्षरता की कमी के कारण बड़ी संख्या में उपयोगकर्ता सुरक्षा-जोखिमों के प्रति अनजान रहते हैं, जिससे रिपोर्टिंग एवं सहायता-प्राप्ति व्यवहार को समझना और मज़बूत करना अत्यंत आवश्यक हो जाता है।

80 करोड़+
भारत में इंटरनेट उपयोगकर्ता

32.80 लाख
2026 में दर्ज साइबर अपराध के मामले

हज़ारों करोड़ ₹
1930 द्वारा रोकी गई धोखाधड़ी की राशि

जितना बड़ा डिजिटल विस्तार, उतनी ही अधिक ज़रूरत है सशक्त रिपोर्टिंग एवं सहायता-प्राप्ति व्यवहार की — ताकि हर पीड़ित समय रहते सही मदद तक पहुँच सके।

साइबर अपराध के प्रमुख प्रकार

Indian Cyber Crime Coordination Centre
सहवीर्य करवावहे • Working Together With Vigour

वित्तीय धोखाधड़ी

UPI, OTP, नेट-बैंकिंग व QR-कोड फ्रॉड

फ़िशिंग / स्मिशिंग

फर्ज़ी लिंक व संदेशों से जानकारी चुराना

महिला-बाल संबंधी अपराध

साइबर स्टॉकिंग, उत्पीड़न, आपत्तिजनक सामग्री

सिम-स्वैप / पहचान चोरी

मोबाइल नंबर व पहचान का दुरुपयोग

फर्ज़ी लोन ऐप / निवेश धोखाधड़ी

अवैध ऋण ऐप व नकली निवेश योजनाएँ

साइबरबुलिंग व ऑनलाइन उत्पीड़न

सोशल मीडिया पर धमकाना व अपमानित करना

"रिपोर्टिंग व्यवहार" क्यों महत्वपूर्ण है?

रिपोर्टिंग व्यवहार से तात्पर्य है — पीड़ित व्यक्ति का साइबर अपराध की घटना को समय रहते सक्षम प्राधिकरण (पुलिस, हेल्पलाइन या पोर्टल) तक पहुँचाना। समय पर की गई रिपोर्ट न केवल पीड़ित की धनराशि व डेटा सुरक्षित कर सकती है, बल्कि अपराधियों की पहचान व भविष्य में होने वाले अपराधों की रोकथाम में भी सहायक होती है।

"गोल्डन ऑवर" सिद्धांत

घटना के पहले कुछ घंटों के भीतर 1930 पर रिपोर्ट करने पर धोखाधड़ी की राशि बैंक/वॉलेट स्तर पर रोकी जा सकती है — पैसा अपराधी तक पहुँचने से पहले।

देर से रिपोर्ट करने के परिणाम

- **धनराशि की वापसी की संभावना घट जाती है**
- **अपराधी को सबूत मिटाने का समय मिल जाता है**
- **अन्य नागरिक भी उसी अपराधी का शिकार बन सकते हैं**

रिपोर्टिंग की श्रृंखला

1. **घटना घटित होना**
2. **जोखिम की पहचान**
3. **सहायता लेने का निर्णय**
4. **1930 / पोर्टल पर रिपोर्ट**
5. **कार्रवाई एवं समाधान**

लोग साइबर अपराध की रिपोर्ट क्यों नहीं करते?

Indian Cyber Crime Coordination Centre
सहवीर्य करवावहे • Working Together With Vigour

1. **शर्म / Social Stigma**
   "लोग क्या कहेंगे?"

2. **Fear**
   "कहीं परिवार को पता न चल जाए।"

3. **Victim Blaming**
   "तुमने OTP क्यों दिया?"

4. **Lack of Awareness**
   "रिपोर्ट कहाँ करनी है?"

5. **Fear of Police / Legal Process**

6. **यह सोच कि पैसा वापस नहीं मिलेगा**

7. **अपराध को छोटा समझना**

8. **Evidence न होने की गलत धारणा**

सबसे खतरनाक मिथक

- ✕ “मैंने गलती की है, इसलिए रिपोर्ट नहीं कर सकता।”
- ✕ “Online crime में police कुछ नहीं कर सकती।”
- ✕ “मेरे पास evidence नहीं है।”
- ✕ “थोड़े पैसे गए हैं, छोड़ देता हूँ।”
- ✕ “पहले scammer से बात करके पैसे वापस ले लूँगा।”
- ✕ “Social media पर report करने से मामला खत्म हो जाएगा।”

Reality

Victim होना आपकी गलती नहीं है।

रिपोर्ट करना आपका अधिकार और महत्वपूर्ण सुरक्षा कदम है।

भारत में कहाँ रिपोर्ट करें?

1	National Cyber Crime Reporting Portal (NCRP)	cybercrime.gov.in
2	Cyber Crime Helpline	1930
3	स्थानीय पुलिस / Cyber Police Station	
4	संबंधित बैंक / Financial Institution	
5	संबंधित Platform / Service Provider	

Emergency Principle

Financial Fraud → 1930 + Bank + NCRP

समय महत्वपूर्ण है — जितनी जल्दी रिपोर्ट, उतनी जल्दी response की संभावना।

1930 हेल्पलाइन — "गोल्डन ऑवर" कब करें? — Financial Cyber Fraud में तुरंत

Indian Cyber Crime Coordination Centre
सहवीर्य करवावहे • Working Together With Vigour

UPI Fraud	**Credit/Debit Card Fraud**	**Internet Banking Fraud**
Wallet Fraud	**Investment Scam**	**Loan App Scam**
Fake Customer Care Fraud	**Digital Arrest Scam**	**Online Trading Scam**

Remember

"Cyber Fraud में हर मिनट महत्वपूर्ण हो सकता है।"

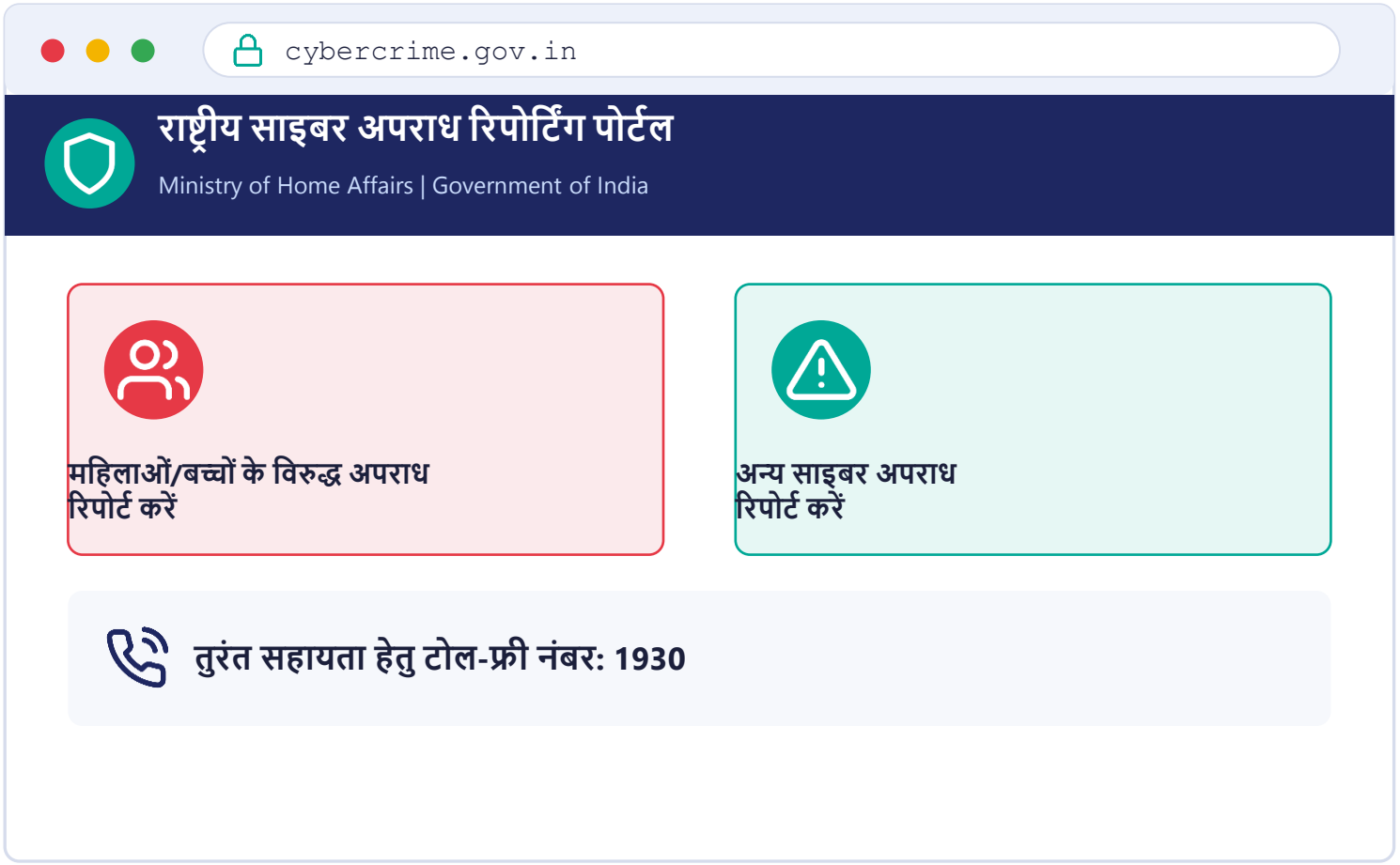
क्या करें?

Fraud हुआ → तुरंत 1930 पर संपर्क करें

- ☑ Bank को inform करें
- ☑ Transaction details सुरक्षित रखें
- ☑ NCRP पर complaint दर्ज करें

Cyber Crime Helpline
1930

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल — cybercrime.gov.in



(यह पोर्टल के वास्तविक ले-आउट पर आधारित प्रतिरूप है — कृपया लाइव डेमो हेतु cybercrime.gov.in खोलें)

पोर्टल की मुख्य विशेषताएँ

- सभी प्रकार के साइबर अपराधों हेतु एकीकृत रिपोर्टिंग
- महिलाओं व बच्चों से जुड़े मामलों को प्राथमिकता
- अन्य साइबर अपराधों हेतु गुमनाम (anonymous) रिपोर्ट का विकल्प
- शिकायत की स्थिति ऑनलाइन ट्रैक करने की सुविधा
- स्वतः संबंधित राज्य/UT पुलिस को अग्रेषित
- 1930 हेल्पलाइन से एकीकृत — तुरंत सहायता

cybercrime.gov.in/Hindi/Defaulthn.aspx

भारत सरकार
GOVERNMENT OF INDIA

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

Language

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal

Indian Cyber Crime Coordination Centre
सहवीर्यं करवावहै • Working Together With Vigour

आज़ादी का अमृत महोत्सव

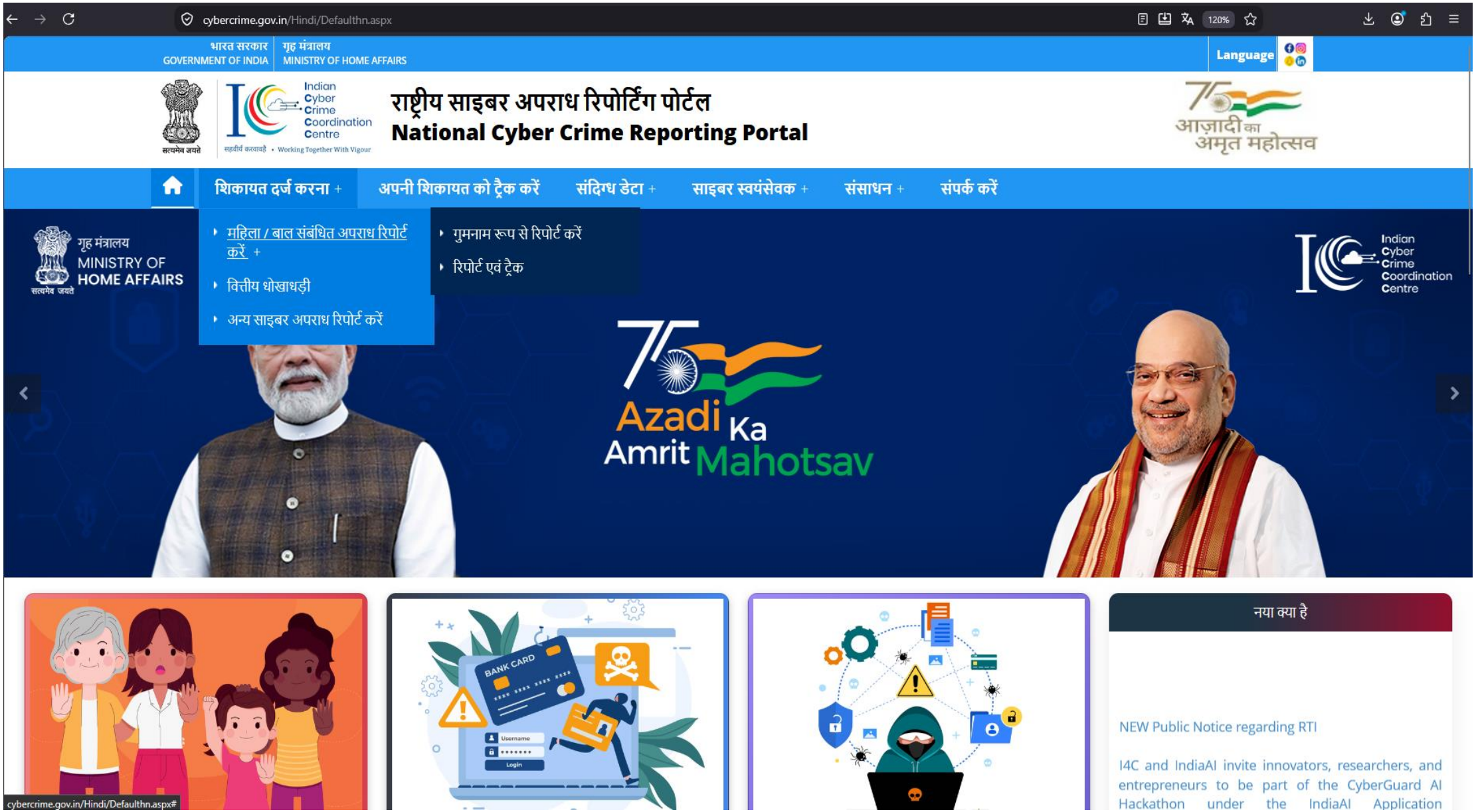
शिकायत दर्ज करना + | अपनी शिकायत को ट्रैक करें | संदिग्ध डेटा + | साइबर स्वयंसेवक + | संसाधन + | संपर्क करें

नया क्या है

search the mobile numbers, e-mail Ids, account numbers, URLs 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


cybercrime.gov.in/Hindi/Defaulthn.aspx
120%
भारत सरकार
GOVERNMENT OF INDIA
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
Language
Indian Cyber Crime Coordination Centre
सहभागिता करवाइहै • Working Together With Vigour
राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal
आज़ादी का अमृत महोत्सव
शिकायत दर्ज करना +
अपनी शिकायत को ट्रैक करें
संदिग्ध डेटा +
साइबर स्वयंसेवक +
संसाधन +
संपर्क करें
महिला / बाल संबंधित अपराध रिपोर्ट करें +
वित्तीय धोखाधड़ी
अन्य साइबर अपराध रिपोर्ट करें
गुमनाम रूप से रिपोर्ट करें
रिपोर्ट एवं ट्रैक
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
Indian Cyber Crime Coordination Centre
Azadi Ka Amrit Mahotsav
BANK CARD
Username
Login
नया क्या है
NEW Public Notice regarding RTI
I4C and IndiaAI invite innovators, researchers, and entrepreneurs to be part of the CyberGuard AI Hackathon under the IndiaAI Application
cybercrime.gov.in/Hindi/Defaulthn.aspx#

पोर्टल पर शिकायत दर्ज करने की प्रक्रिया

1

पोर्टल खोलें

cybercrime.gov.in पर जाएँ और भाषा चुनें

2

श्रेणी चुनें

"महिला/बाल अपराध" या "अन्य साइबर अपराध"

3

पंजीकरण करें

मोबाइल नंबर व OTP से सत्यापन करें

4

विवरण व प्रमाण दर्ज करें

घटना का विवरण, स्क्रीनशॉट/लेन-देन प्रमाण अपलोड करें

5

सबमिट व ट्रैकिंग

शिकायत क्रमांक (Acknowledgement No.) प्राप्त कर स्थिति ट्रैक करें

आवश्यक दस्तावेज़: लेन-देन विवरण/स्क्रीनशॉट, संदिग्ध नंबर/यूआरएल/UPI ID, पहचान प्रमाण (यदि आवश्यक हो) — सभी जानकारी गोपनीय रखी जाती है।

NCRP पर रिपोर्ट करते समय क्या चाहिए?

- ✔ घटना की तारीख और समय
- ✔ **Mobile number**
- ✔ **Email ID**
- ✔ **Social Media ID / URL**
- ✔ **Website / Link**
- ✔ **Transaction ID / UTR**
- ✔ **Bank / Wallet details**
- ✔ **Screenshots**
- ✔ **Chat / Email**
- ✔ **Call details**
- ✔ **Suspect details, यदि उपलब्ध हों**
- ✔ **अन्य संबंधित documents/evidence**

Important: *जितनी स्पष्ट जानकारी → उतना बेहतर incident picture*

Evidence क्यों महत्वपूर्ण है?

Digital Evidence = Investigation का आधार

Screenshots	Chats	Emails	URLs	Call logs
Transaction IDs	Receipts	Profile IDs	Date & Time	Device/account info

लेकिन ध्यान रखें

- ❌ Evidence को edit न करें
- ❌ Original chats/delete न करें
- ❌ Suspect को alert न करें
- ❌ Device को unnecessarily reset न करें

Screenshot ही पूरा Evidence नहीं है

Indian Cyber Crime Coordination Centre
सहवीर्यं करवावहै • Working Together With Vigour

एक screenshot क्या बताता है?

Screenshot →
Visible information

Investigation के लिए आवश्यकता हो सकती है:

- Original message
- URL
- Transaction trail
- Server-side records
- Time information
- Metadata
- Account information
- Device information
- Platform records

"Screenshot शुरुआत है, पूरी investigation नहीं।"

Cyber Incident के तुरंत बाद क्या करें?

Indian Cyber Crime Coordination Centre
सहवीर्य करवावहे • Working Together With Vigour

1

STOP

Scammer से interaction रोकें।

2

SECURE

Account / device / financial access सुरक्षित करें।

3

PRESERVE

Evidence सुरक्षित रखें।

4

REPORT

1930 / NCRP / Police / relevant institution.

5

INFORM

परिवार, school authority, organisation या trusted person को बताएं।

Financial Fraud: Immediate Action

☑ DO

- ☑ Bank को तुरंत inform करें
- ☑ Card / account block करें, जहाँ आवश्यक हो
- ☑ 1930 पर report करें
- ☑ NCRP पर complaint करें
- ☑ Transaction ID सुरक्षित रखें
- ☑ Screenshots रखें

✗ DON'T

- ✗ Scammer को और पैसा न दें
- ✗ OTP / PIN न दें
- ✗ Remote-access app install न करें
- ✗ “Refund fee” न दें
- ✗ Evidence delete न करें

Social Media Account Hacked हो जाए तो?

Immediate Steps

1. Password बदलें
2. All active sessions logout करें
3. 2-Factor Authentication enable करें
4. Recovery email/mobile check करें
5. Unauthorized posts/messages identify करें
6. Platform recovery/report mechanism use करें
7. यदि अपराध हुआ है → NCRP/Police को report करें

Cyberbullying / Online Harassment

अगर कोई लगातार online परेशान कर रहा है:

- Messages delete करने से पहले preserve करें
- Screenshots लें
- Profile URL/username सुरक्षित रखें
- Block / restrict करें, जहाँ उचित हो
- Platform पर report करें
- Trusted adult/teacher/parent को बताएं
- गंभीर स्थिति में police/cybercrime authorities से संपर्क करें

सबसे महत्वपूर्ण

"Bullying को सहना मजबूरी नहीं है।"

बच्चों के लिए विशेष संदेश

☑ DO

- ☑ किसी trusted adult को बताएं
- ☑ Evidence preserve करें
- ☑ Account secure करें
- ☑ Report करें
- ☑ जरूरत पड़ने पर authorities से सहायता लें

✗ DON'T

- ✗ डरकर पैसे दें
- ✗ अकेले situation handle करें
- ✗ शर्म के कारण छिपाएँ
- ✗ evidence delete करें

Sextortion / Online Blackmail

अगर कोई private photo/video के नाम पर धमकी दे

❌ DON'T PAY

❌ DON'T NEGOTIATE

❌ DON'T SEND MORE CONTENT

Instead:

Preserve → **Block/Restrict where appropriate** → **Report** → **Seek trusted support** → **Police/Cybercrime reporting**

"Blackmail करने वाला व्यक्ति आपकी शर्म का फायदा उठाता है।
मदद लेने में शर्म नहीं है।"

Digital Arrest Scam — Common Red Flags

- “आपके नाम पर FIR है।”
- “आपका Aadhaar illegal activity में इस्तेमाल हुआ है।”
- “Video call पर police verification होगा।”
- “आपको घर से बाहर नहीं जाना है।”
- “Security deposit जमा करें।”
- “किसी को मत बताइए।”

Remember: Real law-enforcement processes do not work through fear-based video-call extortion demanding immediate money.

Fake Customer Care Fraud

1. एक व्यक्ति ने Google पर customer-care number search किया।
2. उसे fake number मिला। उसने call किया।
3. Scammer ने कहा: “आपका refund process करने के लिए remote-support app install करें।”
4. Victim ने app install किया। कुछ ही समय बाद account से पैसा निकल गया।

अब सवाल: कहाँ गलती हुई?

- Fake number पर भरोसा
- Remote-access app install करना
- Sensitive information देना
- Fraud के बाद report करने में delay

Learning

Verify → Think → Act → Report

“मैंने गलती की इसलिए मैं report नहीं करूँगा”

1. एक student को social media पर blackmail किया गया।
2. उसने किसी को नहीं बताया। Blackmailer ने pressure बढ़ाया।
3. Student ने account delete कर दिया।

क्या गलत हुआ?

- ✕ Evidence lost
- ✕ Help नहीं ली
- ✕ Situation escalate हुई

Better Response

1. Trusted Adult
2. Preserve Evidence
3. Report
4. Professional Support

Victim से पहला सवाल क्या होना चाहिए?

❌ गलत approach

"तुमने OTP क्यों दिया?"

☑ सही approach

"आप सुरक्षित हैं? पहले हम नुकसान रोकते हैं। फिर देखते हैं कि क्या हुआ और कहाँ report करना है।"

Victim-Centred Response

Listen → Support → Secure → Preserve → Report

School में Cybercrime Response Chain

1. Student
2. Trusted Teacher / Parent
3. School Administration
4. Appropriate Reporting Channel
5. Police / Cybercrime Authorities
6. Follow-up & Support

School का उद्देश्य: Victim को blame करना नहीं — support और safe reporting सुनिश्चित करना है।

Teachers की भूमिका

☑ DO

- ☑ Student को सुनें
- ☑ Victim-blaming से बचें
- ☑ Evidence preserve करने में guide करें
- ☑ Appropriate authority तक मामला escalate करें
- ☑ Confidentiality का सम्मान करें
- ☑ गंभीर मामलों में तत्काल reporting/support सुनिश्चित करें

✗ DON'T

- ✗ Publicly discuss करें
- ✗ Student को shame करें
- ✗ Evidence delete करवाएँ
- ✗ स्वयं suspect से confrontation करें

जब बच्चा कहे: “मेरे साथ online कुछ गलत हुआ है।”

पहला response (गलत)

❌ “मैंने पहले ही कहा था!”
❌ “तुमने ऐसा किया ही क्यों?”

Instead (सही)

☑ “तुमने मुझे बताया, यह अच्छी बात है।”
☑ “हम मिलकर इसे handle करेंगे।”
☑ “पहले तुम्हें safe करते हैं।”

Remember

A supportive first response can determine whether a child seeks help again.

Reporting में Delay क्यों खतरनाक है?

Delay → Evidence Loss + Further Harm + Financial Loss

☑

Fraud → 10 मिनट में Report

vs.

✗

Fraud → 3 दिन बाद Report

"पहले Report, बाद में Regret नहीं।"

विशेष रूप से financial cyber fraud में immediate reporting महत्वपूर्ण है।

Reporting के बाद क्या होता है?

Complaint ≠ End of Process

1. **Complaint Registration**
2. **Initial Assessment**
3. **Agency / Police Action**
4. **Evidence / Transaction Analysis**
5. **Follow-up / Investigation**

Victim की भूमिका

- सही जानकारी दें
- Reference/complaint details सुरक्षित रखें
- Evidence preserve रखें
- आवश्यकता पर investigating authority से cooperate करें

Cybercrime Reporting में क्या सुधार चाहिए?

Awareness

लोगों को पता हो कि कहाँ report करना है।

Accessibility

Reporting mechanism आसान हो।

Trust

Victim को लगे कि उसकी बात सुनी जाएगी।

Speed

Particularly financial fraud में rapid response।

Privacy

Sensitive मामलों में victim dignity और confidentiality का ध्यान।

Support

Legal + technical + emotional support जहाँ आवश्यक हो।

Do's & Don'ts

DO ☑	DON'T ✕
तुरंत report करें	Delay न करें
Evidence preserve करें	Evidence delete न करें
Bank को inform करें	Scammer को और पैसा न दें
Strong password रखें	OTP/PIN share न करें
2FA enable करें	Unknown apps install न करें
Trusted person को बताएं	शर्म के कारण छिपाएँ नहीं
Official channels use करें	Fake helpline पर भरोसा न करें

याद रखने योग्य 7 बातें — CYBER SAFETY

Indian Cyber Crime Coordination Centre
सहवीर्यं करवावहै • Working Together With Vigour

1

STOP

आगे interaction रोकें

2

SECURE

Accounts/device सुरक्षित करें

3

SAVE

Evidence सुरक्षित रखें

4

REPORT

उचित channel पर शिकायत करें

5

INFORM

Trusted person/authority को बताएं

6

FOLLOW-UP

Complaint details संभालकर रखें

7

SUPPORT

जरूरत हो तो सहायता लें

महत्वपूर्ण संपर्क — Cybercrime सहायता

National Cyber Crime Reporting Portal

www.cybercrime.gov.in

Cyber Crime Helpline

1930

Emergency / Immediate Threat

112

इसके अतिरिक्त:

- स्थानीय पुलिस
- Cyber Police Station
- संबंधित Bank / Financial Institution
- संबंधित Online Platform

आपको ₹50,000 का UPI fraud हो गया।

आपके पास केवल:

- Transaction ID
- SMS
- Bank statement
- Scammer का mobile number

आपके पहले 3 कदम क्या होंगे?

Think → Discuss → Answer

Expected Response:

Bank → 1930 → NCRP

और उपलब्ध evidence सुरक्षित रखना।

“Cybercrime से बचना जरूरी है,
लेकिन Cybercrime होने पर मदद माँगना उससे भी जरूरी है।”

- Report करना कमजोरी नहीं है।
- Help माँगना शर्म की बात नहीं है।
- Victim को blame नहीं — support चाहिए।

Indian Cyber Crime Coordination Centre
सहवीर्य करवावहे • Working Together With Vigour

STOP · SECURE · SAVE · REPORT · SEEK HELP

चुप्पी अपराधी को मजबूत करती है।
सही समय पर रिपोर्टिंग पीड़ित को मजबूत बनाती है।

धन्यवाद