



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS



Understanding Financial Cyber Crime & How to Report

Overview of I4C



VALUES

Integrity Innovation Teamwork
Adaptability Initiative Agility
Continuous Learning

I4C was set up with the approval of Hon'ble Home Minister with the main objective to set up a National Cybercrime Coordination Centre as an effective apparatus to handle all issues related to cybercrime in the country.

<https://i4c.mha.gov.in>

VISION

To create a safe cyberspace for the citizens of India

MISSION

To create an effective framework and ecosystem for the prevention, detection, investigation, and prosecution of Cybercrime in the country.

Introduction:

- **Rise in digital transactions**

Digital payments are increasing rapidly as more people use smartphones and online banking for convenience and speed. Government initiatives, UPI, and secure apps have made online transactions easier and widely accepted.

- **Growing financial cyber frauds**

Financial cyber frauds are increasing as criminals use fake links, phishing calls, and scam apps to steal money.

Lack of awareness and sharing OTPs, PINs, or personal details make people easy targets.

- **Importance of awareness & reporting**

Awareness helps people recognize scams and protect their money before fraud happens.

Timely reporting to authorities increases the chances of recovering funds and stopping criminals.

Understanding Financial Cyber Crime

- Financial cyber crime refers to illegal activities carried out using computers, mobile devices or the internet to steal money, financial data, or personal information.
- These criminals target individuals, businesses, banks, and government systems through methods like phishing emails, fake investment schemes, online frauds, identity theft, UPI scams, credit card misuse, and hacking of accounts.

Understanding Financial Cyber Crime

- In today's digital era where we increasingly use online banking, UPI, digital wallets, and e-commerce.
- cyber criminals are becoming smarter and more organized.
- Understanding financial cyber crime helps us stay safe
- detect suspicious activity early
- protect our hard-earned money.
- Knowledge, awareness and timely reporting are the keys to preventing losses.

What is Financial Cyber Crime?

- Online monetary theft

stealing money through digital methods like phishing, fake links, or hacking bank accounts.

- Unauthorized digital transactions

Unauthorized digital transactions occur when money is transferred from your account without your consent or knowledge.

- Digital fraud platforms

Digital fraud platforms are online channels like fake websites, apps, and social media pages used to trick people and steal money.

Why Financial Cyber Crime Happens:

- High digital adoption

High digital adoption means more people and businesses are using online banking, digital payments, and financial apps for everyday transactions. This rapid shift to digital platforms increases convenience but also opens more opportunities for cyber criminals to target users.

- Fear: Scammers create panic to force quick decisions without thinking.
- Greed: Fraudsters attract victims with promises of easy money or high returns.
- Shame: Victims often hide the incident due to embarrassment, allowing fraudsters to continue.
- Weak passwords & data leaks

Weak passwords and data leaks allow hackers to easily access accounts and misuse personal financial information.

Trending Financial Cyber Crime:

- Phishing/Smishing/Vishing
- Investment scams
- Fake Loan app scams
- Digital Arrest
- Online task job fraud/ work from home
- Sextortion
- Online gambling
- Fake gaming apps
- SIM swap fraud
- Crypto scams

Few Examples

Social Engineering:

- - Emotional manipulation
- - Fake bank/authority calls
- - Urgency & panic tactics

Investment & Loan App Scams:

- - Unrealistic returns
- - Fake crypto schemes
- - Loan app harassment

SIM Swap & Mobile Fraud:

- - Duplicate SIM issuance
- - OTP interception

Emerging Frauds:

- - AI voice spoof
- - Deepfake calls
- - Fake customer care numbers

Where to Report:

- - cybercrime.gov.in
- - 1930 Helpline
- - Police/cyber cell
- - Bank customer care



Report a
Cybercrime on
1930

Report a Cybercrime on
www.cybercrime.gov.in



National Cyber Crime Reporting Portal (NCRP)

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

The screenshot displays the homepage of the National Cyber Crime Reporting Portal (NCRP) at cybercrime.gov.in. The browser's address bar shows the URL, and the page features a blue header with the NCRP logo and the text "राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल National Cyber Crime Reporting Portal". Below the header, a navigation menu includes "Register a Complaint", "Track your Complaint", "Report & Check Suspect", "Cyber Volunteers", "Learning Corner", and "Contact Us". The main banner area features portraits of Prime Minister Narendra Modi and Home Minister Anurag Singh Khurana, with the "75 Azadi Ka Amrit Mahotsav" logo. The page is divided into three main sections: "WOMEN/CHILDREN RELATED CRIME" with "Register Anonymously" and "Register & Track" buttons; "FINANCIAL FRAUD" with a "Register a Complaint" button; and "OTHER CYBER CRIME" with a "Register a Complaint" button. A "What's new" section on the right contains a public notice regarding RTI. The footer shows the Windows taskbar with the time 3:10 PM on 11/2/2025.

Salient features

- All types of cyber crime incidents can be reported from anywhere
- Special focus on online child sex abuse/rape-gang rape incidents
- National/State/District-Level monitoring dashboards
- Tagging of several suspect credentials and facility for joint collaboration among LEAs
- Online status tracking facility for the complainant
- Facility to register/participate as cyber volunteers
- Daily Digest
- Cyber Awareness
- Advisory

National Cyber Crime Reporting Portal (NCRP)

CITIZEN INTERFACE



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

← → ↻ https://cybercrime.gov.in/Webform/Crime_AuthoLogin.aspx ☆ 📷 🗨️ 📄 Verify it's you

भारत सरकार
GOVERNMENT OF INDIA

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

Language

  **राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल**
National Cyber Crime Reporting Portal

आजादी का
अमृत महोत्सव

Home > Login

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

CHECK LIST FOR COMPLAINANT

Please keep this information ready before filing your complaint:

Mandatory Information

1. Incident Date and Time.
2. Incident details (minimum 200 characters) without any special characters (#\$%^&*~|-|!).
3. Soft copy of any national Id (Voter Id, Driving license, Passport, PAN Card, Aadhaar Card) of complainant in .jpeg, .jpg, .png format (file size should not more than 5 MB).
4. In case of financial fraud, please keep following information ready:
 - i) Name of the Bank/ Wallet/Merchant
 - ii) 12-digit Transaction id/UTR No.
 - iii) Date of transaction
 - iv) Fraud amount
5. Soft copy of all the relevant evidences related to the cyber crime (not more than 10 MB each)

Optional/Desirable Information:

1. Suspected website URLs/ Social Media handles (wherever applicable)
2. Suspect Details (if available)
 - i) Mobile No
 - ii) Email id
 - iii) Bank Account No
 - iv) Address
 - v) Soft copy of photograph of suspect in .jpeg, .jpg, .png format (not more than 5 MB)
 - vi) Any other document through which suspect can be identified.

CITIZEN LOGIN

[Click Here for New User](#)

LOGIN ID: *

MOBILE NO: *

OTP: *

[Forgot Login Id](#)

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)

This facility has been created for quick reporting of Attempts made to access Sensitive 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*

What do you want to report ?

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

Search Suspect on NCRP Portal



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

Browser address bar: https://cybercrime.gov.in/Webform/suspect_search_repository.aspx

Navigation menu: [Home](#) | [Register a Complaint +](#) | [Track your Complaint](#) | [Report & Check Suspect +](#) | **[Cyber Volunteers +](#)** | [Learning Corner +](#) | [Contact Us](#)

Breadcrumbs: Home > Suspect Search

This Repository of suspect identifier has been created on the basis of multiple complaints filed by citizens for cybercrimes on this portal.

<input checked="" type="radio"/> Mobile	<input type="radio"/> E-mail
<input type="radio"/> Bank Account Number	<input type="radio"/> Social Media
<input type="radio"/> UPI ID	

Do not add +91 with Mobile number


Enter Mobile No

Search Suspect on NCRP Portal

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

Browser address bar: https://cybercrime.gov.in/Webform/suspect_search_websites.aspx

Header: भारत सरकार / GOVERNMENT OF INDIA, गृह मंत्रालय / MINISTRY OF HOME AFFAIRS

Language: 

Logos: Government of India, Indian Cyber Crime Coordination Centre, 75th Anniversary (आज़ादी का अमृत महोत्सव)

Navigation: Home, Register a Complaint +, Track your Complaint, Report & Check Suspect +, Cyber Volunteers +, Learning Corner +, Contact Us

Breadcrumbs: Home > Suspect Search

This Repository of suspect identifier has been created on the basis of multiple complaints filed by citizens for cybercrimes on this portal.

Suspect Type: Website URL:

UNteJ7

S No.	Suspect Type	Name of the Website/ Mobile App
1	Website Url	https://asss.short.gy/PanKyc.https://sysf-6ac.web.app/d1
2	Website Url	https://sbicreditcardhelpd01.wixsite.com/my-site
3	Website Url	https://www.cardcpp.org
4	Website Url	https://customer-care.site/courier-service/
5	Website Url	https://courieractivation.net/
6	Website Url	https://courierserviceonlin0.wixsite.com/onlinecourierservice
7	Website Url	https://travelwithhell.site/
8	Website Url	https://finance288.com/home

Advisories on NCRP Portal





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

→ <https://cybercrime.gov.in/Webform/Advisory.aspx> ☆ 📷 📄 📌 Verify it's you

भारत सरकार
GOVERNMENT OF INDIA

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

Language 🇮🇳 🇬🇧 🇪🇳

  Indian
Cyber
Crime
Coordination
Centre
सहयोग करवावट • Working Together With Vigour

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal

75
आज़ादी का
अमृत महोत्सव

Home > Resources > Advisories

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



Advisories

ADVISORIES

APRIL 08 2025

Advisory on Rise in Fake Captcha Filling Jobs' based cybercrime

There has been significant rise in complaints pertaining to online scams involving fraudulent CAPTCHA-filling jobs.....

ADVISORIES

March 06 2025

Advisory on 'Digital Arrest' based cybercrime in India

Many complaints are being reported on National Cyber Crime Reporting Portal (NCRP) regarding intimidation, blackmail

ADVISORIES

JUNE 27 2024

ADVISORIES REGARDING FAKE JOB RACKET TARGETING INDIAN YOUTH

This advisory is being issued in continuation of the Embassy's advisories on the above subject, issued on 5th July 2022.....

ADVISORIES

April 22 2024

BEWARE OF FAKE STOCK MARKET INVESTMENT WEBSITE/APP.

With increasing adoption of digital communication platforms like Instagram, Facebook, WhatsApp and Telegram, there has been an....

Daily Digest



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

Cyber Crime Portal

in/Webform/dailyDigest.aspx

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

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

Working Together With Vigour

Complaint + Track your Complaint Report & Check Suspect + Cyber Volunteers + Learning Corner + Contact Us

es > Daily Digest

Digest From Date: 03-10-2025 Digest To Date: 03-11-2025

Title : Description :

Search

Sr No.	Title	Description	Daily Digest Date	Download
1	Daily Digest- 31 October 2025	I4C Daily Digest- 31 October 2025	31/October/2025	Download
2	Daily Digest- 30 October 2025	I4C Daily Digest- 30 October 2025	30/October/2025	Download
3	Daily Digest- 29 October 2025	I4C Daily Digest- 29 October 2025	29/October/2025	Download
4	Daily Digest- 28 October 2025	I4C Daily Digest- 28 October 2025	28/October/2025	Download
5	Daily Digest- 27 October 2025	I4C Daily Digest- 27 October 2025	27/October/2025	Download

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

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

CYBER DIGEST

INDIAN CYBER CRIME COORDINATION CENTRE

31.10.2025

CD-737

Report 1930

The Ministry of Home Affairs has launched a toll-free Helpline number '1930'

In today's digital age, the necessity of a dedicated platform to report and combat cybercrimes is more crucial than ever. The helpline plays a vital role within the National Cybercrime Reporting Portal, which aims to establish a safe cyberspace for all citizens.



Reporting Steps:

- Call 1930
- Victim details
- Transaction ID & screenshots
- Bank details
- Fraud account details
- File portal complaint
- Upload proof
- Track progress

Cyber Hygiene



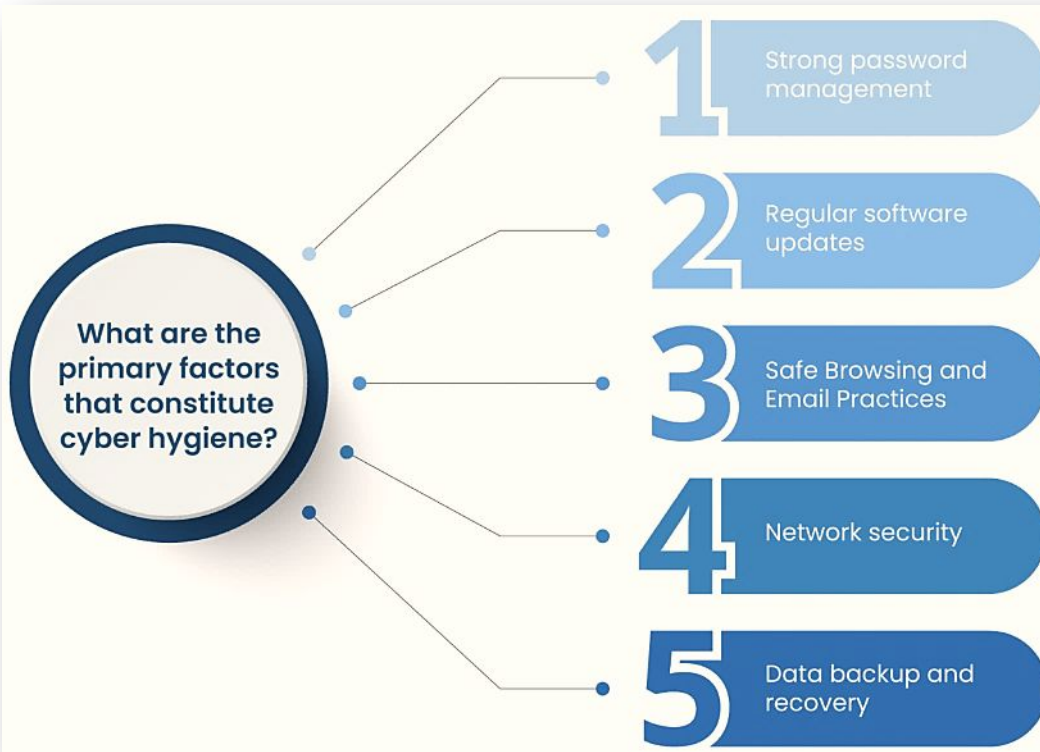
Protecting sensitive data and personal information



Safeguarding business operations and reputation



Preventing financial losses and legal consequences



Cyber Hygiene:

- Strong passwords & 2FA
- App/device updates
- Avoid public Wi-Fi
- Install apps from trusted stores

Do's & Don'ts:

- Do: verify links, secure banking
- Don't: share OTP/PIN/CVV, click random links

Conclusion:

- - Awareness + fast reporting
- - Stay alert, stay secure



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

सत्यमेव जयते

Stay Cyber Safe



Thanks