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

शिक्षा मंत्रालय
MINISTRY OF EDUCATION
सत्यमेव जयते

विद्यया ऽमृतमश्नुते
एन सी ई आर टी
NCERT

Cybercrime Landscape

Risks, Trends, and Impact on School Education

Dr Deepak Kumar
Sr Technical Manager – Cyber

TRENDING CYBER CRIME

Google digital arrest

All Images Videos News Shopping Books Maps More

The Hindu

Digital arrest scams: what to know and how to fight back

Combatting cybercrimes in India requires awareness, vigilance, and reporting to protect individuals and national security effectively.

15 hours ago

The Tribune

Digital arrest: Sec 8 woman loses Rs 57L

In yet another incident of "digital arrest", a woman has been duped of Rs 57 lakh by fraudsters posing as CBI and police officers.

7 hours ago

Times of India

Digital arrest conman held in Rajasthan

Kolkata: A 20-year-old man from Rajasthan, Mahesh Kumar, was apprehended from Alwar on Tuesday by Bidhannagar cops for allegedly defrauding...

10 hours ago

Telegraph India

76-year-old woman victim of cyber gang's 'digital arrest': Rs 11 lakh stolen

The gang members claimed that her Aadhaar card was used for fraudulent activities, including sexual harassment, circulating fake gambling...

3 hours ago

Patrika News

Teacher Receives 'Digital Arrest' Penalty: Case Closed After Cyber Cell Investigation

A fraudulent "CBI officer" proposed a settlement, offering to resolve the case through a digital arrest followed by bail. - Patrika News.

52 minutes ago

Google digital arrest

Live Law

'Apologize To Public If National Cybercrime Helpline Doesn't Work': Bombay HC Summons Officials In Case...

While hearing a petition filed by a septuagenarian woman, a victim of 'digital arrest' who lost Rs 32 lakhs, the Bombay High Court on...

12 hours ago

Deccan Herald

Indore professor loses Rs 33 lakh in 'digital arrest' scam, gets back Rs 26.45 lakh

Indore: In the latest case of "digital arrest" fraud in Indore, a gang of cyber thugs trapped a retired professor and duped him of Rs 33...

1 day ago

Mint

'Digital Arrest' scam: Noida family loses ₹1.10 crore to cyber criminals; here's what happened

A Noida family lost over ₹1 crore in a cyber fraud scheme called 'digital arrest', where fraudsters impersonated government officials.

3 weeks ago

The420.in

Delhi's Biggest Digital Arrest Scam: Senior Citizen Duped of Rs 19 Crore

This incident marks one of the largest digital fraud cases in Delhi, surpassing a previous Rs 12 crore scam in the capital.

3 days ago

The New Indian Express

Digital arrest scam: Two including manpower agency owner arrested in Chennai

During investigation, the police discovered that Venkatesh ran a manpower agency with an associate who later fled to Cambodia.

Indian Cyber Crime Coordination Centre

Source: Varonis
Tweet @D3pak

MYTH	REALITY
A strong password is enough to keep your business safe	1 Two-factor authentication and data monitoring is also needed
Small- and medium-sized businesses aren't targeted by hackers	2 Small businesses made up over half of last year's breach victims
Only certain industries are vulnerable to cyber attacks	3 Any business with sensitive information is vulnerable to attack
Anti-virus and anti-malware software keeps you completely safe	4 Software can't protect against all cyber risks
Cybersecurity threats come from the outside	5 Insider threats are just as likely, and harder to detect

MYTH	REALITY
Cybersecurity is solely the IT department's responsibility	6 All employees play a role in keeping a company cybersafe
If Wi-Fi has a password, it's secure	7 All public Wi-Fi can be compromised, even with a password
You'll know right away if your computer is infected	8 Modern malware is stealthy and hard to detect
Personal devices don't need to be secured at work	9 All smart devices, including wearables, can compromise a network's system
Complete cybersecurity can be achieved	10 Cyber preparedness is ongoing, with new threats emerging every day

EXPLOITING EMOTIONS!

Criminals deceive the human mind by manipulating emotions. Exploiting emotions leads to computer frauds and cyber crimes;

GREED

(Winning Lottery, Free or lucrative deals, offers)

PANIC

(Card or blocking, account hacked, penalty)

TRUST

(Calling from bank, link for payments)

FEAR

(Offer expiring in minutes)

2

CONTEXT

Why this matters

Sensitive data at scale

Schools store student identities, parent contacts, exam records,address and health details.

One attack, wide blast radius

Classes are interrupted, minors’ data is exposed, and panic spreads across parents and staff.

A top target in 2026

Education is now among India’s most targeted sectors for cyber attacks.

Sources: ETCISO / India Cyber Threat Report 2026

3

THREAT TYPES

What cybercrime looks like in schools

Phishing messages

Fake fee notices, attendance updates and exam circulars sent by email or WhatsApp.

Cloned portals

Fake school websites and login pages built to harvest credentials and payments.

Ransomware & theft

Credential theft, locked systems and unauthorized access to student records.

AI deepfakes

Ordinary school photos misused to create fake explicit or defamatory images.

Sources: NDTV and allied 2026 reporting

4

DATA

India 2026 threat snapshot

265.52M

total threat detections

~505

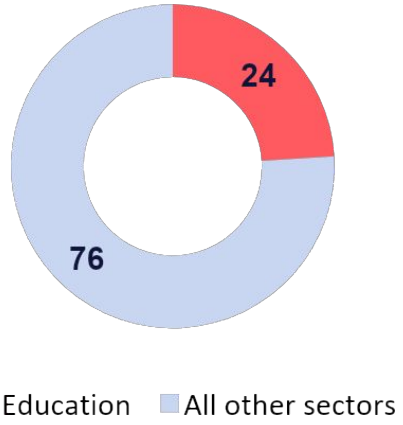
detections per minute

4.92M

in education alone

Education accounted for nearly 24% of all detections — the sector is not just exposed, it is actively targeted at large scale.

Share of detections



Source: India Cyber Threat Report 2026 (ETCISO)

5

ROOT CAUSES

Why schools are easy targets

1	**Weak password hygiene**	Thousands of users, reused passwords, and shared logins across multiple apps/CCTV/HRMS .
2	**Social engineering is easy**	Teachers, student and parents all coordinate over messaging apps and groups.
3	**Small cyber budgets**	Limited monitoring tools mean threats go unnoticed and response is slow.
4	**Expanding cloud surface**	Learning platforms widen exposure when they are not tightly configured.

Sources: ETCISO / India Cyber Threat Report 2026

6

CONSEQUENCES

Impact on education

Lost learning time

Outages and investigations pull classes off track.

Emotional harm

Deepfake abuse and public exposure hurt wellbeing.

Long-lived leaks

Leaked records get reused for scams for years.

Loss of trust

Reputation damage with parents and the community.

Sources: CYFIRMA and allied 2026 reporting

REAL-WORLD CASE 1

Guwahati deepfake school case, 2026

School photos weaponized into harassment content

- A Guwahati school opened an inquiry over AI-generated explicit deepfakes of students and teachers.
- The matter reached the Assam Police Cyber Crime Branch; images were allegedly shared via Telegram.
- Ordinary school photos can be turned into harassment content.

THE TIMES OF INDIA

3 Assam students suspended for creating deepfake images of 64 female teachers, peers; probe on

Tathagata Bhattacharjee / Jun 12, 2026, 22:13 IST

Preferred on G | Comments | Share | AA

Sources: NDTV, Free Press Journal (2026)

REAL-WORLD CASE 2

Student data weaponization, 2026

Student information traded as a cybercrime asset

- CYFIRMA: threat actors advertised a database of ~682,000 student records linked to India.
- Such data fuels cybercrime e.g phishing, impersonation, scholarship scams and fee fraud.
- Social media trauma : A clear example of student data becoming a cybercrime asset.

Source: CYFIRMA (2026)

9

ACTION PLAN

What schools should do

Enforce 2FA / MFA

Multi-factor login for all admins and teachers.

Least privilege

Important data only on a need-to-know basis.

Train everyone

Staff, students and parents verify every link and trust.

Offline backups

Immutable, offline backups tested for real restores.

Incident response

A rapid situational awareness rehearsed process for phishing, leaks and deepfakes.

Sources: ETCISO, CYFIRMA and allied 2026 reporting

CLOSING MESSAGE

Cybercrime is now a student safety issue

Not just IT

School cybercrime directly affects student safety, dignity and trust.

Top 2026 risks

Social media , cyber-bullying phishing, data leaks, AI deepfakes and exam-related scam.

What works

Awareness, **AWARENESS,** secure systems and fast response sharply reduce harm.

Secure the Individual. Protect the School.

ACTION PLAN

Red Flags

Poorly created website and App	No information of the founder	Registration details not found	No complete work details
Lots of bad reviews online	No official contact details	No Proper contact details	Hundreds of Complain online

All certificates and proofs shown in app is fake	No active/legit social media handles and many more	Follow Earning App offer very lucrative plan.

OPERATION CyHAWK 5.0: Delhi Police's Decisive Strike on Cyber Crime

Operation CyHawk 5.0 was a high-intensity, 48-hour nationwide offensive (June 16–17, 2026) involving 2,374 personnel. It targeted the "nerve centers" of cyber fraud, ranging from mule account handlers to malware distributors across 21 States and UTs.

5 Key Data Points

7,189 Detentions & 916 Arrests

The largest mobilization in CyHawk history, with legal action taken against 4,200+ persons.

₹700 Crore Financial Impact

Total cheated amount linked to cases and complaints addressed during the 48-hour operation.

891 Cases Addressed

Comprising 461 fresh FIRs and 410 previously unsolved cases linked to the NCRP portal.

2,300+ Digital Tools Seized

Recovery of 760+ phones, 820 SIM cards, 228 ATM cards, and 104 computers.

21 States & UTs Covered

A massive coordinated strike by 715 raiding teams across India's geographic footprint.

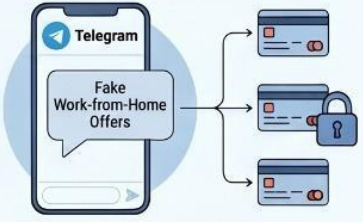
Leadership Vision

"Operation CyHawk reflects Delhi Police's unwavering commitment to stay ahead of cyber criminals... This sends an unequivocal message—those who exploit citizens will be brought to justice."

— Commissioner of Police, Delhi, Sh. Satish Golchha, IPS

The Anatomy of Cyber Fraud (Modus Operandi)

Mule Account Networks



Recruitment for account & access to bank accounts

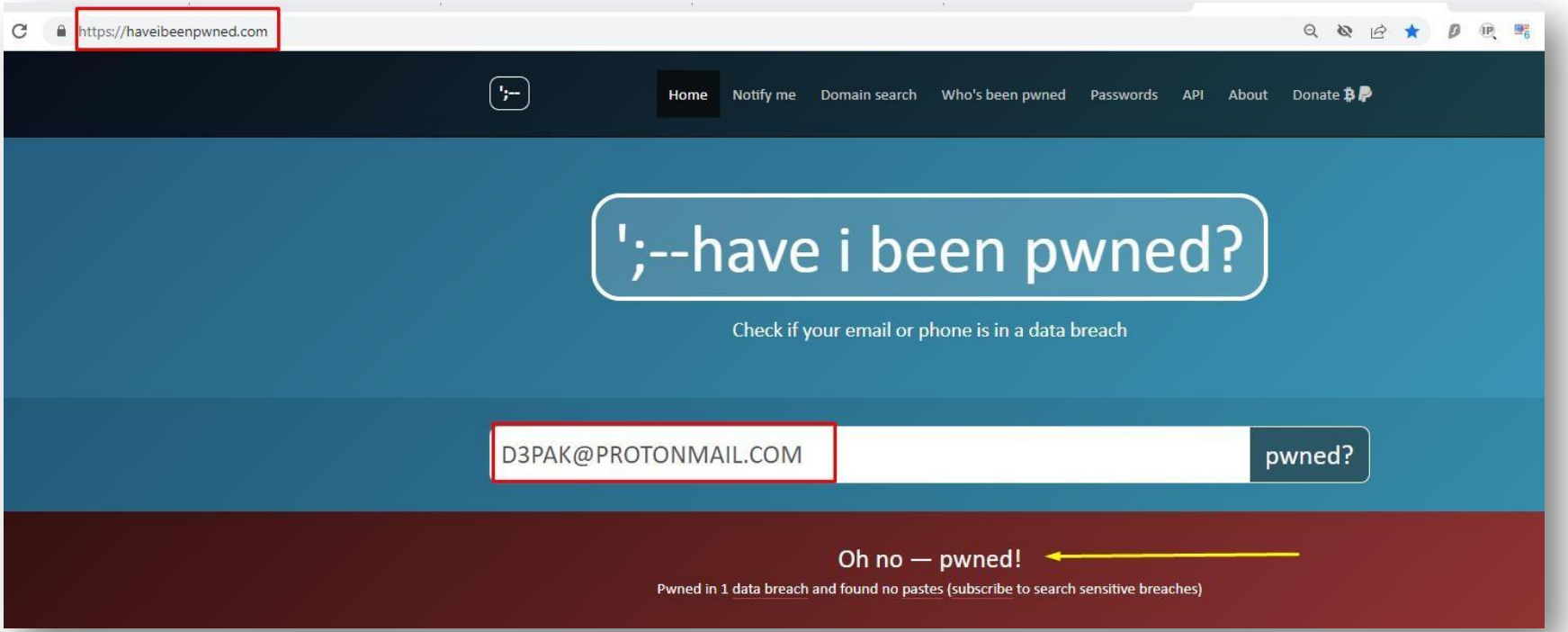
Malicious .apk (MaaS)

Silent malware used to intercept One-Time Passwords

Fraud Call Centres

Tech support hub through domestic and foreign victims

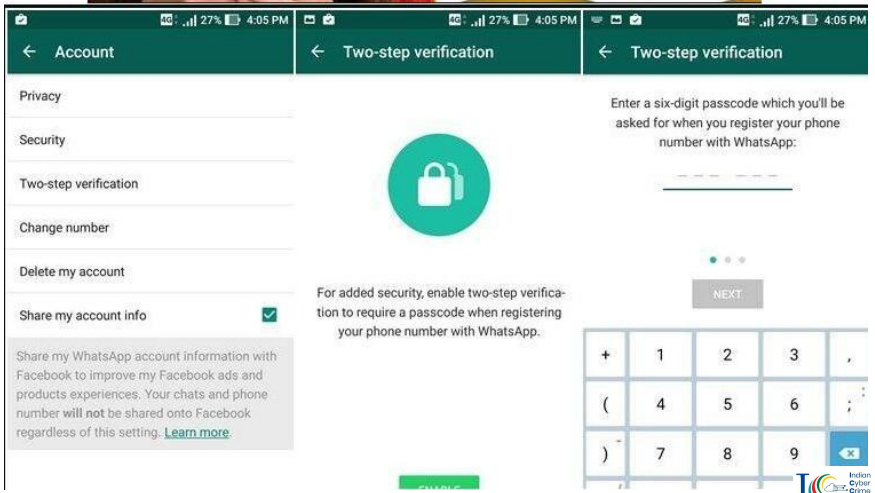
https://haveibeenpwned.com/



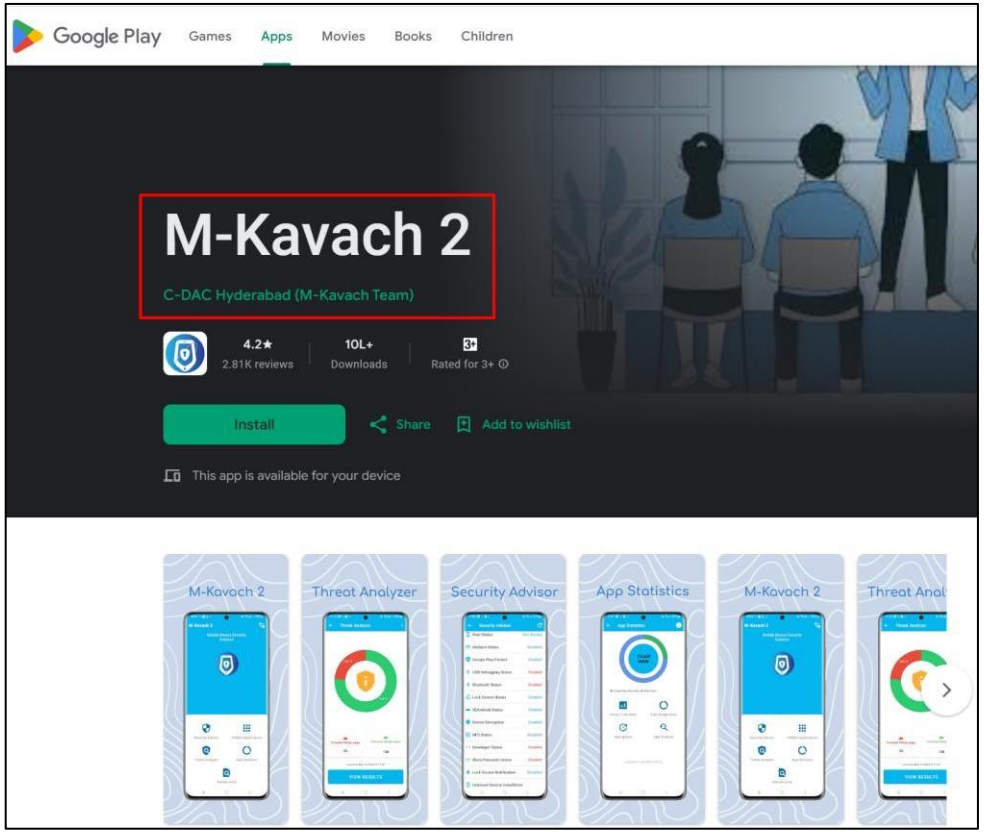
DEMO 1

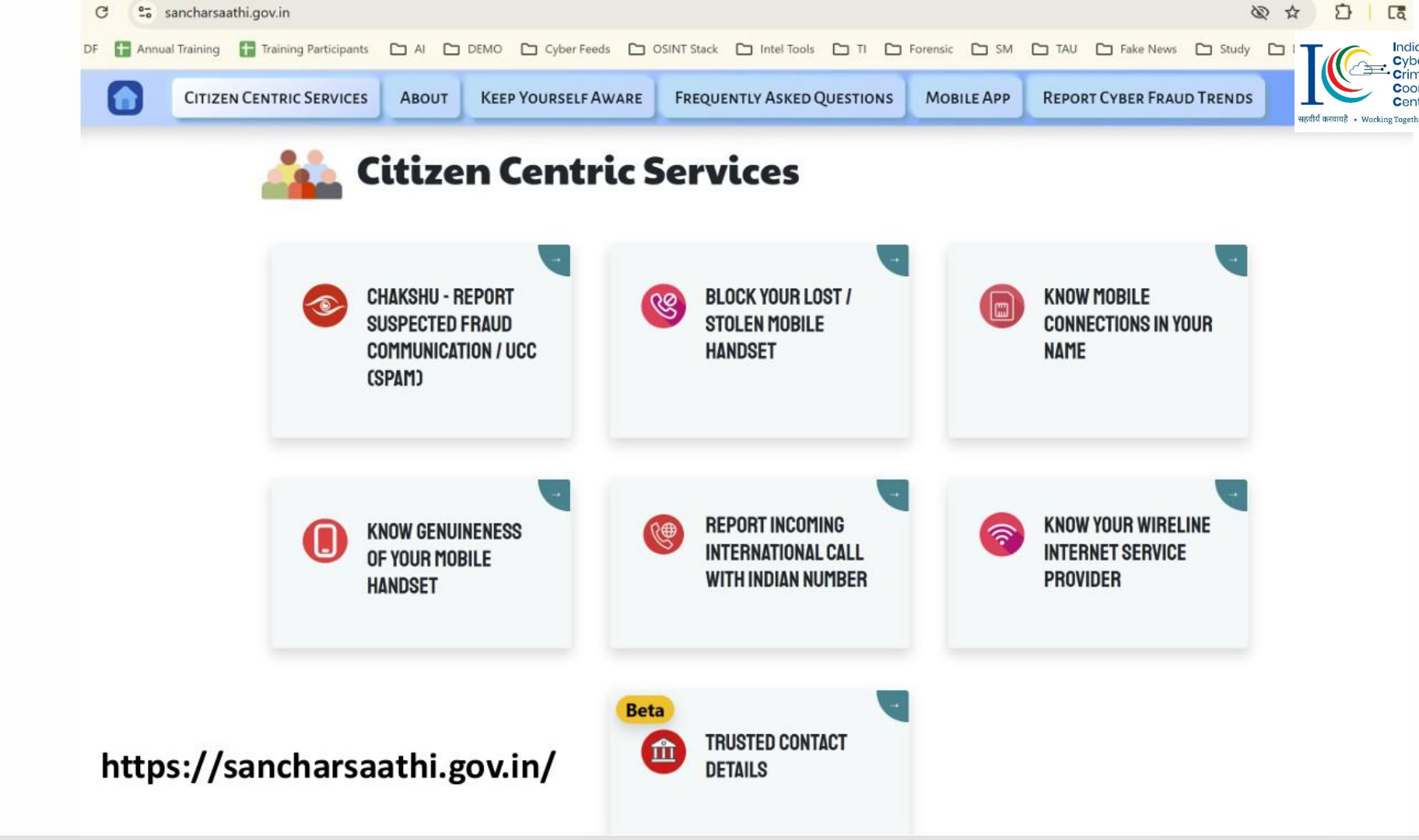
WhatsApp Security

- **Always Enable Two-Step Verification**
- **Settings->Account->Two-step Verification->Enable**
- **Disable Auto-Download Option for Media**



FOR MOBILE SAFETY



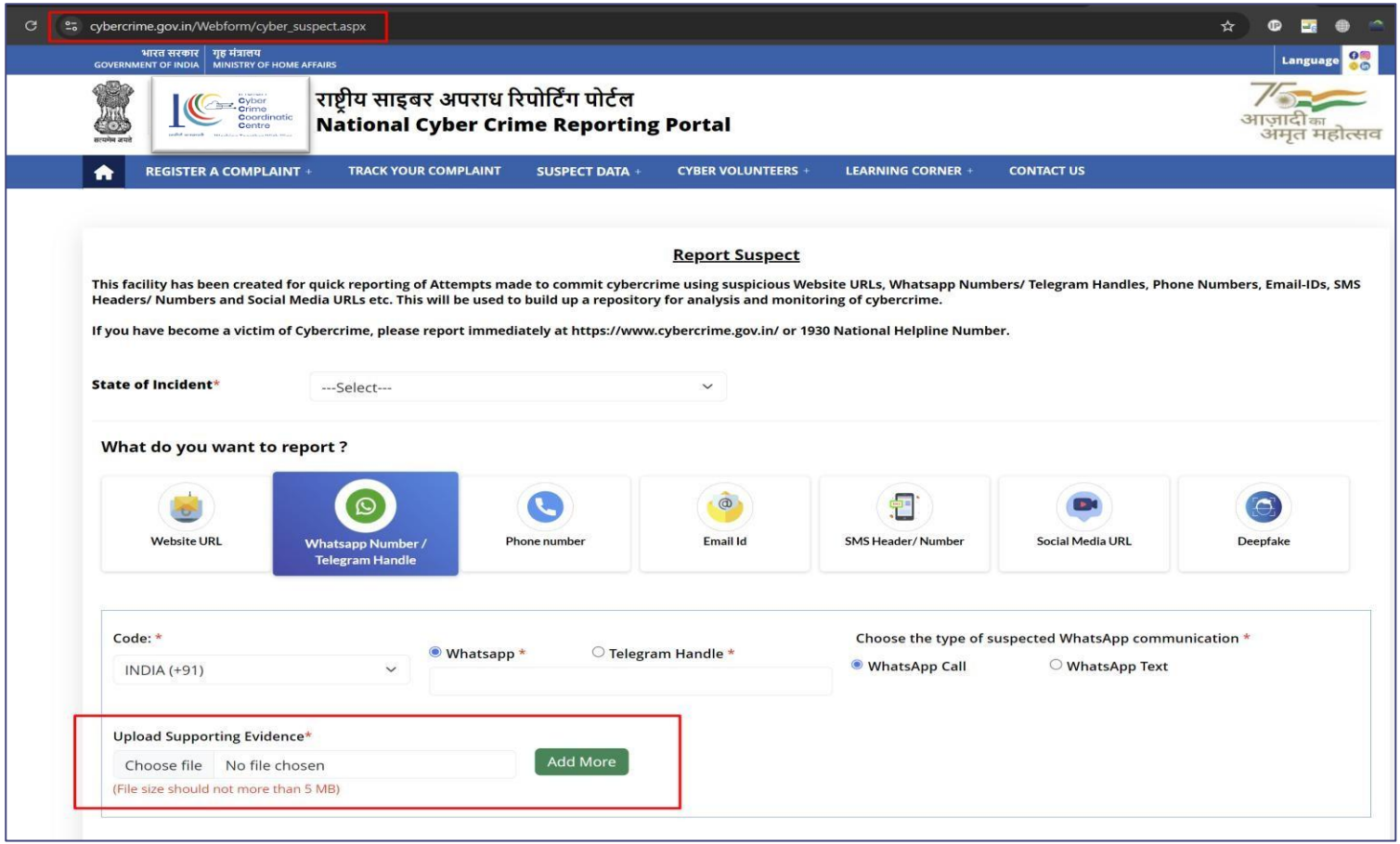

sancharsaathi.gov.in
DF
Annual Training
Training Participants
AI
DEMO
Cyber Feeds
OSINT Stack
Intel Tools
TI
Forensic
SM
TAU
Fake News
Study
CITIZEN CENTRIC SERVICES
ABOUT
KEEP YOURSELF AWARE
FREQUENTLY ASKED QUESTIONS
MOBILE APP
REPORT CYBER FRAUD TRENDS
Indian Cyber Crime Coordination Centre
सहवीर्य करवावहै • Working Together With Vigour
Citizen Centric Services
CHAKSHU - REPORT SUSPECTED FRAUD COMMUNICATION / UCC (SPAM)
BLOCK YOUR LOST / STOLEN MOBILE HANDSET
KNOW MOBILE CONNECTIONS IN YOUR NAME
KNOW GENUINENESS OF YOUR MOBILE HANDSET
REPORT INCOMING INTERNATIONAL CALL WITH INDIAN NUMBER
KNOW YOUR WIRELINE INTERNET SERVICE PROVIDER
Beta
TRUSTED CONTACT DETAILS
https://sancharsaathi.gov.in/

HTTPS://CYBERCRIME.GOV.IN

Step 1: Report Suspect Data online

https://cybercrime.gov.in/

Step 2


cybercrime.gov.in/Webform/cyber_suspect.aspx
भारत सरकार
GOVERNMENT OF INDIA
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
Language
राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal
आज़ादी का अमृत महोत्सव
REGISTER A COMPLAINT
TRACK YOUR COMPLAINT
SUSPECT DATA
CYBER VOLUNTEERS
LEARNING CORNER
CONTACT US
Report Suspect
This facility has been created for quick reporting of Attempts made to commit cybercrime using suspicious 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
Code: *
INDIA (+91)
Whatsapp *
Telegram Handle *
Choose the type of suspected WhatsApp communication *
WhatsApp Call
WhatsApp Text
Upload Supporting Evidence*
Choose file
No file chosen
Add More
(File size should not more than 5 MB)

learning.cte-i4c.live

FOLLOW CYBERDOST

Handle on TWITTER

अधिक जानकारी के लिए **CYBERDOST** को पर फॉलो करें

THANKS

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