



CYBER CENTRE OF EXCELLENCE

Gujarat Police

SOCIAL MEDIA ABUSE

The Hidden Harm in Plain Sight

⚠ *Recognise it. Report it. Stop it.*

A Public Awareness Guide

Cyber Crime Helpline: **1930** | cybercrime.gov.in



What Is Social Media Abuse?

Social media abuse is any deliberate act on platforms like Instagram, Facebook, X (Twitter), WhatsApp, Snapchat, YouTube, or Telegram that is intended to harass, threaten, humiliate, defame, deceive, or harm another person. It includes cyberbullying, online stalking, doxxing, impersonation, hate speech, sextortion, revenge content, deepfakes, and targeted trolling.

Unlike everyday disagreement, abuse is **persistent, targeted, and harmful**. It can come from strangers, anonymous accounts, ex-partners, or even people in the victim's own circle. The damage is real — psychological distress, reputational injury, financial loss, and in severe cases, self-harm.

The single most important fact:

Online abuse is a **crime under Indian law** — covered by the Bharatiya Nyaya Sanhita (BNS), the Information Technology Act, 2000, and the POCSO Act for minors. Anonymity does not protect abusers; IP logs, account data, and platform records can and do lead to identification and prosecution. You have the right to be safe online.

The Scale of the Problem

1 in 3

Indian internet users report facing some form of online abuse or harassment

8,000+

Cyberstalking and online harassment cases against women (NCRB, 2022)

24x7

1930 Cyber Helpline and cybercrime.gov.in available to report online abuse

Women, teenagers, journalists, activists, and members of religious or caste minorities are disproportionately targeted. So are senior citizens new to social platforms. Children face particular risk through gaming chats, messaging apps, and image-sharing platforms. Awareness — at home, in schools, and at work — is the single strongest protection.



Common Forms of Online Abuse

Abuse on social media takes many shapes. Recognising the specific form helps you respond correctly — both in protecting yourself and in reporting accurately.

1**Cyberbullying & Trolling**

Repeated insults, mockery, body-shaming, pile-ons in comments or DMs. Often coordinated by groups. Common against teenagers, women, and public figures. Punishable under BNS provisions on intimidation and the IT Act.

2**Doxxing — Sharing Private Information**

Publishing someone's address, phone number, workplace, family details, or identity documents without consent. Intended to invite harassment or physical danger. A serious offence regardless of where the information was originally obtained.

3**Impersonation & Profile Cloning**

Fake accounts using your photo and name to defraud friends, post offensive content, or damage your reputation. Often used in matrimonial scams and to send phishing links to your contacts.

4**Sextortion & Intimate Image Abuse**

Threatening to share private or intimate images unless money, more images, or favours are provided. Includes "revenge porn" by ex-partners and AI-generated nude deepfakes. Punishable under multiple sections; reporting brings swift action.

5**Cyberstalking**

Persistent unwanted contact, monitoring of your accounts, creation of multiple profiles to follow you after being blocked, or showing up at locations gleaned from your posts. A criminal offence under Indian law.

6**Hate Speech & Threats**

Communal slurs, caste-based abuse, threats of violence, rape threats, or content inciting hatred against an identifiable group. Such content can be reported both to platforms and directly to police.

7**Deepfakes & AI-Generated Abuse**

Synthetic videos, voice clones, or morphed images placing a victim in fake situations — often sexualised or politically inflammatory. A fast-growing threat in 2026; report immediately to platform and police.



Red Flags: How to Spot Abuse

The earlier you recognise abuse, the easier it is to contain. If even one of these signs appears, take it seriously. If two or more appear, treat it as a clear abuse pattern and begin documenting.

- ✗ Repeated messages, comments, or DMs from a stranger after you have ignored or blocked them.
- ✗ A new account appears with **your photo and name** contacting your friends or family.
- ✗ A sudden wave of insulting comments from many accounts at once — coordinated trolling.
- ✗ Someone threatens to **share private photos, chats, or videos** unless you pay or comply.
- ✗ Your private details — address, phone, ID — appear posted publicly without your consent.
- ✗ A morphed or AI-generated image / video showing you in a fake compromising situation surfaces.
- ✗ Messages contain caste-based, communal, gendered, or sexual slurs and threats.
- ✗ You're being pressured to keep an online relationship secret, especially if you are a minor.
- ✗ You feel anxious, sleepless, or afraid to open social media — a clear signal that the situation has crossed a line.

Common Scenarios in 2026

The "Honey Trap" Sextortion

A stranger sends a friend request, video-calls within hours, briefly appears unclothed, then threatens to share a recording of you with your contacts unless paid.

The Cloned Profile

An account with your name and profile photo messages your relatives asking for an urgent loan — they believe it is you. Money is sent to a stranger's UPI.

The Coordinated Pile-On

A post is screenshotted out of context and shared on a hostile page. Hundreds of comments arrive within hours — slurs, threats, even calls and visits to your workplace.

The Deepfake Smear

A morphed video showing the victim "saying" something they never said circulates on WhatsApp and Telegram, damaging reputation before truth can catch up.



What To Do If You're Being Abused

Abuse online thrives on shame and silence. Breaking the silence — to a trusted person, to the platform, and to the police — is the single most effective response. Follow these steps in order.

✓ DO THIS

- **Don't reply or argue.** Engagement is what trolls and abusers want. Silence and reporting work better than any comeback.
- **Take screenshots** of every abusive message, comment, profile, URL, username, and date/time. Save chat exports where possible. This is your evidence.
- **Block and restrict** the account — but only **after** you have captured evidence. On Instagram, "Restrict" is often more useful than block as it hides activity without alerting them.
- **Report on the platform.** Every major app has a "Report" option (see Page 6). Use it for every abusive piece of content separately.
- **Tell someone you trust** — a parent, partner, friend, teacher, or HR. Isolation is the abuser's biggest ally.
- **File a complaint at cybercrime.gov.in** and call **1930**, especially if there are threats, sextortion, doxxing, or impersonation involved.
- **Visit your local cyber police station** with printouts of evidence and request an FIR for serious offences.
- **Look after your mental health.** Speak to a counsellor or call the iCall helpline (9152987821). Abuse takes a toll — support is available.

✗ NEVER DO THIS

- **Never pay a sextortionist.** Payment never ends the threat; it confirms you are a paying target and leads to escalating demands.
- **Never delete evidence in panic.** Even abusive content is the proof you need. Capture first, then report or block.
- **Never share your OTP, password, or "verification" code** with anyone, no matter how the situation is framed.
- **Never confront the abuser offline** alone, especially if threats have been issued. Involve police instead.
- **Never blame yourself** for receiving abuse. Sending an image to someone you trusted is not consent for it to be shared further.
- **Never keep it secret** if you are a minor being approached, befriended, or pressured by an adult online. Tell a parent or trusted adult immediately.
- **Never click suspicious links** in DMs offering to "remove" content, "verify" your account, or check if your photos are leaked. These are phishing traps.

Remember: Anonymity is not invisibility. Indian police cyber cells routinely trace IP addresses, mobile numbers, and bank accounts behind anonymous abuse. Reporting works — but only if you actually report.



How to Report — Step by Step

CYBER CRIME HELPLINE

1930

Toll-free | 24x7 | All India

Operated by the Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, Government of India

The Reporting Process

1**Capture evidence first**

Screenshot the abusive content, the offender's profile (full URL visible), and any chats. Save the date, time, and platform. Note the username exactly as it appears.

2**Report on the platform**

Use the in-app "Report" option for the specific content type (harassment, impersonation, intimate image, threat, hate speech, fraud). Platform takedown is usually the fastest first relief.

3**Call 1930 or file at cybercrime.gov.in**

For serious offences — sextortion, threats, doxxing, deepfakes, stalking, financial fraud — file a formal complaint. Upload screenshots, URLs, and bank transaction details if money was sent.

4**Bank action — the golden hour**

If money was paid (e.g. sextortion, scam impersonation), reporting within ~60 minutes lets banks freeze the receiving account through the Citizen Financial Cyber Fraud Reporting system.

5**Visit your local cyber police station**

Carry printouts of the complaint, all screenshots, bank statements (if any), and a valid ID. Request an FIR. Follow up using your complaint number. For intimate-image cases, you can request a woman officer.

Special note for minors

If the victim is below 18, the case falls under the **POCSO Act** in addition to the IT Act and BNS. Take-down is faster and penalties are much heavier. Parents or guardians can file the complaint on the child's behalf — and should.



Reporting on Each Platform

Every major platform has built-in reporting tools and a Grievance Officer in India under the IT Rules, 2021. Use the in-app option first; if there is no response within 15 days, escalate to the platform's Grievance Officer and to cybercrime.gov.in.

Platform	How to Report Abuse
Instagram	Tap the three dots on the post / profile → Report → choose reason (harassment, impersonation, nudity, hate speech). For DMs, long-press the message.
Facebook	Three dots on post / profile → Find support or report . For Messenger threats, tap the name → Report .
X (Twitter)	Three dots on the tweet / profile → Report → choose abuse, threat, or impersonation. Use "Block" plus "Mute" together.
WhatsApp	Open the chat → tap the contact name → scroll down → Report contact . Also lets you block in the same step.
YouTube	Three dots under video / comment → Report . For channels: About tab → flag icon.
Snapchat	Press and hold the snap / chat → Report . Includes options for sexual content involving minors and threats.
Telegram	Long-press the message → Report . For groups / channels: tap title → three dots → Report .
LinkedIn	Three dots on the post / message → Report this . Strong action on professional harassment and fake recruiter accounts.

Removing Intimate Images

If non-consensual intimate images of you (or AI-generated nude deepfakes) are circulating, you have additional fast-track options:

Service	Use
StopNCII.org	Creates a hash of your image on your device (the image is not uploaded) and shares it with partner platforms to block uploads. Free.
Take It Down (NCMEC)	For images taken when the victim was a minor — works similarly across major platforms.
cybercrime.gov.in	Dedicated " Report Women / Child related Crime " category — option to remain anonymous.



Family & Personal Safety Checklist

Most abuse cases become serious because of small habits — open profiles, reused passwords, screenshots casually shared. Walk through this checklist with every family member, especially children and senior citizens.

- ☐ Set every social media account to **private** by default. Review followers and friend lists once a month.
- ☐ Use **two-factor authentication** on every social account, email, and UPI app. SMS OTP at minimum, an authenticator app where possible.
- ☐ Never share **intimate images or videos** — even with a trusted partner. Devices get lost, stolen, or hacked; relationships change.
- ☐ Avoid posting **real-time location**, home address visuals, children's school uniforms, or daily routines on public profiles.
- ☐ Teach children: **any adult asking them to keep an online chat secret is a warning sign**. They should tell a parent or trusted adult immediately.
- ☐ Use a different, strong password for each social account. A password manager makes this practical.
- ☐ Once a month, search your own name and photos online — early detection of impersonation accounts matters.
- ☐ Agree as a family: **screenshots before reactions**. Capture evidence first, then block / report.
- ☐ Discuss recent online-abuse news at home periodically — awareness fades; refresh it.

Real Cases Reported in India

Pune — college student, sextortion (2024)

A 19-year-old was contacted on Instagram, drawn into a brief video call where the caller appeared unclothed, and was then threatened with circulation of a recording to family. She reported on 1930 within hours; police traced the account and froze the receiving UPI before any money moved.

Ahmedabad — impersonation & loan scam

A cloned Facebook profile of a businessman messaged his relatives requesting urgent loans for a "medical emergency". ₹3.4 lakh was sent before the family verified. Cyber Crime froze the mule account; partial recovery was made within 48 hours.

Bengaluru — deepfake of a teacher

A morphed video of a school teacher was circulated on WhatsApp groups by a former student. Following her complaint at cybercrime.gov.in, the originating account was traced, the content was taken down across platforms, and the accused was charged under the IT Act and BNS.



Important Contacts & Resources

Service	Contact
National Cyber Crime Helpline	1930 (24x7, toll-free)
National Cyber Crime Reporting Portal	cybercrime.gov.in
Police Emergency	112
Women Helpline	1091
Child Helpline (CHILDLINE)	1098
Senior Citizen Helpline	14567
iCall Mental Health Helpline (TISS)	9152987821
Report SIM / spoofed-call fraud (DoT)	sancharsaathi.gov.in
Remove intimate images (StopNCII)	stopncii.org
CERT-In (incident reporting)	incident@cert-in.org.in

Five Things to Remember

1**Online abuse is a real crime.**

It is punishable under the BNS, the IT Act, and the POCSO Act. Your report matters.

2**Screenshot before you block.**

Evidence is everything. Capture username, URL, date, and content before you take any other action.

3**Silence is the abuser's tool.**

Tell a trusted person. Sextortionists and trolls depend on the victim's shame to keep paying or to stay quiet.

4**Never pay a sextortionist.**

Payment never ends the threat. It marks you as a paying target. Report instead.

5**Awareness protects everyone — share it.**

Talk to your children, parents, and colleagues. One conversation can prevent a life-altering trauma.

If you remember only one number from this guide, make it 1930.

If you remember only one website, make it **cybercrime.gov.in**.

If you remember only one rule, make it: **screenshot, report, tell someone.**