![Maharashtra Cyber logo]

ONLINE SEXTORTION SCAM

FROM TRAP TO TRAUMA

CCCMH_CA_2025_15

PUBLIC ADVISORY

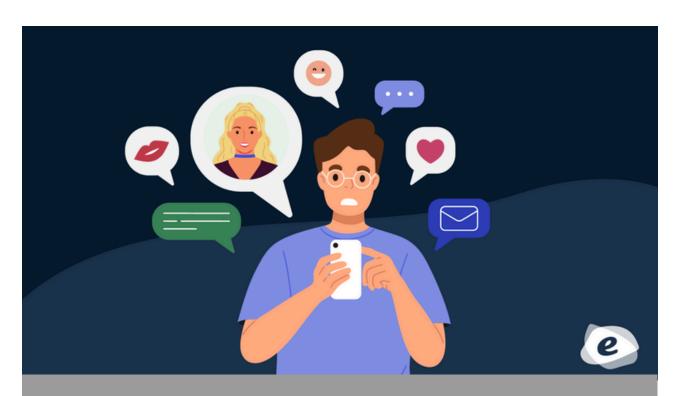# INDEX

PUBLIC ADVISORY

⊕→ **Executive Summary**

Online sextortion is a rising cybercrime where victims are tricked or coerced into sharing intimate content, which is later used to extort money or favors. These scams often begin with fake online friendships or flirtatious chats and escalate into emotional manipulation and threats. Victims can suffer not only financial loss but also emotional trauma, shame, and even social withdrawal.

Sextortion is sexual extortion using images, videos, or conversations as leverage. It often begins with a friendly or romantic approach online, followed by a request for explicit content. Once received, the scammer threatens to leak it publicly unless the victim pays money or sends more content. Scammers often operate across platforms, using fake profiles and emotional manipulation to gain trust

PUBLIC ADVISORY
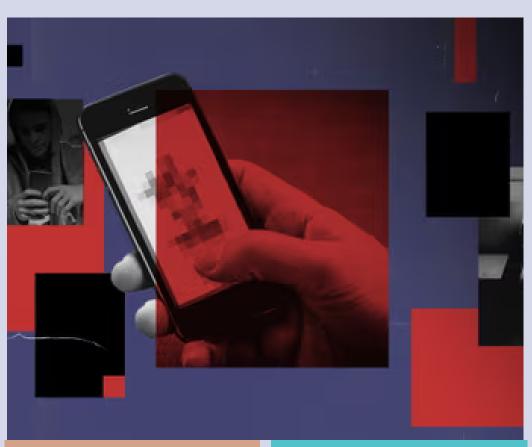
→ **Introduction**

The Rise of Sextortion in the Digital World

Sextortion is a growing cyber threat exploiting deception, fear, and emotional manipulation. Unlike financial scams, it targets victims' dignity and mental well-being. As online interactions increase, so does the risk. Awareness, recognition, and swift response are key to digital safety. Let me know if you need further refinements!

What Is Sextortion?

- Gain intimate content through trickery, emotional manipulation, or hacking.
- Threaten to expose the content to family, friends, or the public.
- Demand money, more explicit content, or silence.
- Exploit the victim's fear, guilt, and social pressure to maintain control.

MAHARASHTRA CYBER

→ How Sextortion Happens

Friendly Approach
Initiated via social media, dating apps, gaming chats.

Blackmail Begins
Threats to leak content unless demands are met.

Fake Identity
Posing as attractive individuals, influencers, or mutual friends.

Trauma Phase:
Threats continue post-payment, causing severe emotional distress.

Flirtation & Requests
Victim is lured into sharing personal or intimate images/videos.

Escalation & Control
Scammers escalate demands, worsening victim distress.

⊕ **Consequences**

✋ **For Victims**

- Anxiety, depression, and psychological trauma
- Guilt, shame, and loss of self-esteem
- Financial losses and privacy violations
- Suicidal thoughts in extreme cases
- Fear of judgment leads to withdrawal from relationships.
- Ongoing distress affecting future interactions and trust.

👫 **For Society**

- Increased cybercrime rates
- Public fear of online interactions
- Strain on mental health and law enforcement resources
- Reduced trust in social media platforms.
- Increased costs for law enforcement, mental health services, and cybersecurity measures.
- Difficulty in tracking offenders due to cross-border cybercrimes.

PUBLIC ADVISORY

→ Targets & Warning Signs

Who Is Being Targeted?

- Teenagers & Students – Targeted via social apps and games.
- Young Professionals – Exploited through LinkedIn, dating apps, WhatsApp.
- Homemakers – Lured with fake social media opportunities.
- Crypto Traders – Tricked via fraudulent trading apps.
- Influencers – Exploited with fake collaborations.
- Senior Citizens – Manipulated through scams and false tech support.

Red Flags

- Sudden messages from unknown people wanting to chat privately
- Push to switch to encrypted apps like WhatsApp or Telegram.
- Urgent or repeated requests for images or video calls
- Threatening language demanding payment in crypto, wallets, or gift cards

→ Prevention & Response

How to Stay Safe

- Never share personal or intimate content with strangers
- Enable strict privacy settings on all social platforms
- Avoid engaging in flirtatious online chats with unknown persons
- Cover webcams when not in use
- Educate youth about consent and digital safety

If You Are Targeted

- Do NOT pay – it rarely stops the threats
- Stop communication immediately and block the perpetrator
- Take screenshots and preserve evidence
- Report at: https://www.cybercrime.gov.in
- Inform the local police or cyber cell
- Seek mental health support and talk to someone you trust

⊕ Recent Incidents

A Pune youth repaid loan but faced extortion threats from fake loan agents. They circulated morphed nude images of his female relative, causing severe emotional distress.

A Maharashtra cyber analyst immediately notified the local police, intervening in time to prevent his suicide.

In Pimpri-Chinchwad, a man was blackmailed with morphed nude images and threatened with public circulation for ₹51 lakh. Tragically, he took his own life

A case was filed, and six individuals were arrested, including call-center operators based in Kolkata.

A 64-year-old man was trapped in a video chat scam and coerced into disrobing. Posing as cyber police, scammers demanded ₹4.6 lakh to delete the footage.

Immediate action by Maharashtra cyber cell helped the victim report the crime, enabling swift intervention.

⊕ References

▶ **PUNE TIMES MIRROR**
https://punemirror.com/pune/crime/pune-techie-loses-rs-7-lakh-to-cyber-fraudsters-in-sextortion-case/cid1687425485.htm?utm_source=chatgpt.com

▶ **PUNE TIMES MIRROR**
https://www.telegraphindia.com/india/fake-cyber-cell-email-used-to-freeze-bank-accounts-case-registered-in-navi-mumbai/cid/2097760

▶ **THE WEEK**
https://www.theweek.in/wire-updates/national/2025/01/13/bes30-mh-cyber-suicide-counsel.html?utm_source=chatgpt.com

▶ **THE WEEK**
https://www.theweek.in/wire-updates/national/2025/01/13/bes30-mh-cyber-suicide-counsel.html?utm_source=chatgpt.com

▶ **THE INDIAN EXPRESS**
https://indianexpress.com/article/cities/mumbai/cyber-sextortion-video-call-facebook-friend-mumbai-software-programmer-loss-9533429/?utm_source=chatgpt.com

▶ **HINDUSTAN TIMES**
https://www.hindustantimes.com/cities/mumbai-news/mahim-programmer-loses-21-lakh-in-sextortion-scam-101724647832200.html?utm_source=chatgpt.com

▶ **PUNE TIMES MIRROR**
https://punemirror.com/PCMC/pimpri-chinchwad-youth-kills-self-due-to-sextortion/cid1717473823.htm?utm_source=chatgpt.com

Call 1945

mhcyber.gov.in