

Sextortion –

Understanding, Preventing, and Responding to Digital Blackmail



1

What Is Sextortion?

Sextortion is illegal. It is a form of cybercrime where someone threatens to share private, sensitive, or sexually explicit images/videos of you unless you meet their demands.

Fact:

- A current trend in sextortion is targeting boys aged 14 to 17.
- Adult predators, masquerading as young girls, express romantic interest in these boys through gaming platforms, apps, and social media sites.
- In 2024, NCMEC received more than **546,000** reports concerning online enticement - a **192%** increase vs 2023.
- **36+** teenage boys have taken their lives as a result of being victimized by financial sextortion



2 Types of sextortion

The common types of sextortion include:

- **Relational sextortion** - often a romantic partner, friend or family member who uses intimate images to control or manipulate the victim
- **Exploitative content sextortion** - the victim is demanded to share more intimate photos, videos or other materials
- **Financial sextortion** - the perpetrator demands money to prevent images from being shared
- **Sadistic sextortion** - recently on the rise, demands include suffering or submission through violence , self-harm and/or destruction





Statistics and Reporting (NCMEC)

20.5M

In 2024, the CyberTipline received 20.5 million reports of suspected child sexual exploitation

546,000

In 2024, there were 546K reports of online enticement, a **192% increase** from 2023.

62.9M

In 2024, 62.9 million files (including images, videos, and other types) reported in connection with child sexual exploitation.

67,000

In 2024, NCMEC's CyberTipline reported a **1,325% increase** in cases involving Generative AI, rising from 4,700 to 67,000 reports.

- *The 2024 NCMEC CyberTipline data highlights a complex shift in the digital landscape.*
- *While total number of reports decreased, the data shows that the most severe and emerging threats—specifically sextortion and AI exploitation—are actually surging*





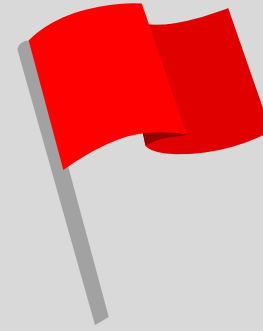
How It Starts : The Tactics

Phase	What Happens
The “Approach”	A stranger follows you on social media or a gaming app. They often use a "catfish" profile (using someone else's photos).
The “Lure”	They quickly move the conversation to a private app (like WhatsApp or Snapchat) and get "flirty" to build trust.
The “Hook”	They send a (usually fake/stolen) explicit photo and pressure you to send one back.
The “Threat”	As soon as they have your explicit photo, the "kind stranger" disappears. Their new friend threatens to expose them by publicizing the photos — unless they pose for more explicit photos or send money.



5

RED FLAGS



- **Rapid Progression:** Someone moving a conversation to an encrypted platform quickly or asking for sexual images too soon.
- **Too-Good-To-Be-True Offers:** Offers of money, gaming credits, or gifts in exchange for photos.
- **Manipulation:** The reciprocation trick, where the offender sends a fake or stolen intimate image of themselves to persuade the victim to send a real one.
- **Use of AI:** Perpetrators may use Artificial Intelligence to create fake nudes (deepfakes) to blackmail victims



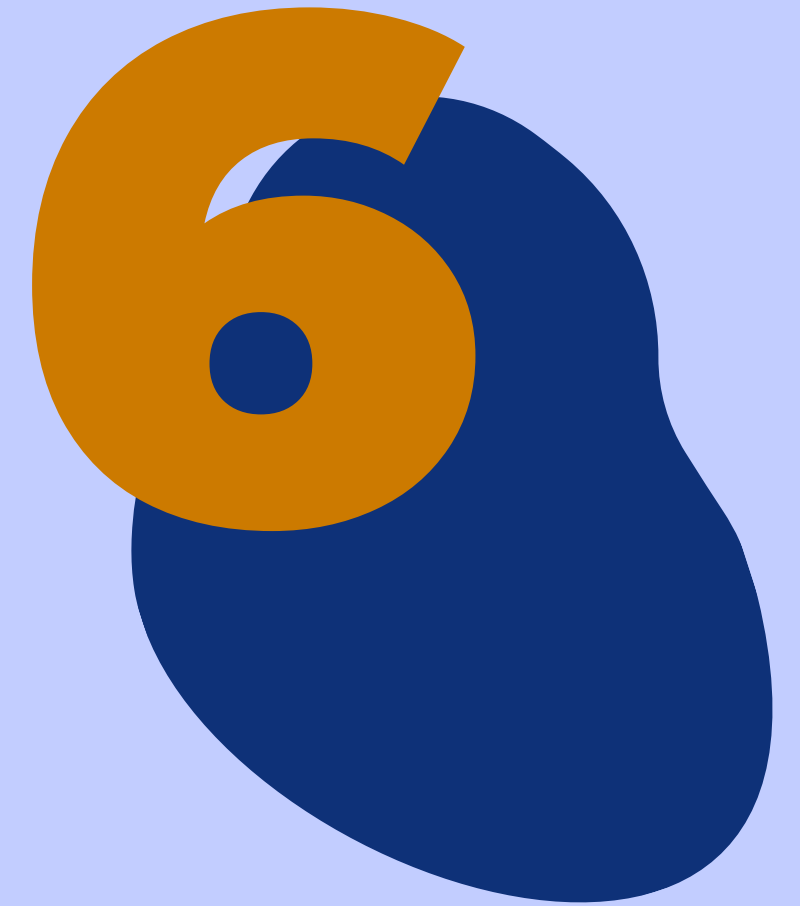
The Perpetrator & Demands

- **Demands:** Often involve requests for money, gift cards, or additional sexual content.
- **The Perpetrators:** Often use fake social media or “catfishing” profiles to groom victims, pretending to be a peer, friend, or romantic interest.



Fact:

- *Organized syndicates often use automated scripts to target thousands of users simultaneously. They set low ransom demands (\$100–\$500) that are high enough to be profitable but low enough that victims might pay quickly out of fear rather than reporting to authorities*
- *If a victim pays, the perpetrator’s “demand curve” shifts upward—they increase their demands, knowing the victim is willing to pay*



7

Case Study

This case study was taken from a real life conversation between “Nikki”, the perpetrator and the victim. Nikki and the victim met on Instagram and started to chat on Whatsapp.



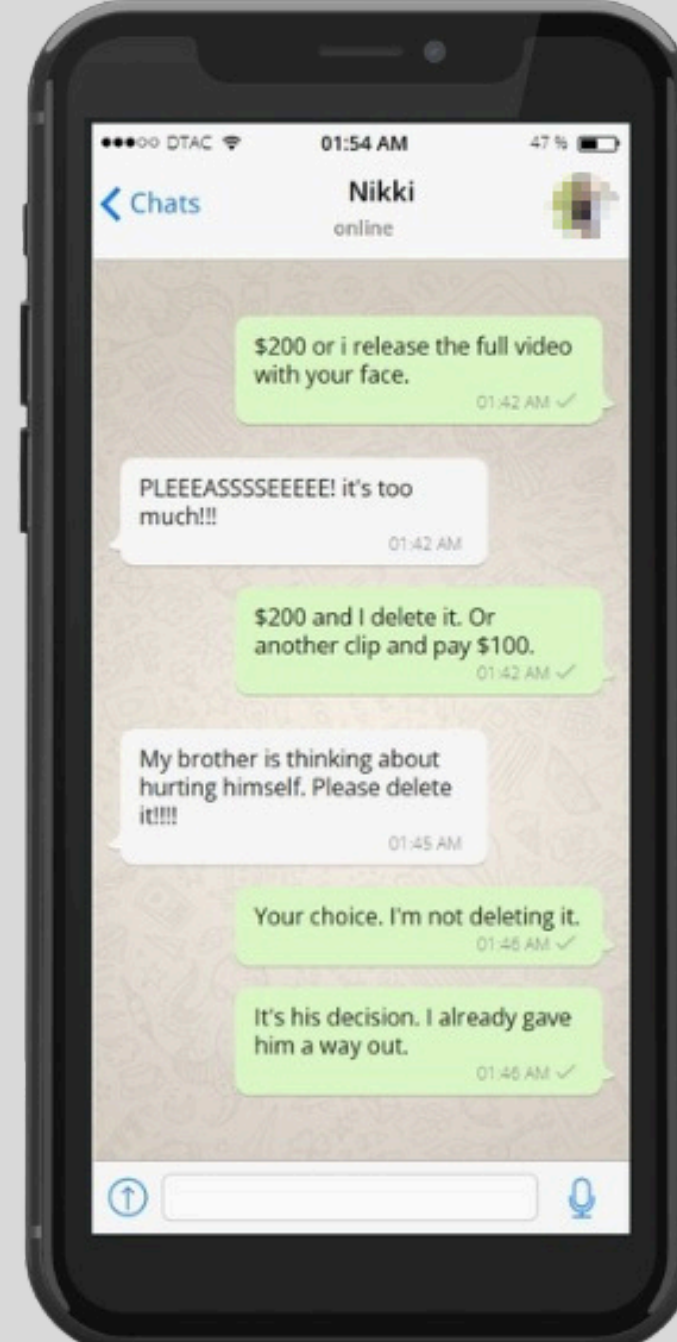
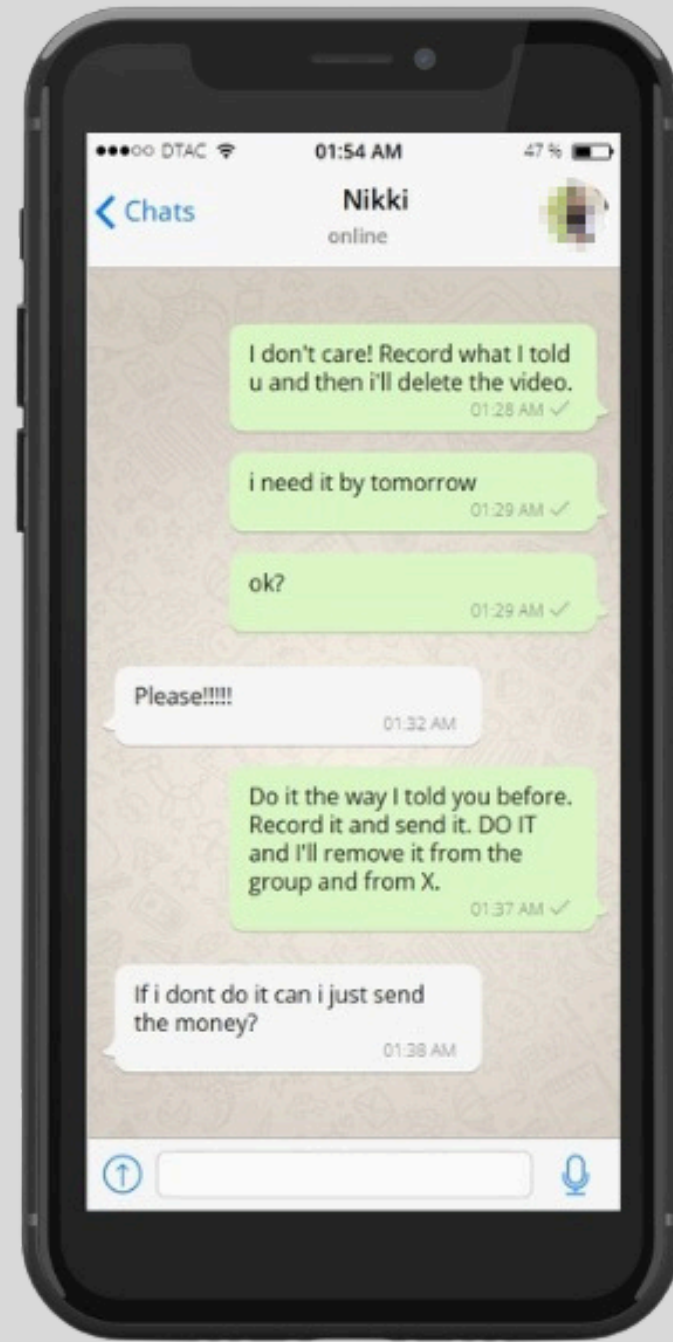
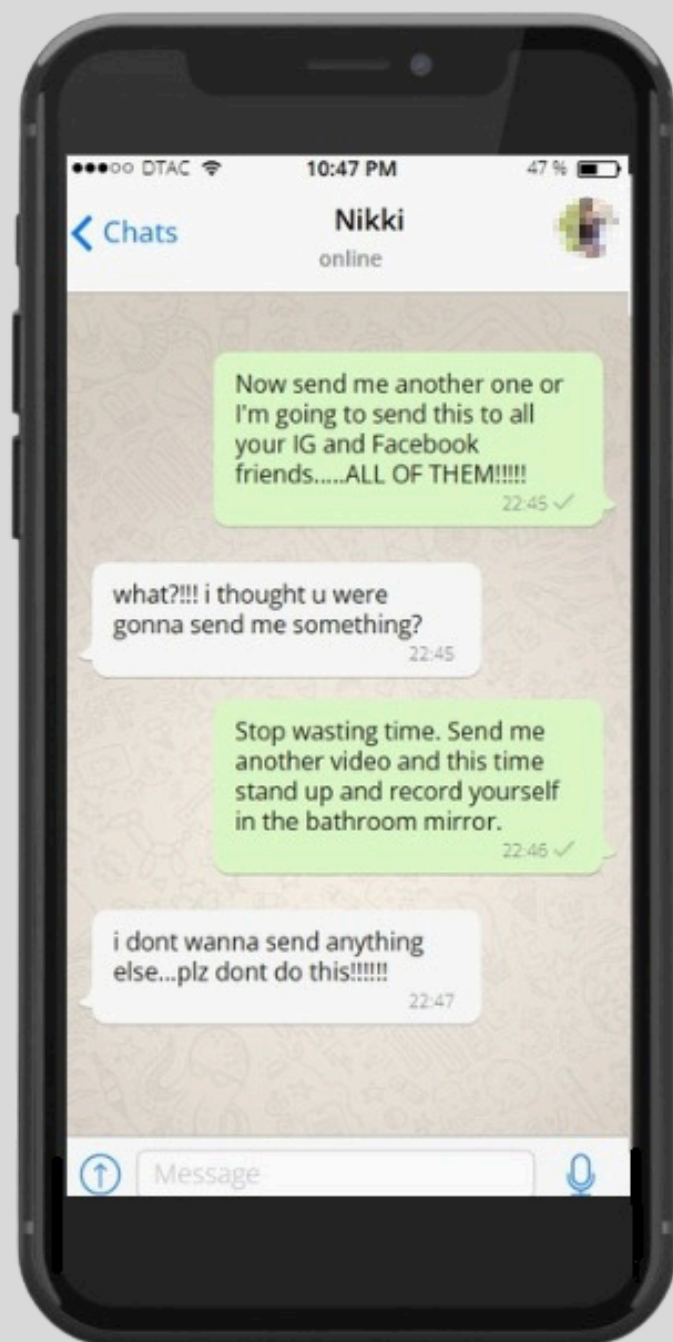
Case Study

- An individual (the perpetrator) masquerading as a female has lured and groomed young boys aged 14 to 17 to record themselves engaging in inappropriate sexual activities.
- Sextortion occurs rapidly, transitioning between various platforms; in this instance, it began on Instagram and shifted to WhatsApp and X.

The conversations in the screenshots are the actual conversations between Nikki and the victim.

All images in the screenshots are generated by AI for illustration.

Case Study Continuation



- The perpetrator later posted previews and advertised the Child Sexual Abuse Material (CSAM) with links to the victims' social media profiles for sale on other platforms and extorted the victims (boys) for money to have the content removed and deleted
- Once the perpetrators have what they need they become ruthless
- Many of the documented suicides related to sextortion occurs **within 24 hours** of the initial threat
- In one high-profile case, the victim committed suicide less than 30 minutes after the exploitation/extortion began

8

What to do if It Happens to You:

If you find yourself in this situation, **do not panic**. Take the following steps:

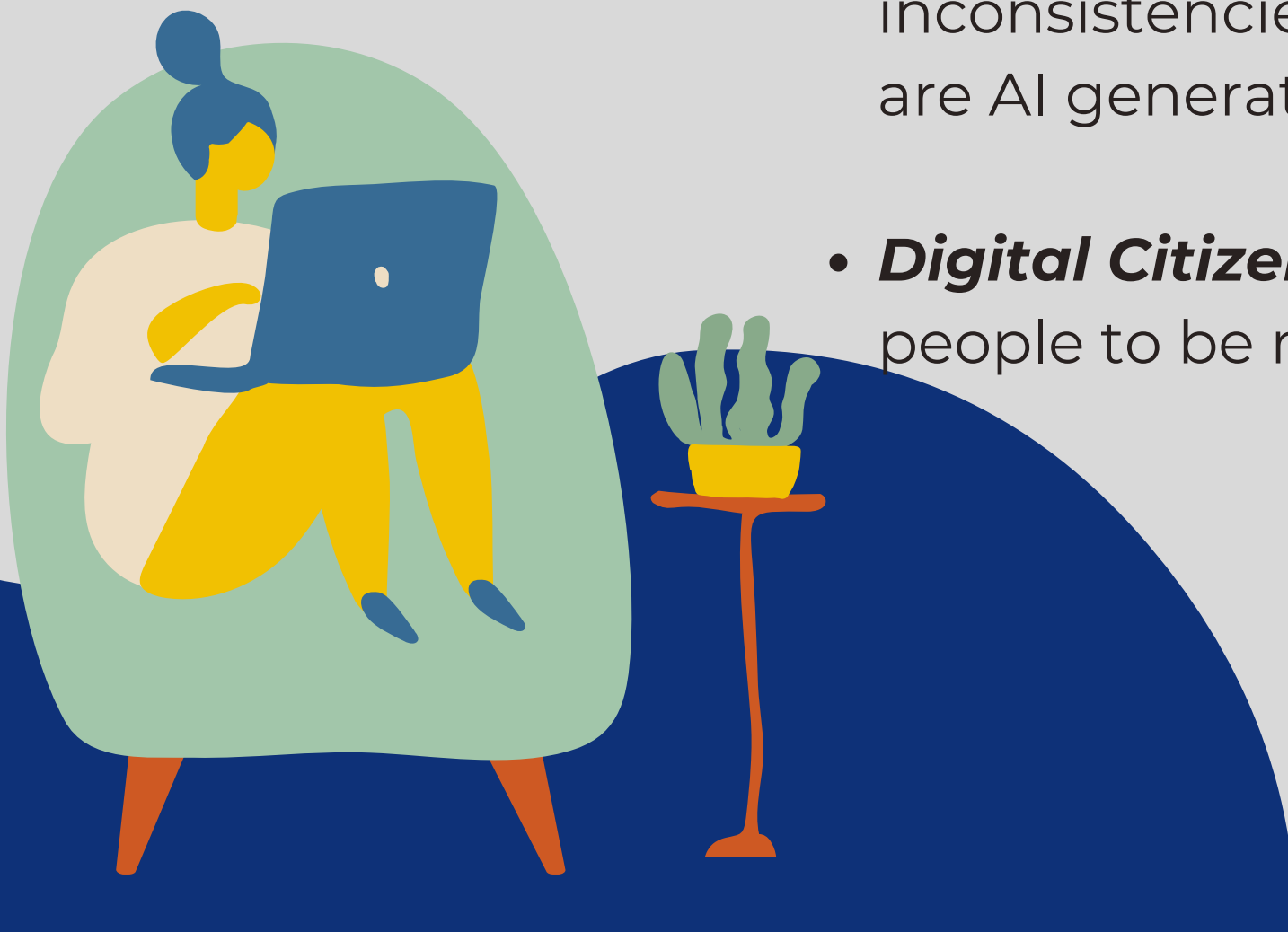
- **Stop All Communication:** Immediately block the extortionist. Do not negotiate, do not plead, and do not send more photos.
- **Do Not Pay:** Paying rarely stops them; it only proves that you have money and are scared, which makes them ask for more. If payment has been made, contact your bank to block and report the transaction.
- **Preserve Evidence:** Take screenshots of the conversation, their profile, and their payment demands. Do not delete the chat until you've captured the info.
- **Tell Someone:** Reach out to a trusted adult, a counselor, or a friend. You should not carry this burden alone.
- **Report:** Contact law enforcement and report the user on the social media platform.





Prevention, Awareness & Safety Habits

- **Privacy Settings:** Keep profiles private on any social media platform
- **Personal Info:** Never share intimate images and personal content online
- **Verifying Identities:** Emphasizing that people online may not be who they claim to be, do a quick search of their names on Google to check for inconsistencies. Use an AI checker to verify if images, videos or even profiles are AI generated.
- **Digital Citizenship:** "If it's too good to be true, it probably is". Reminding people to be more aware and that it is never their fault if they are targeted.



10

Help Available

Here's who you can contact if it happens to you:

- “Take it down” by NCMEC is an international 24/7 call center
- Report to NCMEC at: <https://report.cybertip.org> **OR** call 1-800-THE-LOST (1-800-843-5678)
- Local Law Enforcement
- Local emergency hotline to report on scams



Sextortion

Awareness Quiz



Scenario 1: The “Too Good to Be True”

You've received and accepted a “follow” request on Instagram, and in less than ten minutes, the person:

- *Flirted extensively*
- *Asked to switch to WhatsApp*
- *Suggested a private video call*

What should you do next?

A. Go along—it seems harmless

B. Ask for proof if they're real

C. Continue chatting/messaging but don't share anything

D. Decline and stop engaging, including blocking user

Answer D : Fast escalation is a major red flag. Disengage early.

Scenario 2: The Recorded Video Call

During a video call with someone you befriended online, the person starts behaving in a sexually flirtatious manner by removing their clothes and suggests for you to do the same.

The next day, they send you a recording of the call and threatens to share it.

What should you do next?

A. Apologize and try to reason with them

B. Offer to pay them to delete it

C. Ignore and block immediately

D. Save evidence, stop contact and report

Answer D: Preserve evidence and report. Paying makes it worse.

Scenario 3: The Online Gaming Friend

You meet someone in an online gaming community and after chatting for weeks, they ask you to share a private photo of yourself. Later they say "I am not asking for money, but I want you to do as I say or I'll post this everywhere"

They then begin demanding you to do humiliating acts on camera.

What type of sextortion is this?

A. Financial sextortion

B. Sadistic sextortion

C. Relational sextortion

D. Online scam

Answer B: The perpetrator seeks control, humiliation and psychological harm over financial gain

Scenario 4: The Break-up Threat

After a break up, your former partner sends a message:

"If you don't get back together with me, I'll send your private photos to your coworkers"

What type of sextortion is this?

A. Sadistic sextortion

B. Romance scam

C. Relational sextortion

D. Phishing

Answer C: The threat comes from someone known to the victim. Don't reply emotionally. Gather evidence, stop communication and report.

Scenario 5: The "Last Chance" Threat

After you ignored the perpetrator, they found other ways to message you and they send :

"This is your last chance. I will ruin your life."

What should you do next?

A. Reply to calm them down

B. Send a small amount of money to stall the situation

C. Continue ignoring and report the account

D. Suggest meeting face to face to settle the issue

Answer C : Engagement provides leverage. Silence removes power.

Which of the following is true?

- a. Sextortion is not always about money*
- b. Some perpetrators seek control or humiliation*
- c. Known individuals can also be perpetrators*
- d. Saving evidence and reporting are critical steps*

A. a & c

B. b & c

C. a, b & d

D. a, b, c & d

Answer D