



What do I do if I am a victim of sextortion?

Tell Someone

If you're under 18, tell a trusted adult immediately. If you are over 18, tell someone you can trust who can help you. If you are experiencing a mental health crisis, call or text the 988 Suicide and Crisis Lifeline anytime.

- This could be a parent, school counselor, teacher, or another safe adult.
- You have not done anything wrong and you will NOT get into trouble for reporting that you are a victim of sextortion.
- Adults respond with calm, support, and urgency, not shame or panic.

This could be a life threatening situation. Immediately stop contact with the perpetrator and tell someone. Put your device on airplane mode if needed. Practice a moment of mindfulness grounding yourself in intentionality and the present moment. Then contact a trusted resource. Do not handle this alone.

If you're being harassed, extorted, or threatened, contact local law enforcement immediately and file an IC3 report. If you sent intimate images and are being blackmailed, also report to the National Center for Missing and Exploited Children's CyberTipline at [CyberTipline.org](https://www.cybertipline.org).

If the perpetrator sent messages containing threats of physical violence, sexually explicit materials of minors, or other offensive messages, law enforcement may subpoena Social Media platforms for information on the perpetrator. If social media companies ban an account prior to this subpoena, critical evidence could be lost. Always immediately report any messages to law enforcement that contain the following content prior to reporting the account:

- Threats of violence
- child sexual abuse material (CSAM) or sending sexually explicit messages or photos
- Taking a photo or video of someone in a place where he or she would expect privacy
- Stalking and hate crimes

Sextortion criminal groups like the Yahoo Boys and Black Axe are recognized as transnational organized crime organizations by the DHS and FBI and are being investigated as such. Report sextortion immediately so terrorists like these can be brought to justice. Additionally, follow this guide to ensure evidence can be collected to build national cases against them.

Do NOT Pay

Do NOT pay the perpetrator at all. The perpetrator will not go away if you pay, and will instead ask for more and more money, sometimes setting victims up on a weekly or monthly payment plan, or requiring the victim to perform illegal services on their behalf because they are unable to continue paying or afford the ransom. Illegal activities may include creating accounts for the perpetrator to use to





target additional victims, laundering money, engage in additional scams such as check scams on behalf of the perpetrator, or target others in sextortion scams on behalf of the perpetrator.

Stop the Conversation Immediately

- Do not reply. Do not negotiate. Do not pay.
- Block the person on all platforms.

Gather Evidence

Immediately:

- Gather Evidence
 - Screenshots Aren't Enough
 - Record your screen while scrolling through the messages (especially on Snapchat or IG stories)
 - Save usernames, emails, phone numbers, userIDs, gammertags, timestamps, and context
 - Don't just screenshot, create a timeline of events
 - Use a Second Device
 - Use your phone to record the bullying from a secondary device if the original app doesn't allow saving or notifies the sender
 - Copy all evidence to two external USB drives and/or backup one version to the cloud.
 - Preserve Metadata
 - Export chat logs or files when possible
 - Don't crop screenshots, keep the entire frame intact
 - Apps like Bark or Qustodio can help monitor activity, but they often miss private DMs or "vault" apps. If you're seeing red flags, go straight to manual review.

Report to Law Enforcement

Sextortion is a felony in Ohio and across the U.S. Even if the perpetrator is overseas, law enforcement can help.

Call your local police department (non-emergency number) and ask to file a report with a detective trained in cybercrime or sex crimes.

If you're not sure who to contact:

- Cuyahoga County Sheriff: (216) 443-6000
- Cuyahoga County Sheriff: sheriff.cuyahogacounty.us
- Geauga County Sheriff: (440) 286-1611
- Geauga County Sheriff: co.geauga.oh.us

Report to Federal Agencies

- FBI Internet Crime Complaint Center (IC3)





- Report at: www.ic3.gov
- National Center for Missing & Exploited Children (NCMEC)
 - File a CyberTip: CyberTipline.org
 - You can report anonymously.
 - If you're under 18 and your image is online, NCMEC can help remove it.
- Homeland Security Investigations (HSI) – For child exploitation, sextortion, or trafficking
 - Report anonymously at: ice.gov/tipline
- Secret Service Cleveland Field Office
 - Main federal agency for financial crimes
 - 216-750-2058

Report to the Platform or App

Once law enforcement have given the go ahead, report the perpetrator to the App or Social Media Platform. Most platforms have a Trust & Safety or Report Abuse feature. Report the account that contacted you, even if it's been deleted.

- Instagram: [Help Center](#)
- Snapchat: safety.snapchat.com
- Discord: discord.com/safety
- TikTok: support.tiktok.com
- Youtube/Google/Gmail: support.google.com

Keep all report confirmation numbers or screenshots.

Get Mental Health and Crisis Support

Sextortion is traumatic and isolating, but you're not alone.

In Northeast Ohio:

- Cleveland Rape Crisis Center (CRCC) – 24/7
 - 216-619-6192 or 440-423-2020
 - clevelandrapecrisis.org
 - Offers confidential counseling, advocacy, and support—available to adults, teens, and children.
- Ohio Alliance to End Sexual Violence (OAESV)
 - State Helpline: 1-888-886-8388
 - oaesv.org

Remove Intimate Images If Shared

Several services have been introduced in partnership with NCMEC and Meta to prevent non-consensual imagery from being shared on social media. This includes StopNCII.org (for anyone) and TakeItDown.NCMEC.org (for minors), which hash the photos and block future uploads of the blacklisted photos to social media sites.





Secure Your Accounts

- Review social media privacy settings, limit who can message or tag you.
- Change all passwords immediately.
- Enable multi-factor authentication (MFA).
- Log out of all devices.
- Remove connected apps you don't recognize.

Be Aware of Post-Victimization Recovery Scams

Be aware of post-victimization recovery scams and for-profit entities taking advantage of sextortion victims. There are legitimate and illegitimate businesses targeting sextortion victims.

The FBI warns victims of for-profit firms exploiting sextortion victims by charging high fees for assistance. Unlike law enforcement and non-profit agencies, these companies use deceptive tactics like threats and manipulation to coerce payments. Some services offered, such as cease and desist orders, may provide emotional relief but lack legal enforceability. Additionally, these companies discourage victims from reporting sextortion to law enforcement in their advertisements targeted at victims claiming "the police can't help you."

Furthermore, NCRI has observed coordinated inauthentic activity of accounts promoting illegitimate "sextortion recovery services." These accounts often portray themselves as hackers, cybersecurity experts, or reputation management firms, but are simply another scam fuelling account takeovers.

