



Extortionware

Recovering from Extortionware

Extortionware is when someone threatens to release personal information such as secrets, documents, communications, images, or videos for ransom payment or to force you to do something against your will. This may include demands for money, sexual favors, continued contact, silence, or control over your behavior.

The perpetrator may be:

- A stranger who obtained content through hacking, deception, or impersonation
- Someone you know personally
- A current or former partner
- Someone you trusted online

If you believe there is immediate danger to you or your family, call 911 right away.

If the perpetrator is someone you know and there is a history of domestic abuse, stalking, or coercive control, seek professional guidance and create a safety plan before confronting or blocking them.

Extortionware – Do This First

Stop Engagement Immediately

- Do not respond, argue, negotiate, or comply with demands
- Do not send additional images, money, or information
- Do not threaten the perpetrator

Preserve Evidence

- Take screenshots or screen recordings of:
 - Threats
 - Usernames
 - Profiles
 - Messages
 - Payment demands
- Save:
 - URLs
 - Email addresses
 - Phone numbers





- Platform names
- Dates and times
- Do not edit, crop, or alter files if possible.

Ensure Immediate Safety

- If threats include violence, stalking, or physical harm → Call 911
- If the perpetrator knows your address, workplace, or school → seek law enforcement guidance immediately
- For minors, adult intervention is required immediately

Report the Crime

Report immediately to the following agencies:

- For All Victims
 - FBI Internet Crime Complaint Center (IC3): <https://www.ic3.gov>
 - National Center for Missing & Exploited Children (NCMEC): <https://report.cybertip.org>
 - Call: 1-800-THE-LOST (1-800-843-5678)
 - CISA Incident Reporting Form (for public, private, gov): <https://www.cisa.gov/report>
 - FBI Cleveland Field Office: (216) 522-1400
- For Government Entities in Ohio
 - Ohio Cyber Reserve / Ohio Homeland Security: <https://www.ohio.gov>
 - Statewide Terrorism Analysis & Crime Center (STACC): 1-877-OHS-INTEL (647-4683)
- Legal and Compliance Reporting, If PII, health data, or education records were affected, report to:
 - Ohio Attorney General – Data Breach Reporting: <https://www.ohioattorneygeneral.gov>
 - HIPAA (if applicable): <https://ocrportal.hhs.gov/ocr/breach>
 - FERPA or student privacy contacts (for K-12 or higher ed)

Should I Pay the Ransom?

No. The FBI and CISA strongly discourage paying any ransom. Payment does not guarantee the content won't be shared, many victims are targeted again after complying, compliance often escalates demands, and paying reinforces criminal behavior. Even if the material is shared, support and takedown options still exist.





Recovery – What to Do Next

If you don't feel confident with these steps, ask a trusted IT professional for help.

Report to the Platform

- Report the account and content using the platform's abuse tools
- Request account takedown for extortion or image-based abuse
- Save confirmation emails or report numbers

Seek Victim Support

- 988 Suicide & Crisis Lifeline (24/7, confidential)
 - Call or text 988
- Specialized advocacy organizations can help with:
 - Emotional support
 - Takedown requests
 - Legal next steps
 - Safety planning

Do Not Self-Investigate

- Do not attempt to "track" or expose the perpetrator
- Do not post publicly about the incident
- Allow trained professionals to handle escalation

If the Perpetrator Is Someone You Know

If extortion is coming from:

- A current or former partner
- A family member
- Someone with access to your home, school, or workplace

Do not confront them alone.

Recommended steps:

- Contact law enforcement or a domestic violence advocate
- Create a safety plan first
- Preserve evidence discreetly
- Consider legal protections (restraining orders)





How to Avoid Extortionware

- Never feel pressured to keep online secrets
- Be cautious of sudden intimacy, flattery, or urgency
- Verify identities using a second communication method
- Trust your instincts, discomfort is a warning sign
- Ask for help early, before threats escalate

