



Webcam Blackmail

Recovering from Webcam Blackmail

Webcam blackmail (also called webcam sextortion) occurs when criminals use fake identities to befriend victims online and persuade them to perform sexual acts over a webcam or device camera. These interactions are secretly recorded, and the criminal then threatens to share the video publicly unless the victim pays money or complies with further demands.

In some cases, criminals claim they have hacked your webcam or device and recorded you without your knowledge. These threats may come via:

- Email
- Social media
- Dating platforms
- Messaging or gaming apps

This can happen to anyone, and scammers often exploit whatever they think the person fears losing, often focusing on individuals with:

- Financial resources
- Professional reputations
- Families or public roles
- A belief they have “too much to lose”

If you believe there is an immediate risk to your safety, call 911.

Webmail Blackmail – Do This First

Stop All Communication Immediately

- Do not respond to the blackmailer
- Do not send money, gift cards, cryptocurrency, or images
- Do not attempt to explain, negotiate, or threaten

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.
- Do not store sensitive files in a shared location.

Make sure Immediate Safety

- If threats include violence, stalking, or identifying your location → Call 911
- If the blackmailer claims to already be sharing the content → Report immediately
- If a minor is involved → Immediate reporting is required

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>
 - Use NCMEC for minors or child sexual exploitation. For adult webcam sextortion, use IC3/FBI/local law enforcement and platform reporting; use CISA for cyber incidents.
 - 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 Demand?

No. The FBI and CISA strongly discourage paying any demand. 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 to the platform used
- Change passwords on affected accounts
- Review privacy settings and contact visibility
- Consider temporarily deactivating affected accounts if advised

If the Threat Claims Device Hacking

Many “I hacked your webcam” emails are bluffs, but they should still be taken seriously.

Recommended actions:

- Preserve the message as evidence
- Scan devices using reputable security software
- Cover webcams when not in use
- Seek professional IT or law-enforcement guidance if unsure

Seek Victim Support

- 988 Suicide & Crisis Lifeline (24/7, confidential)
 - If you may hurt yourself or feel unable to stay safe, call or text 988.
- Specialized advocacy organizations can help with:
 - Emotional support
 - Takedown requests
 - Legal next steps
 - Safety planning

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 Webcam Blackmail

- Keep your webcam covered when not in use





This helps with device-privacy worries, but the main protection is avoiding coercive video interactions and securing accounts.

- Be cautious of rapid intimacy or sexual pressure
- Be skeptical of strangers requesting video chats
- Never feel obligated to continue an uncomfortable interaction
- Trust your instincts, discomfort is a warning sign
- Remember: legitimate relationships do not demand secrecy

