

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a sextortion blackmail scam

<https://cyberguardlab.com/blog/sextortion-blackmail-scam>

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.

CYBERGUARDLAB · GUIDE

How to spot a sextortion **BLACKMAIL** blackmail scam

Pay or we leak

Threats to leak intimate images unless you pay.

Crypto / gift cards

Do not pay

Save evidence

Report — stop contact

Paying fuels demands

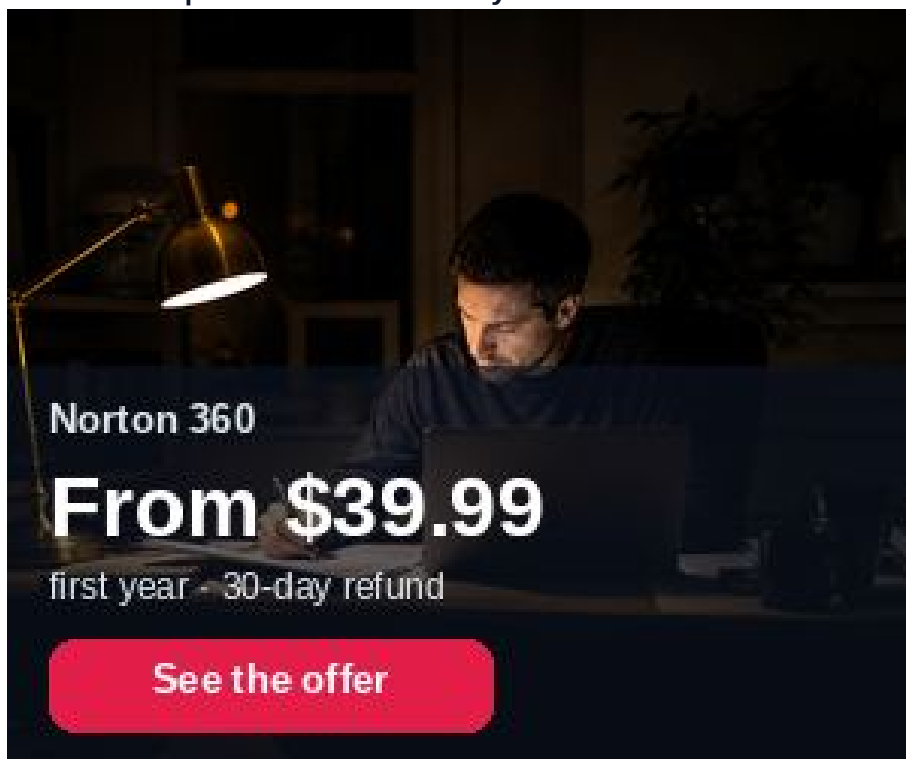
A sextortion blackmail scam threatens to share intimate images, videos, or sexual chat logs unless you pay—often in crypto, gift cards, or wires. Some attackers really captured content; many bluff with old leaks, deepfakes, or nothing at all. Do not pay. Do not send more images "to prove you will cooperate." Stop contact, preserve evidence, and report. If you already paid, still stop—payment rarely ends the demands. This guide is about sexual-image blackmail—not pig butchering trading romance, not military overseas money fees, and not plain catfishing without blackmail.

1. How this scam works

You receive an email, DM, or text claiming the sender has a video of you from a webcam, dating chat, or hacked cloud. They may include a password you once used (from unrelated breaches) to seem credible. Demands arrive with countdown timers and threats to email your contacts. Variants start on Instagram, Snapchat, Discord, or dating apps after a flirty exchange, then switch to payment instructions.

Paid link

Norton 360 | See the Norton first-year offer



[See the Norton first-year offer](https://cyberguardlab.com/norton)

Offer page: <https://cyberguardlab.com/norton>

Some sextortion follows a real private exchange; others are pure bluffs. Either way, paying funds the attacker and often increases demands.

2. Red flags before you pay

3. Safer habits (buy-nothing)

- * Do not pay and do not reply with more intimate content.
- * Stop engaging; take screenshots of threats, usernames, wallets, and URLs.
- * Tighten privacy on social accounts; review tagged photos and friend lists.
- * Change passwords on email and any reused logins; enable two-factor authentication.
- * Report the account on the platform and file at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud); for minors involved, contact appropriate law enforcement immediately.
- * If the lure was a phishing link claiming "your video leaked," compare cues in how to spot a phishing email.

Sextortion targeting students often starts on gaming or social apps. Paying is still the wrong move. Involve a trusted adult and use official reporting-shame is the scammer's tool, not a reason to stay silent.

4. If you already paid

- * Stop further payments-demands usually continue.
- * Document every transaction ID, wallet address, and chat log.
- * Contact your bank, exchange, or gift-card issuer's fraud line right away.
- * Report at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud) and [IC3.gov](https://www.ic3.gov); use [IdentityTheft.gov](https://www.identitytheft.gov) if accounts were compromised.
- * Tell a trusted adult or friend if you feel trapped-isolation helps the scammer.
- * If you typed credentials or opened attachments on a fake page, change passwords, enable two-factor authentication, and scan your device with a trusted tool such as Norton or Bitdefender. Keep one primary real-time antivirus-avoid stacking full

suites. TotalAV, McAfee, and Avast are other on-site comparison options.

FAQ

Will paying make them delete the files?

There is no reliable reason to believe that. Many victims who pay are asked for more.

How is sextortion different from a romance scam?

Romance scams build a fake relationship to extract money over time. Sextortion uses shame and fear of exposure-often quickly-to force payment.

They know one of my old passwords. Does that mean they hacked my camera?

Not necessarily. Passwords appear in unrelated data breaches. Change passwords and enable two-factor authentication; still do not pay.

What if the person in the chat was someone I know?

Accounts get hijacked. Verify through a different channel. Still refuse blackmail payments.

If you still want a paid suite

Avoiding a sextortion blackmail scam does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV ([paid link](#)), Norton ([paid link](#)), Bitdefender ([paid link](#)), McAfee ([paid link](#)), Avast ([paid link](#)).

Sources

- * [FTC ReportFraud](#)
- * [IdentityTheft.gov](#)
- * [FTC: How to protect yourself from sextortion](#)
- * [FBI: Sextortion resources](#)
- * [FBI IC3](#)

Also read

- * [How to spot a catfish profile on a dating app](#)
- * [How to spot a phishing email](#)
- * [How to spot a pig butchering investment romance scam](#)
- * [How to report a scam to the FTC](#)
- * [How to spot a gift card scam](#)