Sexual extortion trends and challenges

- Tech trends position statement

Sexual extortion is a form of blackmail that involves threatening to share an individual's intimate image or video online unless they comply with certain demands. Depending on the situation, the demands are typically for money or cryptocurrency, additional intimate images, meeting for sex or other sexual acts.

The perpetrators often target people through social media, dating apps or emails. Individuals may also be coerced by current or former partners in domestic, family or intimate partner violence situations.

Background

Sexual extortion can sometimes be known as the hybrid word 'sextortion'.

The intimate content used in sexual extortion can be sourced in a number of ways, with or without the consent of the person targeted.

- The perpetrator may establish a fake relationship with the victim, often via social media or a dating site (this is sometimes known as ‘catfishing’). They encourage the victim to send nude photos or join in a sexually explicit video call, then they take screenshots or make a webcam recording.
- The perpetrator may hack into the victim’s photo or video files.
- The perpetrator may digitally alter a photo or video of the victim to make it appear sexual (see **Deepfakes** position statement).
- The perpetrator may claim to have an intimate photo or video of the victim, possibly watching pornography or being sexual with someone under the age of consent, but that is not actually the case.
- The perpetrator may have accessed the photos or videos during a current or previous relationship with their victim.

Once the perpetrator obtains intimate content (either sent voluntarily, under duress, or accessed without consent), they threaten to share it online unless their demands are met. Even if the victim pays, the perpetrator is likely to keep making demands. The perpetrator can also use the intimate content to coerce additional or more explicit photos or videos from the victim, entrapping them even further. It is worth noting that in some cases the perpetrator does not have intimate content at all and is making empty threats.

Sexual extortion can be perpetrated by individuals — usually for financial profit, sexual gratification or, in the case of domestic and family violence, as a way to exercise control over the victim. Sexual extortion is also used by organised crime syndicates to obtain money and/or sexual content that can be sold or bartered.

Sexual extortion can cause serious harm to the victim. Apart from financial loss, the target can be traumatised by fear that the intimate content will made public, even if they meet the demands. The manipulation can make the victim feel ashamed, embarrassed and distrustful. Sometimes, the victim will be forced into making regular payments to prevent the images being posted. This can have a devastating impact on a victim’s mental health, confidence and ability to establish and maintain new relationships, especially if they were deceived as part of a dating scam.

Recent coverage

eSafety often sees an influx of sexual extortion reports following targeted scam email campaigns, which occur sporadically throughout the year. The most recent scam coincided with Australia's nationwide COVID-19 lockdown from March 2020.

In these scams, victims receive an email from a perpetrator claiming to have hacked into their webcam or computer and installed malware to capture intimate footage of them interacting with porn.

In recent years there have been some high-profile examples of sexual extortion.

In early 2020, it was reported that more than 70 South Korean women and girls were victims of a sexual extortion and online sexual abuse ring. Known as the Nth Room case, the abuse was perpetrated using an **encrypted messaging** service. In 2019 Jeff Bezos, Amazon CEO, alleged that an American tabloid newspaper threatened to publish his intimate photos and messages unless he stopped an investigation into the tabloid's reporting practices. Bezos publicly called out the threats, helping to raise awareness of sexual extortion.

Sexual extortion can impact anyone — and transcends culture and socioeconomic status. These cases highlight the nature, scale and types of sexual extortion that can occur.

eSafety approach

Addressing sexual extortion is best achieved through a multipronged approach that involves working with victims, industry and other support agencies.

eSafety's work to address sexual extortion includes:

- raising awareness about sexual extortion and related types of online abuse
- prevention through educational content so Australians can more confidently navigate the online world — this includes education about respectful online relationships, consent, privacy and help seeking
- support for victims who report sexual extortion to eSafety's image-based abuse team, including:
  - alerting social media services to accounts being misused to target victims
  - assisting with removal, if the intimate content is actually shared online
  - referral to police if appropriate
  - referral to external counselling and support services
  - using **Facebook's Non Consensual Intimate Images (NCII) pilot** to proactively block the upload of intimate content if the victim has a copy of the image or video that someone is threatening to share on Facebook
- research into the prevalence, cause and impact of image-based abuse, including sexual extortion
- proactive change through eSafety's **Safety by Design** initiative, which helps industry to embed safety and risk management into their products.

Advice for dealing with sexual extortion

How to help protect yourself against sexual extortion

Sexual extortion is never the victim's fault. Perpetrators exploit victims, prey on vulnerabilities and weaponise technology to cause harm. There are steps you can take to protect yourself against sexual extortion.

- Be aware of the **warning signs**, ways to protect yourself and what to do if sexual extortion happens to you.

- Take care when online dating. Make sure you know how to recognise people who may be untrustworthy, understand how scammers operate and be aware of how your devices work. Remember that online, people are not always who they say they are.
- Check privacy settings on social media accounts, ensuring that you know who can see the content you share and who has access to your images.
- Use secure authentication on all accounts, including two-factor authentication where available.
- Remember to keep your computer or device secure. Make sure your computer has a secure password, up-to-date anti-virus protection and a firewall to prevent someone controlling your webcam or device camera or hacking and accessing your personal details.

What to do if someone is threatening you with sexual extortion

- **Do not pay**, provide more images or videos, or respond to the blackmailer. This may only result in more demands from the blackmailer. (If you have already paid, contact the money transfer site or the bank you used immediately — they may be able to cancel the transfer if you act quickly.)
- **Collect and preserve evidence** of the threats.
- Make an image-based abuse report to eSafety.
- Report to the platform where the threats are occurring — The eSafety Guide provides the relevant links for many popular platforms and services.
- **Block unwanted contact** — The eSafety Guide provides many of these links.
- **If you are concerned about your physical safety** call Triple Zero (000) or contact your local police.
- **Seek further support or assistance** from an expert counselling service.
- **Review and update your privacy and security settings**.

Remember, sexual extortion is not your fault. Anyone can experience it. You are not alone. For more information, read eSafety's advice on responding to sexual extortion.

If you are at risk of immediate harm, call Triple Zero (000).

Published: 4 August 2020

Updated: 5 August 2021