CYBER CIVIL RIGHTS INITIATIVE
Coral Gables, FL
CyberCivilRights.org

CCRI Bulletin: Sextortion Scams

Content Warning

This document reviews sensitive subject matter related to online sexual abuse and financial scams.

What Is Sextortion?

Sextortion (short for “sexual extortion”) occurs when a perpetrator threatens to distribute a nude or sexually explicit photo or video of a person who has not consented to that distribution.

Sometimes the visual material is authentic. Other times, it is inauthentic, manipulated, or completely fabricated visual material, sometimes called “synthetic media” or “deep fakes.”

Sextortion can be committed by a variety of perpetrators (strangers, acquaintances, current or former intimate partners) for a variety of reasons (economic, personal, predatory). This CCRI Bulletin specifically focuses on financial sextortion scams, which have been on the rise in the U.S. and abroad.

How Is Sextortion Perpetrated?

Below are two fictional accounts that describe typical cases. These are only examples of common patterns; sextortion is perpetrated in many different ways and on many different websites and apps.

Fictional Case #1

A met Z on Instagram, a public-facing social media site. Z “liked” A’s profile photo and flirted with A in the comments section for a couple of weeks, and A felt flattered. Z asked A to communicate one-on-one using WhatsApp, a messaging platform with end-to-end encryption. Once on WhatsApp, Z continued flirting with and paying compliments to A. Z then texted a handful of nude selfies and asked A to do the same. A agreed and sent a few nude selfies and a short video. Within minutes, Z sent a text in all caps using demeaning language, threatening to send the images A had just sent to A’s Instagram contacts unless A sent $200 dollars by the end of the day.

Fictional Case #2

B received an email from an unknown sender who claimed to have hacked into B’s cloud storage and found nude images. The unknown sender threatened to post the images of B unless B paid $500 by 8:00 pm that night. B didn’t recall ever taking or storing intimate images but was still frightened by the threat.

Safer Image Sharing

It is important to keep in mind that intimate image sharing always involves some degree of risk. Below are a few tips to enhance your safety if you choose to share intimate images:

- Remain situationally aware. If you meet someone on a website who asks to move your communications to a messaging app, that could be a red flag and a sign to be extra cautious. Similarly, be wary of unknown friend or message requests.

- Most sextortion scammers use fake website profile pictures and content to contact targets (sometimes referred to as “catfishing), and some accounts can be very convincing. It is a good idea to do online research to determine whether a person is who they say they are before agreeing to correspond privately.

- It’s helpful to engage the strongest security settings on all of your technology. If possible, keep your friends or contacts list hidden. This list is often the first thing that perpetrators copy for blackmail purposes.

- When creating an intimate selfie, it is advisable to leave out details that could be used to identify you. Consider excluding your face, tattoos, and scars, as well as any unique furnishings, décor, jewelry, or other personal items. Remember that family members and roommates would likely recognize your wall coverings, bedspread, earrings, and the like.

- Webcams can be used to spy on you without your knowledge. To protect yourself from unwanted surveillance, you can use a piece of paper or masking tape (or a webcam cover) to cover your webcam when not in use.

What Should I Do If This Happens to Me?

- Remember that this is not your fault and you are not alone. Thousands of internet users have been victimized by organized and deceitful sextortion scammers. You are not to blame for someone else’s crime.

- We recommend not sending the perpetrator money, as this usually leads to the perpetrator demanding even more. If you have already sent money, it is best not to send additional funds.

- It’s also a good idea to cease all communication with the perpetrator. Criminal groups are likely grooming hundreds of internet users simultaneously, and they prey on targets who continue to engage with them.

- You may want to take screenshots of all of your communications with the perpetrator in case you ultimately need a record of what took place.

- You can usually report the perpetrator directly to the tech platform and request that their account be taken down. Reporting procedures differ across platforms; some offer in-app reporting and others have a website form. The perpetrator may have multiple accounts using similar handles and profile images, and you may have to report each one. Note that reports will take some time to process, and some sites and apps might not remove the account. While your report is pending, it can help to implement some of the other security steps outlined in this Bulletin.

- After reporting the account, you can then block the perpetrator on all of the websites and messaging apps where you communicated.

- If someone threatened you specifically on Bumble, Facebook, Instagram, or TikTok and you have access to the image(s) in question, StopNCII.org may be able to help you remove or keep some of your images off of these four public-facing platforms.

- It can be difficult to decide whether to stay on, temporarily disable, or delete the website accounts and apps where you were targeted. The best next step is what most matches your own unique circumstances. If you were a minor in any of the images, or if you are an adult intending to file a police report, you may wish to speak with law enforcement prior to deleting any of your accounts or apps. Your open account can be one way to track the perpetrator.

- If you open a new messaging app or open a different social media, gaming, or dating profile, you may want to use a nickname or handle that you have never used before, so that the perpetrator can’t find you elsewhere.

- It is also very important to change your passwords and check that you have activated the highest security settings on your messaging apps and website accounts.

- Sometimes perpetrators do distribute the intimate images. To minimize some of the harm, it could be helpful to alert your contacts with a simple message along the lines of, “Someone online has been threatening me and might communicate with my social media contacts. For your safety, please do not click on or open any suspicious emails or messages, and block unknown senders."

- If the image is disseminated and you are asked for further information by your university, workplace, or family, it may help to print or email this CCRI Bulletin as an explainer.

Who Can Help Me?

- **If you are having thoughts of self-harm:** You may feel very embarrassed or worried. Remember, this is not your fault, and you do not have to go through this alone. Dial "988" to connect directly to the 988 Suicide and Crisis Lifeline.

- **If you are a minor:** If someone created or disseminated an intimate photo or video depicting you when you were under 18 years old (even if you are an adult now)**,** consider contacting law enforcement and/or making a report to The Cyber Tipline at National Center for Missing and Exploited Children (NCMEC) **at https://report.cybertip.org/.** Additionally, consider seeking out a trusted guardian, teacher, school counselor, or therapist to help you navigate next steps.

- **The CCRI Safety Center at https://cybercivilrights.org/ccri-safety-center** offers step-by-step suggestions on various paths you might consider if your intimate image was distributed without your consent.

- **If you are a university student:** You may be able to seek advice from a Title IX Coordinator or other student support offices on your campus.

- **If you are outside the U.S.:** You can search for your country on the CCRI roster of international resources, which can be found here: https://cybercivilrights.org/intl-victim-resources/

- **Other resources could include:** an image monitoring service, law enforcement, or an attorney.

Where Can I Learn More About Sextortion?

- CCRI Safety Center: https://cybercivilrights.org/ccri-safety-center

- The Relationship between Sextortion during COVID-19 and Pre-pandemic Intimate Partner Violence: A Large Study of Victimization among Diverse U.S Men and Women, Victims & Offenders; Asia A. Eaton, Divya Ramjee & Jessica F. Saunders (2022): https://cybercivilrights.org/wp-content/uploads/2022/05/COVID-and-Sextortion-Eaton-2022.pdf

- FBI: https://youtu.be/PMv39d1LJgI or https://www.fbi.gov/video-repository/newss-what-is-sextortion/view