Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

June 5, 2023

Alert Number
I-060523-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes

The FBI is warning the public of malicious actors creating synthetic content (commonly referred to as "deepfakes"[a]) by manipulating benign photographs or videos to target victims. Technology advancements are continuously improving the quality, customizability, and accessibility of artificial intelligence (AI)-enabled content creation. The FBI continues to receive reports from victims, including minor children and non-consenting adults, whose photos or videos were altered into explicit content. The photos or videos are then publicly circulated on social media or pornographic websites, for the purpose of harassing victims or sextortion schemes.

Explicit Content Creation

Malicious actors use content manipulation technologies and services to exploit photos and videos—typically captured from an individual's social media account, open internet, or requested from the victim—into sexually-themed images that appear true-to-life in likeness to a victim, then circulate them on social media, public forums, or pornographic websites. Many victims, which have included minors, are unaware their images were copied, manipulated, and circulated until it was brought to their attention by someone else. The photos are then sent directly to the victims by malicious actors for sextortion or harassment, or until it was self-discovered on the internet. Once circulated, victims can face significant challenges in preventing the continual sharing of the manipulated content or removal from the internet.

Sextortion and Harassment

Sextortion,[b] which may violate several federal criminal statutes, involves coercing victims into providing sexually explicit photos or videos of themselves, then threatening to share them publicly or with the victim's family and friends. The key motivators for this are a desire for more illicit content, financial gain, or to bully and harass others. Malicious actors have

used manipulated photos or videos with the purpose of extorting victims for ransom or to gain compliance for other demands (e.g., sending nude photos).

As of April 2023, the FBI has observed an uptick in sextortion victims reporting the use of fake images or videos created from content posted on their social media sites or web postings, provided to the malicious actor upon request, or captured during video chats. Based on recent victim reporting, the malicious actors typically demanded: 1. Payment (e.g., money, gift cards) with threats to share the images or videos with family members or social media friends if funds were not received; or 2. The victim send real sexually-themed images or videos.

Recommendations

The FBI urges the public to exercise caution when posting or direct messaging personal photos, videos, and identifying information on social media, dating apps, and other online sites. Although seemingly innocuous when posted or shared, the images and videos can provide malicious actors an abundant supply of content to exploit for criminal activity. Advancements in content creation technology and accessible personal images online present new opportunities for malicious actors to find and target victims. This leaves them vulnerable to embarrassment, harassment, extortion, financial loss, or continued long-term re-victimization.

The FBI recommends the public consider the following when sharing content (e.g., photos and videos) or engaging with individuals online:

- Monitor children's online activity and discuss risks associated with sharing personal content
- Use discretion when posting images, videos, and personal content online, particularly those that include children or their information.
    - Images, videos, or personal information posted online can be captured, manipulated, and distributed by malicious actors without your knowledge or consent.
    - Once content is shared on the internet, it can be extremely difficult, if not impossible, to remove once it is circulated or posted by other parties.
- Run frequent online searches of you and your children's information (e.g., full name, address, phone number, etc.) to help identify the exposure and spread of personal information on the internet.
- Apply privacy settings on social media accounts—including setting profiles and your friends lists as private—to limit the public exposure of your photos, videos, and other personal information.
- Consider using reverse image search engines to locate any photos or videos that have circulated on the internet without your knowledge.
- Exercise caution when accepting friend requests, communicating, engaging in video conversations, or sending images to individuals you do not know personally. Be especially wary of individuals who immediately ask or pressure you to provide them. Those items could be screen-captured, recorded, manipulated, shared without your knowledge or consent, and used to exploit you or someone you know.
- Do not provide any unknown or unfamiliar individuals with money or other items of value. Complying with malicious actors does not guarantee your sensitive photos or content will not be shared.
- Use discretion when interacting with known individuals online who appear to be acting outside their normal pattern of behavior. Hacked social media accounts can easily be manipulated by malicious actors to gain trust from friends or contacts to further criminal schemes or activity.

- Secure social media and other online accounts using complex passwords or passphrases and multi-factor authentication.
- Research the privacy, data sharing, and data retention policies of social media platforms, apps, and websites before uploading and sharing images, videos, or other personal content.

Additional Resources

For more information on sextortion, see the 2 September 2021 PSA, "FBI Warns about an Increase in Sextortion Complaints," at https://www.ic3.gov/media/Y2021/PSA210902.

Additionally, the below FBI press releases contain important information regarding this scheme:

- https://www.fbi.gov/news/press-releases/international-law-enforcement-agencies-issue-joint-warning-about-global-financial-sextortion-crisis
- https://www.fbi.gov/news/press-releases/fbi-and-partners-issue-national-public-safety-alert-on-financial-sextortion-schemes

The National Center for Missing and Exploited Children provides a free service known as **Take It Down**, which could help victims, who have possession of the image or video files, remove or stop the online sharing of nude, partially nude, or sexually explicit content that was taken while under 18 years old. For more information, visit https://takeitdown.ncmec.org.

If you believe you are the victim of a crime using these types of tactics, retain all information regarding the incident (e.g., usernames, email addresses, websites or names of platforms used for communication, photos, videos, etc.) and immediately report it to:

- FBI's Internet Crime Complaint Center at www.ic3.gov
- FBI Field Office [www.fbi.gov/contact-us/field-offices or 1-800-CALL-FBI (225-5324)]
- National Center for Missing and Exploited Children [1-800-THE LOST or www.cybertipline.org]

Reporting these crimes can help law enforcement identify malicious actors and prevent further victimization.

---

[a]Deepfake refers to the broad range of generated or manipulated digital media (e.g., images, videos, audio, or text; collectively referred to as "synthetic content" or "synthetic media") created using artificial intelligence and machine learning processes. Deepfakes can depict the alteration or impersonation of a person's identity to make it appear as if they are doing or saying things they never did.

Generally, synthetic content may be considered protected speech under the First Amendment; however, the FBI may investigate when associated facts and reporting indicate potential violations of federal criminal statutes. Mobile applications, "deepfake-as-a-service," and other publicly available tools increasingly make it easier for malicious actors to manipulate existing or create new images or videos. These tools, often freely found online, are used to create highly realistic and customizable deepfake content of targeted victims or to target secondary, associated victims.

[b]Sextortion is a form of coercion and child sexual exploitation which, depending on the circumstances, may violate several federal criminal statutes, (e.g., production of child sexual abuse material (CSAM) [in violation of *Title 18 U.S.C. § 2251(a)*], coercion/enticement of a minor [in violation of *Title 18 U.S.C. § 2422(b)*], receipt/possession/ distribution of CSAM (in violation of *Title 18 U.S.C. § 2252A*), and/or extortion via interstate communications [in violation of *Title 18 U.S.C. § 875(d)*]).