Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

September 12, 2023

Alert Number
I-091223-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

Violent Online Groups Extort Minors to Self-Harm and Produce Child Sexual Abuse Material

The FBI is warning the public of violent online groups deliberately targeting minor victims on publicly available messaging platforms to extort them into recording or live-streaming acts of self-harm and producing child sexual abuse material (CSAM). These groups use threats, blackmail, and manipulation to control the victims into recording or live-streaming self-harm, sexually explicit acts, and/or suicide; the footage is then circulated among members to extort victims further and exert control over them.

VIOLENT ONLINE GROUPS

The violent online groups use many names, including 676, 764, CVLT, Court, Kaskar, Harm Nation, Leak Society, and H3ll, but continuously evolve and form subgroups under different monikers. They operate on publicly available platforms, such as social media sites or mobile applications. To gain access to a majority of these groups, prospective members are required to live-stream or upload videos depicting their minor victims harming animals or committing self-harm, suicide, murder, or other acts of violence. The key motivators of these groups are to gain notoriety and rise in status within their groups.

TARGETING

The groups target minors between the ages of 8 and 17 years old, especially LGBTQ+ youth, racial minorities, and those who struggle with a variety of mental health issues, such as depression and suicidal ideation.

EXTORTION AND SELF-HARM

The groups use extortion and blackmail tactics, such as threatening to SWAT[1] or DOX[2] the minor victims, if they do not comply with the groups' requests, manipulate and extort minors into producing CSAM and videos depicting animal cruelty and self-harm. Self-harm activity includes cutting, stabbing, or fansigning[3]. Members of the groups threaten to share sexually explicit videos or photos of the minor victims with their family, friends, and/or post to the internet. The groups control their victims through extreme fear and many members have an end-goal of forcing the minors they extort into committing suicide on live-stream for their own entertainment or their own sense of fame.

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 minor victims. This leaves them vulnerable to embarrassment, harassment, extortion, financial loss, or continued long-term re-victimization. Further, the FBI recommends looking out for warning signs indicating a minor may be experiencing self-harm or suicidal ideations. Being able to recognize the warning signs of self-harm will help you provide immediate support.

The FBI recommends the public consider the following warning signs regarding self-harm or suicide:

- Sudden behavior changes such as becoming withdrawn, moody, or irritable.
- Sudden changes in appearance, especially neglect of appearance.
- Changes in eating or sleeping habits.
- Dropping out of activities and becoming more isolated and withdrawn.
- Scars, often in patterns.
- Fresh cuts, scratches, bruises, bite marks, burns, or other wounds.
- Carvings, such as words or symbols, on the skin.
- Wearing long sleeves or pants in hot weather.
- Threatening to commit suicide and openly talking about death, not being wanted or needed or not being around.

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 photos or videos. 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. Malicious actors can easily manipulate hacked social media accounts.
- 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

If you are worried about someone who might be self-harming or is at risk of suicide the following resources may help:

- Consult your pediatrician or other health care provider who can provide an initial evaluation or a referral to a mental health professional.
- Connecting your child to a mental health resource can help them learn healthy coping skills for intense emotions and help reduce the risk of a serious injury.
- If it is an immediate, life-threatening emergency dial 9-1-1.

The National Center for Missing and Exploited Children provides a free service known as **Take It Down**, which helps minor victims, even if they are now an adult, but were victimized as a minor, with online image or video files, remove or stop the online sharing of nude, or sexually explicit content 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.

---

[1]SWAT also referred to as SWATTING is the action or practice of making a prank call to police or emergency services in an attempt bring about the dispatch of armed police officers such as a SWAT team to a particular address.

[2]DOX also referred to as DOXXING is the action of obtaining and publishing personally identifiable information (PII) on the internet, usually for malicious intent.

[3]Fansigning is writing or cutting specific numbers, letters, symbols, or names onto your body.