

### **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/contactus/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 SWATi or DOXii 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.iii 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.

# Federal Bureau of Investigation Public Service Announcement

#### 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.

# Federal Bureau of Investigation Public Service Announcement

- 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.

# Federal Bureau of Investigation Public Service Announcement

### **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 <a href="https://takeitdown.ncmec.org">https://takeitdown.ncmec.org</a>.

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.

<sup>&</sup>lt;sup>1</sup> 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.

<sup>&</sup>lt;sup>ii</sup> DOX also referred to as DOXXING is the action of obtaining and publishing personally identifiable information (PII) on the internet, usually for malicious intent.

iii Fansigning is writing or cutting specific numbers, letters, symbols, or names onto your body.



### Alert Number: I-030625-PSA March 6, 2025

## Violent Online Networks Target Vulnerable and Underage Populations Across the United States and Around the Globe

The Federal Bureau of Investigation (FBI) is warning the public of a sharp increase in the activity of "764" and other violent online networks which operate within the United States and around the globe. These networks methodically target and exploit minors and other vulnerable individuals, and it is imperative the public be made aware of the risk and the warning signs exhibited by victims. These networks use threats, blackmail, and manipulation to coerce or extort victims into producing, sharing, or live-streaming acts of self-harm, animal cruelty, sexually explicit acts, and/or suicide. The footage is then circulated among members of the network to continue to extort victims and exert control over them.

### VIOLENT ONLINE NETWORKS

Some of the violent actors in these online networks are motivated by a desire to cause fear and chaos through their criminal conduct. However, motivations are highly individualized, and some threat actors may be engaging in criminal activity solely for sexual gratification, social status or a sense of belonging, or for a mix of other reasons that may not be ideologically motivated.

#### **TARGETING**

These networks exist on publicly available online platforms, such as social media sites, gaming platforms, and mobile applications commonly used by young people. Many threat actors systematically target underage females, but anyone — juveniles, adults, males, and females — can be targeted. Victims are typically between the ages of 10 and 17 years old, but the FBI has seen some victims as young as 9 years old. These violent actors target vulnerable populations to include children as well as those who struggle with a variety of mental health issues, such as depression, eating disorders, or suicidal ideation. Threat actors often groom their victims by first establishing a trusting or romantic relationship before eventually manipulating and coercing them into engaging in escalating harmful behavior designed to shame and isolate them.

### **EXTORTION AND SELF-HARM**

The networks use extortion and blackmail tactics, such as threatening to swat¹ or dox² their victims, if the victims do not comply with the network's demands. The actors can manipulate or coerce victims to produce Child Sexual Abuse Material (CSAM) and other videos depicting animal cruelty and self-harm. Self-harm activity can include cutting, stabbing, or fansigning.³ Members of the networks threaten to share the explicit videos or photos of the victims with the victims' family, friends, and/or post the photos and videos to the internet. The networks control their victims through extreme fear and many members have an end-goal of forcing the victims they extort or coerce to live-stream their own suicide for the network's entertainment or the threat actor's own sense of fame.

### RECOMMENDATIONS

The FBI urges the public to exercise increased vigilance when posting personal photos, videos, or personal identifying information, or direct messaging online. Although seemingly innocuous when posted or shared, the images and videos can provide malicious actors an abundant supply of content to exploit and manipulate or alter for criminal activity. Victims are vulnerable to embarrassment, harassment, extortion, or continued long-term re-victimization. The FBI recommends looking for warning signs indicating a victim may be engaging in self-harm or having suicidal thoughts.

The FBI recommends that family, friends, and associates consider the following potential indicators and warning signs:

- 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.
- A new online "friend" or network prospective victims seem infatuated with and/or scared of.
- Receipt of anonymous gifts, such as items delivered to your home, currency, gaming currency or other virtual items.
- 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.
- Writing in blood or what appears to be blood.
- Threatening to commit suicide and openly talking about death, not being wanted or needed, or not being around.
- Idealization of mass shooting or mass casualty events.
- Family pets or other animals being harmed or dying under suspicious circumstances.
- Family pets uncharacteristically avoid or are fearful of your child or you.

3/6/25, 10:14 AM

• Law enforcement being called to the home under false pretenses (known as *swatted* or doxxed) by an unknown person.

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

- Monitor children's and other vulnerable individuals' online activity and discuss risks associated with sharing personal information.
- Use discretion when posting images, videos, and personal content online, particularly those that include children or their information.

For more information on how to protect children and others refer to information on online risks here: <u>Parents, Caregivers, Teachers — FBI</u>.

### 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, remove or stop the online sharing of nude, or sexually explicit online content. For more information, visit <a href="https://takeitdown.ncmec.org">https://takeitdown.ncmec.org</a>.

If you believe you are the victim of a crime using these 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 <a href="https://www.ic3.gov">www.ic3.gov</a>
- FBI Field Office (<u>www.fbi.gov/contact-us/field-offices</u> or <u>1-800-CALL-FBI (225-5324)</u>)
- National Center for Missing and Exploited Children (<u>www.cybertipline.org</u> or <u>1-800-THE LOST</u>)

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

<sup>&</sup>lt;sup>1</sup> Swat also referred to as swatting is the action or practice of making false emergency calls to police or other emergency services in an attempt bring about the dispatch of armed police officers such as a <u>SWAT</u> 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.  $\stackrel{\checkmark}{}$
- <sup>3</sup> Fansigning is writing or cutting specific numbers, letters, symbols, or names onto one's body.  $\stackrel{\checkmark}{\leftarrow}$



### Alert Number: I-042925-PSA April 29, 2025

### Threat Actors Use "Swatting" to Target Victims Nationwide

The Federal Bureau of Investigation (FBI) is aware of multiple recent "swatting" incidents. This Public Service Announcement (PSA) is intended to provide the public with information about what swatting is, how to take protective steps against swatting, and how to report potential incidents. The FBI takes swatting threats seriously and coordinates with federal, state, local, tribal, and territorial law enforcement partners to respond to and investigate these incidents.

### WHAT IS SWATTING?

Swatting is the malicious tactic of making hoax calls or reports to emergency services, typically feigning an immediate threat to life. Swatting is intended to draw a large response from SWAT teams or other law enforcement resources to an unsuspecting victim's location, causing chaos and the potential for injury or violence.

Targets of swatting often include high-profile public figures, as well as schools, hospitals, places of worship, and centers of mass transportation, but anyone can be a victim. A swatting incident may be an isolated event targeting one victim or part of a larger coordinated effort to target multiple victims.

Swatting may be conducted to harass, intimidate, or retaliate against intended targets. It is a serious crime that can have deadly consequences due to confusion on the part of victims and responding officials, and that also diverts limited public safety resources from valid emergencies.

Threat actors often compile sensitive information from a wide range of publicly available sources, including online accounts, to develop invasive profiles of their targets. They leverage spoofing technology to anonymize their identities, using phone numbers, email addresses, and social media profiles to make it appear the false report is coming from the victim. Threat actors may also use compromised smart home devices to facilitate swatting attacks.

### **WAYS TO PROTECT YOURSELF**

The FBI urges the public to consider the following measures:

- Review your online presence for sensitive personal information that could enable malicious actors to conduct a swatting attack.
- Exercise care when posting content (including photos and videos) or sharing it
  with individuals online. Although seemingly innocuous, images and videos can
  be exploited or manipulated by malicious actors for criminal activity.
- Consider online resources and services that may aid in reducing or removing sensitive publicly available information.
- Use strong, unique passwords, and multi-factor authentication on all devices and accounts, including smart home devices.
- Discuss swatting with your family members or colleagues and have a plan in place in the event of law enforcement contact at your residence, business, or other location.

In the event you are the victim of a swatting attack, stay calm, and listen to and cooperate with responding law enforcement.

### **ADDITIONAL RESOURCES**

If you believe you are the victim of a swatting incident, retain all information regarding the incident, such as usernames, email addresses, websites, or names of platforms used for communication, photos, or videos.

- Immediately report it to your local law enforcement agency.
- To report an emergency or an immediate threat to life, call 911.
- To report any leads, threats, and/or criminal activity you may also visit <u>tips.fbi.gov</u>, call <u>1-800-CALL-FBI</u> (225-5324) or contact your local FBI field office <a href="https://www.fbi.gov/contact-us">https://www.fbi.gov/contact-us</a>.