

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 https://takeitdown.ncmec.org.

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 www.ic3.gov
- 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.

¹ 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. $\stackrel{\checkmark}{}$
- ³ Fansigning is writing or cutting specific numbers, letters, symbols, or names onto one's body. $\stackrel{\checkmark}{\leftarrow}$