PENNSYLVANIA CRIMINAL INTELLIGENCE CENTER

Information Alert

CIKR-06-2025 August 25, 2025

(U) EDUCATION SECTOR LIKELY TO EXPERIENCE INCREASES IN SWATTINGS, HOAX EMAIL THREATS, AND IN-REAL-LIFE VIOLENT PLOTS

(U//FOUO) The Pennsylvania Criminal Intelligence Center (PaCIC) is providing this Information Alert to inform Education Sector partners of a likely increase in swatting, bomb threats, extortion, and real-life incidents of violence perpetrated by juveniles and young adults adhering to nihilistic violent extremism (NVE) activities, coinciding with the start of the 2025-2026 academic school year.

(U) KEY JUDGMENTS

(U//FOUO) The PaCIC assesses the start of the 2025-2026 academic school year and return to school environments will likely result in increases in swatting, hoax email threats, and in-real-life (IRL) plots and acts of violence perpetrated by NVE adherents.

- (U//FOUO) Swatting and Hoax Threats
  - (U//FOUO) NVEs use swattings and hoax email threats to sow chaos and draw emergency responders to a location, including K-12 and higher education facilities. There is competition among NVE actors to draw increasingly larger responses; the bigger, the better among this community, likely increasing the number and severity of future swattings.
  - (U//FOUO) NVEs often conduct swattings and hoax email threats in the name of a victim as a threat tactic to extort the victim into compliance. When emergency services are deployed to a school or residence for a bomb threat or active shooter scenario, if the alleged perpetrator states their name, phone number, or address within the call or email, it should be an indicator this may be a swatting or hoax requiring further investigation into the motive.
- (U//FOUO) IRL Activity
  - (U//FOUO) NVE activity occurs primarily online; however, there has been an increase in calls for individuals to conduct IRL actions, likely increasing the number and severity of future mass casualty attack plots by NVE adherents. The school environment may serve as an attractive target for juveniles wanting to participate in IRL acts of violence to further their online credibility.

(U) NVE OVERVIEW

(U//FOUO) On 04/14/2025, the Federal Bureau of Investigation (FBI) designated NVE as a new terrorism threat category. Nihilism is the belief that everything is meaningless; adherents desire to cause a societal collapse through chaos and the targeting of the next generation purely for destructions' sake. NVEs operate primarily online, across various platforms

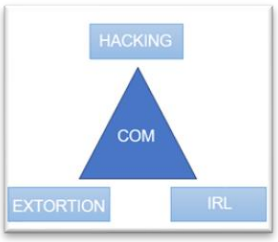
PENNSYLVANIA CRIMINAL INTELLIGENCE CENTER sp-protectpa@pa.gov

Pennsylvania State Police • Bureau of Criminal Investigation • Intelligence Division (855) 772-7768 • FAX: (717) 772-6917

Thank you for taking the time to provide feedback. It is important in helping us improve our products and services.
CLICK HERE FOR PACIC CUSTOMER SURVEY

including but not limited to Discord, Telegram, X, Roblox, Minecraft, and Fortnite. NVEs themselves are typically juveniles and young adults, and use these online platforms to identify, groom, and victimize other vulnerable juveniles into engaging in activities such as self-harm, familial or animal violence, coerced suicide, creating and sending child sexual abuse material (CSAM), or IRL acts of property destruction and violence. NVEs employ tactics including hacking, swatting, extortion, and sextortion to manipulate juvenile victims into complying with their requests. Their goal is to desensitize their victims toward future violence, and to obtain and share online content to increase their online notoriety.

(U//FOUO) Perpetrators are often young males who tend to justify their actions and may even boast about their involvement when given the opportunity. Perpetrators are largely motivated by peer recognition and status, with many of their actions rooted in a competitive drive and outdoing one another. The actions they coerce their victims to do or carry out themselves is viewed and calculated in a "point system."



(U) NVE TACTICS

(U//FOUO) Many NVEs operate in a decentralized online network called "The Community" or "COM." Members of COM operate within and between three primary categories:

- (U//FOUO) Extortion COM
  - (U//FOUO) Often begins with befriending and convincing the victim to send nude images of themselves. The actor then uses the material to extort the victim into increasingly harmful and violent acts, including self-harm, familial violence often on a younger sibling, animal violence often on a family pet, and even coerced suicide.
  - (U//FOUO) Actors will conduct swattings on victims' residences and schools to manipulate and extort the victim into complying with the actor's demands.
- (U//FOUO) In-Real-Life COM
  - (U//FOUO) Increasing calls for COM participants to conduct IRL acts of property destruction (bricking, vandalism, spray-painting), and acts of violence. The IRL acts must be recorded or live streamed to receive credit and so it can be shared among the COM network. The worse and more violent the act, the more points, notoriety, and credibility the extorter receives among the online network.
  - (U//FOUO) Previous studies have shown school attackers experienced stressors in various areas of their lives, with nearly all experiencing at least one in the six months prior to their attack, and half within two days of the attack. For some, the return to school and being thrust back into the school environment may serve as a significant social stressor for juveniles who may have spent the summer isolated or online, consuming violent extremism content and potentially becoming involved in activities moving them toward real-life violence. The school environment may serve as an attractive target for juveniles wanting to participate in IRL acts of violence to further their online credibility.
- (U//FOUO) Hacker COM
  - (U//FOUO) Cyberattacks
  - (U//FOUO) Cryptocurrency theft/scamming

(U) VICTIM INDICATORS

(U//FOUO) Victims are primarily juvenile females between the ages of 10 to 17, but perpetrators will target victims under 10 if they have the chance. Online platforms are often used to exploit victims with pre-existing vulnerabilities such as having an eating or mental health disorder, already self-harming, exploring their gender identity, abnormal family dynamics, or experience of past trauma. Some indicators or warning signs include:

- Sudden behavior changes

PENNSYLVANIA CRIMINAL INTELLIGENCE CENTER sp-protectpa@pa.gov

Pennsylvania State Police • Bureau of Criminal Investigation • Intelligence Division (855) 772-7768 • FAX: (717) 772-6917

Thank you for taking the time to provide feedback. It is important in helping us improve our products and services.
CLICK HERE FOR PACIC CUSTOMER SURVEY

- Changes in appearance, eating, or sleeping habits
- Anonymous gifts delivered to their home
- Law enforcement called to their home under false pretenses (swatting)
- Self-harm in the form of patterns, symbols, or names
- Writing in blood or what appears to be blood
- Idolization of mass violence or shootings
- Threatening to commit suicide and openly talking about death or not wanting to be around
- Family pets fearing a child or suspiciously dying

(U) TERMINOLOGY[1]

(U//FOUO) The following terms are commonly used among the COM network; if observed or heard, may be an indicator of participation or victimization involvement.

Content	Photos of fansigns/cutsigns, nude images obtained by extortion, edits (video compilations or digital art), etc. Groups and participants in Extortion COM that produce content gain notoriety and respect within the community. Those who are accused of stealing (redistributing) old content lose their reputation. Also referred to as OC (original content).
Com Girl	A young, often juvenile female participant in COM, frequently beginning as a victim of grooming and extortion. Associated with Scene, Emo, or Anime-style fashion. Com girls are often degraded by other participants as deserving their victimization for being overtly sexual or materialistic.
Cutshow	A live stream or video call in which a victim self-harms with a blade for the enjoyment of viewers.
Cutslut/Cutslave	A derogatory term in Extortion COM to refer to victims of sextortion who cut themselves at the direction of their "owner."
Doxbin	A website for hosting doxes or identification of online users. The website is heavily used by COM participants to deanonymize rivals.
Fansign/Cutsign	Writing or cutting specific numbers, letters, symbols, or names onto one's body. A form of self-harm fetishized by some sexual sadists. Victims are often extorted into doing fansigns.
IP grabbing	A technique of sending a hidden malicious redirect link to find out a victim's IP address often used by extorters to identify and intimidate victims.
Known	A famous or respected user within COM.
Lorebook	A collection of derogatory material regarding an individual, including a combination of dox, relatives, extorted CSAM, self-harm images, narratives of their activities within com, etc. The targets of lorebooks may be victims or perpetrators and the activities detailed in the lorebook may be the result of extortion.
988twt	988 refers to the Suicide and Crisis Lifeline. 988twt refers to a community of X users who bond over suicidal ideation. 988twt users are targeted as victims by Extortion COM participants.
Shtwt	Shtwt refers to Self-Harm X, a community of often young, female users that engage in self-harm. Shtwt users are targeted as victims by Extortion COM participants.

(U) RECOMMENDATIONS

(U//FOUO) The PaCIC encourages heightened awareness to concerning behaviors of new and returning students and further encourages leveraging multi-disciplinary Threat Assessment and Threat Management Teams to assess the situation and surge resources.

PENNSYLVANIA CRIMINAL INTELLIGENCE CENTER **sp-protectpa@pa.gov**

Pennsylvania State Police • Bureau of Criminal Investigation • Intelligence Division (855) 772-7768 • FAX: (717) 772-6917

Thank you for taking the time to provide feedback. It is important in helping us improve our products and services.
CLICK HERE FOR PACIC CUSTOMER SURVEY

(U//FOUO) The PaCIC encourages school administrators and personnel to discuss NVE indicators with all staff and consider age-appropriate ways to dialogue with students and guardians about the importance of online safety.

(U//FOUO) The PaCIC encourages school administrators to discuss NVE and COM indicators with IT staff equipped to identify or flag these materials, references, and sites on student devices.

(U//FOUO) The PaCIC strongly discourages self-investigation of COM-related websites; they use technology to capture personally identifiable information including IP addresses, which may result in yourself becoming a target.

(U//FOUO) In all situations, a threat should be treated as an emergency in accordance with the organization's emergency operations plan until law enforcement determines its credibility.

(U//FOUO) Report incidents of possible NVE-related activity, swatting, and hoax email threats to the PaCIC at sp-protectpa@pa.gov.

(U) RESOURCES

(U) Federal Bureau of Investigation Public Service Announcement: The Com: Theft, Extortion, and Violence are a Rising Threat to Youth Online

(U) Federal Bureau of Investigation Public Service Announcement: Violent Online Networks Target Vulnerable and Underage Populations Across the United States and Around the Globe

(U//FOUO) Federal Bureau of Investigation Executive Update: Creation of Nihilistic Violent Extremism Threat Category

(U//FOUO) PaCIC is providing this for informational purposes and situational awareness only. The mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics may be constitutionally protected. PaCIC only reports on First Amendment protected activities for operational planning in the interest of ensuring the safety and security of the demonstrators and the general public.

CUSTOMER FEEDBACK

To assist in improving our production and dissemination processes, please provide feedback of this product by completing an online customer survey. A link to the survey can be found at the bottom of this page. This will allow us to ensure that our customers continue to receive valuable, relevant information in a timely manner.

The information used in this bulletin is drawn from open sources, DHS open source reporting, FBI and other law enforcement intelligence reports and court filings. The Pennsylvania State Police (PSP) has high confidence in the information obtained from court documents and those of government agencies. The PSP has medium confidence in the information obtained from open sources, which includes media reports and Internet websites whose information is credibly sourced and plausible but may contain biases or unintentional inaccuracies. When possible, open source information has been corroborated through other law enforcement and government sources.

[1] South Carolina Information and Intelligence Center, Central Florida Intelligence Exchange, Central California Intelligence Center, Minnesota Fusion Center. (2024, October 31). (U//FOUO) Terms and Imagery Used in Some Online Sextortion Groups.

PENNSYLVANIA CRIMINAL INTELLIGENCE CENTER **sp-protectpa@pa.gov**

Pennsylvania State Police • Bureau of Criminal Investigation • Intelligence Division (855) 772-7768 • FAX: (717) 772-6917

Thank you for taking the time to provide feedback. It is important in helping us improve our products and services.
CLICK HERE FOR PACIC CUSTOMER SURVEY