TN Department of Safety & Homeland Security | Office of Homeland Security

Managing Hoax Threats

Hoax threats to our nation's schools continue to occur. Authorities nationwide have conducted investigations into numerous false threats of planned violence against schools and other public locations. These hoax threats, sometimes referred to as "swatting", occur through a variety of means to include phone calls, text messages, social media posts, handwritten notes, and letters.

With the purpose of creating injury or disruption, and triggering a response from law enforcement, hoax threats frequently describe significant incidents such as bombs, hostage situations, active shooters, and murders.

All threats should be treated seriously until they have been proven false. However, all threats, may not necessarily result in the same automatic and reflexive response. Choosing the best response depends on the credibility of the threat and an evaluation of the threat using a totality of the circumstances approach.

Once a threat is received, immediately contact law enforcement to inform them of the incident and report the details to the Tennessee Office of Homeland Security. The Tennessee Office of Homeland Security can compare and assess the information with other known threat reports. This comparison and assessment can help in determining credibility and assist in making informed decisions regarding the appropriate response.

Evacuate or Shelter in Place?

Upon receiving a threat, it is understandable to feel the need to immediately evacuate or shut down the facility. However, immediate evacuation may not be the most suitable course of action, particularly if the credibility of the threat is uncertain. An alternate course of action involves conducting a preliminary investigation, analyzing the information, and then deciding whether an evacuation is necessary. In the absence of supporting information, it may be advisable to follow the **Shelter In Place** protocol until the threat can be thoroughly assessed. Evacuating immediately on every threat may cause disruption to both the facility and the individuals within and often accomplishes the goal of the hoax perpetrator.

In the absence of evidence indicating a present danger on the premises, such as a bomb or an armed assailant, individuals are generally safer indoors. The structure of buildings provides a level of protection, reinforced by security features like access restrictions, locked doors, and sturdy walls. Take advantage of this protection while further details are being collected. Furthermore, sheltering in place enables the creation of secure evacuation routes and ensures the accountability of individuals in case the situation escalates.

Evaluating the Threat

Three common questions are generally recognized to begin assessing a threat:

- What is the motivation of the threat maker and credibility of the threat?
- Could the threat maker have the information on how to carry out the threat (such as information on how to make bombs or homemade weapons, for example)?
- Could the threat maker have access to the tools and the capability to carry out the threat?

When evaluating the credibility of threats, it is important to consider the level of detail and specificity in the threat, as well as the behavioral indicators related to planning and executing the threat. A highly detailed and specific threat is more likely to be credible. Additionally, the presence of evidence such as hit lists, maps, documented times and locations, along with action steps like weapon stockpiling and creation of suicide notes or videos, further enhances the credibility of the threat.

Indicators of a Hoax

Additional information can be found at the sources at the end of this document. The following list contains possible indicators of a hoax.[1] This is not an exhaustive list:

- The hoax call is the only incoming call reporting the incident. In a real incident, multiple calls would likely be received.
- Hoax calls are often received by the non-emergency line. Hoaxers using VoIP services cannot dial 911 directly, so they must call the non-emergency number.
- The incoming telephone number is spoofed or blocked.
- Hoax calls using VoIP services will appear as all zeros or nines, blocked, unavailable, or one of the default VoIP numbers. Skype, TextNow, Google Voice, etc.
- The caller's demeanor is inconsistent with the claimed crises or threat. For example, the caller claims to have witnessed the shooting of several students, but they appear calm and with no background noise.

[1] When a threat is received, immediately report the threat to law enforcement. When a threat is received, law enforcement should be notified immediately, no matter if any or all of the indicators of a hoax are present.

- Background noises include computer mouse clicking and/or typing. The caller is unable to answer follow-up questions requesting details such as their full name, phone number, or current location. Callers may attempt to provide descriptions of interiors or exteriors of buildings gleaned from photos on social media or internet searches.
- The caller mispronounces names such as city, street, or building names. Hoax calls are commonly conducted by perpetrators who are unfamiliar with the local areas they target.
- The caller’s story changes or escalates when challenged with follow-up questions or doubts that their claims are true or legitimate, the swatting caller may intensify their threat or change key details of their story.
- “Call of Duty Speak” - caller uses exotic or specific names of weapons from playing video games.
- Gunshots or explosions heard in the background are inconsistent with other noise or sound fabricated.
- The caller claims to be armed or suicidal and willing to shoot law enforcement.
- The hoax social media post, email, message, etc. is sent to multiple recipients especially across multiple cities and/or states.
- The hoax threat is often vague and unspecific and could refer to numerous locations of a similar name. For example, “I’m shooting up Central tomorrow.”

Threats via Phone Call

Inconsistencies in threats received via phone calls can be detected by asking several questions and revisiting them later during the conversation.

Suggested questions include:

- “What is your full name?” (ask again later during call, and specifically ask for a middle name)
- “Where are you calling from?”
- “What is your call back phone number?”
- “Why didn't you call 911 directly?” (for VoIP calls to non-emergency number)
- “Why are you reporting yourself?”
- “Why is there no noise in the background?”
- “What is that noise in the background?” (when background noise is inconsistent with the story)
- “Why does it sound like you are typing on a computer keyboard?”
- “Are you targeting anyone in particular?”

Online Threats

For threats received online through social media, email, a website, or direct messaging, do not forward or share the threat message. Alert your local law enforcement immediately. It is fortunate that many of these online threats are traceable, enabling law enforcement to conduct investigations on the person responsible and assess the validity of the threat.

Regardless of credibility, a single threat has the potential to trigger the dissemination of false information and an increase in imitated threats. When coupled with instances of real violence, this can result in significant emotional turmoil, fear, and anxiety among individuals. It is imperative for both facilities and law enforcement to treat threats seriously, while responding in a calculated and suitable manner.

Sources:

Federal Bureau of Investigation.

Swatting: Mitigation Strategies and Reporting Procedures. https://rems.ed.gov/docs/WA_Swatting.pdf

Threat Assessment: School Threats, Social Media, Texting, and Rumors. National School Safety and Security Services. https://schoolsecurity.org/trends/threat-assessment-threats-rumors-text-messages/

Social Media Threat Guidance For School Staff And Authorities. CISA. https://www.cisa.gov/sites/default/files/2023-12/Social%20Media%20Threat%20Guidance%20for%20School%20Staff%20and%20Authorities%20Infographic_508.pdf