Swatting: Emergency Management Procedures

Swatting *is defined as a false report of an ongoing emergency or threat of violence intended to prompt an immediate tactical law enforcement response.*

Swatting is not a new threat; it has evolved over the last decade, and it includes a range of tactics and techniques used to cause false public alarm and divert law enforcement resources to a hoax threat. Certain incident types and tactics have tended to receive more media coverage than others. Swatting scenarios include bomb threats, active shooter scenarios, threats of an imminent shooting rampage, hostage scenarios, and threats involving chemical, biological, radiological, nuclear, or explosives agents.

- The motivations for swatting vary and include the attention gained from national media coverage and discussions on social media or online forums, revenge against gamers or those responsible for previous swatting incidents, and financial gain. Perpetrators post advertisements in online forums and black-market sites offering to conduct swatting for a fee and to boast of their previous swatting successes.
- Incidents of swatting across the country are commonly linked, and investigations often lead to groups of perpetrators outside the US. These foreign actors are often contacted and paid to conduct the swatting act by a student of the targeted school or a video game player who provides the name and address or workplace of another gamer against whom they are seeking revenge. However, some incidents are linked to bad actors located in the US.
- Many incidents involve the targeted location receiving the swatting call, as opposed to reporting the emergency directly to law enforcement agencies. There are instances of an anonymous caller using a computerized text-to-speech voice.
- Swatting incidents in which the caller does not provide a name, and there are no claims of responsibility following the incident, differ from historical cases and indicate a potential shift away from motivations of revenge and recognition.
- Commonly, there is an uptick in swatting calls at the beginning of the school year and copycat threats often happen after a school shooting occurs within the US.

CTIC Threat Assessment (Swatting)

- (U//FOUO) The Connecticut Intelligence Center (CTIC) assesses malicious actors will likely continue to target schools with swatting due to the limited resources required, the ability to remain anonymous through device applications, lack of perceived personal risk, and the potential for significant impact within school and the law enforcement community. Swatting incidents may increase in frequency and sophistication as technology evolves.

Indicators

The following are indicators which can be used to identify a potential swatting incident. This is not an exhaustive list, and public and private sector partners are encouraged to contact local law enforcement with lessons learned or success stories of tactics used to dispel a swatting attempt.

- The swatting call is *the only incoming call* to report an active shooter or ongoing emergency situation. If a shooting has occurred or an active shooter scenario is unfolding, multiple calls to dispatch from witnesses or victims are likely.
- The incoming telephone number *is spoofed or blocked*. Swatting calls using Voice over Internet Protocol (VoIP) services will appear as all zeros or nines, blocked, unavailable, or one of the default Skype numbers: (661) 748-0240, (661) 748-0241, or (661) 748-0242.
- The swatting call is *routed through a non-emergency dispatch line*. Swatters using VoIP services cannot dial 9-1-1 directly so instead they look up non-emergency lines of dispatch operations.
- The caller's tone and background noise are *inconsistent with the claimed emergency* or threat. For example, the caller claims to have murdered a family member, coworkers, or innocent bystanders, yet their demeanor is suspiciously calm, with minimal background noise.
- The caller can be heard *typing or clicking a computer mouse* in the background. Swatters will conduct internet searches or use online mapping and geospatial tools during the call to answer follow-up questions and provide exterior descriptions of buildings or residences.
- The caller is *unable to answer follow-up questions* requesting details such as their full name, phone number, or current location. Swatting 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. Swatting calls may be conducted by foreign perpetrators who may have thick accents and will be unfamiliar with the local areas they target.
- For school threats, callers may reference non-existent classroom numbers.
- The caller's *story changes or escalates* throughout the course of questioning. When challenged by 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.
- The caller uses *specific gun names* or terminology to identity their weapon. Swatting callers often refer to weapons commonly depicted in video games, such as an AR-15 assault rifle.
- Gunshots or explosions heard in the *background are inconsistent* with other noise or sound fake.
- Swatting callers may play recordings of gunshots or live firefights from video games or the internet to sound as if they are shooting a weapon while on the call.
- The caller *claims to be armed or suicidal* and willing to shoot law enforcement.

Prevention

- A positive school climate which encourages students to share information (leakage) with staff is a powerful way to prevent swatting. While bad actors are often unknown to victims, some swatting acts are targeted, and elements may be known to students or staff.
- Training students to respond when they recognize threatening behavior has proven to be helpful in preventing targeted violence. A brief video or announcement describing the signs of threats can disrupt targeted violence, including swatting.
- Train all staff, but especially clerical staff who answer phones, on recognizing swatting calls.
- Consider using a campaign to parents and students about the criminal and economic liability of swatting. Research by TDR Technologies in 2022, estimates the cost to taxpayers per swatting threat to schools in Connecticut is over $38,000. This impact does not include the cost of first responders.

Protection

- Technology, including but not limited to phone systems, can screen out these calls making it difficult for the bad actor to complete their act of swatting using the phone.

Mitigation

Swatting calls can be successfully mitigated using follow-up questioning to identify inconsistencies or weaknesses in the caller's storyline or to make the caller feel their attempt is failing. Call receivers should ask **multiple questions** in quick succession, and repeat questions later in the call to identify inconsistencies.

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 phone number?"
- "Why didn't you call 911 directly?" (for VoIP calls to non-emergency dispatch line)
- "I need a call back number in case we get disconnected. What is your mobile or home 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?"

Caller claims to be inside, near, or on the roof of a *school*:

- "How did you get on the roof?"
- "Where exactly are you on the roof?"
- "How are you going to get inside the building?"
- "Do you know a student or employee at the school?"

Caller claims to be inside or near a *mall, hospital, or other commercial venue*:

- "Where are you in the building?"

- “What are you near?”
- “Which building are you in/on?” (when there are multiple buildings in a complex)
- “Do you know an employee?”

Caller claims to be at a *residence*:

- “Where are you in the house?”
- “Is it a one- or two-story house?”
- “What color is the house?“
- “Who owns the house?”
- “Who else lives in the house?”
- “What are your parents’ names?”

Caller claims they are *on their way or planning to target* a location:

- “Where are you coming from?”
- “Are you in a car?”
- “When will you get here?"

Planning, operational coordination, and public information and warning are core capabilities that overlap the five mission areas. An organization can mitigate the impact of the swatting threat by successfully planning, training, exercising, and evaluating their protocols.

- Schools should exercise swatting scenarios with law enforcement and other key stakeholders.

Response

Public and private sector partners should ensure staff and employees are trained on swatting mitigation strategies and reporting procedures for swatting incidents or attempts. First, targeted locations should call 9-1-1 in the event of a reported emergency or threat of violence and clearly indicate if there is suspicion of swatting. If possible, try to keep the caller on the line and ask follow-up questions while another individual speaks to the dispatcher. If the caller stays on the line, use a second phone to call 9-1-1 so the caller stays connected. If possible, use a cell phone or other device to record the swatting call.

Reporting information will aid in the coordination of investigations between local, state, and federal law enforcement, as well as in analysis of trends and the further development of best practices, which will be shared with all partners. Detailed information includes:

1. **Exact time and date** the call was received.
2. **Victim's telephone number** that received the incoming swatting call.
    - If the call was directed to a non-emergency dispatch line and routed through multiple extensions, attempt to provide the original receiving line number and extension.
3. **Victim's telecommunications provider** (for example, Verizon, AT&T, or another carrier).
4. **The incoming (swatting) telephone number**.
    - Was the calling number identified as one of the default Skype numbers: (661) 748-0240, (661) 748-0241, or (661) 748-0242?
    - Was the calling number unavailable, blocked, or displayed as all zeros, ones, or nines?
5. **Detailed description of the nature of the threat**.
    - Incident Type: For example, bomb threat, active shooter, hostage situation, or CBRNE (chemical) threat.
    - Did the caller provide a motivation or reason for the threat?
    - Did the caller specify a timeline for imminent or future threats?
    - Where did the caller claim to be calling from?
    - Was any background noise heard during the call?
6. **Detailed description of caller**.
    - Did the caller provide a name to identify themselves?
    - What was the caller's gender and accent?
    - Was the caller's voice computerized or masked in any way?
    - What was the caller's demeanor and tone (for example, calm, agitated, excited, hysterical, emotional, or confused)?
    - Did the caller seem prepared with a script or preplanned responses?
7. **Report the Incident to CTIC.**
    - To report swatting incidents in Connecticut, please email the Connecticut Intelligence Center (CTIC) at CTIC@ct.gov or call 1-866-HLS-TIPS. CTIC monitors swatting incidents for investigative assistance when needed and conducts evaluation of swatting trends.

Recovery

Swatting incidents which involve deployment of tactical teams to public buildings are certain to inflict fear in the campus environment. Fear erodes a positive school climate and disrupts learning. Furthermore, fear may have a more significant impact in students with disabilities and others who have heightened sensitivities.

- It is important to work closely with law enforcement to ensure the response is adequate to ensure safety and subtle enough to minimize disruption when possible.
- Additionally, as with most other crisis events impacting an entire campus, mental health professionals and school administration may need to guide recovery.
- Messages of safety are critical to students, staff, and parents in restoring the learning environment.
- After a swatting incident occurs, debrief with all involved staff members about what worked and what could be improved. Use staff feedback to improve swatting emergency plans in the future.
- After action reviews that target objectives and identify gaps may help inform other aspects of preparedness.

Credit

This resource was adapted in January of 2023 from a document originally developed by the New Jersey State Police Cyber Crimes Unit, the Intelligence and Analysis Threat Unit at the Regional Operations Intelligence Center, the Office of Homeland Security and Preparedness, and the FBI. Comments or questions about this document can be directed to the CT Center for School Safety and Crisis Preparation at schoolsafetycenter@wcsu.edu.

Representatives from the following organizations contributed to the development of this document: CT Center for School Safety and Crisis Preparation, CT Division of Emergency Management and Homeland Security, CT Intelligence Center, Federal Bureau of Investigation, Amity Regional School District No.5, Bethel Public Schools, Connecticut Association of School Psychologists, and Litchfield Public Schools.