**Vermont School Safety Center**

**“Swatting Calls”**

**Best Practice Considerations**

**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 includes a range of tactics and techniques used to cause false public alarm and divert law enforcement resources to a hoax threat. **Swatting** scenarios threats of an active shooter, bomb threats, hostage situations, and threats involving chemical, biological, radiological, nuclear, or explosives agents.

Incidents of swatting across the country are commonly linked, and investigations often lead to groups of perpetrators who are often located outside the United States. Over time, we have seen the tactics and techniques of communicating these threats change and schools should be prepared for these situations to evolve in the future.

It will be important for each school to quickly evaluate the credibility of the threat. If appropriate, the school should take the necessary response actions to keep students/faculty/staff safe, while the school continues to evaluate the threat. Once a “swatting” call is received, schools should immediately contact their local, county or state law enforcement agency to inform them of this incident.

**Indicators**

The following are indicators which can be used to identify a potential swatting incident:

* 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 are commonly conducted by foreign perpetrators with thick accents who are unfamiliar with the local areas they target.
* The caller’s *story changes or escalates* throughout the course of questioning.
* The caller uses *specific gun names* or terminology to identify 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 in order 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.

**Mitigation**

Schools can use several strategies to identify a “swatting” call. Those receiving these calls should consider asking a number of questions in quick succession to assist in identifying the credibility of the threat.

**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?”
* “I need a call back number in case we get disconnected. What is your mobile or home number?”
* “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?”
* “Do you know a student at the school?”

**Caller claims to be inside the school:**

* “Where are you in the building?”
* “What classroom are you near?”

**Reporting**

Schools should ensure appropriate staff are trained on how to identify and respond to a “swatting” incident. We strongly encourage all schools receiving this type of threat to immediately contact their local law enforcement agency and advise them of the situation. This may help to identify that these threats are happening across the state/nation, possibly reducing the credibility of these threats.

Those receiving these “swatting calls” should try and report accurate details of the calls that may include:

1. The exact time and datethe call was received.
2. Telephone numberthat 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.
1. School’s telecommunications provider(for example, Verizon, AT&T, or another carrier).
2. 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 call number unavailable, blocked, or displayed as all zeros, ones, or nines?
1. Detailed description of the nature of the threat.
* Incident Type: For example, bomb threat, active shooter, hostage situation.
* 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?
1. **Detailed description of caller**.
* Did the caller provide a name to identify themselves?
* What was the caller’s gender, and did they speak with an 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?