



FEDERAL BUREAU OF INVESTIGATION

Public Service Announcement



Alert Number: I-080426-PSA | 04 August 2026 **Ongoing Threats of Swatting and Indicators for Community Members**

This Public Service Announcement (PSA) is an update to Alert Number I-042925-PSA titled, "[Threat Actors Use 'Swatting' to Target Victims Nationwide](#)." This PSA contains updated information about the ongoing threat posed by "swatting" incidents targeting a variety of locations across the United States, including educational institutions, government buildings, religious institutions, public transportation centers, hospitals, and other public buildings.

This PSA intends to provide the public with up-to-date indicators of potential swatting activity and common swatting targets. The Federal Bureau of Investigation (FBI) takes swatting threats seriously and coordinates with federal, state, local, tribal, and territorial law enforcement partners to respond to and investigate these incidents.

WHAT IS SWATTING?

Swatting is the malicious tactic of making hoax calls or reports to emergency services, public locations, or private residences, to falsely report an immediate threat to life or ongoing emergency — such as hoax bomb threats, claims of shootings, or false reports of hostage situations — at a specific location. Swatting is intended to draw a large response from SWAT teams or other law enforcement resources to an unsuspecting victim's location. This causes fear, panic, disorder and disruption within the community through school or event closures, building evacuations and lockdowns, spreading of misinformation on social media, psychological impacts, and the potential for copycat callers when media coverage of swatting also occurs. Additionally, swatting activity wastes government resources, distracts emergency service personnel from legitimate emergencies, and may result in violence, injuries, or deaths.

While traditional swatting incidents have targeted private individuals with whom the perpetrator may harbor animosity, the FBI has seen a shift in swatting incidents targeting educational institutions, government buildings, religious institutions, public transportation centers, hospitals, and other public buildings to disrupt operations or cause general fear and chaos. These recent incidents are part of a larger coordinated effort to simultaneously target multiple community members multiple victims and locations across the United States.

INDICATORS OF SWATTING ACTIVITY

The FBI is providing the following indicators that are characteristic of swatting activity for community member situational awareness. Community members

should observe these indicators in context and not individually, and use discretion and judgement when encountering a potential swatting event:

- Use of Voice Over Internet Protocol (VoIP) telephone numbers to target multiple victims or locations. VoIPs often appear as all zeros or nines, or as blocked or unavailable numbers. Additionally, a call made to the non-emergency telephone numbers of emergency services or other public locations, may indicate that swatters are using VoIP services and cannot dial 911 directly.
- The swatting call is the only incoming call to report an emergency incident instead of multiple calls from witnesses, etc. Generally, in a real emergency, multiple calls are made to an emergency dispatch and not to a non-emergency or public location.
- Calls that originate from outside the United States.
- Vague or inconsistent details about an alleged incident along with a lack of reporting that corroborates the incident. Callers are unable to answer detailed questions such as their full name, phone number, or current location, or responses change when asked the same question.
- Mispronunciation of names, such as cities, streets, or buildings, which may indicate the callers are unfamiliar with the local areas they are targeting.
- Callers who maintain a calm demeanor inconsistent with the incident described or who sound as if they are reading a script.

TIPS FOR MITIGATION

The FBI urges the public to consider the following measures:

- Discuss swatting within your community, including schools, workplaces, places of worship, family members, and colleagues, and have a plan in place in the event of law enforcement contact at your residence, business, or other location.
- Review your online presence for sensitive personal information that could enable malicious actors to conduct a swatting attack.
- Exercise care when posting content (including photos and videos) or sharing it with individuals online. Although seemingly innocuous, images and videos can be exploited or manipulated by malicious actors for criminal activity.
- Consider online resources and services that can aid in reducing or removing sensitive publicly available information.
- Participate in training and preparedness exercises regarding swatting.

In the event you are on the receiving end of a swatting call: stay calm, listen, and cooperate with responding law enforcement personnel.

REPORT IT

If you believe you received a swatting call, retain all information regarding the incident, such as names, usernames, phone number, email addresses, websites, names of platforms used for communications, photos, videos, or call recordings.

- Immediately report the incident to your local law enforcement agency.
- To report an emergency or an immediate threat to life, call 911.
- To report any leads, threats, and/or criminal activity to the FBI you may:
 - Submit a tip at tips.fbi.gov.
 - Call 1-800-CALL-FBI ([225-5324](tel:225-5324)).
 - Contact a local FBI field office www.fbi.gov/contact-us.
 - File a complaint with the FBI Internet Crime Complaint Center (IC3) at www.ic3.gov.