Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-042925-PSA
April 29, 2025

Threat Actors Use "Swatting" to Target Victims Nationwide

The Federal Bureau of Investigation (FBI) is aware of multiple recent "swatting" incidents. This Public Service Announcement (PSA) is intended to provide the public with information about what swatting is, how to take protective steps against swatting, and how to report potential incidents. The 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, typically feigning an immediate threat to life. Swatting is intended to draw a large response from SWAT teams or other law enforcement resources to an unsuspecting victim’s location, causing chaos and the potential for injury or violence.

Targets of swatting often include high-profile public figures, as well as schools, hospitals, places of worship, and centers of mass transportation, but anyone can be a victim. A swatting incident may be an isolated event targeting one victim or part of a larger coordinated effort to target multiple victims.

Swatting may be conducted to harass, intimidate, or retaliate against intended targets. It is a serious crime that can have deadly consequences due to confusion on the part of victims and responding officials, and that also diverts limited public safety resources from valid emergencies.

Threat actors often compile sensitive information from a wide range of publicly available sources, including online accounts, to develop invasive profiles of their targets. They leverage spoofing technology to anonymize their identities, using phone numbers, email addresses, and social media profiles to make it appear the false report is coming from the victim. Threat actors may also use compromised smart home devices to facilitate swatting attacks.

WAYS TO PROTECT YOURSELF

The FBI urges the public to consider the following measures:

- 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 may aid in reducing or removing sensitive publicly available information.
- Use strong, unique passwords, and multi-factor authentication on all devices and accounts, including smart home devices.
- Discuss swatting with your family members or colleagues and have a plan in place in the event of law enforcement contact at your residence, business, or other location.

In the event you are the victim of a swatting attack, stay calm, and listen to and cooperate with responding law enforcement.

ADDITIONAL RESOURCES

If you believe you are the victim of a swatting incident, retain all information regarding the incident, such as usernames, email addresses, websites, or names of platforms used for communication, photos, or videos.

- Immediately report it 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 you may also visit tips.fbi.gov, call 1-800-CALL-FBI (225-5324) or contact your local FBI field office https://www.fbi.gov/contact-us.