SWATTING CALLS AND HOAX THREATS

Homeland Security

Introduction

Throughout the country, schools, hospitals, businesses, places of worship, non-governmental organizations, and individuals to include U.S. government officials, journalists, celebrities, online gamers, and many others have increasingly been victims of swatting calls and hoax threats. These incidents cause fear and potentially dangerous interactions with law enforcement. Swatting calls and hoax threats are a daily occurrence, often come in clusters across the U.S., and are typically made to harass, intimidate, and/or retaliate against their intended target.

Swatting and Hoax Threats

Swatting is making malicious hoax calls to emergency services to falsely report an ongoing emergency such as a violent crime or explosive device at a certain location. The intent is to cause large-scale deployment of Special Weapons and Tactics (SWAT) teams, bomb squads, and other police resources. Individuals and institutions are often unaware of the emergency response, causing confusion, frustration, and potential use of force that may result in harm for the target and responding officials.

Hoax threats are designed to disrupt, distract, or harass locations or organizations. Threats may come in via e-mail, social media, or to a listed phone number in the form of active shooter incidents, bomb threats, hostage situations, or other acts of violence. Threats should be treated seriously and reported to law enforcement who will evaluate and verify if the threat is a hoax.

On January 12, 2024, DHS, the Federal Bureau of Investigation (FBI), and the National Counterterrorism Center issued a bulletin, Malicious Actors Threaten U.S. Synagogues, Schools, Hospitals, and Other Institutions With Bomb Threats, tracking more than 100 separate threats to over 1,000 institutions across 42 states and the District of Columbia over a one-month period.

If you receive a threat, call 9-1-1. Provide the call taker with your name, address, and as many details as possible.

SWATTING CALLS AND HOAX THREATS

Coordinate in Advance with First Responders

- Initiate or strengthen your relationship with local law enforcement; conduct building walk-throughs with the day, night, and weekend shifts; and discuss local response plans. Keep in mind each shift might respond differently.
- Plan how to alert personnel within the building of an incident (cell phones, radios, email, message boards, etc.), and decide who makes notifications. Have a current personnel roster available.
- Provide contact information for key personnel and/or your security team for law enforcement to share with the 9-1-1 Dispatch Center.
- *Swatting specific:* During a suspected swatting incident, the dispatcher may try to contact the institution prior to law enforcement response. Alert law enforcement of any customs or practices that could hinder reaching you in an emergency when you provide your contact information.
- Work with local law enforcement to determine what resources they will need to better respond e.g., floor plans, master keys, combinations to doors, key fobs or access control cards, remote access to live CCTV feeds (if available), etc. Organizational leadership should always carry copies.
- Have a plan for sharing information with your local Fusion Center, the local FBI Field Office, and community-based security focused organizations for national awareness.

Become Familiar with the Characteristics of Hoax Threats and Protect Your Information Online

- Familiarize yourself with the characteristics of hoax emails – use of anonymous email services, vague threats and grand claims (e.g., *I will attack ALL schools, hospitals,* etc.). Bad actors may use publicly available contact information to submit their threats; for example, the *Contact Us* link or generic email address on your organization's website.
- Review the information on your online presence to prevent malicious actors from using personal information to conduct a swatting call or hoax threat. Consult with law enforcement and your security team to determine what public information could make you more vulnerable.
- Consider restricting or adding a delay of public livestreaming services.
- The FBI's Threat Intimidation Guide provides information on phoned and electronic message threats and is translated in 68 languages.
- See DHS OPE's Resources for Individuals on the Threat of Doxing, the Cybersecurity and Infrastructure Security Agency's (CISA) K-12 Anonymized Threat Response Guidance, and the FBI's Think Before you Post: Hoax Threats are Serious Federal Crimes.

SWATTING CALLS AND HOAX THREATS

DEVELOP OR UPDATE YOUR SECURITY PLAN

It is important to prepare for incidents by creating or updating a security plan for your organization. The CISA Security Planning Workbook provides a fillable form to guide planning and information sharing efforts. Additionally, the Office for Bombing Prevention has a Bomb Threat Management Plan and a wealth of information on bomb threat preparedness.

If you receive a threat, notify law enforcement immediately.

- Initiate your security plan and make internal notifications. Tell the 9-1-1 call taker how many buildings are occupied and how many personnel are present. Terminate any live stream broadcast if applicable.
- Save all emails, voicemails, and text messages you receive, and take screenshots or photos of comments on social media. See CISA's Swatting Prevention and Response Guidance for Election Workers and Law Enforcement for helpful information on what to do if you receive a threat.
- When responding law enforcement officers arrive, remain calm. Follow all instructions, keep your hands visible and answer questions to the best of your ability.
- Law enforcement will assess the situation and provide guidance regarding facility lockdown, search, and/or evacuation.
- Law enforcement need to know the locations of bathrooms, kitchen areas, storage rooms, stairs and exits. Provide floor plans and keys/codes as quickly as possible.
- Once the scene is secure, law enforcement will then initiate an investigation.
- If the threat originated online, law enforcement will need your personal or organization's IP address to conduct their investigation. If livestreaming, know who is accessing your meeting through IP addresses.

SWATTING CALLS:

When 9-1-1 receives a call reporting a threat of violence or a violent act is taking place at your location or institution, the responding law enforcement officers will treat the threat as real until they can determine it is a swatting call. If several law enforcement officers arrive at your location/institution unexpectedly, remain calm, keep your hands visible, and follow instructions.

SWATTING CALLS AND HOAX THREATS

After an incident

- Coordinate with responding law enforcement officers to provide updates to personnel and media if applicable.
- Hold post-incident follow up calls with institution leadership, security, and staff and initiate a prompt after action review.
- Connect with your local Fusion Center and FBI Field Office after the incident has concluded. This facilitates information sharing and national awareness with the FBI's Swatting Virtual Command Center – National Common Operating Picture to mitigate additional criminal activities associated with swatting and hoax threats.
- Conduct a post-incident after action review with law enforcement and staff. Identify and remove public information and update action plans. See CISA's Cybersecurity Resources for High-Risk Communities for resources and tools to help keep your online information secure.

If you need support connecting with your local law enforcement or Fusion Center, please contact the DHS Office of Partnership and Engagement at **NGOEngagement@hq.dhs.gov**.