Swatting and Bomb Threat Hoax Overview

Presented by:
Rhode Island State Police Lieutenant Nicholas Rivello
Rhode Island State Fusion Center Deputy Director John Soscia

Rhode Island State Fusion Center Mission Overview

The Rhode Island State Fusion Center (RISFC) is RI's primary intelligence and information-sharing center, as designated by the Governor in 2006. It is a state-level resource formed after 9/11 in partnership with USDOJ and DHS. The primary mission is to facilitate the efficient, timely, and accurate exchange of intelligence and information between local, state, and federal public safety agencies and private sector organizations. Through a cooperative and coordinated approach, the RISFC augments law enforcement operations by acting as a centralized, comprehensive criminal intelligence center to facilitate the exchange of criminal and threat information statewide. The RISFC collects, analyzes, and disseminates intelligence information to identify, investigate, and prevent activity relevant to terrorism and public safety. The RISFC operates under the oversight of the RI State Police, is co-located with the FBI-Providence Office, and is directly linked to the National Fusion Center Association, a robust network connecting 80 Fusion Centers nationwide.

What is Swatting?

- The action or practice of making a prank call to emergency services in an attempt to bring about the dispatch of a large number of armed police officers, to a particular address or location.

- Swatting has been around since the early 2000s. According to FBI statistics, between 2002 and 2006, there were more than 100 victims of swatting in 60 cities across the United States. The Bureau officially warned the public about swatting in 2008 as attacks grew.

Tactics associated with Swatting / Bomb Threat Hoaxes

- Swatting is typically carried out through the use of anonymous phone calls or online messages, using technologies that allow the perpetrator to mask their identity and location. There are several ways in which swatting can be made possible:

  Spoofing: The perpetrator can use a technique called "spoofing" to disguise their phone number or email address, making it appear as though the call or message is coming from a different location or person. This can make it more difficult for law enforcement to trace the source of the swatting threat.

  Hacking: In some cases, the perpetrator may gain access to the targeted individual's personal information or online accounts, allowing them to make more convincing swatting threats or otherwise harass the victim.

  Social Engineering: Swatters may use social engineering tactics to gather information about the victim or their location, using this information to make the swatting threat more convincing or to increase the likelihood of a law enforcement response.

  Collaboration: Some swatters may collaborate with others in order to carry out a swatting incident, such as by sharing information or coordinating the timing of the false report.
- Overall, swatting is made possible through a combination of technological and social factors and is often carried out by individuals with malicious intent and a desire to cause harm or disruption.

RISFC Key Points of Interest

- **Education/Awareness Training**
  - Responding to and Investigating Bomb Threats and Swatting Hoaxes, Provided by the FBI
  - Target audience: law enforcement, intelligence, homeland security, and school safety partners
  - Training provides attendees an overview of the realities of bomb threats and swatting hoaxes and includes a detailed review of statistics and current trends seen across the country. The training will also cover the characteristics of hoax calls, law enforcement best practices for assessment and response, and the decision-making process for evacuation or sheltering in place.
- **Information and Intelligence Sharing is Paramount**
  - **Timely** exchange of information
    - Expedient relay of details such as phone number/social media account used and actual message
  - RISFC and partners may be able to provide context and information on number used/message relayed
    - Routinely are seeing same or similar numbers and messaging (script) used
  - RISFC will relay information to partners such as: JTTF, LE Executives, SROs, Superintendents, RIDE, etc
  - This reporting will assist other agencies with similar events, identify trends, and enable further analysis.

Initial Response to Threats

Email Threat

- Save the email and DO NOT delete it.
- Print, photograph or copy the email.
- Obtain full email header data from the original email.
- Obtain IP address visitors logs to the website.
- Research all IP addresses to determine the telecommunications provider.

VIA Telephone/Swatting/VOIP/Skype

- Record call if possible.
- **Identify the number calling.**
- Document Date, Time and Duration of the call.
- Interview the recipient of call and identity if threat was made in person or by a pre-recorded voice.

SHARING the above information in a timely, accurate manner is key.

Questions?

Thank you for your participation.