FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

# Monthly Newsletter

December 2025
Volume 7, Issue 11

TLP:CLEAR

FB-ISAO Current Threat Level

FB-ISAO Physical Threat Level: ELEVATED

**FB-ISAO Physical Threat Level for US Faith-Based Organizations:** "ELEVATED."

FB-ISAO's definition of the Physical Threat Levels, "ELEVATED" means FB-ISAO is unaware of any specific events. Still, there is a concern that an event is more likely than normal.

**FB-ISAO Cyber Threat Level**: ELEVATED

FB-ISAO has assessed the general Cyber Threat Level for US Faith-Based Organizations as "ELEVATED."

FB-ISAO's definition of the Cyber Threat Levels, "ELEVATED" means FB-ISAO is unaware of any specific events. Still, there is a concern that an event is more likely than normal.

Board of Advisors

Contact Us

Email

Website

How to join

Join FB-ISAO Slack Channel

FB-ISAO Events page

## Winter Holidays

With December underway, we are reminded that these days bring about celebrations, recognitions, and bringing together groups at one time. These celebrations can also be key considerations for threat actors who may plan hostile events, or low-level harassment activities. Some considerations for planning and preparedness around these events include:

- **Form a (Security / Safety) Committee.** This can be very important for Houses of Worship that may not have a dedicated security staff or personnel. Everyone can have a role in security planning and preparedness. Resources:
    - CISA | Securing Public Gatherings
    - Mitigating Attacks on Houses of Worship Security Guide
- **Review or Build a Security Plan.** Review lessons learned from past events. This is an important activity that can help reduce the risk and reinforce success.
    - As noted in the Hostile Events Attack Cycle, many threat actors perform extensive research and planning for their attack. One unexpected change to their plan can disrupt their mindset and alter the attack.
- **Establish a layered perimeter security/review access control protocol.** This means finding ways to slow the attacker down before they can cause the most harm or impact.
- **Devise parking strategies to set up physical barriers from roadways (reduces risk of vehicle ramming).**
    - Vehicle Ramming Attack Mitigation – CISA
- **Ensure greeters/ushers are trained on suspicious activity indicators, encountering unknown persons, and reporting suspicious activity and incidents.**
    - The Power of Hello Houses of Worship Guide
    - CISA De-escalation pamphlet
- **Understand the threat and how to recognize suspicious behaviors.**
    - If You See Something, Say Something campaign.
- **Rehearse or hold an exercise to review the security plan and ensure all parties know their roles and responsibilities.**
- **Review and refine after incidents.** Conduct structured after-action reviews and update procedures based on response performance metrics.

# Event-Driven Scams

Threat actors are increasingly exploiting major world events to execute scams that merge social engineering, financial fraud, and ideological manipulation. **These "event-driven scams" exploit the public's emotional response to breaking news – including sympathy, outrage, or curiosity – to drive donations, clicks, and data exposure.** Essentially, malicious actors move quickly to capitalize on global attention cycles before fact-checking and law enforcement can respond.

For Faith-Based Organizations (FBOs), this creates both exposure and exploitation risks as they may become victims of brand impersonation or conduits for fraud through hijacked or fake donation campaigns.

**Examples of recent Event-Driven Scams:**

- Hurricane Melissa
- Gaza / Israel Conflict
- Death of Charlie Kirk
- ICE/Refugee-Themed Scams

Faith communities are uniquely susceptible to event-driven scam tactics because of their trust-based networks and mission-driven funding models. Small and mid-sized FBOs may lack formal cybersecurity or brand monitoring resources, making them soft targets for spoofing, cloned donation pages, and manipulated fundraising narratives. As actors increasingly blend financial scams with information operations, distinguishing legitimate calls for aid from malicious ones becomes critical to safeguarding both donors and institutional credibility.

Event-driven scams require an agile defensive posture combining digital vigilance, donor communication controls, and incident reporting. FBOs (especially small and mid-sized organizations without dedicated cybersecurity staff) can assume that major global events can trigger fraud attempts exploiting their brand, membership, or charitable identity. Some defensive considerations include:

- Monitoring domain registrations, social media pages, and search results for spoofed or cloned versions of your organization's name.
- Encouraging donors and members to verify URLs before contributing to any campaign, especially following major news events or humanitarian crises.
- Reporting fraudulent use of your organization's name or logo with your financial institution, web host, and law enforcement partners.
- Educating staff and volunteers on recognizing suspicious outreach, especially unsolicited offers to "partner" on relief campaigns or foreign donations.

## Spotlight: FB-ISAO Slack! You Need to Check it Out!

Volunteers tasked with leading security programs at their houses of worship could benefit from networking with others in similar roles. FB-ISAO Slack offers such an opportunity. On FB-ISAO Slack, members share Suspicious Activity Reports (SARs), resources, and ask questions.

Join today and experience the benefits of membership and increased resilience in 2026:

➤ Collaborate on FB-ISAO Slack

➤ Analytical and incident reports on security topics.

➤ Join live discussions and access our recording library

➤ Access community-centric and community-developed best practices.

## Thank you for sharing this newsletter with a friend!