Volume 3, Issue 12
December 2021

FB-ISAO Current Threat Level

FB-ISAO Physical Threat Level: ELEVATED

FB-ISAO has assessed the general Physical Threat Level for US Faith-Based Organizations as **"SEVERE."** As per FB-ISAO's definitions of the Physical Threat Levels, **"SEVERE"** means that an event is highly likely.

Please note that the Pandemic Threat Level has been lowered to ELEVATED.

FB-ISAO Cyber Threat Level: Guarded

FB-ISAO has assessed the general Cyber Threat Level for US Faith-Based Organizations as **"GUARDED."** As per FB-ISAO's definitions of the Cyber Threat Levels, **"GUARDED"** means FB-ISAO is unaware of any specific events, but a general risk of incidents exists.

Stories

FB-ISAO Newsletter

A Ransomware Sharing Experience

FB-ISAO works closely with members and trusted partners to maintain awareness of threats and incidents across our all-hazards environment. When it comes to cybersecurity, we work closely with partners to share potential threat information that could have implications to an organization. Each day, our team reviews alleged ransomware incidents for victims from our community, or third or fourth parties, that may impact our members. Additionally, we work closely with our friends and sponsors at Advanced Intelligence (AdvIntel) and Gate 15 to notify members of suspected activity that could be indicative of an imminent ransomware attack. Based on recent observations and Indicators of Compromise, there have been more frequent cyberattacks, particularly in the form of ransomware, on non-profits. Non-profits are especially vulnerable because of their limited resources and the fact that they often allocate those limited resources to activities that support their mission. Unfortunately, security of their assets is not typically a priority item for non-profits.

Last week, AdvIntel notified Gate 15 of several likely ransomware attacks. One of those affected was a Canada-based faith-based organization (a Chinese Christian church). FB-ISAO reached out to the organization to try to communicate the threat information with them. Regrettably, these conversations are often really difficult. Those non-members we reach out to sometimes suspect we're either attempting to sell them something or even that we're the attackers! In this engagement, those receiving the call attempted to direct us to the right person in the organization. Unfortunately, they told us the sole contact was out of office until after Thanksgiving and the only option was to leave a voicemail. We did that and offered to be available if there were any questions or concerns.

This resource can be a useful tool to educate on ransomware: https://www.cisa.gov/stopransomware/general-information. With ransomware, and other threats, quick response is often needed. We've been glad to have successful engagements where organizations received threat reports and took action to prevent attacks. Too often, that isn't the case. One of the lessons this recent effort reminds us of is the importance of having clear primary and alternate contacts and means for reaching them in an emergency situation. FB-ISAO members are encouraged to consider if they have clear communications protocols for cyber and physical security and to think if those contacts and procedures are clearly understood by those who are most likely to receive initial contact when someone calls or emails member FBOs. Continue reading…

FB-ISAO Advisory Board

Get to Know the Board of Advisors

Contact Us

Company Name
FB-ISAO

Email
Info@faithbased-isao.org

Website
www.faithbased-isao.org

Not Yet a Member of FB-ISAO?

How to join…

Not Yet on FB-ISAO Slack - You Need to Be!

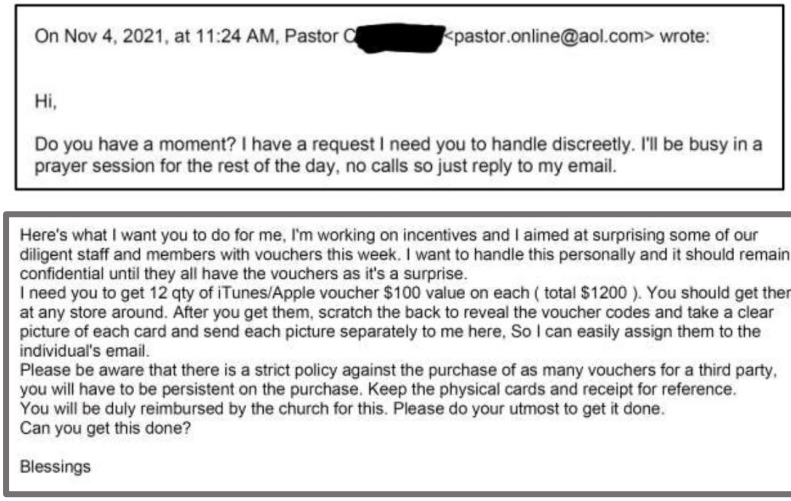
Write to membership

Upcoming FB-ISAO Events

Cyber Road Show	TBD (Join FB-ISAO to register)
National Counterterrorism Center Briefings	19 January, 16 March and 20 April (Join FB-ISAO to register)

Imposter Scams

Around 18 November, a member of FB-ISAO shared an incident that is becoming all too common - Imposter Scams. It is also important to note that FB-ISAO reported on a similar incident in a 15 April 2020 Security Advisory. For Faith-Based Organizations (FBOs), these incidents mean the scammer may attempt to portray a leader within a respective Place of Worship (POW). These are variations of other types of scams, but the general premise is scammers pretend to be a pastor, rabbi, priest, imam, or bishop. They're asking worshipers for gift card contributions for a worthy cause and appeals are often made by email, but they have also started showing up as texts and phone calls, too.



On Nov 4, 2021, at 11:24 AM, Pastor C[redacted]<pastor.online@aol.com> wrote:

Hi,

Do you have a moment? I have a request I need you to handle discreetly. I'll be busy in a prayer session for the rest of the day, no calls so just reply to my email.

Here's what I want you to do for me, I'm working on incentives and I aimed at surprising some of our diligent staff and members with vouchers this week. I want to handle this personally and it should remain confidential until they all have the vouchers as it's a surprise.
I need you to get 12 qty of iTunes/Apple voucher $100 value on each (total $1200). You should get them at any store around. After you get them, scratch the back to reveal the voucher codes and take a clear picture of each card and send each picture separately to me here, So I can easily assign them to the individual's email.
Please be aware that there is a strict policy against the purchase of as many vouchers for a third party, you will have to be persistent on the purchase. Keep the physical cards and receipt for reference.
You will be duly reimbursed by the church for this. Please do your utmost to get it done.
Can you get this done?

Blessings

Unfortunately, this is an all-too-common tactic, and an all too easy one for threat actors to develop. These types of scams are not going away any time soon. We encourage all FBOs to be up front and honest with members - the member who made the report has been subjected to quite a few of these from their POW, and the author's priest has also spoken up during announcements to give a quick security warning to members reinforcing the central premise - they will NEVER ask for support from members in this way. You can read about some dos and don'ts for these types of Imposter Scams here.

FB-ISAO grows stronger through information sharing instances such as this. If you have been subject to this or any type of security event, reach out to FB-ISAO and share with the community.

Spotlight: Engagement

2021 continued to be a challenging year for the Nation and for the community of faith. Due to the on-going pandemic, worship, and other faith-based programs have not been the same.

FB-ISAO has continued to engage the community by providing members with **information**, **analysis**, and **capabilities** to help **reduce risk** while enhancing **preparedness, security, and resilience**. We have done this across faiths and to encompass all-hazards. We have grown through members engagement!

Force Multiplication: In 2021, we saw conversations between members take shape and deepen. Members become a resource to one another - read this post.

Stronger Together: Members collaborated on events and programs that provided information, resources and capabilities that have strengthened the community as a whole.

We thank you for being a part of FB-ISAO and for contributing to the community in the way that you do! We look forward to 2022 as we continue to grow and mature the ISAO - together with you!