Volume 3, Issue 11
November 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

Vigilance and De-Escalation

Houses of worship are meant to be welcoming to all. In fact, sometimes, houses of worship can be a place of refuge from all sorts of things including natural disasters and civil strife such as protests. With the approaching holiday season, some houses of worship might see some unfamiliar faces that are seeking to connect to their faith. To provide that refuge while keeping their facilities safe, houses of worship might consider becoming familiar with and training to recognize the warning signs of someone on a path to violence; assess if the situation or person of concern is escalating, or if an emergency response is needed immediately; de-escalate the situation currently taking place through purposeful actions. Knowing when to report suspicious behavior to the authorities is also an important component of keeping the facilities safe yet welcoming.

There are a few tools available to front-line staff such as members of a security team, or greeters and ushers that can help.

The *Employee Vigilance Through the Power of Hello* (and the Faith-Based version of the same) help critical infrastructure owners, operators, and staff identify and navigate suspicious activity or potentially escalating situations to safely dis-engage and report to local law enforcement or their organization's multi-disciplinary threat management team.

Observe: Stay vigilant of your surroundings
Initiate a Hello: Acknowledging a risk can deter a potential threat.
Navigate the Risk: Navigate the risk by asking yourself if the behavior you observed is threatening or suspicious.
Obtain Help: After navigating the risk, obtain help from management or authorities.

The *De-Escalation Series for Critical Infrastructure Owners and Operators* is as a four-product series to help critical infrastructure owners, operators, and employees:

Recognize the warning signs of someone on a path to violence.
Assess if the situation or person of concern is escalating, or if an emergency response is needed immediately.
De-escalate the situation currently taking place through purposeful actions, verbal communication, and body language.
Report the situation through organizational reporting to enable assessment and management of an evolving threat, and 9-1-1 for immediate threats.

Vigilance and De-Escalation are possible methods to prevent potential violence and have been incorporated into previous FB-ISAO reporting. The Cybersecurity and Infrastructure Security Agency (CISA) further advises that "individuals are encouraged to use purposeful actions, verbal communications, and body language to calm a potentially dangerous situation."

Your safety and the safety of others is the highest priority. Maintain a safe distance and avoid being alone with an individual who is combative or potentially violent. If there is a risk of imminent violence, remove yourself from the situation and seek safety.
Know your limits. Keep in mind that some individuals may be more adept in applying these techniques. Know your own vulnerabilities and tendencies and recognize that sometimes the best intervention is knowing when to seek additional help.
Obtain Help. If you feel the individual or situation is escalating and violence may occur, call for help from your security staff or local law enforcement and move yourself to a safe location.

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

Monthly Threat Brief (re-scheduled from October)	16 November
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)

Holiday Travel Cyber Tips

The holiday season is almost upon us. With that comes faith-based observances and celebrations, and of course the lucrative shopping season. This is also a time of year when families travel to see relatives and friends or take time from the daily grind for a family vacation. And all along the way, it is highly likely that mobile devices will be with many of those individuals taking part in everything the season has to offer. Unfortunately, this time of year also brings out cybercriminals and threat actors who are looking to disrupt the cheer and goodwill for their own motives. For individuals and Faith-Based Organizations (FBOs) it is important to stress mobile device security and the impacts it can have on themselves and their organizations.

This is important for individuals and organizations as an attacker may be able to infect any device with a virus, steal your phone or wireless service, or access the data on your device. So, these activities have implications for your personal information, as well as the potential for serious consequences if the user stores corporate information on the device. Simple access to the device could also allow uninvited actors into an organization's network.

Holiday Traveling with Personal Internet-Enabled Devices. While this Security Tip was developed in 2011, the guidance is still very much applicable today.

Know the risks. Your device can operate as a full-fledged computer. The mobile nature of these devices means that you should also take precautions for the physical security of your device (see Protecting Portable Devices: Physical Security for more information) and consider the way you are accessing the internet.

Do not use public Wi-Fi networks. Avoid using open Wi-Fi networks to conduct personal business, bank, or shop online (see threat above).

Turn off Bluetooth when not in use. Cyber criminals have the capability to pair with your phone's open Bluetooth connection when you are not using it and steal personal information.

Be cautious when charging. Avoid connecting your mobile device to any computer or charging station that you do not control, such as a charging station at an airport terminal or a shared computer at a library. This connection could allow software running on that computer to interact with the phone in ways that a user may not anticipate. As a result, a malicious computer could gain access to your sensitive data or install new software.

Don't fall victim to phishing scams. If the deal looks too good to be true, or the link in the email or attachment to the text seems suspicious, do not click on it! An adage you may use, 'If you have to click, it's [most likely] not legit.'

What to do if your accounts are compromised:

- Call the bank, store, or credit card company that owns your account. Reporting fraud in a timely manner helps minimize the impact and lessens your personal liability.
- Change your account passwords for any online services associated with your mobile device using a different computer that you control.

Spotlight: Monthly Threat Brief

On 16 November, the Monthly Threat Brief (MTB) will address the topic of DRONES. Please sign-up here. After that session, the MTB is taking a break until 2022. Please look for an email from Ed Heyman, the Co-Chair of the Operational Resilience Group. The email will contain a survey which is intended to solicit feedback from you, our members, on all things MTB! We want to continue to deliver a program that is useful and helpful to you as you work on your resilience and preparedness initiatives. The email will go out from our secure portal.