Volume 5, Issue 5
May 2023

TLP:CLEAR

FB-ISAO Current Threat Level

FB-ISAO Physical Threat Level:
Guarded

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 Guarded.

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

Staying Safe On-line While 'Away'

As the COVID-19 pandemic public health emergency ends on 11 May 2023, more and more people are venturing out to attend work related events or to travel for leisure. That means that we will all spend time 'away' form our workplaces and our homes. Whether you are working remotely, traveling through the airport, staying at a hotel, attending a conference, or chilling at your local pub or coffee shop, publicly/freely available open Wi-Fi is super convenient. However, if the public Wi-Fi network isn't secure, other users on the network may be able to see what you see and send.

It is important to stay safe while on-line and 'away', so consider some safe options for staying connected.

- ✓ **Select a public Wi-Fi with at least some security and confirm you are on the correct network.** Threat actors create similar Wi-Fi network names as legitimate networks to trick us into connecting so they can steal our information. Confirm you have the correct network by asking the business hosting the Wi-Fi for the name and the password. If the business doesn't at least secure the connection with a password, consider not using it at all.
- ✓ **Use a virtual private network (VPN).** When using public Wi-Fi can't be avoided, use a VPN. VPNs encrypt your traffic and make it unreadable to snooping. Likewise, if you are connecting to a public Wi-Fi to access your work network or work-related resources, your FBO may REQUIRE you to use a VPN. It's even a good idea to use a VPN when you're on your home Wi-Fi.
- ✓ **Don't enter passwords or other private information.** Be mindful of the data you're sharing when connected to public Wi-Fi. Avoid doing anything that involves sharing sensitive information such as usernames, passwords, financial information, and work-related communications. If login, registration, or credit card details are required, use your mobile data instead, or wait until you're on a secure private network.
- ✓ **Disable file sharing.** Avoid or limit file sharing and AirDrop. If you leave sharing enabled over public Wi-Fi you're giving bad guys easy access, especially if you connect to the wrong network. Disable sharing before you leave the house or office.

The best solution when you need to connect is to consider using your mobile data instead of Wi-Fi by turning your smartphone into a hotspot and tethering your laptop or other non-cellular device as needed. Tethering is most secure via a USB connection, but if you choose to connect using your smartphone's Wi-Fi, establish a strong password so no one can gain access without your permission.

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

Office Hours. Meeting Invitations sent to all members via email.	Every Tuesday at 1:00pm ET
Coaching Session: How We Can Make a Difference	17 May at 2:00pm ET
2023 Educational Series: A Culture of Security	Monthly, the first Wednesday of each month at 12:00pm ET

Attacks on Faith-Based Organizations

The Faith-Based Information Sharing and Analysis Organization has been tracking hostile events since the early release of the Dobbs Ruling on 03 May 2022. In addition, the FB-ISAO issued multiple analytical reports on the topic. Members of the FB-ISAO shared open-source posts related to protests, threats, and attacks on both pro-life and pro-choice organizations. However, since at least 2020 faith-based organizations were frequently targeted by protesters. Hostile events that were most frequently encountered include arson; graffiti (most often with pro-abortion messages); rocks and bricks thrown through windows; statues destroyed (often with heads cut off); thefts and general property destruction.

In late 2022, the FB-ISAO partnered with the Patrick Henry College's (PHC) Strategic Intelligence Program to develop more in-depth analytic reports based on data sets of the hostile events that multiple interested organizations have released as open-source data sets.

The collaborative reports include an executive summary and information related to:

- Attack Timeline on Pro-Life Institutions
- Distribution of Attacks on Pro-Life Institutions
- Attacks by Organizations
- Attack Types & Watchwords Associated with Attacks on Pro-Life Institutions
- Attacks on Pro-Choice Clinics

To read the entire post, follow this link.

To receive the TLP:GREEN reports, please join our vibrant community of security practitioners who are working hard to secure their own faith-based organization and who are also contributing to securing the community of faith as a whole. Membership information is available here.

Spotlight: Information Sharing Community of the National Capital Region

Members of the FB-ISAO Information Sharing Community (ISC) in the National Capital Region are just plain awesome! They readily share valuable resources, Suspicious Activity Reports, and intelligence reports. In doing so, members have reduced their risk while enhancing their preparedness, security, and resilience.

Information Sharing Communities are private channels for members with interests in specific geographic areas to easily collaborate and share information with one another. Members can request an ISC for their community. Learn more here.