FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

Best Practices for Securing Your Streaming Services

Streaming the services for your house of worship has many benefits, such as reaching others from far away, serving those who are homebound, overcoming space limitations, and recording services. Along with the convenience lurks a shadow of vulnerability. Houses of worship need to be concerned about more than serving their congregants; they also need to be concerned for about the privacy and security of their congregations.

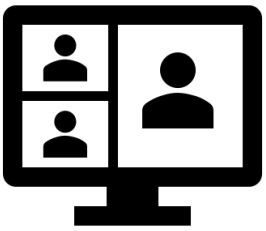
Did You know?

On-line trolls can infiltrate streaming services to insert material that is lewd, obscene, or racist in nature, typically resulting in the shutdown of the session.

The following are some foundational actions to take to better secure your streaming services:

- **Set the tone**: Educate meeting participants on best practices for video conference etiquette, rules of engagement, security, etc. For example: "Don't sharing meeting links publicly", "Be cautious of unexpected attendees", or even "Anyone not following the rules will be disconnected."
- **Require Meeting Passwords**: Require participants to enter a password to join.
- **Beware of**:
  - **Malicious links in the chat**: Attackers can trick participants into clicking on malicious links shared via the chat, allowing the attackers to steal credentials.
  - **Stolen meeting links**: One way to avoid issues of stolen links and unauthorized access to meetings is to turn on notifications that will let you know when someone has joined your meeting room without you.
  - **"Zoombombing"**: Zoombombing (aka Zoom raiding) is the unofficial term for uninvited individuals disrupting webinar meetings with inappropriate content or behavior.
  - Outdated software: Make sure your video conferencing software is patched with the latest vendor-provided updates and have automated upgrades turned on.
- **Who has access?**
  - Remove access, including admin privileges, when someone no longer needs it
  - Pick a regular time (e.g., every 3 months) to review who has access (old accounts can pile up fast!).
- **Use Waiting Rooms**: This feature allows the host to control which participants can join the meeting and when.
- **Use Restricted Screen Sharing**: Limit screen sharing to the host or designated participants.
- **Disable Join Before Host**: Turn off the "Join Before Host" setting to ensure that the meeting host is present before participants can join.
- **Enable Participant Muting**: Allow only hosts or designated participants to unmute themselves.
- **Report Suspicious Activity**: Report suspicious activity to your resident expert or IT/Security and team(s). If necessary, reach out to the vendor for the best way to report suspicious activities. If you encounter threats, report them to your local law enforcement.
- **Patch**. When a patch is available from the vendor, take the time to apply the patch.
- **Get downloads from the vendor**. When downloading the app or a patch, go to the vendor site. Beware of non-vendor sites which may have a download link on their page that could have a corrupted version of the software or contain malicious code.

FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION



Here's guidance for some of the more popular video conference and meeting tools.

- Facebook Live:
  - https://www.secure.facebook.com/business/help/216491699144904?id=1123223941353904
- Google Meet:
  - https://support.google.com/meet/answer/9852160?sjid=4356512316615521955-NC
- GoToMeeting:
  - https://support.goto.com/meeting/help/tips-for-staying-secure-using-gotomeeting
- Webex:
  - https://help.webex.com/en-us/article/8zi8tq/Best-practices-for-secure-meetings:-hosts
- Zoom:
  - https://www.zoom.com/en/products/virtual-meetings/resources/securing-your-meetings/

If you need assistance, you can:

- Ask your local tech guru.
- Post a question in the FB-ISAO Slack **general** or **ask-me-anything** channels.

Stay safe!

This product was developed by the FB-ISAO Cyber Threat Intelligence Working Group.
Get involved! Write to membership@faithbased-isao.org.