FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

Securing Your Social Media Accounts

Social media is an enormously powerful tool for houses of worship - we can connect with members, share messages, and reach new audiences.

Did You know? Because social media encompasses so many platforms and considerations, there are numerous considerations.

- Every opportunity for engagement brings challenges. From protecting a congregation's privacy to safeguarding an organization's reputation.
- Securing those social media accounts is necessary for maintaining trust and fostering a positive digital presence.

Here are some important tips on keeping your social media accounts safe:

- **Strong Password**
  - Use strong, unique passwords for each of your social media accounts. What does "strong" mean? Strong passwords are at least twelve characters long and include a mix of letters, numbers, and special characters. A complex 8-character password can be cracked in 4 hours; a simple one, instantly. And consider using a password manager to keep track of them (the average number of passwords per person? 168).
- **Enable 2FA/MFA**
  - Whenever possible, add that extra layer of security provided by 2FA/MFA (two-factor authentication/multi-factor authentication, respectively). Sometimes, this isn't possible because many organizations have shared accounts. But, 2FA/MFA is a great way to help keep accounts from being taken over.
- **Monitor Account Activity**
  - Keep an eye on your social media accounts for any unusual activity, like unrecognized login locations or unauthorized posts. If you notice anything suspicious, change your password immediately. Maybe even remove offenders (it's a tough but necessary action.)
- **Report and Block Suspicious Users**
  - Don't hesitate to report and block users who behave inappropriately or seem suspicious. Those who are causing trouble publicly may choose to cause trouble privately by trying to get into your accounts. A social media policy for your house of worship will help guide moderators regarding what to look for and appropriate actions to take. Here are links to some popular social media sites about how to report problems:
    - Facebook
    - Instagram
    - X (formerly known as Twitter)
    - YouTube

- **Review Security and Privacy Settings**
    - Ensure that your house of worship's social media pages and groups have the appropriate privacy and security settings. Take control of who can see your posts, profile information, and friend list by reviewing and adjusting your privacy settings. Here are the privacy settings for:
        - Facebook
        - Instagram
        - X (formerly known as Twitter)
        - YouTube
- **Use Official Accounts for Communication**
    - Encourage the use of official social media accounts for all public communications rather than personal accounts of staff members. This helps maintain control over the content and prevents confusion or misrepresentation.
- **Create and Enforce a Social Media Policy**
    - Develop a clear social media policy for your staff, volunteers, and members. This should outline guidelines for what can be shared, how to respond to comments, and what type of content aligns with the values of your house of worship.
- **Think Before You Share**
    - Be mindful of the information you share online. Information such as PII (personally identifiable information), photos, off-site plans and locations, security information - an adversary, regrettably, can and will use any and all available information (aka, intel) to lure, exploit, or otherwise target individuals and organizations.
- **Manage Content and Crises**
    - Content
        - Assign trusted staff or volunteers to monitor and moderate social media accounts regularly and implement a clear social media policy outlining what content is appropriate and who has posting authority.
    - Crises
        - Content and Crises on social media go hand-in-hand. It's way too easy for a simple message – intentionally or not - to start trouble. Have a plan in place for handling negative comments, online harassment, or crisis situations. This includes identifying who will respond, how to address the issue, and when to escalate it to higher leadership.

Start small, but it's important to take the next step.

FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

If you need assistance, you can:

- Ask your local tech guru.
- Post a question in the FB-ISAO Slack **general, #g_cti, #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.