FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

The Art of Defense: How to Secure Your Site Effectively

Your organization may rely heavily on its website, even if it's just used as a digital business card, and may need to remain available 24/7/365. Sure, there are internet outages that occur, leaving your website unavailable, but things like that are out of our control. We need to do our part to ensure our sites stay up and working.

Most threat actors are financially motivated - they're out to make lots of money, so they will target huge organizations. Others may have political, social, monetary or religious motives. Some can't be tracked or anticipated from crime to crime, and they attack simply because, as Alfred said in the Batman movie, "they want to watch the world burn." So while many FBOs may not have large monetary and intellectual property reserves, they still may be targets of hacktivists.

Did You know? Some of the more common attacks faced by FBOs are:

- DDoS (Distributed Denial of Service),
- Website defacement
- Stealing and Sharing Data (often to name-and-shame).

While one doesn't know when cyberattacks will happen, here are 10 aspects of site security that may prevent many, and lessen the severity of those attacks *(These don't all apply to everyone, but the more we know, the safer we are)*:

- **Regular Software Updates.**
  - Keep your website's Content Management System (CMS), plugins, themes, and server software updated. Outdated software is vulnerable to attacks.
  - Did you know? The most popular CMS is WordPress (I'm actually about to get it up-and-running because our church is changing location and name, so this article is for me, too!) 472 million websites use WordPress, which is 43.5% of all the websites on the internet.
- **Strong Access Control (Passwords and Two-Factor Authentication (2FA.))**
  - Not only should those who administer your site use strong, unique passwords and 2FA, but you should also regularly check to make sure that those who can access it are the right people.
- **Web Application Firewall (WAF.)**
  - Use a WAF to filter and monitor HTTP traffic between the website and the internet. It will help block malicious traffic.
- **Security Monitoring and Scanning.**
  - Regularly scan your website for vulnerabilities using security tools or services. Monitor for unusual activity.
- **Security Awareness Training.**
  - Educate your staff on best practices for website security, such as recognizing phishing attempts, using secure passwords, and handling sensitive data properly.
- **Use a CDN with DDoS Protection.**
  - Employ a Content Delivery Network (CDN) that offers Distributed Denial of Service (DDoS) protection. This helps mitigate attacks that aim to overwhelm your website with traffic.
- **Implement Rate Limiting**.

FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

  - Set limits on the number of requests a user can make in a certain time period to prevent brute force attacks and resource exhaustion.
  - Grant access to sensitive data such as donation records and financial information solely to authorized personnel within your congregation on a need-to-know basis.
- **Use Secure Coding Practices.**
  - Ensure that any custom code written for your website follows secure coding practices, such as input validation, output encoding, and proper error handling.
- **Perform Regular Security Testing.**
  - Conduct regular security audits and scans (and, if possible, penetration testing) to identify and address potential vulnerabilities before attackers can exploit them.
- **Enforce Secure File Uploads**.
  - If your website allows file uploads, ensure they are securely handled. You don't want someone to upload a file that has malware or is destructive. This helps avoid attacks such as SQL Injection, or other types of injection where someone can access your data via brute force.
- **Utilize Website Security Software**.
  - Bonus: All the details of site security can be overwhelming, so there are software options that can help. Some of the common ones include ShieldPRO and BulletProof Security that offer a suite of protections.

These *Low Cost/No Cost but High Impact* steps will help FBOs build a strong foundation for website security, protecting their property, privacy, reputation, and their parishioners from potential threats.

You don't have to do it all at once - pick one improvement and work on that.

You might have questions like, “What’s a good security tool for scanning the site?”, “Where can I get good security education training?”, or “How can I get a web application firewall for my website?”

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.