FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

Best Practices for Securing Your Donation Sites

Many Faith-Based Organizations use online donation / giving sites where they can collect dues, tithes and other gifts. These types of tools enable members of the congregation to give securely from anywhere, at any time. They may include features such as secure payment processing to accept donations via credit/debit cards, ACH transfers, and mobile wallets, recurring giving that helps set up automated contributions, customizable donation forms to collect specific information from donors, donation tracking to provide donors with contribution summaries for tax purposes, and communication tools to send thank-you notes to donors.

Did You know?

When Choosing and Using an Online Donation Platform. Usability is important, but did you know that security is paramount?

The following are some foundational actions to take when setting an online donation site capability at your Faith-Based Organization:

- Use a secure payment gateway (technology used by merchants to accept debit or credit card purchases from customers.)
    - Using a reputable and secure payment gateway like PayPal, Stripe, or Authorize.net to handle your online payment processing, despite the fee those services charge, can alleviate many burdens on the organization since these gateways use encryption and comply with credit card industry security standards to protect sensitive the financial information of your donors.
- When creating your donation web forms, consider using security measures such as:
    - CAPTCHA.
    - Password strength requirements.
    - Two-factor authentication (MFA) using a reputable tool to prevent automated attacks and unauthorized access. Learn more about MFA.
- Keep your website up to date with the latest security patches and fixes by regularly updating your website's software, including:
    - The content management system (CMS.) A CMS is software that helps users create, manage, store, and modify their digital content. This all-encompassing system is a one-stop-shop to store content—such as apps, images, and websites—in a user-friendly interface that is customizable to an organization's needs and their employees.
    - Plugins. Plugins are essential for customizing your website without editing code. They add all kinds of features that will make your website more dynamic and functional.
    - Extensions. Extensions control how websites load and behave, and they can add extra features to your browser.
- Install a website firewall to prevent access to your site's code and data from being manipulated or stolen. A web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. Many web hosting providers offer firewalls as part of their service.

FB-ISAO
FAITH-BASED INFORMATION SHARING & ANALYSIS ORGANIZATION

- Avoid storing PII (Personal Identifiable Information) such as credit card data on your site. Secure Payment gateway services (see above) are typically set up to be responsible for the protection of donor data. If in doubt, please ask your provider.
- Limit access to sensitive data.
    - 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.
- Employ a backup solution that automatically and continuously backs up your business-critical data and system configurations. Use on-site and remote backup methods to protect vulnerable information. Make sure the backups are encrypted and tested to assure they are usable. You can use this data to recover in case of a security breach, system failure, or data loss.
- Use secure hosting.
    - Host your website with a reputable and secure hosting provider that offers robust security measures, such as firewalls, malware scanning, and regular backups.
- Monitor and review logs.
    - Assign someone in your organization to regularly monitor and review your website's logs for any suspicious activity or potential security breaches.
- Provide clear privacy and security policies.
    - Communicate your privacy and security policies to your donors, outlining how their personal and financial information will be protected and used in order to set expectations and give them a sense of security.
- Use SSL/TLS encryption on your website.
    - Install an SSL/TLS certificate on your website to ensure that all data transmitted between the user's browser and the server is encrypted. Many web hosting providers will offer this service for an additional cost.
    - Regularly renew the certificate so it is up-to-date and valid to help protect sensitive information like credit card numbers and personal details from being intercepted in transit.

The best practices outlined above should be regularly reviewed and updated as technology best practices change in response to the threat environment.

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.

TLP:CLEAR