Keep Your Content Management Systems (CMS) Up to Date & Websites Secure

Practice:

Your nonprofit hosts a website using a common server platform and CMS, such as WordPress, Drupal, or Joomla on Linux or Windows, and you haven't updated the software or related plugins in several months.

Why It Is Risky:

The developers that support these server and CMS platforms regularly publish security updates to remediate the latest vulnerabilities. If you don't update your website's software, you could become the target of hackers who can exploit the vulnerabilities, which could result in you being hacked or flagged by Google's search results as a potentially harmful website that warns off or even harms potential visitors.

What You Can Do:

Consider making a backup of the site and updating the CMS and plugins on a regular schedule, or working with your vendor to help you update your CMS. Ensure administration interfaces (/admin, ssh, remote desktop) are restricted to trusted IP addresses only. Protect domain registrar (GoDaddy, Network Solutions, Namecheap, etc.) and Domain Name System (DNS) & web hosting provider accounts with strong, unique passwords, registrar locking, and 2-factor authentication.

Limit the Number of User Accounts You Have & Ensure Passwords are Updated as You Experience Turnover

Practice:

Your nonprofit's website has user accounts for volunteers or employees/third parties who provide web management services who may no longer require the access or work there. Your Executive Director has a user account with the highest security permissions, but isn't logging into the site to make updates.

Why it is Risky:

These accounts can be leveraged by a disgruntled employee/third party or used to hack access to your website's administrative functions (see above recommendation to restrict admin access).

What You Can Do:

Implement a process to disable user accounts that are no longer needed and grant permissions to staff members that are consistent with what they actually need and will use. For example, your CFO may only post once a month to update information on the status of the latest giving campaign, so grant access to publish that kind of content. Configure your CMS to require more secure passwords and don't reuse those passwords for other business functions, such as online banking or social media. Consider a password storage tool that does not have the ability to decrypt customer data.

Do Not Request Personal Information via Unsecured Forms

Practice:

Your nonprofit's website includes a volunteer application form with a field for a Social Security Number and a donation form with the name, credit card number, and address of the donor, or optionally an attachment. The forms are sent unencrypted over standard http:// (no lock icon). Or maybe the data is stored in the publicly-accessible section of your website so that anyone with the URL can access the data.

Why It is Risky:

Your donors, volunteers, and supporters count on you to keep their information safe. In addition, you can expose your organization to legal liability and if credit card data is not stored correctly you can even be subject to fines from the major credit card companies. Accepting attachments from anonymous sources can allow delivery of malware into your environment.

What You Can Do:

Stop collecting data your organization doesn't need - you may be better off collecting the data necessary for a background check, or to prepare donor acknowledgment letters via a secure method later on in the process. Also, consider why you are asking for the data in the first place and whether or not it is even necessary. Add https capability to your website and use it to secure all online forms, especially file attachments. Consider restricting file types and evaluate all submissions prior to opening, and requiring a login to upload files. You can check with your website vendor for assistance. In addition, if your organization processes online donations without a third-party vendor to manage payments in a compliant fashion, you may run afoul of Payment Card Industry (PCI) compliance requirements, subjecting your organization to potential legal issues.

Read the PCI for small business website for more information: pcisecuritystandards.org/smb.

A Couple of Final Reminders:

- Never click on suspicious links within comments left by visitors to your site. You could end up with a virus or malware that may affect your computer, and possibly others on your network.
- Access sites using Google instead of typing the domain name. This adds the benefit of Google's malicious website protection.
- Back up your website's files and database regularly.
- Check with your hosting company for recommendations, and consider keeping your files on an external hard drive that is disconnected from the network and stored in a safe location, such as a safe deposit box.