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

### Practice:

Your business 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 business' website has user accounts for volunteers or employees or third parties who provide web management services who may no longer require the access or work there. Your Executives have 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 employees or third parties 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.