Published on National Council of Nonprofits (https://www.councilofnonprofits.org)

Original URL: https://www.councilofnonprofits.org/articles/keeping-your-nonprofits-website-and-data-secure

Keeping Your Nonprofit's Website and Data Secure

By: Rick Cohen

As we mentioned in the July edition of *Nonprofit Knowledge Monthly*, cybersecurity will be an ongoing theme as cyber attacks and ransomware continue to create challenges for businesses, governments, and nonprofits alike. Each month, we'll be featuring a couple of quick things your nonprofit can do and highlighting additional resources. This month, we're focused on the security of your website. Here are a couple of actions your nonprofit can take now to keep its data safe.

Follow the principle of "least privilege access"

Redundancy is important. Shared responsibilities are helpful. But the more people with administrative access to your data, the more vulnerable it is. Your organization should set permissions that allow only as much access as needed for someone to do their work. On your website, that means only certain people have editing privileges or ability to see the overall administration options. For your data, it means that (for example) program staff wouldn't have access to financial information and finance staff wouldn't have access to casework files. If a breach occurs, it means a smaller amount of data is able to be accessed by the hackers. An added benefit of least privilege access is that it streamlines the experience for your team. Fewer options to

navigate makes it easier to find what a person actually needs to do their work.

Keep up-to-date with security updates

Just like your computer needs (seemingly never-ending) Windows updates, your website needs regular updates to remain secure. Whatever content management system (CMS) your website is built on, there are likely regular security updates being released as vulnerabilities are discovered and fixed. Even more vulnerable than the CMS itself are the plug-ins, modules, and extensions that provide added functionality to your website, but can have less rigorous security testing before rolling out. You can do a quick scan of your site with a tool like Securi, but the best way to monitor for updates is to regularly check for status updates in your CMS admin console. Most of the top content management systems also have mailing lists you can sign up for to be alerted when there are new updates to install.

For more cybersecurity tips, see:

- Steps to Keep Your Site Clean: Updates (Securi blog)
- Cybersecurity for Small Business (Federal Communications Commission)
- 5 cybersecurity tips for your small business (GoDaddy blog)