FOR PURPOSE LAW GROUP
A Professional Law Corporation

NONPROFITS: GENERAL INFORMATION

Alert About Your Nonprofit's Website

09.19.18 | Linda J. Rosenthal, JD

“If it isn’t one thing, it’s another.”

— Popular idiom recognized as true by most people on Earth

Now that you’ve come to grips with, and accept, that every computer on the planet is likely to be hacked sooner rather than later, and now that you understand that the new General Data Protection Requirements (GDPR) from the faraway European Union may affect you, there’s something else you need to know about – and handle – as soon as possible.

It’s an important change in the latest version of Google’s Chrome, the world’s most popular web browser. And what happens in Chrome will not long afterward show up as a feature of the other web browsers like Mozilla Firefox and Internet Explorer.

In a nutshell, here it is: Websites that use the prefix “https” will be designated as secure, but sites that still use the prefix “http” will be flagged as insufficiently secure.

Background on the Website Prefixes

If you’re like us, you’ve probably briefly wondered about – but never lost any sleep over – why some websites have the prefix “http” while others use “https.” In the early years of the internet, most sites used the prefix “http.” In recent years, the “https” alternative has become more commonplace, though.

The helpful folks at howtogeek.com explain why:

HTTPS, the lock icon in the address bar, an encrypted website connection—it’s known as many things. While it was once reserved primarily for passwords and other sensitive data, the entire web is gradually leaving HTTP behind and switching to HTTPS.

The ‘S” in HTTPS stands for ‘Secure’. It’s the secure version of the standard “hypertext transfer protocol” your web browser uses when communicating with websites.

For a deeper dive into the specifics of how and why the "https" sites are more *secure,* read further on at *HTTPS is and why it's important and* A secure web is here to stay, for example.

"In the past, when a nonprofit wanted to assure a donor that its website was secure, the nonprofit could suggest that the donor look for the little "lock" icon in the address bar which confirms that a site is using HTTPS. Because of this, using HTTPS was akin to a bonus point in the nonprofit's favor."

But change was brewing. About three years ago, Google told the computer-nerd community that at some point in the future, Google Chrome would be changed so that any websites not using the "https" prefix would be flagged as insecure. The change was delayed to give website owners a chance to make the necessary adjustments.

In the years since then, Google has "helped users understand that HTTP sites are not secure by gradually marking a larger subset of HTTP pages as 'not secure.

On February 8, 2018, Google issued the notice titled "A secure web is here to stay," explaining that Google had been moving "toward a more secure web by strongly advocating that sites adopt HTTPS encryption." And, beginning in July 2018 with the release of Chrome 68, Chrome will mark all HTTP sites as "not secure." On schedule, Google rolled out the latest version of its Chrome browser over the summer. Now, the new programming will automatically flag any website not using the HTTPS security standard as "not secure."

An article dated July 24, 2018, by a techy nerd at CNET explains this important Google change, effective that day: "Chrome's long-promised HTTP 'not secure' website warnings arrive." He includes a reassuring caveat, though: "Take note if you see the warning, but don't panic."

A More Secure Website

Ok. We won't panic.

In early August 2018, the National Council of Nonprofits issued a post titled: New website security warnings raise the bar for nonprofits:

> *Nonprofits need to take notice that Google just raised the bar when it comes to demonstrating a website is secure. Failing to make changes to comply with the new standards can hinder your nonprofit's ability to interact with the public, including potential clients and donors.*

If this message appears on your site, does it mean that your site is *not* secure or that any information entered on it by your supporters, donors, and constituents is now at risk? "Not necessarily."

The precise significance of a website not using the prefix "HTTPS" is that it fails to meet the "best practice standards that Google is now enforcing."

What if a nonprofit never asks anyone to enter data or personal information on its website: does any of this matter? Not really, but the move to the "HTTPS" is a good idea, anyway. In particular, it "matters for SEO, it will score higher in search results." And it's not a good practice to give visitors to your website any reason at all to be wary about proceeding or about interacting with you in any way.

Conclusion

To change a website address that still begins with "http," contact your IT department or website support consulting firm. "Any respected web host should be able to easily make this change. Some may charge you for the required SSL certificate. You can also get an SSL certificate at a significant discount via TechSoup. For more technical users, check out this guide on how to quickly add HTTPS to your site. Another great resource on this comes from Aespire, “Safe and Secure: Creating a Trusted Web Experience.”