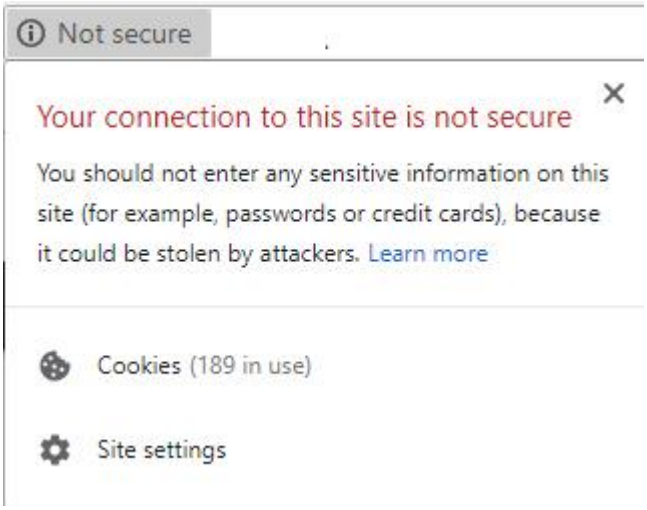
New website security warnings raise the bar for nonprofits

By: Rick Cohen

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.



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 now, that standard has been flipped upside down with the news that the latest version of Google's Chrome web browser will flag any website not using the HTTPS security standard as "not secure." Now, a message like the one next to this paragraph will be displayed at the top of any browser bar on Chrome for websites not using HTTPS. (We won't get too deep into tech-speak in this post, but if you are interested in learning more, we recommend this article about what HTTPS is and why it's important.).

What does this mean?

Does having this message appear mean your site isn't secure or that information entered is automatically at risk? Not necessarily. But if the site isn't using HTTPS, it is no longer meeting the best practice standards that Google is now enforcing. Other browsers, such as Firefox and Internet Explorer/Edge are likely to follow.

And, as they say, perception is reality. If a website is flagged as "not secure," it gives site visitors reason to pause before engaging further with the nonprofit. As we all know, it's hard enough to get someone to fill out a form on a website to subscribe to a newsletter. Attracting donations is even harder. It's best not to give site visitors another reason to opt out of connecting with or supporting your nonprofit.

What if my nonprofit doesn't ask anyone to enter information on its website?

You may still want to move to HTTPS. Aside from the impression a secure versus not secure site can have on site visitors, HTTPS matters for SEO (search engine optimization). This isn't anything new. Google announced back in 2014 that an HTTPS site will come up higher in search results than an HTTP site. So, for this reason alone, it may be beneficial for your nonprofit to switch to HTTPS where it will have a greater chance to gain visibility

So how do I update my nonprofit's website?

If your nonprofit's website address still starts with http:// and not https://, contact your website support team or the company that hosts your website. 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."

The bottom line

Donors and clients trust nonprofits to keep their personal information safe. If there is any reason for a donor to doubt the security of personal information held by a nonprofit, that doubt could cost the nonprofit a donation. Similarly, a potential client may doubt that the client's personal information will be kept private and chose to seek services elsewhere, or not at all. For these reasons alone nonprofits will need to start paying more attention to data security and all its implications.

Data security is not a trend; it needs to be a part of your nonprofit's ongoing plans. As we have seen over the last few months, the standards continue to evolve. Whether it is the General Data Protection Regulations (GDPR) put in place by the EU (that triggered that flood of "we're updating our privacy policy" emails you received a few weeks ago) or this new change from Google, it is important to stay informed. We can expect future data security adjustments will be needed as technology continues to evolve. Be sure you are protecting your nonprofit's data. Your donors and clients will thank you.