Better safe than sorry (or why you need SSL)

Take a look at your browser right now. You should see that the web address starts with https, and that that there is an icon to the left of that that shows a closed lock (and in Chrome, it says “secure”). This means that my website has its SSL certificate in order, and that this website is safe.

SSL stands for Secure Sockets Layer, and it is basically an authentication protocol that establishes a secure connection for your website.

It is better to be safe than sorry

By having that “secure” label, you are creating a safe experience for your readers/users. This helps build trust. But more importantly, starting this year, Google will penalize websites that don’t have the SSL certificate by labeling them as unsafe or “not secure.” Would you want to visit a site that is flagged as “not secure?” Probably not.

SSL certicates may be free with your hosting package

Getting SSL on your website should be a number one priority. If you (like me) manage your own website, check with your host. Most hosts provide free SSL certificates, and can deploy them on your site in a matter of minutes. Just give your website host a call, and follow instructions. If your host does not provide a free SSL certificate, there are plenty of places that will sell you one. Here’s a how-to guide on setting up SSL: https://sucuri.net/guides/how-to-install-ssl-certificate

There may be a few more steps that you need to take to make sure your site is secure. In my case, the browser was telling me some images on my site were not secure. Thankfully, there

was an easy and free fix in the form of a WordPress plugin. If you are using a site that is not WordPress based, you may have to check with a website developer to get some technical help.

Bottom line

In a world that has become rife with cybercrime, it is important to have provide a safe browsing experience. It is free to very low cost to deploy basic SSL on your website. And if you care about Google rankings, you need to do this now.