How & Why to Make Your Website More Secure

Thanks to the buzz around website hacking and personal data theft in recent years, most Internet users are aware that their sensitive information is at risk every time they surf the web.

And yet, although the personal data of their visitors and customers is at risk, many businesses still aren't making website security a priority.

Enter Google.

The folks over at Google are known for paving the way for Internet behavior. Last month, they took a monumental step forward in helping protect people from getting their personal data hacked. The update they released to their popular Chrome browser now warns users if a website is not secure – right inside that user's browser.

While this change is meant to help protect users' personal data, it's also a big kick in the pants for businesses to get moving on making their websites more secure.

Google's Chrome update: What you need to know

On October 17, 2017, Google's latest Chrome update (version 62) began flagging websites and webpages that contain a form but don't have a basic security feature called SSL. SSL, which stands for "Secure Sockets Layer," is the standard technology that ensures all the data that passes between a web server and a browser – passwords, credit card information, and other personal data – stays private and ensures protection against hackers.

In Chrome, sites lacking SSL are now marked with the warning “Not Secure” in eye-catching red, right inside the URL bar:



Google started doing this back in January 2017 for pages that asked for sensitive information, like credit cards. The update released in October expands the warning to all websites that have a form, even if it’s just one field that asks for something like an email address.

What’s the impact on businesses?

Because Chrome has 47% of market share, this change is likely noticed by millions of people using Chrome. And get this: 82% of respondents to a recent consumer survey said they would leave a site that is not secure, according to HubSpot Research.

In other words, if your business’ website isn’t secured with SSL, then more than 8 out of 10 Chrome users said they would *leave your website.*

Ouch.



What’s more, Google has publically stated that SSL is now a ranking signal in Google’s search algorithm. This means that a website with SSL enabled may outrank another site without SSL.

That’s exactly why anyone who owns or operates a website should start taking the steps to secure their website with an SSL certificate, in addition to a few other security measures. Businesses that don’t take care to protect visitors’ information might see significant issues, garner unwanted attention, and dilute customer trust.

“In my opinion, I think security is undervalued by a lot of

marketers," says Jeffrey Vocell, my colleague at HubSpot and go-to website guru. "Almost daily, we hear news about a new hacking incident or about personal data that has been compromised. The saying 'there's no such thing as bad press' clearly isn't true here; or, at the very least, the marketer that believes it has never had to live with the fallout of a data breach."

With Google's Chrome update, those visitors will see a warning right inside their browsers — even before they've entered any information. This means businesses face the potential of losing website visitors' trust, regardless of whether a cybersecurity incident has actually occurred.

If you're ready to join the movement toward a more secure web, the first step is to see whether your website currently has an SSL certificate.

Do you know whether your site has SSL?

There are a few ways to tell whether your website (or any website) has SSL.

If you don't use Google Chrome:

All you have to do is look at a website's URL once you've entered it into the URL bar. Does it contain "https://" with that added "s," or does it contain "http://" without an "s"? Websites that have SSL contain that extra "s." You can also enter any URL into this SSL Checker from HubSpot and it'll tell you whether it's secure without having to actually visit that site.

If you do have Chrome:

It's easy to see whether a website is secured with an SSL

certificate, thanks to the recent update. After entering a URL into the URL bar, you'll see the red "Not Secure" warning next to websites that aren't certified with SSL:



For websites that are certified with SSL, you'll see "Secure" in green, alongside a padlock icon:



You can click on the padlock to read more about the website and the company that provided the SSL certificate.

Using one of the methods above, go ahead and check to see if your business' website is secure.

Yes, it does have SSL! Woohoo!

Your site visitors already feel better about browsing and entering sensitive information into your website. You're not quite done, though – there's still more you can do to make your website even more secure. We'll get to that in a second.

Shoot, it doesn't have SSL yet.

You're not alone – even a few well-known sites, like IMDB and StarWars.com, weren't ready for Google's update. But it's time to knock on your webmasters' doors and have them follow the steps outlined below.

How to make your website more secure

Ready to protect your visitors from data theft and get rid of that big, red warning signal staring every Chrome user in the face in the process? Below, you'll find instructions and resources to help you secure your website and reduce the

chances of getting hacked.

Securing your site with SSL

The first step is to determine which type of certificate you need – and how many. You might need different SSL certificates if you host content on multiple platforms, such as separate domains or subdomains.

As for cost, an SSL certificate will cost you anywhere from nothing (Let's Encrypt offers free SSL certificates) to a few hundred dollars per month. It usually averages around $50 per month per domain. Some CMS providers (like HubSpot) have SSL included, so check with them before making any moves.

(Read this post for more detailed instructions and considerations for SSL.)

Securing your site with additional measures

Even if you already have SSL, there are four other things you can do to make your website significantly more secure, according to Vocell.

1) Update any plugins or extensions/apps you use on your site.

Hackers look for security vulnerabilities in old versions of plugins, so it's better to take on the challenges of keeping your plugins updated than make yourself an easy target.

2) Use a CDN (Content Delivery Network).

One trick hackers use to take down websites is through a DDoS attack. A DDoS attack is when a hacker floods your server with traffic until it stops responding altogether, at which point the hacker can gain access to sensitive data stored in your CMS. A CDN will detect traffic increases and scale up to

handle it, preventing a DDoS attack from debilitating your site.

3) Make sure your CDN has data centers in multiple locations.

That way, if something goes awry with one server, your website won’t stop working all of a sudden, leaving it vulnerable to attack.

4) Use a password manager.

One simple way of protecting against cyberattacks is by using a password manager – or, at the very least, using a secure password. A secure password contains upper and lowercase letters, special characters, and numbers.

Suffering a hack is a frustrating experience for users and businesses alike. I hope this article inspires you to double down on your website security. With SSL and the other security measures outlined in this post, you’ll help protect your visitors and your business, and make visitors feel safe browsing and entering information on your site.

Does your website have SSL enabled? What tips do you have for making your website more secure? Tell us about your experiences and ideas in the comments.