Google SSL Changes 2018 and How It Affects Your Business

Google is making some big changes to the way they display secure and insecure websites in the Google Chrome browser. Beginning with the Chrome 68 release date this month, Google Chrome will mark all HTTP sites as “Not Secure.”

What does this mean for your small business website? The Google SSL changes 2018 can have a huge impact on your website — and your business.

In this post, we’ll explain:

- What the terms SSL, HTTP, and HTTPS mean
- Why an SSL certificate matters to your business
- What changes Google is making and how they could impact your business
- What you should do next to ensure your website is secure

What is SSL (secure sockets layer)?

Ever notice a lock icon in the top left corner of a website? That means the website is equipped with and SSL certificate.

SSL stands for "secure sockets layer,” the technology that protects private information on your website.

An SSL certificate is a digital certificate installed on the server that hosts your website. The SSL certificate has two primary functions:

1. To "encrypt" - or protect - private information that's exchanged on your site, such as credit card numbers or customer account information

SSL certificates establish a secure link between your website and your customer by using encryption. Encryption is the technical process that allows data to be transmitted securely over computer networks. It essentially masks data so that unauthorized sources are unable to read or intercept it. (That makes SSL for e-commerce websites especially important.)

2. To authenticate the identity of your website to visiting web browsers, and authenticate your identity or business to the visiting user

An SSL certificate serves as an electronic ID card, kind of like your driver's license or passport. It establishes an online entity's credentials when doing business on the Web. A certificate authority (the entity that provides SSL certification) will need to validate your certificate by authenticating your domain and business or individual identity. Once your SSL certificate is installed

on your server, customers can view your authenticated information by clicking on the padlock symbol in the browser. They'll be able to see:

- The certificate holder's name
- The certificate's serial number and expiration date
- A copy of the certificate holder's public key
- The digital signature of the certificate-issuing authority

All of this helps build trust in your website — kind of like how doctors, lawyers, and other professionals hang framed copies of licenses, degrees and other credentials on their office walls.

Why Is SSL important?

Having an SSL certificate is vital for small business owners — both for yourself and for your customers. Here's why:

Without the data encryption created by the SSL, sensitive information like customers' credit card numbers, usernames and passwords can be compromised. This puts both your customers and your business at risk. Your customers can lose money or suffer from identity theft. For your business, the consequences can be just as dire: One data breach could lead to a lawsuit that could easily bankrupt a small business.

With news of cyber attacks making headlines almost every day, online customers are more wary than ever of internet fraud, identity theft and "phishing" schemes. Installing the proper security and validation for your site via SSL certificate is essential to gaining your customers' and prospects' trust. It lets potential customers know your site is a secure place where they can feel confident sharing sensitive information, buying products or services, and completing secure transactions.

When you have an SSL certificate installed on your server, your site will display three instantly recognizable symbols that let customers know your site is secure:

- A padlock symbol that appears in their web browser when your site is opened
- The "https" prefix in front of your URL address in the browser (S is for Secure)
- A seal of authority, such as the Web.com Site Seal, that appears on your website

What Google SSL changes 2018 will do

Google really wants to make the Internet secure, and the new Google HTTPS requirements are part of a process that began last October. That's when Google Chrome began marking websites with any type of text input field as "Not Secure" if they don't have an SSL certificate. This includes sites where users input text for filling out forms, making a purchase, subscribing to an email newsletter, or even typing search terms into

a search bar. What's more, the "Not Secure" identification shows up even if a website visitor doesn't use the text input field.

Google's goal was to push more websites to begin using SSL, and it appears to have worked: Search Engine Land reports that more than 68% of Chrome traffic on android and Windows is protected with SSL, as is nearly 80% of Chrome traffic on both Chrome OS and Mac.

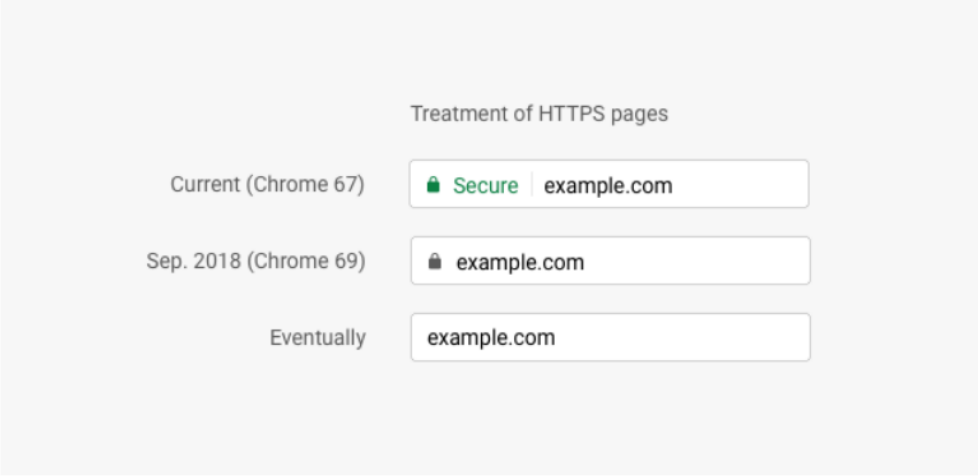
The Google SSL changes 2018 will go even further. Google will move from showing websites with an SSL certificate as a positive to showing websites without SSL certificates as "Not Secure" in the Chrome browser. Since it won't matter if you have no text input fields, this change will affect even the most basic websites.

Here's an example of how this change will look to your website visitors:

(Image Source: Web.com)

Ultimately, Google wants to move to a world where secure websites are the norm. With that in mind, Google announced that going forward, “We’ll step towards removing Chrome’s positive security indicators so that the default unmarked state is secure.” Chrome will roll this out over time, beginning with removing the “Secure” wording and in September 2018, when Chrome 69 rolls out.

Here's how this will look in September:

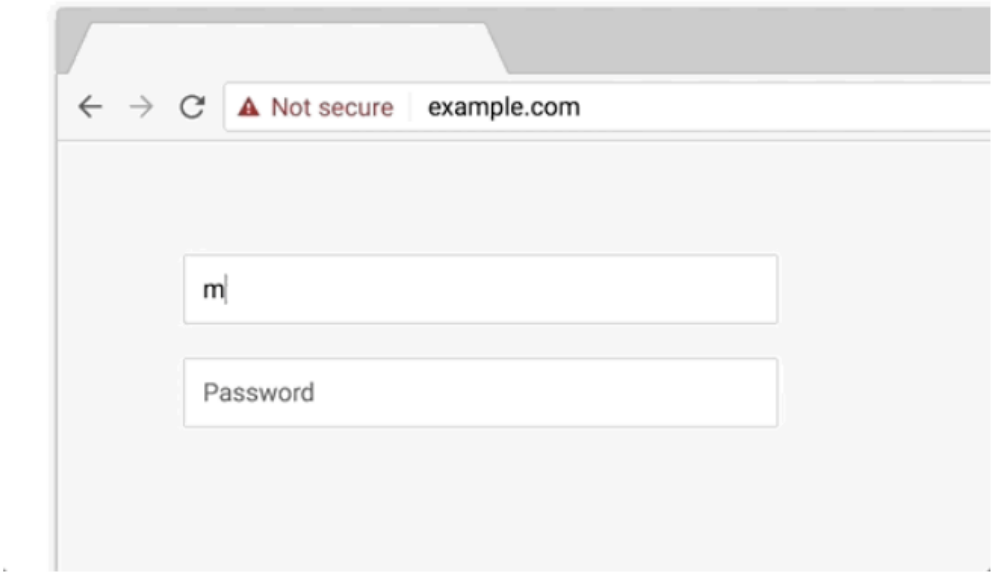


Chrome treatment for HTTPS pages

(Image Source)

In October, when Google releases Chrome 70, the change will be even more drastic. The green lock icon for secure websites will disappear from the browser. However, websites that don't have an SSL certificate will be marked with "Not Secure" in the browser. If a user starts to enter data in a text field, a red warning icon will appear, and the words "Not Secure" will turn red, too.

Here's an example of what that will look like:



Chrome 70 treatment for HTTP pages with user input

(Image Source)

I know seeing a warning like that would definitely scare me away from a website!

Why the new Google SSL requirements matter to your business

Google is giving small business owners some time to adjust to the new Google SSL requirements. However, October will come before you know it, and here's why this change will matter:

Having an SSL certificate enhances trust in your website. Internet-savvy users already know this. However, some of your customers and prospective customers may not be aware of the difference between websites with SSL certificates and those without. They may not know to look for the green lock icon or the word "Secure" in the browser bar.

A big red warning icon, on the other hand, is a whole different matter. Especially if you own an e-commerce business, I don't have to tell you that October is the beginning of the holiday shopping season. SSL for e-commerce will be more important than ever this fall. Do you want your customers to be scared away from your website — or do you want them to feel secure buying from you?

What to do about Google SSL changes 2018

So what do you need to do?

If your business website already has an SSL certificate, there's nothing to worry about, and nothing you need to do. Your website is secure.

But what if your business website is not yet secured with an SSL certificate?

If you're already a Web.com customer, we've got you covered.

Web.com believes that helping small businesses starts with knowledge — and the more you know about how to create a business website that builds trust, the better. That's why we've taken steps to make the transition to *https* a snap.

Here's what to do:

1) If you're a Web.com customer and have an SSL certificate that hasn't been set up yet, you can either call in and get your SSL certificate configured, or do it yourself in a few simple steps. (Watch for an email from Web.com with more information about what to do next, or call us at 1-800-338-1771.)

2) If you're a Web.com customer without an SSL certificate, for a limited time we are offering the option to purchase an SSL certificate at a discounted rate of 50% off.

Not a Web.com customer yet? Learn more about our SSL for small business options and what to look for when you buy an SSL certificate