Symantec | Website Security Partner Program

Google Chrome 56:
What you need to know

Overview

To help users browse websites more securely, Google has announced that the January 2017 release of its Chrome browser will mark all unencrypted HTTP sites as “not secure” in the browser URL. This is part of Google’s plan to discourage use of sites that don’t use appropriate security measures and to transition web traffic from potentially insecure HTTP to the safer alternative HTTPS sites.

Why is Google making this change?

Current versions of Google Chrome cannot indicate whether HTTP connections are secure. This means that when users access a site using HTTP, a hacker could intercept login information, passwords or payment data, increasing the opportunities for fraud.

A recent Google study identified that the current neutral indicator in the web browser has little impact on users, and a “not secure” warning is more effective. In labelling HTTP sites more clearly and accurately Google aims to give users more reassurance when using certain websites. Ultimately, Google plans to label sites that continue to use HTTP with a red warning triangle to indicate that these sites are not functioning securely.

When does this change take place?

Beginning in January 2017, Google’s Chrome 56 browser will label HTTP pages that include sensitive information, such as password or credit card fields, as “not secure”.

Why transition to HTTPS?

HTTPS ensures that when a user accesses a website, this data is encrypted using the Secure Sockets Layer (SSL) protocol or the more modern version, Transport Layer Security (TLS) protocol. In order to implement HTTPS, site owners must obtain a trusted digital certificate for each of their sites. Google reports that HTTPS usage is increasing substantially and that a significant portion of web traffic has transitioned to HTTPS to date.

What are the benefits of encrypting my website?

HTTPS offers many advantages over HTTP, including powerful new features and performance including:

- Always-on SSL (AOSSL): a practical best practice to protect user data and ensure a site’s pages, cookies, APIs, and sessions are secure
- SEO benefits: Google’s search engine algorithms boost rankings of sites that use HTTPS encryption
- Performance: encrypted sites get the performance enhancements that come with HTTPS and performance is a significant search engine ranking signal
- Control: Third parties and Wi-Fi hot spots can insert ads on web pages, potentially slowing site performance and messing up the user experience
- Credibility: the reassurance of encryption to users should not be underestimated. Visual trust cues can help reduce bounce rates, abandoned shopping carts, and improve trust

Is the change in Google Chrome relevant to individual pages or the entire site?

Browsers are looking at pages, so as pages appear they examine them for password or credit card fields. If these fields are present, the site will be flagged. If no fields are present, the site is not flagged. Any pages within the site that are flagged need encryption to prevent browser warnings indicating the page is not secure.

My site isn't ecommerce, why is this important?

As Google Chrome marks all pages with the insecure warning, it leads to a negative impact on the user experience, whether or not encryption is needed in the same fashion as an ecommerce site. Considering this is a browser change that affects all types of sites, it's not just for ecommerce.

Will my internal pages, not accessible to the general public, be subject to the same warning messages?

This is a change controlled at the browser level, not at the user level. So, you'll still have the error messages for internal sites lacking HTTPS, which could cause confusion for users within your internal environment(s).

How can I prioritize which pages to secure?

At a minimum, start with password and credit card pages as we know these are pages that will be impacted by this change. Then, begin looking at other pages. A best practice for prioritization purposes would be to address the pages on your site with the highest traffic, as these will be visited the most and have the highest chance of a negative user experience when error messages are displayed.

Speaking of Google, will not having HTTPS impact my search ranking?

Yes, sites with HTTPS are given preference in search rankings (which has been widely publicized), so it goes to show that using HTTPS is important for your SEO activities.

What can I do next to secure my website?

We partner with Symantec, whose AOSSL security offerings for small and mid-size businesses deliver world class security, helping to prevent cyber-attacks and other repercussions. Providing a prescriptive approach and practical step by step advice, our partnership with Symantec can support your business by securing the exchange of digital information across the web. This means your customers can be confident that their interactions with your website are secure and that they are receiving an optimal user experience.

Where can I find more information?

Speak with your account manager, or visit our content hub: https://go.symantec.com/be-trusted

Symantec World Headquarters
350 Ellis St. Mountain View, CA 94043 USA
+1 (650) 527 8000 +1 (800) 721 3934
www.symantec.com

Copyright © 2016 Symantec Corporation. All Rights Reserved. Symantec, the Symantec Logo, the Checkmark Logo, GeoTrust, the GeoTrust Logo, Thawte, and the Thawte logo and RapidSSL logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.