

EXECUTIVE UPDATE



Directors Report

Claire Birks, MNZIPP II

HTTP vs HTTPS

18 months ago, Google announced some big changes. They proposed that web browsers should label websites using HTTP web pages as unsecure, moving to also boost search rankings for websites using HTTPS URL's.

HTTPS allows your browser (your Safari, Firefox flag, Internet Explorer and Google Chrome) to securely connect with a website. HTTPS being one of the measures that helps keep web browsing safe and secure. This is very important when doing things like logging into your bank's website or using your credit card at an online store.

This works by HTTPS relying on an encryption process to secure the connection. These connections protect against eavesdroppers, man-in-the-middle attacks, and hijackers who attempt to spoof often trusted websites. In other words, it puts a stop to the interception of your information and ensures the integrity of the information that you send and receive.

January marked the start of "HTTPS everywhere" and with the new releases of Firefox and Google Chrome they started designating some HTTP connections as insecure. This is an industry wide push to promote the use of HTTPS secure sites.

In one of the boldest moves yet for Google, sites that still use HTTP will be plainly marked "Not Secure." This non-secure labelling will occur on pages delivered over HTTP that include forms. Specifically, these will be pages that include password fields, and in Chrome credit card fields, placing warnings in the address bar to indicate that the connection is not secure.

Will this labelling affect me?

In short, YES if you have the following on your website:

- Payment facilities
- Login pages for image galleries where a password is needed
- Logging in to your own website
- Client / Account login pages

Initially the warnings will be on pages where users have a higher expectation of privacy, such as where they need to provide you with email addresses, passwords or payment details. Eventually all HTTP pages will be labelled as non-secure.

What will I see in my browser bar?

On a current unsecured HTTP website:

 example.com

The new notification on a HTTP website shown as:

 Not secure | login.example.com

Eventually the notification of an HTTP page will appear as:

 Not secure | example.com

A secure HTTPS website, will show as:

 Secure | https://example.com

Mainly used for larger companies, an EV SSL certificate can be served to a HTTPS website, reflecting the most trusted and secure website possible. The URL will subsequently have the SSL reference alongside the company name.

 SSL Corp [US] | https://www.ssl.com

However, a HTTPS website with an SSL certificate that has not been installed correctly, or with website functions have not been updated to work properly you can expect to see:

 Not secure | ~~https://~~expired.badssl.com

In months to come, websites will be ranked based on their HTTP or HTTPS standing, meaning if your competitor's website uses HTTPS, and yours doesn't, it will be reflected in the website rankings. This will give your competitor an advantage. While at the moment this is fairly insignificant, in the future Google's HTTPS ranking signal will be strengthened, and it will definitely affect your search ranking.

How do you move to HTTPS?

Arrange a SSL certificate for your website. There are many different options available from free to expensive, so I recommend you talk through the options with your web developer or website host for find the best one for you. Some of the options include:

- Basic SSL, which provides a quick and easy validation to protect your website.
- Wildcard SSL, required if you are running multiple subdomains off your domain name. This lets you install 1 certificate for your entire website instead of 1 per subdomain.
- EV SSL, which provides the highest level of validation available. It automatically enables a green (secure) address bar and displays your verified organisation details, while helping boost customer trust.

So, to ensure you get the best outcome from the investment you make in your website, today is the day you need to start thinking about moving your website to HTTPS.

If it's there already ... fantastic!

For those that aren't, no need to panic but ensure you put it on your to-do-list. This will bring clients and potential clients the confidence they deserve when entering your website and you'll also be ready to top the rankings ahead of your competitors.