2017 Edition

SSL CERTIFICATES

Google & SEO

Understanding the benefits of using an SSL certificate on your website in 2017 and the future

FLEXXcreative

DESIGN.DEVELOP.DELIVER

2017 Edition

SSL (HTTPS) CERTIFICATES, GOOGLE AND SEO.

Back in August of 2014 Google officially announced that switching your website over to HTTPS (adding an SSL certificate) will give you a small boost in the search engine rankings.

So it's pretty simple, right? If Google says do it, then we should all do it.

For most companies this is exactly the right way to approach this, but it's still worth learning and understanding the difference between HTTP and HTTPS, how to make the change, and if making the change is the right thing to do.

Google has three main reasons for this that all come back to the desire to create a more secure internet, but before we get to those three reasons, you may be wondering what HTTPS and SSL are.

HTTP: HYPERTEXT TRANSFER PROTOCOL.

Hypertext Transfer Protocol (HTTP) is a system for transmitting and receiving information across the Internet. HTTP is an '**application layer protocol**', which ultimately means that it's focus is on how information is presented to the user, however, this option doesn't really care how data gets from Point A to Point B.

It is said to be 'stateless', which means it doesn't attempt to remember anything about the previous web session. The benefit to being stateless it that there is less data to send, and that means increased speed.

WHAT IS HTTPS?

HTTPS, or 'secure HTTP', was developed to allow authorisation and secured transactions. Exchanging confidential information needs to be secured in order to prevent unauthorised access, and HTTPS makes this happen. In many ways, HTTPS is identical to HTTP because it follows the same basic protocols. The HTTP or HTTPS client, such as a web browser, establishes a connection to a server on a standard port. However, HTTPS offers an extra layer of security because it uses SSL to move data.

For all intents and purposes, HTTPS is HTTP, it's just the secure version.

WHAT IS SSL?

SSL is the acronym for Secure Socket Layer and is often used interchangeably with the term TLS – Transport Layer Security. Both are cryptographic protocols that help encrypt communications over a computer network. Typically, if a website wanted to encrypt the transmission of its data between the server and the client, they would purchase an SSL certificate that contains an encryption key that is placed on the server.

WHY SHOULD YOU CARE ABOUT HTTPS AND SSL?

This gets back to the three reasons why Google is calling for all websites to switch to HTTPS. In order to access most websites, the URL usually begins with 'HTTP'. This is the unsecured version of the protocol that transfers data between the web server and the browser on your computer or smartphone. Remember that fear you had of using your credit card online? Well, it's not just credit cards that are of interest.

Google sees three reasons for securing your website with HTTPS and SSL. They are 'Authentication', 'Data Integrity', and 'Encryption'. These three reasons speak to a number of issues that have come up when it comes to communications over the web.

Check out this **video here**.

Authentication addresses the issue of verifying the ownership of your website. Believe it or not, there are people out there that make replicas of websites and divert traffic to it in an effort to steal from you. Most people know that they need to check for the Green Lock in their browser before entering personal information into the website. You can go one step further and verify the SSL certificate to make sure it belongs to the website you're on.

Data Integrity speaks to whether or not the data on the site has been tampered with while it's in transit. If someone knows what they are doing and your website is not secure, they can tamper with the data transmitted from your server back to the client. The form submission that the client just sent could go to the hacker and not to you.

Encryption refers to the security of communications between the client and the server so that no one else can read them. This is a key point for commercial websites. While it's extremely important to encrypt the communications on an eCommerce website, it's equally important to encrypt the data submitted using forms.

WHAT DOES AN SSL CERTIFICATE COST?

The cost for an SSL certificate will depend on your website's hosting provider, who they buy the certificate through, and the type of certificate they buy. There are three types of certificates.

- **Single Domain** – This type of SSL certificate is only valid on one domain URL
- **Multi Domain** – Also known as a Universal Communication Certificate (UCC) this secures multiple domain names and multiple host names within a domain name. You would set a primary domain and can add up to 99 additional Subject Alternative Names (SANs) in a single certificate. This is great for businesses with multiple sub domains and URLs for different service, product lines or geographic locations
- **Wildcard** – This type of certificate is for securing all of the subdomains you may have for a single domain

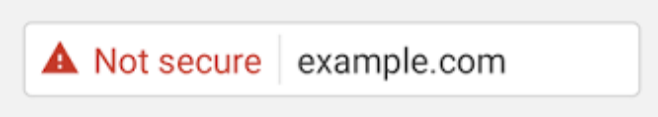
When selecting your SSL Certificate, please consult with your web host, marketing agency, or IT department to make sure you are selecting the right option for your entire business.

2017, THE YEAR OF HTTPS AND SSL?

Back in 2014, Google said that if your website was secure (HTTPS), then it would give that site additional positive ranking signals in the search results. This is a good thing for businesses that have websites that are competing with other businesses for position on search engine results pages. Google also said they wouldn't penalise the websites that are not secure. Well, at least not with their algorithm.

In September 2016, **Google announced** that in January 2017 they would begin displaying the security of the connection in the address bar of Chrome version 56 and up on pages that display a password and/or a credit card field. This is the beginning of a long-term plan to mark all HTTP pages non-secure.

Chrome is already making it really obvious when a website isn't secure and will eventually label all HTTP pages as non-secure (this is already rolling out) and change the HTTP security indicator to the red triangle used for broken HTTPS. It won't be subtle either:



If I'm on a website with that indicator, especially an eCommerce site, you better believe I'm not staying! Would you? I'm willing to bet not, and other users will most likely feel the same way.

Google has conducted a number of studies that concluded that visitors do not consider the absence of a 'secure' icon a warning. But it should be. This is why Google is taking the extra step to warn users of its browser, which is used by more than 55% of internet users, that the site they are visiting and about to enter their sensitive information into is not secure.

In addition, as part of their long-term plan, Google will likely include pages with contact forms in the coming months. So, while they're not susceptible to this warning just yet, they will be and you should do something about it now.

WHAT'S THE PROCESS OF CHANGING MY SITE FROM HTTP TO HTTPS?

At FLEXX Creative, we are prepared to help our clients make this transition as simple as possible with little to no interruption to your website. This means there are potential issues that can happen, which is why this is not a DIY project. Here are a few of the things we will need to do to get your website converted to HTTPS:

- Help you secure the right certificate for your website if you are hosted with us.
- Install the certificate on your website
- Update the configuration of your website to point to HTTPS instead of HTTP
- Redirect all incoming requests for your HTTP website to the location of the HTTPS site
- Re-verify ownership of your website in Google Search Console and update the sitemap location
- Update your web property's configuration in Google Analytics
- Test and confirm that the conversion was successful

Keep in mind that while the domain of your website is not changing, the address to get there is. HTTP and HTTPS request your website from two different ports on the web server. Because of this, there is a risk that traffic to your website will drop briefly as Google works to re-index your site. This is also why making sure you redirects are working seamlessly is extremely important.

From here, there are a few things to consider. If you have any marketing tools or digital ads pointing to your website you will want to update the URLs they are pointing to. While redirects will be set up to send HTTP request to the HTTPS URL it's still best practice to change them as redirects slow the request time and could decrease visitors and conversions.

WHAT DO I DO NEXT?

This isn't a decision about if you should make the switch or not. You need to decide when you want to make the switch to HTTPS. In 2017, every new website project we take on will include HTTPS and SSL in the contract. We want every website we make going forward to be secure, especially WordPress websites. **Matt Mullenweg of Automattic**, the creator of the WordPress project, is heavily advocating that all WordPress websites to be hosted on HTTPS as more and more features in WordPress will require it.

Start the conversation today. **Contact us** sooner rather than later so you can stay ahead of the competition and serve your visitors with a secure connection to your business.

2017 Edition

Want to know more?

Let's talk!

hello@flexxcreative.com
flexxcreative.com
+44 (0)1273 634544

FLEXXcreative

DESIGN.DEVELOP.DELIVER