Michigan SBDC

Why & How to Implement Secure URL Status (TLS/SSL)

What is HTTPS, TLS, & SSL?

HyperText Transfer Protocol Secure (HTTPS) is an internet communication protocol that ensures a safe connection between your web server and your website's visitors. It is extremely important, especially when exchanging private information online, such as personal data and credit card details. This safe connection is commonly provided through TLS (Transport Layer Security), which is a cryptographic protocol that replaced SSL (Secure Socket Layers). Although the former is an enhanced type of cryptographic protocol, the later is still being used today. Many use the term SSL to refer to both SSL and TLS. A URL that is not secured will start with HTTP instead of HTTPS.

Why is an https certificate important for seo?

Google and other search engines prioritize protecting users' privacy, and therefor favor secure web pages (HTTPS). Having an HTTPS certificate became more of an emphasis for SEO practices mainly after Google's announcement in 2014, claiming that they would start using HTTPS as a ranking signal. In 2018, Google Chrome started to classify all non-HTTPS sites as "Not Secure." Therefore, having a certified website with the green letters and the padlock icon displayed in the browser address bar will also transmit an image of trustworthiness to potential clients, which can lead to an increase in your conversion rate.

Three Elements That Are Present in a Secure Website

- Authentication - The internet browser recognizes that the server being reached is a legitimate one.
- Data Integrity - The data is not being modified while in transit between server and browser.
- Encryption - The content of the data is not revealed if it is intercepted.

Best practices to consider when implementing https

- Make sure to use 301 redirects, so users are always pointed toward your new URLs.
- Ensure that your HTTPS pagescan be indexed by Google (avoid 'no index' tags).
- Make sure that you have the newest versions of TLS libraries.
- Make sure that your certificate is always up to date.

What is certificate authority (CA)?

This is an entity that issues digital certificates. It will ensure that your web address is actually yours, giving credibility to your visitors. Google recommends you always go for a 2048-bit key level of security, and that you get your certificate from a reliable Certificate Authority(CA) that offers technical support .

What are the types of certificates?

- Single Certificate - Appropriate for sites with single domains (e.g., www.singledomainexample.com).
- Multi-Domain Certificate - Appropriate for sites with multiple domains, such as when a company has different business lines (e.g., www.lineofbusiness1.com; www.lineofbusiness2.com).
- Wildcard Certificate - Appropriate for sites with multiple sub-domains (e.g., subdomain1.site.com; subdomain2.site.com).

How to migrate from http to https

After choosing a CA, you will have to decide what type of certificate to get, according to your need. One CA we recommend is GoDaddy, but there are many reliable CAs in the market with different prices. In case you decide to work with GoDaddy, after selecting and buying your annuity for a specific type of certificate, they will send you an email letting you know of your certificate's issuance. If they do not host your website, they will give you further instructions on how to generate a CSR (Certificate Signing Request) for your website's domain name.

Michigan SBDC

For more information on how to implement a secure URL on your website, sign up for SBDC consulting at:

MichiganSBDC.org