Why do I need an SSL/TLS Certificate?

What is HTTP vs HTTPS and why is it important?

DEBSWEBS LLC - OCTOBER 19, 2017

HTTP vs HTTPS

Look at the address bar in your browser. Notice at the very beginning, before the "https://debswebsdesign.com/encrypt-your-website/" part, there is a small green padlock. That means that the connection between your browser and the server this article lives on is secure and encrypted.

When you use your browser to visit a website, you use the Hyper Text Transfer Protocol (HTTP) to transfer data back and forth between your device and the server on the web. HTTP is unencrypted and open, which means that data is transferred back and forth as plain text. Anyone "listening in" would be able to hear what's being transferred.

Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP. It means all communications between your browser and the website are encrypted. The "S" at the end of the "HTTP" means the connection is secured through either TLS or SSL. This makes it impossible for eavesdroppers to figure out what you're transferring. You and your communication partner use a secret code to encrypt your conversation and only the two of you have the decryption key.

How Does HTTPS Work and What is Web Encryption?

Historically, HTTPS has only been used by sites that require a high level of security, like bank transactions or credit card purchases that transfer sensitive data. That made getting the HTTPS certificate difficult and expensive. That is no longer the case. TLS and SSL certificates have become very affordable and easy to install on your server.

HTTPS pages use one of two secure protocols to encrypt your communications: SSL (Secure Sockets Layers) or TLS (Transport Layer Security). Both the TLS and SSL protocols use an asymmetric Public Key Infrastructure (PKI) system. This system uses two "keys" to encrypt data, a public key and a private key. Anything encrypted by either key can only be decrypted by the other corresponding key.

As their names suggest, the private key should be kept strictly protected and should only be accessible by it's owner. The public key is intended to be distributed to anybody that needs to be able to decrypt the information that was encrypted with the private key.

When you request a HTTPS connection to a webpage, the website will send its SSL/TLS certificate to your browser. The certificate contains the public key necessary to begin the secure session. The browser and website then initiate the "SSL handshake." The handshake involves the generation of shared secrets to establish a secure connection between your server and the website you are accessing.

Encryption is Essential for Search Results

You may ask why you need an SSL/TLS certificate to encrypt your website if you are not transferring sensitive data. There are several reasons.

Beginning in January 2017, Google Chrome began flagging unencrypted websites which contain a login form or a credit card processing function as "Not Secure" in the user's browser. Other browsers are now following suit. Since your website will likely be a WordPress site, it will have a login form for administrators and members (if you have a membership section). They will receive a message that says the site is not secure.

In addition, Google recently announced that they will start weighting search results based on encryption, giving encrypted sites preference over unencrypted ones. So if you want your site to be competitive in Google searches, you will need to ensure that it is encrypted. This is not likely to make a huge difference in your Google ranking, but it is something you should consider.

Bottom line? With the advent of affordable and easily accessible TLS/SSL certificates, that "S" at the end of the "HTTP", will become one of the most important features of your website. So, between increased security, possibly boosted performance (which we did not address in this article), better search rankings, getting your site flagged as "Secure" in the browser, and the fact that SSL/TLS certificates are now extremely affordable and easy to install, there is no reason to wait on encrypting your site.