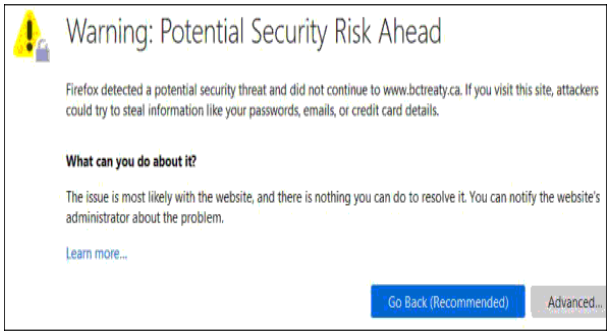
Hello Everyone.
In this newsletter I want to talk about the why and how web sites require SSL Certificates. SSL stands for "Secure Sockets Layer". (updated to Transport Layer Security (TLS) today)

SSH and SSL are abbreviations you will see together sometimes. Both technologies allow you to create secure connections on the Internet. SSH stands for “Secure Shell” that has a built-in username/password authentication system to establish a connection.

In Firefox browser you might see this if not properly certified



Did you know that Google Chrome shows all non-SSL websites as “Not Secure”. This means that if you are not using a SSL certificate on your website, then you’ll lose customers trust.

Google Chrome web browser started with version 0.2.149 - 2008-09-02

We are now at version 83.0 - 2020-03-16.

Version 82 was skipped due to the 2019-20 coronavirus pandemic? Todays date is 2020-04-03. Why? Google in their wisdom has decided that the web should be secure for everyone. Google is Forcing You To Have SSL Certificates on Your Websites, don’t have an SSL Certificate? Google is going to flag your website Not Secure!

With Chrome version 62.0.3202 released in 2017-10-17, websites with any kind of text input will need an SSL certificate. Does your website take text inputs in the form of login panels, contact forms, search bars, newsletter subscriptions? Is your website HTTP://?

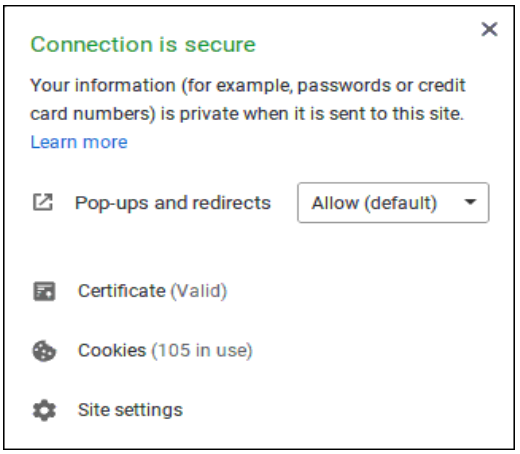
If you answered yes to these questions, then you should install an SSL Certificate.

HTTPS (HyperText Transfer Protocol Secure)

SSL certificates create an encrypted connection and establish trust.

SSL Certificates protects any data by encrypting the connection between your web server and your visitors.

This demonstrates ownership of the domain to the certificate authority at the time of its issuance.



Why:

If you plan on having your customers input their private information online, then you need secure measures provided by an SSL certificate.

Security and trust is most important on the Internet. Without it your visitors will disappear.

SSL certificates build trust between your visitor and your website.

If information like credit card numbers, passwords, and other personal information isn't encrypted hackers can easily steal your personal information.

TERMS Used:

TLS and SSL

Another term you will see used along with SSL (secure socket layer) is TLS (transport layer security). These both are referred to as SSL certificates.

How does they work?

SSL has now become the industry-standard to ensure encrypted data between you and your visitors so information can not be hacked by users diverting traffic to their sites using or seeing the information being transferred.

All the major web browsers like Chrome, Firefox, Opera, Safari, Epic all have SSL capability built into their browsers.

Types of Certificates:

Higher level SSL certificates will have higher levels of encryption, but the standard SSL certificate should be enough for most websites.

(Domain Validated) DV SSL Certificates offer quick, reliable and affordable no-frills encryption. Getting one is easy. Prove you own the registered domain via email and it can be done right away.

DV SSL Certificates activate the standard SSL Visual Indicators – HTTPS and a padlock in the address bar – and are a perfect security solution for any non-e-commerce site that doesn't collect users' personal information.

There are three different identification certificates:

1. Domain Validation Certificates

With a Domain Validation Certificate, you're proving ownership over the domain name. At this level, the identity of the organization won't be checked, just that the person who has the SSL certificate also owns the domain name tied to the website.

This is the most basic level of SSL certificate and is usually the level of certificate that comes free with most hosting plans.

It's well suited for simple websites, but eCommerce sites and other websites that are dealing with sensitive personal information will want to obtain a higher-level certificate.

2. Organization Validation Certificates

With Organization Validation Certificates you'll have to prove that you own the domain name, along with proving that your company is accountable and registered as a business. Usually, this means you'll need to have proof of a registered company name and proof of domain ownership.

This level of certificate can only be issued to businesses and organizations. Individuals running a website won't be issued this level of certificate.

3. Extended Validation Certificates

Extended Validation SSL Certificates are the highest level of SSL certificate available. To obtain this level of certificate you'll need to validate your business, as well as your domain name. Plus, there are additional verification steps that you'll also have to complete.

Obtaining this level of SSL certificate will take longer, but for some website's it'll be worth it. It goes a long way towards showing your visitors that you value their privacy and protection.

When visiting a site with this level of SSL certificate you'll often see the URL bar is entirely green. This is a highly visual form of trust that you'll exhibit to your customers.

Note that this level of certificate is also only available to businesses and organizations. It is not available to individuals.

How To Order An SSL Certificate:

1: Generate a Certificate Signing Request (CSR)

https://www.wikihow.com/Install-an-SSL-Certificate

2: Order your SSL certificate. There are several services online that offer SSL certificates. Make sure to only order from a reputable service, since you and your customer's security is at stake. Popular services include DigiCert, Symantec, GlobalSign

3: Download your certificates. You will need to download the Intermediate Certificates from the service that you purchased your certificates from. You will receive your Primary Certificate via email or through the customer area of the website.

Rename the Primary Certificate to "yoursitename.cer".

https://www.sslshopper.com/how-to-order-an-ssl-certificate.html

What do I need to have before buying an SSL certificate?

A unique IP address.

If you have multiple subdomains on one IP address, you can secure them with a Wildcard SSL Certificate. If you have multiple different domain names on one IP address, you can secure them with a UC Certificate.

You will need to set up SSL Host Headers to do this.

Because of the way that the SSL protocol was set up, you will need a separate IP address for each certificate that you want to use. If you don't, some older devices and browsers won't be able to use your site.

How long does it take to get my certificate?

How quickly you get your certificate depends on what type of certificate you get and which certificate provider you get it from.

If you get a domain-validated only certificate you will receive it within a few minutes. If you get a normal, organization-validated certificate, you may receive it within an hour to a few days after you submit all the documentation. If you get an extended validation certificate (EV), you may wait several days to a few weeks while the validation takes place before you get the certificate.

Verifying the Identity of the Site Owner

The SSL credential identifies the owner of the website, and creates an additional layer of trust. Put simply, your customers will know with whom exactly they're doing business.

Before the certificate can even be issued the identity of the website owner has to be verified through multiple methods. With digital communication, it's often difficult to determine the person on the other side of the connection, but with an SSL certificate you can be sure you're doing business with your intended recipient, and vice versa.

What happens if you don't have an SSL Certificate?

Basically, Google is pushing hard towards an HTTPS/SSL web

For example, Google encrypts all traffic between Gmail and its servers. So, whenever you login to your Gmail account, you'll notice the HTTPS connection.

Most email service providers are currently using an SSL/TLS connection. But, these connections aren't foolproof. For example, SSL/TLS will protect your emails when you're composing them and during any transmission to your email client server. But, there's no guarantee that the person you're sending the email to will have the same level of security in place.

webmasters Central Blog

Official news on crawling and indexing sites for the Google index

https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html

And thanks to all that provided the information I gleened in able to present this in an easy to read and execute manner for those to benefit.

Best to all. See you in June. Hopefully we will have left behind most of the Covid 19 by then.