15 February 2019

Secure Socket Layer (SSL) for websites

If your organization, company or social group has a website, it is nothing without visitors.

For years people with malicious intent have sought ways to penetrate websites with the intent of stealing or making money. In absence of the money aspect there is simple vandalism. According to *Forbes*: With the evolution of the internet, the solutions for better protection of websites increase -- and so does the creativity of cybercriminals.

The many e-commerce industries seek to make all aspects of using the internet more secure. For several years they have pushed the application of a Secure Socket Layer (SSL) for websites. In the last several months the major browsers (Chrome, Firefox, Edge, Safari, etc.) are now displaying notice when one visits a non-SSL website, with words to the effect, "this website is not secure." When websites have secured their data and their website address using a secure server, a browser shows a lock icon and sometimes green script. Example: 

With internet browsers refusing to load the page you want and displaying a scary "NOT SECURE" you will not see the website you want, and you likely won't go back there again. For those of us who own websites, such as my church, I would be very disappointed that someone would think that my church is a virus host and malicious software nest.

What to do? For those who broadcast their websites to a global audience (yes, that really is your audience).

1. Worst solution - do nothing and hope visitors will click the bypass; take me there anyway.
2. Find and apply the several technical hacker solutions which disguise your website as secure. (It fails often and you'll have to reset it frequently. This is as reliable as a so-called free SSL certificate. If your webserver is an old computer in your garage or attic and you host your own website, give this a try. You'll discover that Free Certs are easily found out and search engines like Google will never show you on their search results.
3. Cut rate SSL sellers can sell you a DV SSL which is the lowest level of security. Domain Validated certs are for blogs or online information sites (business card sites) and that's probably all you need. There are services that are free or almost free. *Let's Encrypt, Certbot* and *Cloudflare* can facilitate SSL certificates. However, you must get them to function with your website host. Most major hosting services want to sell you their own SSL certs and won't work with third party certifications (what a surprise). The lesson; if you trust your web host and have been happy with their years of service, buy their SSL cert and have it applied right at the company level. They will in most cases offer a better deal to keep you from having to go shopping for the best price (see the last section below).

DV SSL certs will be seen by Google (and other search engines) as a proper certificate which will improve your search engine ranking. Estimated price for DV SSL $70.00 to $100.00 .

4. The better solution will cost a little more. If you sell anything from your website or solicit donations; or there is an occasion for a user to enter personal information, or if you ever plan to do these things, you will need an OV SSL. Organization Validated certs require more validation than DV certificates, but provide more trust. For this type, the Certificate Authority (or CA) will verify the actual business that is attempting to get the certificate. The organization's name is also listed in the certificate, giving added trust that both the website and the company are reputable. OVs are usually used by corporations (most churches are incorporated) and other entities that want to provide an extra layer of confidence to their donors and visitors. Estimated price for OV SSL; $100.00 to $150.00 annually.

5. There is one other and those are called EV SSL (Extended Validation). They are not addressed here because that is not for the audience this report speaks to.

In closing, if all this seems to have a conspiracy smell to it, your sense is likely correct. Every industry that uses the internet to make money wants it more secure and thus able to increase profits. There is a hard push for SSL on websites. They capitalize on our fear of identity theft and credit card loss. Website browsing and website security are as necessary as locking your home doors and your car, insurance for home and auto, medical coverage for yourself and those you love. The cost of business and services goes up every so often, and that includes broadcasting your website to the people who you want to see it. Read some of the references below and make your own choice. Search "why SSL" and find another hundred links to read.

CompTIA A+ CERTIFIED

Michael Clancy
A+ Technician since 2000 https://michaelogic.com/

references:
https://www.forbes.com/sites/forbestechcouncil/2018/05/18/why-an-ssl-certificate-is-important-for-your-company-website/#3c75407a1dc3
https://opensrs.com/blog/2015/05/dv-ov-or-ev-how-to-offer-the-right-ssl-certificate/
https://www.makeuseof.com/tag/reasons-ssl-certificate/
https://www.digicert.com/blog/not-secure-warning-what-to-do/
https://www.godaddy.com/web-security/ov-ssl-certificate
https://ssl.comodo.com/articles/the-ssl-certificate-domain-validated-organizational-validated-or-extended-validated.php