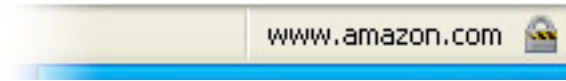


Secure Certificates

If you are transacting sensitive information like a credit card or social security number you should consider getting a secure certificate for your web site. Most

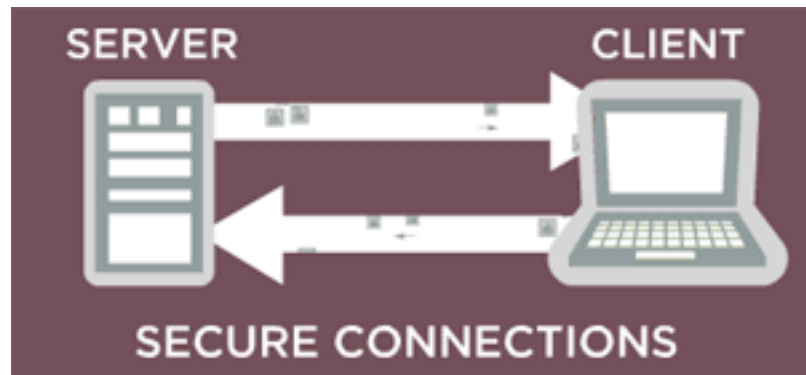


savvy web shoppers look for certain things on your web site before doing business with you like a phone number and your business location. They also look for the little secure lock icon

located either at the bottom right corner of the browser or next the website's urls (web address) or both.

What is a Secure Certificate?

Also known as an SSL (Secure Socket Layer) Certificate consists of a public key and a private key. The public key is used to encrypt information and the private key is used to decipher it.



When browsing a secure page, an SSL handshake authenticates the web page and the web browser. They can now begin a secure session in private as information moves back and forth between you and the secure web page.

An Unsecured page addresses starts like this: “http://...”

A Secure page address starts with: “https://...” Did you notice the “S”?

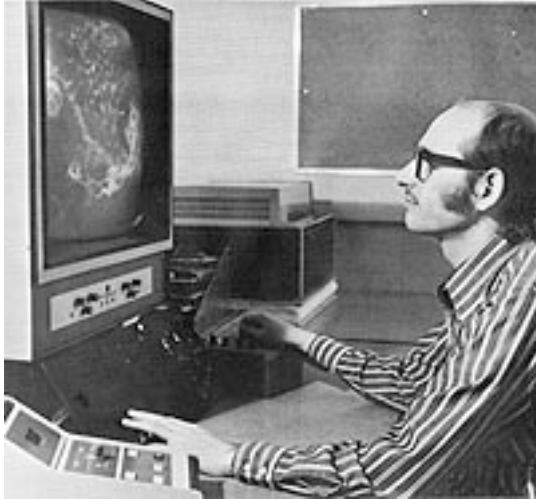
So when you are inputting your credit card information and clicking the “Purchase” button, your information is encrypted into gibberish that will take too much time for a hacker to decode.

That begs the question; “How much time does a hacker need?”. Hackers use sophisticated programs that test random deciphering keys in minutes. So the level of encryption is an important consideration.

SSL encryption depends on keys, you measure the effectiveness or strength of an SSL encryption by the key length or number of bits in the key.

In the old days of Internet Explorer 3.0 and Netscape a 40-bit encryption proved to be too easy to decipher or crack.

A common deciphering technique is **brute-force decryption**. By using a computer program to exhaustively calculate and try every possible key one by one.



For best security practices you should have a unique true-128-bit or better encryption certificate installed on your site. These days 256-bit is common.

Web surfers using old computers might be using old browsers. Many Windows 2000 systems using Internet Explorer will only receive 40 or 56-bit encryption from your 128-bit certificate. So even if you are offering the security, an old system user may be vulnerable on their side.

Experts say that 128-bit encryption will be secure for the next 8 to 10 years.

Where do you Get an SSL Certificate?

Almost every web hosting company offers Secure Certificates because they are the natural reseller of certificates from a certificate provider. There are some differences to be aware of.

Shared certificates are very inexpensive or free, but they come with some pitfalls. Some web owners will have difficulty using Shared SSL Certificates if say their shopping cart software requires a dedicated SSL Certificate. This is due to the need for the cart to function with only your domain/host and not have to send the user to a duplicate of your site somewhere else.

It is important to get a site seal to let everyone know that your site or page is secure. I have not seen a Shared SSL come with a Seal.

Prices have come down considerably from years ago. Here is a list of some of the main certificate providers and their entry level pricing. Certificates are sold at a minimum of 1 year and can be purchased to cover up to 5 years. You might get a discount for multiple years

- Verisign - SecureSite - \$399.00
- Thawte - SSL123 - \$149.00
- GeoTrust - QuickSSL - \$199.00
- Comodo - InstantSSL - \$99.95
- GoDaddy - Standard - \$29.99
- Webcentrica - Standard - \$29.99

All of these include a site seal.



Verisign is probably the oldest in the bunch. In the beginning they were the only ones you could go to for an SSL Certificate. I have used both Thawte (owned by Verisign) and GeoTrust in the past as a way to save some money. They all do the same thing. The only reason I see to using VeriSign is for the prestige. They are the Mercedes of the SSL Certificate market.

These days there are many choices. Both GoDaddy and Webcentrica use Starfield's Turbo SSL which I find to be quite efficient for securing your web pages.

Installing an SSL Certificate

This will require some help from an expert web person, however the Turbo SSL is fairly easy to install if your website is on a GoDaddy or Webcentrica server. In fact that is the only way the Turbo SSL can be installed. It is quick and you will only need to provide a few lines of information to StarfieldTech and they take care of it for you. My favorite!

Other certificate vendors will require the assistance of your server administrator and that is what makes the process complicated. You need to first procure a Certificate Signing Request from the server administrator and give it to the certificate vendor and then they provide you with an encryption key that you need to give to your server administrator to install.

While starting a new SSL from a 3rd party is complicated enough, renewing one is even harder because many times the original company info that was used to start the original certificate is lost. The vendor can not re-issue a certificate if any of the information is out of place. Things like a phone number or address change on a business can really throw the whole process.

That is why I like to suggest 3rd party "hosted" cart systems because they keep up with the security for you. A valuable benefit!

Posted on April 22nd, 2008 by Karl Knelson