Title:
Your Business can suffer due to absence of Digital certificate on your website

Word Count:
705

Summary:
SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

Keywords:
Digital certificates, Certification Authority, SSL security certificate, web server SSL certificates, internet security, internet SSL security, security certificate, code signing SSL certificates,

Article Body:
It is very important to take the protection against online information larceny, because it's getting very easy for people to share digital products. Information theft is a type of computer safety and security risk and it's defined as thieving someone’s private or confidential information. It’s very dangerous to get the information stolen as this can cause as much damage, or possibly more then hardware or software theft.

Most of the systems on the way of your data can see what you send. A lot of companies try to stop information from being stolen by applying some user identification and authentication controls.
These constrictions are most promising for protecting computers along a company's premise. However, to protect information on the Internet and on networks, companies use a handful of encryption methods like digital certificates and SSL security. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. Encryption refers to the process of converting data into an unreadable form. Encrypted data is like any other data because you can send it through a lot of options, but to read it you must decrypt or decipher it into a more readable form with the help of public and private keys provided. Throughout the encryption process, the unencrypted data or input is known as plaintext and the encrypted data, or output is known as cipher text. To be able to create an SSL connection a web server requires an SSL Certificate. When you choose to activate SSL on your web server you will be prompted to complete a number of questions about the identity of your website and your company. Your web server

then creates two cryptographic keys - a Private Key and a Public Key. To encrypt information, the programmer converts the plaintext into cipher text using some type of encryption key. An encryption key is the programmed formula that the person who receives the data uses to decrypt the cipher text. There are varieties of encryption or algorithm methods. However, with an encryption key formula, you will be using more then one of these techniques.

Most common example is a nasty individual stealing credit cards so they can make illegal purchases on another person's account. If information is transmitted over a network then it has a very high chance for nasty users to capture the information.

A digital signature is a type of encrypted code that an individual, website, or company pastes to an electronic document to make sure that the individual is who they claim to be. The code will most likely consist of the user name and a hash of usually part of the message. The complexities of the SSL protocol remain invisible to your customers. Instead, their browsers provide them with a key indicator to let them know they are currently protected by an SSL encrypted session - the lock icon in the lower right-hand corner, clicking on the lock icon displays your SSL Certificate and the details about it. All SSL Certificates are issued to either companies or legally accountable individuals. The main purpose behind using digital signatures is to make sure that it's not a swindler participating in the transaction. So, digital signatures help narrow down e-mail frauds. A digital signature can also make sure that contents of a message have not been changed.

Typically, an SSL Certificate will contain your domain name, your company name, your address, your city, your state and your country. It will also contain the expiration date of the Certificate and details of the Certification Authority responsible for the issuance of the Certificate. When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued.

Many ecommerce websites will usually have digital certificates. A certificate authority (CA) is an authorized company or individual for that matter that has the ability to issue and verify digital certificates. There are several of websites that offer a digital certificate. One of the popular Global Certification authorities is MindGenies (www.sslgenie.com).