Why You Need an SSL Certificate

WEB SITE

Starfield Secure

WHY YOU NEED AN SSL CERTIFICATE

Introduction

Recent numbers from the U.S. Department of Commerce show that online retail is continuing its rapid growth. However, malicious phishing and pharming schemes and fear of inadequate online security cause online retailers to lose out on business as potential customers balk at doing business online, worrying that sensitive data will be abused or compromised.

For e-businesses, the key is to build trust: Running a successful online business requires that your customers trust that your business effectively protects their sensitive information from intrusion and tampering.

Installing an SSL Certificate from Starfield Technologies on your e-commerce Web site allows you to secure your online business and build customer confidence by securing all online transactions with up to 256-bit encryption. An SSL Certificate on your business' Web site will ensure that sensitive data is kept safe from prying eyes. With a Starfield Technologies SSL Certificate, customers can trust your site.

Before issuing a certificate, Starfield Technologies rigorously authenticates the requestor's domain control and, in the case of High Assurance SSL Certificates, the identity and, if applicable, the business records of the certificate-requesting entity. The authentication process ensures that customers and business partners can rest assured that a Web site protected with a Starfield Technologies certificate can be trusted.

A Starfield Technologies SSL Certificate provides the security your business needs and the protection your customers deserve.

With a Starfield Technologies SSL Certificate, customers will *know* that your site is secure.

Why You Need a Starfield Technologies SSL Certificate

In the rapidly expanding world of electronic commerce, security is paramount. Despite booming Internet sales, widespread consumer fear that Internet shopping is not secure still keeps millions of potential shoppers from buying online. Only if your customers trust that their credit card numbers and personal information will be kept safe from tampering can you run a successful online business.

For online retailers, securing their shopping sites is paramount. If consumers perceive that their credit card information *might* be compromised online, they are unlikely to do their shopping on the Internet.

A Starfield Technologies SSL Certificate provides an easy, cost-effective and secure means to protect customer information and build trust. An SSL Certificate enables Secure Sockets Layer (SSL) encryption of your business' online transactions, allowing you to build an impenetrable fortress around your customers' credit card information.

A Starfield Technologies SSL Certificate helps you build an impenetrable fortress around your customers' credit card information.

Starfield Technologies SSL certificates bring the highest level of trust to your online business. A Starfield Technologies SSL Certificate ensures that all sensitive transactions are kept securely encrypted and safe from prying eyes, and rigorous authentication guarantees that Starfield Technologies certificates are issued only to entities whose existence and domains can be verified.

Starfield Technologies SSL Certificates offer industry-leading security and versatility:

- Fully validated
- Up to 256-bit encryption
- One-, two- or three-year validity (Turbo SSL Certificates valid up to 10 years)
- 99% percent browser recognition
- Stringent authentication
- Around-the-clock customer support

What is an SSL Certificate?

An SSL certificate is a digital certificate that authenticates the identity of a Web site to visiting browsers and encrypts information for the server via Secure Sockets Layer (SSL) technology.

A certificate serves as an electronic “passport” that establishes an online entity’s credentials when doing business on the Web. When an Internet user attempts to send confidential information to a Web server, the user’s browser will access the server’s digital certificate and establish a secure connection.

A certificate serves as an electronic “passport” that establishes an online entity’s credentials when doing business on the Web.

Information contained in the certificate includes:

- The certificate holder’s name (individual or company)*
- The certificate’s serial number and expiration date
- Copy of the certificate holder’s public key
- The digital signature of the certificate-issuing authority

To obtain an SSL certificate, one must generate and submit a Certificate Signing Request (CSR) to a trusted Certification Authority, such as Starfield Technologies, which will authenticate the requestor’s identity, existence and domain registration ownership before issuing a certificate.

Public and Private Keys

When you create a CSR, the Web server software with which the request is being generated, creates two unique cryptographic keys: A **public** key, which is used to encrypt messages to your (i.e., the certificate holder’s) server and is contained in your certificate, and a **private** key, which is stored on your local computer and “decrypts” the secure messages so they can be read by your server. In order to establish an encrypted link between your Web site and your customer’s Web browser your Web server will match your issued SSL certificate to your private key. Because only the Web server has access to its private key, only the server can decrypt SSL-encrypted data.

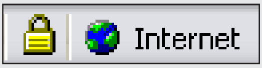
*High Assurance Certificates only. Turbo SSL Certificates only contain the domain name and no information on the individual or company that purchased the certificate.

Enabling Safe and Convenient Online Shopping

A Starfield Technologies SSL Certificate secures safe, easy and convenient Internet shopping. Once an Internet user enters a secure area — by entering credit card information, e-mail address or other personal data, for example — the shopping site's SSL certificate enables the browser and Web server to build a secure, encrypted connection. The SSL "handshake" process, which establishes the secure session, takes place discreetly behind the scenes, ensuring an uninterrupted shopping experience for the consumer. A "padlock" icon in the browser's status bar and the "https://" prefix in the URL are the only visible indications of a secure session in progress.

By contrast, if a user attempts to submit personal information to an unsecured Web site (i.e., a site that is not protected with a valid SSL certificate), the browser's built-in security mechanism will trigger a warning to the user, reminding him/her that the site is not secure and that sensitive data might be intercepted by third parties. Faced with such a warning, most Internet users likely will look elsewhere to make a purchase.

A "padlock" icon in the browser's status bar indicates that a secure session is in progress.



Up to 256-Bit Encryption

Starfield Technologies SSL certificates support both industry-standard 128-bit (used by all banking infrastructures to safeguard sensitive data) and high-grade 256-bit SSL encryption to secure online transactions. The actual encryption strength on a secure connection using a digital certificate is determined by the level of encryption supported by the user's browser and the server that the Web site resides on. For example, the combination of a Firefox browser and an Apache 2.X Web server enables up to 256-bit AES encryption with Starfield Technologies certificates.

Encryption strength is measured in key length — number of bits in the key. To decipher an SSL communication, one needs to generate the correct decoding key. Mathematically speaking, 2^n possible values exist for an *n*-bit key. Thus, 40-bit encryption involves 2^{40} possible values. 128- and 256-bit keys involve a staggering 2^{128} and 2^{256} possible combinations, respectively, rendering the encrypted data de facto impervious to intrusion. Even with a *brute-force attack* (the process of systematically trying all possible combinations until the right one is found) cracking a 128- or 256-bit encryption is computationally unfeasible.

Stringent Authentication — A Matter of Trust

Before Starfield Technologies issues an SSL Certificate, the applicant's company or personal information undergoes a rigorous authentication procedure that serves to pre-empt online theft and to verify the domain control and, if applicable, the existence and identity of the requesting entity. Only through thorough validation of submitted data can the online customer rest assured that online businesses that utilize SSL certificates from Starfield Technologies indeed are to be trusted.

A High Assurance Starfield Technologies certificate guarantees that the entity that owns the certificate is who it claims to be and has a legal right to use the domain from which it operates.

SSL Certificates are only issued to entities whose domain control and, depending on certificate type, business credentials and contact information have been verified. Thus, a Starfield Technologies SSL certificate guarantees that the entity that owns the certificate is who it claims to be and has a legal right to use the domain from which it operates.

Starfield Technologies issues three types of SSL Certificates, each of which relies on authentication of a number of elements:

High Assurance Certificate — Corporate:

Starfield Technologies will authenticate that:

- The certificate is being issued to an organization that is currently registered with a government authority.
- The requesting entity controls the domain in the request.
- The requesting entity is associated with the organization named in the certificate.

High Assurance Certificate — Small Business/Sole Proprietor:

Starfield Technologies will authenticate that:

- The individual named in the certificate is the individual who requested the certificate.
- The requesting individual controls the domain in the request.

Medium Assurance (i.e., Turbo SSL) Certificate:

Starfield Technologies will authenticate that:

- The requesting entity controls the domain in the request.

Phishing and Pharming – How SSL Can Help

Phishing and, recently, pharming pose constant threats to Internet users whose sensitive information is under siege by crackers and other cyber crooks.

An SSL certificate from Starfield Technologies can clip the wings of Internet criminals and help prevent Internet users from being victimized by phishing and pharming schemes when attempting to visit your Web site.

Phishing schemes – attempts to steal and exploit sensitive personal information – typically try to trick victims into accessing fraudulent sites that pose as legitimate, trusted entities, such as online businesses and banks.

Because perpetrators of such attacks will be using and registering domains that resemble those of the spoofed sites, Starfield Technologies, through its stringent fraud-prevention measures, will detect the schemes and deny certificate requests for suspicious domains.

An SSL certificate from Starfield Technologies can help prevent Internet users from being victimized by phishing and pharming schemes.

More sophisticated than phishing, pharming revolves around the concept of hijacking an Internet Service Provider's (ISP) domain name server (DNS) entries. When a "pharmer" succeeds in such DNS "poisoning" every computer using that ISP for Internet access is directed to the wrong site when the user types in a URL (e.g., www.ebay.com).

SSL certificate technology can help prevent pharming attacks, as well. In essence, a "pharmer" simply will not be able to obtain an SSL certificate from Starfield Technologies, as he/she does not control the domain for which the certificate is requested.

By protecting your Web site with a Starfield Technologies SSL certificate Internet users that attempt to access a site that poses as yours will be instantly alerted that there is a problem with the supposedly secure connection:

- **No lock icon:** Because CAs usually won't issue a certificate to fraudulent phishing or pharming sites, such sites usually do not use SSL encryption. Internet users, therefore, are alerted by the absence of a padlock icon in their browser's status bar.

- **Name mismatch error:** A pharming site could try to use a certificate issued by a CA for a domain owned by the attacker, but the user's browser will warn the user that the visited URL does not match the certificate presented by the fake Web server.
- **Untrusted CA:** A pharming site might attempt to use a certificate issued by an untrusted CA. In this case, the user's browser will generate the following warning: "the security certificate was issued by a company you have not chosen to trust."

The alert Internet user will instantly abandon his/her activities/transactions when presented with such warnings. Thus, a Starfield Technologies SSL certificate provides business owners and wary, savvy Internet users with an effective weapon against phishing, pharming and similar cyber swindles.

Phishing or pharming sites will not be able to obtain SSL certificates from a trusted CA.

Establishing a Secure Connection — How SSL Works

An SSL-encrypted connection is established via the SSL "handshake" process, which transpires within seconds — transparently to the end user. In essence, the SSL "handshake" works thus:

- When accessing an SSL-secured Web site area, the visitor's browser requests a secure session from the Web server.
- The server responds by sending the visitor's browser its server certificate.
- The browser verifies that the server's certificate is valid, is being used by the Web site for which it has been issued, and has been issued by a Certificate Authority that the browser trusts.
- If the certificate is validated, the browser generates a one-time "session" key and encrypts it with the server's public key.
- The visitor's browser sends the encrypted session key to the server so that both server and browser have a copy.
- The server decrypts the session key using its private key.
- The SSL "handshake" process is complete, and an SSL connection has been established.
- A padlock icon appears in the browser's status bar, indicating that a secure session is under way.

Conclusion — The Key to Online Security

Demand for reliable online security is increasing. Despite booming online sales many consumers continue to believe that shopping online is less safe than doing so at old-fashioned brick-and-mortar stores.

The key to establishing a successful online business is to build customer trust. Only when potential customers trust that their credit card information and personal data is safe with your business, will they consider making purchases on the Internet.

With a Starfield Technologies SSL Certificate your customers will know that they can trust your business.

A Starfield Technologies SSL Certificate provides a convenient, cost-effective and reliable means to secure your business's online transactions.

Once installed on your business' Web site the certificate will safeguard sensitive data by securing online transactions with up to 256-bit SSL encryption.

With a Starfield Technologies SSL Certificate your customers will *know* that they can trust your business.

Applying a Starfield Technologies SSL Certificate to your online business today will secure your online sales.