WHY YOU NEED AN SSL CERTIFICATE

In the world of electronic commerce, security is paramount. Although Web sales are on the rise, widespread fears about sending private data over the Internet keep millions of potential shoppers from buying online.

According to Connecticut-based IT research firm Gartner, Inc., 15 percent of U.S. Web shoppers are so worried about online fraud that they don't shop on the Internet at all. The numbers are even higher in Great Britain, with 41% of respondents to a CyberSource Ltd. survey citing security fears as one reason they don't shop online.

To run a successful Internet business today, you absolutely *must* assure customers that their credit card numbers and personal information will be kept safe from interception. If consumers perceive that their sensitive data *might* be compromised online, they are unlikely to do their shopping on the Internet.

But the news isn't all bad. In response to the growing number and sophistication of Internet thieves, Web users are getting smart about online security. More and more of them are looking for the padlock icon, the "https" prefix or a green address bar before submitting personal information to *any* website.

It doesn't matter how big or old or trusted your business is -- if your company's website doesn't display the telltale signs of a Secure Sockets Layer (SSL) Certificate, visitors may leave before making a purchase, creating an account or even signing up for a newsletter.

Installing an SSL Certificate on your website protects information flowing to and from your site from cyber thieves intent on stealing personal data. Names, addresses, passwords, account and credit card numbers – all are safe when submitted to a website with a valid SSL.

Go Daddy sells more new SSL Certificates than any other SSL provider in the world, making it #1 in net-new SSL Certificates.

GODADDY.COM® VERIFIED & SECURED VERIFY SECURITY

What is an SSL Certificate?

At its most basic, an SSL Certificate is a piece of software that encrypts all information moving to and from the Certificate holder's website. This means no exchange between the website and its visitors can be intentionally or accidentally "overheard" by a third party, regardless of whether the visitor is placing an order or just signing up for a newsletter.

Once a website visitor enters a secure area of an SSL-protected website, the following takes place:

- The visitor's browser requests a secure session from the server on which the website is stored.
- The server responds by sending the visitor's browser a digital copy of its server certificate.
- The visitor's browser verifies that the server's certificate is valid, is being used by the website for which it was 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 a secure connection has been established.
- A padlock icon and "https://" prefix appear in the visitor's browser bar, indicating that a secure session is under way (unsecured websites showing an http:// prefix typically lose customers at this point). If protected with a Premium SSL Certificate, a green address bar will also appear including the Certificate holder's name.

In a survey conducted by Synovate, 62% of respondents said they look for the lock icon in a web address bar and 55% for a logo from an Internet security provider.

Called the SSL "handshake," this entire process takes place behind the scenes, providing an uninterrupted experience for the site visitor.

If a visitor attempts to submit personal information to a website that is not protected by a valid SSL Certificate, the visiting browser's built-in security mechanism will send a warning to the user. A dialog box will appear telling him/her that the site is not secure and that sensitive data might be intercepted in transit by third parties. When faced with such a warning, most Internet users sever the connection.

SSL Certificates not only confirm the identity of the Certificate holder’s website to the visitor’s browser but also encrypt information sent and received by the holder’s website. Information contained in the digital Certificate includes:

- The Certificate holder’s name (individual or company)*
- The Certificate’s serial number and expiration date
- A copy of the Certificate holder’s “public” cryptographic key
- The digital signature of the Certificate-issuing authority

An SSL Certificate allows you to build an impenetrable fortress around your customers’ most sensitive data.

GODADDY.COM® VERIFIED & SECURED VERIFY SECURITY

Phishing and Pharming

Phishing and pharming continue to pose real threats to unsuspecting Internet users.

Phishing is a common scam that uses fake emails from legitimate companies to trick recipients into revealing their account numbers, passwords – even credit card and social security numbers.

The scam starts when an account holder with a legitimate business receives an email that looks like an authentic notice from the company where they do business. The email recipient is instructed to click through to a website where they are asked to “verify” their personal information. Such emails often threaten a loss of account access if the recipient doesn’t take action.

Once the recipients click through, they’re greeted by a knock-off website that only looks like the real thing. Unless the victim looks carefully or checks for the https:// prefix, they’re likely to submit the requested data, never knowing they’re handing their most private information to thieves.

More sophisticated than phishing, **pharming** is the process by which an Internet Service Provider’s (ISP) domain name server (DNS) entries are hijacked. The idea is to redirect Internet traffic to a fake website instead of the real thing. 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).

* Premium SSL Certificates only. Standard SSL Certificates contain the domain name only and no information on who purchased the Certificate.

How an SSL Protects Consumers Against Online Fraud

The first and most obvious way SSL Certificates protect consumers is by virtue of the verification required to receive one from a Certification Authority (CA) such as Go Daddy.

A "pharmer" simply will not be able to obtain an SSL certificate for the domain they've targeted, since they cannot prove domain ownership.

Those criminals who attempt to purchase SSLs for domains that resemble those of well-known companies will be foiled as well. The stringent fraud-prevention measures of most CAs lead them to detect such schemes, denying certificate requests for suspicious domains.

SSL Certificates protect consumers in other ways as well:

> **No lock icon:** Because CAs typically don't issue certificates to fraudulent phishing or pharming sites, such sites rarely use SSL encryption. Savvy Internet users 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 another domain owned by the pharmer, but the visitor's browser will warn him or her that the URL they're visiting doesn't 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."

When presented with such warnings, most Internet users are only too happy to abandon their activity or transaction. In this way, SSL certificates provide legitimate business owners and wary Internet users with an effective weapon against phishing, pharming and other cyber swindles.

What's Special About GoDaddy.com SSL Certificates

Like other SSL Certificates, GoDaddy.com SSL Certificates ensure that sensitive information is kept securely encrypted and safe from prying eyes. What's more, Go Daddy's rigorous authentication guarantees that our Certificates are issued only to entities whose existence and domain ownership can be verified.

Go Daddy SSLs offer industry-leading security and versatility:

- Fully validated
- Up to 256-bit encryption
- Valid up to 5 years (depending on certificate type)
- 99% browser recognition
- Stringent authentication
- Round-the-clock customer support
- Covers an unlimited number of servers (other Certification Authorities charge for every server)

There IS one thing you won't find in a Go Daddy SSL – an outrageous price tag. While they offer the same protection as other SSLs on the market, Go Daddy SSLs cost up to 90% less. No wonder Go Daddy is the #1 provider of net-new SSL Certificates in the world!

A GoDaddy.com SSL Certificate is an easy, cost-effective and secure way to protect visitor information and build trust.

GODADDY.COM® VERIFIED & SECURED VERIFY SECURITY

Industry-leading Encryption

GoDaddy.com SSL certificates support both industry-standard 128-bit (used by banks to safeguard sensitive data) and high-grade 256-bit SSL encryption to protect online transactions.

The actual encryption strength on a secure connection is determined by the user's browser and the server that the website resides on. For example, the combination of a Firefox® browser and an Apache 2.X Web server secured by a GoDaddy.com certificate results in up to 256-bit encryption.

Encryption strength is measured in key length — or the number of bits in the key. To decipher an SSL communication, one would need to generate the correct decoding key. Mathematically speaking, 2n possible values exist for an n-bit key. Thus, 40-bit encryption involves 240 possible values. 128- and 256-bit keys involve a staggering 2,128 and 2,256 possible combinations respectively, rendering the encrypted data virtually immune to decryption by an unauthorized party.

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.

Public and Private Keys

To obtain an SSL Certificate, an individual or company must generate and submit a Certificate Signing Request (CSR) to a trusted Certification Authority such as GoDaddy.com. It is the Certification Authority's job to verify the requester's identity, existence and domain registration ownership before issuing an SSL Certificate.

When you create a CSR, Go Daddy's Web server software creates two unique cryptographic keys: A **public** key, which is used by the visitor's browser to encrypt messages before sending them to the receiving server, and a **private** key, which is stored on the Certificate holder's local computer and used to "decrypt" the secure messages after receipt.

In order to establish a secure, encrypted link between your website and your customer's Web browser your Web server will compare 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.

Go Daddy's Strict Verification Process

Before GoDaddy.com issues an SSL Certificate, the applicant's company or personal information undergoes a rigorous authentication procedure that serves to verify the domain control and, if applicable, the existence and identity of the requesting entity. Thus, a GoDaddy.com SSL certificate guarantees that the Certificate holder is who it claims to be and has a legal right to use the domain from which it operates.

GoDaddy.com issues three types of SSL Certificates:

Standard SSL Certificate

- Verifies that the requesting entity controls the domain in the request.
- Are identified by the lock icon and "https://" prefix displayed in the user's browser bar.

Deluxe SSL Certificate   To order, call **480-505-8877**

- Available to any organization registered with a government authority.
- Confirms that the individual named in the Certificate is associated with the organization and controls the domain in question.
- Shows a lock icon and "https://" prefix in the user's browser bar.

Premium Extended Validation Certificate (U.S., Canada, U.K., New Zealand & Australia only)

- Available only to corporations that are legally registered and verified to have a status of "Good Standing," "Active" or equivalent.
- Typically requires a letter from an attorney or accountant.
- Displays the "https://" prefix and the certificate-holder's name against a green background in the user's browser bar.

While all certificate types are available for single domains (e.g. MyPersonalDomain.com), Standard certificates are also available in Single Domain, Single Domain with Unlimited Subdomains (Wildcard) and Multiple Domain (UCC) versions.

- **The Single Domain version** works with a single domain, such as: MyPersonalDomain.com.

- **The Single Domain with Unlimited Subdomains (Wildcard)** version secures a domain with unlimited subdomains, like:

  - *http://www.MyPersonalDomain.com/*
  - *shop.MyPersonalDomain.com*
  - *register.MyPersonalDomain.com*

- **The Multiple Domain (UCC) version** protects up to 100 domain names with one certificate. This certificate works exceptionally well with Microsoft® Exchange Server 2007 and Office Communications Server 2007, which often incorporate multiple domains. For example:

  - *http://www.MyPersonalDomain.com/*
  - *http://www.MyPersonalDomain.net/*
  - *http://www.MyPersonalDomain.org/*
  - *shop.MyPersonalDomain.com*

SSL Certificates - the Key to Online Security

Demand for reliable online security is increasing. Despite booming online sales, a significant number of consumers continue to believe that shopping online is less safe than shopping at 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.

A GoDaddy.com SSL Certificate provides a convenient, cost effective and reliable means of protecting your customers' online transactions. Once installed on your business website the certificate will safeguard sensitive data with up to 256-bit SSL encryption.

With a GoDaddy.com SSL Certificate your customers will know they can trust your business.

"Gartner: Financial fraud concerns turn some away from online shopping," Helen Leggatt for BizReport : Research : March 24, 2009,
http://www.bizreport.com/2009/03/consumers_in_the_us_are.html

The 5th annual "Online Fraud Report," CyberSource Ltd.,
http://www.cybersource.co.uk/news_events/releases/11thfeb09.html

"Fear of debt and fraud change the way online shoppers pay," Internet Retailer,
http://www.internetretailer.com/article.asp?id=30955