GUIDE

SSL 101: A Guide to Fundamental Web Site Security

GeoTrust®

SSL 101: A Guide to Fundamental Web Site Security

Introduction

It may seem obvious that more people are going online to shop, send email, manage their bank accounts, and just about everything in between, but when you stop to think about just how many people use the internet, the numbers are dramatic. Just 15 years ago, barely 15 percent of Americans went online; today, almost 80 percent of people in the United States use the internet.[1] Worldwide, the statistics are even more impressive: A decade ago, about 350 million people used the internet across the globe. Ten years later, that number has risen to almost ***two billion*** people.[2]

As use of the internet has grown, the web has also become more popular with scammers, identity thieves, and other cybercriminals. Threats to internet users have become widespread, and it is estimated that more than 3.5 million people fall victim to "phishing"—a type of online identity theft—each year in the United States alone.[3]

Given the number of people who experience phishing and other web-based scams—or hear about them from friends, family, or on the news—many internet users don't feel comfortable sharing their real names or other personal details online. In fact, recent research indicates that more than 62 percent of internet users in the United States are concerned about their online security.[4] If someone doesn't feel safe even sharing their name, then using a credit card to make an online purchase is out of the question. Internet users simply will not share information, much less transact with a web site, that doesn't demonstrate a certain level of security.

Fortunately there is SSL, a standard solution for protecting sensitive information online. But there's more to SSL than just basic safety. In this guide, you'll learn about what SSL does, how it works, and how it can help build credibility online.

SSL: The Foundation of Web Security

First developed in 1995, Secure Sockets Layer (SSL) security is now a universal technology used to secure web sites. Although it may sound complicated at first, SSL is actually a straightforward technology that helps ensure trust. In fact, it's difficult to imagine how the public internet would be possible without the ubiquitous security provided by SSL.

The web site specific element of an SSL certificate itself is essentially a small piece of code that the site owner installs onto the web site. After installation, the SSL certificate uses an extensive system of security checks that involve the server, the browser, and the data-center maintained by the certificate provider to establish a domain and server as trustworthy. After establishing trust, the certificate encrypts information sent over the internet so that cybercriminals can't intercept or decode it. In fact, SSL security is highly effective in protecting against sophisticated cybercrime attacks such as "man-in-the-middle" schemes where hackers can secretly eavesdrop on sensitive communications, including online credit card transactions.

SSL Authentication

When issued by a trusted, independent third party, SSL certificates also serve to authenticate web sites, a process that involves proving that the owner of a web site is who they say they are. To get his or her web site authenticated, the site owner must work with an independent provider, known as a certificate authority (CA), that offers SSL certificates. When a web site uses an SSL certificate from an authorized CA, the CA takes the time to research the site and verify its authenticity, a step that provides a certain level of assurance that this site is legitimate. Usually, a CA will request business registration documents and other types of proof to confirm the web site owner's location and identity.

While it is possible to self-sign SSL certificates—that is, individuals can create certificates and claim that they are legitimate—certificates that are signed by credible third parties are more secure and much easier to manage. When a web site has been authenticated by an independent CA, everyone can trust that the web site is genuine. Some servers will come with a self-signed SSL certificate, but these self-signed certificates are included specifically to be used for testing environments. Vendors, such as Microsoft, strongly recommend that this self-signed certificate be replaced with a third-party authenticated SSL certificate when the server is publically deployed. Web sites and servers that use self-signed certificates may trigger some browsers to display a warning to end-users suggesting that the connection may not be trusted.

SSL security has become so widespread and trusted that it is compatible with every major web server and web browser, and it is used to protect a wide range of online communications, not just web sites. SSL certificates can be used to safeguard emails, instant messages, voice-over-IP (VoIP) calls—virtually any information that passes between two servers over a network connection probably uses SSL security.

How SSL Encryption Works

Web sites secured with an SSL certificate encrypt information before sending it out over the network between server and browser.

To do this, the SSL certificate has two codes called "keys": a private key that is unique to the individual server that hosts the web site, and a public key that is available to any web browser that requests it. The data that is encrypted by the private key can only be decrypted by the public key, and vice versa—data encrypted by the public key can only be decrypted by the private key.

The level of security that SSL provides depends on a few factors, including the type of certificate a web site uses, the type of web browser someone uses, and the host server's capabilities. This is why SSL certificates offer a range of encryption levels, most commonly up to 256 bits.

To give you some idea of just how strong SSL encryption really is, consider this: 128-bit encryption can calculate 2^{88} times as many combinations as 40-bit encryption. **That's over a trillion times a trillion times stronger.** In fact, at current computing speeds, it would take a hacker a trillion years to break into a session protected by a 128-bit SSL certificate, and even longer to hack into a session secured with 256-bit encryption.

What the User Experiences

You don't need a background in IT or HTML coding to know when a site is protected with SSL. In fact, web browsers provide several visual cues to help you see when SSL is working. For example, the web addresses of sites that use SSL will start with **https://**, as opposed to **http://** for non-secured connections.

Most web browsers—including Internet Explorer, Firefox, and Safari—will also display a small padlock icon when you visit a site that uses an SSL certificate. The location and appearance of the icon may differ depending on which browser you use, so be sure to look carefully to find it.

Example of padlock icon in Safari

Example of padlock icon in Firefox

Example of padlock icon in Internet Explorer

When you click the padlock, many browsers will display information about the certificate, including which CA issued it and which company owns it. If you click for additional details, you will see the certificate's expiration date, verification fingerprints, and other technical information.

SSL Is Essential to Building Trust Online

If you own or operate a web site—especially one where visitors conduct online transactions, like making credit card purchases—then your visitors need to trust that your site is safe. Why is this so important? If someone visits your site and their credit card information is stolen by a cybercriminal, then they will probably never visit your site again. They might also post about their bad experience or give your site negative reviews on various social networking sites. Even though you had nothing to do with their loss, this experience can compromise the relationships you've built with your customers or scare away potential new customers.

Using SSL security is one of the quickest, easiest, and most cost-effective ways to build credibility and help ensure the safety of your customers and the success of your business. When data is encrypted, thieves can't steal it as it flows across the internet, so your customers' sensitive information remains protected and they gain confidence in your company. In short, when you protect your visitors, you also protect your online reputation.

The Importance of Choosing the Right SSL Provider

When people visit web sites, many know to look for logos from online security companies—also called trust marks—that indicate a site is safe to use. Recent research shows that 86 percent of shoppers look for trust marks and feel more confident disclosing personal

"The vast majority of our sales are made online, so securing our website is fundamental to our business. If there's no SSL security, then there's always the possibility that a customer's credit card number or other sensitive data can be stolen."

–Ming Keong, Director, iStyles

information on web sites that use them.[5] Considering that fact, choosing an SSL provider for your web site can be one of the most important business decisions you make.

Many companies sell SSL certificates, but only a select few have an established reputation for trust around the world. Before you purchase an SSL certificate, you should do some research and find out if the company is a well-known, credible SSL provider. Working with a provider that specializes in SSL security and associating your company with its brand can help bolster your site's reputation and trustworthiness.

The consequences of choosing an unreliable SSL provider can be serious. For example, on April 4, 2009, Extended Validation SSL certificates from GlobalSign[6] started failing for Firefox users visiting certain web sites because of a technical problem at GlobalSign. That's why choosing to work with a well established SSL provider that maintains a highly reliable infrastructure is critical.

"When I shop online, especially at a new site I'm not familiar with, I always check for a seal to make sure that the site is protected and that my credit card information will be safe. My site has been an ecommerce website from day one, so I knew I needed to offer SSL security."

–Melaine Mueller, Founder and Owner, Mel Boteri

Taking Security to the Next Level: EV SSL

Basic SSL security is a must-have for online stores and other transactional web sites, but you can use advanced SSL technology that offers even stronger encryption and a more rigorous business verification process. This type of SSL is called Extended Validation (EV) SSL, and it can also be used to give visitors an unmistakable sign—a green address bar in their web browsers—that your site is protected, helping to build even more trust in your site.

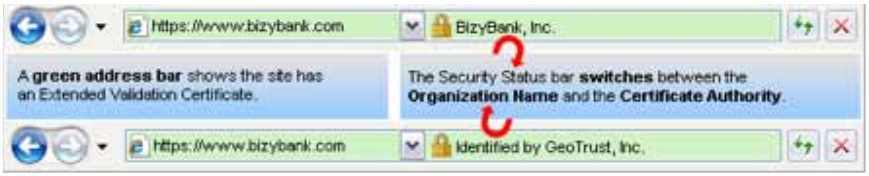
Why EV SSL Was Developed and How it Works

To meet the demand for low-cost SSL, many providers began offering certificates that didn't provide the same levels of encryption and authentication as higher priced certificates. To cut down on confusion and make it easier for users to identify sites that used the strongest SSL, the CA/Browser Forum[7], an independent industry group, established guidelines for an Extended Validation (EV) certificate.

"The EV SSL certificates are fantastic. They allow us to provide our clients with an even more cost-effective protection for their sites, so we're recommending them more and more."

–Kurt Davey, Founder and CEO, neoverve

EV SSL certificates use the same public/private key encryption method to protect data transmissions as other SSL certificates. However, the web site identity authentication is stronger. When a site uses EV SSL the company must undergo a more thorough authentication process to confirm the identity of the business. With EV SSL, the address bar in the latest web browsers will turn green, an obvious signal to web site visitors that a site is safe.



Why EV SSL Is Important

Research has shown that visitors are more likely to interact with your site—whether that means making a purchase, signing up for your newsletter, or registering for your services—if they see the green bar. In fact, in an independent study conducted by Tec-Ed, 97 percent of survey participants said that they would be more comfortable sharing personal and financial information on sites that display the green EV SSL bar.[8]

If you're looking for a surefire way to provide the highest levels of encryption combined with a clear signal that your site can be trusted, EV SSL is an ideal choice.

Getting SSL on Your Web Site

If you're ready to get SSL security for your web site, the first step you need to take is selecting a provider. There are many SSL companies to choose from, but remember that it's always best to choose a credible third-party SSL certificate provider that follows strict security guidelines.

When you work with trusted third-party SSL provider, you will be asked to confirm your business identity before the certificate is issued. Different providers may have different requirements, but many SSL companies ask for articles of incorporation, licenses, and other business documents. For example, GeoTrust requires companies to complete a certificate application and will confirm that your company is registered with a local, state, or national authority by viewing and verifying copies of registration documents. GeoTrust will also verify that the company has the right to use the domain name submitted in its application by checking with the domain name registrar. To make this process easier for customers, GeoTrust performs these checks by researching public databases. Customers are only asked to supply documentation directly if the company information cannot be verified through public sources.

During the purchase process, you will also need to generate a certificate signing request (or CSR) from your web server to the CA. A CSR is a small bit of code that initiates a request for a new SSL certificate and provides essential information enabling the CA to deliver a certificate matched to that server. The process for generating a certificate signing request is very straightforward and simple instructions are available from either GeoTrust or your server manufacturer. GeoTrust publishes information on how to get a CSR from various servers on their web site under Support.

Depending on what type of SSL certificate you've purchased, it can take anywhere from a few minutes to a few days for the CA to issue your certificate. Certificates that offer stronger security and validation usually take longer, but they are well worth the wait. For instance, an EV SSL certificate takes longer to issue, but it provides the best security and maximum reassurance so your customers feel safe using your site. An EV certificate also delivers the biggest business benefit because of the positive impact that can help convert more of your prospects into actual transaction-completing customers.

Once you receive your certificate, you will then need to install it on your web server. Though it may sound daunting, installing an SSL certificate is a straightforward process and some CAs like GeoTrust offer instructions to help you. The process for installing SSL certificates can differ between servers, so be sure to check with the CA if you have any questions. GeoTrust support is standing by to help.

Some CAs also provide a seal or other trust mark that you can display to show visitors that your site is protected by SSL security. To install a seal, you must copy the code snippet from your CA and paste it into the source code for your web site. Be sure to display the seal prominently on your site, including your homepage and—if you have an ecommerce site—any product pages or shopping cart pages. When visitors see an SSL trust mark on your site, they will spend longer on your site and will be more likely to sign up for an email list or newsletter, and make purchases. Web site gurus often recommend that you display your

trust seal above the fold on your home page. Many web sites go ahead and display their trust seal on every page just to make sure their customers have a constant reminder that security is paramount.

Conclusion: The Bottom Line Benefits of Using SSL Certificates

When you use SSL certificates on your site, you send a clear message—you care about the safety of people who visit your site, and your site can be trusted. However, not all SSL certificates are created equal. When you start to look for an SSL provider, be sure to choose a credible company that is widely known for offering trustworthy security. When it comes time to select an SSL certificate, consider opting for EV SSL. An EV SSL certificate from a trusted provider like GeoTrust will help you build trust in your site and protect your online reputation. Not only that, but EV SSL can encourage people to spend more time on your site, helping you to increase sales and conversions—and ultimately making your web site a success.

> "We've taken several steps to improve the shopping experience at our site, and using SSL certificates has been one of the most important. It's been a key factor in our success."
>
> **–Ming Keong, Director, iStyles**

Not All SSL Is the Same

Choose your SSL from an established, reliable and secure independent certificate authority. It should deliver at minimum 128-bit encryption and optimally 256-bit encryption. It should be issued from a globally-available root infrastructure using 2048-bit RSA keys or better. The SSL issuing authority should maintain industrial-strength data centers and disaster recovery sites optimized for data protection and availability. Your SSL certificate authority must have its authentication practices audited annually by a trusted third-party auditor such as KPMG, Deloitte & Touche, or Ernst & Young. GeoTrust meets all of these requirements.

SSL Products from GeoTrust

GeoTrust offers a range of reliable low-cost SSL certificates to meet your individual needs:

- **GeoTrust® True BusinessID with EV** – Get the credibility of a well-established SSL provider, the green address bar and a dynamic trust seal from GeoTrust at an affordable price
- **GeoTrust® True BusinessID** – Get name brand SSL that authenticates your business identity along with a dynamic trust seal at an affordable price
- **GeoTrust® True BusinessID Wildcard** – Protect unlimited subdomains with reliable SSL from a certificate authority that maintains a reliable, military-grade data center
- **GeoTrust® QuickSSL® Premium** – Get inexpensive basic SSL encryption from GeoTrust's fast and convenient issuing system
- **GeoTrust® Enterprise SSL** – Purchase SSL certificates in bulk and issue them on-demand

Contact Us

www.GeoTrust.com

CORPORATE HEADQUARTERS
GeoTrust, Inc.
350 Ellis Street, Bldg. J
Mountain View, CA 94043-2202, USA
Toll Free +1-866-511-4141
Tel +1-650-426-5010
Fax +1-650-237-8871
enterprisesales@geotrust.com

EMEA SALES OFFICE
GeoTrust, Inc.
8th Floor Aldwych House
71-91 Aldwych
London, WC2B 4HN, United Kingdom
Tel +44.203.0240907
Fax +44.203.0240958
sales@geotrust.co.uk

APAC SALES OFFICE
GeoTrust, Inc.
134 Moray Street
South Melbourne VIC 3205
Australia
sales@geotrustaustralia.com

1. Pew Internet & American Life Project, Trend Data: http://www.pewinternet.org/Data-Tools/Download-Data/Trend-Data.aspx [Accessed January 12, 2011]
2. Internet Usage Statistics, The Internet Big Picture: http://www.internetworldstats.com/stats.html [Accessed January 12, 2011]
3. ZDNet.com, "Gartner puts phishing tab at 3.2 billion": http://www.zdnet.com/blog/security/gartner-puts-phishing-tab-at-32-billion/755
4. Survey conducted by Harris Interactive, March 2009 on behalf of Microsoft and NCSA
5. "Consumer Online Shopping Fears"; survey conducted by Javelin Strategy: http://www.firstdata.com/downloads/thought-leadership/fd_consumeronlineshoppingfears_research.pdf
6. https://bugzilla.mozilla.org/show_bug.cgi?id=508408 [8/27/2010]
7. http://www.cabforum.org/
8. http://www.verisign.com/static/040655.pdf