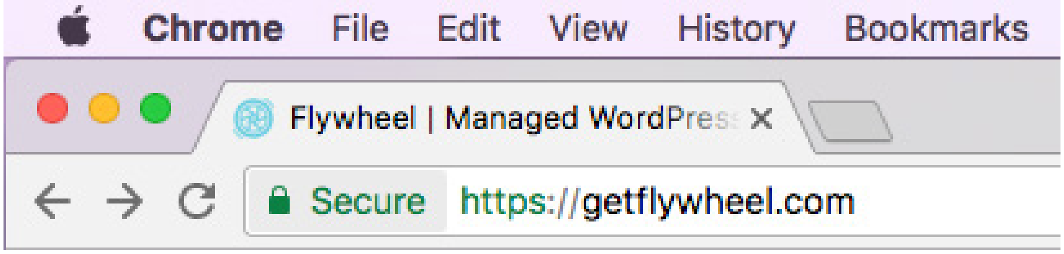
The complete guide to SSL

SSL is an important little acronym that every single site owner should know about. If this is all a new concept, don’t sweat it – this free ebook will give you all the details so you can keep your site secure, follow best practices, and install an SSL certificate easily (and for free!).

What is SSL?

SSL, or Secure Sockets Layer, is a protocol used to secure and encrypt communication between computers. While you may not realize it, you've probably seen this before. Take a look at the address bar of your computer, next to the URL. If you're using Chrome or Firefox, there's usually a little green padlock and the word "Secure." Safari also uses a padlock, but it'll be gray. Here's an example:



Before we go too much further, let's get the technical details out of the way.

At the heart of SSL is asymmetric (or public-key) encryption. This requires each party to generate a public and private key pair. Think of it like a lock on a door: Anyone can walk up to a door, inspect the lock, and even try to open it with their own key, but only the right key will actually unlock it. In this analogy, the door locks are public keys, because they're visible and public. Private keys are, well, keys, and are used to unlock the public keys. If you know a person's public key, you can encrypt a message using it that only they will be able to decrypt and read.

On top of that SSL, has one extra element: a certificate authority, or CA. CAs, such as Let's Encrypt, RapidSSL, or InstantSSL, not only issue SSL certificates but also verify their authenticity. You'll need to get a certificate from a certificate authority in order to utilize SSL (or from Flywheel, if your site is hosted here, but more on that in a second!).

> *"At the heart of SSL is asymmetric (or public-key) encryption.*

Certificate authorities have what is known as a "root certificate," or what is effectively the "master certificate," under which all issued certificates are signed. If you buy a certificate from Let's Encrypt, browsers will use their root certificate to check whether or not yours is legit when they connect to your server. End users don't really see the encryption process happening because most of the work is all done behind the scenes by the certificate authority.

An SSL connection works just like a public key exchange but with the addition of the CA to make sure the server you're trying to get data from is legit. Here's what happens during an SSL connection:

1. **You (the user) navigate to a secured web page, and your computer reaches out to that server.**
2. **The server responds with their public certificate (same as a public key).**
3. **Your computer checks the certificate to make sure it is valid and was issued by a trusted CA.**
4. **Assuming the certificate is valid and trusted, your computer uses the server's public certificate to generate a random key and encrypts your request (all of the data you want from the website), then sends the request and the randomly generated key to the server.**
5. **The server decrypts the data and responds by encrypting its message with your randomly generated key.**
6. **This process repeats until your session is done.**

When should I use SSL?

In the past, SSL was important for one very specific reason: encrypting communication and securely storing information. This is incredibly beneficial (and essentially required) for eCommerce stores or sites handling sensitive information. As a site owner, this is important because you don't want that information to be compromised. Plus, you want to offer your users a stellar experience, right? SSL will help you do that.

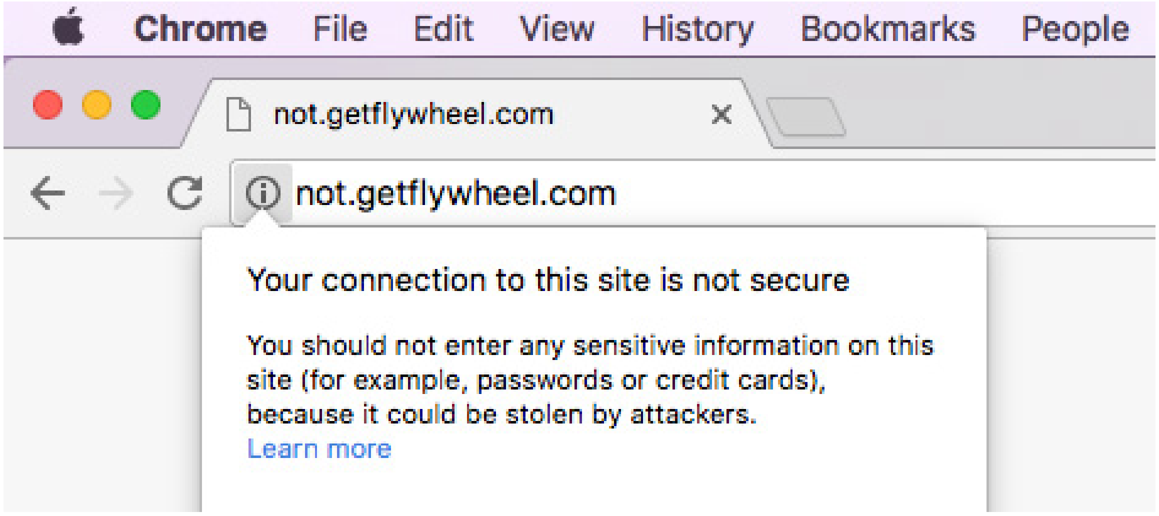
Another benefit of SSL is that it helps to build trust with your users. Before you can install an SSL certificate on your site, you have to answer a few questions about your site and/or business. This allows the certificate authority (the site you buy the certificate from) to verify that you are indeed the website and business you say you are. This means that if your site has SSL installed, your users can trust that you're a legitimate company that won't steal their information. And I'm guessing you want to build that trust with your users.

There's one final reason SSL is important for your WordPress site: SEO. Google has started flagging sites that store passwords or credit card information without SSL as insecure, as part of a long-term plan to mark all sites without SSL as insecure. That's a huge initiative, and if your site doesn't have SSL installed, it could seriously hurt your traffic and conversions.

As of October 2017, Google Chrome is taking proactive steps to help increase awareness around secure versus non-secure websites, and Mozilla Firefox is joining the efforts as well. And the number one requirement is an SSL certificate. Chrome and Firefox released the updates stating their intention to make the web safer for everyone.

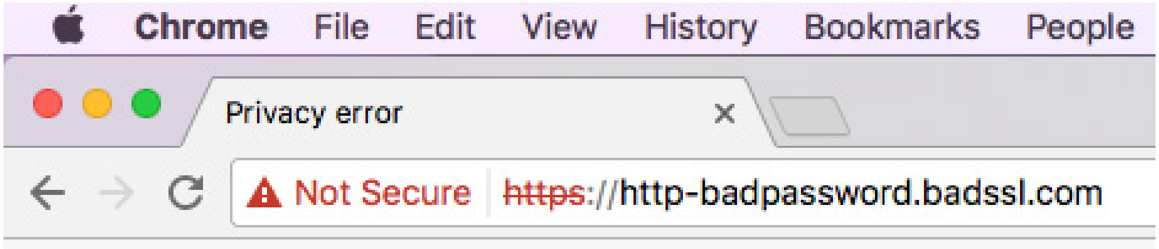
When an SSL certificate has been installed on a site, you can tell by looking at the URL. In Chrome and Firefox, there's usually a little green padlock with the word "Secure." Safari has a gray padlock next to the site name. You can also tell by looking at the beginning of the URL itself. A not secure website will use http while a secure site will use https.

These messages are non-intrusive, and can establish a lot of trust with your users because they know their information is safe on your site! On the other hand, if you don't install an SSL certificate, you're going to see some not-so-welcoming errors that might cause your users to abandon your site. In Firefox, there are various icons, including a gray padlock with a warning triangle and a gray padlock with a red strikethrough. In Chrome and Safari, either an information symbol or red warning symbol will pop up for not secure sites. Here's what they look like.



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers.
Learn more



As you can see, these errors are definitely not something you want your users to see on your site. Luckily, there's a super easy fix to make your site secure and get rid of that message!

The web is moving towards a more secure place, which means that no matter what type of site you're running, having an SSL certificate installed will help your site thrive. SSL keeps your information secure, helps to build trust with your users, and keep your site current with industry standards.

So, how do you get it?

How to add SSL to your sites

In the past, installing an SSL certificate was a bit of a juggling act. You'd have to buy it from a certificate authority, tell your hosting company about it, share information with both parties, and then it could be activated. That's not the worst system in the world, but it's not the smoothest, either.

Another option that may be easier is working with your hosting provider. Many hosts offer SSL certificates that are relatively easy to install or may come free or discounted. For example, if you host your site on Flywheel, thanks to our Simple SSL feature, all it takes is a couple clicks and zero additional cost! On Flywheel, SSL certificates come free with every single site and plan. All you have to do is enable the Simple SSL add-on in your Flywheel dashboard under the add-ons tab. The just click "Add SSL" and follow the instructions!

Get free SSL certificates!

They're included with every Flywheel plan

The easiest way to add Let's Encrypt's free SSL certificates to your WordPress site is by signing up with Flywheel. If you're hosting your site with us, Simple SSL is available at zero cost to you and can be installed with just a few quick clicks. Ready?

GET STARTED

Note: No matter how you go about installing an SSL certificate, make sure your site is validated and your DNS is pointed to your site.

ADDING A CERTIFICATE FROM AN OUTSIDE CERTIFICATE AUTHORITY

If you would like to install an outside SSL certificate on your host, there is a bit of a different process, and it might vary a little depending on who your host is. For sites on Flywheel, first you'll purchase the SSL add-on from the certificate authority you prefer. Then you'll enter the details to create your Certificate Signing Request (CSR), which will send you an email from which you download the CSR and upload it to the SSL provider. Last, you'll send Flywheel the files, and wait a minute to hear back that it's installed!

Like we said, it's not difficult to bring your own SSL certificate, but using our Simple SSL solution is sure fast (and free)! With world-class hosting and encryption all in one place on Flywheel, you don't have to bounce back and forth or find a third party provider.

No matter how you go about installing an SSL certificate, it's critical that your site has one in place. No only will it build trust with your site visitors, but it'll keep your site's information secure and keep it performing well in Google searches.

Interested in trying out a Simple SSL certificate from Flywheel?

GET STARTED TODAY!

What is Flywheel?

Flywheel is a delightful platform that empowers designers, developers, and digital agencies to focus on what they do best — building beautiful, functional sites for their clients. We make it a breeze to create and develop WordPress sites, handle hosting, manage projects, and ultimately scale your business.

Stop wasting time on server management, security plugins, caching, and all those other boring repetitive tasks that take your focus away from growing your business and jeopardize your relationship with clients. Get Flywheel and get back to doing what you love.

CONTACT SALES

sales@getflywheel.com | 402-223-6105

Or, sign up at getflywheel.com

FLYWHEEL