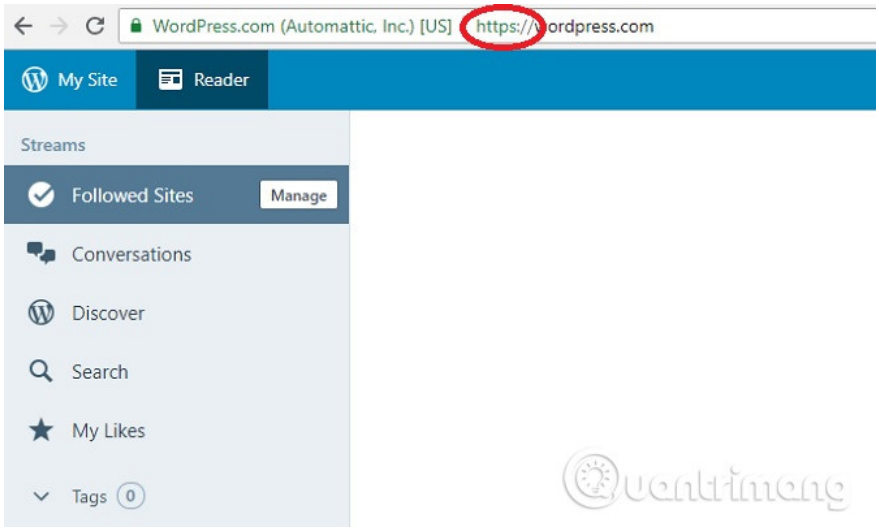
Don't believe 7 'myths' about this SSL and HTTPS certificate

On the network, secure connections are usually set up using SSL certificates (abbreviated as Secure sockets Layer). This can be confusing, in part because there are many 'myths' about them that you should not believe. Let's see 7 of those things.

See the URL of this article and you will see that it starts with https. The word 's' at the end means the connection between your device and this site is safe. On the network, secure connections are usually set up using SSL certificates (abbreviated as Secure sockets Layer). This can be confusing, in part because there are many 'myths' about them that you should not believe. Let's see 7 of those things.

1. Only e-commerce websites need SSL

You may have heard that only websites that require personal data need SSL certificates. This is true when you register or login to the site, you need to check the address bar that says 'https'. However coding is important for all websites, whether ecommerce or small blogs.



First, Google Chrome labels URL safety for HTTPS sites, so Google Chrome users who visit a site without an SSL certificate will see a warning page informing them that the site is unsafe.

Secondly, visitors through other browsers will find your site more reliable. Most users now know about checking for secure connections, so installing SSL certificates is a sign that you value their privacy. In fact, you are saying that the site visitor is a professional organization.

2. SSL will not affect web traffic

If Google Chrome does not fully load the site, its statistics will be affected. Imagine how many people find their connection unsafe and immediately turn away.

The problem is, even if the data does not seem to be dangerous, everyone is frightened to see a security warning. They envision themselves as victims of hackers. Thankfully, most users prioritize their security, so when you can't read your site, they will search for another site that provides similar information.

In addition, SSL certificates are essential for SEO. In order for Google to rank highly your website, in addition to having good keywords, you need to prove that you have implemented security measures. Of course, your website has the first position in the search results, the more people visit the site.

1. How does setting HTTPS affect SEO?

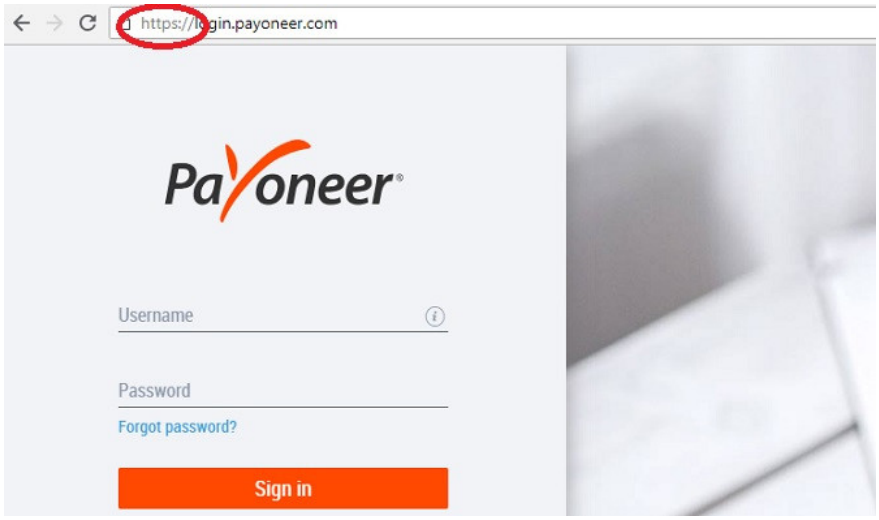
3. SSL makes the website load slower

Many people worry that HTTPS addresses will slow down websites, but this is not true because encryption does not affect your website speed. In most cases, because HTTPS actually refers to HTTP / 2 , a modification on the standard HTTP protocol. It is designed to reduce page load time by 50% by compressing data and reducing related processes.

If you want proof, check out some of your favorite websites, the most popular sites (including social networking sites like Facebook) that have SSL certificates and see how fast they are.

Sometimes the speed will be affected but it rarely happens and is negligible, only about milliseconds apart. This is mainly due to server distance. And cases of slowing down the web will become less and less when the certificate issuer (CA) secretly switches to the TLS protocol (Transport Layer Security).

4. Modern and superior SSL certificate



SSL certificates are great, but they are not the most advanced form of encryption widely used on the internet. In fact, many CA certificate issuers use TLS certificates instead. TLS certification is essentially the next stage in the life cycle of HTTPS.

TLS has been available since 2008, fixing some minor vulnerabilities in SSL certificates. However, until recently, most of it was only used for websites that requested payment information or manage money. PayPal is probably the most notable example of a website that uses TLS.

TLS certificates have become more popular, in fact, many encryption services use TLS instead of SSL certificates as default. However, SSL is more well known, so it is often used where visitors do not need to care about the difference between them, as long as your URL has HTTPS they will feel more secure.

5. expensive SSL certificate

The example below will reject the hypothesis that HTTPS is expensive.

Let's Encrypt is a popular service because it's effective and completely free. Many big name companies support this idea, including Facebook, Yoast, Mozilla, American Library Association, Server Pilot and Google Chrome.

In addition, freemium software is available. Encryption Everywhere, created by security company, Symantec, provides free SSL / TLS certificates and you can pay to own additional additional security features.

Admittedly, SSL certificates can be expensive, but most depend on the server. Sometimes, the host does not support third-party encryption, meaning they want you to use their own linked service to get more money from you. It is a terrible tactic, especially when users are under pressure from Google. You need to spend wisely, don't be fooled by your web host.

1. Instructions for establishing a free SSL security mechanism

6. SSL certificate encrypts all data

We should not assume that SSL certificates can be encrypted all for security. It is true that the data is encrypted but only during the transition process. HTTPS means your connection is secure, it does not mean secure web server.

Imagine it as a tunnel you are driving through. In the tunnel, your car is not attacked by anything from above, below or on either side. However, the problem still occurs when you reach the destination, you don't know what will happen ahead.

Similar to data, it is encrypted so you will not be a victim of man-in-the-middle (MITM) attack while moving between networks. But once that data is static (ie stored on someone's server), the SSL certificate does not do much. This is why HTTPS is now considered a basic security measure.

7. Effective SSL encryption

HTTPS provides good encryption and you may have heard a lot of good things about it. However, you should know that encryption cannot prevent something from being attacked. Companies need to take care of personal information in the safest way possible. However, the methods used to track passwords show how the encryption is ineffective, depending on the form used to store them.

Can you trust the SSL / TLS certificate? You should remember that no security is absolute and that vulnerabilities are inevitable.

Be sure to use a secure web browser

Do not underestimate the importance of basic online security levels. SSL certification is an important part of protecting you from cybercrime. Of course, you also need support from a strong security suite. Fortunately, mainstream browsers also know the importance of keeping their users safe on the Internet.

See more:

1. 7 reasons your website needs an SSL certificate
2. How to view SSL certificate details on Chrome browser?
3. Secure Web servers with SSL