Instructions for setting up HTTPS for simple websites

If you don't want to lose traffic, you should set up SSL for your site so that people can access it via HTTPS protocol. This article will show you how to set up HTTPS on the web in the simplest way.

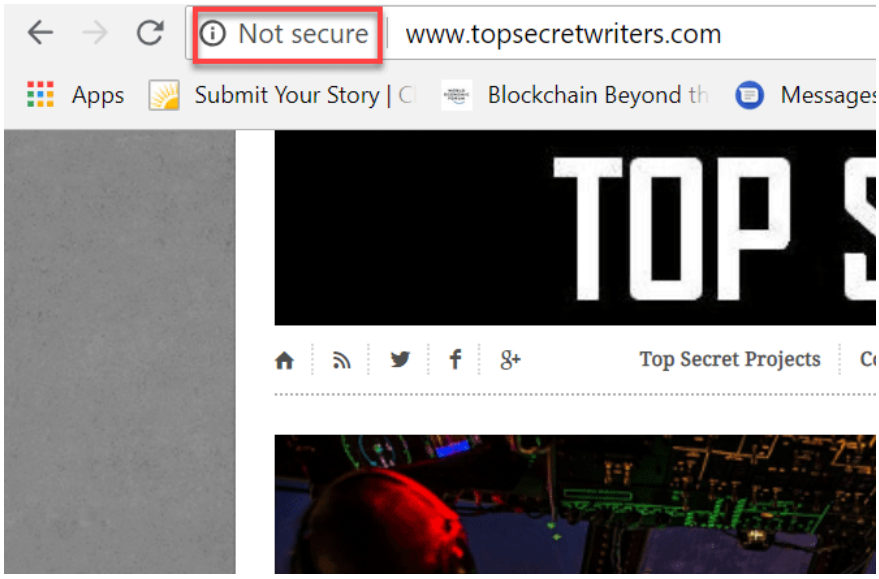
From July 2018, Google Chrome will mark the "Not secure" website if you still run the website using the HTTP protocol. If you don't want to lose traffic, you should set up SSL for your site so that people can access it via HTTPS protocol. This article will show you how to set up HTTPS on the web in the simplest way.

Note : If you still see your site marked 'Not Secure' after successfully installing the SSL certificate, see the problem-solving solutions at the end of the article.

Instructions for setting up HTTPS for simple websites

Get the SSL certificate

According to Google's developer blog, enabling HTTPS on the site is not only intended to protect data integrity, but also makes website visitors feel safer. In addition, many new browser features also require HTTPS. Recently, if you open a website in the Chrome browser, you will see a large 'Not Secure' message in front of the URL.



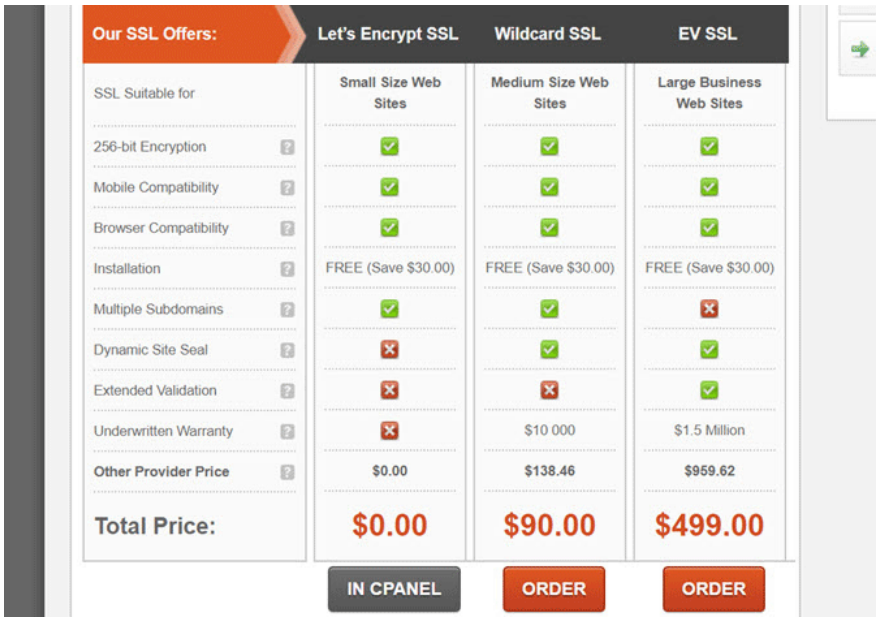
It is annoying to see this text on the website you have invested too much time and effort to develop it into a great website for visitors.

SSL setup is quite simple, but you need to consider your actual situation. If your hosting provider has provided a free SSL solution, you don't need to waste money to buy a new certificate.

Here are the SSL certificate options you can choose:

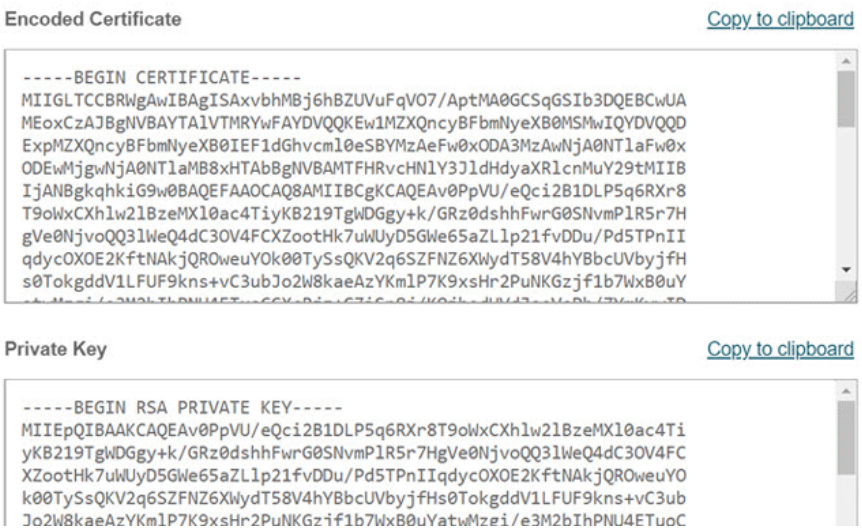
1. Free SSL certificate from your web server provider.
2. Get free SSL certificates from services like Let's Encrypt, Comodo or Cloudflare.
3. Buy SSL certificates from services like DigiCert, Namecheap or GoDaddy.

Free SSL certificate services often also offer paid certificates.



The difference between free and paid certificates is that you need to refresh yourself and do this via cron job (the job is done in a specified cycle). Some web servers provide management of these cron jobs for free such as Let's Encrypt, SiteGround service.

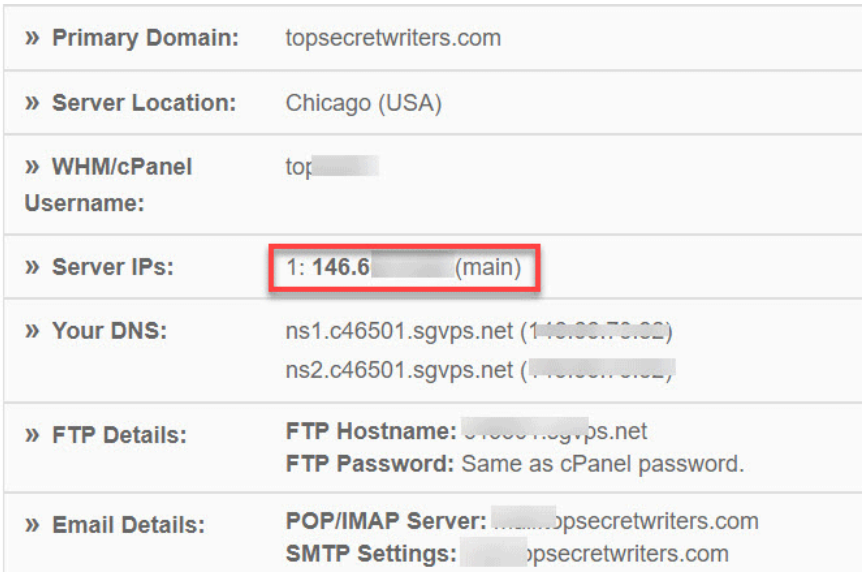
After selecting the SSL certificate, you will see a page like the one below. Certificates and keys are all part of the SSL package.



Copy both of this encrypted text and save them in a safe place.

Install SSL certificate

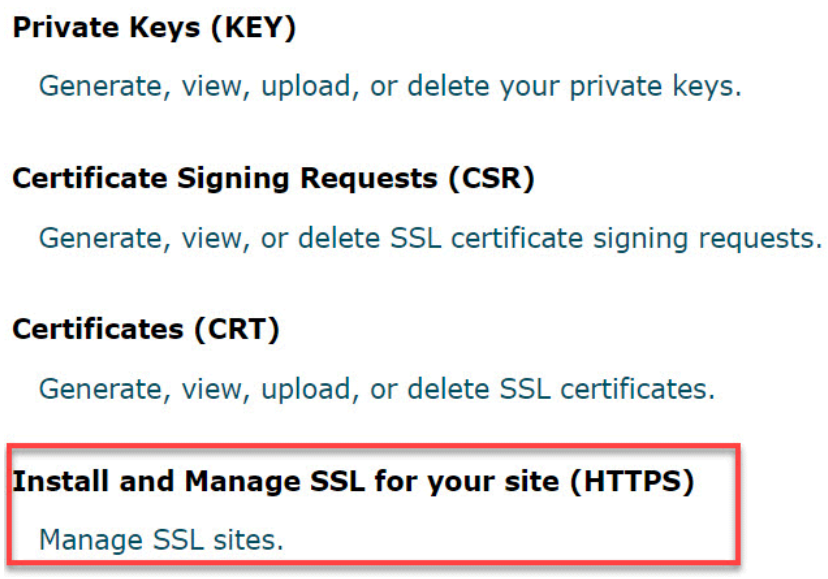
Most instructions that describe how to install an SSL certificate require that you have a private IP, which means you need to buy a more expensive hosting plan. If you have purchased this hosting plan, you can check it by visiting your account.



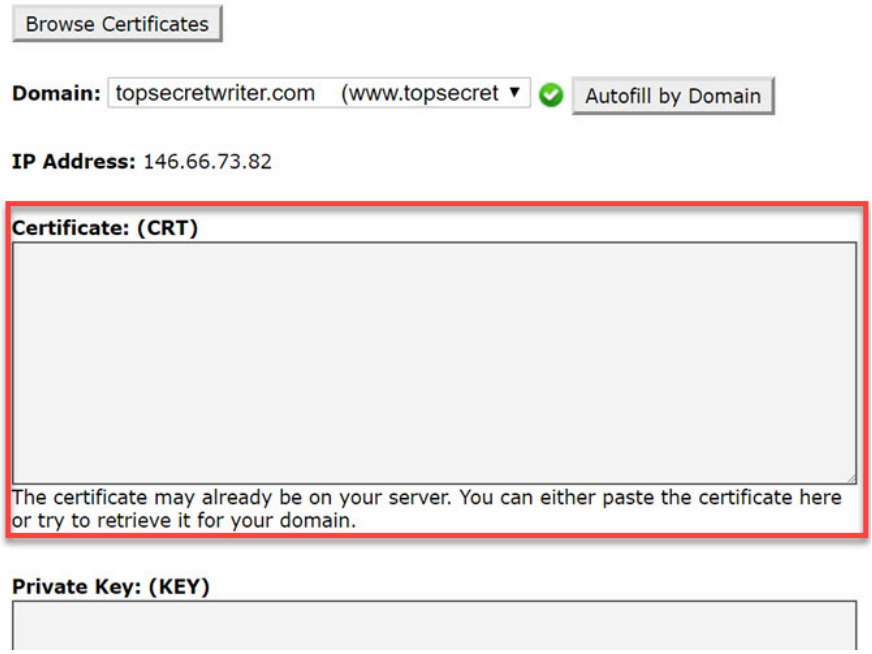
If using a shared hosting plan, it means that many websites share the same server, you will not have a private IP with the URL. However, this does not mean that you cannot install an SSL certificate. Thanks to technology called Server Name Indicator (SNI), you can still install SSL certificate on the website when there is no IP. If using a shared hosting plan, ask your hosting provider if they support SNI for SSL encryption.

To install the certificate, you need to access cPanel and click **SSL / TLS Manager** .

You will see different options for managing SSL certificates. To install the original SSL certificate for HTTPS, select the **Install** option.

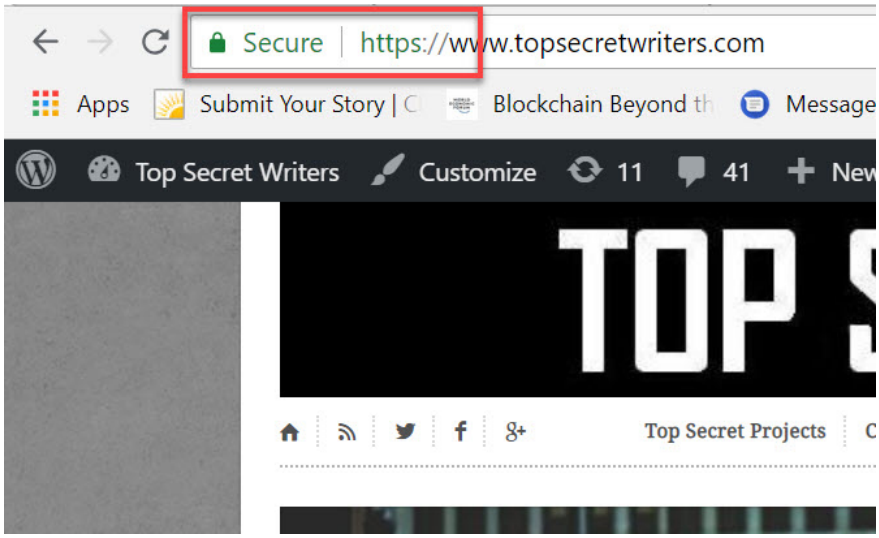


You will see the option to select the domain name you want to install the certificate to, and choose the correct domain name from the drop down box. Next, paste the encrypted certificate text that you copied above into the **Certificate** box.



Then, scroll down and paste the encrypted text for the copied Private Key when purchasing the certificate. When saving, you need to ensure access to WordPress and refresh all web caching and browser cache (press **Ctrl + F5**).

See your website again by typing the website URL with 'https: //' before it. If you have successfully installed you will see the word ' **Secure** ' before the website URL.

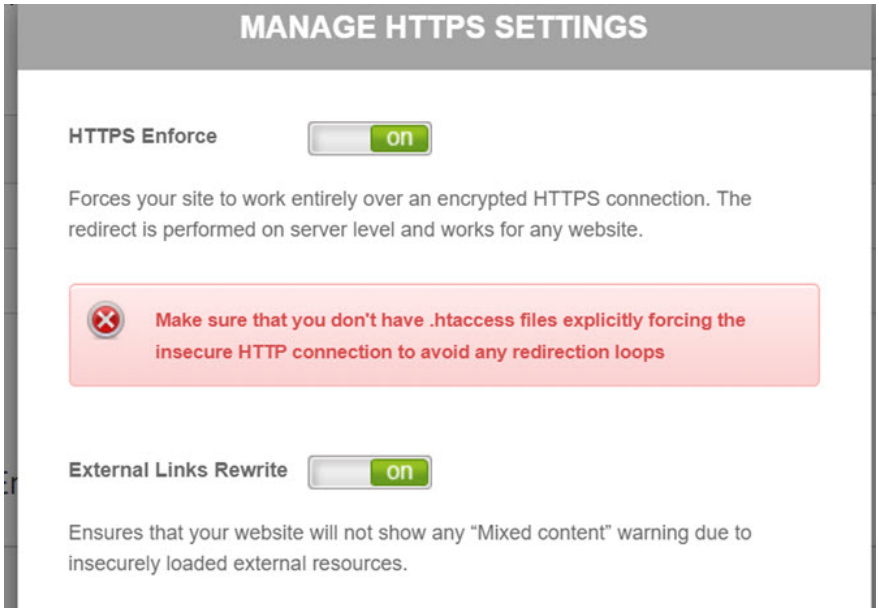


Now your site has an SSL certificate and access via HTTPS. If you still see the insecure version after taking the steps above, you need to force all traffic going through HTTPS.

How to turn on HTTPS on the website

Your server may have managed areas to handle required SSL changes:

1. **HTTPS Enforce** redirects traffic (for those who just enter the website URL without the 'https' in front of it) into HTTPS.
2. **The External Links rewrite** modifies external links starting with 'http' to 'https' to warn 'Mixed Content' not displayed in the browser for your site.



Without this auto feature, you need to do it manually by browsing to the **.htacess** file in the root directory of the web server. Add the following code:

```
RewriteCond %{HTTP_HOST} yoursitedomain.com [NC]
RewriteCond %{SERVER_PORT} 80
RewriteRule ^(.*)$ https://www.yoursitedomain.com/$1 [R,L]
```

Once you've saved this change, anyone who visits your site via HTTP will be redirected to HTTPS.

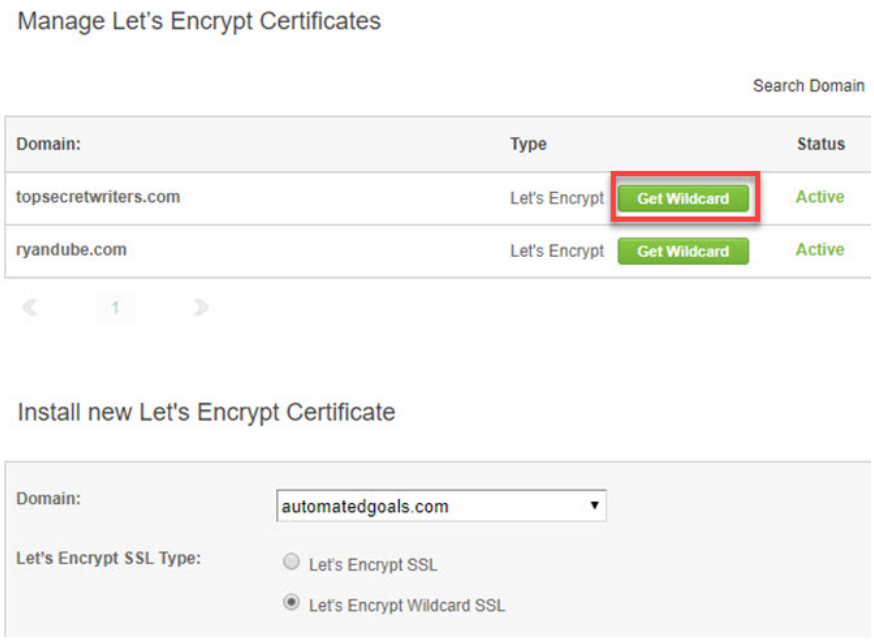
Some problems when setting up HTTPS for the site

Problem 1: Image of CDN

The first problem you encounter after setting up HTTPS on the web is that many images on the page are broken.

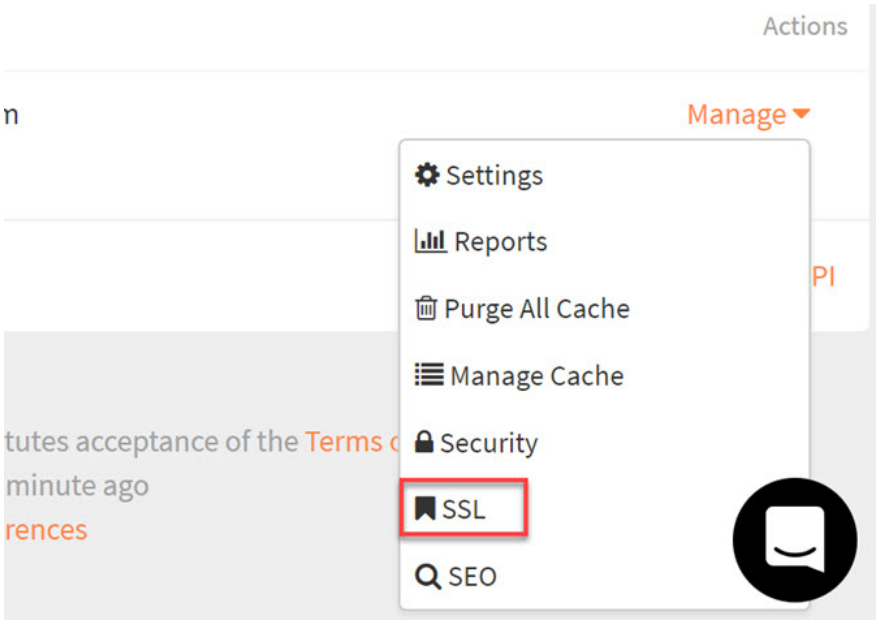
This problem occurs when all images are provided through unsafe CDN links. Because your traffic is redirected to use HTTPS, these images cannot be downloaded.

There are two ways to fix this error. The easiest method is to edit the SSL certificate to be able to use wildcards. For example, if you use Let's Encrypt, you will see the option to use the characters in the SSL management page.

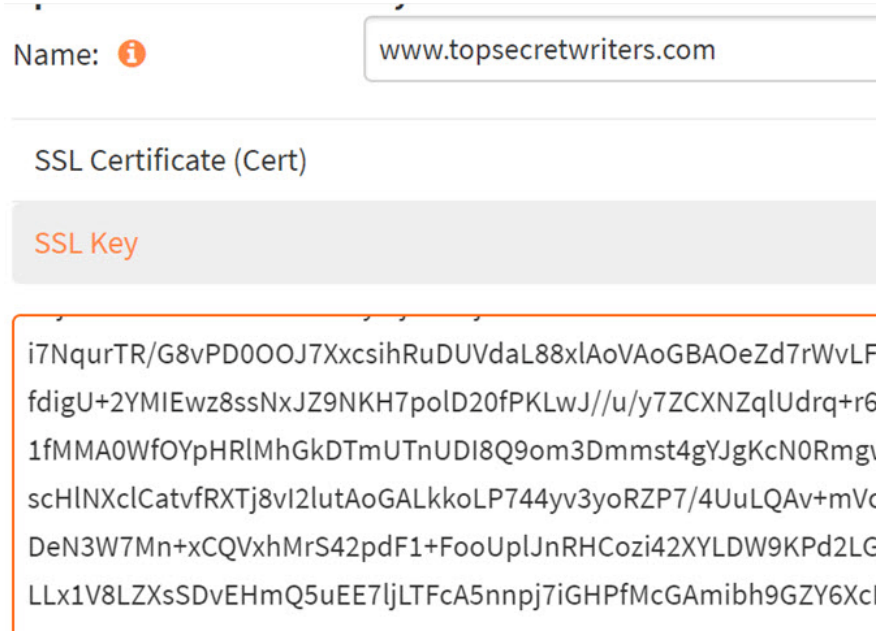


The wildcard allows you to use your SSL certificate on any of the site's subdomains. Enable this feature and get CA-encoded certificates, keys, and text packages from SSL information.

Access the CDB service to paste the SSL certificate and the Private Key into the corresponding fields.



Use the encrypted text you pasted into cPanel in the previous step.



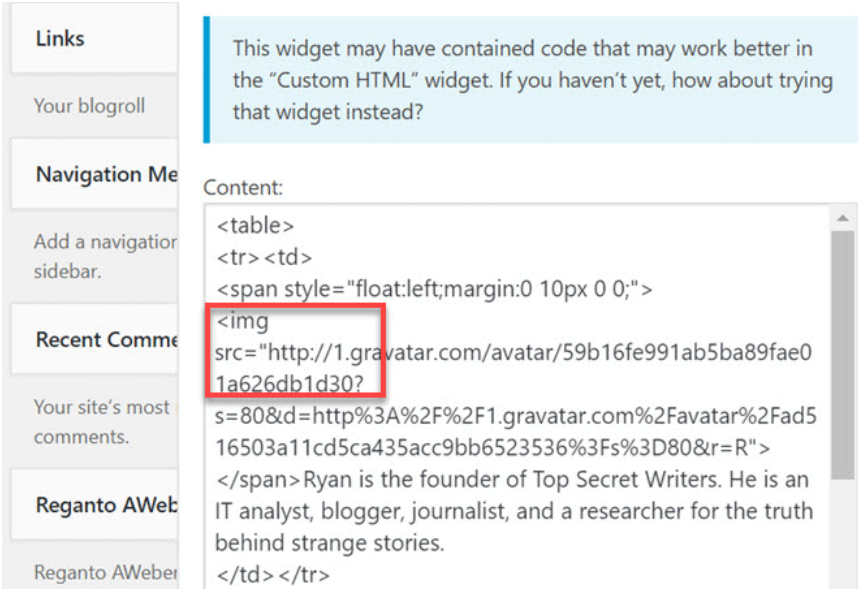
After saving, all photos will be downloaded on your site.

If the SSL service you use does not provide a wildcard option, you need to purchase a second SSL certificate for the CDN image and install it according to the steps above.

Problem 2: Unsafe links

If you haven't done anything except to enable SSL and HTTPS certificates, you'll see a 'Not Secure' error. This error is still displayed when you download the page via HTTPS. The common cause of this error is because you still have unsafe links on the page such as links in the sidebar, header or footer.

Access to WordPress and see header and footer codes as well as sidebar widgets. Also check out the links to services like Gravatar, Facebook and other services.



Change these links to use HTTPS instead of HTTP. Once completed, delete all cache and reload the page. All problems are solved and your site is safer.

I wish you all success!

See more:

1. How to turn on HTTPS for your blog site
2. How to fix SSL connection errors on Chrome and Firefox
3. Don't believe 7 'myths' about this SSL and HTTPS certificate

You finished reading the article "**Instructions for setting up HTTPS for simple websites**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.