create.

Switching from HTTP:// to HTTPS://

Our Guide To Securing Your Website With SSL Encryption

This guide is intended to walk you through all the actions you need to take when you are changing your website from http:// to https://

We have included step-by-step instructions and advice for the updates to services we recommend and for those which are popular with our customers.

As always if you have any questions drop a message to your Account Manager and they'll be happy to advise you.

Contents:

What Is SSL Encryption?

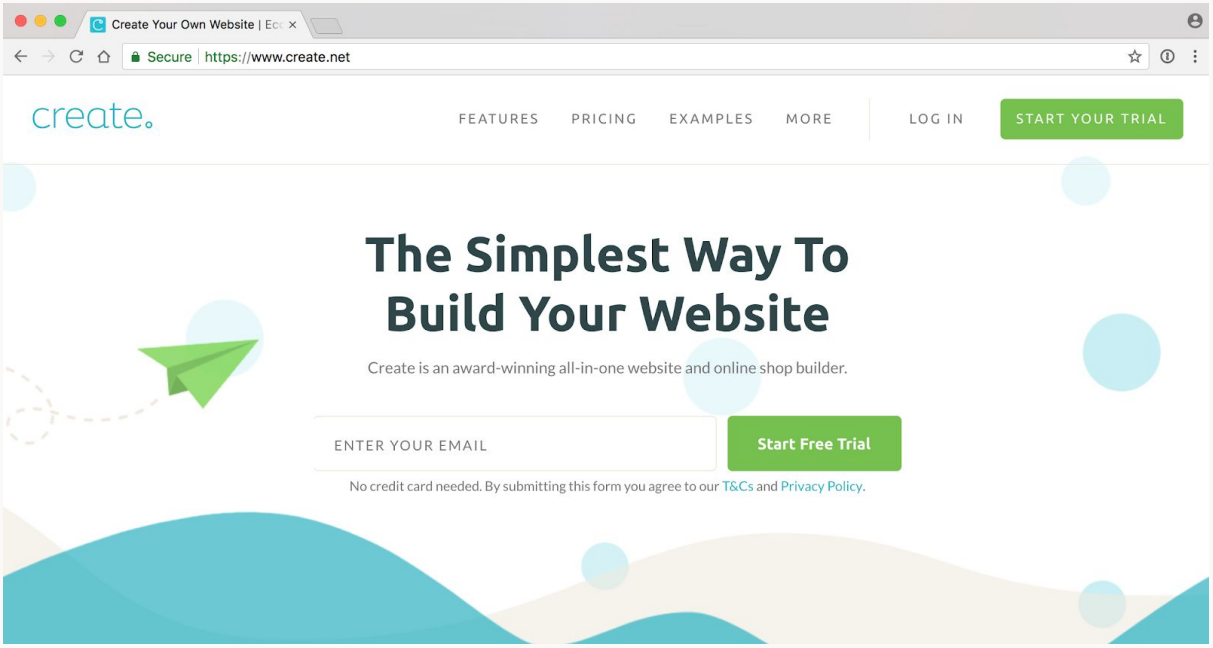
SSL stands for Secure Socket Layer, it provides protection for data and sensitive information passed between the web server and browser by encrypting it. This makes it less likely for a third party to intercept any information that is sent.

Without SSL encryption any data shared on your website is insecurely passed between the web server and browser, and has the potential to be intercepted.

Where sensitive site data, such as card payments are being passed, SSL encryption is crucial. All card processing services that are integrated with Create's checkout have high security standards and already use SSL. This ensures the card details entered by your customers will always be encrypted.

If you have SSL encryption on you will see that your domain name start with https://

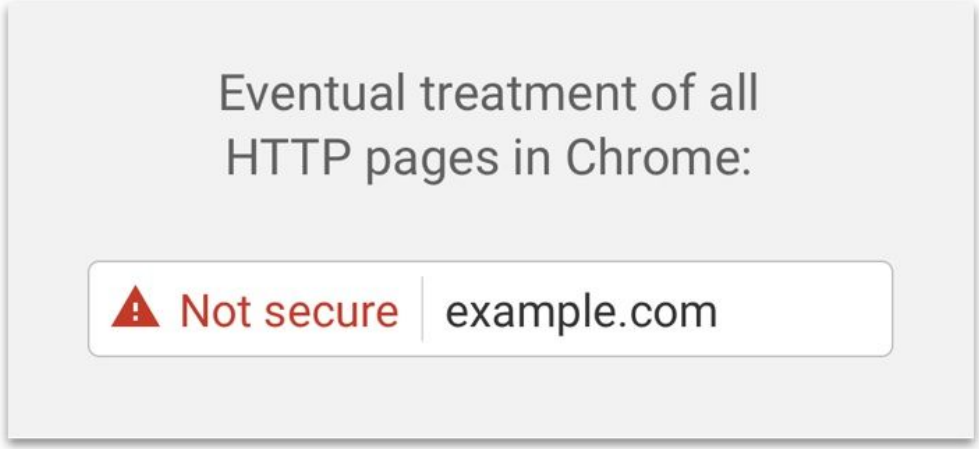
For example, when you look at our website Create.net, you will see that the Google Chrome browser displays a green "Secure" notification before our domain name (which starts https://) in the address bar.



Why Do I Need SSL Encryption On My Website?

Having the green padlock and https:// showing in your domain name indicates a safe website for customers to enter their payment and card details and increases customer trust.

Google plans to gradually increase the prominence of how it informs web site visitors that a site is not encrypted. Over the next year or so Google intends to display this message in red, and whilst a website without https:// may be perfectly safe to view, Google's message could be very off-putting to site visitors.

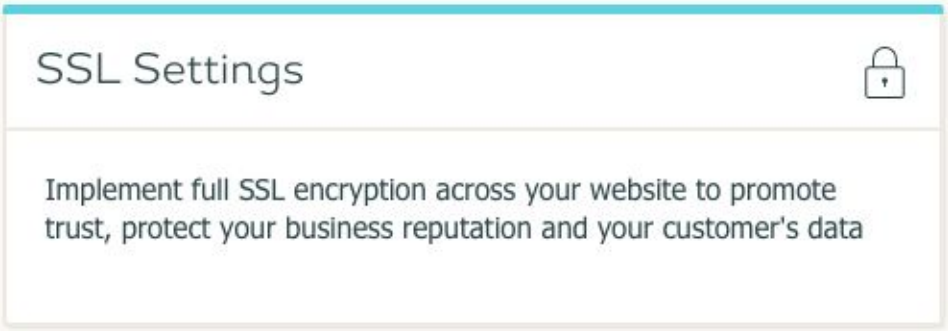


As Google push their agenda to ensure all websites are encrypted they have begun to prioritise secure sites and content. Having SSL encryption on your website will improve its ranking on search engines!

Aside from increased visitor trust and better sales conversion rates, you'll be providing a secure experience for your customers. Plus you won't need to worry about changing in the future as the warnings begin to have a greater impact.

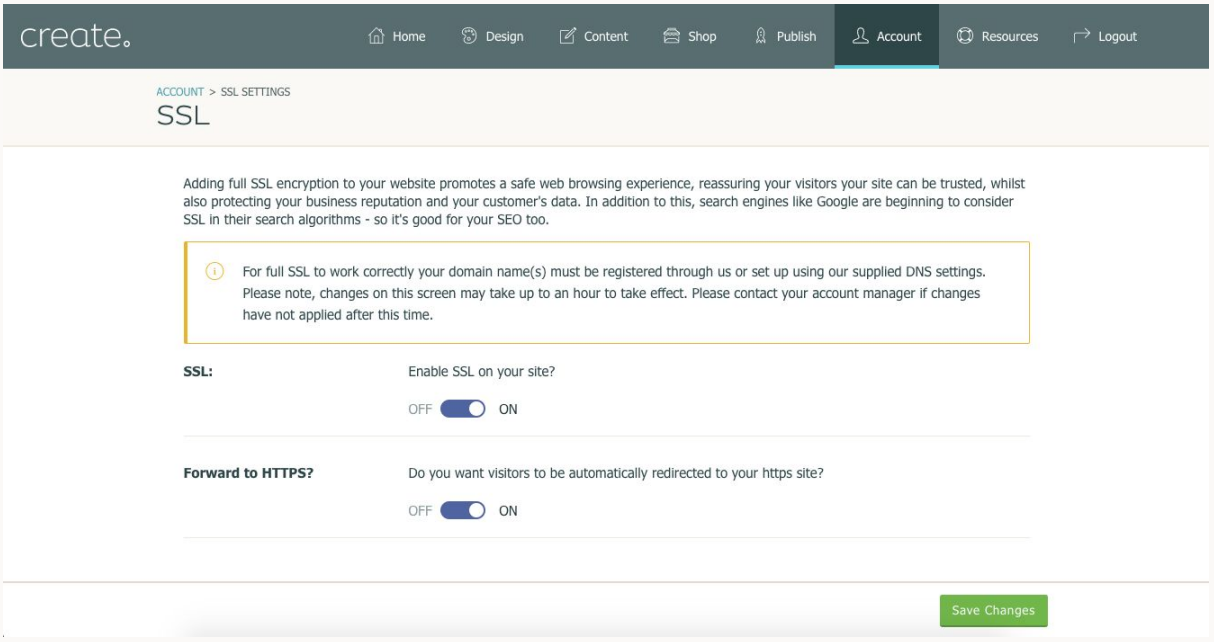
Turning SSL On

SSL Encryption is available on our Website Builder, Shop Builder, Shop Builder Pro, Shop Builder Advanced, Deluxe and Super packages



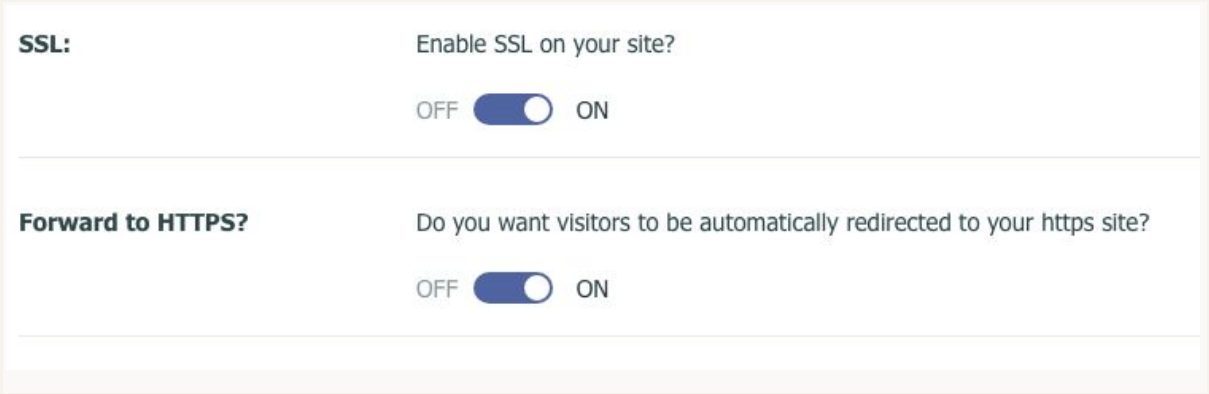
It's very easy to enable SSL encryption. To do this please follow the steps below:

1. Log into your Create account
2. Click on "Account" on the top menu
3. Click on the option "SSL Settings"
4. Turn on SSL with the toggle
5. Click the green "Save Changes" button



An additional option “Forward to HTTPS?” will appear once you have turned on SSL encryption. We recommend turning this on if you want people visiting http://www.yourdomainname.co.uk to be redirected to https://www.yourdomainname.co.uk.

If you leave this off Google and other visitors will see these as different websites with the same content and treat them as separate sites. This could result in duplicate content issues being registered in the search engines.



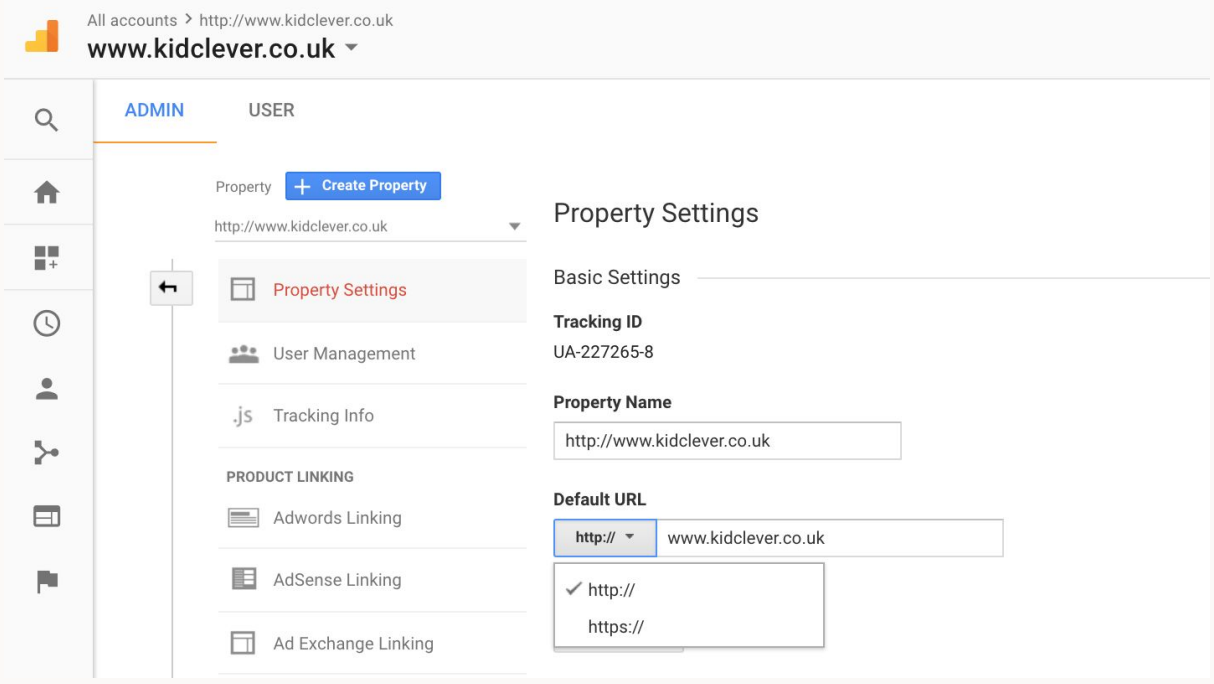
Once you’ve turned on the setting, allow up to an hour before the SSL encryption is fully completed and ready in your account. When it is, you will be able to locate the green https:// prefix in your URL in the browser window search bar, accompanied by a green padlock indicating the site is secure.

If your domain name doesn’t appear to have been updated to https:// after this time message your Account Manager and they can check the setup for you.

Updating Google Analytics

If you're using Google Analytics (or other Analytics programs like Statcounter) you'll need to update the URL to your new https:// one. Follow the steps below to update your URL in Google Analytics:

1. Log in to Google Analytics
2. Click on the "Admin" cog in the bottom left corner
3. Within the "Property" section choose the website you want to update from the drop down list (If you only have 1 you won't need to do this step).
4. Click "Property Settings"
5. In the Default URL drop down select https://
6. Scroll to the bottom of the options screen and press the Blue "Save" button



If you're not using Google Analytics now is a great time to get it set up, read our guide on how to do it.

Updating Google Search Console / Submit Your Sitemap

Once you've turned on SSL encryption and your website is up and running with https:// it's definitely a good idea to let Google know. Google advise that you add the https:// version of your website address as another profile in the Google Search Console.

Follow our guide on how to create a new profile in Google Search Console. Once you've created the profile, you should submit the sitemap. This will tell Google to come and crawl the site as you have made changes.

Once you've added the https:// profile don't delete the http:// one. You can review the progress Google is making indexing your website and see any reported problems by checking both profiles.

You can read more about Google's best practice at
https://support.google.com/webmasters/answer/6033049

Whilst Google has not set out any specific timescales for the amount of time it takes for them to drop the http:// version of your website and ranking the https:// one, we'd recommend allowing at least a week from the time you submit the sitemap.

During this time you may see both versions of your website in the search results and some fluctuation in ranking and visitors. Unfortunately how long this change will take to settle down is an unknown but Google have promised to minimise site disruption as they want website owners to make the change.

Updating Your Payment Gateway

Some of the payment gateways will require you to update your URL with them. While it may not stop working if you have the redirect switched on it's best practice to use the https:// url in case the redirection causes problems when completing your orders. The gateways below require updating.

Barclaycard EPDQ

You'll need to update the URLs in your Barclaycard EPDQ account settings. This is to ensure that your orders continue to be sent through to your Order Management area and your customers are directed to the right Thank you page after ordering.

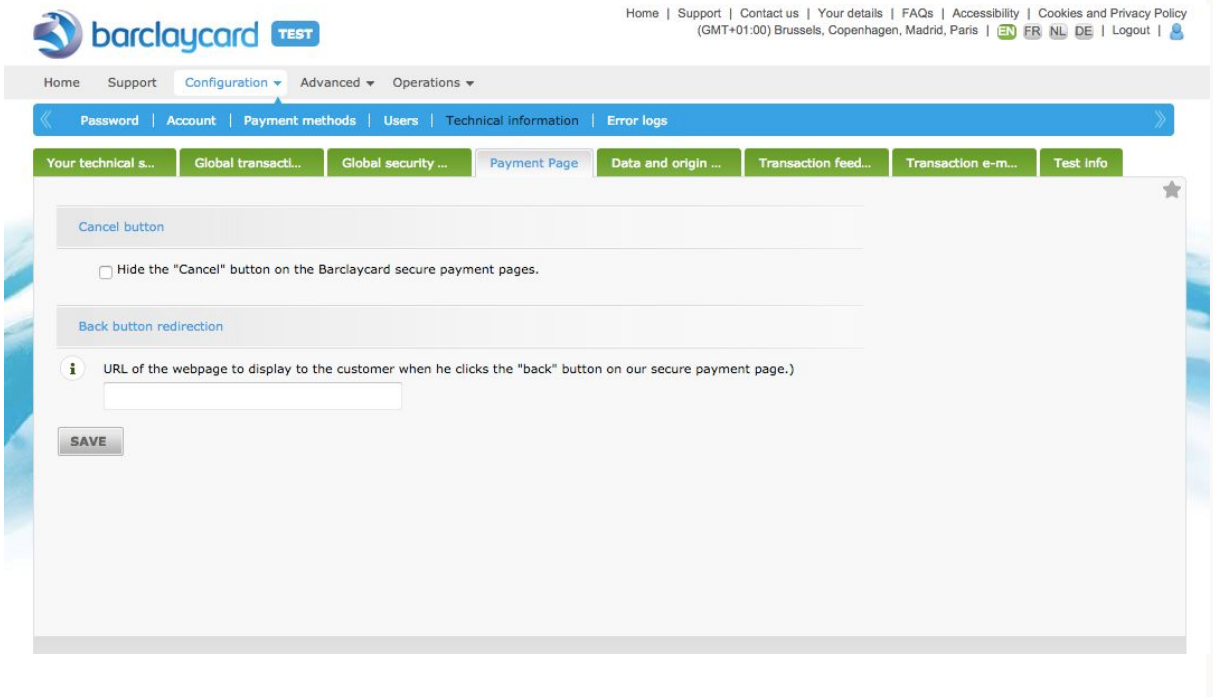
To get your updated URLs from your Create account please do the following:

1. Log into your Create account
2. Select "Shop" from the top menu
3. Click on "Shop Settings" in the left-hand menu
4. Click on "Payment Gateways"
5. Click on the edit icon on the right of the "Barclaycard" payment gateway section
6. You will see the information you require for the Barclaycard Portal.

You'll now need to update this information in your Barclaycard Portal, to do this follow the steps below:

1. Log into your Barclaycard portal
2. Click on "Configuration" on the top menu
3. Click on "Technical Information" on the blue sub menu
4. Click on "Payment Page" on the green menu
5. Copy the "Payment Form URL "Payment form URL" from the Barclaycard setup page in your Create account and paste it into the "URL of the webpage to display to the customer when they click the 'back' button on our secure payment page" field

6. Now click on “Data and Origin Verification” on the green sub menu
7. Copy the “Payment form URL” from the Barclaycard setup page in your Create account and paste it into the “URL of the merchant page containing the payment form that will call the page” field
8. Now click on “Template” on the blue sub menu
9. Copy the “Trusted dynamic template URL” from the Barclaycard setup page in your Create account and paste it into the "Trusted dynamic template URL" field
10. Copy the "Trusted website hostname" into the "Trusted website hostname hosting the dynamic template" field



Realex

If you are using Realex to accept payments through your e-commerce store you will need to let them know that the URL of your store has changed. If this isn't updated your orders will stop appearing in Order Management as Realex may be able to tell us that your order has completed.

To update the URL you'll need to send an email to the Realex team at support@realexpayments.com. Let them know that your URL has changed from HTTP to HTTPS as per the example below and change the red section to your domain name:

Referring URL: https://www.yourdomainname.co.uk/shop/checkout_process.php

To:

Referring URL: https://www.yourdomainname.co.uk/shop/checkout_process.php

Global Iris

If you are using Global Iris to accept payments through your e-commerce store you will need to let them know that the URL of your store has changed. If this isn't updated your orders will stop appearing in Order Management as Global Iris may not be able to tell us that your order has completed.

To update the URL you'll need to send an email to the Global Iris team at globaliris@realexpayments.com. Let them know that your URL has changed from HTTP to HTTPS as per the example below and change the red section to your domain name.

Referring URL: http://www.yourdomainname.co.uk/shop/checkout_process.php

To:

Referring URL: https://www.yourdomainname.co.uk/shop/checkout_process.php

PayPal

Create and Paypal work together so you don't need to setup anything in your PayPal account. However if we have advised you to enter a URL in your IPN callback area you should update it from http:// to https://

To do this follow the steps below:

1. Log into your Paypal account
2. Click on the "Profile" cog icon in the top right corner and select "Profile and Settings"
3. In the section titled "Getting paid and managing risk" click the Update link to the right of "Instant payment notifications"
4. Click the Edit Settings button (you won't see this if you don't have it set up) and edit your domain name to https://
5. Click "Save"

Update Google Adsense, Adwords, Merchant Centre

If you are running advertising, firstly ensure you have set up the domain redirect (steps above in the Enabling SSL section). This means that anyone typing in your domain name will be automatically transferred through to the https:// version of your website.

Next update any adverts or places which need to know you've changed your URL - like Google Merchant Centre. If you don't update your Google Merchant Centre URL Google will disallow your product feed because it has a different URL to the one they have registered.

To update your URL follow the steps below:

1. Log into your Google Merchant Centre account
2. Click on Business information on the left-hand menu
3. Click on Website and change the URL of your website from http:// to https://
4. You will need to verify your site again to show Google that you own the URL you have entered so click on Website on the left-hand menu
5. You'll see some options for verifying your URL. Choose HTML Tag and follow the instructions below to implement it in your Create account.
6. Once done come back to Google Merchant Centre to verify your site and complete the process

1. Log into your Create account
2. Click on "Content" on the top menu
3. Click on the "Page Options" icon for your Home Page
4. Click on "Meta Info" from the top tabs
5. Paste your code from Google into the box labelled "custom HEAD"
6. Click "Save Changes"
7. You will now need to publish your changes to your live site by clicking on "Publish" on the top menu and following the instructions to "Publish to Web"

Update Online Links

If you have turned on the Redirect option when you enabled SSL anyone typing in http:// or just www.mywebsite.co.uk will be directed to the https:// version of your website in their browser. To help inform Google that you've permanently updated your site it's good practice to go through the places you have your company listed and update them.

For example - edit your social profiles, if you have your website in your Twitter profile or on your Linkedin Company page, update them. If you don't have your website address there now is a good time to add them and start directing your followers to your site.

Update any online directories where you have listed your company and if you have people you've exchanged links with or received a mention on their website - drop them an email and ask them to update. It's a great opportunity to re-engage and approach them to see if there are more ways to work together.

Update Offline Materials

If you have your website address listed with http:// on your promotional products, headed paper, brochures, leaflets and business cards, next time you update these remember to change it to https://

Again, if you've turned on the redirect option when you enabled SSL anyone typing in http:// or just www.yourdomainname.co.uk will be directed to the https:// version of your website in their browser anyway - so you don't need to worry about rushing to change things.

Check Your Website For Content That Breaks SSL

Once you have turned on SSL encryption it is worth taking the time to click around the pages of your website and ensure that you don't have content which is insecure that is breaking the SSL encryption. If this is happening you will see the green secure message in the browser change to a red insecure one.

What Is Mixed Content And How Do These Errors Arise?

When you visit a website which is fully SSL encrypted, you're accessing the content over https:// and your internet browser is aware of this.

If any of your content is being served via a non https:// URL, your browser will pick up on this. Depending on the internet browser this can result in an "insecure content" warning for example, or the content could be blocked altogether.

Third Party Content (Not Hosted By Create)

Pay particular attention to any content you have added that was not sourced from Create, or that is being hosted externally, such as:

- HTML Fragments
- Externally hosted images
- A wallpaper that is hosted elsewhere
- Any third-party widgets or tools

It's likely that the provider of any third-party content will have a https:// version available on their website or upon request. If they do, updating to this on your website will stop the insecure message and improve the experience for your visitors.

How Can I Investigate Mixed Or Insecure Content Errors?

If you think you may have content on a page of yours that is being blocked or bringing up certificate warnings, use the steps below for locating that mixed content. Google Chrome makes it really easy to do this, and most modern browsers will have the same tools.

1. Go to the page of your website where the insecure message is displayed
2. In the top right-hand corner of the browser click the browser menu (often looks like three lines or three dots)
3. Click "More Tools"
4. Click "Developer Tools" and a new menu will now open
5. Using either the top menu bar on this page, or the bottom one, locate the “Console” tab
6. (As an alternative to the steps above you can also access the Console area by right clicking the page > click "Inspect Element > click "Console".)
7. The Console area will display any insecure or non https:// content.

I've Found An Error - How Do I Fix The Content?

For an idea on the type of content that could be causing an error take a look at our guide "How To Ensure Your Website Content Is Secure". With this in mind, look at a specific error using the steps above. Here is an example of an error you might encounter:

"Mixed Content: the page at https://yourdomainname.co.uk/page.html was loaded over HTTPS, but requested an insecure image http://yourdomainname.co.uk/page/image.jpg"

In this example it is an image that is causing the error, due to it being loaded via http:// instead of https://. If you click on the second URL (the http:// one), it will show you the insecure content.

Fixing the content will depend on the error shown. If the content, such as an image, is hosted externally we recommend adding the image to your Create account and replacing it on the page. However, using the tips in the above mentioned guide, you can determine how to update the content to be secure.