# My website shows as insecure due to mixed content?

SSH · https://computancy.co.uk/kb/my-website-shows-as-insecure-due-to-mixed-content/

Please note that if you have recently activated a computancy SSL certifcate for your domain, it can take up to 30 minutes to be installed across our load balancers.

**After an SSL has been installed, the website still loads with an insecure warning**

If the website is now showing your certificate but still has an insecure warning, this is often caused by 'mixed content' on the website. This means there is content on the page that is being loaded through a 'https://' URL. For a webpage to be classed as secure, **all** content must be loaded over HTTPS. This includes external images, JavaScript and CSS. You should search the source code of your website to locate the 'https://' references and update or remove them.

**Finding Mixed Content**

When visiting an HTTPS page in Google Chrome, the browser alerts you to mixed content as errors and warnings in the JavaScript console. You can open the console either from the View menu: View -> Developer -> JavaScript Console, or by right-clicking the page, selecting 'Inspect Element', then selecting 'Console'. You need to remove or update the 'https://' URLs listed in these errors and warnings in your sites source.

Alternatively, you can use the site ‘Why No Padlock?’ to identify mixed content: https://www.whynopadlock.com/

If the site is running WordPress, you can use the SSL Insecure Content Fixer plugin that should identify all mixed content and replace it with a secure version for you. You can find the plugin here: https://en-gb.wordpress.org/plugins/ssl-insecure-content-fixer/

Once all references on your website are called using https:// URLs, your site will load securely in your browser.