Insecure or mixed content and ads – FAQ

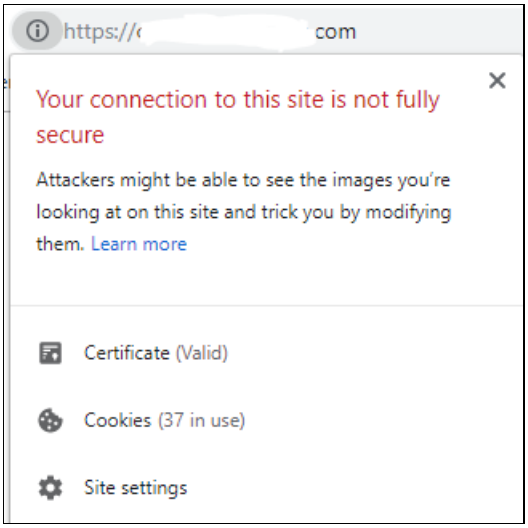
Last Modified on 10/15/2021 10:56 am EDT

What is insecure or mixed content?

Insecure content is any content request loaded in a browser over the insecure HTTP protocol. If your webpage is secure (loaded over HTTPS), but contains scripts, styles, images, or other linked content that are insecure (served over HTTP), this is called mixed content. Note that mixed content could also mean the converse—secure content serving on an insecure webpage.

How do I know if there is insecure content on my site?

Most often, publishers or their website users are alerted to insecure content by a warning in their website address bar. There might be an unlocked padlock icon or an information icon, and clicking on this icon will give a message warning that not all content on the page is secure.



If you are debugging your site with your console log open, you may also see a mixed content warning there.

```
⚠ Mixed Content: The page at 'https://googlesamples.github.io/web-fundamentals/samples/discovery-and-distribution/avoid-mixed-content/image-gallery-example.html' was loaded over HTTPS, but requested an insecure image 'http://googlesamples.github.io/web-fundamentals/samples/discovery-and-distribution/avoid-mixed-content/puppy.jpg'. This content should also be served over HTTPS.                    jquery.js:5562
```

Why am I seeing insecure content serving with ads?

Best practices dictate that all content on the internet should be secure. However, there are thousands of players in the programmatic advertising industry, and not all of them are conforming

to these standards yet.

In any given real-time auction, there are potentially hundreds of requests being made as SSPs, DSPs, and buyers pass information back and forth. Most of the time, if you see insecure content that appears to be related to ad serving, it will be a cookie-syncing pixel being passed during the auction process, and not actual content from an ad creative.

Freestar takes steps to ensure that all requests and content from our servers are served on the correct protocol. Unfortunately, there is nothing we can do to force all participants in an auction to do the same.

Why is insecure content a problem?

There is a risk that an attacker could view or modify any content loaded over the insecure HTTP protocol, compromising the security of your website. If your site is secure (HTTPS), most modern web browsers will automatically block insecure scripts, stylesheets, and other code that could pose a serious threat to your users. Insecure images, such as cookie-syncing pixels, are allowed to serve with just a warning because these cannot interact with the rest of your site. The worst an attacker can do is eavesdrop on the information being passed with the pixel.

The bigger risk to publishers is that the insecure content warning creates a bad user experience, and may deter users from spending time on your site.

How can I prevent insecure content from serving with ads?

Freestar recommends that publishers with secure websites implement a Content Security Policy. Specifically, publishers should add the `upgrade-insecure-requests` directive to their website header.

This directive causes the browser to load all requests over HTTPS, regardless of how they are made. If the requested content is available over HTTPS, it loads as usual, and your website remains secure. If the requested content is not available over HTTPS, it will not load. In the case of a cookie-syncing pixel, this simply means that the individual buyer responsible for the insecure request has less information about the website user when determining how much to bid in the real-time auction. However, publishers should be aware that if there is any insecure content on their websites that is unrelated to ad serving, this content may also fail to load.

More information about implementing the Content Security Policy `upgrade-insecure-requests` directive can be found at mozilla.org.

For industry insights and information about our product offerings, check out our blog!

Want to see our products in action? For a demo, fill out a form here.