

Google Chrome To Block Mixed Content Pages Without HTTPS

Description

Google has announced that in a series of steps starting in Chrome 79, all mixed content will gradually be blocked by default.

What Is Mixed Content?

Mixed content refers to the insecure `http://` sub-resources that load into `https://` pages, thereby creating a possible way in for attackers to compromise what appears to be a secure web page. For example, this could be any audio, video, and images that are loaded insecurely from HTTP but appear as part of an HTTPS page when it loads. Many browsers are already able to block other types of mixed content by default such as scripts and iframes.

Why Worry?

Mixed content from a non-secure source poses privacy and security risks and could provide a way for attackers to spread misinformation. For example, an attacker could alter a chart to mislead viewers or could hide a tracking cookie in a mixed resource load. Also, the mix of secure and insecure content in a page could confuse browser security UX. Google's own research shows that Mobile devices account for the majority of unencrypted end-user traffic.

What Does HTTPS Do?

HTTPS provides a secure, encrypted channel for web connections that can protect users against issues such as eavesdroppers, man-in-the-middle attacks and hijackers spoofing a trusted website. The kind of encryption offered by HTTPS stops interception of your information and ensures the integrity of the information that you send and receive.

Older hardware and software can pose a privacy and security risk because it often doesn't support modern encryption technologies.

Progress

Progress has been made to make web browsing more secure with the move towards the full introduction of HTTPS, and Google is keen to point out that Chrome users now spend over 90% of their browsing time on HTTPS on all major platforms.

Google now sees its next task as ensuring that HTTPS configurations across the web are secure and up to date.

Roll-Out In Steps

Google says that the roll-out of its blocking of mixed content will happen in a series of steps starting with the release of Chrome 79 (in December 2019) with its new setting to unblock mixed content on

specific sites. Next, Chrome 80 (due for release in January 2020) will auto-upgrade mixed audio and video resources to https://. Chrome 80 will display a "Not Secure" chip in the Omnibox for mixed images.

What Does This Mean For Your Business?

The introduction of measures to display warnings about and to block mixed content will put pressure on some businesses to clean up their web pages and make it more difficult for cyber-criminals to find a way through browser security. This is good news for businesses and web users alike.

It should be remembered, however, that secure websites with encrypted connections can still be harmed by certain cryptographic weaknesses e.g. due to external or related-domain hosts, so it's important for businesses and individuals to keep up to date with software patches and fixes.

Category

1. News
2. Security

Date Created

14/10/2019