

What are the consequences of overlooking SSL certification?

How to avoid losing Google positions
and customers



CONTENTS:

What happens to websites that lack proper SSL certificates?

How to avoid losing Google positions and customers

Contents	1
Introduction	2
Glossary	3
Google's stand on HTTP vs HTTPS	4
Examples	5
How to avoid losing business over SSL certification	6
Summary	7

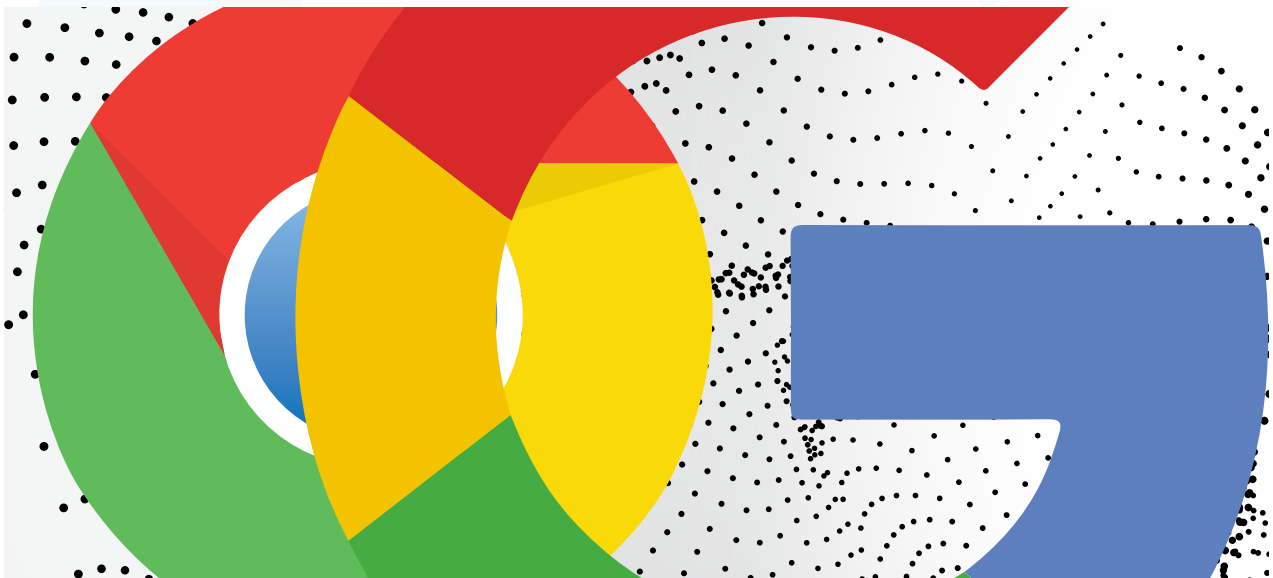
Introduction

In the past, Google has been encouraging website owners to give more attention to cyber security.

For the second half of 2016, websites with SSL certificates have been enjoying much higher positions on Google.

Now, the search engine company is going to enforce a much harsher policy. HTTP websites will stop appearing high in search results and browsers (like the widely popular Google Chrome) will urge users to turn back.

Please note that Google Chrome will be used as a prime example within this PDF, as it is one of Google's flagship products.



Glossary

Browser: A piece of software, used to access (browse) the Internet. Examples: Microsoft Internet Explorer (IE, Edge); Mozilla Firefox, Apple Safari, and Google Chrome.

Certificate Authority (CA): A well-trusted company, specialised in the issuing of SSL certificates.

Decryption: “Un-scrambling” information and putting it back in its original format.

Encryption: Information “scrambling”. This makes it impossible for third parties to use.

HTTP (Hyper Text Transfer Protocol): The standard way to transmit data over the Internet. This data is not protected by encryption

HTTPS (Hyper Text Transfer Protocol Secure): The data transmission protocol, used by SSL protected websites. It provides a high level of data encryption.
SSL Certificate: A type of code used to encrypt and decrypt data online, via the use of keys.

Google's stand on HTTP vs HTTPS

Google has spent a huge amount of time, effort and resources on raising SSL awareness.

In the past, this was done with rather gentle means means.

Any website, using an SSL certificate, would receive a substantial boost to its positions on Google.

However, it was possible to hold a first page position even without using HTTPS.

Now, the company will go on the offensive.

Not only will HTTP websites show much, much lower in search results, they will also be marked as insecure.

The widely popular browser Google Chrome is going to urge users to turn away from any website featuring login fields or requiring credit card information should it fail to provide SSL certification.

How exactly this is going to be implemented is unknown, but it will force a great portion of websites to switch to HTTPS.

Does your website feature user login fields?

Examples:

As of the writing of this PDF, the dreaded change is yet to happen.

The idea here is to help you avoid the potential damage that your website can suffer. Here are a few examples, taken out of previous Google Chrome versions:



Right now, Google Chrome has three indicators about website security:

-  **Secure**
-  **Info**
-  **Not secure**
-  **Dangerous**

As you can clearly see, even now, it equates not secure to borderline dangerous. However, this is merely the first step of Google's crusade against HTTP websites. By the end of the spring of 2017 it is expected that HTTP websites will suffer a great reduction in traffic.

This will happen both due to losing Google positions and because the red insecure messages will turn visitors away.

How to avoid losing business over SSL certification

Most business owners opt for SSL certification, because it helps them appear more credible.

The more credible and authoritative your business is to visitors, the more likely they are to become invested in it.

The main purpose of SSL certificates was to instil trust and lacking them was only an issue for E-commerce websites.

Once the change hits, however, this will not be the case anymore.

Any and all websites, featuring a log-in form will need to have certification, or suffer a huge hit to their credibility in the eyes of visitors.



Summary

The solution is as simple as it is obvious.

The only thing left for business owners, wishing to protect their website from Google's new move, is to implement SSL certification.

As a certified SSL vendor, Go Live UK can provide you with an SSL certificate and answer any questions you might have about the topic.



Thank you!

Thank you for taking the time to download and read this PDF.

Hopefully, the information in it helped you understand **SSL certification** better.

Should you have any further questions, do not hesitate to contact us.
Our experts are always happy to help!

For More Information

Visit our website

<https://www.goliveuk.com/>

Tel: +44 (0)20 3371 7354

E-mail: info@goliveuk.com

This PDF has been created by Go Live UK - <https://www.goliveuk.com>