

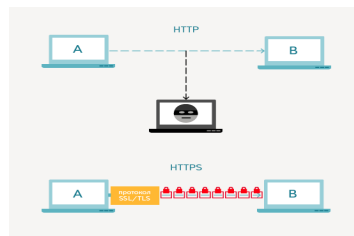
HTTPS ENCRYPTION ON THE WEB

Perminova A.V., Matoshko M.P.
Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Lasarenko A.M. - Senior Lecturer

The issue of HTTPS encryption on the web is considered. In addition benefits and vulnerabilities are discussed. As a conclusion 5 reasons why the https protocol should be connected to your site are presented.

HTTPS helps keep your browsing safe by securely connecting your browser or app with the websites you visit. HTTPS relies on encryption technology—SSL or TLS—to secure these connections. (see Picture 1.)



Picture 1 – connection by HTTP and HTTPS

Let us consider data on the status of HTTPS adoption and usage on Google and across the web:

1.Encrypted traffic across Google

Security is a top priority on Google. Developers are investing and working to make sure that their sites and services provide modern HTTPS by default. Their goal is to achieve 100% encryption across their products and services.

2.Encryption by product on Google

Developers continue to protect services.

3.Encrypted requests to Google worldwide

The volume of encrypted web traffic to Google varies by country/region.

4.Unencrypted user traffic to Google by device type

Mobile devices account for the vast majority of unencrypted end user traffic that originates from a given set of surveyed Google services. Some older devices cannot support modern encryption, standards, or protocols. Unfortunately, these devices may no longer support software updates and, as a result, may never support encryption.

5.Encryption keeps you safe

HTTPS web connections protect against eavesdroppers, man-in-the-middle attacks, and hijackers who attempt to spoof a trusted website.

6.Obstacles to encryption

Several technical and political challenges stand in the way of achieving full encryption of all web traffic. For example, certain countries/regions and organizations block or otherwise degrade HTTPS traffic. Some companies and organizations lack the technical resources to implement HTTPS or don't see it as a priority.

7.HTTPS Encryption by Chrome platform

Desktop users load more than half of the pages they view over HTTPS and spend two-thirds of their time on HTTPS pages.

8.HTTPS on top sites

Google is investing and working to make sure that our sites and services provide modern HTTPS by default. Developers know that the rest of the web is working on moving to HTTPS too, but that move can be challenging for large sites. They're committed to making the web a safer place not only for Google users, but for all users.

In conclusion we reckon HTTPS is a key component to the permission workflows for both these new features and updated APIs.

References:

- [1.https://transparencyreport.google.com/https/overview?hl=ru](https://transparencyreport.google.com/https/overview?hl=ru)
- [2.https://developers.google.com/web/fundamentals/security/encrypt-in-transit/why-https](https://developers.google.com/web/fundamentals/security/encrypt-in-transit/why-https)
- [3.https://habr.com/ru/post/46321/](https://habr.com/ru/post/46321/)