MIGRATING TO HTTPS FROM HTTP

Migrating to HTTPS from HTTP

Back in August 2014, Google announced that it will favour pages on sites in organic search results that are entirely secured by HTTPS, initially Google have said that this will be a relatively weak signal and that they intend to strengthen it as a signal later. This change in policy is what has driven us to recommend that all sites (without exception) that focus on attracting business via organic search migrate to HTTPS as soon as possible.

Migrating from HTTP to HTTPS must be done correctly to ensure that the transition is smooth, and rankings are maintained, and the user experience is not affected negatively.

The aim of this document is to highlight some of the areas to be considered when carrying out the migration.

What is HTTPS?

Hypertext Transfer Protocol Secure (HTTPS) is a scheme for layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol to provide a secure connection, typically over the internet. Historically HTTPS has been used to secure private data transfer such as credit card data in ecommerce site checkouts and booking systems in addition to securing passwords and other sensitive data as it transferred over the web. This primary focus of HTTPS is to prevent data being harvested between the web browser and the host server.

Moving to site-wide HTTPS

Migrating to site-wide HTTPS is not straightforward and you need to plan out the deployment with your host and web developer.

Correct configuration of HTTPS requires several elements

- Purchase of correct type of SSL Certificate with 2048-bit RSA Key and 256-bit signature algorithm for your deployment (single host, multi host or wildcard)
- In most cases, your SSL certificate will also require a dedicated IP address for your host that cannot be shared with other accounts. Other cheaper options (such as SNI shared IP hosting) are available but at this time are not recommended due to issues with compatibility with older versions of Internet Explorer
- Configuration of your web server and website to support use of HTTPS for all pages of the website.
- Update of the website to use HTTPS resources (replace all non-HTTPS resource references with HTTPS references)
- Change internal URIs to use protocol relative URIs (i.e. change http:// & https:// to //)
- Update links to point to HTTPS pages
- Configuration of external resources and tools that are used or referenced by your site.
- Use Canonical URL tag on all pages and use full scheme reference (i.e. https://www.website.com/page)

- Ensure robots.txt is not blocking HTTPS pages – test with Google Search Console (Fetch as Google)
- Consider use of HTTP Strict Transport Security (HSTS) – Please note that there are still some compatibility issues with older versions of Internet Explorer.
- Setup permanent 301 redirects from HTTP pages to HTTPS pages
- Prepare the new (HTTPS) site and test it thoroughly.
- Setup, configure and verify all variants of the domain(s) with Google Search Console (i.e. https://www.website.com, http://www.website.com, https://website.com & http://website.com)
- Setup and verify all variants of the domain(s) with Bing Webmaster tools (i.e. https://www.website.com, http://www.website.com, https://website.com & http://website.com)
- Google Ads
    a. Change all destination and display URLs to HTTPS (remember these may also be in keywords or placements as well as within Ads) – we recommend that this is carried out via search and replace in Google AdWords Editor
    b. Update linked accounts (Analytics and Google Search Console URLs)
- Existing links
    a. Update all social profiles and sites that you control to the new HTTPS address (typically just a link to your home page)
    b. Advise as many providers of inbound links to your website as possible of your change of scheme (typically this will mean they will have to change the link from http://www.website.com to https://www.website.com)
- Google Analytics
    a. Modify settings in your Google Analytics Properties and Views to reflect the new URL scheme (i.e. change http:// to https://)
- Google Tag Manager
    a. Update any references to HTTP in Google Tag Manager to HTTPS, also check any Custom HTML or Custom JavaScript Tags and Macros. Check all Tags, Rules and Macros in addition to container settings.
- Google Merchant Center
    a. Update general configuration to reference the HTTPS site
    b. Update the feeds to be fetched from the new location/URL
- Monitoring following migration
    a. Carry out index status check for stop in HTTP and start in HTTPS indexing within Google Search Console
    b. Test correct deployment with https://www.ssllabs.com/ssltest/
    c. Check Google Analytics for site speed issues
- Other notes
    a. Don't add NOINDEX to the HTTPS URLs on page or via robots.txt
    b. Redirect ALL pages, don't leave any pages on HTTP or not redirected (even custom 404 pages)
    c. Avoid redirect chains (particularly for mobile)
    i.e. http://domain.com > http://www.domain.com > https://www.domain.com

d. Consider use of HTTP Strict Transport Security (HSTS) to eliminate HTTP>HTTPS redirects
e. SSL Certificates expire! Set yourself a calendar a reminder for certificate expiration, well ahead of when it requires renewal
f. Consider images and resources on CDNs or sub domains too
g. If you use sub domains of your site too, these will also require securing via HTTPS, usually a multi domain or wildcard SSL certificate will be required

Website:
www.keyprinciples.co.uk

Phone:
0115 880 0211

Address:
Creative House,
Unit 1, Chase Park,
Daleside Road,
Nottingham,
NG2 4GT