HTTP to HTTPS SEO-Friendly Migration

Google recognized "HTTPS" as an important ranking signal on August 6, 2014. Since then, many webmasters are shifting from HTTP to HTTPS version of their website; and this exodus seems to be heading in the right direction with Ecommerce websites leading from the front. As e-retailers cannot do without a secured encryption, HTTPS versions become the obvious option.

After you have decided to make the switch; do read this checklist that enables you to proceed with the HTTPS upgrade cautiously. In this article, we have compiled a list of pointers that you can keep in mind while upgrading your website to the HTTPS version.

Please note: Not all the points mentioned below are applicable to non-eCommerce websites but all points on HTTP to HTTPS update are relevant for *Magento based eCommerce stores.*

1 **Verify HTTPS version:**
Firstly, you need to verify the website's Https version in Google and Bing Webmaster tools. Verify and confirm whether the version to be updated is www or non-www. The www version is, of course, the preferred one and the update will be made to this.

2 **301 Redirect:**
Implement the SEO friendly "301 Redirect". Always use permanent redirect on the non-preferred version and direct it to the verified HTTPS version. It is recommended that before the 301 redirects are applied, you have a list of all the areas where redirects are to be made and organize all the data which will have 301 redirects implemented. These may include a total number of links, Index stats and sitemap stats, sitelinks and PPC landing pages.

3 **Update Links to HTTPS:**
Once the website is upgraded to the HTTPS version, you need to update all the main internal such as home page, CMS pages, PDFs, URLs in Videos and also links on all external online properties.
Do not forget to update the URLs/ internal links in your newsletters. This will ensure that we are sending unique SEO page signals to search engines.

4 **Update Links on Social Media:**
The external links on social profiles, at least the main and popular ones, should have the HTTPS version of URLs.

5 **New Sitemap:**
Configure a new sitemap with the HTTPS URLs of the website and submit it in both Google and Bing webmasters.

6 **Robots txt:**
Update the existing Robots.txt file of the website and update the new sitemap, configured for the HTTPS version of the website.

7 **Check Robots txt:**
Once the Robots.txt file is updated, you should double check it to ensure that it should not block any pages like CMS, Product page or any other. This needs to be done, especially, if you have introduced new pages or sections while upgrading from HTTP to the HTTPS version.

8 **Configure Canonical Tags:**
Configure canonical tags and make them point to the HTTPS version. The canonical tag should be implemented
on the same pages but this time they should point to the HTTPS versions. Please note that Magento may do this on its own but webmasters will still need to ensure that the implementation was correctly executed.

9 **PPC/ CSE:**
Update PPC / CSE landing pages with the HTTPS version URLs so that they should not affect the landing page score.

10 **Back-up:**
Take a backup of Google Webmaster HTTPS versions (snapshot and details).

11 **Re-Submit the Links:**
Re-submit the Links Disavow file in both the Webmaster tools. This ensures that spammy links will not affect the new verified version of the website. You need to update the Robots. txt file on both Google and Bing webmaster tools.

12 **Manage URL Parameters:**
Make sure that you manage URL parameters for the HTTPS version in both Google and Bing webmaster tools. For this, you can simply copy the URL parameters settings from the HTTP version and reflect them in the HTTPS version.

13 **Update Google Analytics:**
Update Google Analytics Admin settings. Please select "HTTPS " version and save the settings.
This ensures that all the reported data procured in Google Analytics will now be for the HTTPS (new version).

14 **Update URL in Email Signatures:**
Update your email signatures with the new
URL i.e. https://www.example.com

15 **Check CDN:**
Ensure that the existing CDN on the website does not cause any issue once the website is shifted from HTTP to HTTPS version. Coordinate with the CDN team and make the necessary changes.
Make sure that your CDN can handle SSL. Also, ask your CDN company to share their concerns regarding the upgrade beforehand, so that the switch does not become counterproductive.

16 **Re-design the Newsletter:**
Re-design the newsletter templates - Auto-responder emails, Triggers, on site pop-ups and update all the links with HTTPS URLs. Also, update the internal links of Newsletter Welcome series emails that, maybe be configured on Magento or any Newsletter Marketing software.
cause any issue once the website is shifted from HTTP to HTTPS version. Coordinate with the CDN team and make the necessary changes.
Make sure that your CDN can handle SSL. Also, ask your CDN company to share their concerns regarding the upgrade beforehand, so that the switch does not becomecounterproductive.

17 **Plan Your Newsletters:**
Do not send any newsletter or offers for at least 4-5 days before the planned upgrade is due.

18 **Code Check Up:**
Check images, CSS, javascript URLs and ensure that they work in the upgraded version.
The code audit must be vigilantly executed.

19 **Timing:**
Consider upgrading the website at a time when the traffic on the website is at its lowest, for that session. This is really crucial for eCommerce stores.

20 **Optimize Google Webmaster:**
Optimize Google Webmaster crawl time using "Crawl settings. Please minimize the requests sent per second before the upgrade is due. This setting will take 48 hours to be effective, so make this change at least 2-3 days before the planned upgrade.

21 **Update Redirects:**
Update all the implemented 301 redirects to the HTTPS version. This can be done at the server level by your Server team. Basically, all the 301 redirects implemented on 404 pages should be updated to the HTTPS version.

22 **3rd Party Tracking Codes:**
Keep a backup of the 3rd party tracking codes (Adwords, Bing, Conversion codes, Remarketing codes and Analytics codes) and update them to the HTTPS version.

23 **Check Extensions:**
Check hosted Blog extension settings, plugins, etc.
For example, WordPress Blog should work on HTTPS and so should the installed plugins like Yoast extension, social sharing and security plugins.

24 **Evaluate the Mobile Version:**
Evaluate the mobile version of the website and ensure that the HTTPS URLs are responsive or non-responsive. If not, configure the settings accordingly for a mobile-friendly HTTPS version of the website.

25 **Re-submit the Removal Request:**
Re-submit the removal request of URLs in Google and Bing webmaster tools.
For example, The old HTML sitemap or any other page on the website that was submitted for removal needs to be re-submitted for the HTTPS version also.

26 **Update the Dev Version:**
Re-submit the removal request of URLs in Google and Bing webmaster tools.
For example, The old HTML sitemap or any other page on the website that was submitted for removal needs to be re-submitted for the HTTPS version also.

27 **Check 3rd Party Extensions:**
Check to ensure that the 3rd party extension like Website search is working fine in the upgraded version.

28 **Https Version Validation:**
Get the new HTTPS version validated by an online tool such as W3c. This will help you make your website cleaner after the switch. As Google grants more leverage to cleanly coded and glitch-free websites, getting your version checked and reported for errors or warnings is highly recommended.

29 **Compare Page Speed:**
Compare the website page speed for both the HTTP and HTTPS versions using the Google tool and implement the necessary changes.

30 **Check Social Sharing Extension:**
Compare the website page speed for both the HTTP
All the social sharing extensions (buttons on products page or Blog) should work on the updated version. implement the necessary changes.

31 **Configure Data Highlighter:**
Configure Data Highlighter in Google Webmaster tools and set it for HTTPS version.
This enables the HTTPS URL to get picked up in the rich snippet results.

32 **Absolute and Relative URLs:**
If a website is using both Absolute and Relative URLs on the website, then the Relative URLs will update to HTTPS automatically. Absolute URLs have to be updated manually
Please ensure that both URL types are duly updated.

33 **Update URLs on External Links:**
Update "301 redirects" on the external domains owned by you. For example, there can be a number of websites or blogs that might be 301 redirecting to the HTTP version. This needs to be updated so that the external links can redirect to the HTTPS version after the upgrade is pushed live.

34 **Update Blog Links:**
The internal links on the website's images linked from the blog posts also need to be updated to the HTTPS URLs.
Do update these in WordPress.
This can be done under the "General Settings" section where you can mention the 'WordPress Address (URL)' as HTTPS.

35 **RSS Feed:**
Check if RSS subscription feed of the Blog or the website is working for the upgraded version.

36 **Get URLs Updated on 3rd Party:**
Contact the website owners/affiliates and ask them to update the website URL and use the new HTTPS

37 **Use Updated URLs for Link Building:**
If you employ a link building strategy that involves leaving links in different forums and threads, then, continue with your link building efforts but now use the updated URLs of the website.

38 **Check Content:**
Ensure that the content on HTTP and HTTPS website is similar.

39 **Upgrade Your SSL Certificate:**
Upgrade your website SSL certificate to SHA2 to support website pages like Checkout, Category pages, and Product pages.
Otherwise, it can trigger Server errors in the Webmaster tools. Moreover, Google prefers the SHA2 certification and considers it as a ranking parameter.

40 **Upgrade 3rd Party SEO Tools:**
If you are using any 3rd party SEO tool like Moz.com, please submit the HTTPS version to them to make sure it shows the SEO score of HTTPS version.

The HTTPS upgrade, if not done properly, can result in reduced visibility in the search results; a fallout of lowered rankings. Also, there may be other severe long-term effects of not making the switch. These can include insecure connections, compromised referral data and now, a bad rap with Google.

These 40 points must be implemented so that the transition from HTTP to HTTPS is event-less. We'd also like to hear about the cautions that you take or have heard of and can add to this list shared here.

Wishing you a happy and a smooth switch!