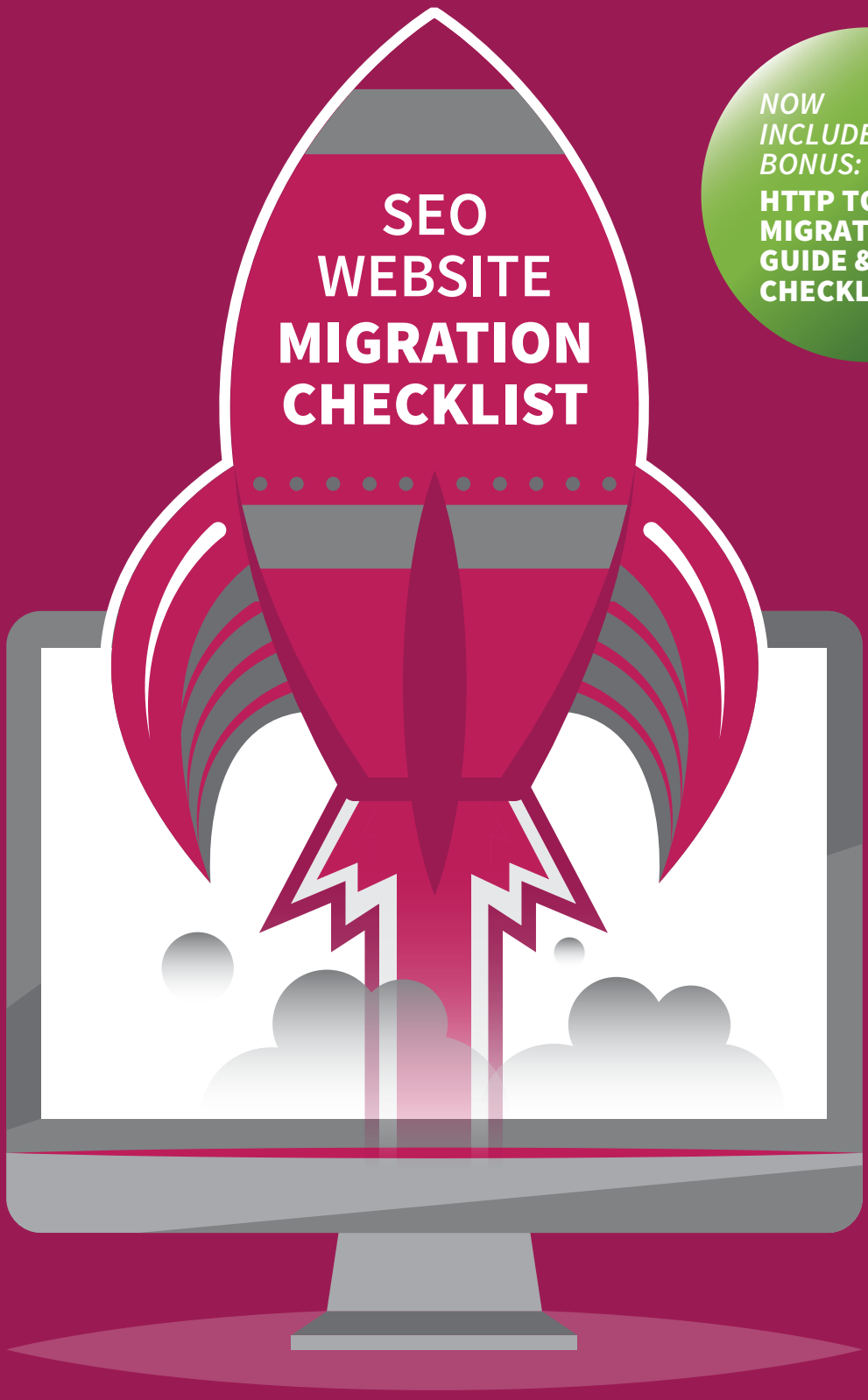
SEO WEBSITE MIGRATION CHECKLIST

NOW INCLUDES BONUS:
HTTP TO HTTPS MIGRATION GUIDE & CHECKLIST



A COMPREHENSIVE GUIDE FOR A SUCCESSFUL WEBSITE RE-LAUNCH

SiteVisibility
Delivering Digital Growth

A SITE MIGRATION IS A SIGNIFICANT PROJECT FROM A SEARCH MARKETING PERSPECTIVE AND AS SUCH SHOULD BE CAREFULLY CONSIDERED AND PLANNED.

WE'VE PULLED TOGETHER A COMPREHENSIVE TO-DO LIST OF EVERYTHING YOU NEED TO CONSIDER, COMPLETE WITH AN EXPLANATION OF WHY THAT STEP IS AN IMPORTANT PART OF YOUR MIGRATION.

PLANNING

1: Establish Potential Impact of Migration

In the long term, site redesigns and migrations are designed to improve sites. Despite this improvement site migration can have an impact.

Rankings will fluctuate, traffic may fall and onsite conversions can be effected.

An estimate of this impact, including the longer term upside should be created and shared with all key stakeholders. Particularly if the website is the main source of leads or sales for your business.

2: Time Migration for Minimal Impact

As discussed site migrations can have a tangible impact of the search channels performance towards a site's objectives. As such it makes sense to time any site migration around seasonal periods of low demand.

This decision should be based on both the traffic to the website, i.e. when is it lowest but also the market as a whole using tools like Google Trends, to understand when demand in the market is lowest as well.

Additionally if you are an international business you may be able to "test" your redesign in smaller markets. i.e. roll-out first in low traffic territory and refine for roll-out in higher traffic geographies.

3: Explore alternative traffic sources to mitigate short term traffic loss

As natural search traffic is likely to decrease in the immediate roll-out of site migration it can be prudent to explore whether investment in other traffic sources can help reduce or eliminate the shortfall. I.e. could budget be allocated to paid search or investment in other organic channels, like social media efforts being increased to deliver more traffic.

If you're planning budgets, it may make sense to allocate spend to mitigate the short term anticipated impact of a redesign and migration.

4: Communicate Scope of Work Required

Website redesigns are complex projects often with tight deadlines, as such it's important to understand the scope of work required for a site migration from an SEO perspective and ensure that the resource required to deliver this is available at the appropriate points in the timeline.

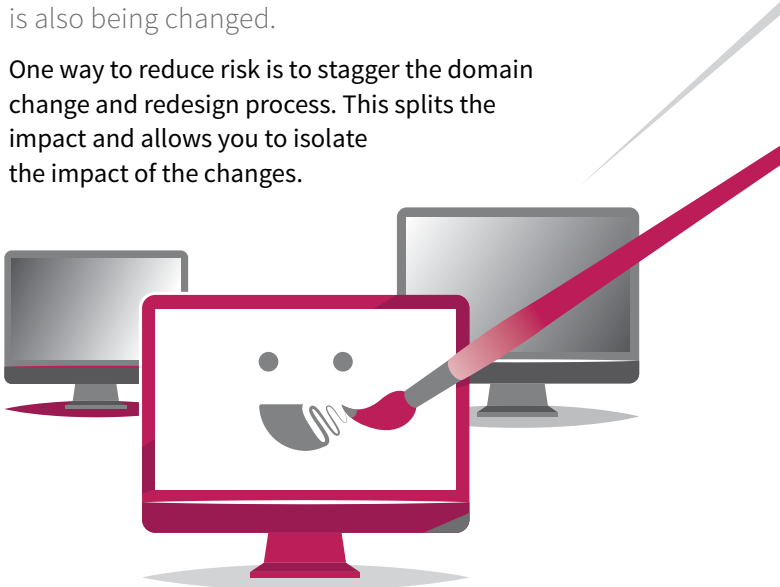
This work will include both time for a search specialist to make the recommendations and the implementation of these changes by web development specialists.

It's worthwhile to share with developers a functional spec of all the work you would equire carried out on a new site. This wil have an impact on the scope of the web development project, when a web design agency are pitching for the work they should understand the nature of these requests and reflect them in the scope of the work.

5: Where domains are being changed consider staggering site redesign.

Site redesigns and migrations where the website and URLs are changed but the domain is remaining the same are lower in risk than where the domain is also being changed.

One way to reduce risk is to stagger the domain change and redesign process. This splits the impact and allows you to isolate the impact of the changes.



PRE-LAUNCH

6: Ensure test environments of the new site cannot be indexed by Search Engines

While working with a staging server or test environment on your new website ensure it can't be indexed by search engines by using both your Robots.txt file and the NoIndex tag in the <head> of all pages of your websites.

Additionally you should password protect your testing area to prevent browsers accessing the site.

7: Take Full Crawl of Old Site

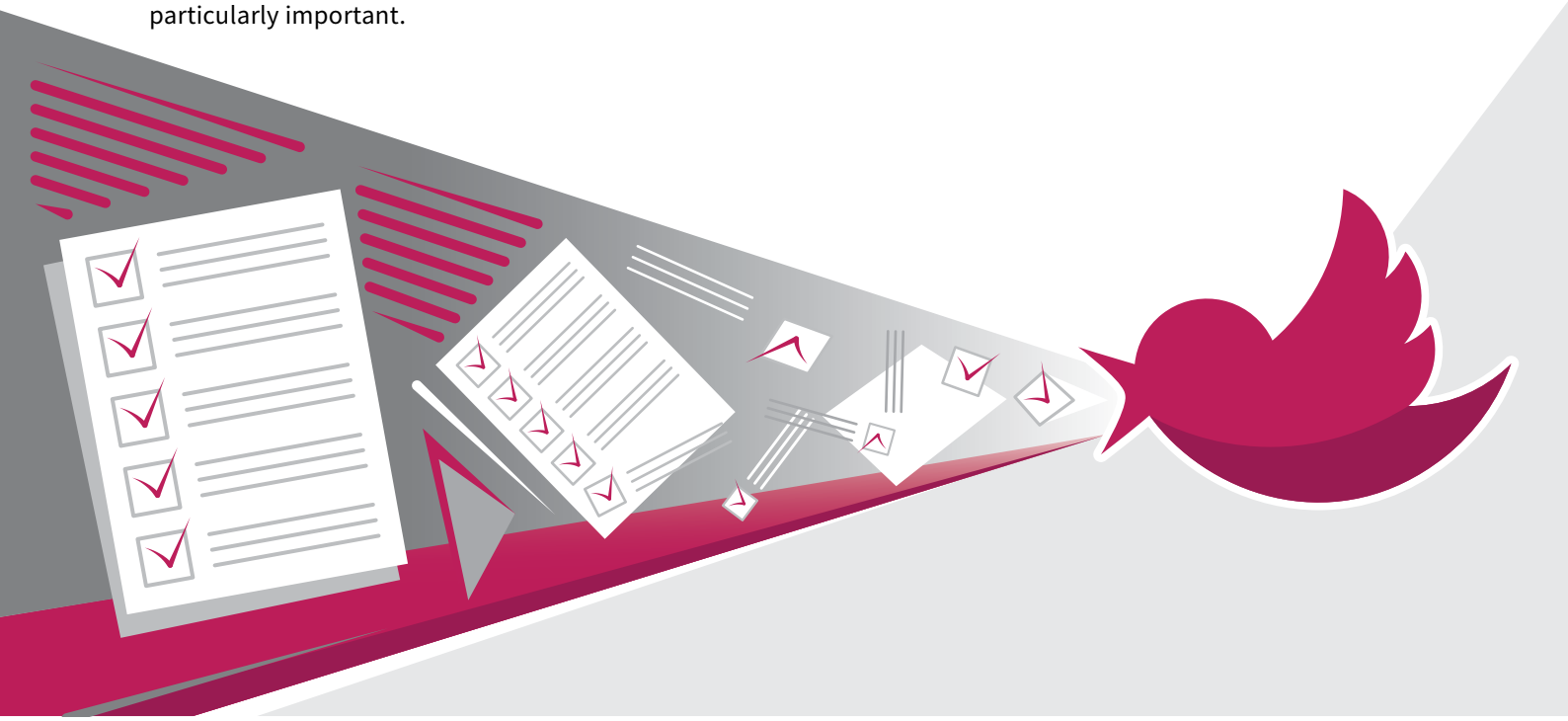
Taking a full crawl of all the pages on the old site and key information about these pages is an important step in the migration process. This will give you the urls which you will need to potentially map to the new website and important information about those pages currently.

If you are expecting an extensive reworking of the site's design and information architecture this is particularly important.

8: Export List of All Pages of Old Site with Links

Using a tool like OpenSiteExplorer or Majestic (or both) compile a list of all the pages with external links pointing at them. These pages will be top priorities to redirect, they will be responsible for your natural search performance.

This, along with the other exports, should be run near the date of the expected migration to fully capture the most recent links and pages added to your website.



9: Export List of All Pages With More Than One Visitor in the Last 12 Months.

From your Analytics platform take a report of all your pages which have received one visitor in the past 12 months.

These will be high priority pages for redirection and you should prioritise their matching.

10: Export List of all Pages Shared on Social Media

Using a tool such as BuzzSumo or Social Crawlytics discover your most socially shared content.

Export a list of these pages, these are likely to be a high priority for redirection as this is content which has clearly connected with your audience now or in the past.

PRE-LAUNCH *CONT.*

11: Export List of All Pages Currently Indexed by Search Engines

Use a tool like Scrapebox to get a list of all of the pages of your site currently indexed by the search engines. If time allows, you would want to ensure each of these links is redirected to the most appropriate page on the new site.

Where this is not possible consider categorising pages into buckets and redirecting them as a group to important category pages or the homepage of your site. In many cases this will require some degree of automation to deal with the scale of the pages within the site.

12: Combine the list of URLs to Redirect and Prioritise

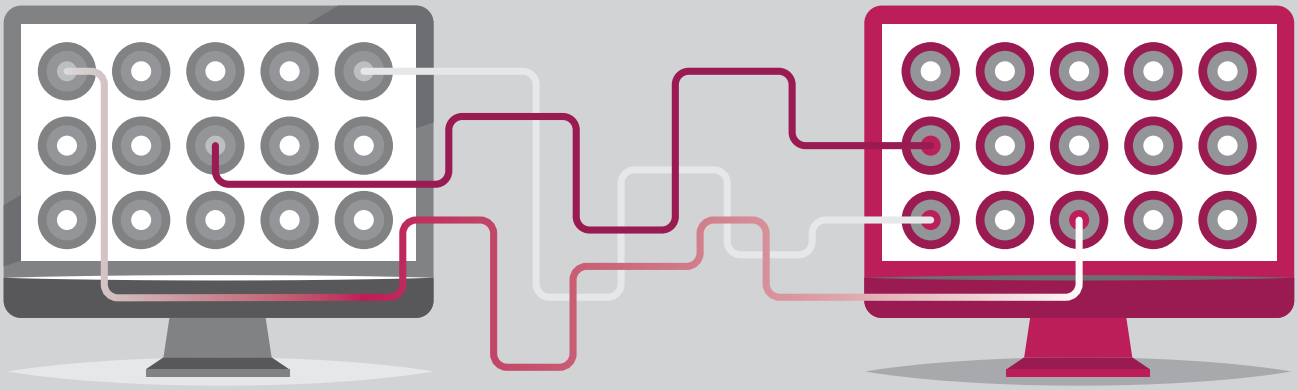
Using Excel combine these different lists, de-duplicate URLs in more than one list and prioritise the URLs and how important their redirection is.

Ideally you want all of these pages redirected, the allocation of resource will dictate how much time you will spend finding the most appropriate page to redirect to.

13: Create URL Redirect Map

With your list of prioritised list of URLs on the old site create a redirect map of where each of these old URLs will be redirected to on the new website. Use 301 rather 302 redirects.

As previously discussed this will often require some degree of automation to deal with the sheer number of the pages within the site and Google Index.



14: Audit Redirect Map for Wildcard and Regular Expression Simplification Opportunities

With your complete map of planned redirects audit the list to see if the total number of redirects can be reduced using either Wildcard or Regular Expression redirects.

Be careful when mapping the redirects as you don't want to redirect to 404 pages.

15: Generate .htaccess File Encapsulating all required Redirects

Assuming the site is using a PHP server create the list of required redirects using the correct syntax used in the .htaccess file that can be cut and pasted into the file by your web developer.

It can be worthwhile running your htaccess file through a validator like http://htaccess.madewithlove.be/

PRE-LAUNCH *CONT.*

16: Make and Keep Backup of Old Website

Where possible it's advisable to keep a version of the old site in a password protected environment blocked to the search engines using the robots.txt file and noindex head tag on this test site.

This backup will allow you to refer back to specific changes. Where certain pages or keywords may have difficult transitions you can look back to what came before the current site.

17: Benchmark the Old Site's Performance

Using tools like Pingdom and Google's Page Speed Insights take a benchmark report on your old website's performance to make a comparison with your new website.

We recommend re-running these tests in close proximity to the relaunch to make the fairest possible comparison.

18: Benchmark Old Site's Number of Indexed pages Across Major Search Engines

Using site:domain.com take a benchmark of the number of pages from your website currently indexed by the major search engines.

This will help you understand changes in website indexation after site migration.

19: Benchmark the Number of Search Engine Entry Pages within your Analytics Platform

Establish a benchmark report in the last year of how many different pages of your site acted as an entry point to your website.

Unless you are are dramatically increasing or decreasing the number of pages on your site the aim is for this number to remain fairly static post launch.

PRE-LAUNCH *CONT.*

20: Carry out Extensive On-Site Audit of the New Site

While on the test server carry out a complete SEO audit of the new website. This will explore and make recommendations to improve the SEO of the website and will cover issues like site information architecture, title tags and content optimisation and schema.org mark-up.

When you've put together an extensive functional spec for the future website, the more closely this is adhered to in the design process the less potential work that will come as a consequence of the audit, however it should be expected that the audit will introduce a number of additional elements to a pre-launch snagging list.

A suitable amount of resource and breathing space in the launch timeline should be allocated.

21: Prepare a Robots.txt File for the New Site

Create a Robots.txt file for your new website. This file will manage which areas of your site are accessible to search engine spiders and how they behave around your site.

Ensure this doesn't block search engines, as this is how it will have been set up in your test environment.

22: Prepare an XML Sitemap for the New Site

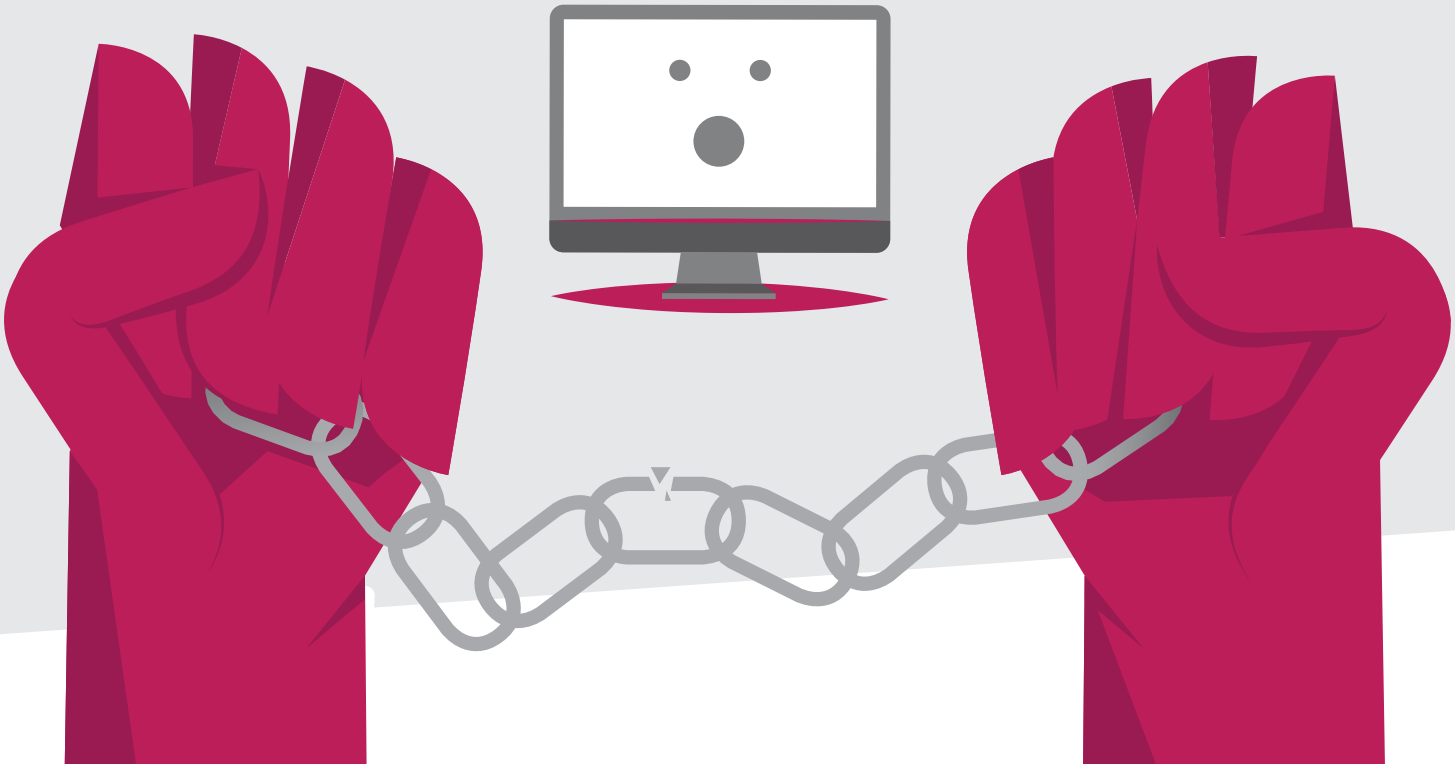
Based upon the pages contained within your content management system ensure all the pages of your site are contained with a valid XML sitemap.

Where you have more than 50,000 URLs in your site, split the sitemaps accordingly and create an index sitemap. I.e. a Sitemap of your XML Sitemaps.

23: Test for Broken Links

On the test server check for broken links to pages that no longer exist. These links may be to internal pages or external websites.

Where possible where internal links are in the body copy, ensure these links are pointing to the new location of pages rather than old location.



LAUNCH

24: Ensure Crawler access

Once the site is live on the web ensure the website is accessible to search engine crawlers using tools like Fetch as Googlebot.

Ensure homepage and important internal pages are accessible and rendering to the Search Engines as you were expecting.

25: Ensure Webmaster Verification Codes are Live

Ensure the Google Webmaster Tools & Bing Webmaster Tools verification codes are in place on the live site to ensure continued access to the Search Engine's reporting, and communication systems.

You will be checking Webmaster Tools site frequently post-launch so it's essential the code is in place post launch.

26: Check Robots.txt file is as expected

Ensure that the robots.txt file live on the site is as expected and as you specified pre-launch.

This is probably one of the most important things to check post launch.

27: Ensure that NoIndex in the <head> has been removed for all pages

In your test environment you will likely have implemented the NoIndex tag within the <head> tag ensure this has been removed from all the pages you want in Google's Index.

If this hasn't been removed you can find yourself receiving no search engine traffic.

28: Check that your redirects are 301s and are working as expected

Test to see your specified redirects are working as expected. Use a HTTP Status Header checker to ensure that the redirects used are 301 and not 302 redirects.

These would appear the same to the user but not to the search engines.

29: Check XML Sitemap is expected

Ensure that the XML sitemap live on the site is as expected and as you specified pre-launch, ideally at domain.com/sitemap.xml.

Additionally check all the links in the sitemap work, investigate any links in the sitemap which aren't returning the page expected.

LAUNCH *CONT.*

30: Upload XML Sitemap to Search Engines

Upload your new and current XML sitemap to the search engines within their webmaster areas.

This will help the indexation of the new site post-launch.

31: Ensure all Title Tags and Meta Descriptions have been implemented

New title tags and meta descriptions will likely be one of the major outcomes of the audit carried out on the site pre-launch.

Ensure the Title Tags and Meta descriptions reflect those you specified.

32: Test for Broken Links

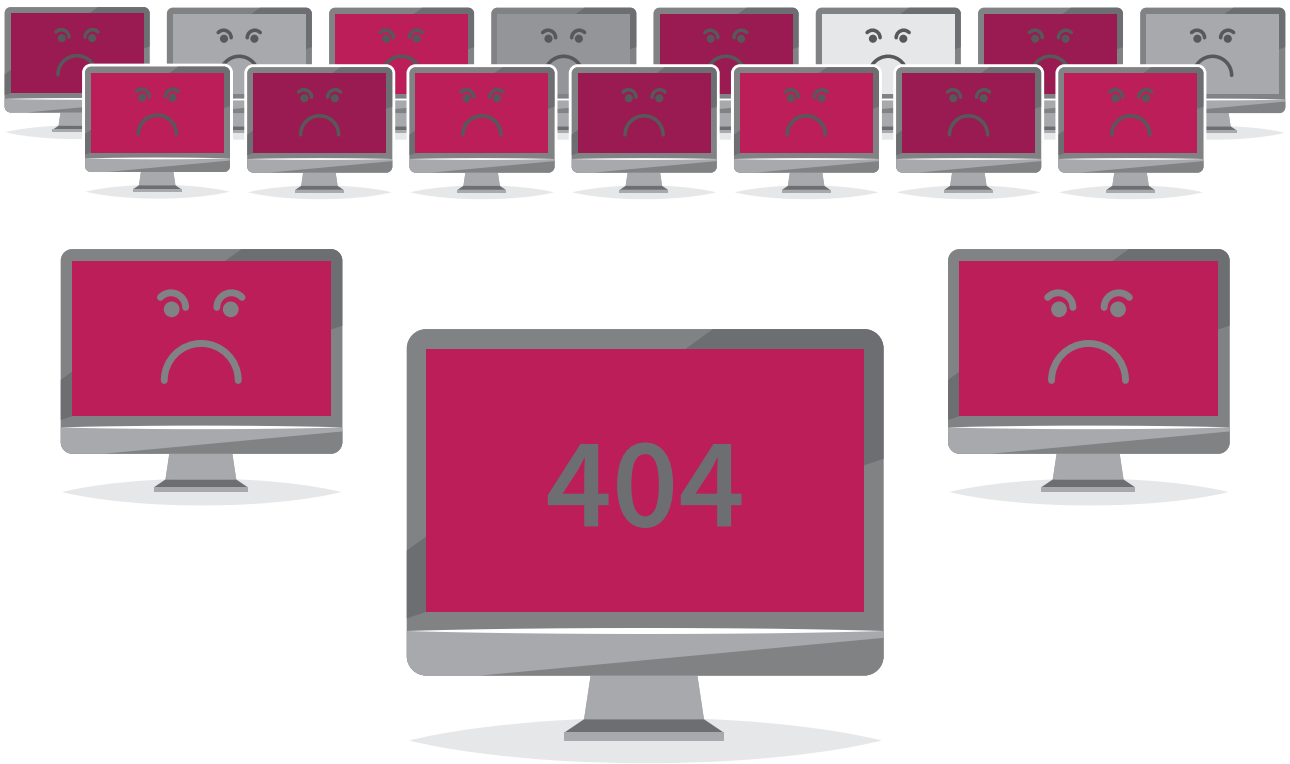
Repeat your test for broken internal links on the live site to ensure that no link is pointing at a page that no longer exists.

Where there are broken links either correct the location the link is pointing or remove the link.

33: Ensure that the live site doesn't show Soft 404s

On the live site test a dummy URL which should lead to a 404, ensure this is a proper 404 error rather than a "Soft 404" which appears to be a 404 but actually returns a 200 status code.

This leads to duplication of content on your website and consequently poor search engine performance.



LAUNCH *CONT.*

34: Check Analytics Codes are in Place and Working

Ensure that your analytics codes are triggering as expected on normal and conversion pages, either on the page direct or within your tag management solution.

GACHECKER is a great tool which can assist in this process http://www.gachecker.com/

35: Monitor Real Time Analytics for Immediate Usability issues

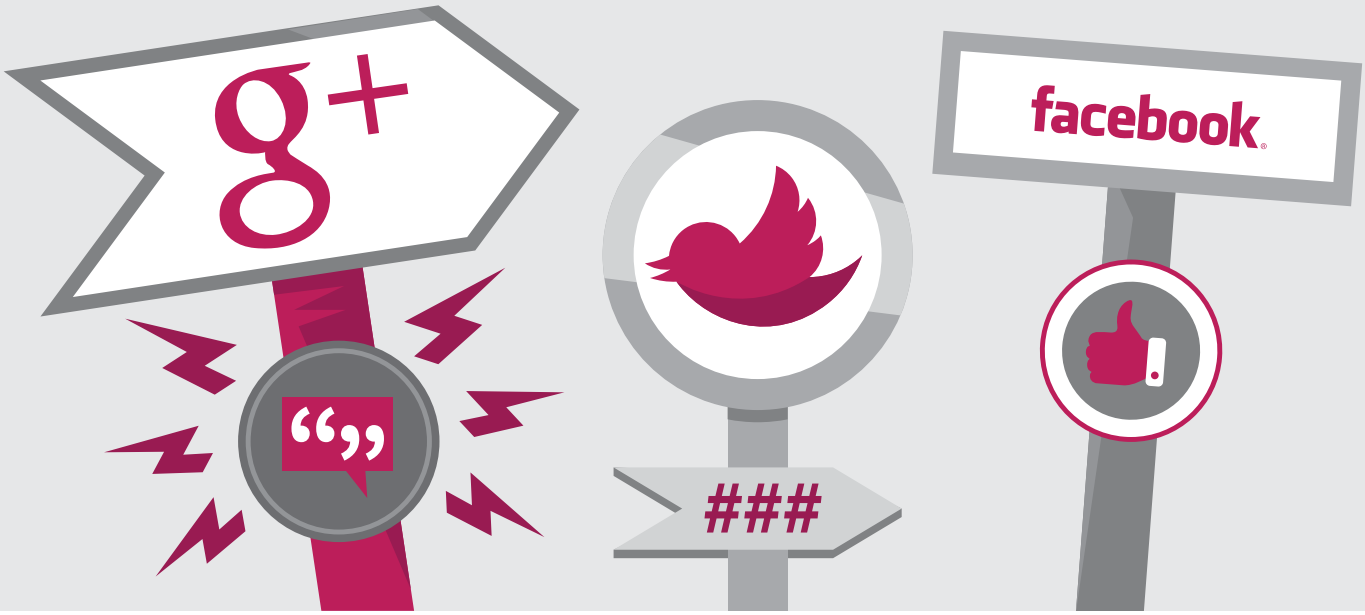
If using Google Analytics allocate some time and resource to monitoring Real Time Analytics on launch day to look for serious usability issues impairing your users ability to carry out key journeys and activities on the site.

Google provide extensive documentation of this aspect of Google Analytics on their website https://support.google.com/analytics/answer/1638635?hl=en-GB

36: Speed up re-indexation with social signals

Social sharing has been known to increase the speed of indexation of new pages and re-crawling of existing pages.

Make use of your social platforms to announce the redesign and hopefully speed up the crawling process. Pay particular attention to Google owned properties like Google+.



37: Check all internal links are followed

Take a sample of pages of different types within the site and ensure that the internal links are not no-followed.

If they are it will be hard for Google to index all your pages or reflect the importance of your most linked to internal pages.

POST LAUNCH

38: Check Google and Bing Webmaster Tools for new Error messages

Log-in to both Google and Bing Webmaster Tools daily to check for new error messages.

Where issues do arise and are signalled by the Search Engines respond urgently to the issues.

39: Contact Key Linking Websites

Where possible contact the most important websites, linking to your website where the URL has changed.

You will have a redirect in place but inform them the URL has changed and ask them to change to the new URL where possible.

40: Change all URLs on Owned Properties

Carry assessment of URLs used on owned media properties like social media accounts, ensure all urls are pointing to the new URLs even where redirects are in place.

This could probably be carried out by using a backlink analysis tool like Majestic or Moz OSE.

41: Check Cache for important internal pages

Regularly check the search engine caches of your homepage and most important pages to understand when they are re-indexed.

Where particular pages are taking longer to get re-indexed than expected consider additional social sharing and opportunities for links from frequently recached sites (e.g. news, social and blogs)

42: Compare Site Performance Benchmark

Using the same tools as the benchmark, i.e. Pingdom and Google's Page Speed Insights compare the new site's performance compared to the old site.

Where required recommend remedial work needed.

43: Compare Site Indexation to Benchmark

Compare site indexation to benchmark report.

Look out for large changes down to suggested areas of the new site not getting indexed or large increases suggesting potential duplication issues.

44: Compare Number of Search Engine Entry Pages with Benchmark

Compare the number of search engine entry pages reported in Web analytics on the new site compared to the old site.

Unless you've dramatically increased or decrease the number of pages on your site, your aim is to be near the benchmark.

SEO WEBSITE MIGRATION CHECKLIST

A site migration is a significant project from a search marketing perspective and as such should be carefully considered and planned.

Below we have a checklist of the necessary steps required for a migration plus further specific explanations of what that work might entail.

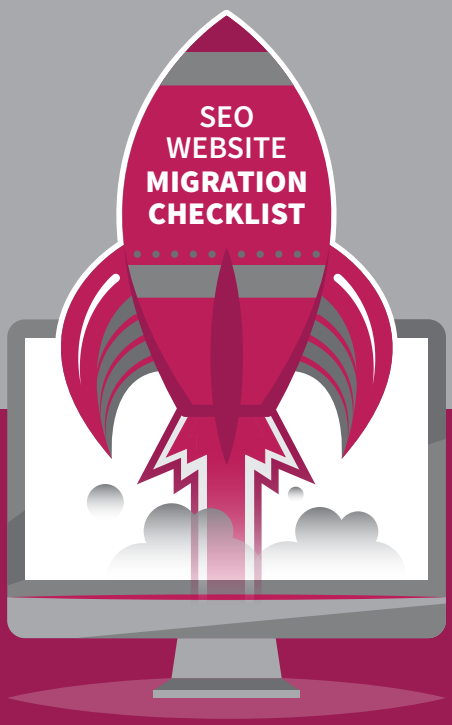
Task	Responsible	Due	Complete
1: Establish Potential Impact of Migration			
2: Time Migration for Minimal Impact			
3: Explore alternative traffic sources to mitigate short term traffic loss			
4: Communicate Scope of Work Required			
5: Where domains are being changed consider staggering site re-design			
6: Ensure test environments of the new site cannot be indexed by Search Engines			
7: Take Full Crawl of Old Site			
8: Export List of All Pages of Old Site with Links			
9: Export list of All Pages With More Than One Visitor in the Last 12 Months			
10: Export List of all pages shared on Social Media			
11: Export List of All Pages Currently Indexed by Search Engines			
12: Combine the list of URLs to Redirect and Prioritise			
13: Create URL Redirect Map			
14: Audit Redirect Map for Wildcard and Regular Expression Simplification Opportunities			
15: Generate.htaccess File Encapsulating all required Redirects			
16:Make and Keep Backup of Old Website			
17: Benchmark Old Site's Performance			
18: Benchmark Old Site's Number of Indexed pages Across Major Search Engines			
19: Benchmark the Number of Search Engine Entry pages Within your Analytics Platform			
20: Carry out Extensive On-Site Audit of the New Site			
21: Prepare a Robots.txt File for the New Site			
22: Prepare an XML Sitemap for the New Site			
23: Test For Broken Links			
24: Ensure Crawler access			

GET IN TOUCH **01273 733 433** grow@**sitevisibility**.com www.**sitevisibility**.com

SEO WEBSITE MIGRATION CHECKLIST *CONT*.

Task	Responsible	Due	Complete
25: Ensure Webmaster Verification Codes are Live			
26: Check Robots.txt file is as expected			
27: Ensure that NoIndex in the <head> has been removed for all pages			
28: Check that your redirects 301s are working as expected			
29: Check XML Sitemap is expected			
30: Upload XML Sitemap to Search Engines			
31: Ensure all Title Tags and Meta Descriptions have been implemented			
32: Test for Broken Links			
33: Ensure that the live site doesn't show Soft 404s			
34: Check Analytics Codes are in Place and Working			
35: Monitor Real Time Analytics doe Immediate Usability Issues			
36: Speed up re-Indexation with social signals			
37: Check all Internal links are followed			
38: Check Google and Bing Webmaster Tools for new Error messages			
39: Contact Key Linking Websites			
40: Change all URLs on Owned Properties			
41: Check Cache for important Internal Pages			
42: Compare SIte Performance Benchmark			
43: Compare Site Indexation to Benchmark			
44: Compare Number of Search Engine Entry Pages with Benchmark			

NEED SOME MORE SUPPORT ON YOUR SITE MIGRATION?



GET IN TOUCH

grow@**sitevisibility**.com

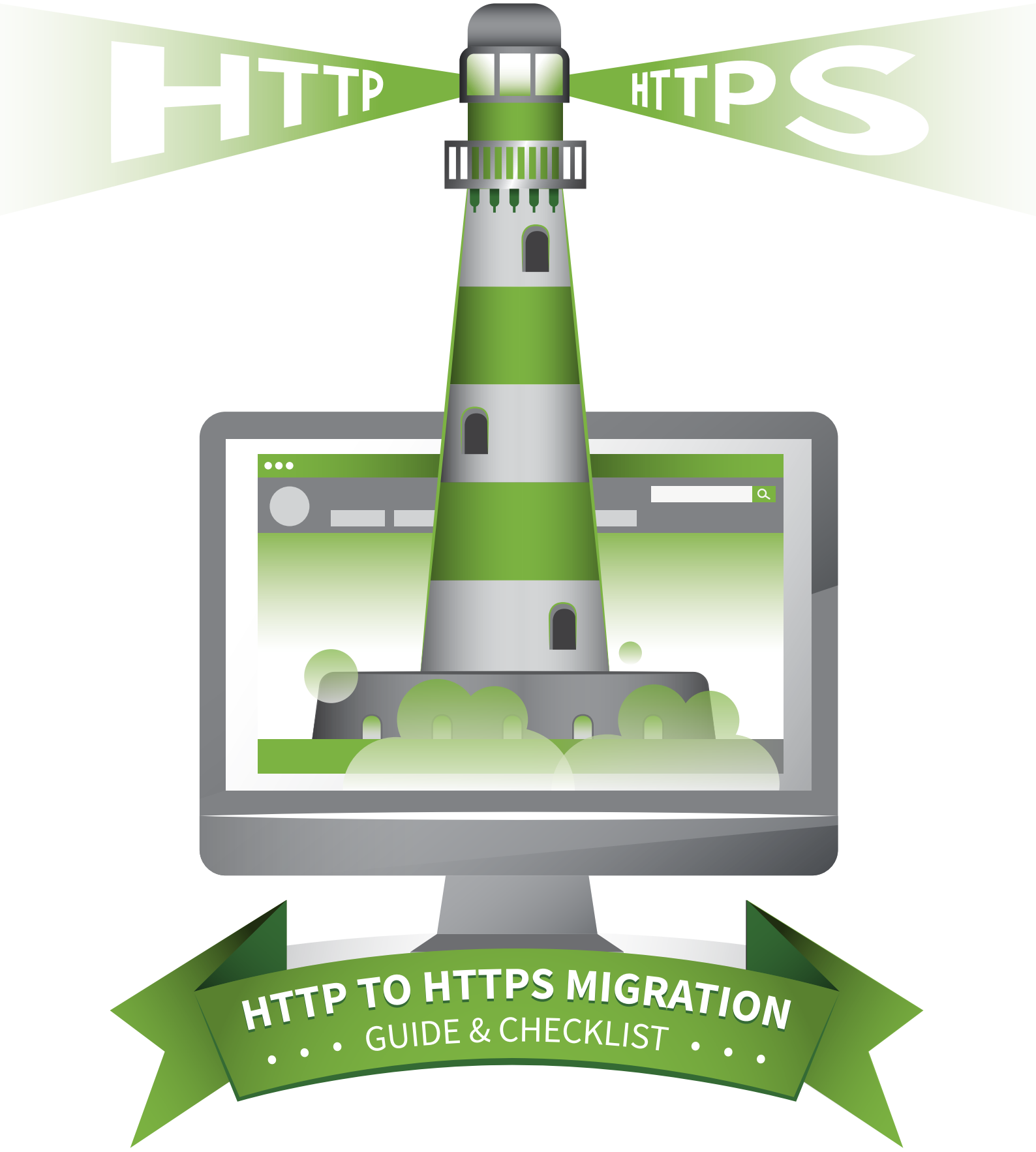
01273 733 433

www.**sitevisibility**.com

NEED EVEN MORE SUPPORT ON YOUR MIGRATION?

WANT TO MAKE YOUR SITE MORE SECURE AND RECEIVE A RANKINGS BOOST IN THE PROCESS?

HERE'S OUR BONUS HTTP TO HTTPS MIGRATION GUIDE & CHECKLIST



HTTP TO HTTPS MIGRATION

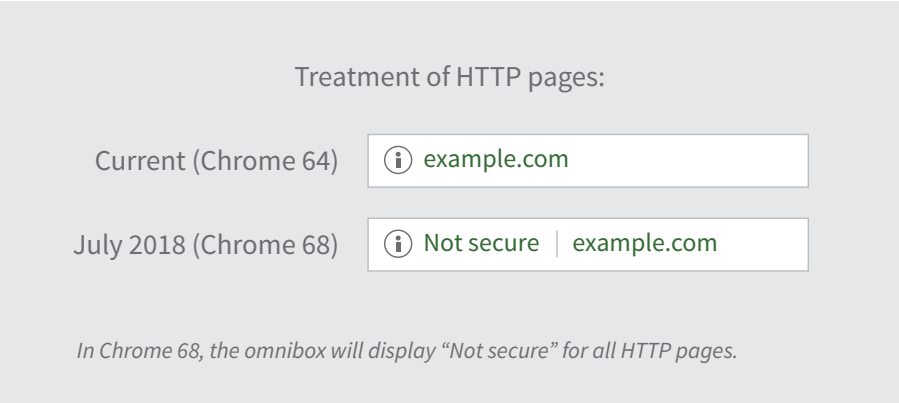
GUIDE & CHECKLIST

INTRODUCTION

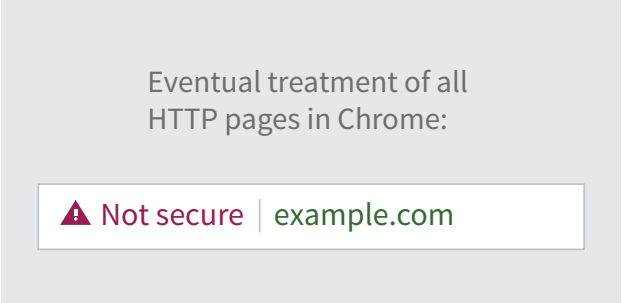
In August 2014, Google announced that they would provide a ranking boost to websites using HTTPS (Hyper Text Transfer Protocol Secure).

In the years since, Google has further signalled their commitment to an HTTPS Everywhere web by gradually providing more prominent browser messages to users accessing HTTP web pages, noting that the pages are not secure.

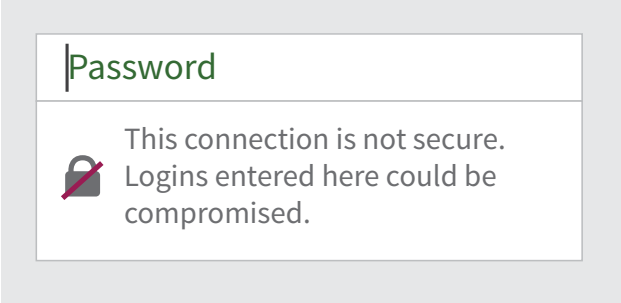
In July 2018, during the release of the Chrome 68 browser, Google started to highlight all HTTP pages as "not secure" in the browser omnibox.



Google has said that eventually, all HTTP pages will be served to users with the following browser message. Note: The scary red text and warning triangle!



In March 2017, Firefox took this one step further by reminding users of when they were using insecure pages with a prompt on username and password fields.



We recommend migrating your site to HTTPS as soon as you can, whether you are undertaking a site migration or not, and below we're providing an extension to our ULTIMATE SEO Website Migration Checklist with the steps to undertake when doing so.

Before we get started with our HTTPS migration checklist however, here's all the background information that you need to know, including the pros and cons of migrating from HTTP to HTTPS.

THE KEY DIFFERENCE BETWEEN HTTP AND HTTPS

Both HTTP and HTTPS are client to server protocols that rely on a request from a browser or operating system and a response from a server.

The biggest difference is that during the request and response process, HTTP web pages will send information to a server as-is. Put simply, if a hacker was able to intercept an exchange between a HTTP web page and a server, they would be able to see the exact information that the user provided.

With HTTPS transfers, the information in this exchange is encrypted. The encryption replaces the plain text with a series of letters and numbers, known as ciphertext.

HOW HTTPS WORKS

An SSL (Secure Socket Layer) is key in making HTTPS work by encrypting the data in the server to browser exchange. This ensures that the data in the exchange is kept private and anonymised.

When a user accesses a secure HTTPS page, a session key is used to encrypt data between the browser and the server.

A browser will request the identity of the server, and the server identifies itself by sending an SSL Certificate in return.

The SSL certificate contains a public key and in HTTPS, this public key is required to unencrypt the data transferred to the server.

WHAT ARE SSL CERTIFICATES?

A browser has to have confidence that a server is who it claims to be, and is able to confirm this through something called an SSL Certificate.

A browser will request an SSL Certificate and check this information against something called a Certificate Authority. A Certificate Authority is the issuer of an SSL Certificate.

Major browsers, operating systems and mobile device companies work with Certificate Authorities to maintain a list of trusted root certificates.

TYPES OF SSL CERTIFICATES

There are three primary types of SSL Certificate; Domain Validation, Business Validation and Extended Validation.

DOMAIN VALIDATION

This is the most common and can be issued within minutes. You'll be able to secure these certificates at a low cost or even for free.

BUSINESS VALIDATION

These certificates can take a few days to be issued as they require you to provide more information to the Certificate Authority. You'll have to pay, but not as much as for an Extended Validation certificate.

EXTENDED VALIDATION

These can take up to a week to be issued and require the maximum amount of information from a Certificate Authority.

You can see several examples of Domain, Business and Extended Validation certificates in use at the articles below from GlobalSign and ExpeditedSSL:

https://www.expeditedssl.com/pages/visual-security-browser-ssl-icons-and-design

https://www.globalsign.com/en/ssl-information-center/types-of-ssl-certificate/

ServerGuy also has an excellent in-depth write up on the differences between the certificate types that can help you choose the right type of certificate for your requirements.

You will need an SSL Certificate to switch to HTTPS. Fortunately, most hosting companies can provide free or paid SSL Certificate options for you at the click of a button.

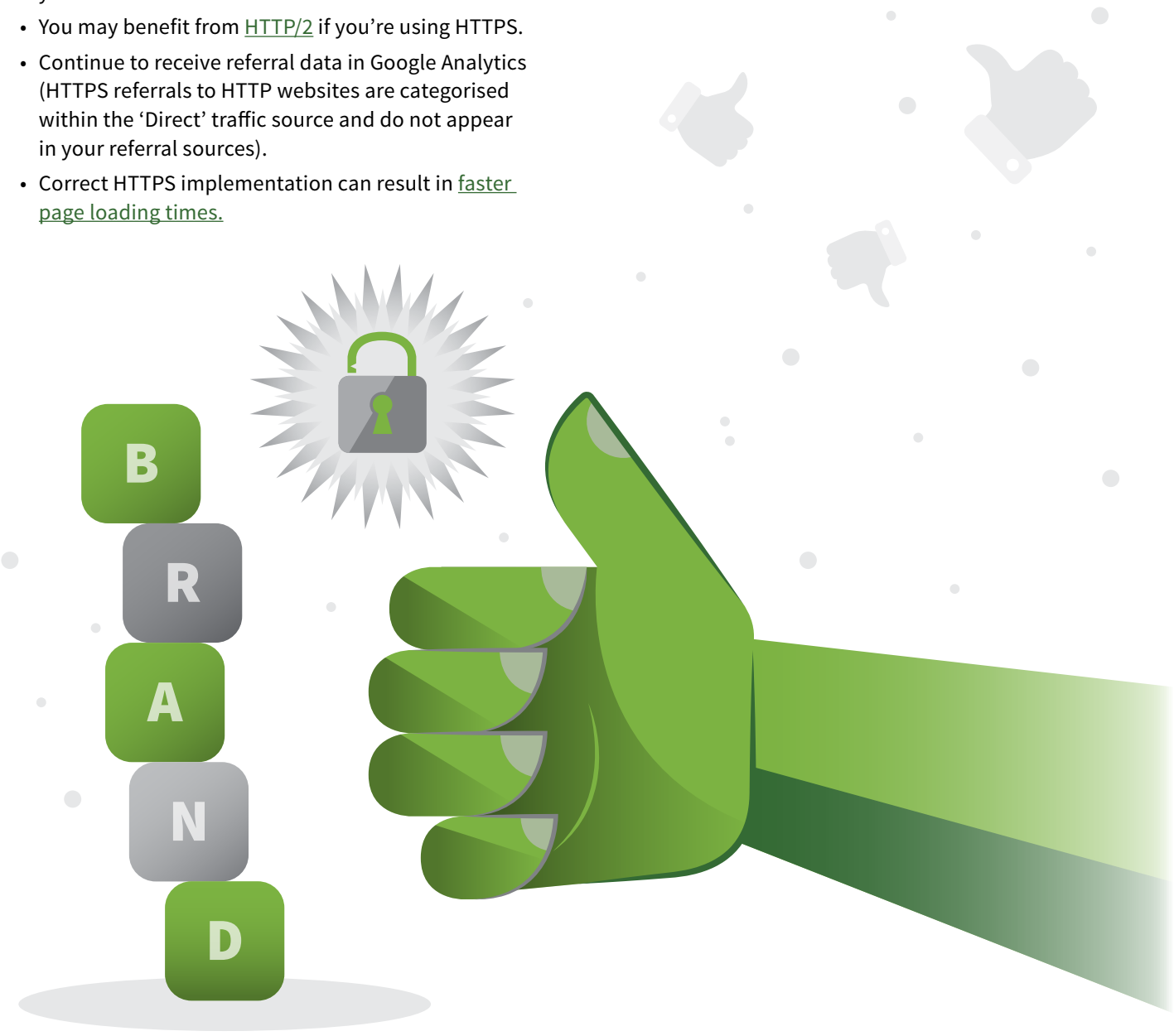
PROS & CONS OF SWITCHING TO HTTPS

PROS

- Google has said that HTTPS pages receive a ranking boost.
- Prevent hackers or third-parties from intercepting user data.
- The level of trust it gives to users when they see that their information is secure, i.e. the green padlock and the extended validation green bar. This is essential for any website that requests a lot of user information, for example, an e-commerce website.
- A level of trust is given to users when they see that you are who you claim to be. This is particularly important if you're still in the process of building your brand.
- You may benefit from HTTP/2 if you're using HTTPS.
- Continue to receive referral data in Google Analytics (HTTPS referrals to HTTP websites are categorised within the 'Direct' traffic source and do not appear in your referral sources).
- Correct HTTPS implementation can result in faster page loading times.

CONS

- Might require support from your development team and hosting provider.
- There is a cost for certain types of SSL Certificate.
- Different certificates have different lengths of renewal. An expired certificate will invalidate your HTTPS implementation.
- You will need to dedicate some time and resource to ensure the switch from HTTP goes smoothly.
- There are opportunities for things to go wrong, which can be a risk for sites that rely on organic search traffic.



HTTP TO HTTPS CHECKLIST

Now you know how HTTPS works, and some the benefits, here are the steps you need to take to ensure a smooth HTTPS migration.

PLANNING AND PRE-MIGRATION

1: Plan your time

The time it takes to complete a HTTPS migration can vary depending on the size of your website, the resources you have available and the support levels of your host or development team.

If you're responsible for a HTTPS switch, plan it for a time of low-seasonal activity. It's also important that you have the time to oversee the migration, so plan it for a time where you know you're going to be freed up and able to concentrate. For smaller sites or non-e-commerce sites with less than 5,000 pages, you might want to book out between 1 and 3 days in your diary. For websites with 5,000-10,000 pages or with e-commerce/ordering functionality, aim for 3-4 days. If you're a large website with 10,000+ pages or have lots of third-party integrations or back-end functionality, you might want to have at least a week free to work through all of the necessary HTTPS processes.

Oh, and never plan a migration for a Friday. Just in case something goes wrong!

2: Communicate the planned migration to your team

Once you've decided on when you're going to migrate, make sure this is communicated to any team that works on the website.

Put the date in the calendars of your colleagues as well as your own. You'll want to ensure sure that you're making the switch at a time where there are no other planned website changes. Doing this will help to minimise the risk of any potential problems. If something does go wrong, it'll be easier to pinpoint the problem.

3: Benchmark

Check the tracking status of Google Analytics and Google Search Console. How will you know if your HTTPS migration has been successful?

The only way you'll truly know is if you have data to compare it against. So check that your current Google Analytics and Google Search Console accounts are collecting accurate data, particularly for organic search. If they're not, you should aim to collect at least a week's worth of data in those accounts before making the switch.

In addition to this, crawl your current website using a tool like DeepCrawl or Screaming Frog so that you have a full HTTP dataset for post-migration comparisons.

4: Speak to your web hosting company or IT team

It's highly likely that in the process of migrating to HTTPS you'll need the support of your web hosting company, development team or IT team (Whoever is currently responsible for hosting your website and maintaining its performance and security). Even if you don't think you're going to need them, it's useful to have them on board during a migration just in case you hit any snags.

For those that aren't particularly comfortable with hosting environments, implementing redirects or working on staging environments, you're most likely going to need support with steps 5 to 10. Be open with them and tell them where you think you'll require most of their time and support.

Handling a website migration of any description alone can be very daunting, so don't underestimate the importance of getting your host or developers engaged in the project.

Some questions you might want to ask your web hosting company or development team include:

- **Have you handled any HTTP to HTTPS migrations recently?**
- **What were the results?**
- **Were there any problems?**
- **Could they have been avoided?**
- **How long did it take?**
- **Were there any frustrations for you in this process?**

You might even want to share this guide with them and ask them if they're comfortable with everything that's featured within. This sometimes the easiest way to identify any potential issues ahead of the migration happening!

5: Decide on your SSL Certificate type

Earlier in this guide, we detailed the different types of SSL Certificates that are available. You'll need to make a decision based on the level of authentication you require, the budget you have available and the technical configuration of your hosting environment.

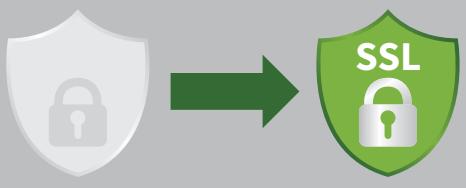
Another factor in deciding which certificate type to use can be whether or not you are using a CDN (Content Delivery Network). Though CDNs can help add an extra layer of security and simultaneously help to improve page performance through speedy delivery, they can make for a slightly more complex HTTPS migration. This is because certificates are needed for the secure transfer of information from your browser to your CDN and then your CDN to your server and vice-versa.

If you're unsure, the best thing to do is speak to your development team or web hosting company. Web hosting companies will usually partner with both free and paid SSL Certificate providers and have simple cPanel (or alternative) functionality to make SSL Certificate activation and CDN configuration much easier than it might appear.

If you're curious, leading CDN provider, Cloudflare has an excellent write up on CDN and TLS integration.

Additional tip alert

You'll also want to check that any SSL Certificates configured are set to auto-renew. SSL Certificates have expiry dates, and if they do not auto-renew, you can lose your HTTPS status. Once the certificates are set to auto-renew, you shouldn't have any problems, but still, mark the renewal date in your diary and check the status of HTTPS on the date your certificate is set to renew.



HTTP TO HTTPS CHECKLIST *Planning and Pre-Migration*

6: Backup your website

Hopefully, you'll already have a tool or process in place to manage routine backups of your website.

But just in case you don't, now is the time to back up your website before you make any changes!

...and maybe speak to your developers about getting some backup management after the migration.

7: Access your staging server

Unless you're SUPER brave, you're probably not going to want to make all of the changes below to your live website.

Instead, you should configure everything below on your staging server to test before 'mirroring' and merging with your production website.

8: Configure the HTTP to HTTPS rewrites

This is the stage where you "force" all requests for HTTP URLs to redirect to the new HTTPS variations.

The type of rewrite you use will be dependent on the web server software you use. Again, if you're unsure, this is a good time to reach out and speak to your web hosting company for support.

WordPress Users Thankfully, forcing HTTP to HTTPS redirects is a little easier on WordPress than some other content management systems. Here are some handy guides from Kinsta and SererGuy on how to edit your .htaccess file and implement your HTTP to HTTPS redirects:

https://serverguy.com/servers/redirect-http-to-https/

https://kinsta.com/knowledgebase/redirect-http-to-https/

MacOS Users Struggling to find your .htaccess file? When viewing your directory files, you might find that macOS natively hides some files. To show all hidden files, follow this guide depending on the macOS version you're using.

Important When configuring your HTTP to HTTPS rewrites, you should also ensure that any legacy redirects are forced to the new HTTPS status.

9: Update all internal links, scripts and code references to HTTPS

Your development team should be able to update all internal links and references from HTTP to HTTPS using "find and replace" server database functionality.

You will want to ensure you update the new HTTPS status for:

- All internal links
- Canonical tags
- Hreflang tags
- Open Graph tags
- Media assets (videos, audio, images and files should all be served via HTTPS)
- Font files
- CSS and JavaScript files

In addition to requesting support from your developer, you should manually review and update the website for any hardcoded links in plugins or widgets you might be using within your CMS as these can sometimes escape a find and replace request

10: Crawl the website and fix issues on staging

Using the crawling tool of your choice, crawl the website and check that all URLs are served in HTTPS, check the points detailed in step 9 and address any issues with mixed content. Both DeepCrawl and Screaming Frog have insecure content discovery functionality within their tools.

What is mixed (or insecure) content? Glad you asked!

If a page is encrypted (served via HTTPS) but elements of that page are unencrypted, this is considered mixed or 'insecure' content.

It's fairly common to find pages with insecure content when using content management systems with lots of third-party integrations such as plugins or widgets. Your job should be to try and eliminate as much mixed content as possible.

Using DeepCrawl and Screaming Frog will help you identify pages with insecure content, but if you're working on a smaller website, you might want to use one of the many Chrome extensions, such as the HTTP Mixed Content Locator to help you find the mixed content on your site quickly.

Once you've identified the mixed content, you'll need to see if a secure version of that content exists. If it does, you should update your internal references accordingly.

If you find there is insecure content without a secure version that's outside of your control, you might want to consider finding an alternative widget or plugin to use that replicates the functionality you're trying to achieve.

HTTP TO HTTPS CHECKLIST *Planning and Pre-Migration*

11: Pause or prepare paid ads and third-party tools

You might find that you'll need to pause any paid advertising campaigns around the time of your migration to avoid any wasted ad spend.

It's likely you'll need to update any paid advertising platforms with the new HTTPS URLs, so give you (or your team) plenty of time to do this ahead of launch if it's achievable.

On a similar note, you might find that third-party tools for CRO, analytics or any other integrations you use for your website might require configuration changes to reflect the website's new HTTPS status.

This is a good time to take stock of what you can update before launch and make a note of any tools that you need to update on launch day.

12: Tell your users (and your customer support team)

A HTTPS migration can go wrong, and users might experience website issues or downtime that they're not used to experiencing.

For that reason, when you have a HTTPS launch day confirmed, it's worth communicating that to your users or customers and your customer support team (if you have them).

You don't have to tell them all the gory HTTPS details (though, why not?), a simple explanation **that server changes are being made that might impact user experience** should suffice. Remember to tell both your users and your customer support teams where to report any issues if they arise.

LAUNCH & POST MIGRATION

13: Launch day!

Congratulations! But...don't celebrate with tequila shots at your desk just yet, we've got some work to do.

It's best to ensure that you have your entire launch day free as there are quite a few tasks best saved for this.

Starting with...

14: Manually check your website (and ask others to do so too)

A HTTPS migration can go wrong, and users might experience website issues or downtime that they're not used to experiencing. For that reason, when you have a HTTPS launch day confirmed, it's worth communicating that to your users or customers and your customer support team (if you have them).

You should sense check:

- What's the browser omnibox showing in respect of your HTTPS status?
- What happens if you type in the original HTTP homepage variation? Does it redirect?
- Test a few other URLs, do they redirect as expected?
- Are media assets all appearing correctly?
- Are pages noticeably slower to load?
- Are Robots meta tags correct? Have you been careful to avoid the dreaded, accidental noindex?
- Is the robots.txt file in place? Does it link to your HTTPS sitemap?
- Can you submit a form, sign up for a newsletter and complete a transaction or conversion as normal?

Set up a bug reporting log (Trello, Google Sheets) for you and anyone else in your team that happens to spot anything unusual with your website after launch day.

You don't have to worry about immediately fixing everything you find, but having an awareness of what might have gone wrong at this stage can help you prioritise your time when it comes to the rest of your post-migration tasks.

LAUNCH & POST MIGRATION

15: Create new HTTPS Google Search Console properties

HTTP and HTTPS website variations are seen as unique in the eyes of Google (duh, that's kinda why we're here!).

This means that on launch day you'll need to configure your new Google Search Console Properties. Both the HTTPS-www and HTTPS non-www versions.

You'll only fully configure your preferred HTTPS variation; the other is to have as a verified property that you can monitor to stay on top of any potential www/non-www issues.

16: Create and submit your new HTTPS sitemap

Create or update your sitemap containing only HTTPS URLs and submit that to Google Search Console.

If you've referenced your sitemap in your robots.txt file, you should double-check that it includes your HTTPS sitemap URL.

17: Configure your HTTPS Google Search Console property

You'll want to make sure that you configure your new HTTPS property so that it matches all of your previous HTTP configurations.

You'll need to:

- Submit your HTTPS sitemap

Upload any disavow files that were previously active on your HTTP Google Search Console property

- Run Fetch & Render Googlebot checks for desktop and mobile
- Configure any URL parameters
- Connect your Google Search Console property to your Google Analytics property (you can also make this connection in Google Analytics)
- Configure Google Search Console Site Settings

18: Crawl the website, again

You should now crawl your website again and compare the crawl data against any previous crawls.

The key things you're looking for at this stage are:

- Any insecure/mixed content warnings
- Ensuring that HTTP to HTTPS redirects are permanent 301 redirects and are going to the correct URLs
- Canonical and hreflang URLs are all HTTPS
- Ensuring that no HTTP URLs are discovered

LAUNCH & POST MIGRATION

19: Check the SSL configuration

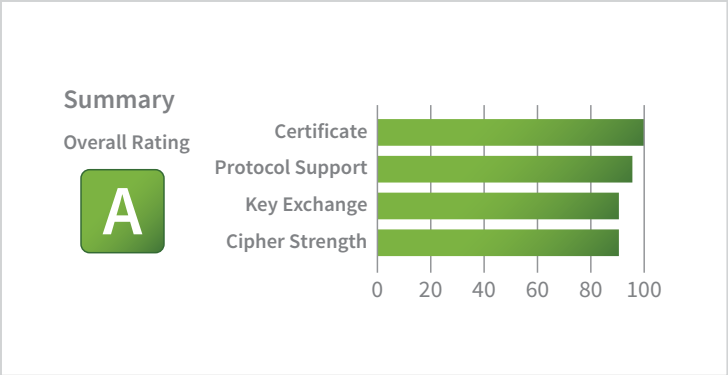
Upon launch, you can also use one of the many handy SSL configuration checkers

ssllabs.com

sslshopper.com

jitbit.com/sslcheck

…here's one we made earlier @ ssllabs.com



20: Update Google Analytics

In Google Analytics you'll need to update the Default URL in your property and Views.

To do this at a property level, go to Admin > Property Settings > Default URL > Save.

Default URL

https:// www.sitevisibility.co.uk

To do this at a View level, go to Admin > View Settings > Website's URL > Save.

Website's URL

https:// www.sitevisibility.co.uk

You'll also need to connect your HTTPS Google Search Console property data with your Google Analytics property. To do this, go to Admin > property Settings > Search Console > Adjust Search Console.

Select the correct property and then save.

Search Console

Adjust Search Console

While you're in Google Analytics, remember to annotate your HTTPS launch day!

21: Update your social media URLs

If you have social media URLs that link back to your website, update those URLs with the new HTTPS location.

This can be particularly important for YouTube where, if you're part of the Partner Programme, you may now need to link to your new HTTPS Google Search Console property to continue to be able to utilise video features.

LAUNCH & POST MIGRATION

22: Monitor the results

At this point, we hope you have the hackers in tears, a website faster than a shooting star and a glowing green box mercilessly patrolling your browser's omnibox..

But if you didn't quite get there, fear not. The best thing to do if you come up against any issues is to go back through the steps in this checklist. Did you skip anything? Was there something you were a little unsure about the first time around? Go back over any uncertainties. Check, double-check and triple check.

Over time you should see Google start to propagate search results with new HTTPS URLs. Your indexed URLs should drop off in your old HTTP Google Search Console account and increase in your HTTPS Google Search Console account as this propagation takes place. The speed at which that happens can vary dependent on the size of your website.

You might see a ranking boost; you might not. You certainly shouldn't expect it. This could be for a variety of reasons, but if you're migrating now (in 2019) there's a fair chance that a number of your search competitors have already upgraded and you might be playing catch up!

23: Consider HSTS implementation

Once you're confident in your HTTPS implementation, you may want to continue to explore the option of utilising HSTS (HTTP Strict Transport Security) with your web host or development team.

HSTS is a further layer of security that can only be implemented if you're using HTTPS. Google recommends sites using HTTPS also use HSTS, stating:

> We recommend that HTTPS sites support HSTS (**HTTP Strict Transport Security**). HSTS tells the browser to request HTTPS pages automatically, even if the user enters **h t t p** in the browser location bar. It also tells Google to serve secure URLs in the search results. All this minimizes the risk of serving unsecured content to your users.

CHECKLIST

Task	Responsible	Due	Complete
1: Plan your time			
2: Communicate the planned migration to your team			
3: Benchmark			
4: Speak to your web hosting company or IT team			
5: Decide on your SSL Certificate type			
6: Backup your website			
7: Access your staging server			
8: Configure the HTTP to HTTPS rewrites			
9: Update all internal links, scripts and code references to HTTPS			
10: Crawl the website and fix issues on staging			
11: Pause or prepare paid ads and third-party tools			
12: Tell your users			
13: Launch day!			
14: Manually check your website (and ask others to, too)			
15: Create new HTTPS Google Search Console properties			
16: Create and submit your new HTTPS sitemap			
17: Configure your HTTPS Google Search Console property			
18: Crawl the website, again			
19: Check the SSL configuration			
20: Update Google Analytics			
21: Update your social media URLs			
22: Monitor the results			
23: Consider HSTS implementation			

WANT SOMEONE TO TAKE CARE OF THIS FOR YOU?

GET IN TOUCH

grow@**sitevisibility**.com

01273 733 433

www.**sitevisibility**.com