SSL Implementation: The Step by Step Process

1. **Website backup**
   Make a backup of the site so that we have a backup on hand in case we run into issues after the SSL implementation process.

2. **WWW or Non WWW**
   Determine if we should utilize www in the web address or not (www or non www) or non www. Dylan said that he prefers the www version, however if Google has already absorbed the www or non www version, use that version.

3. Add site to SANS SSL Certificate list on GoDaddy. Make sure only the www or non www version is listed on the cert.

4. Create a .well-known folder, and a file named godady.html file to verify domain ownership. Upload folder and notify GoDaddy of the changes.

5. **Create the .HTACCESS file**

   Create a blank text document in notepad and name it .HTACCESS

   An example of a .HTACCESS is listed below:

```
#Turns on Rewriting Engine
RewriteEngine on

#Adds www to the site when someone types in a non WWW version
RewriteCond %{HTTP_HOST} ^www\.(.*)$ [NC]

#Enables a 301 redirect to notify Google that the website address has been changed
permanently from the old http:// version to the https:// version.
RewriteRule ^(.*)$ https://%1/$1 [R=301,L]
RewriteCond %{HTTPS} !on
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
```

   Once you have created this file, you can upload it to test its functionality. However, you may way to delete one you are done testing things if the site is a live site.

6. **Look over the site code, and locate mentions of http:// and change them to https://**

   Determine how much content uses non secure / non SSL links (http://)

   In most cases, you need to change all mentions of http:// to https:// so that the SSL works properly on every page of the site.

With that said, this is where get things get tricky, as not all of the website content will support SSL. On one hand, we want to change as many thing from http:// to https://. However, in some cases, we will not be able to change some of the code to https:// as not all website content will support SSL.

Here is an example of a line of code that makes the slideshows on many of our websites work, and this is a good example of a line of code that can be changed so that it will support SSL (as this particular element does indeed support SSL).

Before SSL:

http://c520866.r66.cf2.rackcdn.com/1/js/easy_rotator.min.js

To make SSL work correctly on a page that uses this line of code, we will need to modify it so that it supports SSL. To do this, simply add an "s" to the web address (as shown / highlighted below).

After SSL:

https://c520866.r66.cf2.rackcdn.com/1/js/easy_rotator.min.js

Next, as I mentioned, not all content that our websites may reference will support SSL. A good example of this our Spacecrafted website redirect code. Because Spacecrafted has yet to provide SSL (https://) on their sites (they plan on doing so in August though), we will not be able to add a a "s" to the code that is shown below.

```
<script type="text/javascript">
 <!--
 if (screen.width <= 800) {
  window.location = "http://m.gp-radar.com";
 }
 //-->
</script>
```

Generally, we would add a "s" to the http:// in this line of code (shown above) but due to the fact that Spacecrafted does not support SSL at this time, if you add a "s" to this particular line of code, you will simply create a "404", and of course this would be bad. This is why it is important to test the site as you change lines of code from http:// to https://.

Another example:

The following link is the link that GPRS uses for their Career Opportunities link:

http://newton.newtonsoftware.com/career/CareerHome.action?clientId=8a788260596d6c9b0159897036125756

to add SSL functionality to this link, simply add an "s" to the http:// and it will the look like this:

https://newton.newtonsoftware.com/career/CareerHome.action?clientId=8a788260596d6c9b0159897036125756

7. **Change mentions of http:// to https://**
   Again, this should be done very carefully as not all content will support SSL.

8. **View the site in Internet Explorer, Chrome, Firefox and Safari, and make sure that the padlock shows up in the web address bar when you view every page of the website.**

   As you change code elements from http:// to https:// eventually, you will see that a padlock will display in the web browser bar. When this happens, this means that the SSL is working on the page that are visiting. Note: just because one page on a site may show a padlock, this does not mean that all of the pages of the site will show a pad lock. Therefore, it is important that you look over EVERY page of the website that you are working on.

   While you are looking over the site pages, if you locate a page does not show a pad lock, you will need to look over the HTML code, very likely there is a http:// somewhere in your code that needs to be changed to https://.

   However, as previously mentioned, you need to make these changes very carefully as not all website elements will support SSL.

9. **Troubleshooting "no padlock"**

   If the padlock does not show for a page, and you can't figure out why the padlock is not showing, a helpful tool is this website: https://www.whynopadlock.com/

   This tool will let you know what website contents are causing the SSL to not work. To use this tool, simply copy and paste the link of the page that you are trying to troubleshoot into the tool, and the Why No Padlock website will let you know what section of code on the page you are having trouble with is causing the pad lock to not show up.

   If the https://www.whynopadlock.com/ website tells you that if a certain element of the site is causing the issue, you will need to address these issues.

10. **Run a SEMRUSH site audit**

    Run a site audit on the site that you have added SSL to. SEMRUSH will provide you with a score between 0 and 100 and the closer are to 100, the better. If you have a score of 100, the SSL

implementation went perfectly. For most sites, we should be able to achieve a score 95 or higher in most cases.

After SEMRUSH runs a site audit, it will make several suggestions on what can be done to made to increase the effectiveness of the SSL cert.

11. **Generate a new site map, notify Google of the new sitemap, and request Google to recrawl the site**

    Once you have generated a sitemap, and once you have uploaded the sitemap to the server, the next step that should take is login into Google Webmaster Tools, and notify Google that a new sitemap has been generated.

    After the new site-map has been submitted to Google, the next step is to request Google to recrawl the site (which can be done via Webmaster Tools). By requesting Google to re-crawl the site, they will likely "absorb" the new SSL site in to the search results much quicker.

12. **Update Client's Google Account**

    Login into customer's Google account, and update Adwords, Analytics, and Webmaster tools with new SSL web address.

13. **Documentation**

    Once the SSL implementation process is finished, add the site to the "finished" SSL sites spreadsheet in Google Docs. Be sure to notate the date at which the SSL install was finished. Also, if there is any other information that may be helpful in the future upkeep of the site's SSL, please include this information in the spreadsheet as well.

Editing an SSL Site: Best Practices to Follow

When you are adding content, or making changes to a site that uses SSL, it is important to note that when you make changes to the site, you may cause issues with the SSL.

Therefore, when you are adding content to a SSL site, you will need to make sure that your code uses https:// rather than https:// in all link references.

For example, let's say you are adding a Google Font to the site that you are working on. Below is an example of the code that you would use:

Example code:

<link href="http://fonts.googleapis.com/css?family=Open+Sans" rel="stylesheet">

If you look at the code carefully, you will notice that the web address does not have “s” in the http://. Therefore, the code above would cause issues with a SSL site.

To make that Google font code to work correctly, issues with the SSL, you will need make the code look like this:

<link href="https://fonts.googleapis.com/css?family=Open+Sans" rel="stylesheet">

As you can see, the only change that was made was that a “s” was added to the http:// of the code. Although this is simple change, this change will allow the SSL cert to work correctly. Failure to add this “s” would result in the SSL working on the page where this line of code was added to.

Once you have updated a page on a site that uses SSL, the best practice would be to view the site in several different browsers, and make sure that the padlock shows up in all types of browsers (Edge, Firefox, Chrome, and Internet Explorer).

If the padlock does not show up in the web browser after you edit a page, you will need to figure out why the SSL is not working on the page that you edited. A good tool to determine why the padlock / SSL is not working correctly on the page you just edited, a good tool to use is: https://www.whynopadlock.com/