SEO Standard Operating Procedure (SOP): HTTPS & SSL Certificates

Krishna Results

Purpose:

To ensure the website is secure by implementing an SSL certificate, improving user trust and search engine rankings. Sites without SSL are marked as unsafe by browsers, leading to traffic loss and a negative impact on SEO. This SOP outlines the process for setting up SSL to secure the site and boost SEO performance.

---

1. What is SSL & HTTPS?

- **SSL (Secure Sockets Layer)**: A protocol for encrypting internet traffic and verifying server identity. It ensures that data passed between the server and users is protected from eavesdropping or tampering.

https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/

- **HTTPS (Hypertext Transfer Protocol Secure)**: The secure version of HTTP that uses SSL to encrypt data. When SSL is installed, the website's URL will start with HTTPS instead of HTTP.

---

2. Why is SSL Important for SEO?

1. **Boosts Search Engine Rankings**:

- Search engines like Google prioritize secure sites by giving them a ranking boost.
- SSL helps establish your site as trustworthy and high quality, factors that improve SEO.

2. **Prevents “Not Secure” Warnings**:
   - Browsers display warnings for sites without SSL certificates, stating that the site is not secure. This discourages users from accessing your site, resulting in traffic loss.
   - With SSL in place, the warning is removed, ensuring a smooth user experience.
3. **Protects Website Data & Prevents Diversion**:
   - SSL encryption prevents data breaches and protects sensitive information (e.g., payment details or login credentials).
   - It ensures users are directed to the correct site without risk of being diverted to unsafe alternatives.

---

3. Steps to Set Up SSL on Your Website

1. **Choose an SSL Certificate**:
   - **Free SSL Certificates**: Providers like Let’s Encrypt offer free SSL certificates that are valid for 90 days and can be auto-renewed.
   - **Paid SSL Certificates**: These offer additional features like higher encryption levels, warranties, and extended validation for businesses.
2. **Purchase or Install a Free SSL Certificate**:
   - Use your hosting provider’s control panel or work with your web developer to purchase and install the SSL certificate.
   - **Popular SSL Providers**: Let’s Encrypt, Comodo, DigiCert, and GoDaddy.
3. **Configure SSL with Hosting Provider**:
   - Most hosting providers offer easy one-click SSL installation for free or paid certificates.
   - Ensure the entire site (including subdomains, if necessary) is covered by the certificate.
4. **Update Website Links to HTTPS**:
   - Update internal links, images, scripts, and resources on your website from HTTP to HTTPS.
   - Redirect all old HTTP URLs to the new HTTPS URLs using a 301 redirect to preserve SEO rankings.
5. **Update Your CMS Settings (if applicable)**:
   - For WordPress and other CMS platforms, update the site URL and settings to reflect the change to HTTPS.
6. **Verify Installation**:
   - Test the SSL certificate using tools like **SSL Checker** to ensure it is installed correctly.

- Check for mixed content errors where some elements on the page are still served over HTTP.

7. **Submit the HTTPS Site to Google Search Console**:
   - Once SSL is installed, update your sitemap in Google Search Console to reflect the HTTPS version of the site.
   - Re-crawl and re-index the HTTPS site for better visibility.

---

4. Best Practices for SSL & HTTPS

1. **Ensure Full-Site SSL Coverage**:
   - Every page on the website should be served over HTTPS. Partial SSL coverage can still result in “Not Secure” warnings.
2. **Set Up 301 Redirects**:
   - Redirect all HTTP pages to their HTTPS counterparts using 301 redirects to ensure link equity is passed on and SEO rankings are preserved.
3. **Update Backlinks**:
   - Reach out to any high-quality sites linking to your HTTP pages and request they update their backlinks to HTTPS.
4. **Monitor SSL Certificate Expiry**:
   - SSL certificates typically expire within 1-2 years. Set up auto-renewal or manual reminders to ensure there is no gap in security.
5. **Check for Mixed Content**:
   - Ensure all resources (e.g., images, CSS, JS files) are loaded over HTTPS to avoid browser warnings.

---

5. Common Mistakes to Avoid

1. **Forgetting to Set Up 301 Redirects**:
   - Failing to redirect HTTP to HTTPS can cause SEO issues like duplicate content, ranking drops, and broken links.
2. **Ignoring Mixed Content Warnings**:
   - If some resources on the site are still served over HTTP, browsers will display a warning. Ensure every element is loaded securely.
3. **Using an Expired SSL Certificate**:
   - Expired SSL certificates will result in browser warnings and loss of trust. Set up auto-renewal to avoid expiration.
4. **Not Updating External & Internal Links**:
   - Failing to update all internal links and external backlinks to HTTPS can result in SEO penalties and mixed content errors.

---

6. Final Review Checklist

Before launching the website, follow this checklist to ensure SSL is correctly implemented:

- ☐ SSL certificate is installed correctly for all pages.
- ☐ All pages load using HTTPS (check using browser inspection tools or SSL checker).
- ☐ 301 redirects are set up from HTTP to HTTPS.
- ☐ Internal links, images, and scripts are updated to HTTPS.
- ☐ No mixed content warnings appear in browsers.
- ☐ HTTPS site is submitted to Google Search Console and indexed.
- ☐ SSL certificate is set to auto-renew or expiration reminders are in place.