Migrating to HTTPS Everywhere

digicert®

Table of Contents

This guide gives you an in-depth look at all the benefits—including security, usability, and SEO—of deploying SSL/TLS across your entire website. Now that Google has added a rank boost for HTTPS Everywhere, a lot of companies want to enable SSL site-wide. But where do you start? And what are the implications for your website? DigiCert created this guide for our customers to give you an in-depth look at the security benefits of HTTPS Everywhere and to get you started with implementing HTTPS Everywhere on your own website.

Get Your Company on Top with HTTPS Everywhere

IT administrators know that organization security is a journey, not a destination. There is always something new—whether it's a new OS, new exploits, or new security best practices.

SEO is very similar. Google is constantly changing their search algorithm—adding new factors, taking away factors, and changing their importance. And, just like security, most of the factors aren't obvious. In SEO, Google's algorithm factors are vague and can be difficult to measure. In security, the threat landscape is changing so rapidly it can be difficult to keep up.

With Google's 2014 announcement that HTTPS Everywhere is a factor in their ranking algorithm, enabling SSL across your entire website is a guaranteed win for both security and SEO.

What is HTTPS Everywhere?

HTTPS Everywhere is simply the practice of using HTTPS across your entire website. This is in contrast to a partial deployment of SSL that may only be on certain pages—such as a log-in or checkout page. The use of HTTPS on only these "sensitive" pages was popular when the technical costs of HTTPS, such as memory overhead and CPU load, were high. Now that HTTPS has an insignificant footprint, there is no practical reason to selectively use it.

In fact, due to all major browsers fully embracing HTTPS, you can achieve better performance with it than without by taking advantage of new technologies only available on HTTPS.

Why is Google Pushing HTTPS Everywhere?

HTTPS Everywhere has been recommended as a security best practice for years. Standards bodies, such as the Online Trust Alliance, CA Security Council, and Microsoft, have touted HTTPS Everywhere as the only way to truly secure user data online. The majority of the world's largest websites use HTTPS Everywhere, which Google tracks and regularly updates.

When the internet transitioned from primarily HTTP sites many decided to deploy HTTPS selectively. This was seen a necessary step towards a 100% HTTPS internet, but now major internet companies, including Google and Mozilla, are telling the world it's time to take the next step.

Google is constantly looking for new ways to improve security, both for their customers and for the wider internet population. Whether it's their white hat security team hunting down security vulnerabilities, developing their own version of OpenSSL, or using their domination of the search engine market to push companies toward HTTPS Everywhere, Google is heavily involved in the world of web security.

"Security is a top priority for Google... we're also working to make the Internet safer more broadly. A big part of that is making sure that Websites people access from Google are secure... we'd like to encourage all Website owners to switch from HTTP to HTTPS to keep everyone safe on the Web."

Zineb Ait Bahajji and Gary Illyes
Webmaster Trends Analysts, Google

Benefits of HTTPS Everywhere

HTTPS Everywhere benefits you in a variety of ways, on both the marketing and IT sides of your business.

Improved Security: Implementing HTTPS across your entire site protects you and your customers from the next generation of security threats. These threats, which are described in-depth in the next section, are easy to execute. And it's not just log in credentials or credit card data that attackers are looking for—online browsing habits and personal information shared on social sites can all be used by malicious entities.

Brand Protection: Securing your users' data not only helps browsers, it helps you. Most businesses can't afford the astronomical cost of a data breach—no matter what user information is leaked. In 2017, IBM reported that companies are at an increased risk of repeated data breaches compared to last year. And, according to a 2017 Ponemon study, the average cost of a data breach is $3.5 million.

Increased User Trust: Because users trust SSL certificates, they are proven to increase conversion rates, improve engagement metrics, and elevate brand reputation. According to a study by Tech-Ed, 100% of participants would prefer doing business with a company that has an EV SSL certificate. This benefit extends beyond just log in or checkout pages—by having SSL on every page of your site all of your visitors know that you are legitimate and that your identity has been verified.

How HTTPS Everywhere Protects Your Users

The intermittent use of SSL on your website is not enough to combat today's threats. New methods of hijacking and eavesdropping on unencrypted sessions make it easier than ever to steal your users' information. The consistent and strict use of SSL across your entire site ensures that all pages, cookies, and sessions are secure and all user data is safe, no matter what page they are on.

All the threats that SSL protects against—theft of sensitive information, plaintext traffic analysis, and content injection—are still vulnerabilities on the HTTP portion of your site. So not only are your users missing out on these key protections on HTTP pages, but due to the risk of content injection and sidejacking, there is also a risk they will be unable to safely visit your HTTPS pages.

Any unsecured page is a vector for attack, and leaves your user's data in plaintext, where it can be monitored and recorded by ISPs looking to profile their customers. Simply put, when you use HTTPS on only some of your pages you are providing incomplete security.

HTTPS Everywhere is considered a best practice because it encrypts user sessions the entire time they are on your site, not just on pages that directly handle sensitive data like log-in or checkout pages.

Here are some of the threats you face with partial HTTPS usage:

SESSION HIJACKING AND SIDEJACKING

One popular technique is called session sidejacking. Because websites typically encrypt log-in pages, user credentials are secure while they are being entered. However, once the user has been authenticated they are often redirected to an unprotected page inside their account. At this point the hacker uses a packet sniffer to intercept the network traffic between the browser and server to steal the plaintext session cookie. With this information, the attacker can impersonate the user and alter or steal the exchanged data.

Unsecured Wi-Fi Hotspots are especially vulnerable to this technique since the broadcasted data is easy to intercept. Various easy-to-use tools and even browser plug-ins have been created to conduct session sidejacking attacks on unsecured Wi-Fi Hotspots. One tool, called Firesheep, received global news coverage for making these attacks possible with only a few clicks of a button. It was a wakeup call to major sites, like Facebook.com, which at the time were not using HTTPS Everywhere.

MIXED CONTENT

When you have a combination of unsecure HTTP content and secure HTTPS content you have a mixed content page. This leaves users with only a partially protected connection, which browsers treat as an HTTP page.

Even just one HTTP-delivered resource on an HTTPS page is enough to trigger a mixed content warning. That's because that single resource could be enough to compromise the entire page's security if an attacker replaced it or intercepted it.

These unsecured resources fall into two categories: passive and active. Passive items include images, and sound/video files. Active items are generally scripts, CSS, WebSockets, and iframes, etc. When encountering mixed content, most browsers either display a mixed content warning or block parts of the page. The type of mixed content allowed by browsers varies, but most browsers default to allow passive content while forbidding active content.

Using mixed content can cause a variety of problems, including:

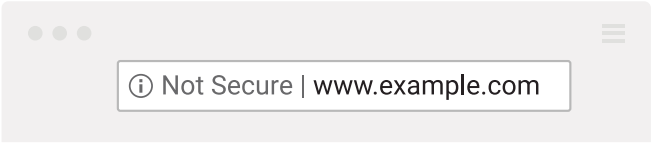
- **Heeded warnings:** Many of your users will encounter the mixed-content warnings (e.g., "This webpage contains content that will not be delivered using a secure HTTPS") and will decide to abandon their visit.
- **Unheeded warnings:** After receiving the warnings your users choose to ignore them. This is training your users to ignore security warnings, which is never a good idea.
- **Blocked Pages/Content:** Active mixed content is automatically blocked by major browsers. This could break key functionality on your site by making scripts and other resources inaccessible, creating usability headaches for your users.
- **Creating Vulnerabilities:** A single exposed script could be used to hijack a connection and compromise your users. Mixed-content warnings advertise the potential vulnerabilities on your site to visiting hackers.

HTTPS Everywhere—Essential For The Future of Your Website

If you consider the security perspective alone, HTTPS Everywhere is an industry best practice, which you should absolutely adopt. But due to activism by Google and Mozilla, adopting HTTPS Everywhere provides even more than those essential security benefits.

From July 2018, Chrome 68 labeled all HTTP pages as "Not secure" with a warning in the address bar. Chrome already applied this label to HTTP pages in certain scenarios—if the page contains a log-in field or the user is in 'Incognito' mode.

This is how your HTTP pages or website now look with Chrome 68.



Mozilla made a similar commitment to demoting HTTP in 2015 and already displays warnings for some HTTP pages.

In addition to UI changes, major browsers are also restricting some browser features to HTTPS to protect user privacy. This includes geolocation, webcam and microphone access, and service workers. Chrome has named these "powerful features," and is continuing to expand the list of features restricted to HTTPS. Firefox has gone a step further, announcing an HTTPS-only requirement for all new features in their browser.

Every major browser (Chrome, Firefox, IE/Edge, and Safari) only supports HTTP/2 when you use HTTPS, which is one of the most significant improvements in internet technology in the last decade. With HTTP/2 you can achieve a quicker load time with SSL than without it. Migrating to HTTPS should no longer be a question of if, but when.

Because of these browser campaigns, websites that don't use HTTPS will find it hard to compete when it comes to speed, functionality, and user trust.

Migrating to HTTPS Everywhere

Moving your site to HTTPS involves more than just going out and purchasing an SSL Certificate. DigiCert recommends reading the following sections thoroughly while you make the transition.

1. FIGURE OUT WHAT CERTIFICATES YOU ALREADY HAVE

If your site deals with sensitive user information, you may already have an SSL certificate on a portion of your website. Before you go buy an SSL certificate, it's best to know what you already have. We recommend using the DigiCert Certificate Inspector tool to find all of the certificates in your environment. This tool will scan your domain or a range of IPs to find certificates. You can also use Certificate Inspector to scan your internal network for SSL certificates.

2. DECIDE WHAT KIND OF CERTIFICATE YOU NEED

Once you understand your current certificate landscape, you will better know what kind of certificate you need. Even if you already have an SSL certificate, you may need to purchase an additional certificate to secure your entire site or other domains.

For example, if you handle sensitive data you may already have an SSL certificate that secures the log-in or checkout page on your site. However, this single-name SSL certificate may not be able to secure the rest of your company's resources if you have multiple subdomains or even multiple domains. You may want to switch to a Multi-Domain (SAN) or Wildcard certificate if you need to secure multiple subdomains or domains.

You may also want to transition to an EV SSL certificate for the added user trust and visual cues, like the green address bar.

DigiCert has many types of SSL certificates designed to meet a variety of needs. For a more detailed description of each certificate type and more information on what type of SSL certificate is right for your situation, try our CertWizard tool.

3. PURCHASE THE CERTIFICATE

Now that you know what kind of certificate you need and you have a CSR, you are ready to buy your certificate. There are a few factors you should take into account when deciding who to purchase your certificate from:

- Issuance Time: Some CAs take days or even weeks to issue a certificate. DigiCert has the fastest issuance times out of any CA. We can even issue an EV certificate in a matter of hours.
- User Trust: Though all SSL certificates can provide the same encryption, the level of trust a certificate provides depends on the issuer. As the leading provider of SSL certificates, DigiCert is well recognized as a provider of high-assurance certificates.
- Powerful Tools: Certificate management tools can save you and your IT team a lot of time. Our innovative Dev team has created tools to help with every step of the certificate management lifecycle.

4. INSTALL THE CERTIFICATE

Once you complete the validation process and receive your SSL certificate, you can install it on your server. You can find step-by-step instructions for installing an SSL certificate on a variety of platforms in the support section of the DigiCert website. Or, if you have a Windows server, you can download the DigiCert Certificate Utility for Windows to automatically install your certificate.

After your certificate is installed, we recommend that you check that everything is working correctly using our free Installation Diagnostics Tool.

If you have any questions, please contact our support team at 1.801.701.9600 or email support@digicert.com.

5. MIGRATE YOUR SITE TO HTTPS

Once your certificate is installed, you must migrate your site to HTTPS. By following some simple steps, you can make your transition to HTTPS easier and make sure you are getting the most out of the SEO benefit.

- **Test your website to make sure your SSL certificate was installed correctly.** Just because your SSL certificate is on your server doesn't mean it's installed correctly. Use a certificate checker like our Installation Diagnostics Tool to make sure your certificate is installed correctly.
- **Test your Website for unsecured content.** Manual testing can help you find pages where content is being accessed over HTTP. During testing, disable access via Port 80 (HTTP). While Port 80 is disabled, all content that was going through Port 80 will be broken and you can quickly find and fix it. Once elements that access Port 80 have been eliminated, re-open Port 80 and redirect it to Port 443 (HTTPS).

- **Add a Server-Side 301 Redirect.** Set up a server-side 301 redirect to direct traffic from port 80 (HTTP) to port 443 (HTTPS). Google considers the HTTP and HTTPS versions of your website to be different sites. Because of this, if you do not redirect traffic Google may see your sites as having duplicate content and penalize you.
- **Track Your Site Migration in Google Webmaster Tools.** List the HTTP and HTTPS versions of your site separately in Webmaster Tools. Because all of your site traffic will move to the new HTTPS version of your site, you should track both sites in any analytics software and in Webmaster Tools to monitor site traffic.
- **Move All Resources to HTTPS.** To get the ranking benefit, your whole site (including all URLs, files, images, dynamic HTML, JavaScript, CSS, assets, and anything with a href attribute) must go through HTTPS. This means going through your entire website and cleaning up the links, as well as making sure all of our resources are accessible through HTTPS to avoid mixed content.
- **Use Relative URLs for Resources that Are on the Same Secure Domain.** There are three types of URLs that you can use for resources on your domain:

  Absolute HTTP URL: <a href="http://www.domain.com/example/about.html">

  Absolute HTTPS URL: <a href="https://www. domain.com/example/about.html">

  Relative URL: <a href="/example/about.html">
  While relative URLs are recommended, if you need to use absolute URLs you should make sure you are including HTTPS instead of HTTP. This will ensure that the user clicking the link will reach the HTTPS version of the resulting page or resource.

  This will also ensure that when Google is scanning your website they will see HTTPS URLs.

- **Use Protocol-Relative URLs for All Other Domains.** Use protocol-relative URLs or absolute HTTPS URLs for all other domains. Protocol-relative URLs for external sites can be formatted as follows: <a href="//domain.com/example/about.html">.
- **Use a Server that Supports HTTP Strict Transport Security (HSTS) and enable it.** HSTS tells browsers to always load pages using HTTPS even when the user enters HTTP in the address bar or another site links to the HTTP version of a page. It also tells Google to serve HTTPS URLs in the search results.

About DigiCert

DigiCert is a leading provider of scalable security solutions for a connected world. The most innovative companies, including the Global 2000, choose DigiCert for its expertise in identity and encryption for web servers and Internet of Things devices. DigiCert supports SSL/TLS and other digital certificates for PKI deployments at any scale through its certificate lifecycle management platform, CertCentral®. The company has been recognized with dozens of awards for its enterprise-grade management platform, fast and knowledgeable customer support, and market-leading growth. For the latest DigiCert news and updates, visit digicert.com or follow @digicert.

DigiCert SSL Retail Phone Number for NAM: 1.866.893.6565
Symantec SSL Retail Phone Number for NAM: 1.866.893.6565
GeoTrust SSL Retail Phone Number for NAM: 1.866.511.4141
Thawte SSL Retail Phone Number for NAM: 1.888.484.2983

DigiCert retail customers (UK): +44 (0) 208.6000.740
French: +41.26.429.77.24
Spanish: 900.931.298
German: +49.69.3807.89081

digicert®