digicert®

Your Quick Reference Guide to HTTPS Everywhere

As a leading provider of SSL certificates, DigiCert is here to help you discover the benefits of using HTTPS across your entire site, and to help you successfully implement it.

https:// What is HTTPS Everywhere?

HTTPS Everywhere is a best practice security measure for websites that ensures the entire user experience is safe from online threats. The term simply refers to using HTTPS—the secure web protocol enabled by SSL/TLS—across your entire website instead of selectively.

HTTPS provides authentication of the website's identity, connection, and data integrity, and encrypts all information shared between the website and a user (including any cookies exchanged), protecting the data from unauthorized viewing, tampering, or mis-use. Maintaining a secure connection across an entire browsing session is vital to ensuring users are safe from advanced spoofing, injection, and man-in-the-middle attacks.

Browsers & the Push for HTTPS

It's no longer acceptable to secure only part of your users' connections. When you intermittently use HTTPS on your website, only some pages are protected by the encryption and authentication of SSL, and others are therefore vulnerable to data theft, content injection/modification, and the privacy-invasion of internet surveillance.

Intermittent deployment of SSL not only fails to meet user's security expectations and rights, but also fails to meet the expectations of browsers and OS platforms. As part of a multi-year effort to encourage the adoption of HTTPS, major browser vendors, including Google, Mozilla, and Apple, have slowly been tweaking the user interface of their browsers to negatively reinforce HTTP and positively reinforce secure HTTPS.

Why You Should Care

Trust is the foundation of the internet economy. To earn that trust, you need end-to-end security to help protect every webpage your users visit—not just the log-in pages and shopping carts. New changes in internet standards and web browsers are also giving websites that use HTTPS a leg up, and are actively punishing unsecure sites that remain on HTTP.

For example, Google has given a search results ranking boost to pages served over HTTPS since 2014. They also display a "Secure" label in the address bar for HTTPS pages. And in July 2018, Google Chrome will start displaying a "Not Secure" warning for every page

served over HTTP. Chrome was the first major browser to warn users on all HTTP pages, and other browsers will follow as the internet moves to a "secure by default" standard.

Additionally, many new web technologies and browser features require HTTPS. This includes HTTP/2, a foundational improvement to the web communication protocol that can greatly improve website performance, as well as browser features including geolocation, notifications, Service Workers, Google's AMP mobile standard, new compression methods, and more. Simply put, without HTTPS, your website will be effectively trapped in the past.

3 The Top 3 Tips for Moving to HTTPS Everywhere

1. Make sure any third-party services you rely on, such as advertising or analytics services running on your site, are available over HTTPS to avoid "mixed content" issues.
2. Purchase additional SSL certificates if different parts of your website run on different servers or domains.
3. Redirect all your web pages to their new HTTPS counterparts and update your Google Webmaster tools. When you switch to HTTPS Everywhere, there are SEO implications. Google and other search engines view this as a website move, similar to moving to a new domain name.

digicert®

Conclusion

- Implementing HTTPS Everywhere on your website secures the user and your organization's data on every page—from start to finish.
- Intermittent use of SSL encryption is no longer sufficient to protect your website visitors or safeguard against data compromise.
- Browser UI will begin showing negative "Not Secure" indicators for HTTP pages, and this trend will only continue as security expectations increase.
- Boost your Google SEO ranking with HTTPS Everywhere, a boost likely to increase in the future.
- HTTPS Everywhere is easy to implement for your website and requires no extra hardware.
- Secure your site with SSL certificates to strengthen your brand and reputation by showcasing your commitment to online security.
- Increased user trust, leads to lower bounce rates and shopping cart abandonments. The benefits: increasing online transactions and conversion rates.