Guía de referencia rápida para HTTPS Everywhere

Como proveedor principal de certificados SSL, DigiCert lo ayudará a descubrir los beneficios de usar HTTPS en todo el sitio, y a desplegar el protocolo de manera correcta.

https:// ¿Qué es HTTPS Everywhere?

HTTPS Everywhere es la mejor medida de seguridad para sitios web que aseguran que toda la experiencia del usuario es segura de las amenazas en Internet. El término simplemente hace referencia a usar HTTPS, el protocolo web seguro habilitado por SSL/TLS, en todo el sitio web en vez de manera selectiva.

HTTPS ofrece autenticación de la identidad, la conexión y la integridad de los datos del sitio web, y cifra toda la información compartida entre el sitio web y un usuario (incluso cualquier cookie intercambiada) para protegerla de la visualización no autorizada, la manipulación y el uso indebido. Mantener una conexión segura durante toda la sesión de navegación es clave para asegurar que los usuarios estén a salvo de spoofing, inyección y ataques de interposición "Man-in-the-middle" de avanzada.

Navegadores y la presión por HTTPS

Ya no se permite asegurar solo una parte de las conexiones de los usuarios. Cuando se usa el protocolo HTTPS de manera intermitente en el sitio web, solo algunas páginas están protegidas por el cifrado y la autenticación de SSL, por lo tanto, otras páginas quedan vulnerables al robo de datos, la inyección/modificación de contenido y la invasión a la privacidad de la vigilancia a través de Internet.

El despliegue intermitente de SSL no cumple con las expectativas y derechos de seguridad de los usuarios ni cumple las expectativas de los navegadores y plataformas de sistema operativo. Desde hace muchos años, se fomenta la adopción de HTTPS, por este motivo, los principales proveedores de navegadores, como Google, Mozilla y Apple, han modificado lentamente la interfaz de usuario de sus navegadores para calificar al protocolo HTTP de manera negativa y calificar al HTTPS seguro de manera positiva.

Por qué debería preocuparme

La confianza es la base de la economía en Internet. Para ganar esa confianza, se necesita una seguridad de extremo a extremo para ayudar a proteger cada página web que visitan los usuarios, no solo las páginas de inicio de sesión y carritos de compra. Los nuevos cambios en los estándares de Internet y los navegadores web también están fomentando el uso de HTTPS y están penalizando activamente a los sitios no seguros que permanecen con el protocolo HTTP.

Por ejemplo, Google brinda a las páginas con HTTPS un mejor posicionamiento en los resultados de búsqueda desde 2014. Además, también se muestra una etiqueta de "Seguro" en la barra de direcciones de las páginas HTTPS. A partir de julio de 2018, Google

Chrome comenzará a mostrar una advertencia de "No seguro" en cada páginas con HTTP. Chrome **fue** el primer navegador principal que **advirtió** a los usuarios de todas las páginas HTTP y los demás navegadores seguirán esta tendencia, ya que Internet se dirige hacia un estándar "Seguro de manera predeterminada".

Además, muchas tecnologías web nuevas y características de los navegadores requieren el uso del protocolo HTTPS. Esto incluye a HTTP/2, una mejora básica del protocolo de comunicación web que puede mejorar significativamente el rendimiento del sitio web, así como características de los navegadores, entre ellas geolocalización, notificaciones, trabajo de servicio, estándar móvil AMP de Google, nuevos métodos de compresión, entre otros. En pocas palabras, sin el protocolo HTTPS, su sitio web quedará, en realidad, atrapado en el pasado.

3 Las tres recomendaciones principales para pasar a HTTPS Everywhere

1. Asegúrese de que cualquier servicio de terceros en el que confía, como servicios de publicidad o análisis que corren en su sitio, estén disponibles en HTTPS para evitar problemas de "contenido mixto".
2. Adquiera certificados SSL adicionales si diferentes partes de su sitio web se ejecutan en servidores o dominios diferentes.
3. Redirija todas las páginas web a las nuevas páginas HTTPS y actualice su herramienta Google Webmaster. La adopción de HTTPS Everywhere influye en el SEO. Google y otros motores de búsqueda consideran a esto un movimiento del sitio web, similar a adoptar un nuevo nombre de dominio.

digicert®

Conclusión

- El despliegue de HTTPS Everywhere en su sitio web asegura los datos del usuario y de su organización en cada página desde el comienzo al final.
- El uso intermitente del cifrado de SSL ya no es suficiente para proteger los visitantes del sitio web o proteger contra los datos comprometidos.
- La UI del navegador comenzará a mostrar indicadores negativos "No seguro" para página HTTP y esta tendencia solo continuará a medida que aumente las expectativas de seguridad.
- Impulse el posicionamiento SEO en Google con HTTPS Everywhere, un incentivo que posiblemente aumente en el futuro.
- HTTPS Everywhere es fácil de desplegar en su sitio web y no requiere hardware adicional.
- Asegure su sitio con certificados SSL que fortalecen su marca y reputación al demostrar su compromiso con la seguridad en Internet.
- Una mayor confianza del usuario permite menor tasas de rebote y abandono del carrito de compras. Los beneficios son mayor cantidad de transacciones en Internet y tasas de conversión.