

PROTOCOLO HTTPS.

¿Qué es y para qué sirve?



22 JUNIO

Barrientos&Asociados

Creado por: Fernando Barrientos

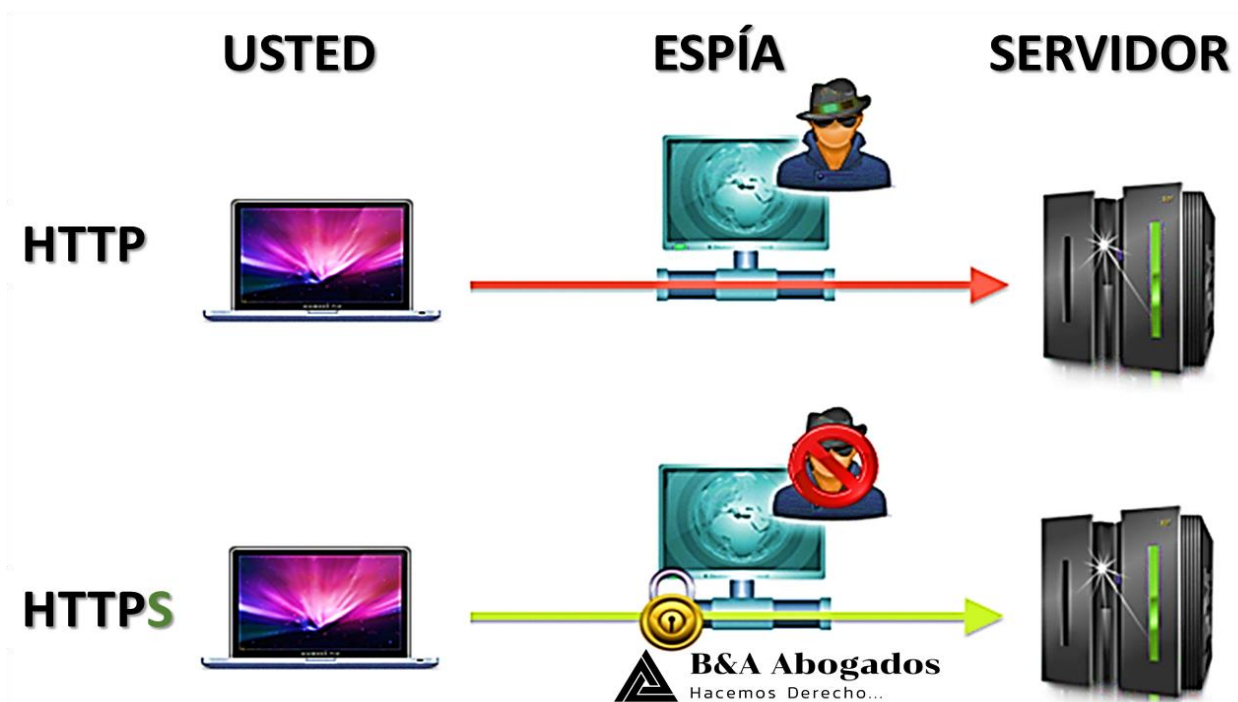


Qué es el Protocolo HTTPS y para que sirve cuando entramos a internet?

Veamos de que se trata

HTTP es el acrónimo de Hypertext Transfer Protocol (en español protocolo de transferencia de hiper texto). HTTPS es igual pero añadiéndole "Seguro". Estos dos protocolos se usan para lo mismo, la transferencia de datos.

La diferencia básica entre ambos es la forma en la que viajan los datos. Si los datos son transferidos mediante HTTP, estos viajan en claro y son accesibles para cualquiera que intercepte la comunicación. En cambio, el protocolo HTTPS usa una conexión segura mediante un cifrado SSL y por tanto los datos viajan de un modo seguro de un lugar a otro.



A mayor abundamiento, el asunto SSL funciona así:

- El navegador intenta conectarse a un sitio protegido con SSL
- El navegador solicita que el servidor web se identifique.
- El servidor envía una copia de su certificado SSL al navegador.
- El navegador comprueba si el certificado SSL es de confianza. Si es así, envía un mensaje al servidor.
- El servidor devuelve un acuse de recibo firmado digitalmente para comenzar una sesión SSL cifrada.
- Los datos cifrados se comparten entre el navegador y el servidor.

¿Qué datos protege el protocolo SSL?

El conjunto de datos que están protegidos por el protocolo de encriptación SSL incluye:

- Información de registro: nombre, dirección, dirección de correo electrónico, número de teléfono
- Datos de identificación: dirección de correo electrónico y contraseña
- Datos de pago: número de tarjeta de crédito, cuenta bancaria
- Formularios de inscripción
- Documentos cargados por los clientes
- El certificado SSL garantiza que la comunicación no se podrá leer ni manipular y que la información personal no caerá en las manos equivocadas.

¿Por qué cambiar a HTTPS?

Google nos indica varias razones para hacer el cambio a HTTPS que casi todas las páginas serias viene utilizando, como es el caso de Facebook, Twitter, YouTube, etc. Etc. Las que si está interesado en conocer puede consultar en la red la guía que tienen sobre la migración: Los datos enviados usando HTTPS están asegurados por el protocolo TLS (Transport Layer Security), que ofrece 3 capas de protección fundamentales:

Cifrado. El cifrado de los datos intercambiados los mantiene seguros de miradas indiscretas. Eso significa que mientras el usuario está navegando en un sitio web, nadie puede "escuchar" a sus conversaciones, realizar un seguimiento de sus actividades a través de múltiples páginas o robar su información.

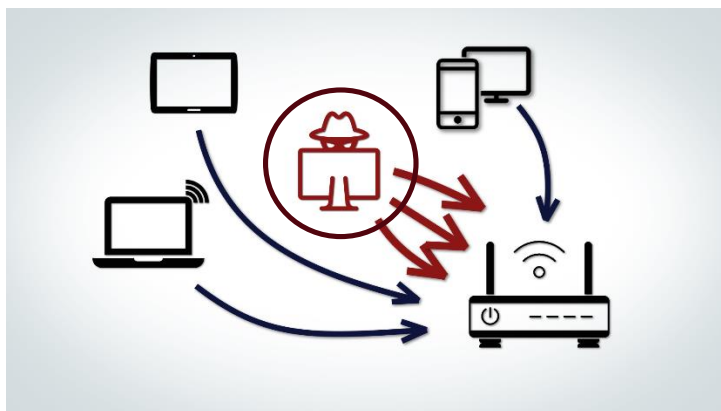
Integridad de los datos. Los datos no pueden ser modificados o dañados durante la transferencia, intencionadamente o no, sin ser detectado.

Autenticación. Demuestra que los usuarios se comunican con la página web deseada. Protege contra los ataques y construye la confianza del usuario, lo que se traduce en más beneficios para el negocio.



LA DIFERENCIA ES CLARA

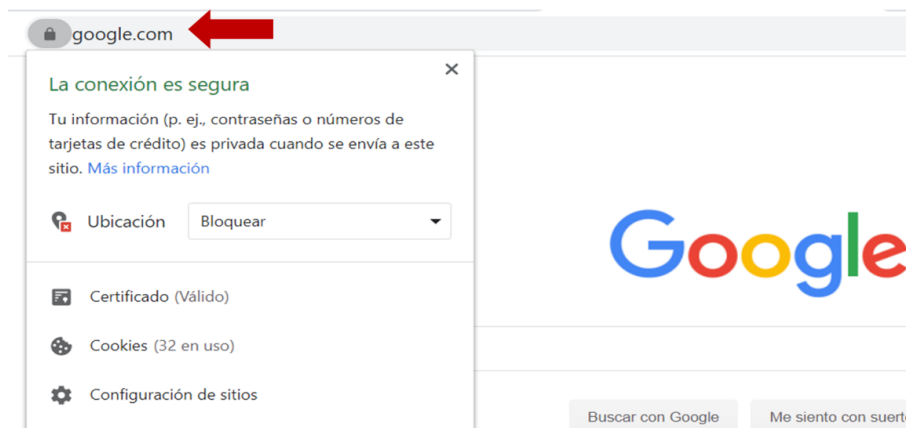
Un código abierto o navegación abierta puede generar que personas indeseadas estén espionando y puedan robar sus datos. (caso enlaces por WiFi)



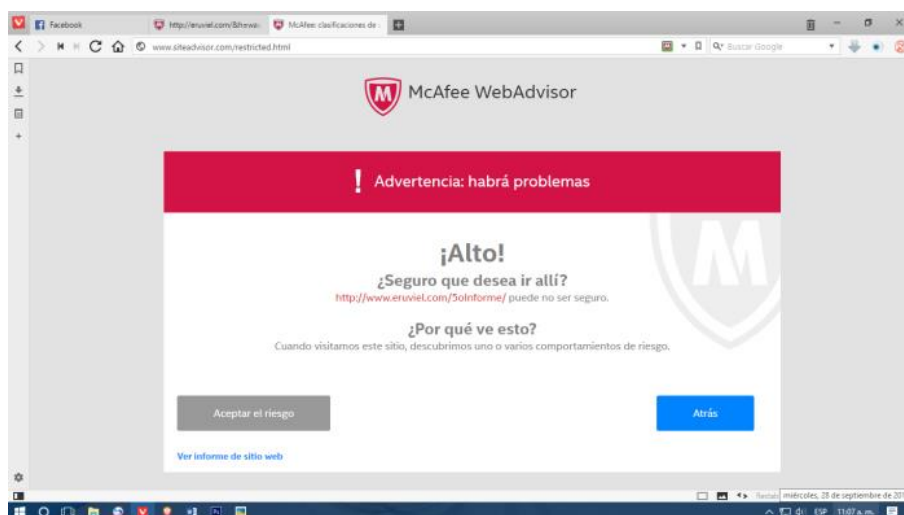
Para realizar este cifrado, cada conexión con HTTP se envía sobre una capa SSL o TLS. El objetivo de usar HTTPS responde a dos cuestiones: en primer lugar certificar que la web visitada es legítima, y en segundo lugar que se mantiene la integridad y la privacidad de los datos de conexión. Al tener cubiertos estos dos aspectos, se obtiene protección contra ataques man-in-the-middle.

Adicionalmente, ofrece cifrado en dos direcciones para las comunicaciones entre servidores y clientes, lo que protege contra el espionaje y la manipulación de los contenidos de la comunicación. En la práctica, sirve como una garantía razonable de que nos estamos

comunicando con la web que queremos y no con un impostor, lo que también protege contra ataques por phishing, como el que se produjo en el Comité Demócrata Nacional antes de las últimas elecciones presidenciales de EE.UU.



Muchas veces, si cuenta con un buen antivirus, puede bloquearse automáticamente el ingreso a un sitio en internet.



Sin embargo no es garantía y no siempre eso funciona así.

Históricamente las conexiones HTTPS se han usado, fundamentalmente, para transacciones económicas, correo electrónico y dotar de mayor seguridad a los sistemas de comunicación corporativos. A finales de la década de 2000 y a principios de la década de 2010, su uso empezó a generalizarse para proteger todo tipo de sitios web.

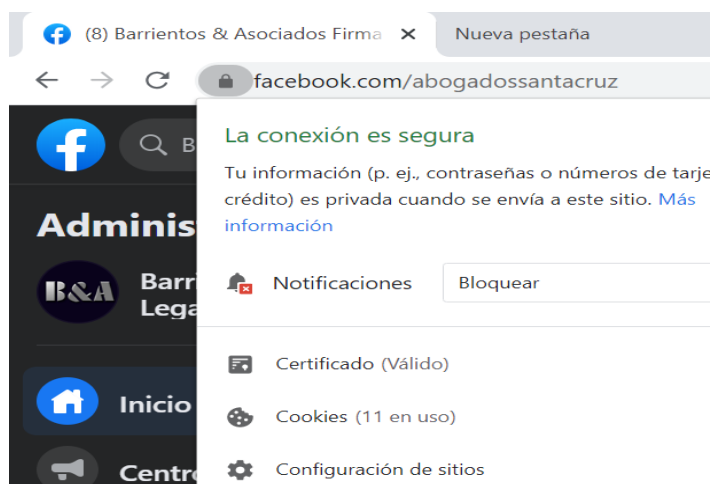
El uso de HTTPS evita el espionaje por parte de intrusos. Los intrusos incluyen desde actores maliciosos, a empresas legítimas pero que se consideran invasivas. En esta última categoría entrarían, por ejemplo, los proveedores de servicios de Internet o ISPs.

Los intrusos explotan las comunicaciones no protegidas para engañar a los usuarios, de forma que ofrezcan información sensible o instalen malware, así como para insertar publicidad no deseada o no legítima en los recursos del usuario. Desde Google se pone el ejemplo de terceras partes que insertan publicidad en webs que pueden arruinar la experiencia de uso y crear vulnerabilidades en la seguridad del usuario.

Los intrusos también pueden explotar cada recurso no protegido que se mueva entre las webs y los usuarios. Estos recursos pueden ser imágenes, cookies, script, código HTML y etcétera. Las intrusiones se pueden producir en cualquier punto de la red: una máquina doméstica, un punto de acceso WiFi o un ISP comprometido, por ejemplo; una idea falsa, pero extendida, es que HTTPS sólo es necesario en webs que manejan comunicaciones e información sensibles. Cada petición HTTP no cifrada puede revelar información sobre los comportamientos y las identidades de los usuarios.

Conclusión

Navegue por sitios seguros y, antes de ingresar al contenido de una página diríjase a la barra de navegación que queda en la parte superior de su computadora y haciendo clic verifique si la conexión es segura.



Hasta la próxima.