¿Qué es HTTPS?

El protocolo de transferencia de hipertexto seguro (HTTPS) es la versión segura de HTTP, que es el principal protocolo utilizado para enviar datos entre un navegador web y un sitio web. El HTTPS está encriptado para aumentar la seguridad de las transferencias de datos. Esto es especialmente importante cuando los usuarios transmiten datos confidenciales, como al iniciar sesión en una cuenta bancaria, un servicio de correo electrónico o un proveedor de seguros médicos.

Cualquier sitio web, especialmente los que requieren credenciales de inicio de sesión, debe utilizar HTTPS. En los navegadores modernos, como Chrome, los sitios web que no utilizan HTTPS se señalan de forma diferente a los que sí lo hacen. Identifica un candado en la barra de URL que te indicará que la página web es segura. Los navegadores web se toman en serio el protocolo HTTPS.

¿Cómo funciona HTTPS?

HTTPS utiliza un protocolo de encriptación para encriptar las comunicaciones. El protocolo se conoce como Transport Layer Security (TLS), aunque antes se conocía como Secure Sockets Layer (SSL). Este protocolo asegura las comunicaciones mediante el uso de lo que se conoce como infraestructura de clave pública asimétrica. Este tipo de sistema de seguridad utiliza dos claves diferentes para encriptar las comunicaciones entre dos partes:

1. La clave privada: esta clave la controla el propietario de un sitio web y se mantiene, como el lector ya habrá supuesto, privada. Esta clave está ubicada en un servidor web y se utiliza para desencriptar la información encriptada por la clave pública.

2. La clave pública: esta clave está disponible para todos los que quieran interactuar con el servidor de forma segura. La información encriptada por la clave pública solo puede ser desencriptada por la clave privada.

¿Por qué es importante HTTPS? ¿Qué ocurre si un sitio web no tiene HTTPS?

HTTPS evita que los sitios web difundan su información de forma que sea fácilmente visible para cualquiera que esté cotilleando por la red. Cuando la información se envía por un HTTP normal, la información se divide en paquetes de datos que se pueden "cotillear" fácilmente con el uso de software libre. Esto hace que la comunicación a través de un medio inseguro, como el Wi-Fi público, sea muy vulnerable a la interceptación. De hecho, todas las comunicaciones que se producen oir HTTP ocurren en texto plano, lo cual las hace muy accesibles a cualquiera con las herramientas adecuadas, y vulnerables a los ataques en ruta.

Con HTTPS, el tráfico se encripta de tal manera que, aunque alguien cotillee los paquetes sean o los intercepte de alguna manera, aparecerán como caracteres sin sentido. Veamos un ejemplo:

Antes de la encriptación:

```
Es una cadena de texto completamente legible
```

Después de la encriptación:

```
ITM0IRyiEhVpa6VnKyExMiEgNveroyWBPlgGyfkflYjDaaFf/Kn3bo3OfghBPDWo6Af
SHlNtL8N7ITEwIXc1gU5X73xMsJormzzXlwOyrCs+9XCPk63Y+z0=
```

En los sitios web sin HTTPS, es posible que los proveedores de servicios de Internet (ISP) u otros intermediarios inyecten contenido en las páginas web sin que lo apruebe el propietario del sitio web. Esto suele ocurrir en forma de publicidad, cuando un ISP que busca aumentar sus ingresos inyecta publicidad de pago en las páginas web de sus clientes. Como es lógico, cuando se produce esto, los beneficios de los anuncios y el control de calidad de los mismos no se

comparten con el propietario del sitio web. HTTPS elimina la posibilidad de que terceros sin permiso inyecten publicidad en el contenido web.

¿Qué puerto utiliza HTTPS?

HTTPS utiliza el puerto 443. Esto distingue HTTPS de HTTP, que utiliza el puerto 80.

(En redes, un puerto es un punto virtual basado en software donde empiezan y terminan las conexiones de red. Todos los ordenadores conectados a la red exponen una serie de puertos para que puedan recibir tráfico. Cada puerto está asociado a un proceso o servicio específico y los diferentes protocolos utilizan puertos diferentes).

¿De qué otra forma se diferencia HTTPS de HTTP?

En términos técnicos, HTTPS no es un protocolo distinto de HTTP. Simplemente utiliza la encriptación TLS/SSL sobre el protocolo HTTP. HTTPS se basa en la transmisión de los certificados TLS/SSL, que verifican que un determinado proveedor es quien dice ser.

Cuando un usuario se conecta a una página web, esta le envía su certificado SSL, que contiene la clave pública necesaria para iniciar la sesión segura. Luego, los dos ordenadores, el cliente y el servidor, pasan por un proceso llamado protocolo de enlace SSL/TLS, que es una serie de comunicaciones de ida y vuelta utilizadas para establecer una conexión segura.

¿Cómo comienza un sitio web a utilizar HTTPS?

Muchos proveedores de alojamiento de sitios web y otros servicios ofrecen certificados TLS/SSL de pago. Estos certificados suelen compartirse entre muchos clientes. Hay certificados más caros que pueden registrarse individualmente para determinadas propiedades web.

Todos los sitios web que usa Cloudflare reciben HTTPS de forma gratuita y utilizan un certificado compartido (el término técnico para esto es un certificado SSL de dominio múltiple). Configurar una cuenta gratuita garantizará que una propiedad web reciba protección HTTPS que se actualiza constantemente. También puedes explorar nuestros planes de pago para obtener certificados individuales y otras funciones. En cualquier caso, una propiedad web recibe todas las ventajas de utilizar HTTPS.