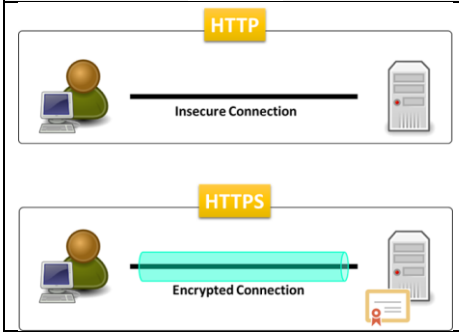
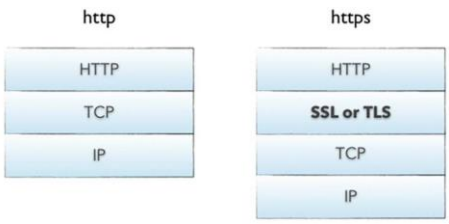
ENVIAR DATOS A TRAVÉS DE LA INTERNET

HTTP de HyperText Transfer Protocol (Protocolo de transferencia de hipertexto) es el método más común de intercambio de información en la world wide web (Internet), el método mediante el cual se transfieren las páginas web desde un servidor a un ordenador, PC, Tablet o Smartphone.

El Protocolo seguro de transferencia de hipertexto (en inglés: Hypertext Transport Protocol Secure o **HTTPS**), es un protocolo de aplicación basado en el protocolo **HTTP**, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de **HTTP**.

Para preparar un servidor web que acepte conexiones HTTPS, el administrador del servidor web, debe crear un certificado de clave pública para dicho servidor web. Este certificado debe estar firmado por una autoridad de certificación para que el navegador web lo acepte. La autoridad certifica que el titular del certificado es quien dice ser. Los navegadores web generalmente son distribuidos con los certificados raíz firmados por la mayoría de las autoridades de certificación por lo que estos pueden verificar certificados firmados por ello.

Usuario		Plataforma Tecnológica
	El Usuario mayormente no percibe la diferencia. Los administradores de tecnología sacrifican velocidad por seguridad	

Concepto	HTTP	HTTPS	Detalle
La URL empieza con	"http://"	"https://"	URL: Dirección web descriptiva para acceder a un servidor
Conexión segura	NO	SI	La información es transmitida de manera no interpretable
Envía los datos a través del puerto	80	443	Puertas estándares de envió de datos electrónicos.
Validación de dominio	NO	SI	Siempre se comprueba que el nombre de dominio exista.
Capa de transmisión	A nivel de aplicación	A nivel de transporte	Si depende del software desarrollado o del medio de transmisión
Usa encriptación	NO	SI	Los datos son transmitidos con cierta codificación no interpretable
Requiere certificados SSL	NO	SI	Constancia de disponer de un certificado adquirido y que valide la ubicación del servidor.
Velocidad transmisión	Rápido	Menos rápido	Se transmite mayor cantidad de bytes

Que tan seguro son el HTTP y HTTPS

Fuente: https://www.kaspersky.es/blog/https-does-not-mean-safe/15135/ visto el: 17 Ene 2018

Cuando en nuestro navegador web, vemos un candado verde acompañado de las palabras "Es seguro" a la izquierda del URL, inmediatamente pensamos que se trata de un sitio web seguro.

Pero, estos símbolos de seguridad no garantizan que una página web esté protegida de todas las amenazas. Un sitio de *phishing*, por ejemplo, puede mostrar ese candado tranquilizador al lado de su dirección https. Entonces, ¿qué sucede?

Una conexión segura no equivale a un sitio seguro

El candado verde significa que el sitio ha emitido un certificado y que, a raíz de ello, se han generado una pareja de claves cifradas. Estos sitios cifran la información transmitida entre el sitio y tú. En este caso, el URL de la página empieza por HTTPS, la última "s" es de "seguro".

Por supuesto, cifrar los datos que se transmiten es algo bueno, ya que la información que se intercambia entre el navegador y el sitio no es accesible a terceros, como el proveedor de servicios, el administrador de red, los intrusos, etc. Esto te permite introducir tus contraseñas y los datos de tu tarjeta de crédito sin que haya fisgones de por medio.

Pero el problema es que el candado verde y el certificado emitido no dicen nada del sitio en concreto. Por lo que una página *phishing* puede conseguir un certificado sin problemas y cifrar todo el tráfico que se genera entre la página y tú. En otras palabras, todos los candados verdes aseguran que nadie *más* puede espiar los datos que introduces. Pero tu contraseña aún puede robarse desde el mismo sitio, si este es falso.

Los estafadores hacen mucho uso de esto. Según Phishlabs, un cuarto de todos los ataques *phishing* de hoy en día se realizan en sitios HTTPS, hace dos años era menos del 1 %. Además, más del 80 % de los usuarios creen que la simple presencia de un candado verde y las palabras "Es seguro" junto a la URL significan que un sitio es seguro y, por lo tanto, no se lo piensan dos veces a la hora de introducir sus datos.

¿Y si el candado no es verde?

Si la barra de direcciones no muestra ningún candado, significa que la página web no cifra los datos, por lo que intercambia información con tu navegador mediante el estándar HTTP. Google Chrome ya ha empezado a categorizar estos sitios web como inseguros. Lo cierto es que el sitio puede llegar a ser seguro, pero no cifra el tráfico entre el servidor y tú. La mayoría de los sitios web no quieren que Google los etiquete como inseguros, así que cada vez son más los que migran a HTTPS. En cualquier caso, introducir datos sensibles en un sitio HTTP en una mala idea, cualquiera podría espiarte.

La segunda opción que puedes encontrar es el icono de un candado tachado con líneas rojas y las letras HTTPS marcadas en rojo. Esto significa que el sitio web tiene un certificado, pero no está verificado o ha vencido. Es decir, que la conexión entre el servidor y tú está cifrada, pero nadie puede garantizar que el dominio pertenezca a la compañía que se indica en el sitio. Esta situación es la más sospechosa, ya que normalmente estos certificados solo se usan a modo de prueba.

Por otro lado, si el certificado ha expirado y el propietario no ha podido renovarlo, los navegadores etiquetarán la página como insegura, pero de forma más visible, con un candado rojo de advertencia. En ese caso, considéralo un peligro real, evita estos sitios y, por supuesto, nunca introduzcas datos personales en ellos.

Cómo no picar el anzuelo

En resumen, la presencia de un certificado y el candado verde solo significa que los datos que se trasmiten entre el sitio y tú están cifrados y que el certificado ha sido expedido por una autoridad de certificados de confianza. Pero no avisa de si un sitio HTTPS es malicioso, algo que manipulan los estafadores de *phishing* con gran destreza.

Por ello debes estar siempre alerta, sin importarte lo seguro que pueda parecer un sitio a simple vista.

- No introduzcas nunca nombres de usuarios, contraseñas, credenciales bancarias, o cualquier otra información personal en el sitio a no ser que estás totalmente seguro de su autenticidad. Para ello, comprueba siempre el nombre del dominio con mucha atención, ya que el nombre de un sitio falso puede diferenciarse solo por un carácter. Y asegúrate de que los enlaces son fiables antes de hacer clic en ellos.
- Ten siempre en cuenta lo que ofrece un sitio, si parece sospechosos y si de verdad es necesario que te registres en él.
- Asegúrate de que tus dispositivos están bien protegidos: Kaspersky Internet Security comprueba si las URL se encuentran en una extensa base de datos de sitios *phishing* y detecta estafas sin tener en cuenta lo "seguro" que puede parecer el sitio.

SOLUCIONES TEC

Gestiona servidores web seguros, y monitoriza permanentemente que nuestros Software desarrollado cumpla los estándares de seguridad exigidos por las normativas nacionales, tales como la NTP-ISO/IEC 17799: Norma Técnica Peruana - PMG SSI y las buenas prácticas internacionales.