¿Como se utiliza y para que es https:?

Al realizar negocios con sus clientes en línea, es posible que necesite solicitar su información personal, por ejemplo, si se inscriben en su boletín informativo o realizan un pedido. Para proteger la información de sus clientes, existe una tecnología llamada "SSL" (capa de conexión segura) que encripta los datos que se transmiten entre un navegador web y un servidor web. Las direcciones web protegidas con SSL empiezan con https: en lugar de http:. Por lo tanto, algunas personas se refieren a SSL como "HTTPS". Al recopilar información personal y financiera determinada, requiere el uso de conexiones con SSL en su página web.

Beneficios de SSL

Usar SSL brinda más privacidad y seguridad que una conexión web sin encriptación. Disminuye el riesgo de que terceros intercepten y usen indebidamente la información. Muchos visitantes de sitios se sienten más cómodos al realizar pagos y compartir información personal cuando saben que están usando una conexión con SSL.

Verificar SSL en páginas web

La mayoría de los navegadores web muestran un ícono de candado cuando se establece una conexión con SSL.

La manera más directa de verificar la tecnología SSL es ingresar la dirección web en el navegador con https:// al comienzo, por ejemplo, https://dominio.com. Si ve un ícono de candado en el navegador, haga clic en él para obtener más información que confirme que es una conexión segura. Si no ve el ícono de candado, significa que la página no está protegida con SSL.

Tenga en cuenta que muchos sitios web solo usan SSL en algunas páginas donde se transmite información confidencial, como contraseñas o números de tarjetas de crédito.

Configurar SSL en su sitio web

Si no tiene SSL y desea implementarla en una o más páginas de su sitio web, estos son los pasos principales que debe realizar:

Obtenga una IP dedicada: Si no tienes una dirección IP dedicada(Protocolo de internet), tu cuenta de hosting comparte la dirección IP de servidor con otras cuentas de hosting. En la mayoría de casos, eso está bien. Pero, es posible que necesites una dirección única que la IP dedicada, también conocida como IP estática, proporciona si tienes un sitio web de hosting dedicado con cifrado SSL o tráfico pesado.

Existen muchas razones para necesitar una dirección IP dedicada. Por ejemplo:

- **Acceso directo:** con una dirección IP única, puedes ver tu sitio web con una dirección IP de hosting o puedes tener acceso directo a los archivos de tu sitio web con FTP o un navegador web.
- **Actualización de DNS:** cuando actualizas el DNS de nombre de dominio, tu sitio se hace inaccesible durante 24 a 48 horas. Esto puede causar problemas importantes para ti si

necesitas FTP o tener una vista previa de algún cambio. Con una dirección única (IP dedicada), puedes cargar contenido y tener una vista previa de tu sitio web sin problemas!. Todo lo que necesitas es escribir tu dirección IP dedicada en tu navegador y tu sitio se mostrará.

- **Certificados SSL:** los certificados SSL requieren una dirección IP dedicada. Un sitio web que solicita información personal o de pago debe tener protección SSL, pero SSL requiere una IP estática (IP dedicada) para funcionar. Con una IP dedicada, puedes configurar SSL que redirija a tus visitantes por medio de una conexión de hosting cifrada.

Las direcciones de IP dedicadas son muy exclusivas y seguras, mientras que las direcciones IP compartidas no lo son. La mayoría de los nombres de dominio comparten sus direcciones IP con cientos de nombres de dominios. Por lo tanto, si un nombre de dominio causa problemas, todos los nombres de dominio pueden afectarse.

Algunos motores de búsqueda o los ISP sancionarán una dirección IP si uno de sus nombres de dominio envía correos electrónicos no solicitados. Con una IP dedicada, puedes evitar las desventajas de compartir tu dirección IP con otros usuarios.

Los expertos en línea creen que una dirección IP estática o una IP dedicada pueden mejorar el posicionamiento en los resultados de un motor de búsqueda. A los motores de búsqueda les gustan las direcciones únicas porque el nombre de tu dominio no está asociado con otros nombres de dominios.

Si usted requiere una IP dedicada, comuníquese con nosotros por medio de un correo a informes@irivinsu.com o soporte@irivinsu.com

Obtenga un certificado SSL para su sitio web. Un certificado SSL es un documento electrónico que verifica la identidad de su empresa y permite que un servidor web establezca una encriptación segura con el navegador web de un visitante.

Si requiere información del costo de un certificado SSL esctibanos a informes@irivinsu.com o soporte@irivinsu.com

Instale el certificado SSL en su servidor web. El método de instalación varía según el servidor web y el tipo de certificado adquirido. Normalmente, IRIVINSU hace esta instalación, pero si usted quiere hacerla indiquenoslo.

Identifique las páginas de su sitio web que desea asegurar con SSL. Los sitios web más seguros usan SSL en todo el sitio. Sin embargo, solo requiere que use conexiones seguras en páginas que recopilen o transmitan información personal y financiera determinada, como contraseñas personales de acceso, información de contacto o números de cuentas bancarias.

Modifique los vínculos a las páginas (y los elementos de las páginas) que quiere que se carguen de forma segura. En el caso de las páginas que quiere que se carguen de forma segura, cambie los

vínculos a esas páginas para que al principio incluyan https:// en vez de http://. Por ejemplo, si desea cambiar http://dominio.com/login.htm?hl=es-419 para que sea una página segura, debe modificar todos los vínculos a esa página en su sitio web a https:// dominio.com /login.htm?hl=es-419. También le recomendamos que configure los redireccionamientos del servidor para que dirijan automáticamente a las personas que intentan visitar una URL insegura, como http://dominio.com/login.htm?hl=es-419 , a una conexión segura, como https://dominio.com/login.htm?hl=es-419.

Realice una prueba para verificar que las páginas sean seguras. Visite todas las nuevas páginas seguras mediante, al menos, dos navegadores modernos diferentes que los visitantes típicos de su sitio podrían usar. Si ve un ícono de candado en el navegador, haga clic en él para obtener más información que confirme que sus conexiones son seguras. El error más común es tener "contenido combinado" en una página https:. Esto quiere decir que uno o más elementos (generalmente imágenes, archivos flash o archivos CSS) se cargan en una página https: con una URL http:// que no es segura. Los navegadores más modernos indican los recursos inseguros en páginas de contenido combinado en su consola de JavaScript (en algunos navegadores, se puede llamar "depurador de Javascript"). Para solucionar estos problemas, examine el código HTML de la página y realice lo siguiente:

- Busque http://.
- Reemplace todas las instancias que encuentre por //.
- Guarde los cambios en el servidor web y vuelva a realizar una prueba.
- Si, de todos modos, obtiene advertencias de contenido combinado en la página, es muy probable que se deba a problemas con su código de Javascript o flash.

Carateristicas de certificado SSL

- Conserva privados los pagos y datos del cliente
- Asegura su sitio rápidamente
- Admite el sólido cifrado SHA-2 y de 2048 bits
- Compatible con todos los navegadores más importantes
- Aumenta el posicionamiento en las búsquedas. Google brinda un posicionamiento más alto a los sitios asegurados con SSL.