

Navega más seguro con el protocolo HTTPS



Seguramente habrás visto miles de veces en la barra de direcciones de vuestro navegador la palabra "http" justo al inicio de la dirección web que estáis visitando. Eso es un protocolo de transferencia de hipertexto, pero con la proliferación de servicios y páginas con acceso mediante contraseña, **HTTP se ha quedado anticuado y es potencialmente inseguro.**

Es por eso que hay que estar muy alerta del protocolo y, en sitios donde puedes ser víctima del robo de datos personales, controlar que la dirección que estamos visitando empieza por **"https://", un protocolo que cifra la**

transferencia de datos de forma mucho más segura.

Conoce cómo activar este protocolo en las principales páginas web y los pasos que tienes que seguir para que tu estancia en la red sea mucho más segura. ¡Allá vamos!

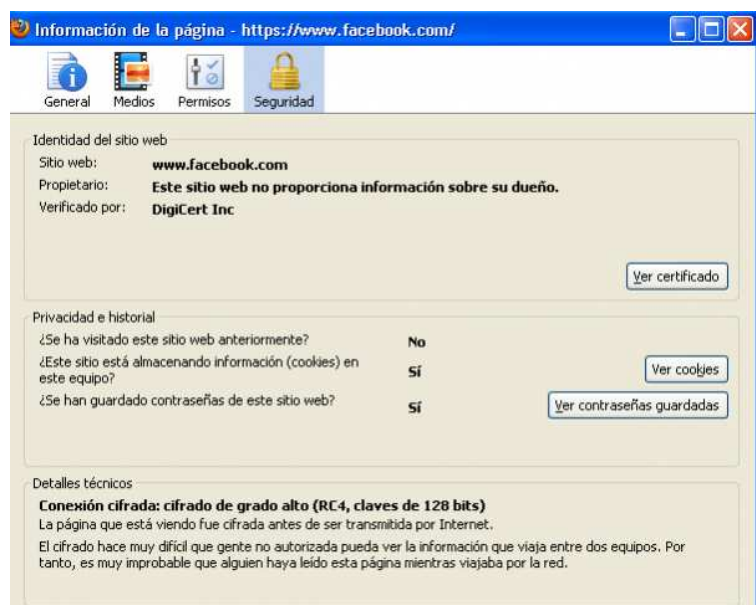
Los inicios de sesión

A continuación te explicaremos cómo configurar tus principales cuentas para habilitar el cifrado de HTTPS, pero primero de todo, un consejo fundamental: **las páginas de registro y de inicio de sesión son el principal foco de peligro**, y por defecto, cargarán con el protocolo HTTP. Prueba de añadir una "s" al final, manualmente. Tan simple como esto. Si quieres estar tranquilo, accede a tus datos personales sólo desde páginas HTTPS:



Los sitios confirman que son seguros con información verificada, que puedes revisar pinchando en el botón que aparecerá en tu barra de navegación.

Si no pueden ser verificados y, por tanto, son inseguros, nuestro navegador nos advertirá con un mensaje de este estilo:





Esta conexión no está verificada

Ha pedido a Firefox que se conecte de forma segura a **es.linkedin.com**, pero no se puede confirmar que la conexión sea segura.

Normalmente, cuando se intente conectar de forma segura, los sitios presentan información verificada para asegurar que está en el sitio correcto. Sin embargo, la identidad de este sitio no puede ser verificada.

¿Qué debería hacer?

Si normalmente accede a este sitio sin problemas, este error puede estar ocurriendo porque alguien está intentando suplantar al sitio, y no debería continuar.

[¡Sácame de aquí!](#)

- ▶ Detalles técnicos
- ▶ Entiendo los riesgos

Tenlo en cuenta especialmente en sitios en los que debemos introducir datos personales privados, como páginas de compra electrónica, tal y como lo explicamos en [nuestro artículo sobre estafas en la red](#).

Cómo activar HTTPS en Facebook

Sin duda, las redes sociales como Facebook son páginas potencialmente peligrosas para ti y tus preciados datos. Entra en Facebook y, en la parte superior derecha de la página principal, haz clic en **Configuración de la cuenta**. Una vez dentro, en la parte inferior de la página encontrarás **Seguridad de la cuenta**. Activa la casilla de **Navegación segura** y dale a **Guardar**.

Normalmente, al hacer un cambio de este estilo, la página desactivará la sesión y deberás volver a acceder con tus datos personales, ahora sí, con más seguridad.

Seguridad de la cuenta 1 Ocultar

Controla la seguridad de navegación y de inicio de sesión

Navegación segura (https)

☒ Usar Facebook mediante una conexión segura (https) cuando sea posible 2

Notificaciones de inicio de sesión

Cuando una computadora o dispositivo desconocido intente acceder a mi cuenta:

☒ Enviarme un mensaje de correo electrónico

Aprobación de inicio de sesión [?]

Cuando una computadora o dispositivo desconocido intente acceder a mi cuenta:

☐ Pedirme que escriba el código de seguridad enviado a mi celular

Guardar 3

Tus dispositivos reconocidos:

Nombre del dispositivo	Hora en que se guardó el nombre	
Softonic PC	Hoy a las 9:39	Eliminar
sem pc	El Martes a las 0:48	Eliminar
Softonic PC	miércoles, 29 de junio de 2011 a las 11:40	Eliminar
Softonic PC	Martes, 21 de junio de 2011 a las 10:36	Eliminar
Softonic PC	Lunes, 20 de junio de 2011 a las 13:45	Eliminar
Sem Pc	Domingo, 19 de junio de 2011 a las 15:57	Eliminar
Softonic PC	Martes, 14 de junio de 2011 a las 11:40	Eliminar
PC de casa	Sábado, 11 de junio de 2011 a las 17:43	Eliminar
Mi Android	Viernes, 10 de junio de 2011 a las 14:41	Eliminar

Si no sucediera, **sal de la sesión y vuelve a entrar**. Si en la pantalla anterior has activado también la opción **Notificaciones de inicio de sesión**, Facebook te pedirá que **identifiques los dispositivos** con los que entres en la red.

Dale un nombre a este equipo

Elige un nombre para este ordenador. Como has activado las notificaciones de inicio de sesión, recibirás un mensaje para informarte de que has entrado en Facebook desde este equipo.

Nombre del ordenador:

☒ Añadir a la lista de dispositivos reconocidos

Continuar

Esto es una medida de seguridad implementada para evitar que ordenadores y dispositivos ajenos al nuestro accedan a nuestra red social. Esta petición te la hará cada vez que accedas desde un sitio nuevo, también desde el móvil.

Incluso si limpias las *cookies* o usas programas como CCleaner, Facebook dejará de reconocer tu ordenador como habitual y volverá a pedirte que lo identifiques. Recibirás un correo a tu cuenta asociada indicándote la entrada en Facebook. Lee bien los datos y **si recibes este *email* y no lo reconoces, haz clic en el enlace para denunciar una intrusión.**

Entrada en Facebook desde "El ordenador de Softonic" Volver a mensajes

Facebook Agregar a contactos
Para Sem Pons

Hola, Sem Pons:

Un dispositivo nuevo llamado "El ordenador de Softonic" inició sesión en tu cuenta de Facebook (jueves, 07 de julio de 2011 a las 8:25) desde Barcelona, B, ES (IP=89. ...). (Nota: esta ubicación se basa en información proporcionada por tu proveedor de internet o de telefonía móvil.)

Se agregó este dispositivo a tu cuenta.

Si se trataba de ti, puedes ignorar el resto de este mensaje.

Si esta entrada en tu cuenta no estaba autorizada, sigue este enlace para proteger la información de tu cuenta de Facebook:
http://www.facebook.com/roadblock/roadblock_me.php?u=6880...8544n=g5c6GJkT

Para informarte sobre cómo este tipo de notificaciones puede ayudarte a proteger la información de tu cuenta, visita el Servicio de ayuda: <http://www.facebook.com/help/?topic=loginnotifications>

Nota: Facebook nunca te pedirá los datos de acceso a tu cuenta por correo electrónico.

Gracias,
El equipo de Facebook

comprueba que los datos sean correctos

si no eres tú, haz clic aquí

En ocasiones, accedemos a páginas y grupos de Facebook que no tienen habilitado el contenido mediante conexión segura. Algunos ejemplos son los juegos basados en Flash o páginas de *fans* de grupos musicales con vídeos y canciones en *streaming*, una opción de Facebook que funciona solo con HTTP. Nos saldrá, eso sí, este mensaje para decidir qué hacemos.

¿Desactivar navegación segura?

No podemos mostrar este contenido mientras estás viendo Facebook mediante una conexión segura (https)

¿Quieres usar una conexión normal (http) de forma temporal para usar esta aplicación?

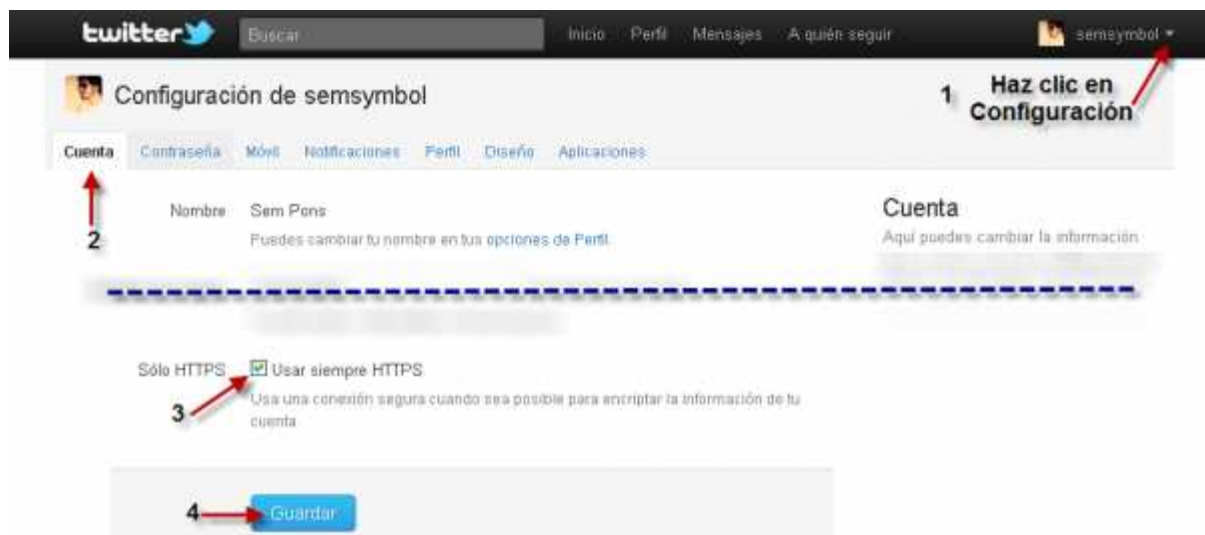
Cuando entres de nuevo en Facebook volverás a tener una conexión segura.

ContinuarCancelar

Twitter y otras redes sociales

Aparte de Facebook, nuestro día a día está dedicado a otras redes sociales. Por ejemplo, **Foursquare por defecto ya viene configurado en HTTPS**, incluso su página de registro y de inicio de sesión. En cambio, **otros sitios como LinkedIn no están aún verificados** como sitios seguros para la navegación.

Otro ejemplo de sitio recurrente es Twitter, así que refuerza su seguridad. Haz clic en la flecha superior derecha y en **Configuración**. Accede a **Cuenta** y baja hasta el final de la página, donde encontrarás la opción **Sólo HTTPS**. Marca la casilla y **guarda los cambios**. Ten en cuenta que esto afecta sólo a la página de Twitter, así que si accedes a tu cuenta desde otro cliente deberás revisar que sean sitios seguros, y ya te advertimos que la mayoría no lo son.



Tus cuentas de correo

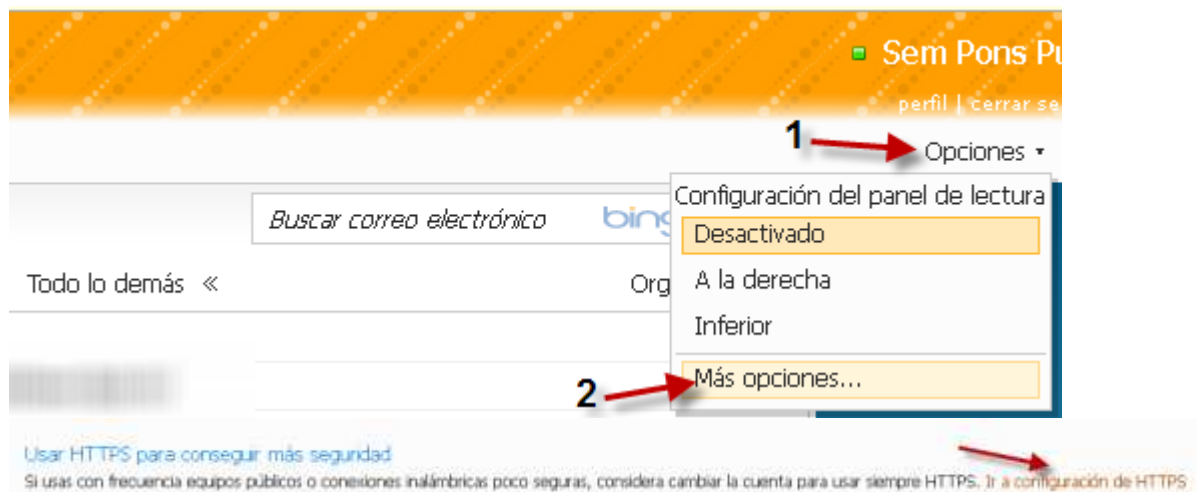
Otro pilar fundamental de nuestra relación con Internet son nuestras cuentas de correo. Aquí hay que extremar la precaución, por diversos motivos. Primero, porque **sitios como Gmail se han convertido en nuestra cuenta de muchos más servicios** como Blogs, Imágenes, Google+ o Docs. Hay muchos más datos que vigilar. Segundo, porque la inmensa mayoría de páginas web que requieren registro tienen la clásica opción de "He olvidado mi contraseña", y te la envían sin ningún tipo de pudor a tu cuenta de correo. **Si alguien tiene tus datos del correo, date por perdido.**

Empecemos por Gmail. Haz clic en el engranaje de la parte superior derecha o **Configuración**, según sea vuestro diseño. En el apartado **General**, en el que estaréis por defecto, hay una opción que debes marcar: **usar siempre https**. **Guarda los cambios, y comprueba que se han hecho efectivos** en la barra de direcciones.



Hotmail sigue en plena forma, con 15 años a sus espaldas y 300 millones de usuarios en todo el mundo. Cabe decir que **cuanto más popular sea un servicio, más goloso será para los ladrones y piratas**.

Tomar precauciones con Hotmail es más complicado, es una opción que cuesta un poco de encontrar. En la parte superior derecha, abajo de tu nombre, haz clic en **Opciones** y en el desplegable elige **Más Opciones**. En la página que aparecerá, en el apartado **Personalizar Hotmail** elige **Opciones avanzadas de privacidad**. Abajo tienes la opción **Usar HTTPS** para conseguir más seguridad. Haz clic en la frase **Ir a configuración de HTTPS** e introduce tus datos personales.



¿Tienes activado HTTPS en tus sitios habituales? ¿Lo echas en falta en alguna de tus web favoritas?