Cinco pasos para seguridad en Firefox

Con los años, muchos han promocionado el navegador Firefox de Mozilla como uno de los más seguros. Pero al igual que con otros navegadores, el nivel de seguridad ofrecido dependerá de la configuración. Algunas de las características de seguridad deben estar activados manualmente. Las que estan activadas de forma predeterminada aún debe tener una doble comprobación.

Siga estos cinco pasos para bloquear las fugas de seguridad de Firefox. Comienza con lo esencial en la propia configuración de tu navegador, elija algunos complementos útiles. Por último, mantenga un registro de sus plug-ins para que pueda actualizarlos agujeros de seguridad que son inevitables.

Habilitar una contraseña maestra

De forma predeterminada, nada impide que otras personas vean toda la información de inicio de sesión guardado en Firefox.

Al igual que otros navegadores, Firefox por defecto permite a cualquier persona que acceda a su ordenador iniciar sesión en sitios donde se ha guardado la contraseña. Y al igual que con Google Chrome, la lista de los nombres de usuario y contraseñas guardados se pueden ver a través del menú Opciones de Firefox.

Afortunadamente, Firefox ofrece una función de contraseña maestra que encripta y protege con contraseña la lista de contraseñas guardada. Cuando está activada, debe introducir la contraseña maestra la primera vez que use una contraseña guardada, una vez por sesión del navegador. Además, a pesar de que ingrese la contraseña maestra la primera vez, siempre hay

que entrar en él antes de que puedas ver las contraseñas guardadas a través del menú Opciones. Esta es una gran característica para ayudar a prevenir la obtención casual de sus contraseñas. Incluso se evita la mayoría de los servicios de terceros para recuperarlos.

Crear una contraseña maestra evita que otros utilicen o ver su información de inicio de sesión guardada.

Para activar la función de contraseña maestra, abra el menú de Firefox, seleccione Opciones, seleccione la ficha Seguridad y, a continuación, active la opción Utilizar una contraseña maestra.

Utilice una contraseña segura para la sincronización

Al igual que Google Chrome, Firefox tiene una función de sincronización para sincronizar sus marcadores, contraseñas y otros datos del navegador a Firefox que se ejecutan en otros equipos y dispositivos. Afortunadamente, Firefox encripta todos los datos sincronizados, no sólo tus contraseñas guardadas (como lo hace Google Chrome). Además, Firefox tiene más seguridad que la que Chrome ofrece de forma predeterminada cuando se está configurando un nuevo ordenador o dispositivo para sincronizar.

Syncing convenientemente sincroniza sus datos de acceso guardados y otros datos de navegación a través de múltiples ordenadores.

En Firefox, debe iniciar sesión con la contraseña de Firefox Sync. A continuación, debe introducir una clave de acceso al azar del nuevo dispositivo en el que usted ya ha configurado, o toma la clave de recuperación de un dispositivo que ya ha creado y la entrada de esa clave en el nuevo dispositivo.

Por lo tanto usted no tiene mucho de qué preocuparse con Firefox syncing, siempre y cuando utilice una contraseña segura, una con las letras en mayúsculas y minúsculas, números y caracteres especiales.Si una persona sabe o rompe la contraseña y tiene acceso a un dispositivo que ya ha configurado con la sincronización, pueden configurar otros dispositivos con la sincronización y acceder a sus contraseñas y otros datos del navegador.

Para activar o cambiar la configuración de sincronización, abra el menú de Firefox, seleccione Opciones, y seleccione la pestaña Sync.

Verifique que las opciones de seguridad están habilitadas

Al igual que otros navegadores populares, Firefox incluye algo de seguridad básica y la configuración de privacidad. Aunque la mayoría están habilitados por defecto, usted debe asegurarse de que no se han desactivado. Comience abriendo el menú Firefox y selecciona Opciones. En la ventana Opciones, seleccione la ficha Seguridad. Asegúrese de que la primera opción Avisarme cuando los sitios tratan de instalar complementos, está capacitado para ayudar a evitar que los sitios desde instalación automática de los complementos, ya que algunos pueden ser peligrosos.

Asegúrese de que las tres primeras opciones de seguridad están

seleccionadas para protegerse contra malware y ataques de phishing.

A continuación, asegúrese de que las siguientes dos opciones, Bloquear sitios de ataque y Bloquear falsificaciones web, también se comprueban para ayudar a activar la protección contra malware y phishing.

A continuación, seleccione la pestaña Privacidad. Y si quieres más privacidad en línea, seleccione la primera opción, Decir a los sitios web que no quiero ser rastreado, que no está habilitado de forma predeterminada. Aunque no se puede prevenir todo seguimiento, se reducirá de seguimiento por los sitios que soportan este tipo de opción.

Marque la primera opción de privacidad para ayudar a evitar que los sitios web puedan rastrear su actividad en línea.

Ahora, seleccione la pestaña Contenido. Para evitar que las ventanas pop-up que puede ser molesto e incluso contener anuncios de phishing, asegúrese de que la primera opción está activada: Bloquear ventanas emergentes.

Por último, seleccione la ficha Opciones avanzadas, seleccione la subpestaña Update, y asegurarse de que instale automáticamente las actualizaciones se selecciona.

Utilizar complementos para mayor protección

Considere la instalación de estos complementos relacionados con la seguridad para la protección adicional:

- **NoScript** ayuda a controlar qué sitios pueden utilizar JavaScript, Silverlight, Flash, y otro contenido integrado, ya que pueden ser utilizados maliciosamente para infectar su computadora o de los intentos de phishing.
- **Adblock Plus** bloquea banners, pop-ups, y los anuncios de vídeo en sitios web para reducir el desorden y la molestia que resulta, incluso pueden reducir tropezar accidentalmente con adware, malware y ataques de phishing.
- **Web of Trust (WOT)** se muestran las calificaciones por los usuarios de sitios y bloquea los sitios peligrosos, tales como aquellos con malware para aumentar el surf, ir de compras, y la búsqueda en la Web seguro.
- **HTTPS Finder** automáticamente detecta y hace cumplir HTTPS / conexiones cifradas SSL cuando estén disponibles-genial para ayudar a reducir las probabilidades de un espía en una red Wi-Fi desde la captura de sus datos de acceso.
- **Xpnd.it!** este expansor de URL le permite pasar sobre enlaces acortados para ver la URL real y otra información básica sobre el sitio para saber a dónde conduce antes de hacer clic.

Comprobar y actualizar los plug-ins

Los ciberdelincuentes utilizan regularmente vulnerabilidades en los plug-ins de los navegadores (productos Java y Adobe similares) para infectar e invadir ordenadores. La mayoría de plug-ins liberan periódicamente actualizaciones de arreglar brechas de seguridad. Muchos plug-ins se establecen de forma predeterminada para actualizar automáticamente o por lo menos para que le notifique de ellos. Sin embargo, es una buena idea

para comprobar periódicamente si hay actualizaciones. Considere la posibilidad de usar el **Mozilla plug-in checker** o sitios de terceros como **Qualys BrowserCheck** para actualizaciones para otros navegadores.

Un poco de vigilancia recorre un largo camino

Firefox es bastante seguro por su cuenta, pero usted puede hacer que sea aún más seguro con la configuración correcta y complementos adecuados. Una buena gestión de la contraseña sigue siendo esencial, también: Crear y habilitar una contraseña maestra para que otros usuarios no pueden usar o ver sus contraseñas. Y si se utiliza la función de sincronización para sincronizar las contraseñas y los datos del navegador a través de dispositivos, utilice una contraseña segura para evitar que otros la sincronicen. Por último, vigilar a sus add-ons y plug-ins para asegurarse de que te están dando la mejor protección posible.