VERSIÓN EN ESPAÑOL

UNAM CERT

OUCH! | Septiembre, 2017

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- Descripción general
- Cómo funcionan los gestores de contraseñas
- Elegir el gestor de contraseñas

Gestores de contraseñas

Descripción general

Uno de los pasos más importantes para protegerte en línea es utilizar una clave única y fuerte para cada una de tus cuentas y aplicaciones. Desafortunadamente, es muy probable que no puedas recordar todas tus contraseñas para tus diferentes cuentas. Esta es la razón por la cual tantas personas reutilizan la misma. Desafortunadamente, la reutilización de tus llaves de acceso para diferentes cuentas es peligrosa porque una vez que alguien compromete tu contraseña, puede acceder a todas tus otras cuentas que utilizan la misma. Una solución simple es usar un gestor, a veces llamado “bóveda de contraseñas”. Estos son programas que almacenan de forma segura todas tus claves, por lo que es fácil tener una diferente para cada cuenta. Los gestores de contraseñas hacen esto sencillo porque en lugar de tener que recordar todas tus llaves de acceso, solo tienes que recordar una.

Editor Invitado

Chris Christianson es un Consultor de seguridad de la información con sede en California, con 20 años de experiencia y numerosas certificaciones técnicas. Ha participado en una variedad de conferencias y colaborado en muchos artículos de la industria. Chris puede ser contactado en **@cchristianson** y **https://ismellpackets.com**.

Cómo funcionan los gestores de contraseñas

Los gestores trabajan almacenando todas tus contraseñas en una base de datos, que a veces se denomina bóveda. El gestor cifra el contenido de la bóveda y lo protege con una contraseña maestra que solo tú conoces. Cuando necesitas recuperar tus llaves de acceso, para ingresar a tu banco o correo electrónico, simplemente ingresas tu contraseña maestra en el gestor para desbloquear la bóveda. En muchos casos, el programa recuperará automáticamente tu contraseña y se conectará de forma segura por ti. Esto hace que sea sencillo tener cientos de claves únicas y fuertes, ya que no tienes que recordarlas.

Algunos gestores almacenan tu bóveda en tu computadora o dispositivo móvil, mientras que otros lo almacenan en la nube. Además, la mayoría de los gestores incluyen la posibilidad de sincronizar automáticamente el contenido de la bóveda a través de varios dispositivos que autorices. De esta manera, al actualizar una contraseña en tu computadora, estos cambios se sincronizan con todos los demás dispositivos. Independientemente de dónde se almacene la base de datos, debes instalar la aplicación de gestor en tu sistema o dispositivo para usarla.

Gestores de contraseñas

Cuando configures un gestor de contraseñas por primera vez, debes introducir o importar manualmente tus inicios de sesión y contraseñas. Posteriormente, el gestor puede detectar cuando intentas registrarte en una nueva cuenta o actualizar la clave de una cuenta existente, actualizando automáticamente la bóveda en consecuencia. Esto es posible porque la mayoría de los gestores trabajan mano a mano con tu navegador web. Esta integración también les permite iniciar sesión automáticamente en sitios web.

Es fundamental que la contraseña maestra que utilices para proteger el contenido del gestor sea fuerte y muy difícil de adivinar para otros. De hecho, te recomendamos que tengas una frase de contraseña como clave maestra, uno de los tipos de contraseñas más fuertes posibles. Si el gestor admite la verificación en dos pasos, utilízalo para tu llave maestra de acceso. Por último, asegúrate de recordar tu contraseña maestra. Si la olvidas, no podrás acceder a ninguna de tus otras claves.

Los gestores de contraseñas son una forma sencilla de almacenar y utilizar claves de acceso.

Elegir un gestor de contraseñas

Hay muchos gestores para elegir. En la sección Recursos, proporcionamos un enlace a las revisiones de los gestores de contraseñas. Mientras tanto, al intentar encontrar el que es mejor para ti, ten en cuenta lo siguiente:

- El gestor debe ser sencillo de usar. Si lo encuentras demasiado complejo para entender, busca uno diferente que se adapte mejor a tu estilo y experiencia.
- El gestor debe funcionar en todos los dispositivos que necesitan de una contraseña. También debería ser fácil mantener las claves sincronizadas en todos los dispositivos.
- Utiliza solo gestores de contraseñas conocidos y confiables. Ten cuidado con los productos que no han existido por mucho tiempo o tienen pocos o ningún comentario de otros usuarios. Los ciberatacantes pueden crear falsos gestores de contraseñas para robar tu información. También sospecha de los vendedores que promueven el desarrollo de su propia solución de cifrado.
- Evita cualquier gestor que asegure ser capaz de recuperar tu contraseña maestra. Esto significa que conocen tu clave maestra, lo que te expone a un riesgo excesivo.
- Asegúrate de que el gestor que elijas cuente con actualizaciones automáticas y cerciórate de utilizar siempre la última versión.

Gestores de contraseñas

- El gestor debe incluir la posibilidad de generar automáticamente contraseñas seguras para ti y mostrarte la fuerza de las contraseñas que has elegido.
- El gestor debe ofrecerte la opción de almacenar otros datos confidenciales, como las respuestas a tus preguntas secretas de seguridad, las tarjetas de crédito o los números de viajero frecuente.

Los gestores de contraseñas son una excelente manera de almacenar tus contraseñas y otros datos confidenciales de forma segura. Sin embargo, puesto que protegen tal información importante, asegúrate de usar una contraseña maestra única y fuerte, que no solo sea difícil de adivinar para un atacante, sino fácil de recordar.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: securingthehuman.sans.org/ouch/archives

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.

Sitio web: http://www.seguridad.unam.mx

Síguelo en Twitter @unamcert

Recursos

Top de gestores de contraseñas 2017:	https://www.pcmag.com/article2/0,2817,2407168,00.asp
Frase de contraseña:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201704_sp.pdf
Verificación en dos pasos:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_sp.pdf
Protege tu Login:	https://www.lockdownyourlogin.org/

Consejo editorial: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traducción: Alicia Manjarrez, Raúl Abraham González y Célica Martínez Aponte.

