OUCH!

En esta edición...

- Resumen
- ¿Cómo funcionan los gestores de contraseñas?
- Elegir un gestor de contraseñas

Gestores de contraseñas

Resumen

Uno de los pasos más importantes que puedes tomar para protegerte en línea es utilizar una contraseña segura y única para cada una de tus cuentas. Desafortunadamente, la mayoría de nosotros tenemos muchas cuentas y es casi imposible acordarse de todas las contraseñas. Una solución simple es utilizar un gestor de contraseñas, a veces llamado bóveda de contraseñas. Estas aplicaciones están diseñadas para almacenar de forma segura los datos de acceso. Además, pueden hacer que sea mucho más fácil el acceso a los sitios web, apps móviles y otras aplicaciones.

Editor Invitado

Lenny Zeltser está encargado de salvaguardar las operaciones TI de los clientes en NCR Corp y capacitar a profesionales de seguridad en el Instituto SANS. Sigue a Lenny en su Twitter **@lennyzeltser** y sus artículos publicados en **zeltser.com**.

¿Cómo funcionan los gestores de contraseñas?

Un gestor de contraseñas actúa como una caja de seguridad digital, almacena tus nombres de usuario, contraseñas y otra información sensible. Cuando un sitio te solicita ingresar con tu cuenta, el gestor puede recuperar en automático tu contraseña e iniciar la sesión de forma segura en el sitio web. Esto hace que sea fácil tener cientos de contraseñas únicas y fuertes, ya que no tienes que recordarlas.

Los gestores de contraseñas almacenan tu información en una base de datos, también conocida como bóveda. El gestor cifra el contenido de la bóveda y la protege con una contraseña maestra que solamente tú conoces. Cuando se necesita recuperar las credenciales, tal vez para acceder a tu banco en línea o tus cuentas de correo electrónico, simplemente escribes la contraseña maestra en el gestor para desbloquear la bóveda.

Algunos gestores de contraseñas almacenan tu bóveda en el sistema local o el teléfono inteligente, mientras que otros lo hacen en sitios web remotos de la compañía que desarrolló el gestor. Además, la mayoría incluye la opción de sincronizar automáticamente el contenido de la bóveda a través de múltiples dispositivos que tú autorizas. De esta forma cuando se actualiza una contraseña en una computadora portátil, los cambios se sincronizan con tu teléfono inteligente, tableta o cualquier equipo que estés utilizando. Independientemente de dónde se almacena la base de datos, necesitas instalar el gestor en tu sistema o dispositivo para usarlo.

Gestores de contraseñas

Cuando configuras por primera vez un gestor de contraseñas, necesitas introducir o importar manualmente los nombres de usuarios y contraseñas. Posteriormente, el gestor puede detectar si estás tratando de registrar una cuenta nueva en línea o cambiar la contraseña de una cuenta existente, por consiguiente en automático actualiza la bóveda. Esta integración también les permite automáticamente ingresarte a sitios web.

Los gestores de contraseña son una forma sencilla de almacenar y utilizar diferentes contraseñas de forma segura.

Los gestores de contraseñas están diseñados para almacenar de forma segura datos sensibles. Sin embargo, es fundamental que la contraseña maestra que utilices para proteger los contenidos de la bóveda sea fuerte y difícil de adivinar. De hecho te recomendamos hacer de tu contraseña una frase de acceso, uno de los tipos de contraseñas más fuertes que existe. Si tu gestor es compatible con la verificación en dos pasos, utilízala para tu contraseña maestra. Asegúrate de no usar tu contraseña maestra para cualquier otro sistema o cuenta. De esta manera, incluso si un atacante logra obtener una copia de tu bóveda, serán incapaces de adivinar la contraseña y acceder al contenido. Finalmente, recuerda la contraseña maestra, ya que si la olvidas no serás capaz de acceder a ninguna de las otras contraseñas.

Elegir un gestor de contraseñas

Hay muchos gestores libres y comerciales para elegir. Al buscar cuál es el mejor para ti, ten en cuenta lo siguiente:

- Comprueba que el gestor de contraseñas funciona en todos los sistemas y dispositivos móviles en los que puedas necesitar acceder a tu bóveda. La solución debería facilitar la sincronización de los contenidos en todos tus dispositivos.
- Usa sólo gestores conocidos y de confianza. Ten cuidado con productos lanzados recientemente o con los que tienen pocos o ningún comentario de la comunidad. Al igual que un software antivirus falso, los ciberdelincuentes pueden crear gestores de contraseñas falsos para robar tu información.
- El gestor debe ser simple en su uso. Si encuentras una solución muy compleja de entender, busca una alternativa que se ajuste a tu estilo y experiencia.
- Asegúrate que cualquier solución que elijas esté actualizada de forma activa y parchada, y que siempre utilices la última versión.
- El gestor debe permitirte elegir una contraseña segura para tus múltiples cuentas, incluyendo la facilidad de generarlas automáticamente y de medir su fortaleza.

Gestores de contraseñas

- El gestor debería darte la opción de almacenar otros datos sensibles, como las respuestas a tus preguntas secretas de seguridad, números de tarjetas de crédito o de viajero frecuente.
- Ten cuidado de los gestores que proporcionan técnicas de cifrado bajo licencia o desconocido, en lugar de cifrar la bóveda utilizando los estándares de la industria. Si el vendedor anuncia cómo desarrollaron su propia solución de cifrado, es mejor mantenerse alejados de ellos.
- Evita cualquier gestor que diga ser capaz de recuperar la contraseña maestra. Esto significa que conocen tu contraseña y te expone a más riesgos.

Los gestores de contraseñas son una solución poderosa para almacenar de forma segura todas tus contraseñas y otros datos sensibles. Sin embargo, ya que protegen la información importante, asegúrate de utilizar una contraseña maestra que no sólo sea difícil de adivinar para los atacantes, sino fácil para que la recuerdes.

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: http://www.securingthehuman.org

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

Frases de acceso: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_sp.pdf

Verificación en dos pasos: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201509_sp.pdf

Gestores de contraseñas: http://www.xataka.com/seguridad/gestores-de-contrasenas-que-son-como-se-usan-y-cual-es-el-mejor

Consejos de seguridad de UNAM-CERT: http://www.seguridad.unam.mx/usuario-casero/consejos/

OUCH! es publicado por SANS Securing The Human y distribuido bajo licencia de Creative Commons BY-NC-ND 4.0.
Puedes distribuir este boletín o utilizarlo en tu programa de sensibilización de seguridad siempre y cuando no se modifique su contenido.
Para más información contáctanos en: ouch@securingthehuman.org

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción: Katia Rodríguez y Célica Martínez

© SANS Institute 2015