El Boletín Mensual de Concientización en Seguridad para ti

Gestores de contraseñas

Resumen

Uno de los pasos más importantes que puedes hacer para protegerte es utilizar una contraseña única y fuerte para cada una de tus cuentas y aplicaciones. Desafortunadamente, es casi imposible recordar todas las diferentes contraseñas. Adicionalmente, sabemos que toma tiempo tener que ingresar tus contraseñas frecuentemente en diferentes sitios. Sin embargo, hay una solución que puede hacer tu vida mucho más simple y segura—gestores de contraseñas.

Cómo funcionan los gestores de contraseñas

Los gestores de contraseñas funcionan almacenando todas tus contraseñas en una base de datos, que muchas veces es llamada bóveda. Los gestores de contraseña cifran el contenido de la bóveda y lo protegen con una contraseña maestra que solo tu sabes. Cuando necesitas tus contraseñas, como para ingresar a tus cuentas de banco en línea o cuentas de correo, simplemente escribes tu contraseña maestra en el gestor para desbloquear las bóveda. El gestor de contraseñas recuperará automáticamente la contraseña correcta e iniciará sesión de manera segura en el sitio web. No tendrás que recordar más tus contraseñas o iniciar sesión manualmente en tus cuentas.

Adicionalmente, muchos gestores cuentan con capacidad para sincronizarse automáticamente en múltiples dispositivos. De esta manera, cuando actualizas una contraseña en tu laptop, esos cambios se sincronizan en todos tus otros dispositivos. Finalmente, muchos gestores de contraseñas detectan cuando intentas crear una nueva cuenta en línea o actualizan la contraseña de una cuenta existente, y estos automáticamente actualizan la bóveda por ti.

Es fundamental que la contraseña maestra, que utilices para proteger el gestor de contraseñas, sea larga y única. De hecho, te recomendamos hacer tu contraseña maestra una frase (una contraseña larga hecha de múltiples palabras o frases). Si tu gestor de contraseñas soporta la verificación en dos pasos, utilízala para tu contraseña maestra también. Finalmente, asegúrate que recuerdas tu contraseña maestra. Si la olvidaste, no podrás acceder a ninguna de tus contraseñas.

Seleccionando un gestor de contraseñas

Existen muchos gestores de contraseñas de los cuales elegir. En la sección de Recursos te compartimos un enlace de una revisión de gestores de contraseñas. Mientras tanto, cuando busques la opción que sea mejor para ti, ten lo siguiente en mente:

Tu gestor de contraseñas debe ser muy sencillo de utilizar. Si la solución es demasiado compleja de entender, busca una diferente que se adapte mejor a tu estilo y experiencia.

El gestores de contraseñas debería funcionar en todos los dispositivos en los que necesitas utilizar contraseñas. También debería mantener fácilmente sincronizadas tus contraseñas en todos tus dispositivos.

Utiliza solo gestores de contraseñas conocidos y confiables. Ten cuidado con los productos que no hayan existido por un largo tiempo o tengan poca o ninguna respuesta de la comunidad. Los ciber criminales pueden crear falsos gestores de contraseñas para robar tu información. También, sospecha de proveedores que prometan que desarrollaron su propia solución de cifrado.

Evita cualquier gestor de contraseñas que afirme recuperar tu contraseña maestra por ti. Esto significa que conocen tu contraseña maestra, lo que te expone a un riesgo excesivo.

Asegúrate que, en cualquier solución que elijas, el proveedor mantenga activas las actualizaciones y los parches del gestor de contraseñas y, verifica especialmente que utilices siempre la versión más reciente.

El gestor de contraseñas puede darte la opción de almacenar algún otro dato sensible, como las respuestas secretas a las preguntas de seguridad, información de tarjetas de crédito, y números de viajero frecuente.

Considera escribir tu frase maestra en un sobre sellado y guarda en un gabinete cerrado, caja fuerte física o caja de seguridad.

Los gestores de contraseña son una gran forma de almacenar todas tus contraseñas y otros datos sensibles, como números de tarjetas de crédito. Sin embargo, asegúrate utilizar una frase maestra única y fuerte y siempre utiliza la última versión de la solución que elijas.

Editor invitado

Russell Eubanks *es líder en seguridad de la información con sede en Atlanta, con más de 20 años de experiencia, y cuenta con muchas certificaciones en seguridad. Es uno de los responsables del Centro de Tormentas de Internet (del inglés, Internet Storm Center) del SANS y colabora en los Controles de Seguridad Críticos. Puedes encontrar a Russell como @russelleubanks y en https://www.securityeverafter.com.*

Recursos

Creando contraseñas simples:	http://www.sans.org/u/Y10
Herencia digital:	http://www.sans.org/u/Z10G
Revisión de los mejores gestores de contraseñas	https://www.wired.com/story/best-password-managers/