VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Octubre 2013

Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

En esta edición...

Gestores de contraseñas

El problema

Una de las primeras cosas que la gente aprende acerca de proteger su identidad personal e información es el uso de contraseñas seguras. Una contraseña segura es aquella que no solo es difícil de adivinar por los criminales cibernéticos, también debe resistir herramientas de hackeo automatizadas. Una regla común es la siguiente: entre más larga y compleja es la contraseña, más fuerte y más segura es. El problema es que las contraseñas seguras pueden ser difíciles de recordar. Como resultado, la gente a menudo crea una contraseña única y usa la misma contraseña o ligeras variaciones de la misma para todas sus cuentas en línea, aplicaciones y dispositivos. Aún más peligroso, muchas personas utilizan la misma contraseña tanto para sus cuentas personales como para las de su trabajo. Si eres de las personas que reutiliza su contraseña para varias cuentas, ten cuidado porque estás en riesgo. Una vez que un atacante cibernético obtiene acceso a tu contraseña, puede tener acceso a todas las cuentas que comparten las contraseñas. En última instancia, lo que necesitas es una contraseña segura y única para cada una de tus cuentas. De esta forma, si alguien obtiene acceso a la contraseña de una de ellas, las demás permanecerán seguras. Desafortunadamente, con tantos dispositivos y cuentas diferentes, se ha vuelto casi imposible que alguien pueda recordar su creciente colección de contraseñas.

Editor Invitado

George Bakos es Director Técnico de Inteligencia y Respuesta de Northrop Grumman y es un instructor certificado del Instituto SANS desde 2001. George estará en Londres el próximo noviembre impartiendo el curso Security 502, Perimeter Protection in Depth (Seguridad perimetral avanzada).

La solución

Una solución que la gente suele usar es escribir todas sus contraseñas en una hoja de papel, o peor aún, escribirlas y luego pegarlas en el monitor de su computadora (basta mirar en las ventanas de los edificios o de oficinas cerradas y ver los monitores cubiertos con notas adhesivas). Estas actividades representan una falta de seguridad, ya que otras personas pueden hallar y leer tus contraseñas, especialmente si viajas y las pierdes o te las roban. En cambio, lo que necesitamos es una solución que almacene de forma segura todas tus contraseñas en un único lugar. Lo mejor sería tener un programa informático que simplifique todo el proceso de lanzar automáticamente tus contraseñas e iniciar sesión en sitios web y aplicaciones por sí misma. Y aún más lo sería un programa que también pueda generar contraseñas seguras e incluso, tal vez, almacenar otra información confidencial como los datos de las tarjetas de crédito. Afortunadamente, existe una solución, se le llama gestor de contraseñas (a veces, bóveda de contraseñas).

Gestores de contraseñas

¿Cómo funcionan los gestores de contraseñas?

Un gestor de contraseñas actúa como una caja fuerte virtual. La primera instalación de esta caja fuerte virtual es como la de un programa en tu computadora o dispositivo móvil. Después, toma todos los nombres de usuario y contraseñas y los cifra en una base de datos que luego se almacena en el dispositivo o en la nube. Esta base de datos es asegurada por una contraseña especial que se crea solo para el gestor de contraseñas. De esta manera solo tendrás que recordar una sola contraseña. Es decir, cada vez que necesites recuperar tus credenciales para acceder a tu banca en línea o cuentas de correo electrónico, simplemente escribes la contraseña de tu gestor de contraseñas. Esto te permite tener una contraseña única para cada cuenta, incluso tener cientos de cuentas, sin necesidad de recordar siquiera alguna de ellas. El gestor de contraseñas almacena toda esta información y puedes asegurarte de que la contraseña maestra que utilizas es muy fuerte y que no se te olvidará.

Los gestores de contraseñas son una forma sencilla de almacenar con seguridad todas las contraseñas diferentes de cada una de tus cuentas.

Ahora, varios gestores de contraseñas también pueden integrarse con tu navegador. Cuando visitas un sitio web, como tu tienda en línea favorita, el gestor de contraseñas se conectará automáticamente. Incluso, si la contraseña para ese sitio cambia, el gestor de contraseñas actualizará las entradas para éste. Algunos gestores de contraseñas funcionan de igual manera en los dispositivos móviles, sin embargo la mayoría de ellos no funcionan con otras aplicaciones, solo se integran con el navegador del dispositivo móvil.

La elección de un gestor de contraseñas

Hay para elegir entre muchos gratuitos, de código abierto y comerciales. Para encontrar el más conveniente para ti, toma en cuenta lo siguiente:

- Utiliza únicamente soluciones reconocidas y de confianza. Ten cuidado con las soluciones que no han existido por mucho tiempo o que tienen poca o ninguna retroalimentación. Los delincuentes cibernéticos pueden crear soluciones falsas diseñadas para robar tu información.
- Asegúrate de que cualquier solución que elijas se mantenga actualizada y cuida que siempre estés usando la versión más reciente.

Gestores de contraseñas

- Debe ser simple de usar. Si encuentras una solución demasiado compleja de entender, puede que cometas errores fácilmente.
- Debe cifrar las contraseñas utilizando un estándar, un cifrado fuerte de la industria. Ten cuidado con algunas soluciones patrocinadas o de propietarios desconocidos.
- El gestor de contraseñas se debe ejecutar en todos los diferentes equipos que utilizas. Algunas versiones más avanzadas también funcionan en dispositivos móviles.
- Una característica útil es tener un cifrado que proporcione medios para sincronizarse en los diferentes dispositivos que utilizas. Si proporciona estos medios, debe cifrar los datos localmente antes de enviarlos al sistema central.
- Debe proporcionar herramientas para generar contraseñas aleatorias y ayudar a controlar las fechas de caducidad de las contraseñas.
- Debe ayudar en la identificación de la fortaleza relativa de las contraseñas que hayas elegido.

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

Comparativa de gestores de contraseñas gratuitos:	http://www.osi.es/es/recursos/utiles-gratuitos/categoria/gestores-de-contrasenas
7 gestores de contraseñas:	http://www.mujeresdeempresa.com/tecnologia/080902-gestores-de-contrase%C3%B1as.asp
¿Debo cambiar mi contraseña? (En inglés):	https://shouldichangemypassword.com/all-sources.php
Glosario de términos de seguridad:	http://www.viruslist.com/sp/glossary
Consejo del día del Instituto SANS:	https://www.sans.org/tip_of_the_day.php
Consejos de seguridad de UNAM-CERT:	http://www.seguridad.unam.mx/usuario-casero/consejos/

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Sarahí Díaz, Pedro Guerrero, Nora Cozaya