OUCH!

SANS SECURITY AWARENESS

Boletín mensual de concientización en seguridad para ti

Creando contraseñas simples

Resumen

A menudo se dice que las contraseñas son factor clave para proteger las cuentas (¡lo cual es cierto!), pero rara vez te ofrecen una forma sencilla de crear y administrar de manera segura todas las contraseñas. A continuación, te compartimos tres pasos para simplificar tus contraseñas, bloquear tus cuentas y proteger tu futuro.

Frases de contraseña

Los días de contraseñas locas y complejas han terminado. Aquellas contraseñas son difíciles de recordar, difíciles de escribir, y con las computadoras súper rápidas de hoy en día, pueden ser fáciles de descifrar por un ciberatacante. La clave para las contraseñas es que sean largas, cuantos más caracteres tenga, mejor. Estas se llaman frases de contraseña, un tipo de contraseña segura que usa una oración corta o palabras aleatorias. Aquí hay dos ejemplos.

¡Hora de tomar un café fuerte!
caracol-rastrero-perdido-playa

Ambas son fuertes, con más de veinte caracteres, fáciles de recordar y fáciles de escribir, pero difíciles de descifrar. Te encontrarás con sitios web o situaciones en las que requieran o que pidan agregar símbolos, números o letras mayúsculas, lo cual está bien. Recuerda que la longitud es lo más importante.

Gestores de contraseñas

Necesitas una contraseña única para cada cuenta. Si reutilizas la misma contraseña para varias cuentas puede ser peligroso. Todo lo que hace un ciberatacante es ingresar a un sitio web, robar todas las contraseñas, incluida la tuya, y luego usar tu contraseña para iniciar sesión en tus otras cuentas. Esto sucede más seguido de lo que crees. Visita el sitio web www.haveibeenpwned.com para ver qué sitios ha utilizado y si tus contraseñas fueron comprometidas. Entonces, ¿qué puedes hacer?, utiliza un administrador de contraseñas.

Estos son programas informáticos especiales que almacenan de forma segura todas las contraseñas en una bóveda cifrada. Solo necesitas recordar una contraseña, la del gestor de contraseñas. Este recupera automáticamente tus contraseñas cuando las necesitas e inicia sesión en los sitios web por ti. También tienen otras características como almacenar tus respuestas y preguntas secretas, te advierte cuando reutilizas contraseñas, tiene un generador de contraseñas que te asegura el uso de

contraseñas seguras y muchas otras más. La mayoría de los gestores de contraseñas también se sincronizan de forma segura en casi cualquier computadora o dispositivo, por lo que, independientemente del sistema que estés utilizando, tiene acceso fácil y seguro a todas ellas.

Finalmente, asegúrate de anotar la contraseña de tu gestor y guardarla en un lugar seguro dentro de casa. Algunos gestores de contraseñas incluso te permiten imprimir un kit de recuperación, de esa manera si olvidas la contraseña del gestor obtendrás una copia de seguridad. Además, si te enfermas o estás en una emergencia, tu cónyuge o familiar de confianza podrán recuperar la información en tu nombre.

Verificación de dos pasos

La verificación en dos pasos (a menudo llamada autenticación de dos factores o autenticación de múltiples factores) agrega una capa adicional de seguridad. Requiere que tengas dos cosas cuando inicias sesión en tus cuentas; tu contraseña y un código numérico generado por tu teléfono inteligente o enviado al mismo. Este proceso garantiza que si un ciberatacante obtiene tu contraseña, no podrá acceder a tus cuentas. La verificación en dos pasos es fácil de configurar y, por lo general, solo necesitas usarla una vez cuando inicias sesión desde una nueva computadora o dispositivo. Actívala siempre que sea posible, especialmente para tus cuentas más importantes como tu cuenta bancaria o de jubilación o para el acceso a tu correo electrónico. Si estás utilizando un gestor de contraseñas, te recomendamos que lo protejas con una frase de contraseña segura y con la verificación de dos pasos.

Puede parecer una tontería, pero estos tres pasos simples ayudan mucho a proteger tu trabajo, tu reputación y tu futuro financiero.

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

Editor Invitado

Justin Henderson *(@SecurityMapper) es cofundador de H&A Security Solutions, instructor certificado del Instituto SANS y autor de los cursos SANS Cyber Defense y SIEM. Le encantan todo lo relacionado con la defensa cibernética y ha sido consultor durante quince años.*

Recursos

¿Mis cuentas han sido comprometidas?:	https://haveibeenpwned.com/
Sitio de autenticación de dos factores:	https://twofactorauth.org/
Pautas de identidad digital NIST SP800-63B:	https://pages.nist.gov/800-63-3/sp800-63b.html
Eres un objetivo:	https://www.sans.org/u/OGi