VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Abril 2017

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- Frase de contraseña
- Usa frases de contraseña de forma segura
- Recursos

Frase de contraseña

Resumen

Las contraseñas son algo que utilizas casi todos los días, ya sea para acceder a tu cuenta de correo electrónico o a la banca en línea, hasta para comprar productos o ingresar a tu dispositivo móvil. Sin embargo, las contraseñas son también unos de tus puntos más débiles, por ejemplo, si alguien la aprende o adivina, esta persona podría acceder a tu cuenta, permitiéndole transferir tu dinero, leer tus correos electrónicos o robar tu identidad. Esta es la razón por la cual mantener contraseñas fuertes es esencial para protegerte. Sin embargo, las contraseñas suelen ser confusas y difíciles tanto de recordar como de escribir. En este boletín aprenderás como crear contraseñas fuertes que sean simples de escribir y fáciles de recordar (conocidas también como frases de contraseña).

Editor Invitado
My-Ngoc Nguyen (pronunciado como Me-Nop Wynn) es instructora certificada del SANS y CEO de la consultora Secure IT Solutions. Tiene experiencia en certificaciones de alto nivel y durante más de 14 años ha desarrollado, madurado y administrado programas de seguridad informática para diferentes sectores e industrias. Síguela en su cuenta de Twitter **@MenopN** y de LinkedIn My-Ngoc "Menop" Nguyen.

Frase de contraseña

El desafío al que todos nos enfrentamos es que atacantes cibernéticos han desarrollado métodos sofisticados y efectivos para realizar fuerza bruta a las contraseñas (que las adivinen de forma automatizada), esto significa que personas malintencionadas pueden comprometer tu contraseña si es débil o fácil de predecir. Un paso importante para protegerte es usar contraseñas fuertes. Típicamente esto se hace creando contraseñas complejas, sin embargo, estas pueden ser difíciles de recordar o teclear. En su lugar, se recomienda usar frases de contraseña, que son una serie de palabras aleatorias o una oración; entre más caracteres tenga, será más fuerte. La ventaja es que son mucho más fáciles de teclear y recordar, además son difíciles de adivinar para los ciberatacantes. A continuación se muestran dos ejemplos diferentes:

Sostener-Fácilmente-Encarcelado
La hora para el té es a la 1:30

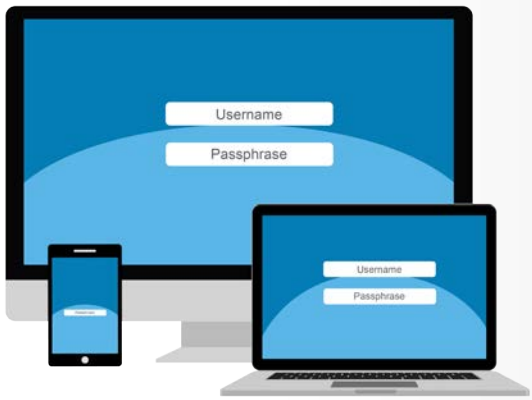
Lo que hace que estos ejemplos sean fuertes no solo es su longitud, sino que usan mayúsculas y símbolos (recuerda, los espacios y signos de puntuación son símbolos); al mismo tiempo, estas frases son fáciles de recordar y escribir. Puedes hacer que tu frase de contraseña sea aún más fuerte si así lo deseas, reemplazando letras con números o símbolos,

Frase de contraseña

por ejemplo, sustituir la letra “a” con el símbolo “@” o la letra “o” con el número cero. Si un sitio web o un programa limita el número de caracteres que puedes utilizar en una contraseña, usa el máximo de caracteres permitido.

Usa frases de contraseña de forma segura

También debes tener cuidado en cómo utilizas las frases secretas. Utilizar una frase de contraseña no te ayudará si personas malintencionadas pueden robarla o copiarla fácilmente.



Las frases de contraseña son una forma más sencilla de crear y recordar contraseñas seguras.

1. Utiliza una contraseña diferente para cada cuenta o dispositivo que tengas. Por ejemplo, nunca uses la misma contraseña para tu cuenta de trabajo o bancaria que para tus cuentas personales como Facebook, YouTube o Twitter. De esta forma si alguna de tus cuentas es comprometida, las otras continuarán siendo seguras. Si tienes demasiadas frases secretas como para recordarlas todas (que es muy común), puedes considerar el uso de un gestor de contraseñas.
2. Nunca compartas una frase secreta o tu estrategia para crearlas con nadie, incluyendo a compañeros de trabajo o tu supervisor. Recuerda que una contraseña es un secreto; si alguien más la conoce, ya no será segura. Si accidentalmente compartes una frase secreta con alguien más o crees que puede haber sido comprometida o robada, cámbiala inmediatamente. La única excepción es si deseas compartir tus frases secretas personales con algún miembro de tu familia altamente confiable en caso de alguna emergencia. Una propuesta consiste en anotar tus frases de contraseña clave (asegurando que no estén relacionadas con tu trabajo), almacénalas en un lugar seguro y comparte la ubicación con un miembro de tu familia altamente confiable. De esa manera, si algo te llega a suceder y necesitas ayuda, tus seres queridos pueden acceder a tus cuentas críticas.
3. No utilices computadoras públicas, como las de hoteles o cibercafés, para iniciar sesión en sus cuentas, ya que cualquier persona puede utilizarlas y estas pueden estar infectadas o capturar todas tus pulsaciones de teclado. Únicamente inicia sesión en tus cuentas desde equipos o dispositivos móviles de confianza.
4. Ten cuidado con los sitios web que requieran que respondas preguntas personales. Estas preguntas se realizan si te olvidas de tu contraseña y necesitas restablecerla. El problema es que las respuestas a menudo se pueden encontrar en Internet o incluso en tu página de Facebook. Asegúrate de utilizar solo información que no está disponible públicamente o que sea información ficticia que inventes. ¿No puedes recordar todas las respuestas? Selecciona un

Frase de contraseña

tema como un personaje de una película y basa tus respuestas en ese personaje. Otra opción es usar un gestor de contraseñas para almacenar de forma segura esta información adicional.

5. Muchas cuentas en línea ofrecen algo llamado autenticación de dos factores, también conocida como verificación en dos pasos. En esta necesitas, más que tu frase de contraseña para iniciar sesión, un código de acceso que es enviado a tu teléfono inteligente. Esta opción es mucho más segura que una frase de contraseña por si sola. Siempre que sea posible, habilita y utiliza estos métodos más fuertes de autenticación.
6. Los dispositivos móviles a menudo requieren un PIN para proteger el acceso a ellos. Recuerda que un PIN no es más que otra contraseña; cuando más largo sea tu PIN, más seguro será. Muchos dispositivos móviles te permiten cambiar el número PIN a una contraseña real o utilizar un biométrico como tu huella digital.
7. Si ya no utilizas más una cuenta, asegúrate de cerrarla, eliminarla o deshabilitarla.

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

Gestores de contraseñas: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_sp.pdf

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

¿Cómo crear contraseñas seguras?: http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=185

Protegiéndose de los ataques contra archivos de contraseña: http://www.cert.org.mx/descarga.dsc?arch=454

Las contraseñas más comunes de 2016: http://www.seguridad.unam.mx/noticia/?noti=3132

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traducción: José Daniel Campuzano, Víctor Arteaga y Katia Rodríguez