VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Abril 2015

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- Las frases de acceso
- Uso seguro de frases de acceso
- Recursos

Frases de acceso

Panorama

Las passwords o contraseñas son algo que utilizas casi todos los días, desde ingresar a tu correo electrónico y a la banca en línea hasta comprar bienes o acceder a tu teléfono inteligente. Sin embargo, las contraseñas son también uno de tus puntos más débiles, si alguien obtiene tu contraseña puede robar tu identidad, transferir tu dinero o acceder a tu información personal. Las contraseñas seguras son esenciales para protegerte a ti mismo. En este boletín aprenderás cómo crear contraseñas seguras y fáciles de recordar mediante el uso de un tipo de contraseña conocida como passphrases, "frases de contraseña" o "frases de acceso".

Editor Invitado

Guy Bruneau es un consultor líder de seguridad en IPSS Inc., instructor del SANS y colaborador del Internet Storm Center (ISC). Guy cuenta con la certificación SANS GSE y completó el programa SANS Cyber Guardian. Puedes seguir a Guy en Twitter en la cuenta **@GuyBruneau** y en el sitio **handlers.sans.org/gbruneau**.

Las frases de acceso

El reto al que nos enfrentamos todos es que los atacantes han desarrollado métodos sofisticados para adivinar u obtener por "fuerza bruta" las contraseñas, y están constantemente mejorando en ello. Esto significa que pueden poner en peligro tus contraseñas si son débiles o fáciles de adivinar. Un paso importante para protegerse es utilizar contraseñas seguras. Mientras más caracteres tenga tu contraseña, es más fuerte y es más difícil para un atacante adivinarla. A pesar de la longitud, las contraseñas complejas pueden ser complicadas de recordar. En su lugar se recomienda utilizar frases de acceso, estas son simples frases u oraciones que son sencillas de recordar pero difíciles de hackear. Aquí un ejemplo:

¿Dónde está el rey Julián?

Lo que hace a esta frase de acceso tan fuerte no son sólo sus 26 caracteres de longitud, sino que utiliza letras mayúsculas y símbolos (recuerda, los espacios, signos de puntuación y acentuación son símbolos). Puedes hacer tu frase aún más fuerte si reemplazas letras con números o símbolos, como la sustitución de la letra "a" con el símbolo "@" o la letra "O" con el número cero. Si un sitio web o un programa limitan el número de caracteres que puedes utilizar en una contraseña, utiliza el número máximo de caracteres permitidos.

Frases de acceso

Uso seguro de frases de acceso

Debes ser cuidadoso con la forma en la que utilizas las frases de acceso. Usar una frase no servirá de nada si los chicos malos pueden robarla o copiarla fácilmente.

Usar frases de acceso es uno de los pasos más eficaces que puedes tomar para proteger tu identidad e información.

1. Asegúrate de utilizar una frase diferente para cada cuenta o dispositivo que tengas. Por ejemplo, nunca utilices la misma frase para tu trabajo o cuenta bancaria que para tus cuentas personales, tales como Facebook, YouTube o Twitter. De esta manera, si una de esas cuentas es comprometida, las otras siguen estando seguras. Si tienes demasiadas frases que recordar (lo cual es muy común), considera el uso de un gestor de contraseñas, es un programa especial que almacena por ti, de forma segura, todas tus frases de acceso. Así las únicas frases de acceso que tienes que recordar son las de tu equipo y del programa de gestión de contraseñas.

2. Nunca compartas una frase de acceso o tu estrategia para crearlas con ninguna persona, incluyendo a los compañeros de trabajo. Recuerda, una frase de acceso es un secreto. Si alguien más sabe tu contraseña ya no es segura. Si accidentalmente compartes tu frase con otra persona, o crees que pudo haber sido comprometida o robada, asegúrate de cambiarla inmediatamente.

3. Al igual que las contraseñas, evita frases de acceso fáciles de adivinar o usadas comúnmente. Por ejemplo, la frase “Hace ochenta y siete años” de Abraham Lincoln no es una buena frase, ya que es muy conocida.

4. No utilices computadoras públicas, como las que hay en los hoteles o en las bibliotecas, para iniciar sesión en una cuenta de trabajo o del banco. Puesto que cualquiera puede utilizar estos equipos, pueden estar infectados con código malicioso que captura todas las pulsaciones del teclado. Sólo ingresa a tu cuenta de trabajo o cuentas bancarias en equipos o dispositivos móviles de confianza.

5. Ten cuidado con los sitios web que te solicitan responder preguntas personales. Estas preguntas se utilizan si olvidas tu contraseña y necesitas restablecerla. El problema es que las respuestas a estas preguntas a menudo se pueden encontrar en Internet o incluso en tu página de Facebook. Asegúrate de que, si contestas preguntas personales, sólo utilices información que no está disponible públicamente o información ficticia. Un gestor de contraseñas puede ayudar con esto ya que muchos permiten almacenar esta información adicional.

Frases de acceso

6. Muchas cuentas en línea ofrecen algo llamado autenticación de dos factores, también conocida como verificación en dos pasos. Aquí es donde se necesita algo más que la frase de acceso para iniciar sesión, como un código de acceso enviado a tu teléfono. Esta opción es mucho más segura que usar únicamente una frase de acceso. Siempre que sea posible, haz uso de estos métodos de autenticación más fuertes.

7. Los dispositivos móviles suelen requerir un PIN para proteger el acceso a ellos. Recuerda que un PIN no es más que otra contraseña. Cuanto más largo sea el PIN, es más seguro. Muchos dispositivos móviles te permiten cambiar el número de PIN por una frase de acceso.

8. Por último, si ya no estás utilizando una cuenta, asegúrate de cerrarla, borrarla o desactivarla.

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

Verificación en dos pasos:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_sp.pdf
Gestores de contraseñas:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_sp.pdf
Ingeniería social:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_sp.pdf
Términos de seguridad comunes:	http://www.viruslist.com/sp/glossary
Revista .Seguridad de UNAM-CERT:	http://revista.seguridad.unam.mx/

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Ricardo Carmona y Lilia González