VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Mayo 2013

Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- Contraseñas seguras: passphrases
- Uso de contraseñas de forma segura
- Recursos

# Contraseñas

## Antecedentes

Las contraseñas son una de las principales maneras para verificar nuestra identidad. Con ellas accedes a tu correo electrónico, banca electrónica, realizas compras en línea e ingresas a dispositivos como tu laptop o teléfono inteligente. En muchos sentidos, las contraseñas son las llaves de tu reino. Como resultado, si alguien tiene tu contraseña puede robar tu identidad, hacer transferencias de dinero o acceder a tu información personal. Las contraseñas fuertes son esenciales para proteger información e identidad. Aprendamos qué es lo que hace robusta a una contraseña y cómo usarla con seguridad.

### Editor Invitado

Raul Siles es el editor invitado para esta edición, él es analista de seguridad experimentado, fundador de Taddong y autor e instructor del SANS. Puedes seguir a Raul en Twitter en **@taddong** y en su blog **blog.taddong.com**.

## Contraseñas seguras: passphrases

El problema es que los cibercriminales han desarrollado programas sofisticados que pueden aplicar fuerza bruta o adivinar tus contraseñas y, constantemente están mejorándolos. Esto significa que pueden robar tus contraseñas si son débiles o fáciles de adivinar. Nunca utilices información común como contraseña, fecha de nacimiento, el nombre de tu mascota o cualquier cosa que se pueda determinar fácilmente a partir de una publicación de redes sociales o Google. La mejor manera de crear una contraseña segura es usar una contraseña larga y entre más caracteres contenga es mejor. De hecho, en lugar de utilizar una sola palabra, usa varias palabras o incluso una frase completa. Este tipo de contraseñas se conocen como passphrase y es una de las más fuertes que se puede utilizar. Un ejemplo es:

**esto es un secreto**

Eso es todo lo que necesitas. Si lo deseas puedes hacer tu contraseña más segura mediante la adición de símbolos, letras mayúsculas o números, como se muestra en el ejemplo siguiente. Esto es muy importante si el sitio web que consultas no permite espacios en blanco o una frase completa como contraseña:

**Est0 3s un S3cr3t0.**

Nota que este ejemplo usa una letra mayúscula. También puedes reemplazar letras por números o símbolos, como reemplazar una letra “a” con el símbolo “@” y la letra “o” con el número cero o utilizar las marcas de puntuación comunes

# Contraseñas

como un signo de interrogación, punto o espacio. Si un sitio web o programa limita el número de caracteres, puedes usar una contraseña con el número máximo de caracteres permitidos.


*Usa contraseñas fuertes, preferentemente frases que contengan múltiples palabras y asegúrate de usarlas de forma segura.*

## Uso de contraseñas de forma segura:

Además de utilizar contraseñas seguras debes tener cuidado de como las usas. Tener una contraseña fuerte no ayuda en mucho si alguien puede robarla o copiarla.

1. Asegúrate de usar diferentes contraseñas para cada tipo de cuenta. Por ejemplo, nunca utilices las contraseñas de las cuentas de tu trabajo o banco para tus cuentas personales como Facebook, YouTube o Twitter. De esta manera, si tu contraseña es comprometida, las otras cunetas estarán a salvo. Si tienes que recordar muchas contraseñas, considera usar un administrador de contraseñas. Esto es un programa especial que se ejecuta en tu computadora o dispositivo móvil que almacena por ti de forma segura todas las contraseñas. Solo tendrás que recordar la contraseña de tu computadora y del programa que administra las contraseñas. Si tus contraseñas son para el trabajo debes consultar a un supervisor o con el departamento de soporte para preguntar si está permitido el uso de gestores de contraseña en la organización.

2. Nunca compartas tus contraseñas con nadie, incluyendo compañeros de trabajo. Recuerda, tu contraseña es secreta. Si alguien más conoce tu contraseña, no es seguro. Si accidentalmente compartes tu contraseña con alguien o crees que ha sido comprometida o robada, asegúrate de cambiarla inmediatamente.

3. No utilices computadoras públicas, como las que se encuentran en hoteles o bibliotecas para iniciar sesión en cuentas de trabajo o bancarias. Dado que cualquiera hace uso de estos equipos, podrían estar infectados con códigos maliciosos que capturan todo lo que tecleas. Solo accede a tus cuentas de trabajo y de banco en computadoras o dispositivos móviles confiables.

4. Se cuidadoso con los sitios que requieren que contestes preguntas personales. Estas preguntas son usadas si olvidaste tu contraseña y necesitas restablecerla. El problema es que las respuestas pueden encontrarse en Internet o, incluso, en tu página de Facebook. Asegúrate de que si respondes preguntas personales, utilices información que no sea pública o que sea ficticia. Los manejadores de contraseñas pueden ser útiles en este caso.sean información que no esté disponible públicamente o que respondas de manera ficticia. Los manejadores de contraseñas pueden ser útiles en este caso.

## Contraseñas

5. Muchas cuentas en línea ofrecen algo llamado autenticación de doble factor o verificación en dos pasos. Esto significa que se requiere más que solo la contraseña para acceder, como puede ser algún código enviado a tu teléfono inteligente. Esta opción brinda mucha más seguridad que una contraseña por sí misma. Usa este método de autenticación siempre que te sea posible.

6. Los dispositivos móviles usualmente requieren de un PIN para acceder a él. Recuerda que el PIN no es otra cosa que una contraseña. Mientras más largo sea el PIN, es más seguro. Muchos de los dispositivos móviles te permiten cambiar tu numero PIN por una contraseña efectiva.

7. Finalmente, si ya no utilizas alguna de tus cuentas, asegúrate de cerrarla 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: http://www.securingthehuman.org

## Versión en Español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad en Cómputo en México reconocido ante FIRST, es una referencia en seguridad de la información en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

## Fuentes

| | |
|---|---|
| Verificación en dos pasos: | http://www.google.com/landing/2step |
| Contraseñas seguras: | http://preview.tinyurl.com/c7exepn |
| Manejadores de contraseñas: | http://www.freepasswordmanager.com |
| Fortaleza de las contraseñas: | https://xkcd.com/936 |
| Términos comunes de seguridad: | http://preview.tinyurl.com/6wkpae5 |
| Tip del día de seguridad del SANS: | http://preview.tinyurl.com/6s2wrkp |



Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: José Luis Sevilla, Fausto Pérez, Andrea Méndez, Célica Martínez