INFOPAPER:
IMPLEMENTAR DE MANERA SEGURA LA CONTRASEÑA

Contenido

¿Por qué es tan importante la seguridad de la contraseña?	1
La seguridad es lo primero: crea contraseñas seguras	2
Una contraseña para todas las cuentas: ¡conveniente pero inseguro!	2
¿Olvidaste tu contraseña? Elige las preguntas de seguridad con cuidado	2
Almacenamiento de contraseña	3
El administrador de contraseñas como solución	3
Checklist	3

¿Por qué es tan importante la seguridad de la contraseña?

Todos conocen las **recomendaciones básicas sobre seguridad de la contraseña, pero muy pocas personas siguen estas pautas.** En cambio, las fechas de nacimiento, los nombres de los niños o los atajos del teclado como "qwertz" o "123456789" aparecen regularmente y son fácilmente pirateados.

¿Te suena familiar? Si es así, tus **hábitos con las contraseñas deberían cambiar para ponérselo más difícil** a los hackers. Una contraseña pirateada puede tener graves consecuencias y provocar el robo de identidad y graves pérdidas financieras.

Los hackers a menudo logran descifrar contraseñas con los llamados ataques de fuerza bruta. **Usando ciertas herramientas, los atacantes prueban una gran cantidad de combinaciones posibles.**

Es sólo cuestión de tiempo que este método tenga éxito. Incluso un ordenador estándar puede probar varios millones de combinaciones en un segundo. A continuación se describe cómo protegerse con éxito contra el robo de contraseñas.

La seguridad es lo primero: crea contraseñas seguras

Asumir una contraseña ordinaria consta de seis caracteres y solo letras minúsculas. **Esto sería un máximo de 308,951,776 combinaciones posibles,** que una herramienta de fuerza bruta habría intentado descifrar la secuencia correcta de caracteres. Eso suena a mucho, pero es posible en solo unos segundos. Para elegir una combinación de contraseña segura, esta debe constar de 12 a 16 dígitos.

Los ataques de fuerza bruta no tendrían ninguna opción. También es importante que la contraseña contenga caracteres especiales como comas o guiones. **Los expertos de Hornetsecurity recomiendan encarecidamente utilizar también letras y números en mayúsculas y minúsculas.** Una contraseña segura que consta de 16 caracteres sería, por ejemplo, „s ~; u + .LT`" tmP?; Y ".

Una contraseña para todas las cuentas: ¡conveniente pero inseguro!

La contraseña sugerida anteriormente no es fácil de recordar, pero es necesario usar una combinación complicada. Sin embargo, hay que tener más consideraciones: **pues muchos usuarios utilizan la misma contraseña para muchas cuentas diferentes.** Si un ciberdelincuente tiene en sus manos esa contraseña, significaría que podría acceder a cuentas de correo electrónico, **cuentas bancarias online o posiblemente incluso a la red de la empresa con una sola contraseña.** Por lo tanto, solo se debe usar una contraseña individual por cada cuenta de usuario. Esto hace que cualquier ataque sea mucho más difícil.

¿Olvidaste tu contraseña? Elige las preguntas de seguridad con cuidado

Todo el mundo ha olvidado uno u otro código de acceso en algún momento. **Afortunadamente, con la mayoría de los servicios online, la contraseña se puede restablecer por correo electrónico.** Un clic es todo lo que se necesitas para establecer una nueva contraseña, a través de un enlace de confirmación enviado por correo electrónico.

También existe la posibilidad de obtener acceso a tu propia cuenta a través de la pregunta de seguridad. Preguntas como "¿Cuál es el nombre de tu mascota?" O "¿Cuántos hijos tienes?" Son parte del repertorio estándar. Muchos usuarios aprecian mucho esta opción. Pero en realidad esto también es una brecha de seguridad. Las preguntas de seguridad seleccionadas son generalmente preguntas personales cuyas respuestas pueden ser conocidas por desconocidos completos y pueden ser pirateadas más rápido que la contraseña real. **Por esta razón, tiene sentido seleccionar preguntas de seguridad cuya respuesta solo la conozcas tú.**

Cada vez con más frecuencia, las plataformas online prescinden de esta función. **Google no ha respaldado este tipo de recuperación** durante mucho tiempo y, desde 2019, los proveedores de correo electrónico GMX y Web.de no han solicitado el registro de la pregunta de seguridad.

Almacenamiento de contraseña

Los expertos de Hornetsecurity recomiendan que bajo ninguna circunstancia la contraseña se almacene en un archivo de texto en el disco duro. **Además, no se debe utilizar el almacenamiento automático de contraseñas en el navegador.** Porque si el ordenador cae en las manos equivocadas, **los delincuentes tienen un juego fácil.** Especialmente si te encuentras en una red pública, por ejemplo, en un café o en el tren, debes asegurarte de que terceros no tengan acceso a tu ordenador.

El administrador de contraseñas como solución

Una gran ventaja para la seguridad de las contraseñas es un administrador de contraseñas como KeePass. **Es un software de gestión que permite que las contraseñas se almacenen de forma segura.** Solo se necesita una clave maestra para iniciar sesión en el programa y acceder a las otras contraseñas. Si bien esto es práctico, hay ciertos puntos a tener en cuenta: La clave maestra para el software de administración debe ser una contraseña de 24 caracteres, que es más larga que el promedio. La clave maestra también debe usar **una combinación de letras, números y caracteres especiales que nunca antes se habían usado en otro lugar.** Terceras personas y también otras que afirman ser una persona o autoridad fiable no tienen derecho a conocer la combinación de contraseña elegida.

Checklist

Si se toman en serio los puntos anteriores, a los **ciberciminales les resultará mucho más difícil obtener acceso a cuentas privadas,** gracias al alto nivel de seguridad de las contraseñas. Usando la siguiente checklist, todos pueden recordar regularmente los aspectos más importantes para el manejo seguro de contraseñas.

- ☑ La contraseña debe ser de **al menos 12 caracteres** largos, incluyendo caracteres especiales y letras mayúsculas y minúsculas.
- ☑ Utilizar **una sola contraseña para cada cuenta**.
- ☑ Solo debes seleccionar preguntas de seguridad cuyas **respuestas nadie puede descubrir.**
- ☑ No guardes contraseñas en archivos de texto o en el navegador.
- ☑ **Nunca compartas contraseñas** con otras personas.
- ☑ Utiliza un **administrador de contraseñas** como KeePass.