¿Cómo crear una contraseña segura?

Secretaría de Industria y Comercio
Ministerio de Economía

Subsecretaría de Defensa del Consumidor y Lealtad Comercial

Dirección Nacional de Defensa del Consumidor

Escuela Argentina de Educación en Consumo

Contexto

Durante los últimos años el desarrollo de las nuevas tecnologías trajo grandes beneficios para los consumidores y usuarios. Nuevas funciones, mayor conectividad, reducción de los tiempos, acortamiento de las distancias y mucho más.

Sin embargo, esta revolución tecnológica trajo también nuevos desafíos y amenazas de seguridad.

Los ciberdelincuentes utilizan nuevas estrategias e ingeniería social para apropiarse de nuestra información y patrimonio virtual.

A pesar de que ningún sistema es totalmente infalible, las contraseñas son la primera barrera para defendernos y por esto es importante que sean **robustas; para dificultar su vulneración.**

En este material veremos algunas características que hacen que una contraseña sea débil o fuerte.

Ataques y ciberdelincuencia

¿CÓMO FUNCIONA UN “ATAQUE DE DICCIONARIO”?

Una de las formas que tienen los ciberdelincuentes para vulnerar las contraseñas es a través de “diccionarios de contraseñas”.

Lo que hacen es forzar el inicio de sesión probando miles y hasta millones de combinaciones, normalmente desde un listado gigantesco de contraseñas usuales o conjugando palabras comunes y números. Esto se hace probando cada carácter y analizando la respuesta del servidor, como probar número por número en un candado de combinación. Mientras más caracteres, más tiempo le llevará a los ciberdelincuentes vulnerar la contraseña.

¿CÓMO FUNCIONA UN ATAQUE DE “PHISHING”?

En esta ciberestafa, los ciberdelincuentes utilizan distintas técnicas como clonar paginas web de sitios legítimos, llamados y mails falsos, etc. Todo con la intención de que las víctimas les compartan las contraseñas o datos de recupero para adueñarse de los datos o patrimonio virtual ajeno. Es importante no compartir las contraseñas por ningún medio y recordar que ningún proveedor de servicio tecnológico nos pedirá nuestra contraseña o número de recupero por teléfono.

Contraseñas seguras

Vamos a repasar algunas pautas generales para **crear contraseñas seguras:**

- **Deben ser difíciles de adivinar;** no contener información personal, como cumpleaños, nombres o palabras comunes.
- **Longitud mínima:** Los expertos recomiendan contraseñas de 12 a 14 caracteres, a mayor cantidad de estos, más difícil será su vulneración.
- **Combinar minúsculas, mayúsculas, números y caracteres especiales** (#,@,!, etc.).
- **No utilizar la misma contraseña** para distintos servicios/plataformas; esto compromete a varias cuentas.
- **Cambiarlas con regularidad;** cada 30, 60 o 90 días.
- **No guardarlas en el explorador;** pueden ser alcanzadas por cualquiera que acceda al equipo.
- **No compartirlas** por ningún medio con ninguna persona.
- Sólo utilizar **gestores de contraseñas de empresas conocidas.**
- **Habilitar la autenticación multifactor** (utiliza doble vía, ej: contraseña + email o sms).
- Si se anotan las contraseñas en un cuaderno o papel **asegurarse que nadie tenga acceso o hacerlo de forma cifrada.**
- **No pegar las contraseñas en un monitor o debajo del teclado.**

Contraseñas inseguras

Ranking de las contraseñas **más utilizadas en 2023***

		Número de veces que se usó	Tiempo para descifrar (en segundos)
1.	**123456**	**4.524.867**	<1
2.	**admin**	**4.008.850**	<1
3.	**12345678**	1.371.152	<1
4.	**123456789**	1.213.047	<1
5.	**1234**	969.811	<1
6.	**12345**	728.414	<1
7.	**password**	710.321	<1
8.	**123**	528.086	<1

*Basado en la evaluaciòn de una base de datos de 4,3TB procedente de 35 países.
Fuente: NordPass

Cómo generar una contraseña segura

Este no es el único método, si no un ejemplo de una ayuda nemotécnica para recordar una contraseña compleja.

1

Elegir una palabra o frase base

Elegimos una palabra o frase que podamos recordar. Veamos un ejemplo:

todaslashojas

2

Agregar mayúsculas y caracteres especiales.

Ponemos en mayúscula al menos una letra. Y al menos un carácter especial. Nos quedaria algo asi::

Todaslashojas.

3

Cambiar vocales por números

Reemplazamos las vocales por su equivalente en números.
Ejemplos: a □ 4, e □ 3, i □ 1, etc.

T0d4sl4sh0j4s.

4

Agregar un contador

¿Qué es un contador? Es un número al que le vamos sumando o restando unidades, de forma que sea dinámico (no siempre el mismo). Un ejemplo podría ser el mes actual + 2. Si estamos en septiembre, ingresamos 11.

T0d4sl4sh0j4s.11

5

Cambiar con regularidad

El contador también nos puede ayudar a recordar que actualicemos la contraseña. Si ahora estuviéramos en octubre, al ingresar vemos que no se cumple la regla nemotécnica y pasamos a cambiar la contraseña.

T0d4sl4sh0j4s.12

Cómo generar una contraseña segura

Probamos la contraseña en un analizador de contraseña **para medir el nivel de seguridad.**

+ compleja

Contraseña	Nivel de seguridad
todaslashojas	Bajo
Todaslashojas.	Medio
T0d4sl4sh0j4s.	Alto
T0d4sl4sh0j4s.11	Muy Alto

+ segura

Fuente: https://www.roboform.com/

Fuentes

Última revisión
Septiembre 2024

- **Microsoft:**

  https://support.microsoft.com/es-es/windows/crear-y-usar-contrase%C3%B1as-seguras-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb

- **Google:**

  https://support.google.com/accounts/answer/32040?hl=es-419#zippy=%2Cc%C3%B3mo-puedo-hacer-que-mis-contrase%C3%B1as-sean-f%C3%A1ciles-de-recordar

- **Ministerio de Justicia:**

  https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/como-crear-una-contrase%C3%B1a-se

¡Gracias!