



La importancia de tener contraseñas seguras y cómo generarlas

Hoy en día, usamos contraseñas para todo: acceder a nuestro correo electrónico, nuestras redes sociales, e incluso para realizar compras en línea. Pero, ¿cuántos de nosotros realmente pensamos en la seguridad de nuestras contraseñas? ¡Es muy importante proteger nuestras cuentas de accesos no deseados! A continuación, te cuento por qué necesitamos contraseñas fuertes y cómo podemos crearlas fácilmente (y gratis!).

¿Por qué es tan importante tener contraseñas fuertes?

Las contraseñas son como las llaves de nuestra casa digital: permiten el acceso a nuestros datos y toda nuestra información personal. Una contraseña débil puede ser fácilmente adivinada o descifrada por los hackers, especialmente si usas algo sencillo como «123456» o «password». De hecho, te aseguro que estas son algunas de las contraseñas más comunes y, tristemente, también las más vulnerables.

Imagina que usas la misma contraseña para varias cuentas. Si alguien la descubre, tendrá acceso a todas tus cuentas, como si tuviera una llave maestra que abre todas tus puertas digitales. ¡Por eso necesitamos contraseñas únicas y complejas!

¿Qué hace que una contraseña sea segura?

Una buena contraseña debe cumplir con ciertos requisitos que la hagan difícil de adivinar:

1. **Longitud:** debe tener al menos 12 caracteres. Cuantos más caracteres tenga, más difícil será de descifrar.
2. **Combinación de caracteres:** debe incluir letras mayúsculas y minúsculas, números y símbolos especiales (como !, \$, %, &).
3. **Evitar información personal:** no uses datos como tu nombre, fecha de nacimiento o el nombre de tu mascota. Esta información puede ser fácil de encontrar.
4. **Sin palabras comunes:** evita palabras como «contraseña» o combinaciones muy simples.

Por ejemplo, una contraseña débil podría ser «**perrito123**», mientras que una contraseña fuerte podría ser «**X7!g\$9Rt&p2W**». ¡Aunque parezca complicada, una contraseña fuerte es tu mejor defensa contra los ciberdelincuentes!

Consejos para gestionar tus contraseñas

- **No reutilices contraseñas:** aunque sea muy fácil y tentador, nunca uses la misma contraseña para diferentes sitios. Si un [hacker](#) logra acceder a una de tus cuentas, también podría acceder a todas las demás.
- **Cambia tus contraseñas con cierta frecuencia:** cambiar las contraseñas cada ciertos meses te ayuda a mantener una capa adicional de seguridad.
- **Activa la autenticación en dos pasos (2FA):** la autenticación en dos pasos es un mecanismo que proporciona un segundo nivel de protección para tus cuentas. Aun si alguien consigue tu contraseña, no podrá acceder a tu cuenta sin el segundo factor de autenticación.

Un ejemplo frecuente

Para entenderlo mejor, imagina respecto a tu propia cuenta de correo. La contraseña «**miemail123**» puede parecer buena porque es fácil de recordar, pero también es fácil de adivinar. Un [hacker](#) podría usar programas que prueban miles de combinaciones de palabras y números hasta dar con la tuya. En cambio, una contraseña como «**Em%3Q9@bNvWz**» es casi imposible de adivinar. ¡No tiene sentido, pero eso es lo que la hace fuerte!



Utilidad de los generadores de contraseñas en línea como VPNMentor

Una excelente herramienta para generar contraseñas seguras es el [generador de contraseñas de VPNMentor](#). Este generador te permite crear contraseñas aleatorias y muy seguras de manera rápida y sencilla. Podés personalizar la longitud de la contraseña, así como los tipos de caracteres que deseas incluir (mayúsculas, minúsculas, números y símbolos especiales).

El uso de VPNMentor resulta especialmente útil porque proporciona una forma cómoda de crear contraseñas fuertes sin esfuerzo, en línea y sin cargo. Además, podés hacerlo desde cualquier dispositivo con acceso a internet, lo cual es ideal cuando necesitas generar una nueva contraseña estando fuera de casa o cuando no tienes acceso a un [gestor de contraseñas](#). Utilizar herramientas como VPNMentor te asegura que tus contraseñas sean lo suficientemente complejas para evitar cualquier intento de vulneración, manteniendo así tus cuentas a salvo.

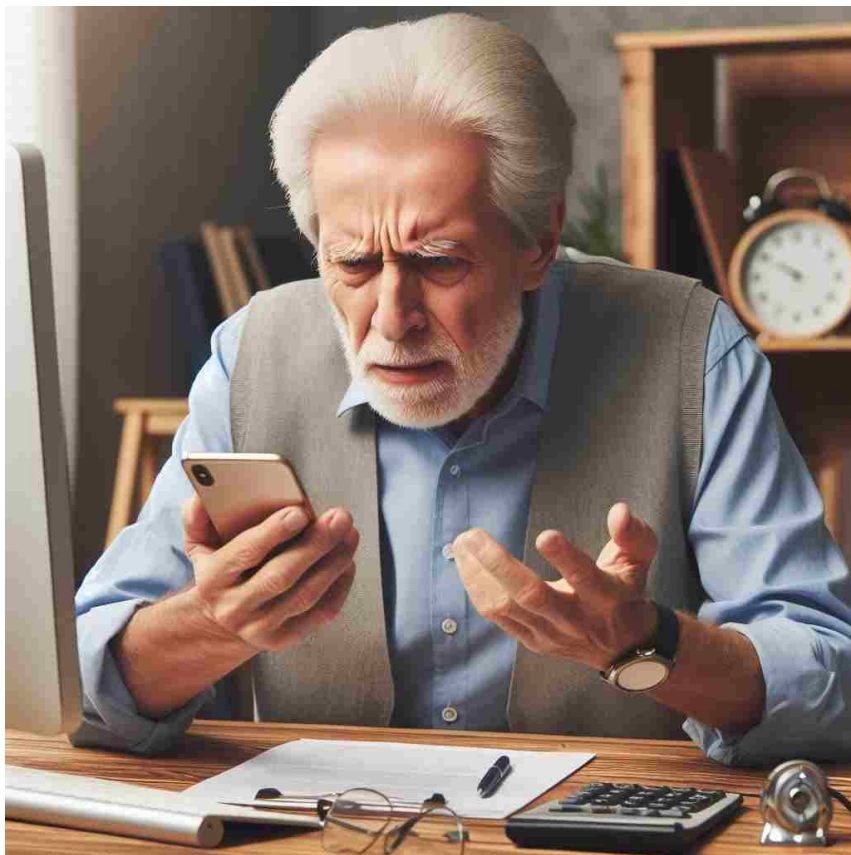
Además de permitirte generar contraseñas seguras, VPNMentor ofrece varias funcionalidades adicionales que te ayudan a mejorar la seguridad de tus claves:

1. **Personalización Avanzada:** podés elegir la longitud exacta de tu contraseña, desde 8 hasta 64 caracteres, y también decidir qué tipos de caracteres incluir, lo cual es útil para adaptarse a las

políticas específicas de cada plataforma o sitio web.

2. **Indicador de Fuerza de Contraseña:** a medida que generas una contraseña, VPNMentor te muestra qué tan fuerte es, basándose en su longitud y complejidad. Esto te da una buena idea de si tu contraseña es lo suficientemente segura o si necesita ajustes.
3. **Generación de Contraseñas Memorizables:** pero si preferís una contraseña más fácil de recordar, VPNMentor también te permite crear contraseñas que incluyan palabras reales, pero con suficiente complejidad para ser seguras, mezclando símbolos y números.
4. **Sin Registro:** no necesitas crear una cuenta ni registrarte para usar el generador, lo que añade una capa extra de privacidad. Tus contraseñas generadas no se almacenan en ningún servidor, lo cual asegura que solamente tú las conozcas.

¿Por qué VPNMentor es mejor que otros métodos manuales o aplicaciones parecidas?



El generador online de contraseñas de VPNMentor es mejor por varias razones:

- **Eficiencia y Facilidad de Uso:** mientras que crear contraseñas manualmente puede ser muy tedioso y propenso a errores, VPNMentor genera contraseñas en cuestión de segundos, eliminando el riesgo de olvidarse, de incluir todos los tipos de caracteres necesarios o de cometer errores durante la creación. Además, la interfaz es simple y accesible incluso para usuarios no tecnológicos.
- **Nivel de Seguridad Superior:** al ser completamente aleatorio y personalizado, el generador de VPNMentor crea contraseñas que están más allá del alcance de las técnicas comunes de adivinación de contraseñas, como ataques de diccionario o de fuerza bruta. Métodos manuales a menudo conducen a patrones predecibles, lo que reduce la seguridad.
- **Indicador de Fuerza:** muchos métodos manuales no permiten evaluar la seguridad de una contraseña de forma precisa. VPNMentor, en cambio, incluye un indicador que facilita a los usuarios determinar la solidez de sus contraseñas y realizar ajustes en tiempo real para fortalecerlas aún más.
- **Privacidad sin Compromiso:** a diferencia de algunos generadores en línea, VPNMentor **no requiere un registro ni almacena tus contraseñas**, lo que significa que no hay riesgo de que esta información pueda ser comprometida. Esta característica asegura que tú seas la única persona con acceso a tus contraseñas.

- **Accesibilidad Multiplataforma:** mientras que los métodos manuales dependen del contexto (por ejemplo, escribir una contraseña en una libreta), VPNMentor es accesible desde cualquier dispositivo, en cualquier lugar. Esto ofrece una comodidad significativa cuando se trata de generar contraseñas seguras sin importar dónde te encuentres.

En este video sobre el Generador de Contraseñas de vpnMentor, te muestro las características principales:

1. **Generación de Contraseñas:** la aplicación genera tantas contraseñas como necesitamos en el momento a crearlas.
2. **Añadir Etiquetas:** la herramienta permite añadir etiquetas (dato identificador de qué aplicación se trata) y nombres de usuario a las contraseñas, para aprovechar esta funcionalidad y organizar mejor las contraseñas.
3. **Personalización de Contraseñas:** a continuación te muestro cómo ajustar la longitud de la contraseña mediante un deslizador o campo de entrada y activar opciones como incluir letras mayúsculas, minúsculas, números y símbolos, como excluir caracteres ambiguos (ej., O y 0) y duplicados, o comenzar la contraseña con una letra para mejorar la legibilidad.
4. **Exportación de Contraseñas:** si ya definimos todas las características, usamos la funcionalidad para exportar las contraseñas generadas a un archivo CSV, importable, por ejemplo, en MS Excel (o similar) mostrando cómo se puede organizar y almacenar luego en otros sistemas.

Estas características y beneficios hacen que VPNMentor sea una herramienta valiosa y práctica, superando las limitaciones de métodos tradicionales y de otros generadores que no tienen en cuenta factores cruciales como la privacidad, facilidad de uso y personalización. ¡Así puedes estar seguro de que estás poniendo la mejor defensa posible frente a los ataques en línea!

Finalmente, yo creo que si queremos tomar medidas sobre como usamos y creamos nuestras contraseñas, comenzar con **vpnMentor** es una excelente opción, antes de tener que usar un generador de claves más sofisticado localmente en nuestro ordenador, como en mi caso se trata de **KeePassXC** ([+ info aquí](#))

Por favor, síguenos y danos «me gusta»:

