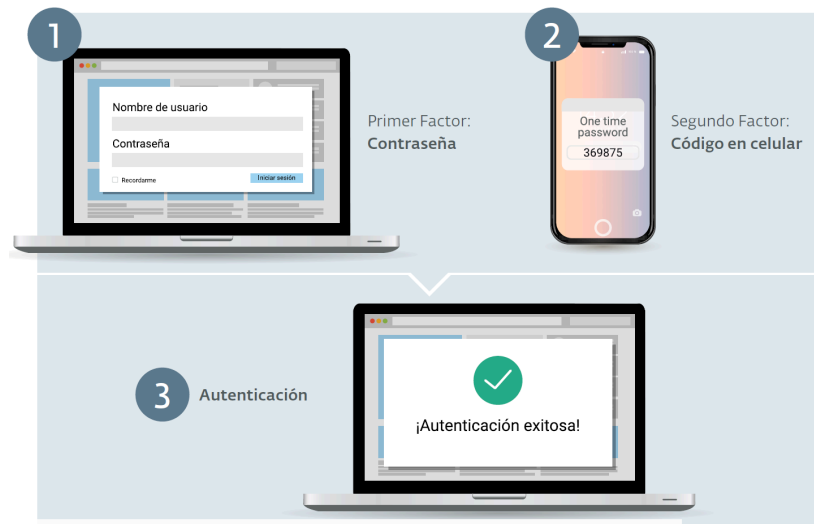


Mecanismo de autenticación



La autenticación es el proceso de verificar que algo o alguien es quien dice ser. En la actualidad existen varios métodos para llevar a cabo esta tarea, entre ellos podemos mencionar:

- Algo que el usuario sabe: contraseñas, PIN, patrón, etc.
- Algo que el usuario tiene: tarjeta de coordenadas, códigos de Token, USB keys.
- Algo que el usuario es: reconocimiento facial, dactilar, de iris, de voz, etc.



Contraseñas

Uno de los principales problemas de las personas que utilizan tecnología, es la cantidad de cuentas de usuario que deben administrar. Si se suman redes sociales, emails, homebanking, servicios en la nube, etc., probablemente estemos hablando de más de 15 cuentas.

Resulta muy complicado gestionar tanta cantidad de usuarios y más cuando los sistemas de seguridad piden cambiar las contraseñas con frecuencia, que además sean complejas y que no se repitan las últimas 6 - 12 utilizadas.

Este tipo de casos, genera finalmente situaciones poco seguras, como las siguientes:

- Se repite la misma clave en todos lados.
- Se almacenan, de forma errónea, en un lugar de fácil acceso.
- Dificultad para poder recordarlas

Sumado a lo antes mencionado, también existe otro problema que no es generado por los usuarios, sino por las empresas que prestan servicios. Los datos como el usuario y la contraseña, se almacenan en una base de datos; si esta no está protegida como corresponde, se corre el riesgo de que alguien la pueda vulnerar y robar los datos allí almacenados. Este tipo de incidentes de seguridad suceden con alta frecuencia. La última gran filtración de usuarios y contraseñas, Collection #1, dejó expuestas públicamente en Internet a más de 700 millones de cuentas y sus respectivas passwords.

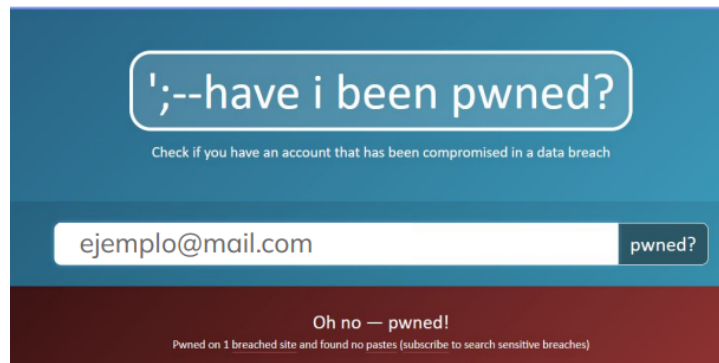
Conociendo esta situación, resulta vital poder tomar conciencia de la importancia que representa cuidar nuestras contraseñas en un medio tan hostil como es Internet.

Filtraciones de datos

Lo primero que vamos a hacer es verificar si hemos sido víctimas de una filtración, y si nuestros datos personales, como usuarios y contraseña, están públicos en Internet.

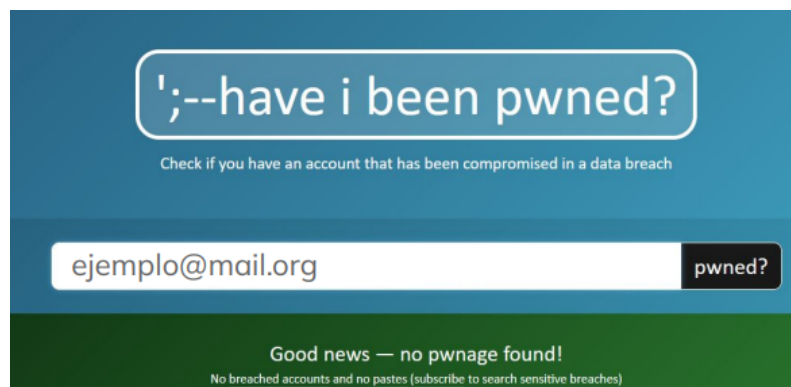
Para realizar esta comprobación utilizaremos el sitio haveibeenpwned.com. Una vez en la página, ingresamos nuestro correo electrónico y hacemos clic en el botón cuyo nombre es pwned?.

Si el resultado aparece en rojo, significa que se han filtrado datos personales en Internet. Bajando en la misma página podemos saber en qué plataforma o servicio ocurre y cuándo.



Si el resultado está en rojo, es muy importante cambiar la contraseña de ese correo y de todos aquellos servicios o plataformas donde estemos utilizando ese correo y su contraseña.

Si por el contrario, el resultado que aparece está en verde, significa que por el momento no hemos sido víctimas de una filtración de datos. Esto no implica que en un futuro lo podremos ser; por ese motivo, nos conviene regularmente verificar con esta plataforma si existen filtraciones o no de nuestras cuentas de correo.



Complejidad de las contraseñas

Algo a tener en cuenta sobre las contraseñas, es su robustez. Es necesario crear contraseñas que sean complejas, para evitar que un atacante pueda adivinarlas, u obtenerlas por medio de un ataque de fuerza bruta, o un diccionario. Cuanto más difícil sean, más compleja será la tarea de poder obtenerla, y así aseguraremos de manera correcta, nuestras cuentas de usuario.

Para que una clave sea compleja, tener en cuenta estas características:

- Tener más de 10 caracteres.
- Utilizar letras, números y caracteres especiales.
- Utilizar mayúsculas y minúsculas.
- No utilizar datos personales, tales como nombre, fecha, etc.

Una forma muy sencilla es diseñarlas a través de frases, en lugar de usar palabras sueltas. Por ejemplo, una clave compleja podría ser: Me gusta Soda Stereo. Ahí tenemos cuatro palabras, usamos mayúsculas, minúsculas, más de

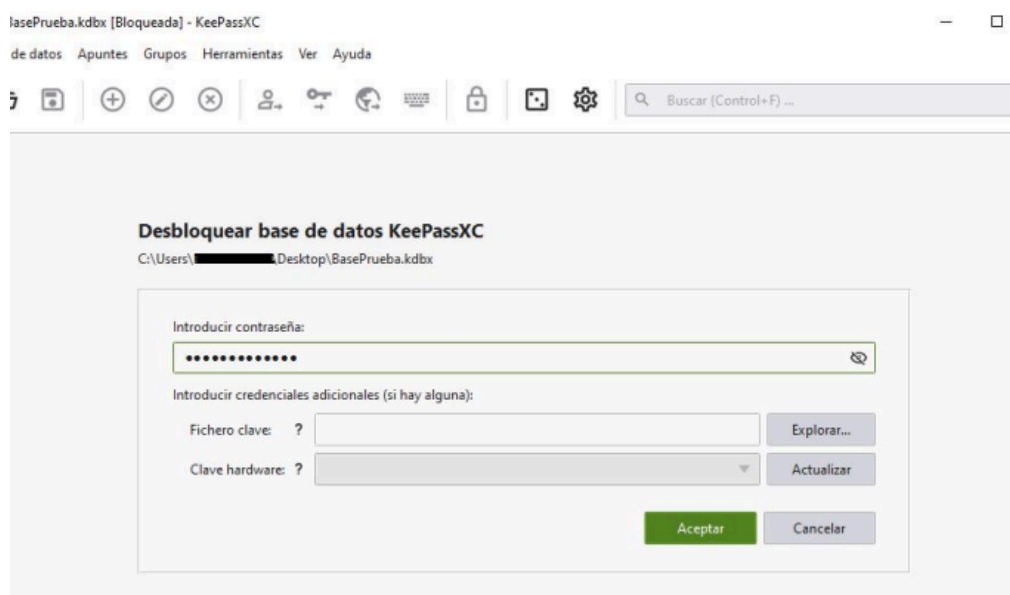
diez caracteres y encima tenemos caracteres especiales como el espacio. Crearlas de esta manera se vuelve muy fácil y resulta nada difícil de recordar.

Gestores de contraseñas locales y de nube

Además de crear contraseñas robustas, debemos pensar en cómo los usuarios manejarán tanta cantidad de contraseñas. Entonces, no podemos pedirle al usuario que recuerde o administre quince contraseñas y no repita la misma, o escribirlas en un papel y tenerlo cerca de su equipo. A fin de evitar estos problemas, podemos utilizar los Gestores de Contraseñas. Estos programas permiten almacenar passwords y guardarlos de forma segura; porque se crea una base de datos cifrada, la cual asegura el resguardo de las contraseñas y garantiza que se cumpla el principio de la confidencialidad. Existe una amplia gama de programas que cumplen esta función. Entre ellos, podemos mencionar alguno como: KeePass, LastPass, entre otros.

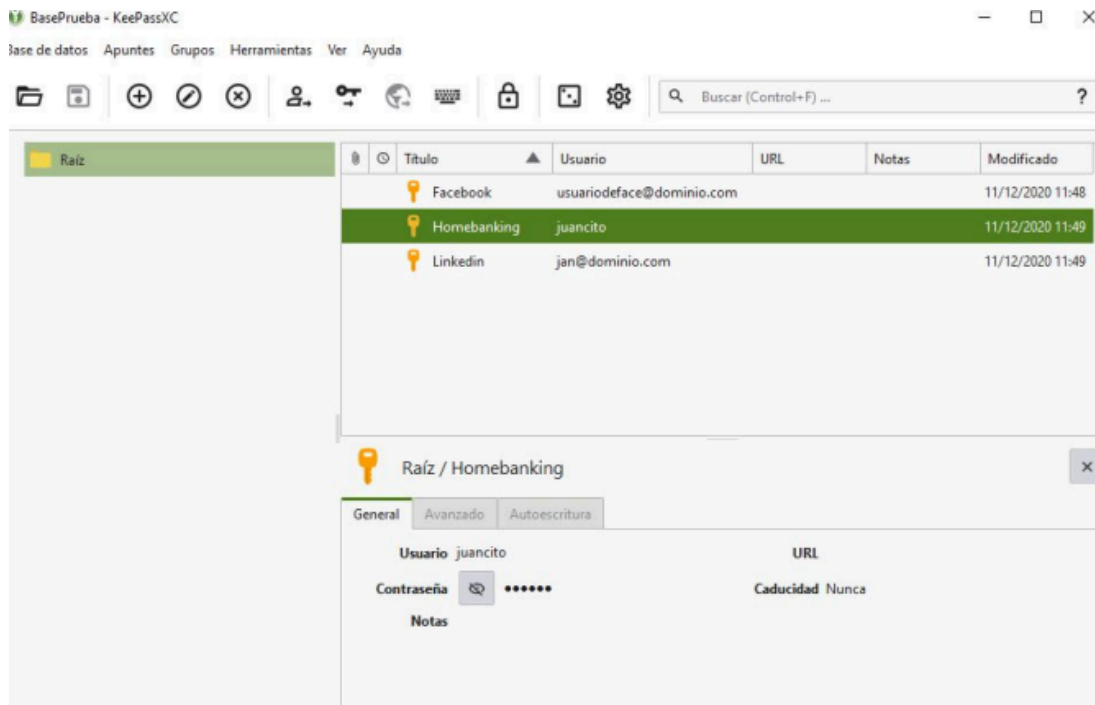
¿Cómo funciona? El programa solicita la creación de una contraseña “Maestra” la cual tendrá que ser muy robusta porque será la única que tendremos que utilizar para acceder a la base donde tenemos almacenadas el resto. Entonces, al ingresar esta contraseña, podemos usar las que están allí guardadas.

→ Ingreso al sistema con la contraseña “maestra”:



Femme Net- *Mecanismo de autenticación*

→ Base de Datos con los usuarios y contraseñas almacenados:



La base de datos podemos guardarla en nuestro dispositivo, tenerla en la nube, o en algún soporte como discos externos o pendrives y llevarlo al lugar donde lo necesitemos. Este programa posee una versión portable, lo cual permitiría que abramos la base desde cualquier computadora sin la necesidad de instalar el software. Para los usuarios será de gran utilidad ya que podrán almacenar allí todas sus contraseñas con una alta seguridad.

Autenticación de Dos Factores (2FA)

Si bien el uso de una contraseña robusta y de los gestores de contraseñas mejoran notablemente la forma de preservar nuestros datos personales, podemos igualmente ser víctimas de un ciberdelincuente que robe nuestras passwords e ingrese en nuestras cuentas de usuario.

Por ello, últimamente se ha implementado una medida adicional de seguridad que impide el ingreso ilegal por parte de delincuentes a nuestros datos. A este nuevo sistema de seguridad se le denomina 2FA – Autenticación de Dos Factores.

Su función es agregar una capa más de protección al solicitar además del usuario y contraseña, un código de token que se envía al dueño de la cuenta para que lo ingrese cuando vaya a iniciar sesión. Este token se envía a través de una aplicación móvil que tiene instalada el usuario y que tiene que colocar, si quiere ingresar en su cuenta o servicio donde lo quiera habilitar.

Existen muchas aplicaciones de 2FA en el mercado, entre las mejores podemos mencionar: LATCH, MICROSOFT AUTHENTICATOR, GOOGLE AUTHENTICATOR.

En caso de utilizar un 2FA, es recomendable hacerlo a través de alguna de las aplicaciones mencionadas y evitar, en la medida de lo posible, los códigos de token enviados por medio del SMS, ya que este es un canal de comunicación que no cifra los datos y podrían quedar expuestos a un tercero que los podría leer.