

¿Y SI YA TE HAN ROBADO LA CLAVE...Y NO LO SABES?



Proyecto P-45 "Audaz"



Buenas a todos ciber-navegantes. En esta entrega quería datos un consejo de seguridad que creo que puede ser muy útil de cara a vuestro día a día. ¡Y lo mejor de todo es que se trata de un servicio gratuito! Y se trata nada más y nada menos que una página web donde puedes **comprobar si te han robado la clave de alguno de tus servicios**, de forma que, si te sale que sí, puedes cambiarla lo antes posible...y antes de que sea demasiado tarde!: **Have I Been Pwned?** (<https://haveibeenpwned.com/>)

 La traducción del nombre de esta página es un tanto discutible. Pero podemos aceptar que significa algo como "¿Me han engañado?"

¿Qué es este servicio?

Y es que hoy os quiero hablar de algo un poco diferente y que además os puede dar un pequeño susto. Pero tranquilos, porque **eso os puede ahorrar un susto mayor más adelante**. Como seguramente habréis leído en la prensa, frecuentemente hay lo que se llaman filtraciones de datos.

 El 25 de Enero de 2024 se batió el récord de la filtración más grande de la historia, con 26.000 millones de cuentas de distintos servicios: <https://www.xataka.com/seuridad/acabamos-descubrir-mayor-filtracion-datos-historia-26-000-millones-cuentas-al-descubierto>.

Esto por desgracia les pasa cada vez a más empresas, a veces por no tener las medidas de seguridad adecuadas pero, aunque pueda parecer mentira, mucho más frecuentemente es **por un descuido de alguno de sus empleados**. Sí, no estoy de broma, de cada diez ataques se ha calculado que 8 se deben a algo que alguien ha hecho mal lo que, como dijimos en otras programadas, se traduce a que **ha hecho clic donde no debería**.

El caso es que esa filtración de datos lo que hace es robarle a una empresa un fichero con un montón de información personal de muchos de sus usuarios, entre los cuales podemos estar, por supuesto, nosotros. Eso es malo, porque lo más probable es que se publiquen datos personales que no son de conocimiento público en lugares accesibles a otros (entre ellos, delincuentes ☹). Pero uno de los peores efectos es que **se puede filtrar el nombre de usuario y clave de una cuenta de usuario que tengamos en esa empresa**.

🔍 Es muy malo que conozcan nuestro nombre completo, dirección, nº de NIF, etc. pero ahora imagínate que además conocen nuestro nombre de usuario (que probablemente usas el mismo en otros servicios) y nuestra contraseña (que también probablemente usas en otros servicios) 😞

¿Qué pasa cuando hay una filtración?

¿Quiere decir que la clave queda automáticamente descubierta cuando hay una filtración de datos? **no, no siempre ocurre eso**, pero la probabilidad aumenta bastante. Si, además, tenemos en cuenta que la mayoría de nosotros usamos la misma clave en muchos servicios, descubrir una clave le puede dar a un delincuente **la llave de las puertas de muchas cosas que tenemos**, y ahí es donde la situación se pone bastante más complicada.



¿Como es eso de que aunque roben la clave no saben la clave? A ver. **Una empresa seria nunca sabe la clave de tus cuentas**. Lo que sabe es un texto derivado de la misma que **se llama hash** (no intentes buscar la traducción de la palabra 😊). Este texto es “mágico”. Si yo meto la clave correcta, a la empresa le llega su hash. **Claves iguales generan hashes iguales**, por lo que la empresa sabe que he introducido la clave correcta. Pero ¿sabes lo que pasa? Es imposible obtener la cadena original a partir de su hash. Por eso, las empresas puedan saber si has introducido o no tu clave correctamente, pero no cual era. ¿A que es interesante? 😊

🔍 ¿Qué quiero decir con lo de “empresa seria”? Pues que **hay empresas que no lo son y guardan tu clave tal cual la introduces**. Huye de ese tipo de sitios. Si, por ejemplo, pides recordar tu clave y en lugar del típico enlace para recuperar la clave te envían tu clave tal cual por correo...¡no es un sitio serio! 😞

Esta es la razón por la cual **si se roba una hash no se sabe tu clave aún**. El delincuente tendría que probar todas las posibles claves hasta dar con la que genera la misma hash que tiene guardada. ¿Entiendes ahora por qué se insiste tanto en poner claves largas con caracteres variados? Una clave bien creada es un infierno en vida para los delincuentes: cuanto más compleja, más tiempo se tarde en averiguarla...

🔍 **Obviamente hay técnicas para averiguar claves que no son probar claves a lo bruto (por ese motivo a la técnica esta se le llama “fuerza bruta” 😊)** pero, sin meterme en temas técnicos, lo que he dicho se mantiene en general: **clave compleja, delincuente cuya máquina se hace vieja :P**

Para que entiendas que esto no es algo que digo por decir, en este enlace: <https://www.hivesystems.io/blog/are-your-passwords-in-the-green>, puedes ver que incluso con las máquinas más potentes de la actualidad, averiguar por fuerza bruta una contraseña en la actualidad que sea lo suficientemente fuerte es impracticable, como ves en esta imagen.

USING CHATGPT HARDWARE TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 secs
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hours	12 months	10 years	47 years
14	Instantly	1 days	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years



Learn how we made this table at hivesystems.io/password

¿Por qué esta página es importante?

Ahora que has llegado a este punto entenderás que aunque un delincuente tenga la hash y con ella no pueda hacer directamente nada, puede ser cuestión de tiempo que sí pueda hacerlo. Por eso, tiene bastante sentido que haya un servicio que nos avise de cuando nuestras claves se podrían haber filtrado, **para que las podamos cambiar**. ¡Y ese es del que vamos a hablar! 😊

Si accedes a esa página, que sepas que lo que hace es **recopilar y organizar todas las filtraciones de datos que se conocen hasta la fecha** y, por tanto, es capaz de decirte (gratis) si tu clave está en peligro. ¿Cómo? Pues porque asume que al registrarnos en cualquier sitio damos una cuenta de correo electrónico (seamos sinceros, ya todos los servicios la piden...). Si introducimos una cuenta de correo electrónico, entonces te dirá **si esa cuenta está asociada a alguna filtración que se haya producido históricamente**. Además te dice el servicio concreto, las circunstancias y cuánto hace de eso. Si hace mucho que no cambias la clave y ves, por las fechas que se ha filtrado, que puede estar en peligro... ¡cámmbiala cuanto antes!.

Cuando introduces una **cuenta sin filtraciones**, obtienes esto, que es lo ideal:

@uniovi.es

pwned?

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

Donate

En cambio, **cuando pones una que está asociada a filtraciones**, mira qué información te da. En este caso, como ves en la imagen te dice que ese email está asociado a una cuenta de *Dropbox* que se filtró en 2012 (¡hace mucho!) y que en su día la propia *Dropbox* forzó el cambio de contraseñas. Esta filtración no es por tanto realmente peligrosa, porque ya no debería tener afectados debido a las medidas que tomó la propia empresa (¡bravo por *Dropbox*, y bravo por esta web por darnos información tan completa!).

The screenshot shows a search result from the Pwned website. At the top, there's a blue header bar with a dark blue square icon on the left, followed by the text '@uniovi.es' and 'pwned?' on the right. Below the header, the main content area has a dark red background. In the center, it says 'Oh no — pwned!' in white. Below that, in smaller white text, it says 'Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)'. Underneath, there are social media sharing icons (Facebook, Twitter, Bitcoin, PayPal) and a 'Donate' button. A horizontal line separates this from the next section. Below the line, the heading 'Breaches you were pwned in' is in white. Underneath it, a small note says 'A "breach" is an incident where data has been unintentionally exposed to the public.' To the left of the breach details is a blue icon of the Dropbox logo. The breach details themselves are in white text: 'Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt). Compromised data: Email addresses, Passwords'

🔍 **Si no entiendes inglés, recuerda que le puedes pedir a los navegadores que te traduzcan automáticamente la página. ¡Y gracias a la IA hoy en día lo hacen muy bien! 😊**

Por supuesto, el problema se agrava si hay muchos servicios con contraseñas filtradas, la información que da el servicio atacado no es muy buena, no nos acordamos de haberla creado y, lo que es peor, aparecen servicios en los que no hemos creado una cuenta pero la ha creado por nosotros otro servicio que lo usa “por debajo”, pero sin darnos cuenta. Es el caso de la siguiente imagen, donde el dueño de la cuenta **no recordaba** haber creado un usuario en un servicio llamado *Cit0day* ni en *Gravatar*. En el caso del segundo, resultó que se debía a haber creado una cuenta en otra página, pero del primero aún está buscando de dónde ha salido...

🔍 **Por casos como estos es importante entender por qué se da el consejo de usar claves distintas en cada sitio, o al menos en servicios que consideremos importantes, además de activar el segundo factor de autenticación (que muchos conocemos por la aplicación de los números del móvil que tienes que meter cuando te los piden 😊, pero de eso hablamos otro día).**

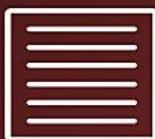
Oh no — pwned!

Pwned in 2 data breaches and found no pastes (subscribe to search sensitive breaches)

[!\[\]\(2e897e890e69d81eae4503a8342c36b0_img.jpg\)](#) [!\[\]\(ce4e2504c7100a62a9a9496b2e01b6e4_img.jpg\)](#) [!\[\]\(d6653e1cf2c96f17cfd897a08e4b2bd5_img.jpg\)](#) [!\[\]\(2a4acc7e9f5aa18684d23855a44c15c0_img.jpg\)](#) [Donate](#)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public.



Cit0day (unverified): In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords



Gravatar: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars. 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an FAQ detailing the incident.

Compromised data: Email addresses, Names, Usernames

¿Tengo que andar mirando todo el día?

¡Qué va! De hecho la propia página tiene un servicio donde si le das un correo **te notificará si hay una filtración asociada al mismo** en cuanto la conozca, para que estés informado y te olvides de mirar cada poco, que no es práctico 😊

 [Home](#) [Notify me](#) [Domain search](#) [Who's been pwned](#) [Passwords](#) [API](#) [About](#) [Donate !\[\]\(01c7efd7015ff5bee40ce18a2d741282_img.jpg\) !\[\]\(f9527c4f594db100cb0abd62ebbd461e_img.jpg\)](#)

Notify me

Subscribe to breach notifications

Get notified when future pwnage occurs and your account is compromised.

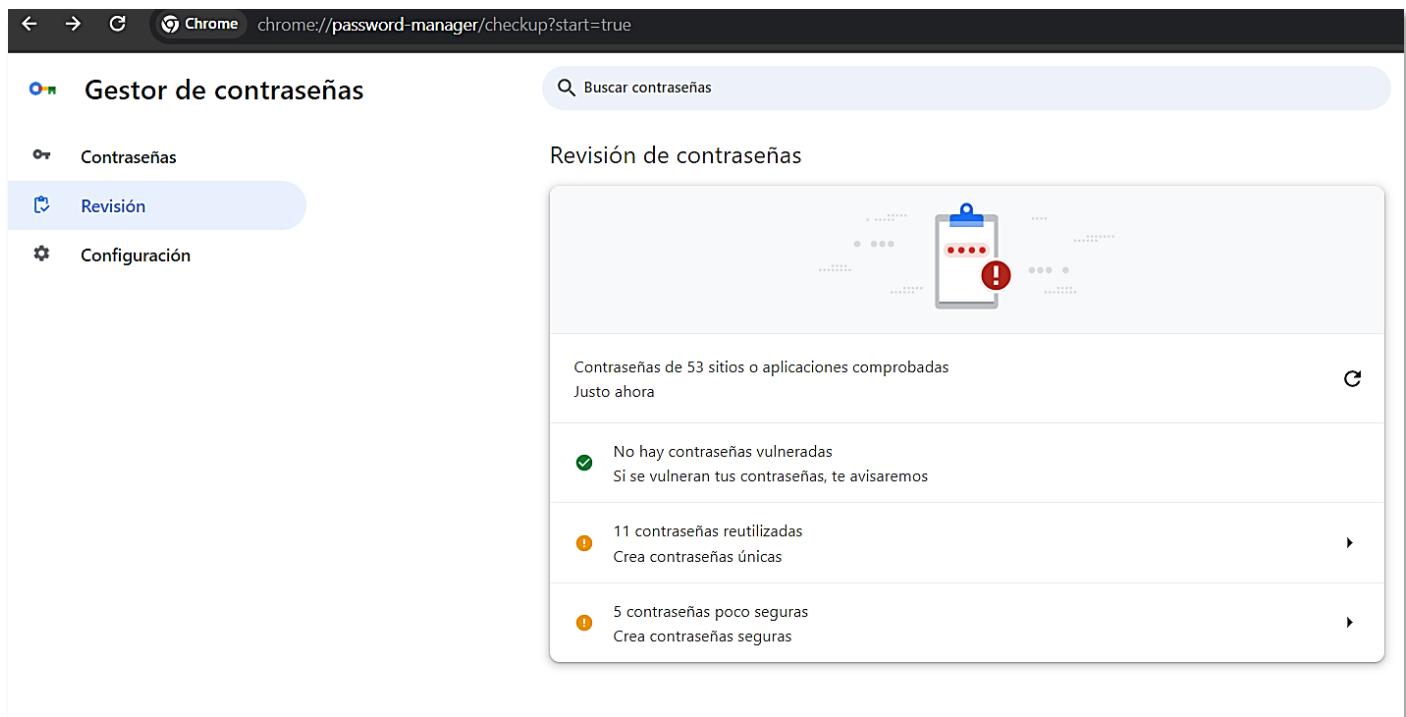
No soy un robot 
reCAPTCHA
Privacidad - Términos

Using Have I Been Pwned is subject to the [terms of use](#)

[notify me of pwnage](#)

Por cierto, si esta web no te gusta por lo que sea, que sepas que los navegadores tienen ya funciones parecidas. Por ejemplo, *Google Chrome* tiene esta opción en su **Gestor de Contraseñas**, en el apartado de revisión.

 **Muchas veces te informa aunque no lo mires, así que si tu navegador te da un aviso de esto ¡hazle caso!**



The screenshot shows the 'Revisión de contraseñas' (Password Review) section of the Google Chrome password manager. It displays a summary of 53 checked sites and provides three main findings:

- No hay contraseñas vulneradas (No vulnerable passwords). A note says: Si se vulneran tus contraseñas, te avisaremos (If your passwords are compromised, we'll alert you).
- 11 contraseñas reutilizadas (11 reused passwords). A note says: Crea contraseñas únicas (Create unique passwords).
- 5 contraseñas poco seguras (5 weak passwords). A note says: Crea contraseñas seguras (Create strong passwords).

¿Esta página puede poner en riesgo mi privacidad?

Pues lamento decirte que sí...y te lo puedo explicar fácilmente. Nada impide que **yo pueda poner ahí el correo de quien quiera**, ya que no se comprueba que el correo que pongo sea mío. Esto puede dar lugar a que si pongo un correo de alguien que ha sido filtrado en varios sitios, pueda saber que **ese correo se ha usado para registrarse en esos sitios**.

¿Qué pasa si esos sitios son, digamos, "inadecuados"? (aplicaciones de citas donde se supone que no se debería estar, servicios de la competencia, ...). Es un problema porque no podemos evitar que esa información salga en esos registros (son filtraciones) y cualquiera podría usar esta información para saber cosas sobre nosotros....

 **Piénsalo bien, seguro que a poco que le des una vuelta se te ocurre una combinación de cosas que puede llevar fácilmente a una extorsión... 😱**

Por tanto, paradójicamente un servicio anti-filtraciones **puede acabar siendo un servicio que haga filtraciones**, aunque no de contraseñas...pero si de cosas de nuestra vida personal. Mira por ejemplo esta imagen, que revela que una cuenta se ha registrado en un servicio de correo ruso (a saber por qué), en una editorial que tiene sospechas de tener revistas con prácticas editoriales cuestionables y en VK (V-Kontakte, una especie de Facebook ruso). Si lo piensas bien, es información de una persona que de otra forma no se podría saber fácilmente...



discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post [The 773 Million Record "Collection #1" Data Breach](#).

Compromised data: Email addresses, Passwords

dailymotion

dailymotion: In October 2016, the video sharing platform Dailymotion suffered a data breach. The attack led to the exposure of more than 85 million user accounts and included email addresses, usernames and bcrypt hashes of passwords.

Compromised data: Email addresses, Passwords, Usernames



Exploit.In (unverified): In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read [Password reuse, credential stuffing and another billion records in Have I Been Pwned](#).

Compromised data: Email addresses, Passwords

@mail.ru

mail.ru Dump (unverified): In September 2014, several large dumps of user accounts appeared on the Russian Bitcoin Security Forum including one with nearly 5M email addresses and passwords, predominantly on the mail.ru domain. Whilst unlikely to be the result of a direct attack against mail.ru, the credentials were confirmed by many as legitimate for other services they had subscribed to. Further data allegedly valid for mail.ru and containing email addresses and plain text passwords was added in January 2018 bringing to total to more than 16M records. The incident was also then flagged as "unverified", a concept that was introduced after the initial data load in 2014.

Compromised data: Email addresses, Passwords



MDPI: In August 2016, the Swiss scholarly open access publisher known as MDPI had 17.5GB of data obtained from an unprotected Mongo DB instance. The data contained email exchanges between MDPI and their authors and reviewers which included 845k unique email addresses. MDPI have confirmed that the system has since been protected and that no data of a sensitive nature was impacted. As such, they concluded that notification to their subscribers was not necessary due to the fact that all their authors and reviewers are available online on their website.

Compromised data: Email addresses, Email messages, IP addresses, Names



Twitter (200M): In early 2023, over 200M records scraped from Twitter appeared on a popular hacking forum. The data was obtained sometime in 2021 by abusing an API that enabled email addresses to be resolved to Twitter profiles. The subsequent results were then composed into a corpus of data containing email addresses alongside public Twitter profile information including names, usernames and follower counts.

Compromised data: Email addresses, Names, Social media profiles, Usernames



VK: In approximately 2012, the Russian social media site known as VK was hacked and almost 100 million accounts were exposed. The data emerged in June 2016 where it was being sold via a dark market website and included names, phone numbers email addresses and plain text passwords.

Compromised data: Email addresses, Names, Passwords, Phone numbers

Y ese es mi consejo de hoy. Tengo además que insistir en que hay que tener mucho cuidado con dónde se pone la dirección, porque los malos se la saben todas **y han hecho copias falsas de esta página** con nombres muy parecidos, para robarte precisamente la clave. La página real **solo te va a pedir tu dirección de correo electrónico y nada más**, y en función de lo que te salga pues ya sabes si tienes o no que actuar. Y recuerda, **¡Que corra la voz!**

¡Y esto es todo! Muchas gracias y... ¡nos vemos en la próxima entrega!

Y recuerda amigo/a, una cuenta filtrada es un problema potencial, ¡así que cambia la clave cuanto antes no vaya a ser que seas presa del mal!



¿Quieres escuchar como hablo de esta estafa en menos de 5 minutos?



- [Escúchalo en IVOOX](#)
- [Escúchalo en Amazon Podcast](#)
- [Escúchalo en YouTube](#)
- [¿Tienes otro cliente de Podcast? Este es el feed RSS](#)

¿Quieres saber enlaces relacionados?



- El servicio *Have I been pwnd?* <https://haveibeenpwned.com/>
- *Dehashed*, un servicio parecido pero de pago: <https://www.dehashed.com/>

Este documento usa material generado con IA²



¹ Audio emitido en "Más de Uno". 95.2 Onda Cero Oviedo (<https://www.ondacero.es/emisoras/asturias/oviedo/directo/>) el 19/12/2022

² Las imágenes del texto del documento han sido generadas con la IA *Bing Chat*