

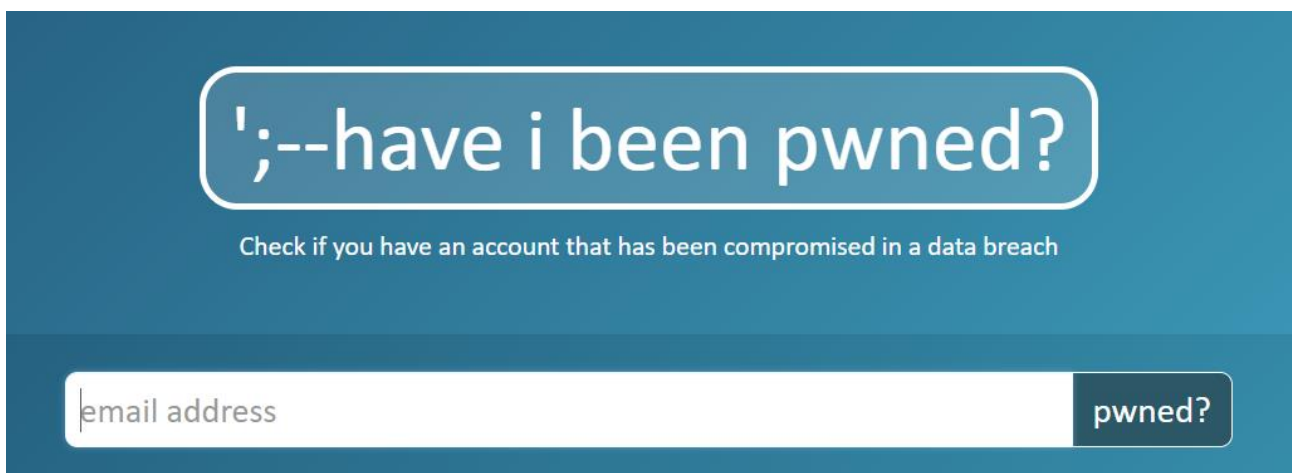
Cómo saber si tu email ha sido hackeado



Seguro que en alguna ocasión te has preguntado si alguien más tiene o ha tenido acceso a tu cuenta de **correo electrónico**, y es que hoy en día es muy importante tener protegidas nuestras cuentas para evitar que alguien más pueda acceder a datos personales y confidenciales. Para que podáis comprobar si vuestra cuenta ha sido hackeada, hoy en nuestro White Paper veremos algunas herramientas que podemos utilizar para tal fin.

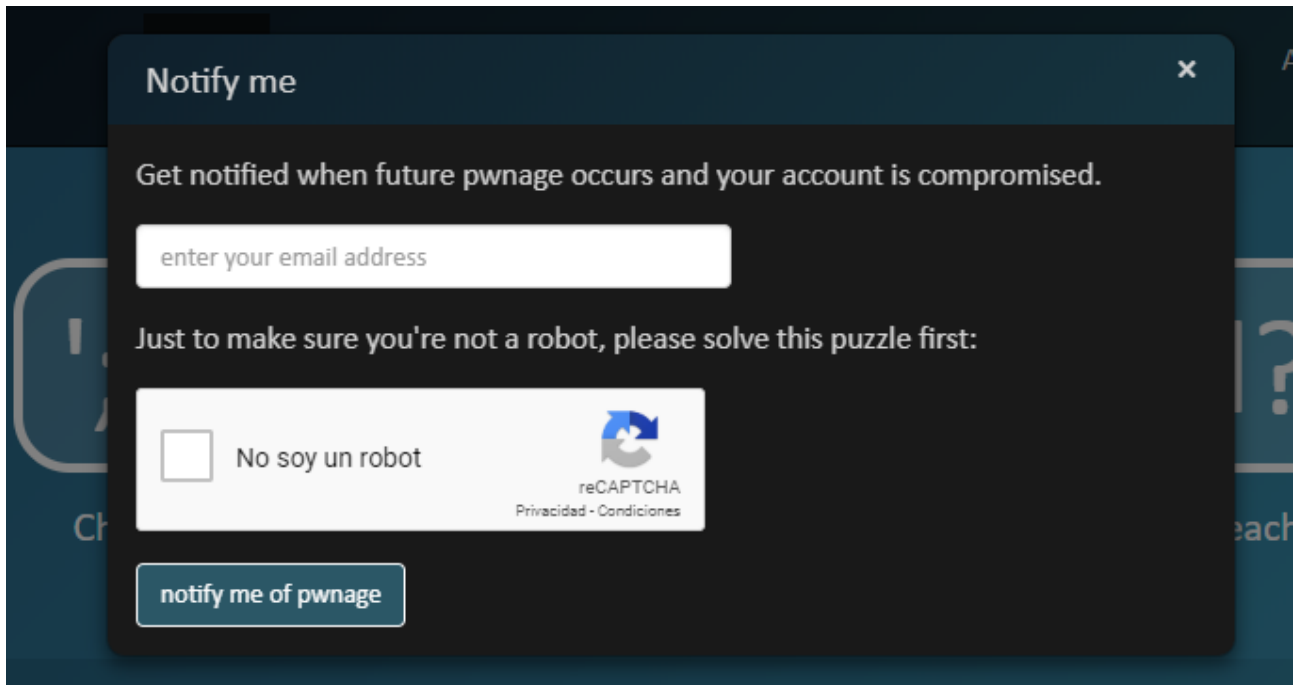
Antes de ponernos a repasar las distintas **páginas web** a las que podemos acudir para asegurarnos de que no hemos sido hackeados, es importante resaltar que el hecho de que no aparezca nuestra dirección de email en estas herramientas no significa que nuestros datos estén a salvo. También es importante destacar que son los propios usuarios los que deben preocuparse de mantener a raya la seguridad de sus cuentas.

Have I Been Pwned?

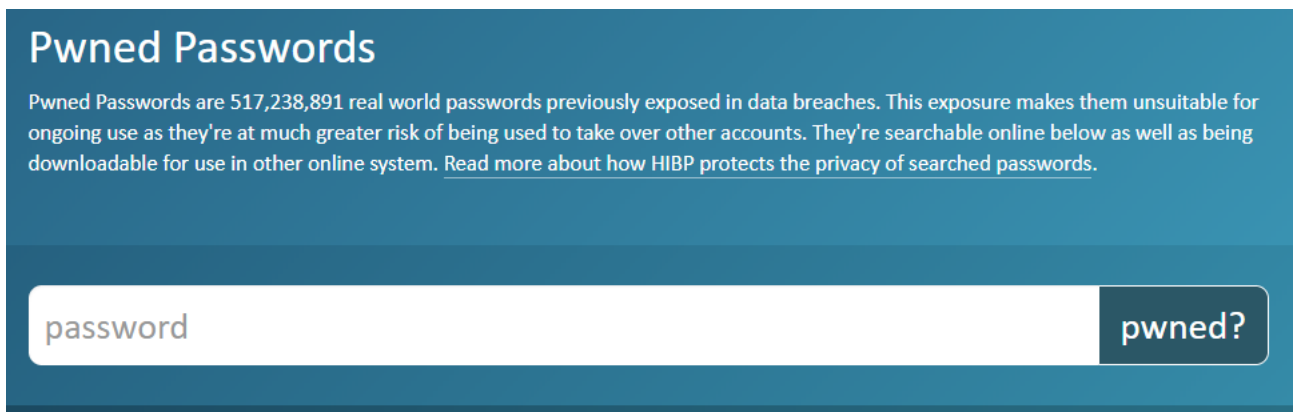


Para muchos expertos en seguridad, **Have I Been Pwned?** es la herramienta más precisa para determinar si nuestra cuenta de correo electrónico ha podido ser hackeada en alguna ocasión debido a que para su desarrollo se ha volcado las listas de webs Anti Public y Exploit.in. El procedimiento de evaluación de esta web funciona sobre la base de numerosos fallos de seguridad de sitios reconocidos. Su funcionamiento es muy sencillo. Únicamente tienes que indicar tu dirección de email y esperar unos segundos para que la web te muestre información sobre su seguridad.

En el caso de que tu cuenta sea segura, la web te mostrará una etiqueta de color verde informando que tus datos no aparecen en la base de datos. En el caso de que hayas sido hackeado, la base de datos arrojará una advertencia de color rojo que te indica que es probable que alguien esté accediendo a tus datos con malas intenciones, informando de los posibles problemas.



Otra de las funciones interesante que nos ofrece este portal, está la opción de recibir notificaciones cuando en un futuro nuestra cuenta haya sido comprometida. Mientras que no recibamos ningún aviso por su parte, todo irá bien.



Por último, destacar la función que nos permite conocer si la contraseña que estamos utilizando es segura comparándola con las almacenadas en base de datos y que han sido hackeadas en alguna ocasión.

BreachAlarm

my email address OR

El funcionamiento de la página web [Breachalarm](#) es muy similar al caso visto anteriormente. Una vez que el usuario indica su dirección de correo electrónico, la herramienta empieza una búsqueda en su base de datos para determinar si la cuenta ha sido comprometida en alguna ocasión. La información que almacena en su base de datos es obtenida de buscar en las “profundidades de Internet”, donde se suele negociar con este tipo de información.

En el caso de que nuestra cuenta aparezca en su base de datos, nos informarán mediante un cuadro como el que os dejamos a continuación.

X Password compromised!

A password associated with your email address has been compromised at least 2 time(s). The most recent recorded incident is June 16, 2016.


You should change any of your passwords that you created before this date as soon as possible. Do not reuse the same password across multiple sites!

Al igual que el caso anterior, ofrece la posibilidad de suscribirnos a un servicio de notificación que se encargará en un futuro de avisarnos cuando alguien publique la contraseña de nuestra cuenta en la red. De esta forma podremos actuar de forma inmediata para evitar cualquier tipo de problema. Aquí hay que decir que ofrecen un servicio gratuito para una cuenta pero también planes de pago para monitorizar varias direcciones.

Over 150 million users had their passwords hacked this past year.

How many of your employees were among them?

We scan the Internet for stolen password data posted by hackers, and let you know if we spot any of your company's email addresses in a security breach.



my domain (mycompany.com) **Check Now** OR [Notify me of password hacks affecting my staff: Business Watchdog Plans & Pricing](#)

Otra de sus características está destinada a las empresas. Desde esa sección podrás registrar y controlar el **dominio** de tu empresa. De esta forma es posible identificar cuántas cuentas de correo de los empleados se han visto afectadas.

X Password compromised!

A password associated with one of your company's email addresses has been compromised at least 2 time(s). The most recent recorded incident is August 30, 2016.

Your employees should change any passwords that they created before this date as soon as possible. Do not reuse the same password across multiple sites. [Contact us](#) if you would like assistance identifying the specific address or addresses that have been compromised.

Al igual que el caso anterior, si alguna cuenta ha sido comprometida nos mostrará información de ello, aunque para determinar qué cuentas han podido sufrir el problema habrá que pasar por caja.

Identity Leak Checker

Accounts	Leaks	Leaked accounts per day
5,973,309,472	801	901,035

Is someone spying on you?

Everyday personal data is stolen in criminal cyber attacks. A large part of the stolen information is subsequently made public on Internet databases, where it serves as the starting point for other illegal activities.

With the HPI Identity Leak Checker, it is possible to check whether your email address, along with other personal data (e.g. telephone number, date of birth or address), has been made public on the Internet where it can be misused for malicious purposes.

The email address you have entered will only be used for searching in our database and, when applicable, to subsequently send an email notification. It will be saved in an obfuscated way to protect you from potential email spam and is never given to a third party.

[Check email address!](#)

Identity Leak Checker cuenta con una amplia base de datos donde tiene almacenada información sobre los robos que se han llevado a cabo, actualizándose continuamente. Al igual que los casos anteriores, deberemos indicar nuestra cuenta de correo electrónica para que empiece la búsqueda. A diferencia de las anteriores, el resultado será enviado por correo electrónico.

The following sensitive information was freely found on the Internet in connection with your e-mail address:

Affected Service	Date	Verified	Affected users	Password	First and last name	Date of birth	Address	Telephone number	Credit card	Bank account details	Social security number	IP Address
taringa.net	Aug. 2017	✓	28,212,120	Affected	-	-	-	-	-	-	-	-
Combolist	Feb. 2017		28,341,234	Affected	-	-	-	-	-	-	-	-
Unknown (Anti-Public Combolist Jan. 2017)	Jan. 2017		948,385,599	Affected	-	-	-	-	-	-	-	-
Unknown (Exploit.in Compilation)	Aug. 2016		686,582,779	Affected	-	-	-	-	-	-	-	-
twitter.com	Jun. 2016		26,119,857	Affected	-	-	-	-	-	-	-	-
linkedin.com	Jun. 2012	✓	160,144,040	Affected	-	-	-	-	-	-	-	-

Además de indicarnos si nuestra cuenta ha sido hackeada, también nos indica si nuestra información personal ha sido publicada o utilizada de forma indebida en la red: nuestro número de teléfono, tarjeta de crédito, cuenta bancaria...

¿Cómo evitar que mi correo sea hackeado?

Las herramientas que hemos visto, muestran información muy fiable que nos permiten comprobar si nuestra cuenta de correo ha sido hackeada alguna vez. Pero como ya comentamos al principio, que no aparezca en estos listados no significa que esté comprometida.

Para mayor seguridad, y antes cualquier situación anómala, lo más recomendable es realizar un cambio de contraseña lo antes posible. Esta nueva contraseña debería estar compuesta por letras, números y símbolos para mayor tranquilidad. También es muy recomendable utilizar un [gestor de contraseñas](#) donde guardar todas las que gestionamos. Y lo más importante, cambiarla cada cierto tiempo.