Comment vérifier si vos données personnelles ont été piratées

Pour vérifier si vos données personnelles (compte courriel ou site internet) ont été piratées, la solution la plus connue est sans doute https://haveibeenpwned.com (HIBP), un site Web disponible uniquement en anglais mais facile à utiliser. Vous pouvez y inscrire votre adresse courriel pour la faire vérifier et celui-ci vous indiquera si votre adresse électronique a été trouvée dans une quelconque violation de données, laquelle et quand. **La procédure de contrôle se base sur de nombreuses violations de données connues des grands sites Web** - plus de 670 sites différents et 12,5 milliards d'adresses piratées figurent déjà dans la base de données.

Si votre adresse courriel a été piratée, vous devez immédiatement **changer votre mot de passe ainsi que pour tous les autres comptes des sites internet mentionnés par HIBP qui utilisent le même mot de passe** ou un mot de passe similaire. On vous conseille également de rechercher les logiciels malveillants sur votre ordinateur (voir le lien).

Pour maximiser vos chances d'être en sécurité, **vous devriez régulièrement consulter le service HIBP** pour vérifier si votre adresse électronique a été exposée lors d'autres violations de données, et ainsi prendre rapidement les mesures nécessaires pour protéger votre identité et votre vie privée en ligne.

Ci-dessous un exemple avec mon adresse courriel qui a été piraté plusieurs fois, la première fois en 2008 auprès de Myspace. Bien entendu j'ai changé plusieurs fois mon mot de passe pour l'adresse courriel et pour les sites internet mentionnés par HIBP.

[redacted]i@bluewin.ch pwned?

Oh no — pwned!

Pwned in 8 data breaches and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Start using 1Password.com

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

Why 1Password?

Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

MySpace: In approximately 2008, MySpace suffered a data breach that exposed almost 360 million accounts. In May 2016 the data was offered up for sale on the "Real Deal" dark market website and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowercase and stored without a salt. The exact breach date is unknown, but analysis of the data suggests it was 8 years before being made public.

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

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

Collection #1 (unverified): In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was 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

Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

LinkedIn Scraped Data (2021): During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on An update on report of scraped data.

Compromised data: Education levels, Email addresses, Genders, Geographic locations, Job titles, Names, Social media profiles