

Vérifier si les mots de passe de comptes en ligne ont été piratés

Vous voulez savoir si les mots de passe que vous utilisez sur Android ou Google Chrome ont déjà été piratés ? Une nouvelle fonctionnalité de Google vous permet de le vérifier en deux clics. Voici comment obtenir facilement la liste de vos mots de passe compromis.

- [Vérifier la sécurité de vos comptes avec le Gestionnaire de mots de passe de Google](#)
- [Comprendre les résultats de la vérification de vos mots de passe par Google](#)
- [Utiliser un autre service web pour vérifier si vos mots de passe sont compromis](#)

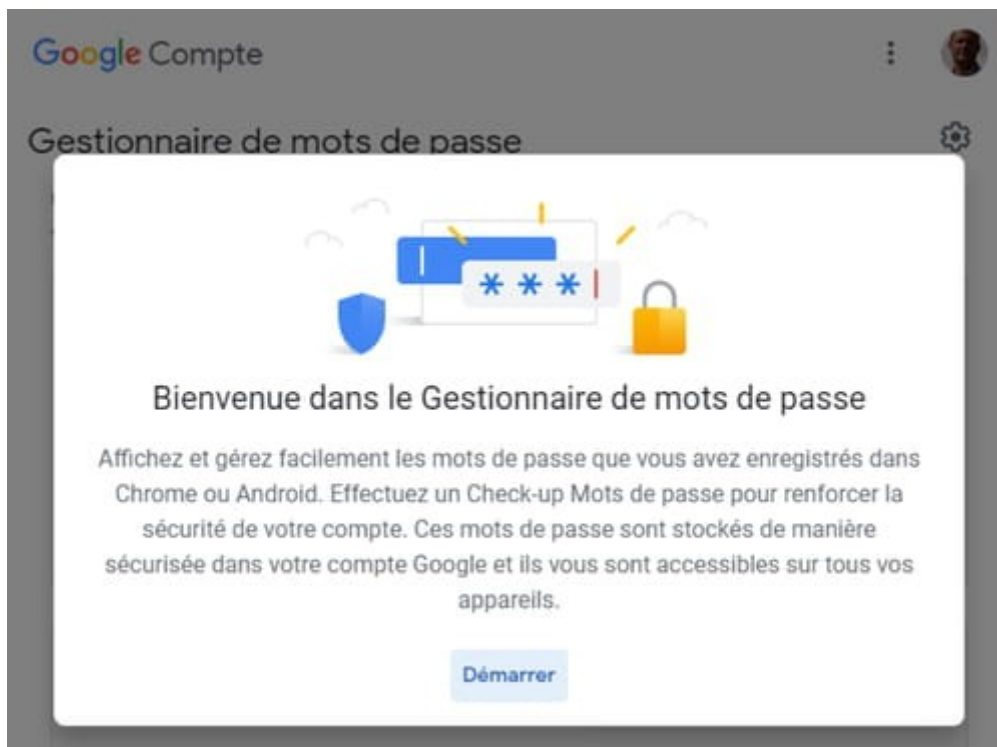


Les techniques des pirates sont toujours plus sophistiquées. [Phishing](#), piratage de services Web, applications infectées ou malwares cachés dans des logiciels... La liste est longue et il est de plus en plus difficile de protéger ses différents comptes en ligne (messagerie et autres services).

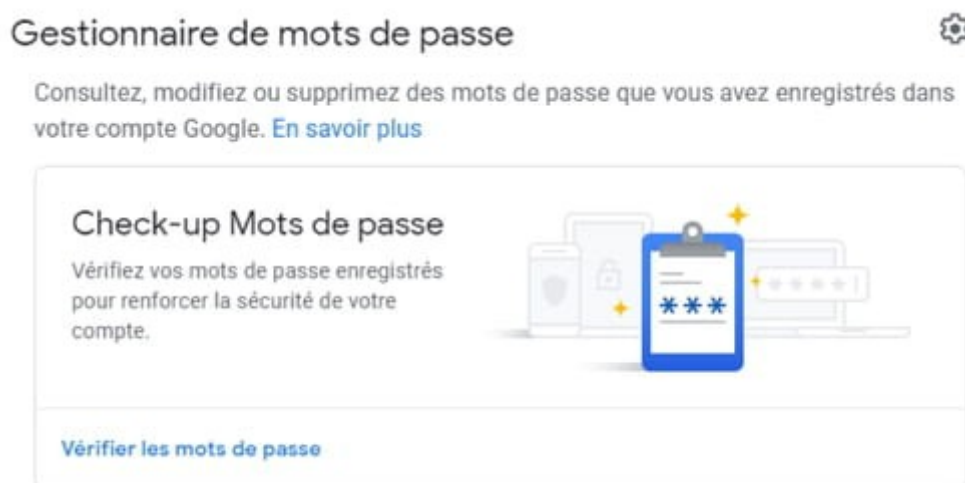
Vous avez donc tout intérêt à vérifier régulièrement que vos précieux sésames n'ont pas été compromis dans l'un des piratages massifs de services en ligne régulièrement repérés par les experts en cybersécurité.

C'est pour faciliter cette vérification que Google a ajouté une nouvelle fonction dans le gestionnaire de [mots de passe](#) intégré à Chrome et Android. L'outil permet de savoir si un identifiant de connexion sauvegardé dans le navigateur Web ou sur Android est toujours sécurisé, ou si vous devez en changer sans attendre.

Vérifier la sécurité de vos comptes avec le Gestionnaire de mots de passe de Google



- Ouvrez Chrome et rendez-vous sur le **Gestionnaire de mots de passe** du navigateur en saisissant l'adresse <https://passwords.google.com> dans le champ d'URL.
- Cliquez sur **Démarrer** pour accéder à la fonction de vérification de vos mots de passe.



- Cliquez sur **Vérifier les mots de passe** dans la rubrique **Check-up Mots de passe** en haut d'écran.

- Si vous utilisez l'outil de vérification de mots de passe pour la première fois, Google vous demande de confirmer votre identité : saisissez le mot de passe de votre compte Google et cliquez sur **Vérifier**
- A ce moment-là, Google compare vos mots de passe enregistrés dans le gestionnaire avec l'ensemble des bases de données d'identifiants compromis. Et en quelques secondes, le résultat s'affiche.


Comprendre les résultats de la vérification de vos mots de passe par Google

Si Google indique qu'aucun de vos mots de passe n'est piraté, félicitations : vous avez réussi à passer à travers tous les piratages repérés à ce jour.

Dans le cas contraire, Google vous indique trois niveaux de compromission pour chaque mot de passe :



- en rouge, vos **mots de passe piratés**. Cliquez sur la **flèche vers le bas** pour obtenir la liste de tous les comptes et pour les modifier sans attendre.

 **2 mots de passe piratés** 

Modifiez ces mots de passe maintenant

Les comptes suivants utilisent des mots de passe qui ont été compromis par une violation des données tierce. Modifiez ces mots de passe immédiatement pour protéger vos comptes. [En savoir plus](#)

La sécurité de ce compte est compromise

 paypal.com
paypal.com
paypal.com@gmail.com
lucylorenz@protonmail.com
lucylorenz@gmail.com



 [Modifier le mot de p...](#) 

La sécurité de ce compte est compromise

 http://10.5.50.1
http://10.5.50.1
http://10.5.50.1
pass:1
quest

 [Modifier le mot de p...](#) 


- dans la rubrique **La sécurité de ce compte est compromise**, cliquez sur le bouton **Modifier le mot de passe** pour accéder au service et changer votre mot de passe immédiatement.



 **293 mots de passe réutilisés** 


Créez des mots de passe uniques



Afin de mieux vous protéger, choisissez un mot de passe différent pour chaque site ou application. Si quelqu'un découvre un mot de passe que vous utilisez pour plusieurs comptes, il pourra s'en servir pour se connecter à ces derniers.


Le même mot de passe est utilisé sur 120 sites ou applications



 56789.com
56789.com
56789.com@protonmail.com

 [Modifier le mot de p...](#) 

 Tredias - Tr... les Tr... & Re...
Tredias - Tr... les Tr... & Re...
Tredias - Tr... les Tr... & Re...

 [Modifier le mot de p...](#) 

 Vive la France
Vive la France
Vive la France

 [Modifier le mot de p...](#) 

- en jaune, Google vous alerte sur vos **mots de passe réutilisés**. Cliquez sur la **flèche vers le bas** pour obtenir la liste de tous ces comptes pour lesquels vous utilisez toujours le même mot de passe. Par mesure de précaution, il est recommandé d'utiliser un mot de passe différent pour chaque service. Cliquez sur le bouton **Modifier le mot de passe** pour accéder au service et changer votre mot de passe immédiatement.

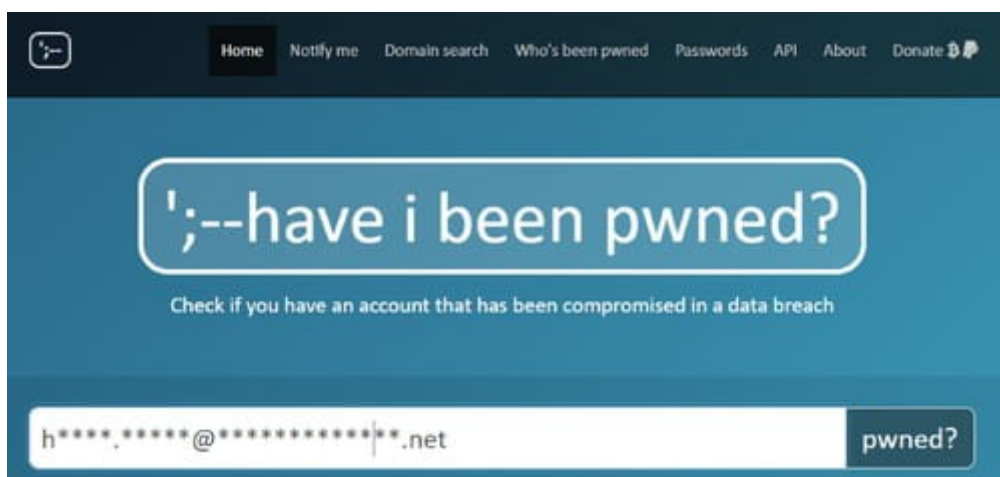


- enfin, Google liste vos **comptes qui utilisent un mot de passe peu sécurisé**. Les identifiants peuvent être facilement devinés par des algorithmes de piratage et Google vous conseille de les modifier. Cliquez sur la **flèche vers le bas** pour obtenir la liste et sur le bouton **Modifier le mot de passe** pour accéder au service et renforcer votre mot de passe.

Utiliser un autre service web pour vérifier si vos mots de passe sont compromis

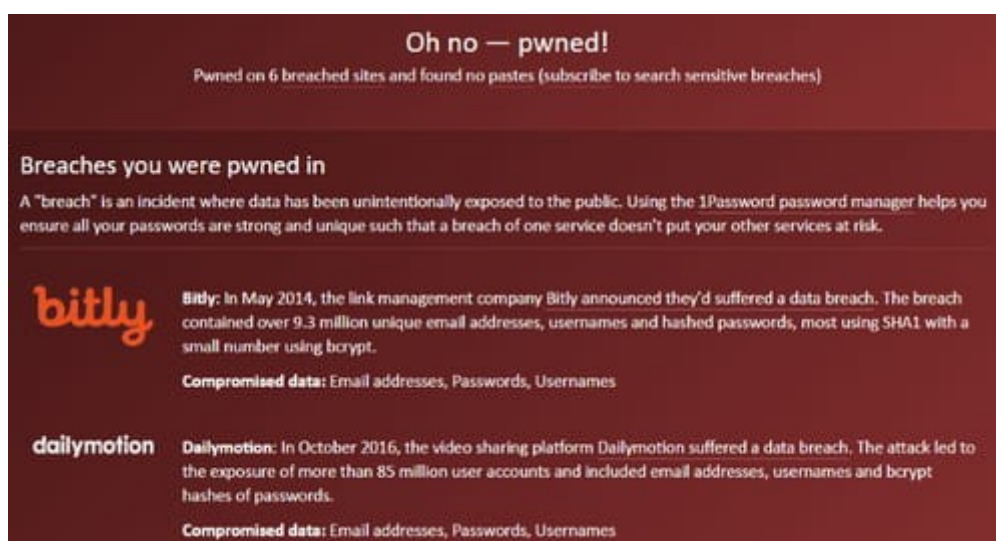
Si vous ne voulez pas utiliser le Gestionnaire de mots de passe de Google, ou si vous voulez vérifier un compte qui n'est pas sauvegardé dans Chrome ou dans Android, vous pouvez réaliser facilement le même type de vérification vous-même.

Pour savoir si vos identifiants (adresse mail, mot de passe...) ont déjà été piratés lors d'une fuite de données massive, utilisez un service de vérification comme Have I Been Pwned.



- Avec votre navigateur Web, rendez-vous sur le site [Have I Be Pwned](https://haveibeenpwned.com/).

- Saisissez l'adresse mail à tester dans la champ de recherche et validez en cliquant sur le bouton **pwned?**.
- Et constatez les dégâts. ;-)



Oh no — pwned!
Pwned on 6 breached sites and found no pastes (subscribe to search sensitive breaches)

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.

bitly **Bitly:** In May 2014, the link management company Bitly announced they'd suffered a data breach. The breach contained over 9.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a small number using bcrypt.
Compromised data: Email addresses, Passwords, Usernames

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

Si votre adresse figure dans des bases de données déjà piratées dans le passé, un message d'alarme s'affiche (en anglais), et vous retrouvez la liste des services en ligne dans lesquels vos identifiants et mots de passe ont été compromis. Il ne vous reste plus qu'à vous connecter sur chacun d'entre eux pour les modifier.

https://www.commentcamarche.net/faq/53570-verifier-si-les-mots-de-passe-des-services-de-google-ont-ete-pirates?utm_campaign=CommentCaMarche+High+Tech+2019-11-20&utm_medium=email&utm_source=MagNews