

# 1. Vérifier si mon email est compromise

## Solutions de vérifications d'email compromise

L'époque dans laquelle nous vivons en terme informatique est complexe pour la plupart des personnes, on entend beaucoup d'entreprises qui ont des fuites de données mais qu'en est-il de si votre email est présente dedans ? A travers cet article je vais vous présenter différentes solutions afin de vérifier la compromission d'une email.

1. [Antivirus](#)
2. [have i been pwned?](#)

### 1. Antivirus

Beaucoup de nos Anti Virus proposent dans leurs formules d'abonnement des solutions pour vérifier et vous avertir d'une fuite de mots de passe... Je peux en citer quelques-uns tels que [McAfee](#), [Norton](#) et [Kaspersky](#).

Ci-Dessous vous trouverez les abonnements proposés par les antivirus cités plus haut, dans leur ordre d'apparition et uniquement ceux contenant une vérification de fuites.

Abonnements individuels

Abonnements familiaux

		MEILLEUR PRIX	EXCLUSIF
	<b>McAfee+   Premium</b>	<b>McAfee+   Advanced</b>	<b>McAfee+   Ultimate</b>
	44,95 €* /an <del>129,95 €</del> Économisez 85,00 €	64,95 €* /an <del>149,95 €</del> Économisez 85,00 €	104,95 €* /an <del>189,95 €</del> Économisez 85,00 €
	Acheter	Acheter	Acheter
<b>📘 Fonctionnalités de protection de l'identité</b>			
<b>NEW</b> Experts de la restauration d'identité à votre service	●	✓	✓
<b>NEW</b> Protection en cas de perte de portefeuille	●	✓	✓
Surveillance de l'identité	✓	✓	✓
Gestionnaire de mots de passe	✓	✓	✓
<b>📘 Fonctionnalités de confidentialité</b>			
<b>NEW</b> Nettoyage de comptes en ligne	Analyses	Analyses	Service complet
<b>NEW</b> Confidentialité sur les réseaux sociaux	✓	✓	✓
VPN - réseau privé virtuel	✓	✓	✓
<b>📘 Fonctionnalités de sécurité</b>	Nombre d'appareils illimité*	Nombre d'appareils illimité*	Nombre d'appareils illimité*
Contrôle parental	●	●	●
Antivirus	✓	✓	✓
<b>NEW</b> protection anti-fraude McAfee	✓	✓	✓
<a href="#">Afficher tout ce qui est inclus</a> ▾	Acheter	Acheter	Acheter

Windows\* | macOS\* | Android™ | iOS\* | ChromeOS™

\* Prix de la première année. Prix de lancement pour les nouveaux clients. [Consultez les détails de l'offre.](#)

Le plus populaire

## Norton 360 Deluxe

1 an

2 ans

~~104.99 €~~ **66% de réduction\***

**34.99 €** la 1ère année

Les économies sont calculées par rapport au prix de renouvellement de 104.99 €/an.

[Voir les détails de l'abonnement ci-dessous.\\*](#)

Obtenir la version  
Deluxe

- ✓ 5 PC, Mac, tablettes ou téléphones
- ✓ Protection contre les virus, les malwares, les ransomwares et le piratage ⓘ
- ✓ Promesse 100 % contre les virus<sup>2</sup> ⓘ
- ✓ Sauvegarde cloud de 50 Go<sup>\*\*4</sup> ⓘ
- ✓ Gestionnaire de mots de passe ⓘ
- ✓ Connexion Internet privée VPN ⓘ
- ✓ Contrôle parental<sup>†</sup> ⓘ
- ✓ Dark Web Monitoring<sup>§</sup> ⓘ

Avec la Protection de l'identité

## Norton 360 Advanced

1 an

2 ans

~~134.99 €~~ **70% de réduction\***

**39.99 €** la 1ère année

Les économies sont calculées par rapport au prix de renouvellement de 134.99 €/an.

[Voir les détails de l'abonnement ci-dessous.\\*](#)

Obtenir la version  
Advanced

- ✓ 10 PC, Mac, tablettes ou téléphones
- ✓ Protection contre les virus, les malwares, les ransomwares et le piratage ⓘ
- ✓ Promesse 100 % contre les virus<sup>2</sup> ⓘ
- ✓ Sauvegarde cloud de 200 Go<sup>\*\*4</sup> ⓘ
- ✓ Gestionnaire de mots de passe ⓘ
- ✓ Connexion Internet privée VPN ⓘ
- ✓ Contrôle parental<sup>†</sup> ⓘ
- ✓ Dark Web Monitoring<sup>§</sup> ⓘ
- ✓ Aide à la restauration d'identité ⓘ
- ✓ Assistance en cas de portefeuille volé ⓘ
- ✓ Social Media Monitoring<sup>17</sup> ⓘ

## Meilleur Choix

### Protection Premium



Kaspersky Premium  
Total Security

★★★★★ 469 avis

**ÉCONOMISEZ 62%**

À partir de **29,99 €\*/an**

Windows® | macOS® | Android™ | iOS®

- ✓ Antivirus en temps réel
- ✓ Protection des paiements en ligne
- ✓ Optimisation des performances
- ✓ VPN illimité ultra-rapide
- ✓ Vérification des fuites de données
- ✓ Protection de l'identité
- ✓ Recherche et suppression des virus par un expert

Offre limitée



Kaspersky Safe Kids  
**1 AN GRATUIT**

En savoir plus

### Protection Plus



Kaspersky Plus  
Internet Security

★★★★★ 384 avis

**ÉCONOMISEZ 52%**

À partir de **25,99 €\*/an**

Windows® | macOS® | Android™ | iOS®

- ✓ Antivirus en temps réel
- ✓ Protection des paiements en ligne
- ✓ Optimisation des performances
- ✓ VPN illimité ultra-rapide
- ✓ Vérification des fuites de données

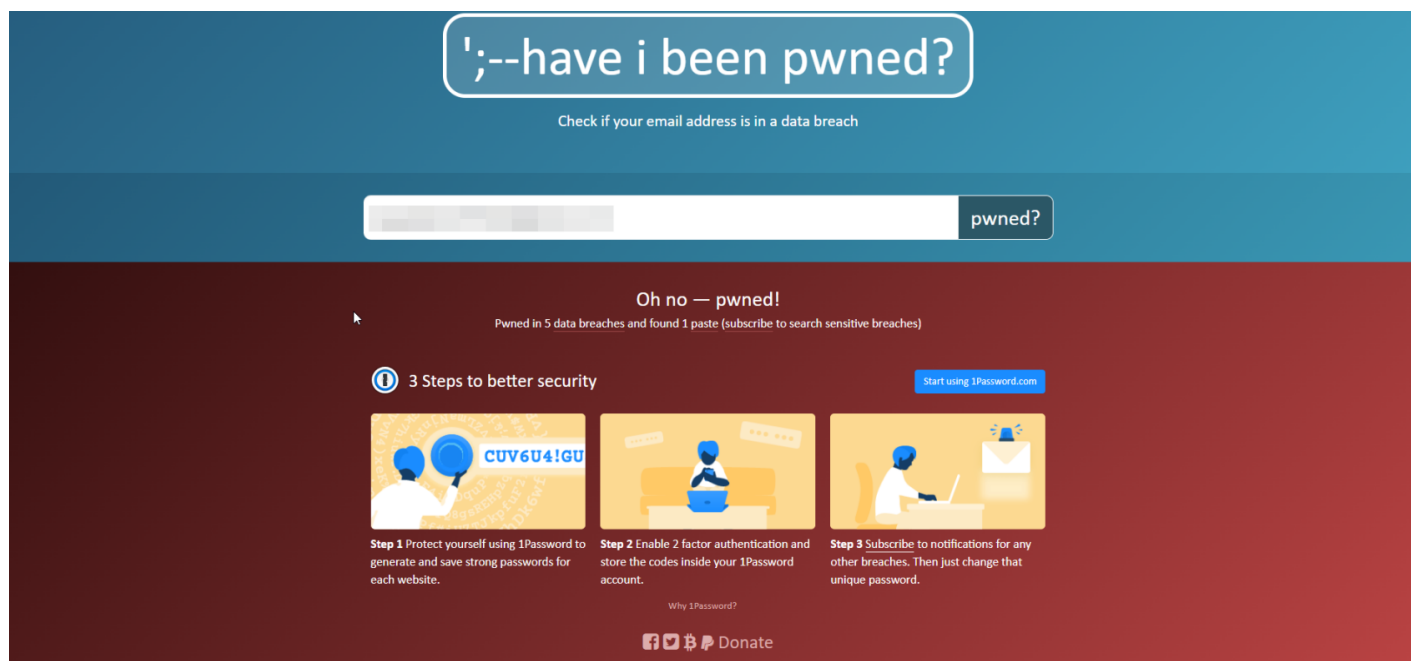
En savoir plus

Chacun de ces antivirus a ses points forts et inconvénients je ne suis pas ici pour vous en faire une promotion ni une démonstration. Je ne fais que vous exposer des possibilités.

## 2. have i been pwned?

Peut-être en avez déjà entendu parler ou pas du tout mais c'est un site permettant de manière simple de vérifier si une email est compromise. Un des petits bémol du site est qu'il est en anglais cependant si vous vous sentez apte à traduire ou utiliser la traduction automatique de votre navigateur les portes vous sont ouvertes.

Voici un exemple ci-dessous d'une email qui a été compromise, on peut retrouver dans la partie supérieure dans combien de fuites en l'occurrence ici 5 ainsi que dans un fichier déposer sur internet.



The screenshot shows the 'have i been pwned?' website interface. At the top, there is a search bar with the text 'have i been pwned?' and a button labeled 'pwned?'. Below the search bar, the results indicate that the email address is 'Pwned in 5 data breaches and found 1 paste (subscribe to search sensitive breaches)'. The page then displays '3 Steps to better security' with three numbered steps:

- 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.

At the bottom of the page, there is a 'Donate' button with social media icons for Facebook, Twitter, and Bitcoin.

Maintenant descendons un peu sur le site et nous pourrons savoir exactement sur quel site et quelles données ont été rendues public. Cependant je tiens à vous informer que à partir du moment où un site est compromis peu importe la nature des données changées le mot de passe et activer l'authentification à 2 facteurs est important pour garantir l'intégrité de vos données.

## 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.



**Aptoide:** In April 2020, the independent Android app store [Aptoide](#) suffered a [data breach](#). The incident resulted in the exposure of 20M customer records which were subsequently shared online via a popular hacking forum. Impacted data included email and IP addresses, names, IP addresses and passwords stored as SHA-1 hashes without a salt.

**Compromised data:** Browser user agent details, Email addresses, IP addresses, Names, Passwords



**Canva:** In May 2019, the graphic design tool website [Canva](#) suffered a [data breach](#) that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

**Compromised data:** Email addresses, Geographic locations, Names, Passwords, Usernames



**Deezer:** In late 2022, the music streaming service [Deezer](#) disclosed a [data breach](#) that impacted over 240M customers. The breach dated back to a mid-2019 backup exposed by a 3rd party partner which was subsequently sold and then broadly redistributed on a popular hacking forum. Impacted data included 229M unique email addresses, IP addresses, names, usernames, genders, DoBs and the geographic location of the customer.

**Compromised data:** Dates of birth, Email addresses, Genders, Geographic locations, IP addresses, Names, Spoken languages, Usernames



**GameSprite:** In December 2019, the now defunct gaming platform [GameSprite](#) suffered a [data breach](#) that exposed over 6M unique email addresses. The impacted data also included usernames, IP addresses and salted MD5 password hashes.

**Compromised data:** Email addresses, IP addresses, Passwords, Usernames



**SwordFantasy:** In January 2019, the now defunct MMO and RPG game [SwordFantasy](#) suffered a [data breach](#) that exposed 2.7M unique email addresses. Other impacted data included username, IP address and salted MD5 password hashes.

**Compromised data:** Email addresses, IP addresses, Passwords, Usernames

## Pastes you were found in

A [paste](#) is information that has been published to a publicly facing website designed to share content and is often an early indicator of a data breach. Pastes are automatically imported and often removed shortly after having been posted. 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.

Paste title	Date	Emails
<a href="#">No title</a>	18 Jun 2018, 22:17	2,679

Maintenant que nous avons passé tout ce qui était rouge qu'est-ce que je dois faire si le site est vert comme suis :

## Good news — no pwnage found!

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

Dans le cas où vous voyez le message ci-dessus, aucune inquiétude à avoir pour l'instant. Vos données n'ont pas été rendues publiques.

---

Revision #4

Created 2024-05-22 14:33:26 UTC by Ludovic

Updated 2024-06-18 09:48:30 UTC