Les fuites de données

Par Patrick Sentinel – 29a.ca

Fuite de données : Comment savoir si vos mots de passe traînent dans la nature (et éviter la catastrophe) ?

Vous avez déjà ressenti ce petit frisson d'angoisse en lisant un news du genre **"500 millions de comptes piratés"** ? Vous vous demandez si votre adresse électronique et votre précieux **"motdepasse123"** circulent en ce moment sur le *dark web*, vendus à prix cassé par un hacker en chandail à capuche ? 😱

Respirez un bon coup, on va voir ensemble **comment vérifier si vos données ont fuité**, **quoi faire si c'est le cas**, et surtout **comment éviter que ça ne recommence**. Accrochez-vous, ça va secouer (mais avec humour, promis).

C'est quoi une fuite de données ? (Et pourquoi c'est grave)

Une **fuite de données**, c'est quand des informations censées rester secrètes (comme vos identifiants, mots de passe, numéros de carte bancaire…) se retrouvent dans la nature à cause d'un piratage ou d'une mauvaise sécurité.

Comment ça arrive ?

🔹 **Un site mal sécurisé se fait pirater** → Les hackers volent des millions de comptes et les revendent. Aujourd'hui, un site mal sécurisé est l'une des failles les plus exploitées par les attaquants.

🔹 **Vous utilisez le même mot de passe partout** → Une seule fuite et tous vos comptes sont en danger. Sérieusement, soyez professionnel!

🔹 **Vous tombez dans un piège de *phishing*** → Vous donnez (sans le vouloir) votre mot de passe à un escroc.

🔹 **Vous avez installé un malware** → Un virus espion capte tout ce que vous tapez (y compris vos secrets les plus honteux).

💡 **Le problème ?** Une fois les données volées, elles **sont souvent revendues sur le *dark web***… et utilisées pour pirater vos autres comptes. 😬

Comment savoir si vos données sont dans la nature ?

Méthode 1 : *Have I Been Pwned* ? (Hé oui, ce site existe)

Il existe des outils gratuits pour savoir si votre adresse électronique ou votre mot de passe a fuité. Le plus connu ? Have I Been Pwned.

- **Tapez votre adresse électronique** et voyez si elle figure dans une base de données piratée.
- Si **"Oh no! Pwned!"** s'affiche en rouge, c'est que votre adresse et potentiellement vos mots de passe sont compromis.
- Si c'est vert, vous pouvez souffler (mais restez quand même prudent).

Méthode 2 : *Google Password Checkup*

Google propose un outil intégré à *Chrome* qui vous dit si vos mots de passe ont fuité. Rendez-vous dans **Paramètres > Mots de passe > Vérifier les mots de passe**.

- Il vous affichera les comptes à risque et vous proposera de changer vos mots de passe trop faibles ou compromis.

Méthode 3 : Firefox Monitor

Si vous utilisez *Firefox,* ***Firefox Monitor*** fait le même job que *Have I Been Pwned* : il surveille les fuites et vous alerte si votre courriel est exposé.

Que faire si votre mot de passe a fuité ? (Ne paniquez pas… mais réagissez vite !)

😱 **Étape 1 : Changez immédiatement votre mot de passe**
Si un de vos comptes est compromis, **changez son mot de passe dès maintenant**. Et si vous utilisez **le même partout (ce qui est une très mauvaise idée), changez-les tous**.

🔑 **Un bon mot de passe, c'est quoi ?**
✓ Long (minimum **12 à 16 caractères**).
✓ Un mix de **lettres, chiffres et caractères spéciaux**.
✓ Pas un mot courant ni une information personnelle (non, "P@ssword123" n'est pas un bon mot de passe).
✓ **Unique pour chaque site** (oui, ça fait beaucoup, mais j'ai une solution 👇).

💡 **Astuce : Utilisez un gestionnaire de mots de passe**
Plutôt que de retenir 25 mots de passe ultra compliqués, laissez un outil sécurisé le faire pour vous. **Bitwarden, 1Password, LastPass**. Attention aux gestionnaires de mots de passe dans le cloud car ils sont déposés dans un environnement que vous ne maîtrisez pas.

😱 **Étape 2 : Activez l'authentification à deux facteurs (2FA)**

Même si un hacker a votre mot de passe, il ne pourra pas se connecter **sans un code supplémentaire** (souvent envoyé sur votre téléphone). C'est **LE meilleur moyen** de sécuriser vos comptes.

😱 **Étape 3 : Surveillez vos comptes bancaires et courriels**
Si un pirate a accès à vos infos, il pourrait tenter d'**usurper votre identité** ou d'utiliser votre carte bancaire. Jetez un œil à vos relevés et activez les alertes de connexion suspecte.

Comment éviter une future fuite de données ? (Soyez plus malin que les hackers)

✓ **N'utilisez jamais le même mot de passe partout.** (C'est LE piège à éviter.)
✓ **Évitez les mots de passe ridicules.** ("password", "123456", "azerty" = catastrophe assurée.)
✓ **Activez toujours l'authentification à deux facteurs** (même si ça rajoute une étape, ça protège vraiment).
✓ **Ne cliquez pas sur les liens suspects** (les courriels du "Prince" ou de "*Netflix* qui veut vérifier votre compte" = danger).
✓ **Mettez à jour vos logiciels** (les mises à jour corrigent souvent des failles de sécurité).

Bonus : Le top des pires mots de passe trouvés dans les fuites

Pour rigoler (et pleurer en même temps), voici une liste réelle des mots de passe les plus utilisés… et donc les plus piratés :

🔥 **123456** (sérieusement, encore en 2025 ?????? 😅)
🔥 **password** (classique mais toujours aussi dangereux).
🔥 **qwerty** (pour ceux qui ont la flemme).
🔥 **iloveyou** (c'est mignon, mais pas très sécurisé).
🔥 **admin** (si vous utilisez ça sur votre réseau Wi-Fi… bon courage).

Si l'un de ces mots de passe est le vôtre… changez-le. **Tout de suite.** 😳

Conclusion : Mieux vaut prévenir que guérir

Les fuites de données sont **de plus en plus fréquentes**, mais il existe des solutions simples pour protéger vos comptes et dormir tranquille.

- **Vérifiez si votre courriel a fuité** (*Have I Been Pwned* est votre ami).
- **Modifiez vos mots de passe compromis** (et évitez les classiques comme "password123").

- **Utilisez un gestionnaire de mots de passe** pour vous simplifier la vie.
- **Activez l'authentification à deux facteurs** pour une sécurité maximale. ***C'EST UN MUST***

Parce qu'au final, perdre un mot de passe, c'est embêtant… mais perdre **tous ses comptes en même temps**, c'est un cauchemar.

Alors, êtes-vous prêt à tester vos courriels pour voir si vos données ont fuité ? Ou préférez-vous continuer à vivre dans le déni ? 😌
