

« Vos données ont fuité » : que faire, concrètement

Un service que vous utilisez s'est fait pirater et vos identifiants circulent : évaluer, réagir, et transformer l'alerte en réflexe d'équipe.

7 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/fuite-donnees-que-faire

L'email arrive un matin : « nous vous informons d'un incident de sécurité affectant vos données » — ou c'est haveibeenpwned qui signale votre adresse dans une nouvelle fuite. C'est désormais une expérience banale : les fuites de données se comptent en milliards d'identifiants. La bonne nouvelle : la réaction utile tient en quelques gestes, et l'événement est l'occasion parfaite de solder de vieilles mauvaises habitudes.

1. Évaluer : qu'est-ce qui a fuité, vraiment

- Lire la notification (les services sérieux détaillent) : email seul ? mot de passe ? haché ou en clair ? données bancaires ? documents ?
- Le mot de passe est LA donnée critique : s'il a fuité — même « haché » —, considérez-le comme public, surtout s'il était faible
- L'email seul alimente le spam et le phishing ciblé : gênant, pas critique — la vigilance monte d'un cran, c'est tout
- Vérifier l'étendue sur haveibeenpwned.com : votre adresse y révèle TOUTES ses fuites connues — souvent instructif
- Méfiance envers les fausses notifications : la « fuite » qui exige de « vérifier votre compte » via un lien est du phishing surfant sur l'actualité

2. Réagir : les gestes dans l'ordre

- Changer le mot de passe du service touché — depuis le site officiel, jamais depuis le lien d'un email
- LA question décisive : ce mot de passe servait-il ailleurs ? Chaque service qui le partageait se change aussi, en commençant par la messagerie et la banque — c'est le credential stuffing qu'on désamorce
- Activer la MFA sur le service touché et les comptes importants — la fuite devient alors quasi inoffensive
- Données bancaires concernées : surveillance des comptes, opposition au moindre débit inconnu
- Surveiller les tentatives dans les semaines qui suivent : phishing personnalisé (« suite à l'incident... »), tentatives de connexion — la fuite se revend et s'exploite avec délai

CAS CONCRET

Le scénario type d'exploitation : un site de e-commerce mineur fuite en 2024 ; l'attaquant teste en 2026 le couple email + mot de passe sur les messageries professionnelles — et entre, car le mot de passe n'a jamais changé et servait partout. La fuite d'hier ouvre la boîte d'aujourd'hui. C'est LE mécanisme que le duo « mots de passe uniques + MFA » éteint définitivement.

3. En entreprise : passer de l'individuel au collectif

- Surveiller le domaine entier sur haveibeenpwned (gratuit) : chaque nouvelle fuite touchant une adresse @votreentreprise notifie le référent
- Traiter les alertes comme un mini-incident : qui est touché, le mot de passe concerné servait-il en interne, rotation faite ?
- Le rapport de santé du gestionnaire de mots de passe fait le reste : il signale les mots de passe présents dans des fuites connues
- L'occasion pédagogique : une fuite réelle touchant l'équipe vaut dix sessions de sensibilisation — racontez-la (sans désigner personne)

4. Et si c'est VOTRE service qui a fuité

Perspective inverse : si les données fuitées sont celles de VOS clients (votre base, votre outil piraté), vous êtes dans le cadre de la violation de données RGPD — documentation, notification CNIL sous 72 h si risque, information des personnes si risque élevé (voir notre guide RGPD), et la gestion d'incident complète (voir notre guide). La transparence rapide y est à la fois l'obligation et la meilleure stratégie.

L'essentiel à retenir

- 01 Changer le mot de passe du service touché, depuis le site officiel
 - 02 Traquer et changer toutes ses réutilisations
 - 03 Activer la MFA sur les comptes qui comptent
 - 04 Surveiller le domaine de l'entreprise sur haveibeenpwned
 - 05 Redoubler de vigilance phishing dans les semaines suivantes
 - 06 Profiter de l'alerte pour généraliser gestionnaire + MFA
-

Questions fréquentes

Un mot de passe « haché » qui fuité est-il vraiment en danger ?

Le hachage protège... proportionnellement à la force du mot de passe : les mots de passe courts ou courants se « cassent » en masse depuis les fuites hachées, les phrases de passe longues résistent des années. Comme vous ignorez la qualité du hachage utilisé par le service, la règle pratique reste : mot de passe fuité = mot de passe à changer, partout où il servait.

Peut-on faire supprimer ses données du dark web ?

Non — ce qui a fuité est copié, revendu, recompilé : aucune prestation ne peut réellement l'effacer, méfiez-vous des offres qui le promettent. La seule stratégie efficace est de rendre les données fuitées inutiles : mots de passe changés et uniques, MFA partout, et vigilance sur les tentatives qui exploitent les infos personnelles fuitées.

Le service fautif me doit-il quelque chose ?

Il doit la transparence (notification) et, selon les cas, répond de manquements devant la CNIL — des actions collectives existent pour les fuites majeures. À votre échelle : exigez les réponses (quelles données, quelles mesures), et votez avec vos pieds si le service a été négligent. Pour l'entreprise, une fuite chez un fournisseur interroge aussi le contrat (voir notre guide prestataires).

Pour aller plus loin

Have I Been Pwned — vérifier et surveiller — haveibeenpwned.com

CNIL — violation de données : les réflexes — www.cnil.fr/fr/les-violations-de-donnees-personnelles

Besoin d'aide pour le mettre en place ?

Audit, durcissement, accompagnement : Cyberionis sécurise les TPE, PME et collectivités, à Nancy, Lure et à distance.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr