



Comment survivre à une violation de données

Un service que vous utilisez a été attaqué et vos données figurent dans la fuite. **Vous n'y êtes pour rien, mais vous êtes le seul à pouvoir en limiter les conséquences** : ce qui a fuité servira à vous atteindre ailleurs, souvent des mois plus tard.



Dès l'annonce

URGENCE

1

Vérifiez que l'alerte est authentique.

Les fausses notifications de fuite sont elles-mêmes un hameçonnage classique. N'utilisez pas le lien du message : rendez-vous sur le site officiel du service ou consultez son communiqué.

2

Identifiez ce qui a fuité.

Une adresse e-mail, un mot de passe, des coordonnées bancaires ou une pièce d'identité n'appellent pas les mêmes mesures. Le service est tenu de le préciser.

3

Changez le mot de passe du service concerné.

Puis celui de **tous les comptes où vous utilisiez le même** : c'est la mesure la plus efficace, et la plus souvent négligée.

4

Activez l'authentification multifacteur.

Sur le service touché et sur votre messagerie.

5

Si des données de paiement sont concernées, prévenez votre banque.

Surveillez les opérations et demandez si le renouvellement de la carte est nécessaire.

6

Si une pièce d'identité est concernée, conservez la notification.

Notez la date : c'est votre preuve en cas d'usurpation d'identité ultérieure.



Dans les mois qui suivent

VIGILANCE

- **Attendez-vous à des messages très crédibles.** Les données volées servent à fabriquer des hameçonnages personnalisés, citant votre nom, vos achats ou votre numéro de client.
- **Vérifiez régulièrement vos adresses e-mail** sur un service reconnu de recherche de fuites, pour savoir dans quelles bases elles apparaissent.
- **Surveillez vos relevés** et les notifications de connexion à vos comptes principaux.
- **Exercez vos droits** auprès du service : savoir quelles données il détient, les faire rectifier, faire supprimer votre compte si vous ne l'utilisez plus.
- **Fermez les comptes dormants.** Chaque service inutilisé reste une fuite potentielle avec vos données à l'intérieur.



À ne pas faire

- ✗ Cliquer sur le lien « vérifier si je suis concerné » contenu dans l'e-mail d'alerte.
- ✗ Payer un service promettant de « supprimer vos données du dark web » : une fois diffusées, ces données ne peuvent pas être retirées.
- ✗ Ne rien faire parce que « ce n'était qu'un mot de passe » — c'est précisément ce qui ouvre les autres comptes.
- ✗ Répondre à un appel ou un message se réclamant du service pour « sécuriser votre compte » et demandant un code.



Pour limiter la prochaine fuite

PRÉVENTION

- **Un mot de passe unique par service** : la fuite reste alors confinée à ce seul compte.
- **Une adresse e-mail dédiée aux inscriptions**, distincte de votre adresse personnelle et professionnelle.
- **Le minimum de données fournies** : un champ facultatif qui n'est pas rempli ne peut pas fuiter.
- **L'authentification multifacteur**, qui rend un mot de passe volé inexploitable.

OJCS — Organisation des Jeunes pour un Cyberspace Sécurisé · Guide de survie cyber, fiche 6 sur 6.

Fiche librement reproductible avec mention de la source. Campagne inspirée du *Cyber Survival Guide* de la National Cybersecurity Alliance.