Fiche Pratique N°58 : Réagissez à une fuite de données V1.3

7 nov, 2026 · @Gabriel

Objectif : *savoir quoi faire, et dans quel ordre, quand vous apprenez que vos données personnelles ont fuité : vérifier, changer, surveiller, sans céder à la panique ni aux escrocs.*

- ***Public visé :*** *débutant*
- ***Temps estimé :*** *1 heure le premier jour, puis quelques minutes par semaine pendant un mois*
- ***Difficulté :*** ★☆☆☆☆ *(Très facile)*
- ***Prérequis :*** *aucun ; un gestionnaire de mots de passe aide beaucoup (fiche N°16)*
- ***Fiches associées :*** *N°16 (mots de passe), N°18 (double authentification), N°39 (nettoyer son empreinte numérique), N°47 (arnaques en ligne), N°56 (alias de courriel)*

1. Pourquoi ça vous concerne (Le problème)

Les fuites de données sont devenues banales. En 2026, **45 % des Français** disent avoir été prévenus d'une fuite de leurs données personnelles, contre 30 % un an plus tôt (baromètre Cybermalveillance.gouv.fr et Ipsos). Opérateurs, administrations, mutuelles, sites marchands : personne n'y échappe. En février 2026, par exemple, les données d'environ **1,2 million de comptes bancaires** (identité, adresse, IBAN, date et lieu de naissance) ont été consultées dans le fichier national FICOBA.

Ce qui a fuité	Ce que les escrocs peuvent en faire
Nom, adresse e-mail, téléphone	Faux messages crédibles à votre nom (hameçonnage, fiche N°47)
Mot de passe	Se connecter à vos comptes, surtout si vous réutilisez ce mot de passe
IBAN	Tenter des prélèvements, ou se faire passer pour votre banque
Date de naissance, pièce d'identité	Usurper votre identité (crédit, abonnement, location)

Le risque : une fuite ne veut pas dire que vos données ont déjà servi. Mais elle rend les arnaques plus crédibles, et elles arrivent souvent dans les semaines qui suivent.

Le bénéfice : quelques gestes, dans le bon ordre, ferment la porte avant que quelqu'un ne la pousse.

2. D'abord : vérifier que l'alerte est vraie

Un faux message « vos données ont fuité, cliquez ici » est lui-même une arnaque classique.

- ☐ Le message vient-il vraiment de l'organisme ? **Ne cliquez sur aucun lien** : ouvrez vous-même son site ou son application.
- ☐ L'organisme ne vous demande **jamais** de mot de passe, de code reçu par SMS ni de coordonnées bancaires pour « sécuriser » votre compte.
- ☐ Notez la date du message et la liste des données concernées. **Gardez ce message** : il servira en cas de litige.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°58 : Réagissez à une fuite de données V1.3

3. Savoir si vous êtes touché

1. Ouvrez `haveibeenpwned.com` et saisissez votre adresse e-mail.
    - **Vous devez voir :** la liste des fuites connues où apparaît votre adresse, ou un message « Good news — no pwnage found! ».
2. Cliquez sur **Notify me** pour être prévenu par e-mail des prochaines fuites. Le service est gratuit pour les particuliers ; confirmez votre adresse via le lien reçu.
3. Autre possibilité : **Mozilla Monitor** (`monitor.mozilla.org`) surveille gratuitement jusqu'à 20 adresses e-mail.
4. Votre gestionnaire de mots de passe (Proton Pass, Bitwarden…) signale souvent lui-même les mots de passe apparus dans une fuite : consultez son rapport de sécurité.

⚠️ **Cloud Act :** Bitwarden est une société américaine. Même si vous choisissez ses serveurs européens, vos données restent soumises au droit américain (Cloud Act), qui permet aux autorités des États-Unis d'en exiger la communication. Pour y échapper, hébergez vous-même Vaultwarden (fiche N°35), ou choisissez Proton Pass (Suisse) ou KeePassXC (local).

4. La première semaine : sécuriser, dans cet ordre

C'est la démarche que recommandent la CNIL et Cybermalveillance.gouv.fr (octobre 2026).

1. **Changez le mot de passe de votre messagerie principale en premier.** C'est elle qui permet de réinitialiser tous vos autres comptes.
    - **Vous devez voir :** un message de confirmation, et une déconnexion de vos autres appareils si vous la demandez.
2. **Changez le mot de passe du compte touché**, puis celui de **tout autre compte qui utilisait le même** mot de passe. Un mot de passe différent par site, c'est le rôle du gestionnaire (fiche N°16).
3. **Activez la double authentification** sur la messagerie, la banque et les comptes importants (fiche N°18).
4. **Vérifiez les sessions ouvertes** et déconnectez celles que vous ne reconnaissez pas (dans les réglages de sécurité de chaque compte).
5. **Vérifiez l'adresse et le téléphone de récupération**, ainsi que les **règles de transfert automatique** de votre messagerie : un pirate peut en ajouter une pour recevoir une copie de vos courriels.
6. **Méfiez-vous** de tout appel, SMS ou courriel inhabituel, même s'il connaît votre nom et votre IBAN.

5. Si vos coordonnées bancaires ont fuité

- Prévenez votre banque, et faites **opposition sur votre carte** si son numéro est concerné.
- Surveillez vos relevés chaque semaine pendant plusieurs mois.
- Ne signez aucun **mandat de prélèvement** douteux. Un prélèvement que vous aviez autorisé peut être contesté sans justification pendant **8 semaines** ; un prélèvement que vous n'avez jamais autorisé se signale à la banque sans attendre.
- Dans votre espace bancaire, **bloquez ou limitez les prélèvements** des créanciers que vous ne connaissez pas, si votre banque le permet.

gabriel.ananda@mailo.com
CC BY SA

- Rappel : votre banque ne vous demandera **jamais** votre mot de passe ni un code reçu par SMS, ni par téléphone ni par courriel.

6. Les semaines suivantes : surveiller

Quoi surveiller	Signe d'alerte	Que faire
Relevés bancaires	Petit prélèvement inconnu (souvent un test)	Contestez-le auprès de la banque
Courrier postal	Lettre d'un organisme de crédit ou d'un opérateur que vous ne connaissez pas	Contactez l'organisme : quelqu'un a peut-être ouvert un contrat à votre nom
Messagerie	Alertes de connexion, courriels de réinitialisation que vous n'avez pas demandés	Changez le mot de passe et vérifiez la double authentification
SMS et appels	« Conseiller bancaire », « livreur », « Ameli » insistants	Raccrochez, rappelez le numéro officiel ; transférez les SMS frauduleux au **33700** (gratuit)

7. Obtenir de l'aide et porter plainte

- **17Cyber** (`17cyber.gouv.fr`) : le service public d'assistance aux victimes, ouvert 24 h/24. Un diagnostic guidé vous dit quoi faire et, si l'incident est grave, vous met en relation par tchat avec un policier ou un gendarme.
- **Cybermalveillance.gouv.fr** : fiches pratiques et mise en relation avec des professionnels près de chez vous.
- **Plainte :** si vous êtes victime d'une fraude (prélèvement, usurpation d'identité), déposez plainte au commissariat ou à la gendarmerie, en apportant le message de l'organisme et vos relevés.
- **CNIL :** si l'organisme ne vous a pas informé ou ne répond pas à vos questions sur vos données, vous pouvez adresser une plainte à la CNIL (`cnil.fr`).

8. Au quotidien : limiter la casse de la prochaine fuite

- Un **mot de passe unique** par site, dans un gestionnaire (fiche N°16).
- Un **alias de courriel** par site marchand (fiche N°56) : si l'alias fuit, vous le coupez.
- Ne donnez pas de **copie de pièce d'identité** sans avoir vérifié qui la demande, et pourquoi.
- **Supprimez les comptes inutilisés** (fiche N°39) : un compte fermé ne peut plus fuir.
- Séparez les usages **personnels et professionnels**.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°58 : Réagissez à une fuite de données V1.3

9. À savoir avant de se lancer

Crainte fréquente	La réalité
« Mes données sont dans la nature, c'est fichu. »	Une fuite augmente le risque, elle ne vide pas votre compte. Les bons gestes le réduisent fortement.
« Je dois tout changer, tous mes comptes. »	Commencez par la messagerie, le compte touché et ceux qui partageaient le même mot de passe.
« On ne peut pas changer un IBAN. »	C'est vrai, mais la vigilance et la contestation des prélèvements vous protègent.
« Porter plainte ne sert à rien. »	La plainte vous protège en cas de contrat ouvert à votre nom, et aide les enquêtes.

10. Challenge 7 jours

- **Jour 1 :** vérifier vos adresses sur `haveibeenpwned.com` et activer **Notify me**.
- **Jour 2 :** changer le mot de passe de votre messagerie principale.
- **Jour 3 :** activer la double authentification sur la messagerie et la banque.
- **Jour 4 :** vérifier les sessions ouvertes et les transferts automatiques de votre messagerie.
- **Jour 5 :** remplacer les mots de passe réutilisés, avec votre gestionnaire.
- **Jour 6 :** regarder vos prélèvements et bloquer ceux que vous ne reconnaissez pas.
- **Jour 7 :** enregistrer `17cyber.gouv.fr` et le 33700 dans vos contacts.

Vous allez constater : la prochaine alerte de fuite ne vous fera plus peur, car vous saurez exactement quoi faire.

11. En résumé (ce que vous gagnez)

Action	Bénéfice
Vérifier l'alerte avant de cliquer	Vous ne tombez pas dans le faux message de « fuite »
Messagerie sécurisée d'abord	Le pirate ne peut plus réinitialiser vos autres comptes
Double authentification	Un mot de passe volé ne suffit plus
Surveillance bancaire	Une fraude repérée tôt est plus facile à contester
Alertes Have I Been Pwned	Vous êtes prévenu des prochaines fuites

12. À retenir absolument

- **Ne cliquez pas** dans un message qui annonce une fuite : allez vous-même sur le site.
- **Messagerie d'abord,** puis le compte touché, puis les mots de passe réutilisés.
- **Double authentification** partout où c'est possible.

gabriel.ananda@mailo.com
CC BY SA

- **17Cyber** (`17cyber.gouv.fr`) si vous êtes victime, **33700** pour les SMS frauduleux.

Test final : saisissez votre adresse sur `haveibeenpwned.com`. Pour chaque fuite listée, vérifiez que le mot de passe de ce site a été changé et n'est utilisé nulle part ailleurs. Si c'est le cas, vous avez réussi ✅

Références

- Leto – les 3 étapes de la CNIL et de Cybermalveillance.gouv.fr (octobre 2026)
- CNIL – Cybermois 2026
- Siècle Digital – près d'un Français sur deux touché par une fuite de données (septembre 2026)
- Futura – piratage de FICOBA : 1,2 million d'IBAN consultés (mars 2026)
- Have I Been Pwned – questions fréquentes
- Troy Hunt – le service de notification gratuit de Have I Been Pwned
- Mozilla – Fin de Monitor Plus, surveillance gratuite de 20 adresses maintenue
- IT-Connect – lancement de 17Cyber
- Selectra – le 33700 pour signaler les SMS frauduleux

gabriel.ananda@mailo.com
CC BY SA