

# Fuite de données de Free : comment se protéger ?

■ ADVISORY ■ CYBER

■ *Newsletter N°3*



## Fuite de données chez Free : Conséquences et mesures de protection

**En novembre 2024, Free a subi une cyberattaque de grande envergure qui a compromis les données personnelles de près de 19 millions d'abonnés.**

Des informations sensibles telles que des noms, adresses, numéros de téléphone, ainsi que des IBAN ont été volées et partiellement divulguées sur le Dark Web.

**Au-delà d'un petit feuillet à rebondissement dans le milieu de la Cybersécurité, cette violation des données soulève des préoccupations majeures, notamment en matière de sécurité bancaire et de fraude. Reprenons ensemble.**

### Récapitulatif des événements

- **Octobre 2024 - Début de l'attaque :** Fin octobre 2024, Free découvre une cyberattaque majeure visant ses systèmes internes. Des cybercriminels ont accédé à une vaste base de données contenant des informations sur plus de 19 millions d'abonnés. Parmi les données compromises figurent des informations personnelles telles que des noms, adresses, numéros de téléphone, ainsi que des IBAN de certains clients Freebox.
- **31 octobre 2024 - Free communique sur la fuite :** Free annonce publiquement la fuite de données et informe ses abonnés concernés. Il recommande à ses utilisateurs de vérifier leurs comptes bancaires pour toute activité suspecte et rappelle que des prélèvements non autorisés peuvent être contestés dans un délai de 13 mois.

- **2 novembre 2024 - Réaction de la CNIL** : la CNIL (Commission Nationale de l'Informatique et des Libertés) confirme avoir été informée de la fuite de données et ouvre une enquête pour déterminer la nature exacte de la violation. L'organisme met en place une procédure pour que les victimes puissent déposer plainte.
- **3 novembre 2024 - Publication d'un message de prévention sur Cybermalveillance.gouv.fr** : Le site Cybermalveillance.gouv.fr publie des conseils pour les victimes de cette attaque.
- **5 novembre 2024 - Mise en vente des données sur le Dark Web par « Drussellx »** : Des informations commencent à circuler selon lesquelles les IBAN volés ont été mis en vente sur le Dark Web, ce qui a alimenté les craintes concernant la possibilité de fraudes à grande échelle. Drussellx publie gratuitement un « échantillon » des données pour prouver l'attaque. Le pirate informe assez rapidement qu'un acheteur potentiel s'est manifesté.
- **7 novembre 2024 - Free intensifie les efforts de communication** : Free met en place un centre d'assistance dédié pour aider les clients concernés et répondre à leurs questions. L'opérateur annonce également avoir informé ses partenaires bancaires de la fuite de données, afin de prévenir d'éventuelles tentatives de fraude.
- **8 novembre 2024 - Révélation de YuroSh** : Un hacktivist du nom de "YuroSh" revendique la responsabilité de l'attaque et dit que les données n'ont pas été vendues et que les vendre n'est pas en projet. Il dévoile plus de détails sur ses intentions : le pirate affirme avoir informé Free de vulnérabilités par le passé, que l'opérateur aurait ignorées. Il explique « détester la surveillance globale » et voit ce piratage comme un moyen de mettre un coup de pied dans la fourmilière.
- **10 novembre 2024 - La CNIL confirme l'ouverture d'une procédure** : La CNIL confirme l'ouverture d'une procédure de contrôle afin de vérifier la conformité de Free avec les obligations légales en matière de protection des données personnelles. Cette enquête vise à déterminer si Free a suffisamment protégé les informations de ses abonnés et à évaluer l'ampleur de la fuite.
- **A ce jour - Suivi des actions de sécurité** : Free continue de collaborer avec les autorités pour limiter les effets de la fuite et renforcer ses mesures de sécurité. L'opérateur annonce qu'il met en place des solutions techniques et renforce son équipe et leur formation pour prévenir de futures cyberattaques.

## Les conséquences de la fuite de données

**Peu importe les explications données par les pirates informatiques : les données sont susceptibles d'être dans la nature, et même si elles ne sont pas vendues, ils n'ont pas dit qu'ils allaient les détruire.** La vigilance reste donc de mise : les informations extraites des bases de données de Free comprennent des éléments personnels tels que des coordonnées complètes et des données bancaires (IBAN).

Bien que les mots de passe et numéros de carte bancaire ne soient pas concernés, le vol d'IBAN augmente le risque de fraudes bancaires. En effet, ces données peuvent être utilisées pour générer de faux mandats de prélèvement, émettre des ordres de prélèvement illégitime ou être revendues à des cybercriminels pour des opérations malveillantes.

## Que faire si vous êtes victime de la fuite de données ?

Si vous êtes client de Free et craignez que vos données aient été compromises, plusieurs mesures peuvent être prises pour limiter les risques de fraude :

1. Soyez particulièrement méfiant face à tout appel téléphonique ou message (mail, SMS...) de personnes qui prétendraient vous connaître à partir des informations dérobées.
2. Surveillez régulièrement le compte bancaire dont vous auriez été informé que l'IBAN a été dérobé et demandez à votre banque le remboursement de toute opération dont vous ne seriez pas l'auteur. En cas de doute, rapprochez-vous de votre conseiller bancaire habituel.
3. Vérifiez également régulièrement la liste des créanciers autorisés de votre compte bancaire : il s'agit de la liste des bénéficiaires de vos prélèvements !
4. Alertez immédiatement votre opérateur en cas de perte prolongée de connexion sur votre ligne téléphonique mobile, pour vous assurer que vous n'avez pas été victime d'un échange frauduleux de votre carte SIM (*SIM Swapping*).
5. Déposez plainte en cas d'utilisation frauduleuse de vos données personnelles divulguées.
6. Déposez plainte à la CNIL (pour la France) si vous estimez que vos données personnelles n'ont pas été suffisamment protégées ;
7. Engager au besoin une [action de groupe](#) ou un recours collectif qui permet aux victimes, de saisir la justice pour demander la cessation de la violation de données personnelles et la réparation du préjudice – Dans les pays où cela est possible.

**Retrouvez le détail de ces consignes de protection sur le site Internet de Cybermalveillance.gouv.fr : <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/violation-de-donnees-personnelles-free-202410>**

## Conclusion

En 2022, Free avait déjà été sanctionné par une amende de 300 000 € par la CNIL pour avoir stocké des mots de passe en clair, ce qui montre un manque de vigilance en matière de protection des données personnelles. En 2024, la fuite de données chez Free est un rappel alarmant des vulnérabilités auxquelles les entreprises peuvent être confrontées, ainsi que des risques auxquels leurs clients sont exposés.

L'incident souligne également la nécessité de renforcer les protections contre la fraude et les cyberattaques, tant au niveau des entreprises que des utilisateurs individuels. Les victimes doivent prendre des mesures de protection immédiates et signaler toute activité suspecte aux autorités compétentes.

## Sources

---

- **MACG** : <https://www.macg.co/services/2024/11/piratage-de-free-la-base-de-donnees-naurait-pas-ete-vendue-et-ne-le-sera-pas-147057>
- **CLUBIC** : <https://www.clubic.com/actualite-541829-cyberattaque-de-free-fuite-de-donnees-iban-banques-l-operateur-nous-explique-ce-qui-s-est-passe-et-sa-reaction.html>
- **Cybermalveillance.gouv.fr** : <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/violation-de-donnees-personnelles-free-202410>
- **RTL** : <https://www.rtl.fr/actu/sciences-tech/fuite-de-donnees-chez-free-comment-savoir-si-votre-iban-et-vos-informations-ont-ete-pirates-7900434238>
- **FUTURA-SCIENCES** : <https://www.futura-sciences.com/tech/actualites/technologie-piratage-comptes-free-nouvelle-revelation-seme-trouble-117397/>
- **CNIL** : <https://www.cnil.fr/fr/fuite-de-donnees-sur-internet-et-vol-de-votre-iban-comment-vous-proteger-si-vous-etes-concerne>
- **CNIL** : <https://www.cnil.fr/fr/comment-reagir-face-une-usurpation-didentite>

## Auteurs

---



Sabina DEBUSSY

Directeur Associé • Advisory • KPMG Monaco

[sdebussy@kpmg.mc](mailto:sdebussy@kpmg.mc)

---



Clément MAILLIOUX

Directeur • Advisory • KPMG Monaco

[cmaillieux@kpmg.mc](mailto:cmaillieux@kpmg.mc)

---

## Contactez-nous



**Bettina RAGAZZONI**

Associé

[bragazzoni@kpmg.mc](mailto:bragazzoni@kpmg.mc)



**Stéphane GARINO**

Associé  
Principal

[sgarino@kpmg.mc](mailto:sgarino@kpmg.mc)



**Xavier CARPINELLI**

Directeur Associé  
Expertise

[xaviercarpinelli@kpmg.mc](mailto:xaviercarpinelli@kpmg.mc)



**Anne Marie FELDEN**

Directeur Associé  
Audit

[afelden@kpmg.mc](mailto:afelden@kpmg.mc)



**Sylvie ROTI**

Directeur Associé  
Expertise

[sroti@kpmg.mc](mailto:sroti@kpmg.mc)



**Sabina  
DEBUSSY**

Directeur Associé  
Advisory

[sdebussy@kpmg.mc](mailto:sdebussy@kpmg.mc)



**Patrice  
DARMON**

Directeur Associé  
Expertise

[pdarmon@kpmg.mc](mailto:pdarmon@kpmg.mc)



**Mélanie  
LE MOIGN**

Directeur Associé  
Audit

[mlemoign@kpmg.mc](mailto:mlemoign@kpmg.mc)



**Cécile  
BOZANO-BODIN**

Directeur Associé  
Advisory

[cbozanobodin@kpmg.mc](mailto:cbozanobodin@kpmg.mc)



**Alain  
CHARPENTIER**

Directeur Associé  
Audit

[acharpentier@kpmg.mc](mailto:acharpentier@kpmg.mc)

## KPMG GLD & Associés Monaco



2, rue de la Lujerneta • "Athos Palace" • 98000, Monaco



[mc-news@kpmg.mc](mailto:mc-news@kpmg.mc)



[www.KPMG.mc](http://www.KPMG.mc)



[@KPMG\\_Monaco](https://twitter.com/KPMG_Monaco)



[+377 977 777 00](tel:+37797777700)



[@kpmg-monaco](https://www.linkedin.com/company/kpmg-monaco)



[@KPMGMonaco](https://www.facebook.com/KPMGMonaco)

Les informations contenues dans ce document sont d'ordre général et ne sont pas destinées à traiter les particularités d'une personne ou d'une entité. Bien que nous fassions tout notre possible pour fournir des informations exactes et appropriées, nous ne pouvons garantir que ces informations seront toujours exactes à une date ultérieure. Elles ne peuvent ni ne doivent servir de support à des décisions sans validation par les professionnels ad hoc. KPMG International ne propose pas de services aux clients. Aucun cabinet membre n'a le droit d'engager KPMG International ou les autres cabinets membres vis-à-vis des tiers. KPMG International n'a le droit d'engager aucun cabinet membre.

[Déclaration de Confidentialité | Mentions légales](#)