ISS GLOBAL / RAPPORT D’ANALYSE

La fuite de données chez Maileva

22 millions de destinataires touchés par une fuite chez un prestataire de courrier

PÉRIODE COUVERTE ET ARRÊT DES RECHERCHES

De la mi-septembre au 17 novembre 2026. Sources consultées jusqu’au 17 novembre à 15:51 (heure de Paris), soit 14:51 GMT.

DATE DE PUBLICATION

2026-11-17

Les hôpitaux et d’autres organismes peuvent confier l’envoi de leurs courriers à un prestataire que les destinataires ne connaissent pas forcément. Selon La Poste, une cyberattaque contre Maileva en septembre a exposé les noms, prénoms et adresses postales de 22 millions de personnes.

L’avis publié par un hôpital montre que les conséquences d’une fuite peuvent varier selon l’expéditeur et le contenu du courrier. [1] [2] [3] [4]

Édition française traduite de la version anglaise. Traduction révisée avec une assistance linguistique automatisée, sans certification humaine.

01 / SYNTHÈSE

Les faits et leurs conséquences

PAYS

France

LIEU

France. Maileva est une filiale de Docaposte, qui appartient au groupe La Poste. Des organismes clients ont précisé les conséquences de l'incident pour leurs propres courriers. [1] [3] [4]

DATE

Intrusion à la mi-septembre 2026. L'ampleur de la fuite a été confirmée publiquement les 14 et 15 novembre. Sources consultées jusqu'au 17 novembre. [1] [2] [7]

Les faits

La Poste a annoncé qu'une cyberattaque contre Maileva, son prestataire de gestion du courrier professionnel, avait exposé les noms, prénoms et adresses postales de 22 millions de destinataires. Le groupe a indiqué que la CNIL avait été informée et qu'une plainte avait été déposée. Le parquet de Paris a confirmé à l'AFP qu'un service de police spécialisé était chargé de l'enquête. [1] [2] [6]

Risques

Les données d'identité exposées peuvent faciliter les tentatives d'usurpation d'identité et les demandes de paiement frauduleuses. Les avis publiés par certains expéditeurs montrent que les risques varient selon les courriers et peuvent concerner des informations sensibles. [3] [4] [8]

> CONCLUSION
>
> Pour un destinataire, la question est de savoir quel expéditeur et quel envoi sont concernés. Pour les enquêteurs, l'exposition des données d'identité, celle des métadonnées d'envoi, l'accès aux documents et les fraudes ultérieures doivent chacun être établis par des éléments distincts. [1] [3] [4] [5] [8]

02 / CHRONOLOGIE

De l’intrusion de septembre à l’annonce de novembre

DATE	ÉVÉNEMENT	CE QUE LA SOURCE ÉTABLIT
Mi-septembre	Cyberattaque contre Maileva	La Poste situe l’intrusion à la mi-septembre. Le groupe indique avoir commencé à informer les organismes clients concernés dans les jours qui ont suivi l’identification de l’incident. [1]
9 octobre	Avis d’un service de santé au travail	Santé au travail en Cornouaille publie un avis décrivant l’exposition de données de suivi du courrier et précise quels champs supplémentaires sont concernés dans son cas. [3]
28 octobre	L’Hôpital Foch est informé d’un possible accès à des courriers	L’hôpital indique avoir appris le 28 octobre que certaines relances de paiement avaient pu être consultées. Un média spécialisé date l’avis de l’hôpital du 6 novembre. [4] [5]
14–15 novembre	Annonce publique de l’ampleur de la fuite	La Poste confirme le chiffre à l’AFP le 14 novembre et publie un communiqué le 15 novembre. Le parquet de Paris confirme qu’un service spécialisé est chargé de l’enquête. [1] [2] [6]
16–17 novembre	Suivi médiatique	La presse spécialisée précise la distinction entre le bilan communiqué par le groupe et les avis publiés par certains de ses clients. [7] [13]

Il faut distinguer la date de l’attaque en septembre, celle à laquelle un expéditeur en a appris les conséquences et celle de l’annonce publique en novembre. Les sources consultées ne permettent pas de dater précisément la notification à la CNIL ni de savoir quand chaque destinataire a été informé. [1] [3] [4] [7] [9]

03 / PÉRIMÈTRE DE LA FUITE

Quelles données ont été exposées, et pour qui ?

PÉRIMÈTRE	CE QUE LES SOURCES ÉTABLISSENT	LIMITE
22 millions de destinataires	La Poste indique que des noms, prénoms et adresses postales ont été exposés.	L'estimation porte sur le nombre de personnes déclarées concernées. Elle ne chiffre ni les documents volés, ni les pertes financières, ni les fraudes ultérieures. Le communiqué ne précise pas la méthode de comptage. [1] [2]
Suivi du courrier chez un client	Le service de santé au travail indique que des données sur les expéditeurs, la civilité ou le genre des destinataires et des noms de fichiers ont également pu être exposés.	L'avis porte sur ce service, qui ne dispose d'aucun élément établissant que le contenu de ses documents a été consulté ou extrait. [3]
Certaines relances de l'Hôpital Foch	L'hôpital indique que certaines relances de paiement ont pu être consultées. Elles contenaient des numéros de facture, des dates de soins et les montants dus. L'hôpital cite Kiwee comme intermédiaire.	L'avis concerne les courriers en question. Il n'établit ni qu'une intrusion a touché le réseau de l'hôpital ni que l'ensemble des documents traités par Maileva étaient accessibles. [4] [5]

La différence pour les destinataires

Un nom et une adresse postale peuvent rendre une usurpation d'identité crédible. L'identité de l'expéditeur ou le contexte du courrier peut rendre les données plus sensibles, notamment si ces éléments révèlent un lien avec un organisme de santé. Les sources établissent une exposition ou un accès possible aux données, sans chiffrer les fraudes qui auraient suivi. [1] [3] [4] [8]

04 / UN CAS DOCUMENTÉ

Un courrier hospitalier, plusieurs organismes impliqués



Photo 1. L'Hôpital Foch à Suresnes, photographié par Celette le 23 juin 2018. Image d'archives de l'établissement qui a publié un avis. Photo redimensionnée. CC BY-SA 4.0 [4] [12]

EXPÉDITEUR	INTERMÉDIAIRE	PRESTATAIRE DE COURRIER	DESTINATAIRE
Hôpital Foch	Kiwee	Maileva	Patient destinataire d'une relance visée par l'avis [4] [5]

L'avis de l'hôpital concerne des relances de la période du 9 au 23 septembre. Cette chaîne d'intervenants est propre à ce cas. Un patient peut connaître l'hôpital qui lui a écrit sans avoir de relation directe avec l'entreprise qui a traité le courrier. [4] [5]

Lorsqu'un expéditeur signale que des courriers ont été concernés ou que des documents ont pu être consultés, il importe de connaître le type de document, la période, les champs exposés et les destinataires concernés. Ces précisions comptent davantage que le chiffre global annoncé. [1] [3] [4]

05 / CONSÉQUENCES POUR LE PUBLIC ET LES ENTREPRISES

Qui supporte le coût d'une telle fuite ?

Pour les destinataires

Face à une demande inattendue d'argent ou de données personnelles, vérifiez-la auprès de l'expéditeur en utilisant des coordonnées dont vous êtes sûr ou que vous trouvez sur son site officiel. Si vous avez déjà envoyé de l'argent ou communiqué des coordonnées bancaires en réponse à une sollicitation suspecte, contactez rapidement votre banque et conservez les échanges. [4] [8]

Pour les organisations

Les coûts probables comprennent l'enquête sur le périmètre de la fuite, l'identification des envois concernés, le traitement des demandes des destinataires et la coordination des avis entre prestataires. Les sources consultées ne fournissent aucun chiffrage fiable pour Maileva. Dans le cadre du RGPD présenté par la CNIL, les rôles et le niveau de risque déterminent qui doit informer l'autorité et les personnes concernées. Le communiqué ne suffit pas à déterminer quelles obligations de notification s'appliquaient ni si elles ont été respectées. [1] [3] [4] [9]

L'intérêt de la comparaison avec un vol financier

Le 12 novembre, le ministère américain de la Justice a annoncé des mesures de saisie et de gel autorisées par la justice, portant sur plus de 1,2 milliard de dollars en cryptomonnaies volées à Binance. Le 4 novembre, Crédit Mutuel Arkéa a indiqué que des opérations frauduleuses avaient touché ses propres fonds et que le montant était encore en cours d'évaluation. Pour Maileva, le chiffre de 22 millions porte sur des personnes. Dans une fuite de données, fermer l'accès ne permet pas de récupérer les informations déjà sorties. [1] [10] [11]

La comparaison porte sur les conséquences et les possibilités de récupération. Les sources consultées n'établissent aucun lien opérationnel entre ces affaires. [1] [10] [11]

06 / EXAMEN DES ÉLÉMENTS DE PREUVE

Ce qui pourrait changer l’évaluation

QUESTION	ÉLÉMENTS À RECHERCHER
Comment le chiffre de 22 millions a-t-il été établi ?	Un bilan daté précisant la méthode de comptage, la suppression des doublons et, le cas échéant, un total révisé. [1]
Pour quels courriers un accès était-il possible ?	Un rapprochement, expéditeur par expéditeur, entre les avis, les champs concernés et les périodes visées, en distinguant un accès possible d’une divulgation confirmée. [3] [4] [5]
Les données ont-elles ensuite servi à commettre des fraudes ?	Des signalements de victimes corroborés ou des conclusions d’enquête reliant une escroquerie précise à cette fuite, dans le respect des données personnelles. [6] [8]

La publication du chiffre de 22 millions par La Poste et l’existence d’avis propres à certains clients sont bien établies. Les sources publiques consultées ne permettent pas de connaître le jeu de données exact, la liste complète des destinataires concernés, l’identité de l’auteur ni les pertes imputables à la fuite. [1] [3] [4] [6] [7]

REGISTRE DES SOURCES

Sources 01–05

Le registre indique l'origine des informations et les limites d'accès. La reprise d'une déclaration ne constitue pas une preuve indépendante.

01 Cyberattaque de Maileva, ce qu'il faut savoir

La Poste Groupe · 15 nov. 2026

Origine de l'information – Communiqué du groupe · Confirme le chiffre de 22 millions et précise les données des destinataires concernées.

https://www.lapostegroupe.com/fr/actualite/cyberattaque-de-maileva-ce-quil-faut-savoir

02 Une filiale de La Poste victime d'un vol de données massif, 22 millions de personnes concernées

AFP / **TV5MONDE** · 14 nov. 2026

Origine de l'information – Dépêche reprenant la confirmation du groupe · L'AFP relaie le bilan du groupe. Ces déclarations ont la même origine que celles du communiqué [1].

https://information.tv5monde.com/economie/une-filiale-de-la-poste-victime-dun-vol-de-donnees-massif-22-millions-de-personnes-concernees-2845846

03 Incident de sécurité ayant affecté l'un de nos prestataires, la société MAILEVA

Santé au travail en Cornouaille · 9 oct. 2026

Origine de l'information – Avis publié par un client · Données de suivi propres à cet organisme et réserves sur l'accès à ses documents.

https://www.stc-quimper.org/type-dactualite/vie-de-lassociation-13

04 Violations de données Maileva-Kiwicare

Hôpital Foch · 6 nov. 2026, date rapportée

Origine de l'information – Avis publié par un client, extraits indexés · Les extraits indexés précisent les faits. La page n'était pas directement accessible lors de la vérification. À lire avec [5].

https://www.hopital-foch.com/actualites/violations-de-donnees-maileva-kiwicare/

05 Docaposte confirme le vol des adresses de 22 millions de Français après une cyberattaque chez cette filiale de La Poste

Cyberattaque.org · Mis à jour le 12 nov. 2026

Origine de l'information – Enquête spécialisée et avis d'expéditeurs · Rend compte de l'avis de l'hôpital et le date du 6 novembre. L'article relaie la réponse de l'opérateur.

https://www.cyberattaque.org/maileva-docaposte-la-poste-cyberattaque/

REGISTRE DES SOURCES

Sources 06–09

Le registre indique l'origine des informations et les limites d'accès. La reprise d'une déclaration ne constitue pas une preuve indépendante.

06 Cyberattaque d'une filiale de La Poste : la Brigade cybercriminalité enquête

AFP / **Zonebourse** · 15 nov. 2026

Origine de l'information – Parquet de Paris, par l'intermédiaire de l'AFP · Attribution limitée à la confirmation du service chargé de l'enquête.

https://www.zonebourse.com/actualite-bourse/cyberattaque-d-une-filiale-de-la-poste-la-brigade-cybercriminalite-enquete-ce785ededc81ff21

07 Criminals attack French postal operator subsidiary, grab contact details of 22M people

The Register · 16 nov. 2026

Origine de l'information – Presse spécialisée, déclarations de l'opérateur et de clients · Consulté pour recouper le périmètre communiqué et les avis publiés par les clients.

https://www.theregister.com/cyber-crime/2026/11/16/criminals-attack-french-postal-operator-subsidiary-grab-contact-details-of-22m-people/5310070

08 Violation ou fuite de données personnelles, que faire ?

Cybermalveillance.gouv.fr · Consulté le 17 nov. 2026

Origine de l'information – Recommandations officielles au public · Risques généraux et conseils de protection.

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-fuite-de-donnees-personnelles

09 Chapitre IV – Responsable du traitement et sous-traitant

CNIL · Consulté le 17 nov. 2026

Origine de l'information – Autorité de protection des données / RGPD · Cadre général, notamment les articles 33 et 34. Aucune conclusion sur ce dossier.

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4

REGISTRE DES SOURCES

Sources 10–13

Le registre indique l'origine des informations et les limites d'accès. La reprise d'une déclaration ne constitue pas une preuve indépendante.

10 Justice Department Announces Actions to Disrupt North Korea's Massive Theft of Cryptocurrency

Ministère américain de la Justice · 12 nov. 2026

Origine de l'information – Communiqué officiel sur les mesures judiciaires · Utilisé uniquement pour les mesures autorisées par la justice sur les avoirs liés à Binance.

https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-north-koreas-massive-theft-cryptocurrency

11 Informations complémentaires suite à l'attaque dont le Crédit Mutuel Arkéa a été victime

Crédit Mutuel Arkéa · 4 nov. 2026

Origine de l'information – Communiqué de l'entreprise · Utilisé uniquement pour préciser que les fonds de la banque ont été touchés et que le bilan restait provisoire.

https://www.cm-arkea.com/arkea/banque/assurances/pa_38386/fr/informations-complementaires-suite-a-l-attaque-dont-le-credit-mutuel-arkea-a-ete-victime

12 Hôpital Foch (Suresnes) 1.jpg

Celette / **Wikimedia Commons** · 23 juin 2018

Origine de l'information – Photographie d'archives · CC BY-SA 4.0. La légende renvoie à la licence. Photo redimensionnée sans recadrage.

https://commons.wikimedia.org/wiki/File:H%C3%B4pital_Foch_(Suresnes)_1.jpg

13 22 million impacted in attack on French postal subsidiary

IT Pro · 17 nov. 2026

Origine de l'information – Suivi par la presse spécialisée · Article de suivi. La reprise du chiffre de l'opérateur ne constitue pas une vérification indépendante.

https://www.itpro.com/security/cyber-attacks/22-million-impacted-in-attack-on-french-postal-subsidiary