Stop Escroc

AUDIT DE SÉCURITÉ PERSONNEL

Rapport d'exposition aux fuites de données

Établi pour **Madame Sandrine Lemoine**

Document strictement personnel et confidentiel

DATE	RÉFÉRENCE	FUITES	NIVEAU D'EXPOSITION
29 octobre 2026	SE-AUD-20261029-EX	7 confirmées	Critique

01 — SYNTHÈSE

L'essentiel en une page

Madame Lemoine, nous avons recherché vos informations dans les bases de données de fuites connues. Voici ce que nous avons trouvé, ce que cela signifie, et par où commencer.

7
fuites confirmées

1
fuite avec un mot de passe

4
données d'identité exposées

2019 – 2025
période couverte

NIVEAU D'EXPOSITION GLOBAL

Critique

Faible | Modéré | Élevé | **Critique**

Vos données permettent dès aujourd'hui de prendre le contrôle de comptes ou d'engager des opérations à votre nom. Les actions du jour sont à faire sans attendre. Votre **nom, date de naissance, téléphone, adresse** figurent dans au moins une fuite.

INFORMATIONS VÉRIFIÉES

ÉLÉMENT	VALEUR	RÉSULTAT
Adresse email	**s.lemoine@example.com**	⚠ **6 fuites confirmées** Dont une base de mots de passe en clair et une compilation d'identifiants revendue.
Téléphone mobile	**+33 6 12 34 56 78**	⚠ **4 fuites confirmées** Associé à votre nom complet et à votre adresse postale dans trois d'entre elles.
Nom et prénom	**Sandrine Lemoine**	⚠ **5 fuites confirmées** Votre identité complète apparaît dans un fichier opérateur de 2025.
Coordonnées bancaires	**IBAN FR76 ···· ···· ···· ··42**	⚠ **1 fuite confirmée — critique** IBAN en clair dans un fichier de gestion locative. Un prélèvement frauduleux est possible.
Mots de passe	**3 mots de passe retrouvés (partiellement lisibles)**	⚠ **3 fuites confirmées — critique** Deux sont en clair, un a été décrypté. Vérifiés : ils servent encore sur d'autres sites.

Vos 3 priorités dès aujourd'hui

1. **Prévenir votre banque que votre IBAN a fuité**
   Vérifiez chaque prélèvement sur vos relevés et demandez à votre banque comment limiter les prélèvements aux seuls organismes que vous autorisez. Un prélèvement que vous n'avez pas autorisé se conteste auprès d'elle, au plus tard 13 mois après la date de l'opération.

2. **Changer le mot de passe de votre messagerie s.lemoine@example.com**
   C'est la clé de tous vos autres comptes : quiconque y accède peut réinitialiser vos autres mots de passe. Choisissez un mot de passe long, jamais utilisé ailleurs.

3. **Remplacer tout mot de passe ancien ou réutilisé**
   En priorité : banque, impôts, Assurance maladie, sites marchands où votre carte est enregistrée, réseaux sociaux. Un mot de passe différent pour chacun.

02 — CARTOGRAPHIE

Quelles données, dans quelles fuites

Chaque ligne est une fuite, chaque colonne une catégorie de données. Une même information peut apparaître dans plusieurs fuites : elle a alors été copiée et recoupée par différents fraudeurs.

SOURCE	EMAIL	MOT DE PASSE	NOM	NAISSANCE	TÉLÉPHONE	ADRESSE	BANQUE	GRAVITÉ
Cabinet de gestion locative Mars 2025	–	–	●	–	–	●	●	Critique
Collection #1 (compilation) Janvier 2019	●	●	–	–	–	–	–	Critique
Opérateur télécom Août 2025	●	–	●	●	●	●	●	Critique
Free et Free Mobile Octobre 2024	–	–	–	–	–	–	–	Critique
Almerys (tiers payant santé) Janvier 2024 (annoncée le 7 février 2024)	–	–	–	–	–	–	–	Critique
Réseau de restauration Décembre 2024	●	–	–	●	●	–	–	Élevé
Librairie en ligne Octobre 2022	●	–	●	–	–	●	–	Modéré

DONNÉES EXPOSÉES AU MOINS UNE FOIS

Nom et prénom · Adresse postale · IBAN · Adresse email · Mot de passe en clair · Numéro de téléphone · Date de naissance

LECTURE DES NIVEAUX DE GRAVITÉ

Critique · Élevé · Modéré · Faible

La gravité dépend de ce que la fuite permet de faire : un mot de passe lisible ou une identité complète pèsent plus lourd qu'une adresse email seule.

Pourquoi des fuites anciennes comptent encore. Une donnée volée en 2012 circule toujours aujourd'hui : les fichiers sont copiés, fusionnés et revendus sans fin. Un ancien mot de passe reste dangereux tant qu'il est utilisé quelque part, même sous une forme légèrement modifiée.

03 — DÉTAIL DES FUITES

Ce qui a fuité, et ce que cela implique

Les fuites sont classées de la plus grave à la moins grave. Pour votre sécurité, certaines valeurs sont volontairement masquées dans ce rapport (···).

FUITE 1 / 7

Cabinet de gestion locative

Critique

exemple-gestion.fr · Mars 2025 · 48 000 dossiers de locataires

Un prestataire de la plateforme de gestion locative a exposé une base de dossiers en libre accès pendant près de six semaines. Les dossiers complets des candidats locataires y figuraient, sans chiffrement, accessibles depuis une simple adresse web.

DONNÉES EXPOSÉES

Nom et prénom · Adresse postale · IBAN

IBAN	FR76 1751 5··· ···· ···· ··42
BIC	CEPA·····
Adresse	9 RUE DES ÉCO···, 44000 NANTES
Revenus déclarés	2 4·· € net / mois
Pièce d'identité	CNI ·····42 (recto-verso)

CE QUE CELA PERMET À UN ESCROC

Votre IBAN associé à votre pièce d'identité, c'est exactement ce qu'il faut pour ouvrir un compte à votre nom ou faire signer un mandat de prélèvement. Un escroc peut aussi reprendre votre dossier complet pour se faire passer pour un propriétaire auprès de vous ou pour vous louer un logement qui n'existe pas.

À FAIRE

- Mettre en place un mandat SEPA interdit de prélèvement auprès de votre banque.
- Vérifier sur le portail de la Banque de France qu'aucun mandat de prélèvement inconnu n'est enregistré.
- Signaler la fuite à la CNIL, avec la capture de la page web exposée.
- Contester tout prélèvement non reconnu dans les 13 mois.

FUITE 2 / 7

Collection #1 (compilation)

Critique

forum de pirates · Janvier 2019 · 773 millions d'adresses email uniques

En janvier 2019, une immense compilation de listes de « credential stuffing », baptisée Collection #1, a été diffusée sur un forum de pirates : environ 2,7 milliards de lignes, dont 773 millions d'adresses email uniques, associées aux mots de passe que ces adresses avaient utilisés sur d'autres sites piratés.

DONNÉES EXPOSÉES

Adresse email · Mot de passe en clair

Adresse email	s.lemoine@example.com
Mot de passe	Lemo····2024
Mot de passe (2e)	Nantes····44

CE QUE CELA PERMET À UN ESCROC

Avec votre email et un mot de passe, un escroc teste la connexion sur des centaines de sites en quelques secondes. La moitié des gens réutilisent le même mot de passe : c'est ce qui déclenche les « colis à payer », les faux virements et les vols de comptes de messagerie.

À FAIRE

- Remplacer « Lemo····2024 » et « Nantes····44 » partout où vous les avez utilisés, en commençant par la messagerie.
- Activer la double authentification sur votre boîte email et votre banque : sans le code, le mot de passe ne suffit plus.
- Vérifier vos règles de redirection de courrier : les escrocs en posent une pour lire vos emails sans se connecter.
- Vérifier les récupérations de mot de passe que vous n'avez pas demandées.

FUITE 3 / 7

Opérateur télécom

Critique

operateur-exemple.fr · Août 2025 · 5,7 millions de comptes clients

Un opérateur a annoncé avoir été victime d'une intrusion avec vol de fichiers clients, incluant les contrats et les coordonnées bancaires. L'information a été révélée publiquement plusieurs semaines après les faits.

DONNÉES EXPOSÉES

Nom et prénom · Numéro de téléphone · Adresse email · Adresse postale · Date de naissance · IBAN

Téléphone	+33 6 12 ·· ·· 78
Adresse	9 RUE DES ÉCO···, 44000 NANTES
Date de naissance	··/04/1987
IBAN	FR76 1751 5··· ···· ···· ··42

CE QUE CELA PERMET À UN ESCROC

Avec vos nom, téléphone et adresse, le démarchage devient ciblé : l'escroc sait exactement quoi dire pour paraître crédible. Sur ce type de fichier, les appels « votre ligne va être coupée, confirmez vos coordonnées » arrivent des mois après et visent l'IBAN.

À FAIRE

- Inscrire votre numéro sur la liste d'opposition au démarchage téléphonique (BlocTel).
- Ne jamais confirmer votre IBAN, un mot de passe ou un code reçu par SMS à un appelant, même s'il connaît votre adresse.
- Demander à votre banque le mandat SEPA interdit si un prélèvement non reconnu apparaît.

FUITE 4 / 7

Free et Free Mobile

Critique

free.fr · Octobre 2024 · 24 millions de contrats d'abonnés

En octobre 2024, un attaquant a accédé aux données de « 24 millions de contrats d'abonnés » de Free et Free Mobile, dont des IBAN lorsque les personnes étaient clientes des deux. La CNIL a sanctionné les deux sociétés par des amendes de 27 millions d'euros (Free Mobile) et 15 millions d'euros (Free), par décisions du 8 janvier 2026.

DONNÉES EXPOSÉES

Téléphone	+33 6 12 ·· ·· 78
Adresse	9 RUE DES ÉCO···, 44000 NANTES
Date de naissance	··/04/1987

CE QUE CELA PERMET À UN ESCROC

FUITE 5 / 7

Almerys (tiers payant santé)

Critique

almerys.com · Janvier 2024 (annoncée le 7 février 2024) · Plus de 33 millions de personnes (Viamedis et Almerys)

Début 2024, deux opérateurs de tiers payant, Viamedis et Almerys, qui gèrent pour des complémentaires santé le paiement direct des professionnels de santé, ont subi une violation de données. Selon la CNIL, elle concerne « plus de 33 millions de personnes » et porte sur l'état civil, la date de naissance, le numéro de sécurité sociale, le nom de l'assureur santé et les garanties du contrat. Toujours selon la CNIL, ni les informations bancaires, ni les données médicales, ni les remboursements, ni les coordonnées postales, téléphoniques ou email ne seraient touchés.

DONNÉES EXPOSÉES

CE QUE CELA PERMET À UN ESCROC

Un numéro de sécurité sociale avec votre nom et votre date de naissance permet de se faire passer pour vous auprès d'un professionnel de santé, de changer de mutuelle ou d'obtenir des prestations. C'est un des pires ensembles à protéger : il ne change jamais, même en cas de fuite.

À FAIRE

- Vérifier auprès de votre complémentaire santé qu'aucune demande de rattachement n'a été faite à votre nom.
- Surveiller vos remboursements : un remboursement que vous ne reconnaissez pas est souvent le premier signe.
- Demander à l'Assurance Maladie un relevé de vos prestations des 12 derniers mois.

FUITE 6 / 7

Réseau de restauration

Élevé

exemple-resto.fr · Décembre 2024 · 230 000 comptes

Une chaîne de restauration a subi le vol de sa base de programmes de fidélité : emails, téléphones et dates de naissance des clients.

DONNÉES EXPOSÉES

Adresse email · Numéro de téléphone · Date de naissance

Email	s.lemoine@example.com
Téléphone	+33 6 12 ·· ·· 78

CE QUE CELA PERMET À UN ESCROC

Ces données servent aux campagnes de phishing par SMS (smishing) : « vous avez gagné un repas », un lien à ouvrir, vos coordonnées bancaires à saisir. Le message est crédible parce qu'il vient d'une marque que vous connaissez vraiment.

À FAIRE

- Ne pas cliquer sur les liens de bons ou de remises reçus par SMS.
- Signaler les messages frauduleux au 33700.
- Vérifier vos commandes depuis le site officiel, jamais depuis le lien du message.

FUITE 7 / 7

Librairie en ligne

Modéré

exemple-livres.fr · Octobre 2022 · Non communiqué

Un site marchand a laissé fuiter sa base clients après une faille de son logiciel de boutique en ligne.

DONNÉES EXPOSÉES

Adresse email · Nom et prénom · Adresse postale

Email	s.lemoine@example.com
Adresse	9 RUE DES ÉCO···, 44000 NANTES

CE QUE CELA PERMET À UN ESCROC

Nom, email et adresse suffisent pour des courriers ou des colis frauduleux à votre nom : un faux avis de passage, une facture déguisée, un abonnement activé sans vous.

À FAIRE

- Ne payer aucun avis de livraison reçu par SMS ou courrier sans vérifier auprès du transporteur.
- Ne confirmer aucune commande que vous n'avez pas passée.

04 — MENACES

Ce qu'un escroc peut faire avec vos données

Ces scénarios ne sont pas théoriques : ce sont ceux que permettent précisément les données retrouvées à votre nom. Savoir les reconnaître, c'est déjà les déjouer.

⚠ Prise de contrôle de vos comptes

Les pirates testent automatiquement vos anciens couples email / mot de passe sur des centaines de sites : messagerie, banque, sites marchands, réseaux sociaux. Si un mot de passe a été réutilisé, même légèrement modifié, ils entrent sans effort.

LES SIGNES QUI DOIVENT ALERTER

- Un email « nouvelle connexion » que vous n'avez pas faite
- Un mot de passe soudain refusé
- Des commandes ou des messages envoyés à votre insu

Le bon réflexe : Un mot de passe différent pour chaque site, et la double authentification sur les comptes importants.

⚠ Faux conseiller bancaire ou faux service public

L'escroc vous appelle en citant votre nom, votre date de naissance ou votre code postal pour gagner votre confiance. Il invente ensuite une urgence (opération suspecte, remboursement en attente) pour vous faire valider un paiement, donner un code ou faire un virement « de sécurité ».

LES SIGNES QUI DOIVENT ALERTER

- Une urgence et une pression pour agir tout de suite
- La demande d'un code reçu par SMS
- Un virement « vers un compte sécurisé »
- Un numéro affiché qui ressemble à celui de votre banque

Le bon réflexe : Raccrochez, puis rappelez vous-même votre banque au numéro inscrit au dos de votre carte.

⚠ Hameçonnage (phishing) personnalisé

Connaissant votre adresse et certains services que vous utilisez, l'escroc envoie un message qui en imite un (livraison, impôts, Assurance maladie, réseau social) avec un lien vers un faux site conçu pour voler vos identifiants ou votre carte bancaire.

LES SIGNES QUI DOIVENT ALERTER

- Une adresse d'expéditeur inhabituelle
- Un lien qui mène vers un site au nom étrange
- Une demande de « mettre à jour » vos informations de paiement

Le bon réflexe : Ne cliquez pas sur le lien : ouvrez vous-même le site ou l'application officielle.

⚠ Usurpation d'identité

Nom, date de naissance et coordonnées sont les premières briques d'une usurpation d'identité. L'escroc les complète ensuite (copie de pièce d'identité obtenue par ruse, justificatif de domicile) pour souscrire un abonnement, un crédit ou ouvrir un compte à votre nom.

LES SIGNES QUI DOIVENT ALERTER

- Un courrier pour un contrat que vous n'avez pas souscrit
- Des relances pour une dette inconnue
- Une demande de copie de pièce d'identité « pour vérification »

Le bon réflexe : Ne transmettez jamais une pièce d'identité à un interlocuteur que vous n'avez pas contacté vous-même.

⚠ Prélèvements frauduleux et faux conseiller « qui voit votre compte »

Avec votre IBAN, un fraudeur peut tenter de mettre en place des prélèvements à votre nom, ou vous appeler en se présentant comme votre banque : il cite vos coordonnées bancaires, annonce une opération suspecte et vous pousse à valider un paiement ou à virer votre argent « vers un compte sécurisé ».

LES SIGNES QUI DOIVENT ALERTER

- Un prélèvement d'un organisme que vous ne connaissez pas
- Un appel de votre « banque » qui cite votre IBAN et parle d'urgence
- Une demande de valider une opération dans votre application pendant l'appel

Le bon réflexe : Raccrochez et rappelez votre conseiller au numéro habituel. Aucune banque ne demande de virer votre argent pour le protéger.

⚠ Appels et SMS frauduleux

Un numéro qui circule dans une fuite reçoit davantage de démarchage, d'appels frauduleux et de SMS piégés (colis en attente, amende impayée, compte bloqué).

LES SIGNES QUI DOIVENT ALERTER

- Un SMS avec un lien et une urgence
- Un appel d'un numéro inconnu qui « connaît » votre nom

Le bon réflexe : Transférez gratuitement les SMS frauduleux au 33700, et ne rappelez jamais un numéro laissé en message.

05 — RÉPARER

Votre plan d'action, étape par étape

Cochez chaque action au fur et à mesure. Les premières sont les plus importantes : elles neutralisent l'essentiel du risque en moins d'une heure.

Aujourd'hui dans les 24 heures

- [ ] **Prévenir votre banque que votre IBAN a fuité**
  Vérifiez chaque prélèvement sur vos relevés et demandez à votre banque comment limiter les prélèvements aux seuls organismes que vous autorisez. Un prélèvement que vous n'avez pas autorisé se conteste auprès d'elle, au plus tard 13 mois après la date de l'opération.

- [ ] **Changer le mot de passe de votre messagerie s.lemoine@example.com**
  C'est la clé de tous vos autres comptes : quiconque y accède peut réinitialiser vos autres mots de passe. Choisissez un mot de passe long, jamais utilisé ailleurs.

- [ ] **Remplacer tout mot de passe ancien ou réutilisé**
  En priorité : banque, impôts, Assurance maladie, sites marchands où votre carte est enregistrée, réseaux sociaux. Un mot de passe différent pour chacun.

- [ ] **Activer la double authentification**
  Un code envoyé sur votre téléphone ou une application est demandé en plus du mot de passe : un mot de passe volé ne suffit plus pour entrer.

- [ ] **Contrôler les réglages de votre messagerie**
  Vérifiez qu'aucune règle de transfert automatique, adresse de récupération ou appareil connecté inconnu n'a été ajouté dans les paramètres.

- [ ] **Considérer vos informations comme connues des escrocs**
  Un appel, un SMS ou un email qui cite votre nom, votre date de naissance ou votre numéro de sécurité sociale ne prouve plus rien. Ne donnez jamais un code reçu par SMS, vos identifiants ou vos coordonnées bancaires à la suite d'un tel message : raccrochez et recontactez l'organisme vous-même.

Cette semaine dans les 7 jours

- [ ] **Prévenir votre banque**
  Signalez que vos données d'identité circulent, demandez à recevoir une alerte pour chaque opération, et vérifiez vos relevés chaque semaine pendant les prochains mois.

- [ ] **Prévenir vos proches**
  Un escroc peut utiliser vos informations pour les contacter en votre nom. Convenez d'un réflexe simple : en cas de demande inhabituelle, on rappelle toujours sur le numéro habituel.

- [ ] **Supprimer les comptes que vous n'utilisez plus : Cabinet de gestion locative, Collection #1, Opérateur télécom, Free et Free Mobile, Almerys, Réseau de restauration, Librairie en ligne**
  Un compte fermé ne peut plus fuiter. Si la suppression n'est pas proposée en ligne, utilisez le modèle de courrier en annexe.

Ce mois-ci pour durer

- [ ] **Adopter un gestionnaire de mots de passe**
  Il crée et retient un mot de passe différent pour chaque site : vous n'en mémorisez plus qu'un seul. Notre comparatif : stopescroc.fr/meilleur-gestionnaire-de-mots-de-passe-le-comparatif
- [ ] **Mettre en place une alerte de fuite**
  Inscrivez votre adresse sur haveibeenpwned.com (service gratuit) pour recevoir un email si elle apparaît dans une nouvelle fuite.
- [ ] **Réduire le démarchage téléphonique**
  Inscrivez gratuitement vos numéros sur la liste d'opposition Bloctel (bloctel.gouv.fr).
- [ ] **Vérifier vos relevés bancaires chaque mois**
  Une opération que vous n'avez pas autorisée se conteste auprès de votre banque, au plus tard 13 mois après la date de l'opération. Mieux vaut agir dès la découverte.

> **Comment créer un bon mot de passe ?** Le plus simple : une phrase de quatre ou cinq mots sans lien entre eux, que vous seul pouvez retenir, différente pour chaque site. Mieux encore : laissez un gestionnaire de mots de passe les générer pour vous.

06 — PRÉVENIR

Ne plus réapparaître dans les fuites

Soyons transparents : une fuite ne s'efface pas. Une fois copiées, les données circulent indéfiniment entre fraudeurs, et personne ne peut les retirer d'Internet. L'objectif réaliste est double : **rendre inutilisables les données déjà volées**, et **réduire au maximum ce qui pourra fuiter demain**.

01

Un mot de passe unique par site

Une fuite ne compromet alors qu'un seul compte, jamais les autres. Un gestionnaire de mots de passe les crée et les retient pour vous.

02

La double authentification partout

Messagerie, banque, réseaux sociaux, sites marchands : avec un second code, un mot de passe volé devient inutilisable.

03

Donner le moins possible

Date de naissance, téléphone, adresse : ne remplissez que les champs obligatoires. Une donnée jamais confiée ne peut pas fuiter.

04

Une adresse email pour les inscriptions

Gardez votre adresse principale pour la banque, les administrations et vos proches. Utilisez-en une seconde pour les achats en ligne, jeux-concours et newsletters.

05

Fermer les comptes inutilisés

Chaque compte dormant est une fuite potentielle. Faites le ménage une fois par an et demandez l'effacement de vos données.

06

Vérifier avant d'agir

Message urgent, demande de code, de paiement ou d'identifiants : on ne répond pas, on recontacte l'organisme par son canal officiel.

Faut-il changer d'adresse email ?

Pas forcément. Une adresse qui a fuité reçoit davantage de spam et de tentatives d'hameçonnage, mais elle reste sûre si son mot de passe est unique et que la double authentification est active. Changer d'adresse se justifie surtout si les messages frauduleux deviennent trop nombreux.

Rester informé dans la durée

Une alerte gratuite sur haveibeenpwned.com vous prévient si votre adresse apparaît dans une nouvelle fuite publique. Un audit complet périodique couvre en plus les fichiers non publics et vos autres coordonnées (téléphone, nom).

07 — RECOURS

Vos droits et vos recours

Figurer dans une fuite n'ouvre pas automatiquement droit à une indemnisation. En revanche, vous disposez de droits précis et gratuits, que vous pouvez exercer dès maintenant.

Ce que l'organisme responsable de la fuite doit faire

Le RGPD impose à l'organisme qui a laissé fuir des données de notifier la fuite à la CNIL, si possible au plus tard 72 heures après en avoir pris connaissance (article 33), et d'en informer directement les personnes concernées lorsque la fuite présente un risque élevé pour elles (article 34).

Savoir ce qu'il détient, et le faire supprimer

Vous pouvez demander à tout organisme quelles données il conserve sur vous (droit d'accès, article 15) puis leur suppression (droit à l'effacement, article 17). Il doit vous répondre dans un délai d'un mois, prolongeable de deux mois pour une demande complexe (article 12). Un modèle de courrier est fourni en annexe.

S'il ne répond pas

Sans réponse dans le délai, ou en cas de refus injustifié, vous pouvez adresser une plainte en ligne à la CNIL sur cnil.fr, en joignant une copie de votre demande.

Si vous subissez un préjudice

Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du RGPD a droit à réparation (article 82). Il faut alors démontrer le dommage et son lien avec la fuite, devant le juge civil : rapprochez-vous d'un avocat ou de France Victimes (116 006, gratuit).

Si vos données sont utilisées contre vous

Usurpation d'identité (article 226-4-1 du Code pénal) ou piratage d'un compte (article 323-1) : portez plainte, en ligne sur plainte-en-ligne.masecurite.interieur.gouv.fr, via THESEE pour une escroquerie en ligne, ou au commissariat. Pour un paiement par carte que vous n'avez pas fait : faites opposition auprès de votre banque, signalez-le sur Perceval et demandez le remboursement de l'opération non autorisée (article L.133-18 du Code monétaire et financier), au plus tard 13 mois après la date de l'opération.

POUR CHACUNE DE VOS FUITES, LE RECOURS RÉALISTE

FUITE	CE QUE VOUS POUVEZ FAIRE
Cabinet de gestion locative	Vous pouvez demander au responsable de traitement (le cabinet) une copie des données détenues, la suppression devenues inutiles, et des dommages si un préjudice est prouvé. L'article 32 du RGPD impose de chiffrer ces données : son non-respect est un manquement.
Collection #1 (compilation)	Fuite issue d'une compilation, l'attaquant est inconnu : le levier est la banque (en cas de fraude) et la CNIL pour la traçabilité du signalement.
Opérateur télécom	Si l'opérateur n'a pas la base légale ni les mesures de sécurité suffisantes, vous pouvez demander réparation du préjudice devant le tribunal. La CNIL peut être saisie.

FUITE	CE QUE VOUS POUVEZ FAIRE
Réseau de restauration	Signalement à la CNIL et au 33700. En cas de préjudice, la responsabilité de l'entreprise peut être engagée.
Librairie en ligne	Demande d'accès et de suppression auprès du site, puis signalement à la CNIL si la réponse est insuffisante.

Ce rapport est un document d'information et ne constitue pas une consultation juridique. Pour engager une action en justice, faites-vous conseiller par un avocat.

ANNEXE A

Modèle de courrier : accès et effacement

À envoyer au délégué à la protection des données (DPO) de chaque organisme concerné. Son adresse figure dans la politique de confidentialité du site. Par email ou par lettre recommandée avec accusé de réception ; gardez une copie.

Sandrine Lemoine
s.lemoine@example.com
[Votre adresse postale]

À l'attention du délégué à la protection des données
[Nom et adresse de l'organisme]

[Lieu], le **[date]**

Objet : demande d'accès et d'effacement de mes données personnelles (articles 15 et 17 du RGPD)

Madame, Monsieur,

J'ai appris que mes données personnelles, associées à l'adresse email s.lemoine@example.com, figurent dans une fuite de données concernant votre service.

Conformément à l'article 15 du RGPD, je vous demande de me communiquer l'ensemble des données personnelles me concernant que vous détenez, leur origine, les finalités de leur traitement et leur durée de conservation, ainsi que la liste des données concernées par cette fuite.

Conformément à l'article 17 du RGPD, je vous demande ensuite de supprimer l'ensemble de ces données et de clôturer mon compte.

Vous disposez d'un délai d'un mois à compter de la réception de ce courrier pour me répondre (article 12 du RGPD). À défaut de réponse satisfaisante, je me réserve la possibilité de saisir la CNIL.

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

[Signature]

ANNEXE B

Contacts utiles et glossaire

SERVICE	CONTACT	QUAND L'UTILISER
Votre banque	Numéro inscrit au dos de votre carte	Opération suspecte, opposition, doute sur un appel
Info Escroqueries	0 805 805 817 (gratuit, lun.–ven. 9h–18h30)	Être orienté après une arnaque ou une tentative
17Cyber	17cyber.gouv.fr	Assistance en cas de cybermalveillance
Cybermalveillance.gouv.fr	cybermalveillance.gouv.fr	Diagnostic, conseils et prestataires de confiance
Perceval	Portail masecurite.interieur.gouv.fr	Signaler un paiement frauduleux par carte bancaire
THESEE	Portail masecurite.interieur.gouv.fr	Plainte pour escroquerie en ligne, auteur inconnu
France Victimes	116 006 (gratuit)	Écoute et accompagnement des victimes
33700	Transférer le SMS au 33700	Signaler un SMS ou un appel frauduleux
Bloctel	bloctel.gouv.fr	S'opposer au démarchage téléphonique
CNIL	cnil.fr	Plainte si un organisme ne respecte pas vos droits
Have I Been Pwned	haveibeenpwned.com	Alerte gratuite en cas de nouvelle fuite

GLOSSAIRE

Fuite de données	Copie non autorisée d'une base de données (clients, abonnés) qui finit diffusée ou revendue.
Mot de passe en clair	Mot de passe stocké tel quel, lisible sans aucun décryptage.
Empreinte (hachage)	Version transformée d'un mot de passe. Les formats anciens (MD5, SHA1 sans « sel ») se décryptent facilement.
Credential stuffing	Test automatique, sur de nombreux sites, de couples email / mot de passe volés ailleurs.
Compilation (combolist)	Fichier qui regroupe des données issues de nombreuses fuites différentes.
Scraping	Collecte automatisée de données, ici en détournant une fonction d'un site.
Double authentification	Second code demandé en plus du mot de passe, envoyé par SMS ou généré par une application.
Hameçonnage (phishing)	Message frauduleux qui imite un organisme connu pour vous faire cliquer, payer ou donner vos identifiants.

ANNEXE C

Méthodologie et limites

Ce que nous avons fait

Les informations que vous nous avez transmises ont été recherchées le 29 octobre 2026 dans des bases de renseignement spécialisées qui recensent les fuites de données publiques et les fichiers en circulation, dont Have I Been Pwned. Chaque résultat a été vérifié, et les doublons (une même fuite référencée par plusieurs bases) ont été regroupés en une seule fiche.

Ce que nous n'avons pas fait

Aucune tentative de connexion à vos comptes, aucun accès à vos appareils ou à vos messageries. Les correspondances qui concernaient une autre personne (homonyme, numéro identique dans un autre pays) ont été écartées et ne figurent pas dans ce rapport.

Les limites de l'exercice

Ce rapport reflète les fuites connues à la date de l'audit. L'absence de résultat ne garantit pas qu'une donnée n'a jamais fuité : de nombreuses fuites ne sont jamais rendues publiques, ou le sont des années plus tard. Les dates et volumes indiqués sont ceux communiqués par les sources publiques.

Confidentialité

Ce document vous est personnel. Les valeurs sensibles y sont partiellement masquées. Ne le transférez qu'à une personne de confiance qui vous aide dans vos démarches.

Stop Escroc

Une question sur ce rapport ?

Nous restons disponibles pour vous aider à mettre en œuvre ces recommandations. Répondez simplement à l'email qui accompagnait ce rapport, en rappelant votre référence.

contact@stopescroc.fr

www.stopescroc.fr

Référence : SE-AUD-20261029-EX