AU QUOTIDIEN

03 Je me protège en adoptant de bonnes pratiques

- **Je ne communique que les informations nécessaires** dans mes démarches et j'évite de partager trop de données personnelles en ligne.
- Je ne transmets pas mes documents d'identité **sans m'être assuré de la légitimité du destinataire** (pièce d'identité, fiche de paie, avis d'imposition, RIB, etc.).
- **Je n'enregistre pas ma carte bancaire** lors d'achats en ligne.
- **J'utilise différentes adresses électroniques,** selon mes besoins.
- **Je sépare mes usages pros et persos** (messagerie, mots de passe, etc.).
- **Je supprime** les comptes inutilisés.

Et aussi :

- J'utilise des mots de passe robustes et différents pour chaque service.
- J'active la double authentification lorsque cela est possible.
- Je mets régulièrement à jour les appareils, logiciels et applications que j'utilise.
- Je fais des sauvegardes régulières de mes données.





Retrouvez l'ensemble des recommandations de la CNIL et de Cybermalveillance.gouv.fr sur :

cnil.fr

Cybermalveillance.gouv.fr

CYBER MOIS

Violation de données personnelles



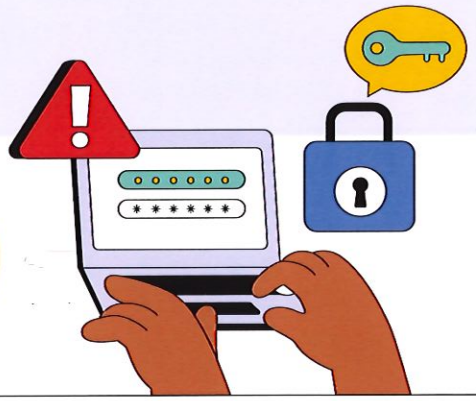
QUE FAIRE EN 3 ÉTAPES CLÉS

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en cybersécurité

J'ai reçu un message m'informant qu'une entreprise, une administration, une association ou un service en ligne a subi une fuite de données personnelles qui peut concerner mes informations.

Cela ne signifie pas que mes données ont déjà été utilisées de manière frauduleuse. Mais le risque d'hameçonnage, d'usurpation d'identité, d'arnaque ou de piratage de mes comptes peut augmenter. L'essentiel est de réagir rapidement, de rester vigilant dans les semaines suivantes, et d'adopter de bonnes pratiques au quotidien pour réduire les risques dans le temps.



01

LA PREMIÈRE SEMAINE

J'agis tout de suite, sans paniquer

****

Je vérifie les **données qui ont fuité.**

- **Je lis attentivement le message** que j'ai reçu.
- **Je conserve ce message,** qui pourra m'être utile plus tard.

Je change sans tarder mon mot de passe s'il a été compromis et choisis un mot de passe solide.

- Je modifie aussi le mot de passe **des autres comptes en ligne** utilisant le même mot de passe compromis, en priorisant celui de mon compte de messagerie principal.
- **J'active la double authentification,** si possible (par ex : code reçu par SMS, courriel ou par reconnaissance d'empreinte ou visage sur le téléphone).



Je suis très vigilant face aux tentatives d'arnaques (hameçonnage, fraude au faux conseiller bancaire...).

- **Je me méfie** des courriels, SMS ou appels inhabituels, alarmants ou trop attrayants.
- **Je ne clique pas sur les liens** dans les courriels ou SMS suspects et ne communique pas d'information par téléphone. **Je me connecte directement depuis le site ou l'application officiels.**

JE PROTÈGE MON COMPTE BANCAIRE

- J'informe ma banque de la fuite si des données bancaires sont concernées par la violation.
- Je surveille les éventuels mouvements suspects sur mes comptes.
- Je signale à ma banque toute opération non autorisée et demande son remboursement.
- Je fais opposition à ma carte si nécessaire.

02

DANS LES SEMAINES SUIVANTES

Je reste vigilant

Je continue à surveiller **mes comptes bancaires.**

- En activant les **notifications de paiement** si possible.
- En ne **signant aucun mandat de prélèvement dont je doute** de l'origine.
- Si ma banque le permet, en mettant en place **une « liste blanche »** des créanciers autorisés à effectuer des prélèvements sur mon compte.

Je protège **mon identité. Je reste vigilant si je constate notamment :**

- un courrier **inattendu** ;
- une demande de crédit **inconnue** ou un contrat ou abonnement **souscrit à mon insu** ;
- une **activité inhabituelle sur mes comptes** en ligne (Assurance maladie, impôts, etc.).

EN CAS D'ANOMALIE

Je contacte rapidement l'organisme concerné pour contester les opérations ou démarches frauduleuses.

Je vérifie **mes comptes en ligne** et leurs **paramétrages.**

- Je vérifie les appareils connectés ou sessions actives et **supprime tout accès non reconnu.**
- Je vérifie **mes numéros de téléphone** et **adresse électronique** de récupération.
- Pour ma messagerie, **je vérifie l'absence de redirection automatique** ou règle de filtrage créée à mon insu.
- Je fais des **captures d'écran des activités suspectes.**
- Je **modifie mon mot de passe** si je repère une activité suspecte et active si possible la double authentification.