



FUITE OU VIOLATION DE DONNÉES PERSONNELLES



Une fuite ou violation de données personnelles est l'accès ou la divulgation non autorisés d'informations personnelles détenues par un tiers (site Internet, entreprise, association, collectivité, administration...). Une donnée personnelle est une information susceptible de permettre d'identifier une personne (nom, adresse postale ou de messagerie, numéro de téléphone ou de sécurité sociale...). L'origine de la fuite peut être accidentelle ou malveillante. Selon la nature des informations concernées et si elles sont récupérées par des cybercriminels, une fuite de données personnelles peut avoir de multiples conséquences pour la personne qui en est victime : hameçonnage ciblé, escroquerie, usurpation d'identité, piratage de compte en ligne...

BUT RECHERCHÉ

Les informations personnelles divulguées (identité, mot de passe, données bancaires...) peuvent être récupérées par des cybercriminels pour en faire un usage frauduleux.

COMPRENDRE LES RISQUES

SI VOUS ÊTES VICTIME

Si vous êtes informé d'une violation de vos données personnelles, **LISEZ ATTENTIVEMENT LE COMMUNIQUE D'INFORMATION DE L'ORGANISME** afin de savoir quelles informations ont été compromises. Contactez au besoin le service ou organisme concerné pour la confirmer.

SOYEZ MÉFIANT FACE A TOUT APPEL TÉLÉPHONIQUE OU MESSAGE (mail, SMS, messageries instantanées, réseaux sociaux...) de personnes ou d'organismes qui prétendraient vous connaître à partir des informations dérobées.

CHANGEZ VOTRE MOT DE PASSE sur les sites ou services concernés par la fuite de données et sur tous les autres sites ou vous utilisiez ce même mot de passe. Si cela est disponible, **ACTIVEZ LA DOUBLE-AUTHENTIFICATION**.

Si des données bancaires (numéro de compte ou de carte, IBAN, RIB) sont dans la fuite de données, **SURVEILLEZ RÉGULIÈREMENT VOS COMPTES BANCAIRES** et signalez à votre banque tout opération suspecte.

SIGNELEZ ET DEMANDEZ LA SUPPRESSION DES PAGES, COMPTES, MESSAGES DIVULGUANT VOS INFORMATIONS PERSONNELLES auprès des plateformes sur lesquelles elles sont diffusées.

DEMANDEZ À CE QUE VOS DONNÉES PERSONNELLES DIVULGUÉES NE SOIENT PLUS RÉFÉRENCÉES PAR LES MOTEURS DE RECHERCHE lorsqu'elles y apparaissent.

Si, un mois après votre demande de suppression, vos données personnelles sont toujours accessibles, **VOUS POUVEZ ADRESSER UNE RÉCLAMATION (PLAINTÉ) À LA CNIL**.

En cas d'utilisation frauduleuse de vos données personnelles, conservez toutes les preuves et **DÉPOSEZ PLAINTÉ** au commissariat de police ou à la brigade de gendarmerie ou encore par écrit au procureur de la République du tribunal judiciaire dont vous dépendez.

MESURES PRÉVENTIVES

Ne communiquez que le minimum d'informations nécessaires sur les sites ou services en ligne.



Ne communiquez pas de documents d'identité de manière inconsidérée (pièce d'identité, fiche de paie, avis d'imposition, RIB, etc.).



N'enregistrez pas vos coordonnées de carte bancaire pour des achats ponctuels sur un site Internet. Si vous les avez enregistrées, supprimez-les.



Utilisez des mots de passe différents et complexes pour chaque site et application pour que la compromission d'un de vos mots de passe n'impacte pas vos autres comptes. Tous nos conseils pour gérer vos mots de passe.



Activez la double authentification pour augmenter le niveau de sécurité d'accès à vos comptes lorsque le site ou le service le permettent.



Désabonnez-vous ou supprimez les comptes en ligne que vous n'utilisez plus pour limiter les risques de fuite de vos données.



Faites valoir votre droit de suppression de vos données personnelles auprès des organismes et services avec lesquels vous n'avez plus de relation. La CNIL peut être saisie en cas de difficulté.





LES INFRACTIONS

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

- **Escroquerie (article 313-1 du code pénal)** : l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. Délit passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende.
- **Usurpation d'identité (article 226-4-1 du code pénal)** : le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est passible d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende.
- **Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite (article 226-18 du code pénal)** : une telle collecte constitue un délit passible d'une peine d'emprisonnement de cinq ans et de 300 000 euros d'amende.
- **Contrefaçon et usage frauduleux de moyen de paiement : (articles L163-3 et L163-4 du code monétaire et financier)** : délit passible d'une peine d'emprisonnement de sept ans et de 750 000 euros d'amende.
- **Accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal)** : le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de trois ans d'emprisonnement et de 100 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine encourue est de cinq ans d'emprisonnement et de 150 000 euros.
- **Atteinte au secret des correspondances (article 226-15 du code pénal)** : infraction passible d'une peine d'emprisonnement d'un an et de 45 000 euros d'amende.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :

www.cybermalveillance.gouv.fr

