FUITE OU VIOLATION DE DONNÉES PERSONNELLES

CENTRE CYBER DU PACIFIQUE

EN BREF

QU'EST-CE QUE C'EST ?

Une fuite de données personnelles est l'accès ou la divulgation non autorisés d'informations permettant d'identifier une personne (nom, adresse, numéro de téléphone, données bancaires, etc.), détenues par un site, une entreprise, une administration ou toute autre organisation. Elle peut être d'origine accidentelle ou malveillante et, si ces informations sont récupérées par des cybercriminels, elles peuvent être utilisées pour commettre diverses fraudes comme l'hameçonnage, l'escroquerie, l'usurpation d'identité ou le piratage de comptes 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.

Voici 8 bonnes pratiques à adopter si vous êtes victime

1. CONTACTEZ AU BESOIN LE SERVICE OU ORGANISME CONCERNÉ
2. CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE
3. PRÉVENEZ IMMÉDIATEMENT VOTRE BANQUE
4. SIGNALEZ ET DEMANDEZ LA SUPPRESSION DES CONTENUS DIFFUSANT VOS DONNÉES
5. LE DÉRÉFÉRENCEMENT
6. ADRESSEZ UNE RÉCLAMATION À LA CNIL
7. DÉPOSEZ PLAINTE AVEC PREUVES EN CAS D'UTILISATION FRAUDULEUSE
8. ENGAGEZ AU BESOIN UNE ACTION DE GROUPE OU UN RECOURS COLLECTIF

▶ Voir détail page "8 BONNES PRATIQUES À ADOPTER"

FUITE OU VIOLATION DE DONNÉES PERSONNELLES

CENTRE CYBER DU PACIFIQUE

8 BONNES PRATIQUES À ADOPTER

1. CONTACTEZ AU BESOIN LE SERVICE OU ORGANISME CONCERNÉ

Si vous êtes informé d'une possible violation de vos données personnelles, contactez au besoin le service ou organisme concerné pour la confirmer et savoir quelles informations ont pu être compromises.

2. CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE

Changez au plus vite votre mot de passe sur les sites ou services concernés par la fuite de données ainsi que sur tous les autres sites ou comptes sur lesquels vous pouviez l'utiliser.

3. PRÉVENEZ IMMÉDIATEMENT VOTRE BANQUE

Si vos coordonnées bancaires figurent dans la fuite de données, prévenez immédiatement votre banque et faites au besoin opposition aux moyens de paiement concernés. Contrôlez régulièrement vos comptes pour détecter toute opération anormale.

4. SIGNALEZ ET DEMANDEZ LA SUPPRESSION DES PAGES, COMPTES, MESSAGES DIVULGUANT VOS INFORMATIONS PERSONNELLES

Signalez et demandez la suppression des pages, comptes, messages divulguant vos informations personnelles auprès des plateformes sur lesquelles elles sont diffusées.

5. DÉFÉRENCEMENT

Demandez à ce que vos données personnelles divulguées ne soient plus référencées par les moteurs de recherche lorsqu'elles y apparaissent.

6. VOUS POUVEZ ADRESSER UNE RÉCLAMATION (PLAINTE) À LA CNIL

Si, un mois après votre demande de suppression, vos données personnelles sont toujours accessibles, vous pouvez adresser une réclamation (plainte) à la CNIL.

7. DÉPOSEZ PLAINTE

En cas d'utilisation frauduleuse de vos données personnelles, conservez toutes les preuves et déposez plainte 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.

8. ENGAGEZ AU BESOIN UNE ACTION DE GROUPE OU UN RECOURS COLLECTIF

Engagez au besoin une action de groupe ou un recours collectif qui permet aux victimes de demander la cessation de la violation de données personnelles et la réparation du préjudice.

FUITE OU VIOLATION DE DONNÉES PERSONNELLES

CENTRE CYBER DU PACIFIQUE

COMMENT S'EN PROTÉGER ?

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.

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.