# Réagir à une violation de données...

Ces étapes vous aideront à entreprendre des changements positifs afin de vous protéger vous-même.

### 1. Changez vos mots de passe

Commencez par le service concerné et ce que vous utilisez le plus : services bancaires, e-mail, achats en ligne, réseaux sociaux.

### 2. Activez la 2FA (« authentification à double facteur »)

Ce système rend le piratage de votre compte plus difficile, car il requiert deux codes ou « facteurs » pour déverrouiller votre compte. Même si une personne connaît votre mot de passe, elle ne possède pas le deuxième "facteur", généralement un code envoyé sur votre téléphone. Le site web Authy[1] cherche pour vous les plateformes équipées de la 2FA et vous assiste dans la configuration.

### 3. Bloquez les accès à vos comptes bancaires, si nécessaire

Informez votre banque et bloquez votre cote de crédit, si nécessaire. Selon le type de violation, il est peut-être souhaitable de contacter votre banque et votre bureau de crédit (ou l'organisation chargée des cotes de crédit dans votre pays).[2]

Cette démarche empêche qu'une autre personne demande de nouvelles cartes de crédit en votre nom et limite le problème. Les groupes locaux de défense du consommateur peuvent également s'avérer d'une grande aide. Votre banque vous communiquera si vous devez demander de nouveaux numéros de compte et de nouvelles cartes bancaires.

### 4. Expliquez les faits à votre cercle de personnes de confiance

Parlez-en à vos amis et vos parents proches. Ils seront plus attentifs aux appels téléphoniques ou aux e-mails d'éventuels escrocs.

Maintenant, vous pouvez chercher comment limiter les dégâts de la violation à proprement parler.

### 5. Renseignez-vous en ligne

Il est utile de savoir quelles informations circulent en ligne à votre sujet. Quelles informations trouvez-vous lors d'une simple recherche ? Commencez par votre moteur de recherche classique et utilisez des termes de recherche qui ne sont pas trop révélateurs, par exemple, votre nom et les quatre derniers chiffres de votre numéro de téléphone, mais pas votre numéro complet. La recherche Firefox Monitor vous permet de savoir si vos informations ont été violées, vous pouvez également vous inscrire pour être tenu informé des dernières actualités en matière de violation des données.

### 6. Demandez directement aux sites web de supprimer vos données

Règlement Général de Protection des Données (RGPD). Nombreux sont les sites web désireux de se conformer aux nouvelles lois relatives à la protection des données visées par le RGPD. Si vous leur demandez de supprimer des informations, ils ne manqueront pas de réagir rapidement afin d'éviter tout tracas ou frais. Généralement, s'il s'agit d'un produit ou d'un service proposé au sein de l'UE, le traitement des données doit respecter le RGPD, que vous vous trouviez physiquement dans l'UE ou non et idem pour la société.

Vous pouvez également utiliser des services de suppression des données. Les sites tels que Reputation Defender, Privacy Duck et « Delete Me » d'Abine contacteront les sites web concernés pour supprimer vos informations. Ces services sont payants, mais ils peuvent aussi vous informer sur la marche à suivre pour supprimer vous-même les données.

# À faire quand vous voulez...

### 1. Vérifiez les données accessibles en ligne à votre sujet

(commencez par vos comptes importants, par exemple, votre e-mail, vos données bancaires, vos comptes d'achat en ligne et de chat)

Demandez-vous :

1. Quels sont les comptes qui contiennent des données à mon sujet ? Quels seraient les problèmes si ces données étaient violées ?
2. Pourquoi sont-elles visibles à cet endroit ? (Est-ce nécessaire ?)
3. Quel est le niveau de sécurité du site ? Consultez la politique de confidentialité ou les conditions de service du site et recherchez des termes comme « chiffrement au repos » ou « chiffrement en transit », ce qui signifie que vos données sont sécurisées.
4. Quelles sont la politique d'accès et la durée de conservation appliquées par le site ? Les conditions de service mentionnent-elles si l'ensemble du personnel peut accéder à vos informations ? Quelle est sa politique de conservation des données ? Lorsqu'un site web ne stipule pas combien de temps vos données sont conservées, elles les ont probablement pour toujours.

### 2. Désencombrez et faites le tri régulièrement

Aucun risque de fuite ou de violation existe si les services ne disposent pas de vos données. Lorsqu'ils disposent seulement des informations des trois derniers mois, le risque de violation est limité. Veillez à désencombrer régulièrement vos données en ligne. Demandez-vous s'il est vraiment nécessaire de les conserver, supprimez ce dont vous n'avez pas besoin et téléchargez tout ce dont vous avez besoin, afin de pouvoir supprimer les données du site web ou de l'application.

### 3. Vérifiez à nouveau

Puis-je mieux me protéger avec des meilleurs mots de passe et la double authentification ?

### 4. Dites aux entreprises de mieux prendre soin de vos données

Certains disent qu'il y aura toujours des violations, de même qu'il y aura toujours des crimes. Mais les entreprises peuvent faire plus pour protéger vos données. En les contactant, vous pouvez attirer leur attention sur le fait qu'elles se doivent d'écouter et d'agir. Par exemple, envoyez un message comme « nous aimerions savoir combien de temps vous conservez nos données, elles ne devraient pas être conservées pour toujours ».

[1] Ou https://twofactorauth.org

[2] Pour le Luxembourg: Appelez au plus vite SIX Payment Services (accessible 24 heures sur 24, 7 jours sur 7) via le numéro de téléphone (+352) 49 10 10 et informez votre banque.

Traduction :

BEE SECURE HELPLINE Tel: 8002 1234

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG

Co-financed by the European Union Connecting Europe Facility

Concept et contenu :

TACTICAL TECH

DATA DETOX #datadetox datadetoxkit.org