Comment lancer une récupération après une exposition de mot de passe

Votre mot de passe peut être exposé de plusieurs façons à des parties non autorisées :

1. Les mots de passe sont parfois « mémorisés » sans filet de sécurité par souci de commodité dans des documents électroniques ou papier. Votre mot de passe sera exposé en cas de perte ou de vol du document.
2. Les attaques par hameçonnage tentent de vous convaincre de saisir votre mot de passe sciemment sur un site Web qui le collecte aux fins de revente ou d'utilisation. Si vous ne détectez pas l'attaque, votre mot de passe sera exposé.
3. Vous, votre employeur ou toute organisation avec laquelle vous échangez par voie numérique pouvez faire l'objet d'une violation de données.
4. Les technologies liées aux mots de passe comme les navigateurs mémorisant les mots de passe, les extensions de navigateurs, les outils de gestion de mots de passe, ou le trousseau d'accès (Keychain) d'Apple peuvent faire l'objet d'une violation de données.

Vous serez informé des violations de données susceptibles de vous affecter via les médias de presse traditionnelle et numérique ou directement par le biais de l'organisation victime d'intrusion si elle est tenue de vous en faire part. Vous pouvez également acheter divers services de surveillance du dark web pour recevoir des notifications. Certains outils et services gratuits permettent de vérifier par vous-même ou de vous notifier de manière proactive que vous avez été affecté, à savoir :

- ';--have i been pwned? (ai-je été compromis) vous permet de rechercher des informations sur plusieurs violations de données afin de déterminer si votre adresse électronique a été compromise.
- Apple peut envoyer des notifications aux utilisateurs d'iPhone (voir la fonctionnalité Détection de mots de passe compromis) et du navigateur Safari.
- Google peut envoyer des notifications aux utilisateurs de Chrome et fournir un outil de Contrôle de mots de passe en tant que ressource de suivi.

Ce blog est axé sur les violations de données susceptibles de se produire en cas d'incident de sécurité survenu sur un outil de gestion de mots de passe, qui expose les données de mots de passe d'un utilisateur.

En août 2022, LastPass, un outil populaire pour la gestion de mots de passe, a été victime d'une violation de données. Bien que la société assure aux utilisateurs que les coffres-forts de mots de passe chiffrés restent sécurisés, certains codes sources et informations techniques ont été volés. Cet incident qui a concerné bon nombre d'utilisateurs, a conduit ces derniers à remettre en doute la sécurité de la plateforme.

Si vous utilisez tout outil de gestion de mots de passe et envisagez de changer de fournisseur, voici ce qu'il faut savoir :

Comprendre les intrusions et violations de données

LastPass reconnaît que les informations subtilisées lors du premier incident ont permis aux attaquants d'accéder à des volumes de stockage réputés suffisamment protégés, amplifiant ainsi les risques de compromission de tous les mots de passe connexes. Bien qu'ils aient cherché à rassurer leurs clients en soutenant qu'aucune donnée client n'avait été directement consultée, cette violation de données met en exergue l'importance d'une protection des mots de passe selon les plus hauts niveaux de sécurisation possibles.

Vous voudrez comprendre la nature de toute violation de vos conditions. N'hésitez pas à contacter votre fournisseur actuel via son canal de support client pour obtenir tout éclaircissement quant à vos éventuelles questions.

Que dois-je donc faire par la suite ?

1. **Évaluer vos besoins et votre tolérance aux risques :** rechercher d'autres gestionnaires de mots de passe. Parmi les options populaires, on relève entre autres 1Password, Bitwarden et Dashlane. Tenez compte de fonctionnalités telles que la prise en charge de plusieurs appareils, les mesures de sécurité, la prise en charge de l'authentification à deux facteurs ou multifacteurs, les procédures de récupération de compte et la facilité d'utilisation. Et surtout, évaluez votre tolérance aux risques pour divers types de comptes.

   À noter qu'il ne s'agit-là que d'exemples; vous devriez évaluer vos risques en fonction de vos besoins et de votre tolérance aux risques :

   - **Risque faible :** comptes de réseaux sociaux et site de e-commerce que vous utilisez rarement et sur lesquels vous ne conservez pas de coordonnées de paiement.
   - **Risque modéré :** adresses e-mail autonomes non utilisées pour authentification/connexion ponctuelle ou gestion de services à risques accrus.
   - **Risque élevé :** comptes bancaires, applications financières, portails de santé, stockage cloud et autres comptes sur lesquels vous communiquez des renseignements relatifs à votre situation financière.
   - **Risque extrême :** comptes utilisés pour prendre en charge des services d'authentification/connexion ponctuelle populaires tels que votre identifiant Apple, Microsoft ID ou compte Google.

2. **Priorisez en fonction du risque :** en fonction de votre évaluation des risques, donnez la priorité aux mesures relatives à vos comptes les plus critiques.

Approches de sécurité basées sur le risque

- **Essentielle (que vous passiez à un nouvel outil ou pas) :**
  - Utilisez un mot de passe fort pour votre outil de gestion de mots de passe et changez-le régulièrement.
  - Activez la méthode d'authentification multifactorielle la plus forte disponible pour l'outil en question :
    - Parmi les méthodes les plus faibles, on relève les vérifications par e-mail, SMS ou appel téléphonique.
    - Parmi les méthodes les plus fortes, on relève les applications ou dispositifs d'authentification biométrique ou à mot de passe ponctuel, comme Google Authenticator ou Microsoft Authenticator.
    - Parmi les méthodes les plus fortes disponibles, on relève les clés passe et les certificats.
  - Si prises en charge, veillez à avoir le contrôle sur les clés de chiffrement.
  - Effacer tous les cookies et mots de passe de votre navigateur.
- **Bien :**
  - S'il vous faut opérer une migration vers un nouvel outil, suivez les instructions communiquées.
  - Utilisez l'outil prévu pour modifier les mots de passe de vos comptes.
  - S'il y a lieu, détruisez tous les fichiers utilisés pour exporter les anciens mots de passe de votre outil de gestion des anciens mots de passe.
- **Mieux :**
  - Cette approche ajoute une couche de sécurité supplémentaire.
  - S'il vous faut opérer une migration vers un nouvel outil, suivez les instructions communiquées.
  - Envisagez de changer l'identifiant utilisateur ou l'adresse e-mail connexe après avoir utilisé l'outil prévu pour définir des mots de passe forts pour tous les comptes à risque ÉLEVÉ ou EXTRÊME.
  - S'il y a lieu, détruire tous les fichiers utilisés pour exporter les anciens mots de passe de votre outil de gestion des anciens mots de passe.
  - Envisagez de créer plusieurs profils de navigateur sans plugins ni extensions (à l'exception de ceux requis par votre gestionnaire de mots de passe) pour servir de conteneurs aux fins d'utilisation directe de vos comptes à risque EXTRÊME.
- **Le mieux :**
  - Cette approche sera plus sécurisée, mais sera chronophage.
  - S'il vous faut opérer une migration vers un nouvel outil, suivez les instructions communiquées.
  - À ce stade, vous devrez changer le mot de passe de tous vos comptes (quels que soient les risques) en utilisant le nouvel outil et modifier l'identifiant utilisateur et l'adresse e-mail connexes pour CHACUN de vos comptes à risque ÉLEVÉ et EXTRÊME afin qu'ils soient uniques.

- Cette approche permet de créer des identifiants de connexion distincts pour vos comptes les plus critiques, réduisant ainsi l'impact de toute violation de données sur ces comptes.
- L'inconvénient de cette approche est que vous ne pourrez peut-être pas utiliser les services de connexion ponctuelle couramment disponibles pour vos comptes les plus à risque.
- S'il y a lieu, détruisez tous les fichiers utilisés pour exporter les anciens mots de passe de votre outil de gestion des anciens mots de passe.
- Envisagez de créer plusieurs profils de navigateur sans plugins ni extensions (à l'exception de ceux requis par votre gestionnaire de mots de passe) pour servir de conteneurs aux fins d'utilisation directe de vos comptes à risques ÉLEVÉS et EXTRÊMES.

Rappel :

- Faites attention aux tentatives de hameçonnage.
- Ne stockez jamais vos mots de passe de façon claire, que ce soit sous format électronique ou papier.
- Choisissez des mots de passe forts et uniques pour tous vos comptes. Un gestionnaire de mots de passe peut faciliter la génération et la conservation de ces mots de passe en toute sécurité.
- Activez la méthode d'authentification multifactorielle la plus forte disponible pour vous n'importe où.
- Et n'oubliez pas les autres données sensibles que vous pourriez avoir conservées dans un gestionnaire de mots de passe, telles que des informations financières, des informations de récupération de compte, voire des informations de portefeuille de cryptomonnaies. Bien que cela ne soit pas abordé directement dans cet article de blog, vous devez procéder à une analyse des risques pour déterminer les mesures de récupération à entreprendre. Les mesures à envisager doivent inclure le changement de comptes financiers ou de numéros de cartes de crédit/débit, ou la migration vers un nouveau portefeuille de cryptomonnaie.

Les violations de données évoquées soulignent l'importance du principe de vigilance en matière de cybersécurité. En évaluant vos besoins et votre tolérance aux risques et en y répondant, vous pourrez faire en sorte de protéger vos comptes en ligne contre les criminels les plus compétents et déterminés.