Devolutions

Comment vérifier si vos données ont été compromises par la fuite massive de Facebook

LA DEVISE DE FACEBOOK EST « BOUGER VITE ET TOUT CASSER »

La devise de Facebook est « bouger vite et tout casser ». Bien que la « confiance des utilisateurs » ne figure probablement pas sur la liste des choses que l'entreprise veut casser, ç'a peut-être été le cas à la suite d'un important vol de données chez le géant des médias sociaux.

À propos du vol de données

Le 3 avril dernier, le chercheur en sécurité Alon Gal a révélé que les données personnelles de 533 millions d'utilisateurs de Facebook avaient été divulguées sur le dark Web. Les données exposées comprennent :

- Numéro de téléphone
- Identifiants Facebook
- Nom et prénom
- Localisation actuelle
- Endroits fréquentés dans le passé
- Date de naissance
- Date de création du compte
- Statut de la relation
- Biographie

Dans certains cas, des adresses courriel ont également été volées. On s'attend à ce que les pirates utilisent ces informations pour mener des attaques d'ingénierie sociale et autres activités illicites. Comme le rapporte theconversation.com, la faille serait liée à une vulnérabilité que Facebook prétend avoir corrigée en août 2019. Bien que la source précise des données ne puisse pas être confirmée, certains experts en cybersécurité pensent qu'elle a été acquise grâce à l'utilisation abusive de fonctions légitimes dans les systèmes Facebook.

L'impact

Si tous les vols de données sont inquiétants, ce qui rend celui-ci particulièrement alarmant, c'est qu'il comprend des numéros de téléphone. Voici ce que le créateur de Have I Been Pwned?, Troy Hunt, avait à dire sur le sujet :

« Quand tu connais le nom et le pays de quelqu'un, c'est facile de trouver le numéro de téléphone lors d'une attaque ciblée. C'est beaucoup plus difficile à faire pour une attaque de masse. Je ne pourrais pas prendre une grande liste de courriels et trouver des numéros de téléphone, parce que les courriels sont rares dans les données. Sauf que pour les pourriels basés uniquement sur l'utilisation de numéros de téléphone, c'est de l'or. Et pas seulement les SMS! Il existe des tas de services qui nécessitent juste un numéro de téléphone aujourd'hui. Ils sont classés par pays avec la possibilité de catégoriser par nom et par sexe. »

Quoi faire

Si vous êtes l'un des 2,6 milliards d'utilisateurs de Facebook – et il y a de très bonnes chances que vous en soyez un – la première chose à faire est de voir si vous avez été victime de cette attaque. Plusieurs sites peuvent vous aider, dont :

- Have I Been Pwned? Vous pouvez également voir si vous avez été victime d'autres vols de données connus.
- The News Each Day. Pour protéger la confidentialité, ce site génère des numéros de téléphone aléatoires qui commencent par les mêmes 5 chiffres que votre numéro, puis envoie 99 faux et 1 vrai numéro au serveur. Ça fait en sorte que le serveur ne sait pas quel numéro est réel – et les pirates non plus.

Conseils supplémentaires

J'espère que vous ne faites pas partie des utilisateurs touchés par ce vol de données. Quoi qu'il en soit, nous supplions tous les utilisateurs d'adopter les meilleures pratiques de gestion des mots de passe :

- Utilisez l'authentification à deux facteurs (A2F) sur tous vos comptes. Il existe plusieurs bons outils d'A2F, y compris le nôtre (qui est gratuit) : Devolutions Authenticator.
- Utilisez un gestionnaire de mots de passe robuste. Encore une fois, il existe plusieurs bons gestionnaires de mots de passe, y compris le nôtre (et oui, il est aussi gratuit) : Password Hub Personal.
- N'utilisez jamais le même mot de passe plus d'une fois et ne réutilisez jamais un ancien mot de passe.
- Avant de choisir un mot de passe, vérifiez s'il a été compromis dans le passé. Vous pouvez le faire en allant sur le site Have I Been Pwned? Comme vous le savez peut-être, la fonction de vérification des mots de passe de Remote Desktop Manager est intégrée à la base de données Have I Been Pwned?. Pour une présentation vidéo et pour savoir comment configurer la vérification du mot de passe Pwned, cliquez ici.
- Faites très attention à ce que vous partagez sur les médias sociaux! Même des activités apparemment inoffensives, comme la publication d'une photo d'une carte d'embarquement d'une compagnie aérienne, peuvent mener à un vol d'identité. Et ça, c'est un cauchemar!

Nous tenons ce vol de données de Facebook à l'œil et publierons des mises à jour dès qu'elles seront disponibles. Jusque-là, soyez prudent et restez en sécurité!