Piratage de Facebook trois bons réflexes pour sécuriser son compte

Face aux failles en série du géant du Web, plusieurs réflexes s'imposent pour limiter la fuite de ses données personnelles.

Des pirates informatiques ont attaqué Facebook. Leur butin? Près de 50 millions de comptes, dont les accès ont été dérobés et dont les données personnelles pourraient avoir été récupérées. Face à cette faille d'une ampleur inédite pour le réseau social américain, les utilisateurs disposent de plusieurs outils pour tenter de protéger leur vie privée. Voici trois solutions à mettre en œuvre.

1. Adopter l'authentification à deux facteurs

Pour sécuriser leurs services, tous les grands sites Web mettent à disposition une fonction de double authentification (accessible à cette adresse). Elle consiste à demander à l'utilisateur un second élément, en plus de son mot de passe. Dans la plupart des cas, il s'agit d'un code reçu par SMS sur son smartphone - Facebook part du principe que seul l'utilisateur est susceptible d'avoir accès à son smartphone.

L'opération implique de préciser son numéro de téléphone à Facebook, qui l'utilise également à des fins publicitaires. Le réseau social propose une autre solution: faire appel à une application tierce (comme Duo ou Google Authenticator) pour envoyer ce second code. Notons que le piratage tout juste révélé par Facebook ne semble pas avoir mis en danger les mots de passe des utilisateurs.

2. Vérifier la liste des appareils connectés

Smartphones, tablettes, ordinateurs, objets connectés: nos moyens d'accéder à Facebook se multiplient. Avec le temps, nous avons donc de plus en plus d'appareils connectés à notre compte. Il est important de vérifier régulièrement la liste des machines qui y ont accès - accessible dans la catégorie "Sécurité" des paramètres de Facebook - afin de vérifier qu'un appareil suspect ne soit pas dans la liste.

Au besoin, il est possible de déconnecter automatiquement l'ensemble des machines liées à notre compte. Toujours sur la page "Sécurité et connexion", Facebook propose de recevoir des alertes (par mail ou sur Facebook) en cas de connexion depuis un appareil suspect.

3. Limiter la quantité de données personnelles offertes à Facebook

Malgré ces précautions, la faille révélée de 28 septembre prouve qu'aucune précaution n'est infaillible. Ainsi, il est préférable de limiter au maximum les données que l'on partage avec le réseau social. Depuis son profil, il est possible de supprimer toutes les informations qui ne sont pas indispensables (ville de naissance, établissement scolaire fréquenté etc.). Une page est par ailleurs prévue pour gérer ses préférences publicitaires. Elle permet de supprimer l'ensemble de ses centres d'intérêts répertoriés ou encore de mettre un frein au partage de données avec les partenaires extérieurs de Facebook.

Une solution complémentaire consiste à désactiver le service de géolocalisation. Les applications Facebook et Messenger sont très insistantes pour obtenir la liste des contacts de notre répertoire. Un

accès qui lui permet de retrouver le numéro de téléphone de nos amis, sans qu'ils n'aient désiré le fournir. Désactiver cet accès est donc recommandé.

https://www.msn.com/fr-be/actualite/technologie-et-sciences/piratage-de-facebook-trois-bons-r%c3%a9flexes-pour-s%c3%a9curiser-son-compte/ar-BBNHokP?li=BBqj2K4&ocid=mailsignout