

Piratage de ses comptes de réseaux sociaux. Comment réagir ?



Prévenir un piratage

Aucune personne ou ordinateur ne doit être en mesure de le deviner. La CNIL publie des conseils pour créer un mot de passe efficace, le retenir et le stocker dans une base.

Ne communiquez pas votre mot de passe
Il est vivement déconseillé de communiquer votre mot de passe à une tierce personne, de l'enregistrer dans un navigateur si vous n'avez pas défini de mot de passe maître ou dans une application non sécurisée.

Activez un dispositif d'alerte en cas d'intrusion
La double authentification est une option activable sur la plupart des réseaux sociaux. Lorsque vous vous connectez depuis un poste informatique inconnu, le réseau social vous demandera de confirmer l'accès en entrant un code que vous aurez reçu par sms ou par courrier électronique. D'autres fonctions proposent simplement de vous alerter si une personne extérieure tente de se connecter à votre compte depuis un terminal inconnu (PC, smartphone, tablette, mac).

En outre, cette option disponible sur la plupart des réseaux sociaux vous permet d'identifier l'ensemble des terminaux avec lesquels vous vous êtes connectés à votre compte. Lorsque cela est possible, il est conseillé de désactiver le lien avec les terminaux dont vous ne vous servez plus. Une connexion identifiée depuis un navigateur inconnu ou une ville inconnue pourra vous mettre la puce à l'oreille.

Il arrive que les applications tierces connectées à votre compte soient vulnérables à une attaque extérieure. Il est conseillé de désactiver les applications tierces dont vous avez autorisé l'accès par le passé et qui ne vous servent plus.

En devinant votre nom, votre fonction, votre liste d'amis, une personne mal intentionnée pourrait facilement déduire des informations qui servent à réinitialiser votre compte ou simplement à usurper votre identité afin de changer votre mot de passe par exemple.

- votre mot de passe est invalide
- des tweets/posts imprévus sont envoyés depuis votre compte
- des messages privés sont envoyés de façon non volontaires
- des comportements inhabituels ont lieu sur votre compte sans consentement (comme suivre, se désabonner, ou bloquer)
- une notification de la part du réseau social vous informe que « Vous avez récemment changé l'adresse électronique associée à votre compte.

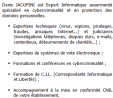
1. Signalez le compte piraté auprès du réseau social
2. Demandez une réinitialisation de votre mot de passe
3. Une fois votre compte sécurisé, n'oubliez pas de parcourir les rubriques « sécurité » proposées par ces réseaux sociaux

Donneur d'avis : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sélectifs, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sélectifs, actions de formations en cybersécurité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du Travail de l'Emploi et de la Formation Professionnelle n°93 BA 00941 84)

Denis JACQUIN réalise des audits et anime dans toute la France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la cybersécurité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés.

Vous pouvez nous contacter à l'adresse suivante : contact@protectiondesdonneespersonnelles.fr

Plus d'informations sur le <https://www.insee.fr/fr/themes/actualites/information-protection-des-donnees-personnelles>



Réagir à cet article

Original de l'article mis en page : Prévenir, repérer et réagir face au piratage de ses comptes sociaux | CNIL