

Piratage de ses comptes sociaux : prévenir, repérer et réagir ! | Le Net Expert Informatique

 Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité  vous informe...	Piratage de ses comptes sociaux : prévenir, repérer et réagir !
--	---

Vos comptes sociaux abritent une somme considérable de données personnelles. Veillez à bien les sécuriser pour éviter les piratages d'individus malveillants.

I- Prévenir un piratage

Choisissez des mots de passe complexes, différents et non-signifiants !

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 mail. 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).

Déconnectez à distance les terminaux encore liés à votre compte

Là encore, 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.

Désactivez les applications tierces connectées à votre compte

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 autorisés l'accès par le passé et qui ne vous servent plus.

Réglez vos paramètres de confidentialité

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.

II- Repérer un piratage

- 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 email associée à votre compte.

III- Réagir en cas de piratage

1. Signalez le compte piraté auprès du réseau social
2. Demandez une réinitialisation de votre mot de passe.

Si un site/réseau social n'apporte pas de réponse satisfaisante, contactez la CNIL

3. Une fois votre compte sécurisé, n'oubliez pas de parcourir les rubriques « sécurité » proposées par ces réseaux sociaux

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source :
<http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/piratage-de-ses-comptes-sociaux-prevenir-reperer-et-reagir/>