Facebook

Que faire en cas d'usurpation d'identité

Jean Marie Herbaux

Table des matières

Vous venez de vous apercevoir que quelqu'un se faisait passer pour vous sur Facebook à l'aide d'un faux profil ? Voici comment réagir pour supprimer ce compte frauduleux et, surtout, pour éviter que cela ne se reproduise.

Les motivations des pirates

Les motivations des pirates sont vastes.

- Il peut s'agir d'une vengeance ou de la volonté de nuire. *Dans ce cas, il s'agit d'une personne qui vous connaît.*
- Il peut aussi s'agir d'opération d'envoi de spams, du plaisir de pirater des comptes, de tentative d'extorsion d'argent.
- Dans tous les cas, Facebook est tellement présent dans nos vies que le piratage ou la duplication de notre compte est un phénomène très désagréable qui nous touche personnellement.

Les usurpations d'identité, les violations du droit à l'image et les créations de faux comptes ne sont pas rares sur Facebook.

S'il est de plus en plus difficile de pirater un compte Facebook, il est en revanche extrêmement facile de *créer un faux compte*. Il suffit de recopier quelques photos d'un profil Facebook puis de créer un compte avec le nom et prénom du propriétaire des photos. Il ne reste plus qu'à ajouter quelques informations réelles comme la date de naissance, la ville d'origine, le métier et tour est joué. Évidemment, le faussaire ne s'arrêtera pas là. Il enverra des demandes d'amitié à vos vrais amis qui vont pour la plupart accepter en pensant que c'est vous. Après ces opérations simples, la personne malveillante dispose d'un faux compte en bon état de marche avec lequel elle peut très facilement se faire passer pour vous sur Facebook.

Même si elle très facile à mettre en œuvre, l'usurpation d'identité sur Facebook n'est pas une fatalité.

Vous pouvez, et même vous devez, réagir dès que vous en apercevez. Nous vous expliquons comment procéder et comment prévenir Facebook pour que le faux compte soit supprimé. Une fois le problème réglé, nous vous conseillons de protéger au mieux votre compte et de continuer à utiliser Facebook afin d'occuper le terrain. Vous pourrez ainsi rapidement repérer les éventuelles actions malveillantes.

Une usurpation d'identité sur Facebook peut provenir soit du piratage de votre compte, soit de la création d'un faux compte. Le premier cas est beaucoup plus rare que le second.

Le piratage de votre compte

Historiquement le piratage de compte est la première méthode d'usurpation d'identité sur Facebook. Il y a encore quelques années, il suffisait de connaître ou de deviner l'identifiant et le mot de passe d'un compte Facebook pour se connecter. Comme de nombreuses personnes utilisaient le même mot de passe pour leurs différents comptes, il était assez facile de pirater le compte d'un ami ou d'une connaissance. Aujourd'hui, c'est beaucoup plus difficile car les utilisateurs commencent à être sensibilisés aux problématiques de sécurité de leurs comptes de réseaux sociaux. Ils utilisent le plus souvent plusieurs mots de passe et leurs mots de passe sont plus robustes qu'auparavant. De plus, Facebook a beaucoup travaillé sur la sécurité.

Désormais, par défaut vous recevez une notification dès que quelqu'un se connecte à votre compte Facebook à partir d'un appareil inhabituel.

De plus si vous avez opté pour l'identification à deux facteurs, vous devez saisir un code reçu sur votre téléphone en plus de votre mot de passe lorsque vous vous connectez à partir d'un appareil Inconnu.

La création d'un faux compte

La grande majorité des cas d'usurpation d'identité sur Facebook s'effectue en créant des faux comptes qui sont la copie de comptes existants. Il est en effet très facile de créer un faux compte. Il suffit à la personne malveillante de se rendre sur le compte Facebook qu'elle souhaite usurper. Ensuite, elle copie quelques photos et quelques informations comme le nom, la date de naissance, la ville. Elle crée alors un nouveau compte avec les informations volées. Il est difficile pour Facebook de lutter contre la création de faux comptes. En effet, ce n'est pas parce qu'un compte est créé avec un nom et un prénom identiques à un autre, déjà existant, qu'il est faux puisqu'il existe des quantités d'homonymes de par le monde. Si, en plus, le faussaire vole des photos sur d'autres comptes de réseaux sociaux que Facebook, les procédures de sécurité du réseau ne détecteront pas le faux compte.

Comment détecter une usurpation d'identité ?

Facebook est en train de mettre en place une fonctionnalité qui vous préviendra lorsqu'un compte comportant votre nom et votre prénom sera créé. Vous disposerez alors d'un lien pointant vers le compte suspect afin de l'examiner et d'un lien pour indiquer à Facebook que le compte est une usurpation d'identité. Rappelons qu'il peut tout fait légalement exister des comptes Facebook comportant les mêmes patronymes que les vôtres. En attendant que la fonctionnalité de détection automatique de faux comptes soit mise en place par Facebook, il n'est pas forcément facile de se rendre compte que quelqu'un a usurpé votre identité.

En fait, vous disposez essentiellement de deux possibilités :

- Rechercher régulièrement vos nom et prénom sur Facebook. Toutefois, si le pirate est malin. il vous aura bloqué sur Facebook ce qui fait que vous ne verrez pas le compte frauduleux.
- Être averti par un de vos amis qui s'étonne de voir que vous avez un nouveau compte.

Que faire rapidement ?

Faites des copies d'écran

Dès que vous avez connaissance d'une usurpation d'identité sur Facebook, faites des copies d'écran du compte frauduleux car vous aurez peut-être besoin de ces copies d'écran pour signaler le profil frauduleux à Facebook. Il est effectivement conseillé de réaliser quelques copies d'écran du faux profil tant que vous en avez la possibilité. Le pirate peut vous bloquer à tout moment afin que vous n'ayez plus accès à son faux compte. Si cela vous arrive, demandez à un de vos amis de prendre quelques copies d'écran pour vous.

NB : Vous devez savoir que les copies d'écran réalisées par vous-même ou par vos amis ne sont pas considérées comme des preuves permettant d'établir la réalité d'une publication sur Internet. Si vous avez besoin d'une preuve irréfutable, vous pouvez obtenir des copies d'écran certifiées auprès d'un huissier de justice. Cela vous coûtera 150€.

Prévenez vos amis

Lorsque vous êtes informé qu'un faux compte Facebook usurpe votre identité, vous devez informer vos amis très rapidement. Il faut que vos amis soient au courant le plus tôt possible afin qu'ils ne tombent pas dans le panneau en acceptant les demandes d'amitié du pirate.

Informez vos amis et demandez-leur de faire des copies d'écran du faux compte puis de signaler ce faux compte à Facebook. Plus vous serez nombreux à signaler un faux compte à Facebook, plus vite Facebook supprimera ce faux compte.

Montez votre dossier

Avant de signaler à Facebook le faux compte usurpant votre identité vous devez constituer votre dossier. La procédure de signalement sera plus facile à réaliser de cette manière :

- Commencez par rassembler les copies d'écran du faux compte.
- Ajoutez des copies d'écran de votre véritable compte.
- Nommez clairement les copies d'écran de manière à ce que Facebook reconnaisse facilement les captures du faux compte et celles de votre vrai compte.
- Notez l'adresse Facebook du faux compte et celle de votre vrai compte.
- Préparez également une copie recto verso de votre carte d'identité.

Les pirates les plus efficaces recopient des photos de la personne sur d'autres sites de réseaux sociaux que Facebook comme Instagram par exemple. Ils utilisent ces photos pour illustrer le faux compte Facebook en s'assurant que ces photos ne sont pas présentes sur le vrai compte Facebook. C'est assez efficace car Facebook compare les photos du faux compte avec celles du vrai compte. S'il ne trouve pas de correspondance, Facebook aura tendance à considérer que le faux compte est légitime. Pour éviter cela, si le pirate utilise des photos de vous provenant d'autres comptes de réseaux sociaux, réalisez des captures d'écran de vos comptes de réseaux sociaux utilisés par la personne malveillante.

Signalez le faux compte

Si un compte se fait passer pour vous ou pour quelqu'un que vous connaissez, vous pouvez découvrir comment le signaler pour usurpation d'identité.

Cette procédure fonctionne lorsque vous avez accès au faux compte.

Facebook a mis en place une procédure simple pour signaler les comptes qui usurpent l'identité d'une personne. Pour mettre en œuvre cette procédure, vous devez :

- Accéder au profil usurpant votre identité. Si vous ne trouvez pas ou plus ce profil, demandez l'adresse à vos amis.
- Cliquer sur le bouton représentant trois petits points alignés affiché sous la bannière d'en-tête.
- Sélectionner Signaler.
- Suivre les instructions qui s'affichent.

Si vous n'y avez pas accès

Vous ne pouvez pas signaler ce faux compte de cette façon.
Dans ce cas, nous vous conseillons de vous déconnecter de Facebook puis d'ouvrir le formulaire Facebook permettait de signaler une usurpation d'identité,
https://www.facebook.com/help/contact/295309487309948
Choisissez l'option Quelqu'un a créé un compte usurpant mon Identité ou celle d'un ami puis suivez les instructions. Notez qu'avec cette procédure, vous devez obligatoirement joindre une copie d'une pièce d'identité de la victime. Facebook vous constatera sous 72 heures pour vous indiquer la suite donnée à votre requête. Si tout se passe bien. Facebook désactive et supprime le faux compte.

Que faire en cas de refus de Facebook ?

La procédure de signalement des comptes frauduleux fonctionne correctement et généralement les faux comptes sont supprimés au bout de deux ou trois jours. Il arrive quelquefois que Facebook refuse de supprimer le faux compte car le réseau social estime que le compte est conforme, qu'il n'enfreint aucune règle et qu'il n'usurpe pas votre identité. Si vous êtes dans ce cas, rien n'est perdu.

Vous disposez encore de deux voies de recours :

- contacter l'assistance Facebook,
- déposer plainte contre X.

CONTACTEZ l'ASSISTANCE FACEBOOK

Lorsque vous signalez un compte frauduleux à Facebook, vous recevez un rapport vous indiquant la suite que le réseau social donnera à votre demande. Ce rapport comporte un lien permettant de contacter l'assistance Facebook pour laisser un commentaire. Lorsque Facebook refuse de supprimer le faux compte, cliquez sur ce lien et laissez un commentaire précisant que votre signalement porte sur une usurpation d'identité. Ajoutez quelques Précisions comme les dates de publication qui devraient être systématiquement plus récentes sur le faux compte. Précisez également que vous pouvez leur une copie de votre carte d'identité et que vous avez l'intention de déposer une plainte.

DÉPOSEZ PLAINTE CONTRE X

Lorsque votre contact avec l'assistance Facebook ne donne aucun résultat, vous pouvez déposer une plainte contre X et assigner Facebook en vous appuyant sur l'article 22641 du Code pénal qui stipule :

- Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.
- Vous pouvez déposer votre plainte auprès de n'importe quel commissariat de police ou brigade de gendarmerie.

Vous avez également la possibilité de déposer plainte directement auprès du Procureur de la République.

Vous pouvez faire ces démarches vous-même mais il est plus simple et plus efficace de vous faire assister par votre assurance assistance juridique ou de prendre un avocat. Vous pouvez également déposer une pré-plainte en ligne via Internet en vous connectant sur le site gouvernemental Pré-plainte en ligne : https://www.pre-plainte-en-ligne.gouv.fr
Ce service est prévu pour vous faire gagner du temps lorsque vous souhaitez déposer une plainte. Vous remplissez un formulaire en ligne dans lequel vous vous identifiez. Vous décrivez les faits et vous indiquez le préjudice matériel. Il ne vous restera plus qu'à aller signer votre plainte dans le commissariat ou la brigade de gendarmerie que vous avez choisie. Attention, votre plainte ne sera valide qu'une fois que vous l'aurez signée.

Continuez à utiliser Facebook

Quels que soient les problèmes d'usurpation d'identité et de comptes frauduleux que vous rencontrez sur Facebook, nous vous conseillons de continuer à utiliser le réseau social. Occupez le terrain. Faites vivre votre compte. Publiez des informations et des photos. C'est la bonne manière pour être rapidement informé des problèmes de sécurité et confidentialité qui pourraient vous concerner. En effet en étant absent de Facebook, vous laissez le champ libre aux personnes malveillantes, vous ne vous rendrez pas compte d'une éventuelle usurpation d'identité et vos amis ne vous préviendront peut être pas.

Comment protéger son compte Facebook

Victime ou non d'une usurpation d'identité, vous devez protéger votre compte Facebook. En effet, un piratage de votre compte est encore pire qu'une usurpation d'identité. Partant du principe qu'il vaut mieux prévenir que guérir, voici quelques conseils à suivre pour sécuriser au mieux votre compte :

- Choisissez soigneusement votre mot de passe. Utilisez un mot de passe unique pour votre compte Facebook. Veillez à ce qu'il comporte des lettres, des chiffres, des symboles, des minuscules et des majuscules et changez-le régulièrement. Bien entendu, votre mot de passe ne doit pas comporter de nom ou mot connu. Comme il est très difficile de se rappeler un mot de passe respectant les règles précédentes, utilisez un

gestionnaire de mots de passe comme Roboform ou inscrivez votre mot de passe sur un papier que vous conserverez dans un endroit séparé de votre ordinateur et mobile.

- Ne communiquez jamais vos informations de connexion. Rappelons que les informations de connexion sont votre identifiant Facebook et votre mot de passe. Aucun site sérieux ne vous les demandera. Ne les communiquez à personne. Il s'agit de données personnelles. SI vous avez le moindre doute sur l'intégrité de vos données de connexion, modifiez votre mot de passe.
- N'oubliez pas de vous déconnecter lorsque vous utilisez Facebook sur un ordinateur partagé. Cela peut arriver au travail, chez des amis, dans un cybercafé. SI vous avez oublié de vous déconnecter ou si avez un doute, vous pouvez vous déconnecter à distance. Pour cela, connectez-vous à Facebook avec votre ordinateur ou votre mobile. Ouvrez les paramètres de sécurité puis la partie *Où vous êtes connecté(e*). Sélectionnez la connexion que vous souhaitez Interrompre puis cliquez sur *Arrêter l'activité*.
- N'acceptez pas les invitations Facebook des personnes que vous ne connaissez pas. Il peut s'agir de comptes malveillants.
- Ne cliquez jamais sur des liens que vous recevez sur Facebook. par mail, par Messenger, par SMS. Il peut s'agir de faux sites qui cherchent à voler vos identifiants de connexion.
- Sécurisez votre compte en activant les alertes de connexion et les contacts de confiance sur Facebook :
    - Pour activer les alertes de connexion, accédez aux *paramètres de sécurité* puis sélectionner *Alertes de connexion*. Vous recevrez une notification dès que Facebook détectera qu'un appareil Inhabituel s'est connecté à votre compte.
    - Pour activer les contacts de confiance. accédez aux *paramètres de sécurité* puis sélectionnez *Contacts de confiance*. Saisissez des contacts de confiance. Les contacts de confiance sont des amis que vous pouvez contacter si vous n'arrivez plus à vous contacter à votre compte Facebook. Dans ce cas, vos amis contacts de confiance pourront vous envoyer un code qui vous permettra de vous connecter. C'est pratique lorsqu'un pirate réussit à se connecter sur votre compte Facebook et modifie le mot de passe.