



USURPATION D'IDENTITÉ



EN BREF

QU'EST-CE QUE C'EST ?

L'usurpation d'identité est un délit (article 226-4-1 du Code pénal). Cela désigne le fait d'utiliser des informations personnelles, permettant d'identifier une personne, sans son accord pour réaliser des actions frauduleuses (ouverture de compte bancaire, création de comptes sur les réseaux sociaux, souscription de crédit, fausses petites annonces, cyberharcèlement...)



En résumé, c'est lorsque quelqu'un utilise votre photographie et/ou votre nom, sans votre consentement, sur Internet et/ou les réseaux sociaux pour effectuer des actions en votre nom.



Agir rapidement est essentiel pour minimiser les dommages potentiels et récupérer le contrôle sur votre identité en ligne.



QUE FAIRE ?

1. Obtenir des preuves
2. Signaler l'abus à la plateforme
3. Contacter les autorités
4. Alerter vos contacts

► Voir détail page "Que faire"



COMMENT S'EN PROTÉGER ?

- En prévention, la protection de vos informations est indispensable

► Voir détail page "comment s'en protéger"





USURPATION D'IDENTITÉ



QUE FAIRE ?

Si vous êtes victime, voici les démarches prioritaires à suivre :

1. Obtenir des preuves :

- **Captures d'écran** : Prenez des captures d'écran de la page ou du profil où votre photo et votre nom sont utilisés. Assurez-vous d'inclure l'URL, la date, et toutes les informations pertinentes.
- **Preuves supplémentaires** : Si possible, sauvegardez la page en question.

2. Signaler l'abus à la plateforme :

- **Réseaux sociaux** : Presque tous les réseaux sociaux (Facebook, Instagram, Twitter, etc.) ont des procédures pour signaler les usurpations d'identité ou l'utilisation non autorisée de photos. Cherchez l'option "Signaler" sur le profil ou la publication.
- **Demandes de retrait** : La plupart des plateformes vous permettent de demander le retrait des contenus incriminés. Elles peuvent vous demander de prouver votre identité.

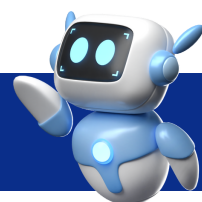
3. Contacter les autorités :

- **Porter plainte** : Si l'usurpation cause des dommages (par exemple, diffamation, fraude), vous pouvez porter plainte auprès de la police ou des autorités compétentes.
- **Signalement de l'abus** : signaler l'infraction sur la plateforme Pharos du Ministère : [PHAROS](#) ; et obtenez les démarches à suivre avec le site [cybermalveillance](#).
- **Commission nationale informatique et libertés (CNIL)** : Vous pouvez également contacter la CNIL pour signaler une atteinte à votre vie privée.

4. Alerter vos contacts :

- **Prévenir votre réseau** : Informez vos amis, famille et collègues que votre photo et votre nom sont utilisés sans votre permission. Cela les aidera à reconnaître et signaler l'abus.
- **Publier une annonce** : Faites un post public pour informer vos contacts que quelqu'un utilise votre identité sans autorisation.

Agir rapidement est essentiel pour minimiser les dommages potentiels et récupérer le contrôle sur votre identité en ligne.





USURPATION D'IDENTITÉ



COMMENT S'EN PROTÉGER ?

En prévention, la protection de vos informations est indispensable :

Appliquez les mesures essentielles de sécurité dans vos usages numériques :

- mots de passe robustes : Il est possible d'utiliser un gestionnaire de mots de passe pour sécuriser ses mots de passe (disponible sur internet) et il ne faut pas les divulguer à un tiers (famille, amis, collègues etc).
- mises à jour de vos navigateurs
- réseaux sociaux et comptes divers : **Activez l'authentification à deux facteurs (2FA)** pour tous vos comptes, lorsque le site le permet.

Marquez les copies des documents d'identité que vous transmettez en inscrivant par-dessus le motif de l'envoi, la date et le destinataire pour que vos documents ne soient pas réutilisés à des fins frauduleuses. Exemple d'utilitaire : <https://filigrane.beta.gouv.fr>

Ne donnez que le minimum d'informations personnelles indispensables sur un site ou un service en ligne sur lequel vous vous enregistrez.

Vérifiez régulièrement vos relevés de compte bancaire afin d'identifier toute opération anormale.

Conservez vos informations personnelles et bancaires ainsi que vos documents d'identité en lieu sûr pour qu'ils ne tombent pas dans de mauvaises mains.

Détruisez tous les documents qui contiennent des informations personnelles avant de les jeter. Ils pourraient être récupérés et utilisés par des criminels à vos dépens.

Agir rapidement est essentiel pour minimiser les dommages potentiels et récupérer le contrôle sur votre identité en ligne.

