Particuliers
Publié le 19/11/2022 – Mis à jour le 06/03/2023

Usurpation d'identité

Une personne utilise vos données personnelles et réalise des actes en votre nom (par exemple, ouverture d'un compte ou d'un crédit, démarche administrative) ? Vous êtes victime d'une **usurpation d'identité**. Nous vous expliquons les démarches à entreprendre et comment vous protéger.

Qu'est-ce que l'usurpation d'identité ?

L'usurpation d'identité est le fait de prendre, **sans son accord**, l'identité ou les données personnelles d'une autre personne et de les utiliser dans un **but malveillant**.
Les informations volées peuvent servir à réaliser des **opérations financières** (par exemple, obtention d'un crédit), **administratives** (par exemple, délivrance d'une carte d'identité…) ou **commerciales** (par exemple, achat). Elles peuvent servir à commettre des **infractions** (par exemple, escroquerie) ou à porter atteinte à la **réputation de la victime** (par exemple, diffamation).
C'est un **délit pénal**.
En cas d'utilisation malveillante des **données personnelles** de la victime, on parle d'**usurpation d'identité numérique**.
L'usurpation d'identité est différente de l'usage d'une **fausse identité**. La fausse identité consiste à créer de toutes pièces une **personne inexistante** et à se faire délivrer à ce nom des documents d'identité.

Comment l'identité d'une personne peut-elle être usurpée ?

L'usurpation d'identité peut résulter par exemple des situations suivantes :
Vol ou perte d'une pièce d'identité
Piratage sur les réseaux sociaux (par exemple, récupération de données personnelles)
Envoi de documents personnels à de fausses annonces de location ou d'emploi
Envoi de renseignements personnels à un faux organisme ou une fausse administration
Récupération de documents sensibles (relevé bancaire, bulletin de salaire…) dans la poubelle

Quelles peuvent être les conséquences de l'usurpation d'identité ?

L'usurpateur peut utiliser le **nom** et les **données personnelles** de la victime pour, par exemple :
Ouvrir un compte et utiliser la carte de crédit ou le chéquier pour faire des achats
Souscrire un crédit au nom de la victime et ne pas le rembourser
Bénéficier d'aides sociales auprès de la sécurité sociale ou de la Caf
Ouvrir une ligne téléphonique
Créer des comptes sur les réseaux sociaux
Fabriquer de faux papiers
Commettre une infraction (par exemple, incitation à la violence, chantage, cyberharcèlement sous l'identité de la victime)

Comment vérifier qu'il y a eu usurpation d'identité ?

La victime peut vérifier qu'elle fait l'objet d'une usurpation d'identité en :
Vérifiant ses relevés bancaires
Surveillant la réception de contraventions ou d'amende et s'assurer qu'elle n'a pas personnellement commis l'infraction (par exemple, un excès de vitesse)
Vérifiant si des comptes ont été ouverts à son nom au fichier des comptes bancaires et assimilés (Ficoba)
Vérifiant auprès de la Banque de France qu'elle n'est pas inscrite sur le fichier central des chèques (FCC) ou le fichier des incident de remboursement des crédits (FICP)
Tapant régulièrement son nom dans un moteur de recherche pour voir quelles informations circulent sur internet

Que peut faire la victime en cas d'usurpation d'identité ?

En cas de **soupçon** d'usurpation d'identité, la victime peut déposer une main courante pour **signaler les faits** (perte de son document d'identité, envoi des documents personnelles à une fausse annonce d'emploi…).
Quand la victime se rend compte qu'**on utilise son nom ou ses données personnelles à son insu**, elle est **victime** d'une usurpation d'identité. Elle peut **porter plainte** et avertir les administrations et organismes concernés.

Déposer une main courante

En cas de **soupçon d'une éventuelle usurpation d'identité** (par exemple suite à un piratage informatique ou à la perte de documents d'identité), une peut être déposée.

C'est une déclaration qui doit être faite en **dans un commissariat ou une gendarmerie**.

Les faits (nature, date, lieu…) sont consignés dans un registre de police ou de gendarmerie.

Cette main courante pourra servir à dater les faits ou de justificatif dans une procédure pénale ultérieure.

Porter plainte

La victime peut dès qu'elle se rend compte qu'une infraction a été commise. Par exemple quand elle reçoit une demande de remboursement d'un crédit qu'elle n'a pas souscrit.

La plainte doit être accompagnée de toutes les **preuves** (capture d'écran, messages, adresses des pages Internet concernées, documents de demande de remboursement…).

Lors du dépôt de plainte, la victime peut donner son accord pour être enregistrée au fichier des personnes recherchées (FPR) pour les besoins de l'enquête.

À savoir

La main courante et la plainte ont de **buts** différents.

Si vous estimez être **victime** d'une infraction pénale et que vous souhaitez que **l'auteur soit poursuivi**, alors vous devez **porter plainte**.

Si vous souhaitez faire **constater** une situation, **signaler** ou **dénoncer** des faits dont vous êtes **témoin ou victime** sans qu'il y ait des poursuites pénales, alors vous devez déposer **une main courante**.

Prévenir les organismes, administrations …

Si l'usurpation d'identité concerne le domaine financier

La victime doit **prévenir les établissements bancaires** ou financiers (société de crédit…).

Elle peut obtenir la liste des comptes bancaires ouverts à son nom en consultant le fichier des comptes bancaires et assimilés (Ficoba)

Elle peut vérifier qu'elle n'est pas fichée à la Banque de France en consultant le fichier central des chèques (FCC) et le fichier des incident de remboursement des crédits (FICP).

La victime peut établir une attestation sur l'honneur aux organismes qui la mettent en cause pour déclarer qu'elle n'est pas l'auteur des actes en joignant une copie de sa plainte.

Si l'usurpation d'identité concerne le domaine administratif

La victime **doit informer les organismes et administrations** (Caf , sécurité sociale, caisse de retraite, mutuelle, impôts…) de l'usurpation d'identité.

L'usurpation d'identité concerne une amende

La victime qui reçoit une **demande de paiement d'une amende** pour des faits qu'elle n'a pas commis doit déposer plainte pour usurpation d'identité.

Elle doit contester l'amende.

Pour les infractions routières (par exemple, excès de vitesse), en cas d'usurpation de plaques d'immatriculation, elle peut demander l'attribution d'un nouveau numéro d'immatriculation et une nouvelle carte grise.

Il s'agit d'une usurpation d'identité numérique

On parle d'**usurpation d'identité numérique** lorsqu'une personne utilise sur Internet les éléments d'identification d'une autre personne, sans son accord. Il peut s'agir de ses nom et prénom, de photos, de son adresse électronique, mais aussi des adresses IP, des logos…

La victime peut porter plainte et **signaler** l'usurpation d'identité numérique directement aux **plateformes concernées** (Facebook, X, Instagram, Snapchat, YouTube…).

La victime peut demander le retrait de la publication malveillante.

Quelles sont les sanctions en cas d'usurpation d'identité ?

L'usurpation d'identité est un délit.

La peine prévue est 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 social.

Lorsque cette infraction est commise par l'**époux**, le **partenaire de Pacs** ou le **concubin** de la victime, la peine est portée à **2 ans d'emprisonnement** et 30 000 € d'amende.

Le fait de prendre le nom d'un tiers lors de la commission d'une infraction pouvant entraîner des poursuites pénales est puni de **5 ans d'emprisonnement** et 75 000 € d'amende. Par exemple, lorsqu'une personne se fait interpeller avec des stupéfiants et qu'elle donne le nom, l'adresse… d'une autre personne qui est par la suite convoquée devant le tribunal pour être jugée.

Comment se protéger d'une usurpation d'identité ?

Pour éviter une usurpation d'identité, certaines précautions peuvent être prises , comme par exemple :

Installer un **logiciel anti-spam**, un **anti-virus**
Mettre régulièrement à jour les appareils, logiciels ou applications de sécurité
Utiliser des mots de passe différents et **complexes** pour chaque sites et applications
En cas de doute sur l'expéditeur d'un message, **vérifier le site Internet** en entrant manuellement son adresse (URL) dans le navigateur
Avant de jeter des documents sensibles (relevés bancaires, bulletins de salaire, avis d'imposition….), les **déchirer** de manière à les rendre illisibles ou impossible à reconstituer
Ajouter une mention sur les documents transmis (filigrane) indiquant le motif de l'envoi, la date et le destinataire afin qu'ils ne soient pas réutilisés à des fins frauduleuses
Bien se **déconnecter de tous les comptes** lors d'une connexion à un **ordinateur** ou un **réseau Wi-Fi public**
Vol – Vandalisme – Escroquerie

Questions – Réponses

- Qu'est-ce qu'une main courante ?
- Responsabilité des contenus publiés sur internet : quelles sont les règles ?
- Que doit faire un étranger en cas de vol de sa carte de séjour ?

Toutes les questions réponses

Et aussi…

- Arnaques sur internet (THESEE, Pharos …)
- Porter plainte
- Usurpation de plaque d'immatriculation d'un véhicule
- Amendes
- Carte d'identité d'un majeur : en cas de perte
- Carte d'identité d'un mineur : en cas de perte
- Carte d'identité d'un majeur : en cas de vol
- Fichier des personnes recherchées (FPR)
- Fichier des comptes bancaires (Ficoba)
- Fichier central des chèques (FCC)
- Fichier des incidents de remboursement des crédits aux particuliers (FICP)

Pour en savoir plus

- Cybermalveillance.gouv.fr
  Source : GIP ACYMA (Actions contre la cybermalveillance)

Où s'informer ?

- **116 006 – Numéro d'aide aux victimes**
  Ce service permet aux victimes d'infractions (hors atteintes aux biens sur internet) d'être écoutées et dirigées vers un réseau associatif et/ou tout professionnel spécialisé dans la protection des victimes.
  En France métropolitaine
  116 006
  Appel gratuit
  Service joignable tous les jours de l'année, de 9h à 19h.
  Hors métropole (ou depuis l'étranger)
  + 33 (0)1 80 52 33 76
  Appel gratuit
  Service joignable tous les jours de l'année, de 9h à 19h.
  Pour les personnes malentendantes
  Par mail : victimes@116006.fr

- **Info Escroqueries**
  Par téléphone
  0 805 805 817
  Du lundi au vendredi de 9h à 18h30.
  Numéro vert (appel gratuit depuis la France).

- Banque de France Particuliers

Services en ligne

- Assistance pour les victimes de cybermalveillance – 17Cyber
  Téléservice
- Filigrane
  Téléservice

Textes de référence

- Code pénal : article 226-4-1
- Code pénal : articles 226-16 à 226-24
  Article 226-18
- Code pénal : articles 434-7-1 à 434-23-1
  Article 434-23
- Décret n°2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées (FPR)
  Inscription au FPR d'une personne dont l'identité est usurpée

Luberon Monts de Vaucluse
Horaires : Lundi au vendredi de 8h30 à 12h00 et de 13h30 à 17h00
Adresse : 315 avenue Saint Baldou 84300 Cavaillon
Tél. : 04 90 78 82 30