

Le Manuel **Anti-Usurpation** **d'identité**

**empêche les fraudeurs
d'utiliser ton identité
pour te créer des dettes,
et des problèmes
administratifs à ton insu**



présentation



Par **Eléna Senoussy**, **ingénieure d'affaires internationales** diplômée de l'Instivoust Mines Télécom Business School.

Après une année d'apprentissage **dans la cybersécurité à la Société Générale**, je me suis lancée sur les réseaux sociaux pour démocratiser l'accès à ce sujet jugé complexe.

D'abord sur Instagram puis ensuite sur TikTok, **mes conseils pratiques ont été vus 7M+ de fois en 3 ans**. La marque *Acronis* m'a fait confiance pour promouvoir leur produit Cyber Protect Home Office auprès de ma communauté.

- **50K+ abonnés** sur les réseaux sociaux,
- **7M+ vues** générées en moins d'un an
- **160K+ likes** cumulés sur tous mes contenus

avertissement

Avant de commencer cette formation, je souhaite préciser un point essentiel : le but n'est pas de t'inquiéter, de te rendre méfiant envers tout ni de créer une forme de paranoïa numérique.

La cybersécurité n'est pas là pour faire peur, mais pour te donner du pouvoir.

Aucune formation, aucun outil, aucune personne ne peut garantir à 100 % que tu ne seras jamais victime d'une attaque, d'une tentative d'arnaque ou d'un piratage. *Cela n'existe pas, et si on te le promet : pars en courant, car en cybersécurité le risque 0 n'existe pas.*

En revanche, ce que cette micro-formation t'apporte, ce sont les bonnes pratiques, les bons réflexes et la compréhension nécessaire pour réduire considérablement les risques et naviguer en ligne de manière plus sereine et plus consciente.

Tu auras toutes les cartes en main :

- à toi de choisir comment les utiliser,
- à toi de décider où mettre tes limites,
- à toi d'appliquer ce qui fait le plus de sens dans ton quotidien.

L'objectif est simple : te rendre plus autonome, plus confiant et mieux préparé, sans jamais tomber dans l'excès de vigilance.

SOMMAIRE

MODULE 1 : Comprendre le danger réel de l'usurpation d'identité

MODULE 2 : Faire ton audit de vulnérabilité

MODULE 3 : Créer ton bouclier numérique

MODULE 4 : Créer ton bouclier administratif

MODULE 5 : Les 15 arnaques qui servent à te voler ton identité

MODULE 6 : Vérifier si tes données sensibles circulent déjà

MODULE 7 : Le plan d'urgence en cas d'usurpation d'identité



BONUS #1 : 4 MODÈLES DE COURRIERS PRÊTS À L'EMPLOI EN CAS D'USURPATION D'IDENTITÉ



BONUS #2 : LA CHECKLIST 10 MINUTES PAR MOIS

INTRODUCTION

Si tu lis ce guide, c'est probablement parce que tu as déjà entendu parler d'une personne victime d'une usurpation d'identité.

Peut-être même que cela t'est arrivé, ou que tu as peur que cela puisse arriver un jour. Et tu as raison de t'y intéresser.

Aujourd'hui, les fraudeurs n'ont plus besoin de cambrioler une maison ou de voler un portefeuille pour faire des dégâts. Quelques informations personnelles suffisent parfois à ouvrir un compte bancaire, souscrire un crédit, créer un abonnement ou réaliser des achats au nom d'une autre personne.

Le plus inquiétant, **c'est que la plupart des victimes découvrent le problème plusieurs semaines, voire plusieurs mois après le début de la fraude.**

La bonne nouvelle, c'est que **tu peux considérablement réduire les risques en mettant en place quelques mesures simples.**

Dans ce guide, tu vas apprendre :

- Comment les fraudeurs récupèrent tes informations
- Quelles sont les données les plus sensibles
- Comment protéger efficacement ton identité
- Comment détecter rapidement une usurpation
- Que faire immédiatement si cela t'arrive

L'objectif est simple : te donner les outils pour reprendre le contrôle de ta sécurité.

MODULE 1 :
COMPRENDRE
LE DANGER RÉEL
DE L'USURPATION
D'IDENTITÉ

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

L'usurpation d'identité consiste à **utiliser les informations personnelles d'une autre personne sans son autorisation afin d'obtenir un avantage financier, administratif ou commercial.**

Ces informations peuvent être :

- Ton nom et prénom
- Ton adresse
- Ton numéro de téléphone
- Ton adresse email
- Une copie de ta carte d'identité / de ton passeport
- Ton RIB
- Ton numéro de sécurité sociale
- Ton permis de conduire

Les fraudeurs peuvent utiliser **une seule information** ou **plusieurs données combinées.**

Pourquoi les fraudeurs s'intéressent-ils à ton identité ?

Parce que **ton identité a de la valeur**. Une copie de carte d'identité accompagnée d'un justificatif de domicile peut parfois suffire pour :

- ouvrir certains comptes bancaires
- souscrire des services
- louer du matériel
- réaliser certaines démarches administratives

Pour un fraudeur, **voler une identité est souvent plus rentable que voler directement de l'argent.**

Comment les fraudeurs récupèrent tes informations ?

1. Les faux emails

Tu reçois un message qui semble provenir de ta banque, d'un transporteur ou d'une administration.

Le message **t'invite à cliquer sur un lien.**

Une fois sur le faux site, **tu saisis toi-même tes informations. Le fraudeur n'a plus qu'à les récupérer.**

2. Les faux SMS

Tu reçois un message : "Votre colis est bloqué. Cliquez ici." ou "Une activité suspecte a été détectée sur votre compte bancaire."

Ces messages sont conçus **pour créer un sentiment d'urgence.** Quand tu paniques, tu réfléchis moins.

3. Les réseaux sociaux

De nombreuses personnes affichent publiquement :

- leur date de naissance
- leur ville
- leur banque
- leur employeur
- leurs photos de documents sensibles
- leurs habitudes quotidiennes

Chaque information peut être utilisée pour construire un dossier sur (et contre) toi.

4. Les fuites de données

Même si tu es prudent, **certaines entreprises peuvent être victimes de piratages**. Tes données peuvent alors circuler sur Internet sans que tu en sois responsable.

Les 10 données les plus convoitées

Voici les informations que tu dois protéger en priorité :

1. Carte d'identité
2. Passeport
3. Permis de conduire
4. Numéro de sécurité sociale
5. Relevé d'identité bancaire
6. Adresse email principale
7. Numéro de téléphone
8. Justificatif de domicile
9. Identifiants bancaires
10. Mots de passe

Les conséquences possibles

Certaines victimes découvrent :

- **des crédits** effectués en leur nom
- **des abonnements** souscrits sans leur accord
- **des achats** qu'elles n'ont jamais effectués
- **des comptes** ouverts frauduleusement

Dans certains cas, **plusieurs mois de démarches sont nécessaires pour rétablir la situation**.

EXERCICE

Réponds honnêtement :

- **As-tu déjà envoyé une copie de ta carte d'identité par email ?**
- **Utilises-tu le même mot de passe sur plusieurs sites ?**
- **Tes réseaux sociaux sont-ils publics ?**
- **As-tu activé la double authentification sur tes comptes importants ?**
- **Connais-tu les démarches à effectuer en cas de fraude financière ou usurpation d'identité ?**

Plus tu réponds "oui" aux trois premières questions ou "non" aux deux dernières, **plus ton niveau d'exposition est élevé.**

MODULE 2 :
FAIS
TON AUDIT
DE
VULNÉRABILITÉ

Avant de renforcer ta protection, **il faut identifier les failles**, alors imagine que tu sois un fraudeur.

Quelles informations pourrais-tu récupérer sur toi facilement ? C'est **exactement** ce que nous allons vérifier.

Documents

- ☐ J'ai déjà envoyé ma pièce d'identité à plusieurs organismes par email sans aucune protection
- ☐ Je conserve mes documents sensibles dans un dossier non protégé
- ☐ Je garde des photos de mes documents dans mon téléphone

Mots de passe

- ☐ J'utilise le même mot de passe sur plusieurs sites
- ☐ Certains mots de passe sont simples à deviner
- ☐ Je ne possède pas de gestionnaire de mots de passe

Réseaux sociaux

- ☐ Mon profil est public
- ☐ Ma date de naissance est visible
- ☐ Mon adresse ou mon lieu de travail est visible
- ☐ J'accepte régulièrement des demandes d'inconnus

Sécurité des comptes

- ☐ Je n'utilise pas la double authentification
- ☐ Je ne vérifie jamais les connexions à mes comptes
- ☐ Je ne reçois pas d'alertes de sécurité

Calcul de ton score de risque

Compte un point pour chaque case cochée.

→ 0 à 3 points : risque faible.

→ 4 à 8 points : risque modéré. Des améliorations sont nécessaires.

→ 9 points et plus : risque élevé, tu es une cible facile pour un fraudeur.

MODULE 3 :
CRÉER
TON BOUCLIER
NUMÉRIQUE

Maintenant que tu connais tes faiblesses, il est temps de **construire ton bouclier numérique**. Le principe est simple : même si un fraudeur obtient une information sur toi, **il doit rencontrer suffisamment d'obstacles pour abandonner**.

Sécurise ton adresse email

Ton adresse email est **la clé de presque tous tes comptes**. Si un fraudeur prend le contrôle de ton email, **il peut souvent réinitialiser tes autres mots de passe**.

Commence par :

- **utiliser une adresse email secondaire pour éviter de donner ton adresse email principale partout, et limiter les risques de piratage et d'usurpation d'identité**
- changer ton mot de passe
- utiliser un mot de passe unique pour CHAQUE compte
- activer la double authentification
- vérifier les appareils connectés

Utilise un gestionnaire de mots de passe

Beaucoup de personnes réutilisent le même mot de passe partout. C'est l'une des erreurs les plus dangereuses. Imagine qu'un site soit piraté, si tu utilises le même mot de passe pour ta banque, tes réseaux sociaux et ton email, **tous tes comptes deviennent vulnérables**.

Un gestionnaire de mots de passe permet de **générer et stocker des mots de passe complexes sans avoir à les mémoriser**. Voici le meilleur gestionnaire [ici](#).

Active la double authentification

Même si quelqu'un découvre ton mot de passe, **il devra encore valider une seconde étape.**

Par exemple :

- un code reçu sur ton téléphone
- une application d'authentification
- une clé de sécurité

Cette mesure réduit énormément le risque de piratage.

Vérifie les appareils connectés

Au moins une fois par mois :

- consulte les appareils connectés à tes comptes
- déconnecte ceux que tu ne reconnais pas
- change immédiatement ton mot de passe en cas de doute

Un appareil inconnu est un signal d'alerte précoce à ne pas ignorer.

MODULE 4 :
CRÉER
TON BOUCLIER
ADMINISTRATIF

La plupart des personnes pensent immédiatement aux mots de passe lorsqu'on parle de sécurité.

Pourtant, **les documents administratifs** sont souvent **la cible préférée des fraudeurs**.

Une copie de **carte d'identité**, un **justificatif de domicile** ou un **relevé bancaire** peuvent parfois suffire à monter un dossier crédible.

Ton objectif est donc simple : **limiter au maximum l'accès à tes documents sensibles**.

Les documents à protéger en priorité

Voici les documents les plus recherchés par les fraudeurs :

- Carte nationale d'identité
- Passeport
- Permis de conduire
- Carte Vitale
- Justificatif de domicile
- Relevé d'identité bancaire (RIB)
- Avis d'imposition
- Bulletins de salaire
- Contrats d'assurance
- Documents bancaires

Considère chacun de ces documents comme de l'argent liquide. Tu ne laisserais pas 5 000 € traîner sur une table ! Tes documents méritent la même protection.

Où stocker tes documents ?

À éviter

- Galerie photo du téléphone
- Bureau de l'ordinateur
- Clé USB non protégée
- Pièces jointes dans les emails

Ces emplacements sont faciles à consulter si ton appareil est compromis.

À privilégier

- **Coffre-fort physique pour les originaux**
- **Dossier chiffré avec mot de passe sur ordinateur**
- **Service cloud sécurisé** avec double authentification
- **Gestionnaire de documents sécurisé**

La règle des copies inutiles

Plus il existe de copies d'un document, plus le risque augmente. Pour éviter ça : fais régulièrement le ménage.

Supprime :

- les anciennes copies
- les scans inutiles
- les photos de documents conservées "au cas où"

Comment envoyer une pièce d'identité sans prendre de risques ?

C'est probablement l'une des questions les plus importantes. **Tu seras parfois obligé de transmettre une pièce d'identité, mais tu peux limiter les risques.**

Utilise un filigrane

Lorsque tu envoies une copie : ajoute un texte visible sur le document.

Exemple : "COPIE DESTINÉE À L'AGENCE IMMOBILIÈRE XYZ UNIQUEMENT – 15 MAI 2026". Même si le document fuit, son utilisation sera beaucoup plus difficile.

La solution à utiliser pour mettre un filigrane est [ici](#).

Vérifie le destinataire

Avant d'envoyer un document :

- vérifie l'adresse email de l'expéditeur
- appelle l'organisme pour confirmer la demande

Ne te fie jamais uniquement à un email reçu.

Envoyer le document via un fichier chiffré

De cette manière, si une personne intercepte le document, il ne pourra pas y accéder sans mot de passe. Tu communicates le mot de passe de vive-voix au téléphone, ou par SMS mais SURTOUT PAS par email.

Word (PC et MAC)

- >Fichier
- >Informations
- >Protéger un document
- >Chiffrer avec un mot de passe
- >Saisir le mot de passe
- >Cliquer sur OK
- >Saisir une seconde fois le mot de passe
- >Cliquer sur OK

Pages (MAC)

- >Fichier
- >Définir un mot de passe
- >Saisir une seconde fois le mot de passe
- >Indiquer un indice du mot de passe
- >Cliquer sur définir le mot de passe

Ne jamais envoyer plusieurs documents sensibles en une fois

Évite d'envoyer tout d'un seul coup : pièce d'identité + RIB + contrat

Supprime les emails après leur envoi

Ta boîte mail est une archive accessible. Supprime les documents une fois qu'ils ont été envoyés.

N'envoie jamais plus que nécessaire

Si seul un justificatif de domicile est demandé, n'envoie pas également ta carte d'identité.

Les fraudeurs adorent accumuler les informations.

MODULE 5 :
LES 15 ARNAQUES
LES + UTILISÉES
POUR VOLER TON
IDENTITÉ

Les fraudeurs utilisent souvent les mêmes méthodes. Lorsque tu connais leurs techniques, **il devient beaucoup plus facile de les repérer.**

1. Le faux conseiller bancaire

Tu reçois un appel, la personne connaît ton nom. Elle parle comme un professionnel et t'explique qu'une fraude est en cours. Puis elle te demande :

- ton identifiant
- ton mot de passe
- un code reçu par SMS

À ce moment-là, **il s'agit presque toujours d'une fraude.** Ta banque ou quiconque ne te demandera jamais ces informations.

2. Le faux colis

Tu reçois un SMS : "Votre colis ne peut être livré. Cliquez ici." **Le site ressemble à celui d'un transporteur.**

Tu renseignes alors :

- ton adresse
- ton téléphone
- parfois même tes coordonnées bancaires

Le fraudeur récupère tout.

3. Le faux CPF

Tu reçois un appel concernant tes droits à la formation. **Le but réel est souvent de récupérer tes informations personnelles.**

4. Le faux support technique

Un message apparaît sur ton ordinateur : "Votre appareil est infecté, un numéro s'affiche.

Lorsque tu appelles, le fraudeur tente de prendre le contrôle de ton ordinateur.

5. Le faux employeur

Tu postules à une offre d'emploi. L'entreprise demande :

- carte d'identité
- RIB
- justificatif de domicile

Le poste n'existe pas.

6. Le faux propriétaire

Dans le cadre d'une location, **certains fraudeurs réclament des dossiers complets avant même une visite.**

7. Le faux acheteur

Sur les plateformes de vente entre particuliers, **le fraudeur prétend acheter ton bien et cherche à obtenir tes coordonnées bancaires.**

8. Le faux concours

"Félicitations ! Vous avez gagné." Pour recevoir ton prix, il faut fournir plusieurs informations personnelles.

Le prix n'existe pas.

9. Le faux QR Code

Tu scannes un QR Code placé sur un parking ou un automate. **Tu arrives sur un faux site.**

10. Le faux remboursement

Impôts, assurance maladie, énergie...

Le fraudeur annonce un remboursement et te demande de confirmer tes informations.

11. Le faux proche en difficulté

Un message : "Bonjour maman, j'ai changé de numéro."

L'objectif est d'obtenir de l'argent ou des informations personnelles.

12. Le faux organisme administratif

Le fraudeur se fait passer pour :

- les impôts
- la sécurité sociale
- une mairie
- une administration

13. Le faux réseau Wi-Fi

Un réseau public porte un nom rassurant. **Tu t'y connectes. Tes données peuvent être interceptées.**

14. Les deepfakes

Grâce à l'intelligence artificielle, **les fraudeurs peuvent désormais imiter une voix ou une image.** Ne fais jamais confiance à une vidéo ou à un appel uniquement parce qu'il semble authentique.

15. Les réseaux sociaux

Certaines personnes publient elles-mêmes suffisamment d'informations pour faciliter l'usurpation de leur identité. **Fais attention à ce que tu rends public.**

MODULE 6 :
VÉRIFIE
SI TES DONNÉES
CIRCULENT DÉJÀ
QUELQUE PART

L'objectif n'est pas seulement de prévenir.
Il faut aussi **détecter rapidement un problème.**

Vérifie tes adresses email

Si ton adresse email a été compromise lors d'une fuite de données, il est préférable **de le savoir rapidement.**
Effectue régulièrement **une vérification** sur des services spécialisés. Test à effectuer [ici](#).

Si ton adresse apparaît dans une fuite :

- change ton mot de passe
- active la double authentification
- surveille les connexions inhabituelles

Surveille tes comptes bancaires

Prends l'habitude de consulter régulièrement :

- les virements
- les prélèvements
- les paiements par carte

Une petite anomalie est parfois le premier signe d'une fraude plus importante.

Vérifie tes comptes en ligne

Tous les mois :

- consulte les appareils connectés
- vérifie les alertes de sécurité
- contrôle les modifications récentes

Fais ton audit Google

Tape régulièrement :

- ton nom
- ton adresse email
- ton numéro de téléphone

Tu pourrais être surpris de ce qui est visible publiquement.

Fréquence recommandée

Chaque semaine

- Contrôle bancaire rapide.

Chaque mois

- Vérification des comptes importants.

Chaque trimestre

- Audit complet de sécurité.

MODULE 7 :
PLAN D'URGENCE
EN CAS
D'USURPATION
D'IDENTITÉ

Si tu découvres une fraude, **chaque heure compte**.
L'objectif est de limiter les dégâts le plus rapidement possible.

LES PREMIÈRES 24 HEURES

Étape 1 : Sécurise immédiatement tes comptes

Change :

- ton mot de passe email
- tes mots de passe sensibles
- tes accès bancaires

Active la double authentification partout où elle est disponible.

Étape 2 : Contacte ta banque

Explique la situation.

Demande :

- la surveillance du compte
- le blocage si nécessaire
- des conseils adaptés à ton cas

Étape 3 : Conserve toutes les preuves

Ne supprime rien.

Conserve :

- emails
- SMS
- captures d'écran
- relevés bancaires

LES PREMIÈRES 72 HEURES

Dépose un signalement

Plus la fraude est signalée rapidement, plus il est facile de démontrer ta bonne foi.

Contacte les organismes concernés

Si un document a été compromis :

- mairie
- préfecture
- assurance
- banque
- opérateur téléphonique

Informe les plateformes concernées

Si un compte a été piraté :

- réseau social
- messagerie
- boutique en ligne

LES SEMAINES SUIVANTES

Continue à surveiller :

- tes comptes
- tes courriers
- tes démarches administratives

Certaines fraudes apparaissent plusieurs semaines après le vol initial des données.

BONUS #1 :
4 MODÈLES
DE COURRIERS
PRÊTS À L'EMPLOI

1 - SIGNALER UNE FRAUDE À TA BANQUE

Objet : Signalement immédiat d'une opération frauduleuse sur mon compte bancaire

Madame, Monsieur,

Je vous contacte en urgence concernant une ou plusieurs opérations suspectes détectées sur mon compte bancaire. Je pense être victime d'une fraude ou d'une tentative d'escroquerie.

Voici les informations dont je dispose :

- Nom : [Ton nom]
- Numéro de compte : [XXX]
- Date(s) des opérations suspectes : [XX/XX/XXXX]
- Montant(s) concerné(s) : [XXX €]
- Description : [virement, paiement carte, prélèvement inconnu...]

Je vous demande de bien vouloir :

- Bloquer immédiatement les opérations suspectes similaires
- Me confirmer les démarches à suivre pour contester ces opérations
- Me conseiller sur les mesures de sécurité à mettre en place

Je reste disponible pour toute information complémentaire.

Cordialement,

[Nom / Prénom]

[Numéro de téléphone]

2 - CONTESTER UNE OPÉRATION FRAUDULEUSE À TA BANQUE

Objet : Contestation d'une opération bancaire non autorisée

Madame, Monsieur,

Je vous écris afin de contester une opération bancaire que je n'ai pas autorisée. Cette opération me semble frauduleuse.

Détails de l'opération :

- Date : [XX/XX/XXXX]
- Montant : [XXX €]
- Libellé : [description visible sur le relevé]
- Moyen de paiement : [carte / virement / prélèvement]

Je certifie ne pas être à l'origine de cette transaction.

Je vous demande donc :

- Le remboursement de cette opération non autorisée
- L'ouverture d'une procédure de contestation
- La sécurisation de mon moyen de paiement concerné

Je reste à votre disposition pour toute information complémentaire.

Cordialement,

[Nom / Prénom]

[Numéro de compte]

3 - DÉCLARATION D'USURPATION D'IDENTITÉ

Objet : Déclaration d'usurpation d'identité

Madame, Monsieur,

Je vous informe être victime d'une usurpation d'identité. Des tiers ont utilisé ou tentent d'utiliser mes informations personnelles sans mon consentement.

Informations me concernant :

- Nom et prénom : [XXX]
- Date de naissance : [XX/XX/XXXX]
- Adresse : [XXX]
- Pièce d'identité concernée : [CNI / passeport...]

Je constate les faits suivants :

- [ex : ouverture de compte / crédit / abonnement non autorisé / utilisation frauduleuse de mes données]

Je vous demande :

- De prendre en compte cette déclaration officielle
- De bloquer toute activité suspecte liée à mon identité
- De m'indiquer les démarches à suivre pour protéger mes droits
- De conserver cette déclaration dans votre système

Je reste à disposition pour toute vérification ou document complémentaire.

Cordialement,

[Nom / Prénom]

[Coordonnées]

4 - SIGNALER UNE FRAUDE À UN ORGANISME (IMPÔTS, CAF...)

**Objet : Signalement d'une tentative de fraude /
usurpation d'identité**

Madame, Monsieur,

Je vous contacte afin de signaler une tentative d'utilisation frauduleuse de mon identité auprès de votre organisme.

Je pense être victime d'une usurpation d'identité ou d'une tentative de fraude.

Informations me concernant :

- Nom : [XXX]
- Numéro d'identification (si applicable) : [XXX]
- Adresse : [XXX]

Faits constatés :

- [ex : demande inhabituelle / création de dossier / email suspect / activité non autorisée]

Je vous demande :

- De vérifier l'intégrité de mon dossier
- De bloquer toute action suspecte
- De m'informer de toute activité liée à mon identité
- De m'indiquer les démarches à suivre

Je vous remercie pour votre vigilance.

Cordialement,

[Nom / Prénom]

[Coordonnées]

BONUS #2 :
LA CHECKLIST
10 MINUTES
PAR MOIS

À VÉRIFIER CHAQUE MOIS

- ☐ Vérifier ses comptes bancaires
- ☐ Contrôler les appareils connectés
- ☐ Vérifier les alertes de sécurité
- ☐ Mettre à jour les mots de passe sensibles
- ☐ Contrôler ses réseaux sociaux
- ☐ Supprimer les documents inutiles
- ☐ Vérifier les connexions inhabituelles
- ☐ Sauvegarder ses données importantes
- ☐ Mettre à jour ses appareils
- ☐ Vérifier ses paramètres de sécurité

**C'EST
DÉJÀ
TERMINÉ !**

Merci pour
ta confiance 🤝

À bientôt,
Eléna.

Le Manuel Anti-Usurpation d'identité

**empêche les fraudeurs
d'utiliser ton identité
pour te créer des dettes,
et des problèmes
administratifs à ton insu**

