GOUVERNEMENT

Liberté
Égalité
Fraternité

TASK FORCE NATIONALE DE LUTTE CONTRE LES ARNAQUES

GUIDE DE PRÉVENTION CONTRE LES ARNAQUES

AVANT PROPOS

La Task-Force lance un appel à la vigilance et propose un guide de prévention contre les arnaques

La vulnérabilité des consommateurs et des entreprises face à des manoeuvres frauduleuses s'est accrue avec la crise sanitaire engendrée par l'épidemie de la Covid 19. Il est essentiel de maintenir une vigilance permanente en rappelant les attitudes réflexes qu'il convient d'adopter pour déjouer de potentielles arnaques. À cette fin, les services de l'État et les autorités de contrôle s'associent et proposent des fiches préventives d'identification des principales fraudes.

SOMMAIRE

INTRODUCTION
La Task-Force nationale de lutte contre les arnaques se mobilise et publie un guide de prévention contre les arnaques

L'épidémie de COVID-19 s'est accompagnée d'une recrudescence de fraudes et d'arnaques, notamment en ligne, d'autant plus inacceptables qu'elles visent des personnes et des entreprises déjà durement touchées par la crise sanitaire et les mesures de confinement.

Les administrations et autorités de contrôle se sont rapidement mobilisées, pour mettre en place une coopération renforcée que la gravité de la situation exigeait, dans la prévention et la lutte contre ces fraudes et arnaques protéiformes.

A cet effet, le Ministre de l'économie, des finances et de la relance a proposé, au début du mois d'avril 2020, la création d'une « Task-force » nationale de lutte contre les fraudes et arnaques liées à la crise de la Covid19 pilotée par la DGCCRF.

La vulnérabilité des consommateurs et des entreprises face à ces pratiques frauduleuses s'est encore accrue avec la reprise, partielle dans plusieurs secteurs, de l'activité économique fortement déstabilisée.

Face à cette situation, la Task-Force se pérennise avec pour objectif de maintenir les échanges de signalements et d'informations en vue d'une réaction rapide contre les fraudes exploitant l'incertitude et la fragilité économique induite par la crise.

La Task-Force nationale de lutte contre les arnaques propose un guide pour se prémunir contre les fraudes et les arnaques.

Les fraudes et arnaques sont très variées et touchent tant les consommateurs que les entreprises :

– achat de produits sanitaires (gel hydro-alcoolique, masques...),
– produits ou méthodes miracles,
– faux ordres de virements,
– usurpations d'identité de professionnels,
– faux sites administratifs collectant illicitement des données personnelles ou les coordonnées bancaires,
– fraudes s'appuyant sur la générosité des donateurs,
– offre de produits d'épargne et de crédits aux conditions particulièrement attractives,
– prospections commerciales non sollicitées (SPAM),
– hameçonnage, phishing,
- pratiques abusives dans le domaine du « dropshipping »,
- ventes en réseau multi-niveaux illicites ;

soit autant d'exemples de pratiques infractionnelles.

L'ensemble des services de l'Etat est mobilisé pour faire cesser ces pratiques et les faire sanctionner.

La Task Force mutualise les compétences de chacun afin d'optimiser l'action de l'Etat.

Le guide est accessible au grand public sur les sites suivants :

https://www.police-nationale.interieur.gouv.fr

https://www.gendarmerie.interieur.gouv.fr/Notre-communication2/Publications-Documentations

https://acpr.banque-france.fr

https://www.amf-france.org/fr

https://www.abe-infoservice.fr

https://www.economie.gouv.fr/dgccrf

PRÉSENTATION
Des administrations impliquées

- Le Ministère de l'Intérieur :
• la direction générale de la police nationale (DGPN)
• la direction centrale de la police judiciaire (DCPJ)
• la direction générale de la gendarmerie nationale (DGGN)
• le pôle judiciaire de la gendarmerie nationale (PJGN)

- Le Ministère de l'Économie et des Finances :
• la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), chargée de la protection des consommateurs

- Le Ministère de l'action et des comptes publics :
• la direction générale des finances publiques (DGFIP)
• la direction générale des douanes et des droits indirects (DGDDI)

- Le Ministère de la Justice :
• la direction des affaires criminelles et des grâces (DACG)

- Le Ministère de l'Agriculture :
• la direction générale de l'alimentation (DGAL)

- L'Autorité des marchés financiers (AMF) et l'Autorité de contrôle prudentiel et de résolution (ACPR), les autorités de contrôle du secteur financier

- La Commission Nationale de l'Informatique et des Libertés (CNIL) :
• pour les atteintes aux données personnelles

- L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

ARNAQUES AUX ACHATS EN LIGNE
Achat sur internet : achetez serein

La pandémie de COVID-19 a conduit de nombreux consommateurs à se tourner vers le commerce électronique. Dans le même temps, de nombreuses fraudes et arnaques ont été mises en évidence par les services de contrôle : produits de faible qualité, voire dangereux ou qui ne sont pas livrés.

➔ Pour acheter serein, suivez les conseils suivants !

Vérifiez l'identité du vendeur

Avant toute commande, il est recommandé de contrôler que le site internet sur lequel vous naviguez n'est pas seulement une façade mais qu'il y a bien une entreprise réelle derrière celui-ci. Les vendeurs en ligne sont tenus de mettre à la disposition des consommateurs des informations claires et facilement accessibles sur leur identité. Recherchez les mentions légales (nom, dénomination sociale, adresse, les contacts comme un numéro de téléphone ou une adresse électronique). Ces informations, généralement présentes dans les conditions générales de vente, doivent obligatoirement vous être fournies !

➔ **Important :** Lorsque vous achetez sur une « place de marché » ou « marketplace », le vendeur n'est pas la plateforme en elle-même mais un vendeur tiers. L'identité du vendeur doit vous être fournie. Soyez particulièrement vigilants !

Choisir un site français ou européen

Il est préférable de choisir un site français ou européen plutôt que ceux installés hors de l'Union européenne. En effet, ces derniers n'ont pas toujours une bonne connaissance de la réglementation applicable, présentent des prix qui n'incluent pas toujours les droits de douane et de TVA. Par ailleurs, en cas de litige, vos recours contre des sites étrangers auront peu de chance d'aboutir.

➔ **Attention :** Ne supposez pas qu'un site est situé dans le pays indiqué dans son url : «. fr » ne signifie pas forcément que le site est français.

Vérifier la e-réputation

Si vous ne connaissez pas le site sur lequel vous naviguez, il est important de vérifier sa e-réputation. Cela peut être le cas en entrant le nom du site ou du produit sur un moteur de recherche, éventuellement associé avec le terme « arnaque ».

➔ **Attention :** Certains vendeurs peuvent laisser des faux avis positifs sur leur propre site. Ils peuvent aussi payer des moteurs de recherche pour que leur site apparaisse en haut de page. Diversifiez vos sources d'information pour avoir un avis objectif sur un site.

Soyez très attentif à la description des produits

N'achetez pas à l'aveuglette ! Puisque vous ne pouvez ni toucher, ni essayer les produits, ni interroger le vendeur, lisez attentivement le descriptif du produit (ne vous contentez pas de la photo !). Vous devez avoir accès à un maximum d'informations sur le produit ou le service acheté : dénomination complète, qualité, taille ou mesures, composition, accessoires fournis, etc. Si la description est floue, passez votre chemin !

➔ **Important :** Pour certains produits de protection, comme les masques ou les gels hydroalcooliques, assurez-vous des performances des produits que vous achetez et notamment des normes qu'ils respectent ou des tests qui ont été réalisés par les fabricants. (voir fiche dédiée pour les gels hydroalcooliques et la FAQ masques sur le site de la DGCCRF).

➔ **Attention :** La pandémie de COVID-19 a conduit à l'émergence de « produits miracles » : lampes ultra-violet susceptibles d'assainir l'air ou de stériliser des masques ou encore huiles essentielles, infusions ou autres compléments alimentaires supposés vous protéger du coronavirus. Ne vous laissez pas abuser par des promesses sans fondements.

Faites attention au marketing trop agressif

Certains sites jouent sur un marketing très agressif pour influer sur votre comportement d'achat en induisant un sentiment d'urgence et accélérer votre décision : « offre flash », réduction très forte limitée dans le temps, affichage du nombre de consommateurs connectés simultanément sur le site ou encore compteur des produits encore en stock.

Même si une offre est très attractive, prenez le temps de la réflexion et de la comparaison !

MESSAGE DE PRÉVENTION :

1. **Soyez vigilants face à des annonces proposées sur les réseaux sociaux et que vous n'avez pas spécialement sollicitées.**
2. **Prenez le temps de comparer et faites jouer la concurrence ; les mêmes produits sont certainement vendus sur d'autres sites.**
3. **Vérifiez l'identité et les coordonnées du vendeur ; elles doivent toujours être présentes sur le site.**
4. **Repérez les méthodes marketing agressives : compteur de temps (« timer » promotionnel fictif) et de stock (valeur fictive de stock restant), nombre d'acheteurs connectés en même temps (faux compte de visites et de commandes en cours), prix barrés élevés, forte réduction de prix, pop-up automatiques simulant des commandes immédiates d'autres clients.**
5. **Attention à la pression d'achat ; elle est souvent synonyme de pratiques commerciales frauduleuses.**
6. **Sachez identifier les faux avis de consommateurs ; diversifiez vos sources d'informations avant d'acheter.**

Je suis victime, que faire ?

- Je suis victime d'une pratique commerciale frauduleuse sur internet :

Vous pouvez le signaler à la DGCCRF https://www.economie.gouv.fr/dgccrf/contacter-dgccrf

- Je suis victime d'une tentative escroquerie ?

Vous pouvez signaler ces escroqueries sur la plateforme PHAROS (plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements), accessible sur le site www.internet-signalement.gouv.fr.

Cette plateforme, gérée par la police nationale et la gendarmerie nationale, permet notamment de signaler les sites internet dont le contenu est illicite.

Pour s'informer sur les escroqueries ou pour signaler un site internet ou un courriel d'escroqueries, vous pouvez contacter INFO ESCROQUERIES au 0811 02 02 17 (prix d'un appel local depuis un poste fixe, ajouter 0,06€/minute depuis un téléphone mobile), du lundi au vendredi de 9h à 18h.

DROPSHIPPING :
Futurs vendeurs : gare aux mirages !

Vous voulez vous lancer dans le e-commerce ? Vous préférez acheter les produits au fur et à mesure et les faire expédier directement à vos clients par vos fournisseurs ? C'est du dropshipping !

Attention, vous restez soumis à la réglementation et devrez respecter un certain nombre d'obligations. Renseignez-vous avant de vous lancer !

Qu'est-ce que le dropshipping ?

Le dropshipping ou « livraison directe » est une vente sur internet dans laquelle le vendeur ne se charge que de la commercialisation et de la vente du produit. C'est le fournisseur du vendeur qui expédie la marchandise au consommateur final. Le consommateur n'a généralement ni connaissance de l'existence du fournisseur ni de son rôle.

Le dropshipping permet donc de se lancer dans le e-commerce avec un faible investissement de départ, puisque le vendeur ne gère ni le stock, ni la logistique. Ses seules dépenses sont liées à la création de la boutique en ligne et à la mise en avant de ses produits sur le web.

Pour autant, même s'il ne se charge pas de la livraison, le vendeur reste responsable de plein droit de la bonne exécution de la commande passée par le consommateur !

Le dropshipping n'est pas interdit par la réglementation. **Comme pour toute vente, le vendeur doit s'assurer de proposer des produits licites, conformes et non dangereux. Il doit aussi respecter les règles du code de la consommation applicables à la vente à distance, notamment en matière d'information pré-contractuelle du consommateur et ne pas mettre en œuvre de pratiques commerciales déloyales**

Les obligations du vendeur

Le professionnel vendant à distance doit communiquer au consommateur, préalablement à la conclusion de la vente plusieurs **informations, en langue française, de manière lisible et compréhensible**, parmi lesquelles :

- **l'identité et les coordonnées du vendeur ;**
- **l'information sur la date de livraison du bien ou d'exécution du service ;**
- **les caractéristiques des produits ou services proposés ;**
- **le prix en euros toutes taxes comprises ;**
- **l'information sur les garanties légales et contractuelles ;**
- **les conditions, les délais et les modalités d'exercice du droit de rétractation.**

Pour plus d'informations, reportez-vous à la fiche n° 1 « Vente sur internet : achetez serein »

Vous devrez être loyal quant aux informations mises en ligne sur votre ou vos sites de vente.

Vous ne devez pas diffuser d'informations inexactes, incomplètes, trompeuses ou de nature à induire en erreur pour inciter à l'achat, notamment sur :

- **les promotions offertes (pourcentage de réduction et durée) ;**
- **l'origine du produit ;**
- **le nombre de visites et commandes en cours ou passées ;**
- **les avis des clients ;**
- **l'existence d'une marque déposée;**
- **les délais de livraison** (le vendeur professionnel doit livrer le bien ou fournir le service à la date ou dans le délai indiqué au consommateur). Il s'agit d'un point critique de ce mode de vente dans la mesure où le dropshipper maîtrise mal ces délais, le produit étant livré directement par son fournisseur au client final !

Les publicités faites via les réseaux sociaux et/ou par le biais d'influenceurs doivent également respecter ce principe de loyauté.

L'accompagnement à la création de boutiques de dropshipping:

Des sociétés proposent des solutions « clé en main » de création de boutiques en ligne. Elles proposent notamment des pages préconfigurées, appelées « thèmes ».

De nombreuses formations sont également mises en ligne à titre payant par des personnes se présentant comme ayant fait fortune facilement avec ce mode de vente et vous proposant de vous expliquer leurs stratégies commerciales.

MESSAGE DE PRÉVENTION à destination des futurs vendeurs en dropshipping

1. **Soyez vigilants face aux promesses alléchantes de gains financiers et volumes de ventes annoncés par certains formateurs en dropshipping ; les gains affichés résultent souvent de la vente des formations et non des produits vendus en ligne ;**
2. **Il n'existe aucune solution ou pack juridique permettant de s'exonérer de la réglementation en vigueur ou des contrôles. Méfiez-vous des influenceurs proposant des formations miracles.**
3. **Attention aux faux avis positifs utilisés par certains formateurs ;**
4. **Attention aux sites vendus « clé en main », vérifiez qu'ils incluent bien toutes les informations pré-contractuelles obligatoires (cf. ci-dessus). Leur absence vous exposerait en effet à des amendes administratives ; Soyez également vigilant sur le contenu des « thèmes » proposés qui utilisent parfois des supports constitutifs d'infraction pénale (faux rabais, faux compte à rebours de fin de promotion, stocks fictifs..)**
5. **Votre responsabilité peut être engagée si les produits ne respectent pas la réglementation française, notamment en matière de sécurité et de conformité des produits; vous êtes en effet responsable de la qualité, de la conformité et de la sécurité des produits vendus.**

Je suis victime de pratiques abusives, que faire ?

Vous pouvez les signaler à la DGCCRF sur le site : https://www.economie.gouv.fr/dgccrf/contacter-dgccrf

Pour s'informer sur les escroqueries ou pour signaler un site internet ou un courriel d'escroqueries :

INFO ESCROQUERIES au 0811 02 02 17 (prix d'un appel local depuis un poste fixe, ajouter 0,06 €/minute depuis un téléphone mobile), du lundi au vendredi de 9h à 18h.

BESOIN DE GEL HYDRO ALCOOLIQUE
Attention au prix et à la composition

En l'absence de point d'eau disponible, l'utilisation de solutions et gels hydro-alcooliques est recommandée par les autorités sanitaires pour mettre en place les gestes barrière et lutter contre la propagation du virus responsable de la COVID-19.

Comment s'assurer de la qualité d'un gel ou d'une solution hydro-alcoolique ?

Pour se protéger efficacement contre le coronavirus, lorsque le lavage des mains avec de l'eau et du savon n'est pas possible, vous devez vous frictionner les mains pendant au moins trente secondes et jusqu'à l'obtention de mains sèches avec un produit efficace en matière de désinfection.

Vous pouvez utiliser pour ce faire :

- des produits testés selon la norme NF EN 14476.
- des gels ou solutions hydro-alcooliques, dans le cas général à base d'alcool éthylique (ou éthanol), d'alcool propylique (propane-1-ol ou n-propanol) ou encore d'alcool isopropylique (propane-2-ol ou isopropanol).

➔ **Attention :** pour que ces produits soient efficaces, il faut qu'ils contiennent **une concentration d'alcool supérieure à 60% (exprimée en volume/volume ou v/v)**. Sauf cas spécifique (voir ci-dessous), la concentration en alcool doit figurer sur l'étiquetage, prenez le temps de vérifier !

Pour permettre de répondre aux besoins importants des professionnels et des citoyens, les pouvoirs publics **ont autorisé de manière dérogatoire** certains établissements, notamment des fabricants de cosmétiques, de médicaments ou de produits biocides, à en produire selon 4 formulations bien précises permettant de garantir une action virucide. Ces produits peuvent être dénommés : « Solution hydro-alcoolique recommandée par l'Organisation mondiale de la santé pour l'antisepsie des mains » ou « Gel hydro-alcoolique pour l'antisepsie des mains - arrêté dérogatoire ». Certains de ces produits fabriqués avant la fin du mois de mai n'indiquaient pas encore la concentration d'alcool qu'ils contiennent, sans pour autant remettre en cause leur qualité !

À quel prix peut-on acheter des solutions ou des gels hydro-alcooliques ?

Pour garantir l'accessibilité de ces produits et éviter les rares mais inacceptables pratiques spéculatives identifiées début mars 2020, **le prix des gels et solutions hydro-alcooliques a été réglementé** jusqu'à la fin de l'état d'urgence sanitaire pour fixer un prix maximum en fonction du volume des contenants.

Les prix de vente au détail maximum **toutes taxes comprises (TTC) des gels et solutions hydroalcooliques** sont les suivants :

50 ml ou moins : 35,17 € /litre	> soit **un prix unitaire par flacon de 50 ml maximum de 1,76 €**
Plus de 50 ml à 100 ml inclus : 26,38 € /litre	> soit **un prix unitaire par flacon de 100 ml maximum de 2,64 €**
Plus de 100 ml à 300 ml inclus : 14,68 € /litre	> soit **un prix unitaire par flacon de 300 ml maximum de 4,40 €**
Plus de 300 ml :13,19 €/litre	> soit **un prix unitaire par flacon d'un litre maximum de 13,19 €**

Ces prix de vente maximaux sont applicables quel que soit le mode de distribution, y compris en cas de vente en ligne. Ils n'incluent pas les éventuels frais de livraison.

➔ **Important :** certaines pharmacies peuvent préparer des solutions hydro-alcooliques. Cela permet d'augmenter les quantités commercialisées mais coûte également plus cher à produire. Pour tenir compte de ces surcoûts de production, les prix de vente maximum mentionnés ci-dessus sont augmentés d'un facteur : de 1,5 pour les contenants de 300 ml ou moins et de 1,3 pour les contenants de plus de 300 ml.

Dans les cas de vente en vrac (c'est-à-dire lorsque le consommateur apporte son propre contenant), ces coefficients de majorations sont plus faibles : 1,2 pour les contenants de 300 ml ou moins et 1,1 pour les contenants de plus de 300 ml.

Où puis-je acheter un gel ou une solution hydro-alcoolique ?

La vente de ces produits n'étant pas réglementée, ils peuvent être commercialisés dans divers commerces (pharmacies, commerces alimentaire ou spécialisé…). Soyez toutefois vigilants sur la description des produits et lisez attentivement les étiquettes. Lorsque vous achetez en lien, assurez-vous de la fiabilité du site !

Quelles précautions d'utilisation pour les gels ou les solutions hydro-alcooliques ?

Les gels et solutions hydro-alcooliques sont des produits chimiques (on parle de produits *biocides*) contenant des substances actives destinées à détruire certains virus et certaines bactéries mais qui présentent également des dangers. En particulier, l'alcool est un produit facilement inflammable. Ces dangers et les précautions d'emploi à suivre pour les utiliser en toute sécurité doivent être indiqués sur l'étiquette. Prenez-en connaissance et suivez-les attentivement !

L'Anses **a communiqué** en avril 2020 que les centres antipoison signalent de nombreux accidents domestiques et intoxications en lien avec la COVID-19, liés notamment à une ingestion par de jeunes enfants de solutions ou gels hydro-alcooliques. Il est ainsi particulièrement important de tenir les gels et solutions hydro-alcooliques hors de portée des enfants.

Il convient d'être particulièrement vigilant lorsqu'il s'agit de produits déconditionnés (c'est-à-dire qui ne sont plus dans leur emballage d'origine) de mentionner très clairement la nature du contenu (nom du produit au feutre, étiquette de couleur…) et tenir ces produits hors de portée des enfants. Réutiliser des contenants alimentaires pour ces produits doit être proscrit pour éviter toute ingestion accidentelle.

MESSAGE DE PRÉVENTION :

1. **Soyez vigilants car tous les produits se présentant sous la forme d'un gel pour les mains n'ont pas nécessairement d'activité de désinfection garantie.**
2. **Certains contenant une teneur en alcool trop faible pour cela (à 60 %). Cela peut être le cas de certains produits dont la fonction est de nettoyer les mains, mais pas de les désinfecter.**
3. **En tout état de cause, n'hésitez pas à demander conseil à votre commerçant et à lui demander la confirmation que vous achetez un produit ayant une activité de désinfection.**
4. **Jusqu'à la fin de l'état d'urgence sanitaire, les prix sont réglementés, à titre d'exemple, un flacon de 300 mL ne peut être vendu au-delà de 4,40 € TTC.**

J'ai acheté un produit dont la composition et/ou le prix me semblent en contradiction avec la réglementation, que faire ?

En cas de doute sur un produit acheté, vous pouvez le signaler à la DGCCRF
https://www.economie.gouv.fr/dgccrf/contacter-dgccrf

ÉPARGNE / CRÉDITS
Attention aux offres frauduleuses

L'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Autorité des marchés financiers (AMF) constatent, depuis plusieurs années, une recrudescence des arnaques aux placements, crédits et assurances à la faveur d'un usage toujours plus grand d'internet, d'outils de communication mobiles toujours plus accessibles et d'un contexte de taux d'intérêt bas.

Comment reconnaître ces arnaques ?

➔ Attention aux sites internet ou aux personnes qui :

- Vous proposent un produit à des conditions financières beaucoup plus attractives que celles des établissements traditionnels ;
- Vous présentent un placement, à la fois très rentable et sans risque de perte en capital, permettant de gagner rapidement beaucoup d'argent ;
- Vous proposent d'obtenir un crédit, parfois en quelques minutes, à un taux fixe et bas, sans vérification de votre solvabilité ni recueil de garantie, quels que soient son montant et sa durée ;
- Insistent fortement pour que vous souscriviez sans délai ;
- Vous demandent vos coordonnées bancaires, des données personnelles ou le versement d'une somme d'argent ;
- Vous indiquent que le produit est garanti par l'ACPR ou la Banque de France ou prétendent être liés à une autorité publique (AMF, ACPR, Banque de France, Direction du Trésor, …) ;
- Vous informent que votre établissement actuel a changé de nom et que vous devez signer un nouveau contrat.

Comment s'en protéger ?

- Soyez vigilant face aux appels téléphoniques non sollicités et renseignez-vous sur votre interlocuteur ;
- **Méfiez-vous des promesses de gains rapides et sans contreparties : il n'y a pas de rendement élevé sans risque élevé ;**
- **Ne cédez pas à l'urgence ou aux pressions de votre interlocuteur, prenez le temps de la réflexion ;**
- Vérifiez systématiquement que la société est autorisée à proposer ses produits et services en France ;
- Consultez les **listes noires et tableau des alertes** publiés par les autorités sur les sites internet Assurance Banque Épargne Info Service (ABEIS) ainsi que l'Autorité des marchés financiers (AMF) et vérifiez que le site ou l'entité proposant le service financier n'y figure pas ;
- Ne faites pas de transfert d'argent vers des pays sans aucun rapport avec la société. En cas de doute, contactez votre établissement bancaire ;
- Ne communiquez aucun renseignement personnel (téléphone, mail, pièce d'identité, RIB, etc.) sur internet ou par courriel ;

➔ **Attention** aux publicités que vous voyez sur internet et particulièrement sur les réseaux sociaux. Les escrocs sont très actifs sur le web.

FOCUS SUR LES USURPATIONS D'IDENTITÉ DES PROFESSIONNELS AUTORISÉS

1. **Attention aux usurpations d'identité des acteurs autorisés !**
2. **Elles sont fréquentes, nombreuses et faciles à réaliser.**
3. **Pour en savoir plus, consultez la fiche 6 dédiée aux risques d'usurpation d'identité.**

Comment vérifier qu'un professionnel est autorisé à proposer ses produits et services en France ?

➔ Attention soyez vigilant, consultez :

- le registre **REGAFI** qui recense les établissements financiers agréés,
- les **listes des organismes d'assurance** agréés et bénéficiant d'un **passeport européen,**
- le site internet de **l'ORIAS,** organisme chargé de tenir le registre des intermédiaires financiers,
- la base **GECO** des organismes de placement collectif (OPC) et sociétés de gestion agréés,

➔ **Attention** les placements atypiques dans des biens concrets doivent impérativement être enregistrés par l'AMF, dans ce cas, consultez la **liste blanche** des offres enregistrées.

Que faire si vous êtes victime d'une telle arnaque ?

Si vous pensez être victime d'une offre frauduleuse et subissez un **préjudice**, déposez une plainte dans les meilleurs délais : https://www.pre-plainte-en-ligne.gouv.fr

Contactez INFO ESCROQUERIES en appelant le 0805 805 817 (service et appel gratuits du lundi au vendredi de 9h à 18h30). Effectuez un signalement sur le **portail officiel du Ministère de l'intérieur** même si vous n'avez pas subi de perte financière. Ce signalement peut être utile pour empêcher d'autres tentatives d'escroquerie.

Si vous avez été sollicité par un courriel, contactez la **plateforme Signal Spam** en vous inscrivant gratuitement.

Pour plus d'informations, consultez les sites **ABEIS** et de l'**AMF** ainsi que leurs chaînes YouTube (**ABEIS et AMF**)

FAUX ORDRES DE VIREMENTS
Escroquerie : professionnels

Depuis 2010, **plus de 3760 escroqueries aux faux ordres de virements internationaux** ont été commises à l'encontre de sociétés implantées en France et/ou de filiales domiciliées à l'étranger.

Le préjudice est d'environ **890 millions d'euros pour les faits commis** et plus de **1,8 milliard d'euros pour les faits tentés.**

Différentes techniques ont été identifiées (par ordre d'importance) :

- **le changement de Relevé d'Identité Bancaire :** de nouvelles coordonnées bancaires sont adressées par courrier électronique avec des caractéristiques de messagerie très proches de celles du fournisseur et/ou de l'interlocuteur habituel,
- **l'usage d'une fausse identité :** par usurpation de l'identité du dirigeant ou d'un responsable de la société ciblée ou d'une personnalité (de type faux président ou faux ministre),
- **via un lien frauduleux :** un lien contenant un logiciel espion invite à se connecter sur le portail de la banque gestionnaire des comptes et à composer les identifiants et codes d'accès. De faux ordres de virement sont alors établis, les mots de passe modifiés, privant les services comptables de toute vérification de leur trésorerie.

En cette période de crise, des groupes criminels organisés en profitent pour usurper l'identité de sociétés produisant et/ou distribuant du matériel de protection et/ou médical. Ils ciblent des établissements et les incitent à réaliser des commandes et des paiements sur des comptes bancaires français ou étrangers.

Les procédures habituelles de lutte contre les fraudes financières, et notamment celles relatives au changement de domiciliation bancaire, sont désorganisés.

De nombreuses escroqueries en lien avec la crise visent des pharmacies, des hôpitaux, des cliniques, des EHPAD et des fournisseurs de matériel de protection médicale.

MESSAGE DE PRÉVENTION :

1. **Méfiez-vous de toute proposition commerciale prétendument « urgente ».**
2. **Ne communiquez pas d'informations susceptibles de faciliter le travail des escrocs (noms des différents managers, chefs de division, moyens de règlement, listing fournisseurs…).**
3. **Sensibilisez l'ensemble du personnel et les partenaires** (exemples : affiches de sensibilisation, E-learning mis à disposition sur le site du Club des directeurs de sûreté et de sécurité des entreprises – CDSE https://www.cdse.edu/catalog/elearning/index.html)
4. **Réalisez une veille régulière sur les évolutions des escroqueries.**
5. **Prenez le temps de vérifier,** même dans l'urgence et sous la pression, **les demandes de virement.**
   Les contre-mesures les plus simples :
   - contre-appel avec le numéro habituel connu en interne et non celui fourni par l'escroc,
   - vérification auprès du site internet de la société si elle signale avoir été victime d'une escroquerie.
6. **Sécurisez les installations informatiques.**
7. **Veillez à la sécurité des accès aux services de banque à distance.**

Un établissement bancaire ne sollicite jamais les informations de connexion de ses clients.
Les mots de passe doivent être confidentiels, complexes et régulièrement renouvelés.

RECOMMANDATIONS, EN CAS D'ATTAQUE :

- → **prendre attache immédiatement avec votre banque** pour effectuer un rappel des fonds, la rapidité de la réaction est primordiale,
- → **contacter le service de police ou de gendarmerie** le plus proche en apportant un maximum d'éléments (entête de mails et contenus, numéros de téléphone, dates et heures des appels, éléments confidentiels communiqués aux fraudeurs...).

USURPATIONS D'IDENTITÉ

Les nouvelles technologies, l'opportunisme des escrocs, la dimension internationale des infractions, l'ingénierie de plus en plus sophistiquée, les propositions frauduleuses de crédits ou de produits d'épargne adaptées aux attentes du moment... sont autant de défis que les services en charge de la prévention et de la répression de la fraude doivent affronter en faisant preuve de réactivité.

L'usurpation d'identité est un moyen, de plus en plus répandu, de commettre une escroquerie. Il peut s'agir de l'usurpation de votre identité ou de celle d'un professionnel, en particulier ceux autorisés à commercialiser en France des produits financiers. Des institutions publiques ou des autorités de contrôle ainsi que leurs agents sont également visés.

Principes / Définitions :

L'usurpation de votre identité

L'usurpation d'identité est un délit[1] ! L'usurpation d'identité « **classique** » est basée sur la perte ou le vol d'une pièce d'identité (carte nationale d'identité, passeport, permis de conduire), d'un justificatif de domicile ou la simple photocopie de l'un de ces documents. L'escroc utilise vos données personnelles pour réaliser des actes en votre nom. L'usurpateur peut, par exemple, ouvrir des comptes bancaires en ligne, souscrire des crédits à la consommation, des assurances, etc.

L'usurpation d'identité la plus moderne, dite « **numérique** », est commise sur un réseau de communication en ligne, ce qui comprend notamment les courriers électroniques, les sites web, les messages publiés en ligne et les profils sur les réseaux sociaux. L'usurpation d'identité numérique est généralement commise de deux manières : par la technique du phishing (ou hameçonnage) ou par la création d'un faux site web ou d'un faux profil sur un service de réseau social.

En France, plus de 200.000 personnes seraient victimes d'usurpation d'identité en ligne chaque année. **De nombreux problèmes peuvent en découler :** le dépôt d'une plainte à votre encontre, la création de faux documents d'identité à votre nom, le détournement d'aides sociales, une interdiction bancaire, un fichage à la Banque de France, des poursuites engagées par un ou plusieurs créanciers, etc.

L'usurpation d'identité d'un professionnel

L'ACPR et l'AMF, les autorités de contrôle des secteurs bancaire, de l'assurance et des marchés financiers, ont constaté une forte recrudescence des usurpations d'identité de professionnels français agréés et aussi d'acteurs européens, parfois moins connus, autorisés à proposer leurs produits et services en France. Les escrocs reproduisent notamment sur des sites internet ou dans de faux contrats les nom, logo, adresse, numéro d'agrément ou d'autorisation de vrais organismes ou intermédiaires financiers pour rendre crédibles leurs offres frauduleuses de crédits, d'assurance ou d'instruments financiers et/ou collecter vos informations personnelles à des fins d'escroqueries.

L'usurpation d'identité d'institutions publiques ou d'autorités de contrôle

Pour tromper la confiance du public, les fraudeurs utilisent également les noms, logos et adresses postales d'institutions publiques ou d'autorités de contrôle. Ils peuvent recourir à des sites internet ou à des courriels frauduleux envoyés à partir d'adresses à l'apparence officielle mais qui renvoient, en réalité, vers des adresses n'appartenant pas aux autorités. Ces escroqueries visent à obtenir des victimes la communication d'informations personnelles (pièces d'identité, RIB, etc.), de fichiers clients ou le versement de fonds pour des motifs divers (taxes, frais, etc.).

[1] Le délit d'usurpation d'identité suppose qu'il soit fait usage de l'identité d'un tiers en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération (article 264-4-1 du code pénal)

MESSAGE DE PRÉVENTION :

1. **Soyez vigilant** lorsque vous recevez des appels téléphoniques ou des courriels visant à soutirer de l'information vous concernant.
2. **Ne jetez jamais** des documents comportant des données personnelles sans les avoir détruits au préalable.
3. **Ne fournissez aucune** photocopie de documents d'identité à des tiers qui ne sont pas de confiance.
4. **Renforcez votre sécurité numérique** en vous référant aux fiches idoines et au guide disponibles sur le site de cybermalveillance.gouv.fr ; utilisez des mots de passe complexes et ne les communiquez pas à des tiers ; activez les protections anti-phishing existant dans certains navigateurs web ; évitez de vous connecter sur des sites sensibles (sites de banques ou de vente en ligne), dans les lieux publics ou chez des tiers ; ne répondez jamais à des emails provenant de prétendus organismes de confiance vous demandant de communiquer vos mots de passe ou autres coordonnées personnelles confidentielles ; ne cliquez jamais sur les liens ni n'ouvrez les documents contenus dans ces messages (etc.).
5. **Assurez-vous que la personne qui vous propose un produit ou un service n'usurpe pas l'identité (numéro d'autorisation, dénomination, adresse, etc.) d'un professionnel autorisé** en effectuant, par exemple, un contre-appel au siège de ce dernier, à partir d'un numéro de téléphone que vous aurez trouvé par vos propres moyens, et/ou en comparant son adresse de messagerie électronique avec celle dudit professionnel. Consultez également le registre de l'autorité de contrôle du pays d'origine si la société a son siège social dans un pays européen. Pour en savoir plus, consultez la fiche : « Épargne / Crédits : Attention aux offres frauduleuses ».
6. **N'oubliez pas que les institutions publiques (DGCCRF, Banque de France, ...) ou les autorités de contrôle (ACPR, AMF...) ne sollicitent jamais** la communication d'informations personnelles, de fichiers clients ou le versement d'une quelconque somme d'argent, que ce soit par messagerie électronique ou par téléphone.

Je suis victime... Que faire ?

Si mon identité est usurpée ?

- **Prévenez dans les plus brefs délais** tous les établissements financiers (banques, assureurs, etc.) dont vous êtes client.
- **Contactez la Banque de France** afin de savoir si des incidents ont été déclarés au fichier central des chèques (FCC) ou au fichier des incidents de remboursement des crédits aux particuliers (FICP).
- **Consultez le fichier des comptes bancaires (FICOBA)** pour savoir si des comptes ont été ouverts à votre nom par l'escroc. Pour cela, écrivez, en joignant une copie de votre pièce d'identité, à la CNIL - 3 Place de Fontenoy - TSA 80715 - 75334 Paris cedex 07.

Et si vous avez versé des fonds à un escroc ?

- **Contactez immédiatement votre banque** pour bloquer le virement s'il n'est pas trop tard ou demander le retour des fonds versés (procédure dite de « recall »). Attention, le résultat n'est pas du tout garanti.
- **Cessez tout contact avec votre interlocuteur,** même si vous êtes relancé.

Dans tous ces cas

- **Collectez un maximum d'informations** sur l'usurpation d'identité et conservez tous éléments utiles (courriels, enregistrement, ordres de virements, etc.).
- **Déposez plainte** dès la constatation des faits auprès d'un service de Police ou de Gendarmerie ou par courrier auprès du Procureur de la République.

FAUX SITES ADMINISTRATIFS : **attention aux arnaques**

De nombreux sites proposent, moyennant rémunération, de faciliter l'accomplissement de certaines démarches administratives courantes (demandes de permis de conduire, de carte grise, d'extrait d'acte de naissance, extrait de casier judiciaire, attestation de déplacement, démarches COVID, par exemple) ou encore de vous renseigner sur la mise en œuvre de réglementations spécifiques (traitement automatisé de fichiers de données à caractère personnel, accessibilité des établissements recevant du public...).

Faut-il payer pour effectuer des démarches administratives ?

Certaines démarches administratives sont proposées gratuitement par l'administration française sur des sites officiels: elles permettent, par exemple, de consulter le nombre de points restant sur un permis de conduire, demander un extrait d'acte de naissance, demander une carte grise ou demander un extrait de casier judiciaire.

Rien n'interdit cependant à un professionnel de proposer ces prestations de services, en contrepartie d'un paiement, à condition de respecter des règles précises :

- Le caractère privé et commercial du service, l'identité du prestataire, comme le tarif des prestations doivent clairement apparaître d'emblée ;
- si le consommateur souhaite que l'exécution de la prestation de services proposée commence avant la fin du délai de rétractation de 14 jours, le professionnel doit recueillir sa demande expresse en ce sens ;
- dans cette hypothèse, le consommateur doit être informé qu'une fois la commande passée auprès de la société, il pourra se rétracter dans un délai de 14 jours en contrepartie d'un montant proportionnel à l'exécution de la prestation jusqu'à la communication au professionnel de sa décision de se rétracter, sauf s'il a expressément reconnu perdre son droit de rétractation si le service a été pleinement exécuté avant l'expiration de ce délai;
- le consommateur doit recevoir une confirmation de commande.

Les autorités de contrôle reçoivent de nombreuses réclamations de consommateurs visant de faux sites administratifs qui proposent d'effectuer, moyennant rémunération, certaines démarches administratives en lieu et place des demandeurs.

Ces sites n'hésitent pas à tromper le consommateur en prenant l'apparence de sites officiels : reproduction de la charte graphique du site de référence, usage des couleurs bleu-blanc-rouge du logo Marianne, référence à des ministères, référencement en tête des moteurs de recherche.

Certains sites vont plus loin que le simple paiement du service et peuvent conduire de façon opaque à un abonnement non souhaité.

Le point d'entrée privilégié pour les démarches administratives en ligne est le site officiel www.service-public.fr

MESSAGE DE PRÉVENTION :
Il est conseillé, avant d'entreprendre toute démarche administrative :

1. de vérifier la possibilité d'accomplir les démarches administratives auprès des sites officiels en consultant par exemple le site officiel de l'administration française, service-public.fr, avant de passer une commande et de fournir des données à caractère personnel, y compris ses coordonnées de carte bancaire,
2. de consulter les conseils du Centre européen des consommateurs pour vérifier le sérieux de la société qui propose le service (https://www.europe-consommateurs.eu/index.html),
3. de contacter, si le paiement a été effectué, le Centre européen des consommateurs, en particulier si le site est basé dans un autre pays de l'UE, en Islande ou en Norvège. À défaut, ne pas hésiter à prendre contact avec sa banque pour une éventuelle procédure de remboursement (encore appelée procédure de rétro-facturation ou de chargeback),
4. de consulter le site de la Commission nationale de l'informatique et des libertés afin de connaître vos droits en matière de protection des données à caractère personnel (https://www.cnil.fr/).

J'ai des doutes sur un site administratif ?

En cas de doute sérieux sur un site administratif, vous pouvez le signaler à la DGCCRF (https://www.economie.gouv.fr/dgccrf/contacter-dgccrf).

Vous êtes victime d'une escroquerie, vous pouvez initier une plainte sur internet : https://www.pre-plainte-en-ligne.gouv.fr/

HAMECONNAGE / PHISHING
Comment faire ?

L'hameçonnage (phishing en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc... Ces techniques d'attaque évoluent constamment. Les conseils suivants vous aideront à déterminer si un message est légitime ou non.

MESSAGE DE PRÉVENTION :

1. Attention aux expéditeurs inconnus : soyez particulièrement vigilants sur les courriels provenant d'une adresse électronique que vous ne connaissez pas ou qui ne fait pas partie de votre liste de contact.
2. Soyez attentif au niveau de langage du courriel : même si cela s'avère de moins en moins vrai, certains courriels malveillants ne sont pas correctement écrits. Si le message comporte des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées, c'est qu'il n'est pas l'œuvre d'un organisme crédible (banque, administration …).
3. Vérifiez les liens dans le courriel : avant de cliquer sur les éventuels liens, laissez votre souris dessus. Apparaît alors le lien complet. Assurez-vous que ce lien est cohérent et pointe vers un site légitime. Ne faites pas confiance aux noms de domaine du type impots.gouvv.fr, impots.gouvfr.biz, infocaf.org au lieu de www.caf.fr.
4. Méfiez-vous des demandes étranges : posez-vous la question de la légitimité des demandes éventuelles exprimées. Aucun organisme n'a le droit de vous demander votre code carte bleue, vos codes d'accès et mots de passe. Ne transmettez rien de confidentiel même sur demande d'une personne qui annonce faire partie de votre entourage.
5. L'adresse de messagerie source n'est pas un critère fiable : une adresse de messagerie provenant d'un ami, de votre entreprise, d'un collaborateur peut facilement être usurpée. Seule une investigation poussée permet de confirmer ou non la source d'un courrier électronique. Si ce message semble provenir d'un ami - par exemple pour récupérer l'accès à son compte - contactez-le sur un autre canal pour vous assurer qu'il s'agit bien de lui !

Source : plateforme Cybermalveillance.gouv.fr

Je suis victime, que faire ? Comment signaler les tentatives d'escroquerie sur internet ?

Comment s'en prémunir ? Utilisez un logiciel bloqueur de publicités, de filtre anti-pourriel, ou activer l'option d'avertissement contre le filoutage présent sur la plupart des navigateurs. Installez un anti-virus et mettez-le à jour. Désactivez le volet de prévisualisation des messages. Lisez vos messages en mode de texte brut.

Comment réagir ? Si vous avez un doute sur un message reçu, il y a de fortes chances que celui-ci ne soit pas légitime : N'ouvrez surtout pas les pièces jointes et ne répondez-pas. Supprimez le message puis videz la corbeille.

S'il s'agit de votre compte de messagerie professionnel : transférez-le au service informatique et au responsable de la sécurité des systèmes d'information de votre entreprise pour vérification. Attendez leur réponse avant de supprimer le courrier électronique.

Si vous voyez une fenêtre POP-UP, ne cliquez jamais sur l'annonce, même si le bouton de fermeture est énorme. Utilisez toujours la croix (X) dans le coin. Si l'escroquerie que vous souhaitez signaler vous est parvenue par un spam (pourriel), rendez-vous sur www.signal-spam.fr.

Signalez les escroqueries auprès du site www.internet-signalement.gouv.fr, la plateforme d'harmonisation, d'analyse de recoupement et d'orientation des signalements. Pour s'informer sur les escroqueries ou pour signaler un site internet ou un courriel d'escroqueries, un vol de coordonnées bancaires ou une tentative d'hameçonnage : contacter Info Escroqueries au 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile) - Du lundi au vendredi de 9h à 18h

Rendez-vous sur cybermalveillance.gouv.fr, la plateforme nationale d'assistance aux victimes d'actes de cybermalveillance. Que vous soyez un particulier, une entreprise ou une administration, retrouvez :
- des conseils / vidéos pour sensibiliser votre entourage professionnel ou personnel,
- des services de proximité en cas de dommages causés par une attaque informatique.

APPELS FRAUDULEUX AUX DONS
Fausses cagnottes - Vigilance !

Dans le contexte de l'épidémie COVID 19, le risque d'escroquerie généré par des appels frauduleux aux dons s'est accentué. Que vous soyez acteur du financement participatif ou consommateur voulant contribuer à des actions de solidarité, soyez vigilant.

Ces escroqueries peuvent prendre différentes formes.

- Des appels aux dons ou des cagnottes solidaires à destination du public peuvent être organisés par des entités ou des sites internet **non autorisés** à exercer cette activité en France.
- Des escrocs peuvent également tenter de recourir à des **cagnottes mensongères**, dont ils demandent la mise en ligne sur des sites de financement participatif de dons dûment enregistrés, pour tromper le public et détourner les sommes collectées.

Les intermédiaires en financement participatif proposant des cagnottes en ligne ont été invités par l'Autorité de contrôle prudentiel et de résolution (ACPR) et la Direction générale de la concurrence, de la consommation et de la Répression des Fraudes (DGCCRF) à :

- faire preuve de vigilance face au risque d'être utilisés par des escrocs pour relayer des appels frauduleux aux dons,
- s'assurer du respect des obligations de sélection des cagnottes et de la qualité de l'information fournie aux potentiels donateurs sur les projets et les porteurs de projets. Ces informations doivent notamment porter sur les conditions d'éligibilité, les critères d'analyse et de sélection des projets et des porteurs de projets.

➔ **Si vous souhaitez réaliser un don via une cagnotte en ligne,** prenez les précautions nécessaires pour vous protéger des escroqueries.

MESSAGE DE PRÉVENTION :

1. **Obtenez des informations nécessaires sur l'entité qui vous propose ce service (dénomination sociale, pays d'établissement, adresse du siège social, numéro d'immatriculation, site internet…) et vérifiez systématiquement qu'elle est autorisée en consultant le site internet de l'ORIAS (www.orias.fr), registre des intermédiaires du secteur financier.**
2. **Vérifiez que la participation au financement du projet vous est proposée depuis le site internet d'une plateforme dédiée, régulièrement autorisée à exercer son activité, et sur laquelle vous vous êtes inscrit au préalable. Si vous avez été démarché par des opérateurs vous invitant à procéder directement par le biais d'un virement sur un compte bancaire au financement d'un projet, il s'agit sans doute d'une pratique frauduleuse. La réglementation applicable encadre strictement les possibilités de démarchage pour ces opérateurs.**
3. **Consultez la liste noire publiée par l'ACPR sur le site internet Assurance Banque Épargne Info Service – ABEIS (www.abe-infoservice.fr) et vérifiez que le site ou l'entité n'y figure pas.**
4. **Assurez-vous de disposer d'informations suffisantes sur le projet et le porteur de projet. Un contrat-type doit être mis à votre disposition, ainsi que l'adresse et le numéro de téléphone du service de réclamation. En cas de doute ou en l'absence d'informations précises, n'effectuez aucun don.**

J'ai des doutes sur une cagnotte en ligne ?

En cas de doute sur une cagnotte en ligne, vous pouvez le signaler à la DGCCRF (https://www.economie.gouv.fr/dgccrf/contacter-dgccrf) ou à l'ACPR (https://www.abe-infoservice.fr/vos-demarches/nous-contacter#1).

Vous êtes victime d'une escroquerie, déposez une **plainte en ligne.**

FRAUDES AUX FAUSSES RÉPARATIONS
Informatiques ou « faux supports techniques »

Le mode opératoire

Les victimes à l'occasion d'une navigation sur internet sont inopinément interrompues par **un message de sécurité anxiogène** ayant les apparences d'une fenêtre d'alerte légitime du système d'exploitation. Ce message est fréquemment généré par le navigateur internet.

Cette alerte peut faire état de la présence d'un maliciel ou de tout autre forme de problème technique a priori en dehors du champ de compétence de l'utilisateur moyen. **Cette alerte incite la victime à contacter un service de support technique afin de remédier à la difficulté fictive avec l'aide d'un téléopérateur.** Le message comporte généralement une contrainte temporelle indiquant qu'à l'expiration d'un délai de quelques minutes l'appareil compromis sera rendu inutilisable à moins de contacter le service indiqué.

MESSAGE DE PRÉVENTION :

1. **Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine, en particulier vos navigateurs.**
2. **Tenez à jour votre antivirus et activez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications et services légitimes.**
3. **Évitez les sites non sûrs ou illicites, tels ceux qui hébergent des contrefaçons (musique, films, logiciels…) ou certains sites pornographiques qui peuvent infecter votre machine ou héberger des régies publicitaires douteuses.**
4. **N'installez pas d'application ou de programme « piratés », ou dont l'origine ou la réputation sont douteuses.**
5. **N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.**
6. **N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez pas sur les liens provenant de chaînes de messages, d'expéditeurs inconnus, ou d'un expéditeur connu mais dont la structure du message est inhabituelle ou vide.**
7. **Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine.**
8. **Aucun support technique officiel ne vous contactera jamais pour vous réclamer de l'argent.**

Source : plateforme Cybermalveillance.gouv.fr

Je suis victime, que faire ?

- **Ne répondez pas aux sollicitations** et n'appelez jamais le numéro indiqué.
- **Conservez toutes les preuves**. Photographiez votre écran au besoin.
- S'il semble « bloqué », **redémarrez votre appareil**. Cela peut suffire à régler le problème.
- Si votre navigateur reste incontrôlable, **purger le cache, supprimez les cookies, réinitialiser les paramètres par défaut** et si cela ne suffit pas, supprimez et recréez votre profil.
- **Désinstallez toute nouvelle application suspecte** présente sur votre appareil.
- **Faites une analyse antivirus** approfondie de votre machine.
- Si un faux technicien a pris le contrôle de votre machine, **désinstallez le programme de gestion à distance, et changez tous vos mots de passe**. En cas de doute ou si vous n'arrivez pas à reprendre le contrôle de votre équipement par vous-même, vous pouvez faire appel à un prestataire référencé sur www.cybermalveillance.gouv.fr.
- Si vous avez fourni vos coordonnées bancaires ou n° de carte de crédit, **faites opposition** sans délai. Si un paiement est débité sur votre compte, **exigez le remboursement** en indiquant que vous déposez plainte.
- Si vous avez été contacté par un faux support technique, **signalez les faits au ministère de l'intérieur** sur sa plateforme Internet-signalement.gouv.fr.
- **Déposez plainte** au commissariat de police ou à la brigade de gendarmerie ou en écrivant au procureur de la République dont vous dépendez. Faites-vous, au besoin, assister par un avocat spécialisé.

VOL DE COORDONNÉES BANCAIRES : **que faire ?**

En consultant votre compte bancaire, vous découvrez des opérations réalisées à votre insu avec les références de votre carte bancaire que vous avez toujours en votre possession.

MESSAGE DE PRÉVENTION :

1 **Sur interne :**

Réaliser les achats uniquement sur des sites de confiance signalés par le logo « cadenas » et dont l'adresse commence par « https » au moment de la transaction.

Ne pas enregistrer son numéro de carte bancaire sur le site commerçant, ni sur l'ordinateur.

Éviter le piratage de sa carte bancaire en protégeant son ordinateur avec un antivirus et un pare-feu.

Favoriser les paiements avec un numéro de carte bancaire unique.

2 **Au distributeur automatique de billets ou lors d'un paiement avec un distributeur :**

Toujours cacher avec sa main le pavé numérique.

Ne pas se laisser distraire par des inconnus qui vous proposent leur aide.

3 **Dans un magasin ou au restaurant :**

Ne jamais quitter sa carte bancaire des yeux.

Ne jamais confier sa carte bancaire à un inconnu.

Ne pas conserver son code secret au même endroit que sa carte. Apprendre plutôt son code secret par cœur.

Je suis victime, que faire ?

Informations, conseils, assistance par du personnel de la police nationale et la gendarmerie nationale, contacter INFO ESCROQUERIES au 0811 02 02 17 (prix d'un appel local depuis un poste fixe, ajouter 0,06€/minute depuis un téléphone mobile), du lundi au vendredi de 9h à 18h.

RANÇONGICIELS (RANSOMWARES) **Des logiciels malveillants qui peuvent s'infiltrer dans vos ordinateurs**

Qu'est-ce qu'un rançongiciel ou ransomware ? Précision sur le mode opératoire

Un ransomware, ou rançongiciel, est un **logiciel** malveillant, **prenant en otage les données**. Il infecte les ordinateurs, chiffre les fichiers contenus dans le système infecté et **demande une rançon** (en cryptomonnaie) en échange d'une clé ou d'un mot de passe permettant de les déchiffrer.

MESSAGE DE PRÉVENTION :

1 **Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.**

2 **Tenez à jour l'antivirus et configurez votre pare-feu. Vérifiez qu'il ne laisse passer que des applications, services et machines légitimes.**

3 **N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez par sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide.**

4 **N'installez pas d'application ou de programme « piratés » ou dont l'origine ou la réputation sont douteuses.**

5 **Évitez les sites non sûrs ou illicites tels ceux hébergeant des contrefaçons (musique, films, logiciels…) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.**

6 **Faites des sauvegardes régulières de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.**

7 **N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.**

8 **Utilisez des mots de passe suffisamment complexes et changez-les régulièrement, mais vérifiez également que ceux créés par défaut soient effacés s'ils ne sont pas tout de suite changés (notre fiche dédiée aux mots de passe sur www.cybermalveillance.gouv.fr).**

9 **Éteignez votre machine lorsque vous ne vous en servez pas.**

Source : plateforme Cybermalveillance.gouv.fr

Je suis victime de rançongiciels (ransomwares), que faire ?

- **Débranchez la machine d'internet** ou du réseau Informatique.
- **Isolez** les supports touchés par le Ransomware.
- **En entreprise, alertez immédiatement** votre service informatique.
- **Ne payez pas la rançon**, vous alimenteriez le système mafieux, sans certitude de récupérer les données.
- **Déposez plainte** auprès de la police ou de la gendarmerie ou en écrivant au procureur de la République dont vous dépendez.
- **Se rapprochez** de sa société fournisseur d'anti-virus ou prestataire de service.
  A défaut vous trouverez de l'**aide sur le site** cybermalveillance.gouv.fr
- Vous pouvez trouver quelques **clés et outils de déchiffrement sur le site :** nomoreransom.org/fr/index.4html**.**

MARKETING DE RÉSEAU (MLM) :
Méfiez-vous des promesses d'enrichissement facile !

Dans le cadre de la crise sanitaire actuelle et grâce au développement des réseaux sociaux, le marketing de réseau (ou MLM – « *Multi Level Marketing* ») connaît un nouvel essor et peut être perçu comme une opportunité de gains rapides, faciles et importants. L'activité de distributeur pour un réseau de MLM ne nécessite pas de qualification professionnelle particulière ou d'infrastructure, et pas ou peu de démarches administratives préalables. Il suffit en général d'être parrainé par un membre du réseau pour l'intégrer.

Il faut néanmoins distinguer :

– la vente multi-niveaux qui est un modèle de vente directe légal en France.

Les vendeurs/distributeurs/représentants sont rémunérés sur leurs ventes personnellement réalisées, et perçoivent également une commission sur celles réalisées par les vendeurs qu'ils ont directement recrutés. Leur rémunération est issue de la vente des produits ou services de la marque à laquelle ils sont affiliés.

– les réseaux de vente à la boule de neige, de vente pyramidale ou schémas de Ponzi, dans lesquels la rémunération des recruteurs résulte principalement de l'affiliation au réseau de nouveaux membres, et non de la vente de produits ou services. Les pratiques commerciales mises en œuvre par ce type de réseaux sont, elles, interdites en France.

Comment détecter un schéma MLM frauduleux ?

Dans ces systèmes de vente prohibés, les adhérents du réseau ont pour principale activité de recruter de nouveaux membres, dans leur entourage direct, ou leurs abonnés sur les réseaux sociaux. L'adhésion implique le paiement de frais d'entrée et/ou d'un abonnement périodique.

Le recrutement de nouveaux affiliés génère les principaux gains financiers, pour l'adhérent, mais aussi pour ses parrains et tous les membres placés au-dessus du recruteur dans la généalogie du réseau. Les gains générés par la vente des produits ou services aux affiliés sont moindres et servent uniquement de « vitrine légale ». **L'intérêt principal pour les distributeurs n'est donc pas la vente de services mais la perspective de gains financiers importants résultant de la seule progression du nombre d'affiliés.**

Ces réseaux reposent essentiellement sur des pratiques commerciales prohibées (article L. 121-15 du code de la consommation), qui peuvent également constituer une escroquerie.

De nombreux opérateurs, dont les maisons-mères sont souvent implantées à l'étranger (USA notamment) exercent en France une activité qui se situe à la frontière entre vente multi-niveaux légale et réseau de vente illicite.

Dans ces systèmes de vente, les recrues sont incitées à adhérer par la promesse :

- d'offres exceptionnelles (prix promotionnels) sur des voyages, des produits de beauté, des compléments alimentaires, etc.
- de services permettant des gains ou des rendements très supérieurs aux taux du marché sur des produits et placements financiers (formation au trading en ligne, actions, cryptomonnaies, parts dans une société financière, dans un fonds d'investissement, etc...).
- des bonus importants en fonction du niveau atteint dans la hiérarchie (montres, voitures de luxe, voyages, pierres précieuses, etc.).

Le recrutement s'opère selon les mécanismes suivants :

- une forme d'endoctrinement et une certaine pression psychologique (relance régulière du « parrain » pour inciter ses filleuls à recruter à leur tour) ;
- l'emploi de formules accrocheuses du type : « *devenir riche en travaillant depuis son domicile* », « *opportunité financière* », « *investir pour gagner* », « indépendance financière », liées à un discours d'appartenance à un cercle fermé d'initiés…
- l'utilisation de chaînes dédiées ou de vidéos de présentation sur Internet, souvent d'accès restreint via un code fourni par le « parrain » ;
- de réunions sur invitation souvent payantes, dans lesquelles sont mises en avant les perspectives d'enrichissement facile ;
- des « statuts » et niveaux de rémunération aux noms prestigieux tels que « leader », « *gold* », « *platinium* », « Legend » ;
- la mise en avant sur les réseaux sociaux du train de vie des membres les mieux placés dans la hiérarchie.

Ces réseaux à structure pyramidale ont vocation à s'effondrer dès lors que les adhésions ne sont plus assez nombreuses pour répartir les gains issus du recrutement au bénéfice des anciens inscrits. Souvent, les têtes de réseau, seules gagnantes, finissent par sortir du réseau et en créent un nouveau pour « réinitialiser » le système.

MESSAGE DE PRÉVENTION :

1. **Attention, ce sont souvent des proches ou des connaissances qui vous invitent à intégrer un système de vente illicite, ignorant eux-mêmes qu'ils en sont victimes. Soyez vigilant aux discours récurrents, voire obsessionnels tenus, parfois proches de la dérive sectaire.**

   cf. Communiqué : https://www.amf-france.org/fr/actualites-publications/communiques/communiques-de-lamf/lautorite-des-marches-financiers-met-en-garde-le-public-lencontre-de-la-societe-kuvera-llckuvera, repris par la Miviludes : https://www.derives-sectes.gouv.fr/missions/actualites/communiqué-de-presse-de-lautorité-des-marché-financiers

2. **la pression, n'effectuez aucun paiement ;**
3. **Posez-vous des questions sur le produit proposé et sur la légalité de l'offre ;**
4. **Réalisez des recherches sur l'offre sur Internet et demandez des conseils objectifs à un professionnel**

   Ne répondez pas ou ne signez aucun document sous

Je suis victime... Que faire ?

Collectez un maximum d'information sur la pratique et son mode opératoire (copies écran du site internet, enregistrement audio/vidéo des séances, échanges de mails, numéros de téléphones, compte bancaire bénéficiaire des fonds, etc.).

Déposez plainte, dès la constatation des faits, auprès d'un service de Police ou de Gendarmerie, ou par courrier auprès du Procureur de la République ou contactez la DGCCRF (https://www.economie.gouv.fr/dgccrf/contacter-dgccrf)

Réalisation graphique Direction Générale de la Police nationale