

PLACEMENTS FRAUDULEUX COMMENT DÉTECTER UNE ARNAQUE

En 2026, investir est devenu un parcours du combattant. À la complexité du choix du bon placement s'ajoute désormais un volet que nul candidat à faire fructifier son patrimoine ne peut ignorer : les escroqueries financières.

Le phénomène est massif et le chiffrer reste toujours un exercice approximatif. Le parquet de Paris évalue à au moins 500 millions d'euros le montant annuel des préjudices liés aux escroqueries financières. Un chiffre stable depuis 2021, mais probablement sous-estimé au regard de la hausse continue des signalements.

Un rapport de l'ACPR (Autorité de contrôle prudentiel et de résolution), publié en juillet 2025, apporte un éclairage complémentaire : en 2023, les banques ont identifié et fermé plus de 70.000 comptes utilisés pour faire transiter l'argent des victimes avant de le dissimuler

à l'étranger (communément appelés «comptes rebonds»). Ces comptes auraient vu passer près d'un milliard d'euros, soit près du double de l'estimation du parquet de Paris. Ces deux chiffres illustrent la difficulté d'avoir des montants fiables. Cela réside, notamment, dans le fait que les victimes ne se signalent pas systématiquement et ne portent pas toujours plainte.

Pour lutter contre ce phénomène, les autorités se basent sur une stratégie en trois points : détecter, prévenir, sanctionner. Nous voyons donc que la prévention est un axe prioritaire qui précède la réponse pénale. Et c'est heureux, car l'évolution technologique, les nombreuses fuites

de données et le dynamisme des réseaux d'escroquerie font que les épargnants sont de plus en plus pris pour cibles. Il est alors indispensable d'être correctement informé pour savoir identifier un interlocuteur frauduleux et mettre en échec les tentatives d'arnaque.

L'ESCROC SURFE SUR L'ACTUALITÉ

Les arnaques reposent sur deux piliers : les produits à la mode et les produits familiers. Elles jouent la carte du déjà-vu et vont généralement demeurer dans les sentiers battus. Les escrocs sont avant tout des opportunistes qui surfent sur l'actualité : l'envolée du bitcoin a déclenché ►



une vague d'arnaques aux cryptoactifs, la période de taux bas a relancé les faux livrets d'épargne, l'engouement pour l'Intelligence artificielle (IA) alimente aujourd'hui les arnaques aux robots de trading. Plus un sujet est po-

“

Les escrocs utilisent souvent des sociétés basées dans des pays étrangers, afin de rendre les vérifications plus difficiles.

pulaire, plus il sera utilisé comme appât. L'escroc ne crée pas la tendance, il l'exploite. L'intérêt pour les arnaqueurs

est de capitaliser sur la communication faite par d'autres, de la parasiter pourrait-on dire. C'est en s'appuyant sur de nombreux articles, émissions et sur la communication d'entreprises légitimes qu'ils peuvent faire croire à la réalité de leur offre. Pas de montage aberrant, pas de produit incroyablement exotique, du banal, du normal, mais du normal plus performant. Car pour les escrocs, l'enjeu est de réussir un acte de vente avant tout. Et pour vendre, cela est plus facile lorsque le produit est meilleur. Ils vont simplement mentir pour lui attribuer les qualités souhaitées.

LES BONS RÉFLEXES À ADOPTER

Pour chaque type de « produit » va se jouer une partition différente, en ciblant tous les profils. Pour chaque arnaque,

il y a des réflexes de base à adopter pour les détecter.

La première règle est de contrôler la légitimité de la société par laquelle vous êtes contacté en s'assurant de son existence et des adresses affichées. Il faut commencer par vérifier leur présence éventuelle sur la liste noire de l'AMF (Autorité des marchés financiers).

Mais aussi sur les listes noires de nos voisins :

- la FSMA (Financial Services and Markets Authority), en Belgique ;
- la Finma (Swiss Financial Market Supervisory Authority), en Suisse.

La présence sur liste blanche, avec les enregistrements sur :

- le Regafi (Registre des agents financiers) ;
- l'Orias (Registre unique des intermédiaires en assurance, banque et finance).

Cette première étape est

indispensable mais, hélas, est loin d'être suffisante.

La seconde règle est de connaître le produit dans lequel vous souhaitez investir. C'est en comprenant son fonctionnement qu'il est possible de détecter une offre qui sonne faux.

LES PIÈGES TYPES

Chacun de ces produits, lorsqu'il est utilisé à des fins d'escroquerie, présente des caractéristiques typiques. Passons-les en revue, du plus courant au plus technique.

Les arnaques bancaires classiques

Pour les plus prudents, les escrocs misent sur les faux livrets d'épargne et les faux crédits, conçus pour imiter au plus près les pratiques bancaires officielles. Les rendements proposés ne sont

pas élevés afin de paraître crédibles, mais quelques recherches simples suffisent à faire apparaître des incohérences : société introuvable dans les registres officiels, adresse fantaisiste, conseillers qui disparaissent dès que l'argent est versé.

Ces valeurs refuges qui n'en sont pas

Au rayon des classiques, nous retrouvons les offres dans les actifs réels tels que l'or, d'autres métaux précieux, le vin, ou encore les terres rares.

Ici, le ressort psychologique est double : la « garantie » du concret dont la valeur ne pourra raisonnablement jamais descendre à zéro et la rareté du produit. Sur de telles arnaques, les signaux d'alerte sont les rendements déconnectés de la réalité du marché et une société incapable de justifier qu'elle détient effectivement les actifs proposés.

Des projets qui n'existent que sur le papier

Certaines escroqueries ne reposent sur rien de tangible, juste une histoire bien racontée. Les fausses offres de financement participatif (*crowdfunding*) font appel à un ressort émotionnel : le sentiment d'appartenance à une communauté. Vous êtes invité à la rejoindre autour d'un narratif totalement faux.

Ce type d'arnaque est plus subtil à déjouer, car il joue sur l'engagement : le projet devient un coup de cœur, et c'est là le point faible. Il faut creuser autour de la réalité de ce programme pour découvrir bien souvent qu'il n'existe que sur une plaquette PDF plus que douteuse.

Les mirages du trading

Changement d'univers avec des produits financiers plus techniques : dérivés, Forex (Foreign Exchange Market) et CFD (*Contract for Difference*).

500

millions d'euros

C'est l'estimation annuelle du préjudice global subi par les victimes d'escroqueries financières en France en 2025 (parquet de Paris).

3,2 %

Telle est la proportion de Français qui seraient victimes d'arnaques à l'investissement financier en 2024 (contre 1,2 % en 2021).

69.000 €

Soit le montant moyen du préjudice par victime pour les faux livrets d'épargne.

1.190

C'est, en 2025, le nombre d'inscriptions par l'ACPR (Autorité de contrôle prudentiel et de résolution) sur la liste noire des sites ou entités proposant des services financiers sans y être autorisés.

Sources : ACPR, AMF, Banque de France.

Ici, les escrocs jouent la carte de la *gamification* et du levier, présentés comme des outils de gain rapide sur de fausses plateformes de *trading*. Ils s'accompagnent de conditions de volume irréalistes et de bonus extravagants. Sur ce type d'offre, ce sont les rendements mirifiques qui doivent être le signal d'alerte. Un rendement outrageusement supérieur aux pratiques courantes cache toujours le pire.

La garantie, argument favori de l'escroc

Plus sophistiqués encore : les faux produits structurés.

OPCVM (organismes de placement collectif en valeurs mobilières), ETF (*Exchange Traded Funds*) vont jouer sur la complexité et la difficulté de l'investisseur particulier à évaluer des faux justificatifs, en promettant des rendements « garantis ». Mais à trop promettre, les incohérences finissent par apparaître. Il faut demander le DIC (document d'information clé) et prendre le temps de l'étudier, en étant attentif aux incohérences entre les éléments fournis.

Les cryptoactifs : le nouvel eldorado

Ils constituent aujourd'hui le terrain le plus fertile pour les escroqueries financières, en raison de leur complexité et d'une régulation récente.

- Premier subterfuge : les faux *exchanges*. Un *exchange* est une plateforme permettant d'acheter, de vendre ou d'échanger des cryptoactifs. Les escrocs en créent de fausses en usurpant l'identité d'acteurs légitimes. Pour attirer les investisseurs, ils promettent des gains rapides, grâce à des robots de *trading* prétendument entraînés par l'Intelligence artificielle. L'argument est efficace : qui refuserait de laisser un algorithme gagner de l'argent à sa place ? En réalité, la plateforme est une coquille vide. Les gains affichés sont fictifs, conçus uniquement pour inciter à investir davantage. Le signal d'alerte : aucun *exchange* sérieux ne garantit des rendements, et encore moins via un robot.
- Deuxième subterfuge : les faux *tokens* (jetons). L'escroc crée un jeton numérique, imitant un cryptoactif bien réel en reproduisant ses caractéristiques, puis l'envoie sur un portefeuille numérique (*wallet*) appartenant à l'in-

vestisseur. Tout semble authentique : le jeton apparaît bien dans le portefeuille avec une valeur affichée. Mais en réalité, ce faux *token* n'a qu'une valeur fictive et n'est pas négociable, donc impossible à revendre. L'argent est perdu.

- Troisième subterfuge, et sans doute le plus cynique : faire croire à l'investisseur que ses jetons sont bloqués et qu'il doit payer pour les débloquent. Les escrocs n'hésitent pas à usurper l'identité d'institutions bien réelles comme la Securities and Exchange Commission (l'équivalent de l'AMF aux États-Unis) ou la BCE (Banque centrale européenne). Une autre variante est d'avancer le paiement d'impôts qui devraient en réalité être prélevés à la source.

Si vous entendez les mots « fonds bloqués » ou « robot », soyez en alerte maximale ! Pour autant, ces vérifications qui doivent être la base ne sont pas suffisantes pour déjouer toutes les tentatives.

QUATRE CANAUX D'APPROCHE

Quel que soit le produit proposé, les escrocs vont utiliser quatre canaux pour approcher leurs victimes.

- Le premier canal est la société non régulée pure : une invention complète. La société n'existe pas, les autorisations sont fantaisistes et les produits purement fictifs. Une vérification sur les registres officiels comme Regafi, Orias ou leurs équivalents européens suffit généralement à déjouer l'escroquerie. Mais attention, les escrocs utilisent souvent des sociétés basées dans des pays étrangers pour rendre les vérifications plus difficiles : barrière de la langue ou difficulté à accéder aux informations de vérification. ►

Dans le doute, il est toujours préférable de s'abstenir.

- Le deuxième canal, simple mais redoutable: l'usurpation. Le clone. La vérification de la société et de ses autorisations ne montrera pas d'anomalie. Le site internet est parfait, et pour cause c'est un vrai. Le hic, ce sont les interlocuteurs qui ne sont pas du tout ceux qu'ils prétendent être. Méfiez-vous des canaux de communications atypiques et non professionnels comme WhatsApp ou Telegram. Vérifiez les adresses mail et les noms de domaines associés. Rappelez systématiquement le numéro officiel de la société pour confirmer l'identité de votre interlocuteur. Si un inconnu répond ou si vous constatez une différence, c'est un numéro usurpé.
- Le troisième canal: l'usurpation d'une autorité. AMF, Banque de France, institution européenne, Interpol, Eurojust (Unité de coopération judiciaire de

l'Union européenne)... Ce cas est facile à déjouer. Si vous n'avez pas vous-même sollicité ces organismes, ils ne vous contacteront jamais spontanément. La seule autorité qui puisse vous solliciter sans démarche préalable de votre part est un tribunal qui vous envoie un courrier «Avis à victime», ou une demande de la police ou de la gendarmerie de votre lieu de domicile. Tout autre contact se réclamant d'une institution officielle doit être considéré comme une tentative d'escroquerie.

- Enfin, le dernier canal d'approche: le relais. Un intermédiaire (influenceur, sponsor, publicité ou faux article de presse) se charge de promouvoir l'offre frauduleuse à la place de l'escroc. En instaurant une distance apparente avec le produit, il rend les vérifications plus difficiles et ajoute une couche de confusion. Méfiez-vous des recommandations non sol-

“

Commencer à se poser les bonnes questions, même sans avoir toutes les connaissances, permet souvent de se replier.

licitées, aussi séduisantes soient-elles: même un visage connu ne garantit pas la légitimité d'une offre.

LA TECHNIQUE ULTIME ANTI-ARNAQUE

Ces vérifications sont indispensables, simples et accessibles à tous. Pourtant, il y a de nouvelles victimes tous les jours. Il faut se rendre à l'évidence, cela ne fonctionne pas. Alors, où est le problème?

La réalité, c'est que même si nous savons qu'il faut le faire, nous ne vérifions pas. Commencer à vérifier et à se poser les bonnes questions, même en n'ayant pas toutes

les connaissances ou les compétences, permet souvent de tout arrêter avant qu'il ne soit trop tard. L'important est de se poser les bonnes questions au bon moment. Or, la plupart des victimes ont été entraînées par un tour de passe-passe à ne pas s'interroger. La raison principale vient des techniques utilisées qui reposent sur de la manipulation psychologique et l'ingénierie sociale.

Pour y résister, il existe une méthode simple: la méthode «RAD», pour «Ralentir, Authentifier, Documenter». Prendre le temps de vérifier ce que vous explique votre interlocuteur. Il est important de constituer un dossier en consignait les informations qui pourraient être utiles plus tard.

La pression temporelle doit être le signal d'alerte le plus fort. Il n'est pas possible de prendre une décision sereine dans la panique. C'est un moyen simple mais efficace pour les escrocs de manipuler leurs victimes: «la dernière offre», «le dernier créneau»,



Maître Anne Bernard-Dussaulx

Avocate. Défend les victimes d'escroqueries depuis de nombreuses années.

« Une promesse de rendement mirifique doit alerter »

Est-il facile de détecter un faux courtier en investissement ?

Non, ce n'est pas si évident, surtout pour un particulier. L'escroquerie aux investissements est une véritable industrie et les faux conseillers sont très bien formés: ils connaissent parfaitement le vocabulaire financier, les placements en vogue, l'actualité et utilisent tous les ressorts de la manipulation psychologique. Ils communiquent beaucoup par téléphone, ce qui ne les expose pas beaucoup, contrairement aux échanges par mail.

Malgré tout, quels sont les éléments qui peuvent alerter dans le discours des faux conseillers ?

D'abord, une promesse de rendement élevée. Ensuite, un empressement certain à vous faire investir au prétexte d'un «coup à faire», d'une offre éphémère, du désistement d'un autre investisseur qui offrirait une belle opportunité, etc. Et enfin, l'instauration d'une relation prétendument amicale pour convaincre l'investisseur qu'il bénéficie d'un traitement particulier (tutoiement, loisirs et

goûts communs, parcours de vie similaire, naissance d'un enfant fictif, envoi de cadeaux ou de bouquets de fleurs, etc.)

Faut-il dès lors privilégier la communication écrite ?

C'est préférable car la manipulation est plus difficile à l'écrit. Mais cela ne suffit pas toujours. Il faut toujours demander à signer un contrat. On peut alors plus facilement comprendre qu'il s'agit d'un contrat fictif: fautes d'orthographe, réglementation visée erronée, tribunaux compétents pour statuer sur un litige situé à l'étranger.

Quel conseil général donneriez-vous ?

Le premier conseil est de renoncer au moindre doute. Bien souvent, les victimes qui me consultent m'avouent avoir eu un doute et s'être malgré tout laissé convaincre par les explications du conseiller. Le second conseil est d'en parler à son entourage, afin d'éviter de s'enfermer dans une relation exclusive avec le faux conseiller. L'entourage est en général de bon conseil et vous aidera à prendre conscience de l'escroquerie.



Quatre sites frauduleux qui figurent sur la liste noire de l'AMF

ORBISOLYX.COM, Le trading de façade

Le nom ne dit rien à personne, et c'est probablement voulu. Orbisolyx prétend donner accès aux marchés Forex, aux cryptos et aux actions, avec, en prime, des outils d'analyse et un suivi de portefeuille. Le tout est enrobé d'un slogan rassurant : la plateforme « comprend les besoins des *traders* ». Sauf qu'en cherchant un peu, on ne trouve ni société, ni adresse, ni frais affichés, ni conditions de retrait, ni la moindre mention légale. Rien qui permette de savoir à qui nous avons réellement affaire.

AURUDIUM.COM,

Une marque inventée pour faire briller les yeux

Il s'agit d'un site internet qui se base sur une entreprise purement inventée. Comme son nom le laisse supposer, « *aurum* » signifiant or en latin, il met en avant la vente d'or. C'est un mélange habile de produit à la mode, surfant sur les hausses records de l'or depuis plusieurs années, et une valeur refuge prétendument rassurante. Quoi de moins high-tech que les métaux précieux ? Chez les arnaqueurs, il y en a pour tous les goûts.

MAKARYWALLETS.COM,

Arnaquer les victimes d'arnaque

Ce site cible des victimes d'arnaques déjà fragilisées, en leur promettant de récupérer leurs fonds perdus. Le procédé est rodé avec un discours qui se veut rassurant, une urgence fabriquée et la promesse de l'intervention d'experts. Tout cela est prétexte à réclamer des avances qui ne seront jamais remboursées. Derrière cette façade, il n'y a aucune société identifiable et aucune légitimité réelle. Inscrit sur la liste noire de l'AMF, le site endosse les habits du sauveur pour mieux piéger ses cibles. Le piège est d'autant plus cruel qu'il vise ceux qui ont déjà beaucoup perdu.

BCQECOAIN.FR,

Derrière le jargon crypto... le vide

BCQE Coin se présente comme « la principale plateforme de *trading* d'actifs numériques au monde », rien de moins. L'interface est soignée avec des graphiques de cours en temps réel et des promesses de *trading* par intelligence artificielle. Et que dire de la réserve de sécurité annoncée à 10.000 bitcoins. Tout est fait pour inspirer confiance. Mais en réalité, il n'y a aucune société identifiable, aucune adresse, aucune licence et encore moins de mentions légales affichées sur le site. Le schéma est classique : une fois déposés, les fonds ne peuvent plus être retirés.

« plus qu'une place disponible avant clôture »... C'est en ralentissant qu'il devient possible d'analyser froidement la situation et d'être attentif aux facteurs de risques suivants :

- promesse « sans risque » et rendement élevé sont incompatibles ;
- opacité de la personne en face (y compris moyen de communication inhabituel : WhatsApp, Telegram, numéros étrangers injustifiés...);
- circuit de paiement atypique (compte à l'étranger, cryptomonnaie, compte bancaire de particulier...);
- frais importants pour recouvrer des fonds ou des avances sur le paiement d'impôts ou de taxes;
- changements d'interlocuteurs fréquents;

- changements de numéros de téléphone, d'adresses du site internet ou d'adresses e-mail;
- prise en main de votre équipement à distance (AnyDesk);
- demande de mots de passe ou d'identifiants.

De tout ce que nous venons de voir, nous devons retenir une chose : l'évolution technologique, de l'apparition d'Internet à l'arrivée de l'IA, a rendu les falsifications d'identité beaucoup plus crédibles et les anomalies de plus en plus difficiles à déceler. La seule défense sérieuse repose désormais sur l'analyse de la logique de l'offre, et qu'en cas de doute, le plus raisonnable est de s'abstenir. •

MARC BOUZY
ET YANN SKOROCHOD
Broker Defense