

Quand les réseaux sociaux deviennent le terrain de jeu des fraudeurs

Mathieu Dagenais, étudiant à la maîtrise en criminologie,
Université de Montréal

Les réseaux sociaux sont des outils essentiels de notre quotidien : on les utilise pour se divertir, pour socialiser, pour s'informer et même parfois, pour y trouver des conseils en matière d'investissement. Malheureusement, ces espaces ne sont pas aussi sécuritaires qu'il n'y paraît. Au contraire, ils **facilitent même la propagation des fraudes**, spécifiquement des fraudes à l'investissement, **par leur manque de neutralité** ¹ ou la diffusion de publicités faisant la promotion d'opportunités douteuses.

Les plateformes sont construites de manière à capter notre attention, à nous faire interagir et réagir, mais elles peuvent aussi **nous exposer à des contenus problématiques**. Ces mécanismes d'interaction peuvent être exploités par les fraudeurs pour manipuler les internautes.

Cette courte synthèse a pour but d'informer sur l'effet plus spécifique des **algorithmes, des dynamiques sociales et de la littératie financière** dans la fraude à l'investissement.

Comment les algorithmes amplifient-ils les contenus frauduleux ?

Des systèmes qui sont basés sur l'engagement et non la véracité

Les réseaux sociaux mettent de l'avant **le contenu qui capte notre attention, mais pas nécessairement ce qui est vrai**. Chaque clic, visionnage, « j'aime » ou recherche sur un certain sujet permet aux plateformes de mieux nous connaître. À travers une meilleure connaissance des utilisateurs, elles peuvent identifier ce qui permettra de nous garder connectés le plus longtemps possible.

Le résultat ? De multiples contenus accrocheurs sont mis de l'avant afin de nous intéresser, même s'ils sont frauduleux, faux ou trompeurs.

Dans le cas des fraudes à l'investissement, il peut s'agir de **vidéos ou de publicités promettant un enrichissement rapide**, l'accès à de nouvelles techniques d'investissement, une vie luxueuse, etc. Ce genre de publicités attire de nombreux clics et donc beaucoup de visibilité aussi, augmentant les chances de voir ce contenu. Ces dernières peuvent donc **se propager très rapidement** et rejoindre le fil de recommandations de presque tout le monde, y compris les personnes n'ayant jamais pensé à investir auparavant.

Une pente glissante qui commence par une simple curiosité

Sur les réseaux sociaux et sur internet en général, tout est connecté. Ainsi, une vidéo peut rapidement nous mener vers une autre, un clic peut nous mener vers un autre lien, etc. Souvent, le tout se passe sans qu'on s'en rende compte activement. Cette interactivité peut nous exposer à du contenu frauduleux.

En effet, le simple fait de naviguer sur internet augmenterait les chances d'investir dans une fraude à l'investissement ². Pourquoi ? Parce qu'en cherchant à s'informer sur, par exemple, les cryptomonnaies ou les placements financiers fructueux, on se tourne souvent, par habitude, vers les plateformes numériques. Or, malgré la présence de bonnes informations sur celles-ci, elles contiennent aussi beaucoup d'**éléments trompeurs qui ne sont pas retirés par les services de modération** de ces plateformes.

Plus une personne clique ou effectue des recherches sur un sujet, plus elle manifeste de l'intérêt par rapport à celui-ci. Les plateformes réagissent alors **en proposant davantage de contenu similaire**. Ce qui en résulte est ce qu'on appelle des « **bulles informationnelles** », soit un environnement dans lequel l'utilisateur est continuellement exposé au même type de contenu. Cela donne l'impression, au fil du temps, que tout le monde pense pareil ou reçoit les mêmes informations et qu'elles paraissent donc crédibles.

Par conséquent, une simple curiosité pour les cryptomonnaies peut donc, après quelques clics, lancer l'utilisateur dans une **spirale de promesses de profits rapides**, de témoignages de réussite et de nouvelles monnaies à ne pas manquer. Ce qui a commencé par un intérêt d'apparence anodine devient alors un terrain glissant menant à une situation où les conseils frauduleux et les fausses promesses semblent alors plausibles, voire convaincants. Chaque vidéo visionnée ou commentaire lu devient alors une sorte de **confirmation que vous êtes sur la bonne voie, même si c'est totalement faux**.

Une plus grande exposition, mais aussi une influence subtile

À travers l'exposition continue à des messages positifs sur l'investissement en cryptomonnaies et des promesses d'un futur aisé, ce type de contenu peut devenir de plus en plus « **normalisé** ». Ainsi, une annonce vantant le succès d'une plateforme d'investissement sur YouTube et expliquant les démarches à suivre afin d'investir avec succès peut facilement passer pour une offre sérieuse.

En effet, par la consultation quotidienne de ce genre de contenu sur les différentes plateformes, les individus sont poussés à ne plus interpréter ces annonces comme suspectes ou frauduleuses, mais plutôt comme une partie intégrante de la navigation sur le web. Un élément central contribuant à cette exposition accrue est le recours aux systèmes de publicité payante offerts par les plateformes elles-mêmes.

YouTube, Facebook, Instagram, TikTok ou Google utilisent tous des outils d'achat publicitaire comme Google Ads, Meta Ads et TikTok For Business, permettant aux annonceurs de payer pour que leur contenu apparaisse dans le fil d'actualité ou les recommandations vidéo. **Ces systèmes permettent aussi un ciblage très précis** selon les intérêts, les recherches récentes, l'âge ou même le comportement en ligne.

Cette grande capacité de ciblage constitue une **opportunité immense pour les fraudeurs**, qui utilisent les mêmes outils que les entreprises légitimes afin de promouvoir leurs offres frauduleuses, souvent en contournant les mécanismes de vérification des plateformes ³. De telles préoccupations ont été exprimées par plusieurs organismes de régulation. Par exemple, la Financial Conduct Authority (FCA) rapporte avoir observé que plusieurs activités non autorisées outrepassent les processus de vérification existants ⁴. De même, une enquête journalistique d'Investigate Europe en 2024 a pu montrer que Meta (Facebook) **ne vérifie pas systématiquement les entreprises** avant de leur permettre de diffuser des annonces, ce qui permet aux fraudeurs de facilement s'acheter des emplacements publicitaires ciblant des investisseurs potentiels ⁵.

Ces plateformes permettent ainsi une **visibilité rapide, massive et ciblée**, et ce, même pour des publicités frauduleuses, ce qui explique pourquoi ces annonces peuvent couramment se retrouver dans le fil de recommandations de toute personne, et ce, à presque tout moment. Ainsi, il devient plus rare, sur ces plateformes qui encouragent le visionnage rapide et une grande interactivité, que les individus prennent le temps d'analyser toutes les informations d'une publicité ou d'une offre quelconque avant de s'y lancer. Cela s'inscrit dans une sorte de routine généralisée qui s'est créée et s'est répandue au fil des années à travers l'utilisation des réseaux sociaux. Les plateformes deviennent alors un environnement propice à l'exploitation de l'influence sociale et de la persuasion pour faciliter les fraudes. Au travers de cette exposition constante, les utilisateurs peuvent **diminuer leur vigilance et accorder plus facilement leur confiance**.

Le fonctionnement des plateformes elles-mêmes, qui se traduit souvent par des publicités omniprésentes, un encouragement d'activités de routine à l'apparence banale, des moments d'excitation, un accès constant à des visuels attractifs ainsi que des liens vers d'autres plateformes, **est devenu quelque chose de familier et normal** pour plusieurs personnes. Les usages décrits précédemment font partie intégrante des habitudes quotidiennes de multiples individus. Par conséquent, les publicités d'investissement frauduleuses **se fondent facilement dans ce paysage familier, prenant l'apparence de messages publicitaires émis par des entreprises légitimes cherchant à rejoindre des investisseurs potentiels plutôt que des fraudes sophistiquées visant à tromper.**

Comment les fraudeurs transforment-ils certains aspects des réseaux sociaux en instruments de manipulation ?

Des contenus conçus pour se propager et qui sont difficiles à contrôler

Ce type d'arnaque se propage rapidement puisqu'il repose sur des éléments qui poussent à cliquer et à s'y intéresser :

- Un ton sensationnaliste;
- Une opportunité unique;
- Des promesses exceptionnelles;
- Un sentiment d'urgence.

En plus d'être confronté à ces éléments et de devoir évaluer leur légitimité, **des comptes automatisés (bots) ou des faux comptes** sont aussi utilisés afin de créer des « j'aime », des commentaires et ainsi donner l'**impression que l'offre est populaire ou qu'elle a été vérifiée et confirmée** par d'autres.

D'autre part, les plateformes ont du mal à freiner la machine. Plus précisément, les **systèmes de modération sont souvent lents, fastidieux et peu efficaces**, alors que les fraudeurs eux, sont rapides

à s'adapter et changer leurs tactiques. Dès qu'une publicité frauduleuse est supprimée, il n'est pas surprenant qu'une autre prenne sa place très rapidement.

De surcroît, les fraudeurs profitent souvent du fonctionnement des réseaux sociaux, dont les revenus dépendent de la publicité. Comme ces annonces leur rapportent des profits, les plateformes sont parfois moins strictes sur ce qui est diffusé ³. Ainsi, les fraudeurs peuvent simplement **payer pour diffuser leurs annonces** et toucher rapidement et facilement de potentielles victimes en les rejoignant dans leur fil d'actualité ^{1&3}.

Ces plateformes, qui sont **perçues par plusieurs comme des sources légitimes et fiables**, peuvent contenir un nombre considérable d'annonces frauduleuses qui passent souvent inaperçues.

L'effet de groupe et des fausses communautés

Les fraudeurs ont souvent recours à une dynamique de groupes pour rendre leur offre d'investissement plus crédible. Sur des plateformes comme Telegram, WhatsApp, Facebook ou Discord, ils créent **de faux groupes** où de prétendus investisseurs, qui sont bien souvent, en réalité, des complices ou des comptes automatisés (bots), partagent des témoignages de succès, des conseils ou même des captures d'écran des profits impressionnants qu'ils ont faits.

Dans ces groupes où les fraudeurs ont le contrôle total, ceux-ci diffusent constamment du contenu à l'intention trompeuse et filtrent ou suppriment les messages critiques qui les visent.

Ces groupes donnent ainsi l'**illusion que tout le monde réussit** et gagne de l'argent en mettant de l'avant seulement le contenu d'apparence positive. Cela permet de renforcer un faux sentiment de sécurité et pousse les nouveaux membres à faire confiance rapidement. Ce phénomène repose sur ce qu'on appelle la **validation sociale**, où plus on voit d'autres personnes croire ou faire quelque chose, et plus on est tenté de faire pareil ^{6 7}.

L'influence des conversations privées et ciblées

Les fraudeurs ne se contentent pas seulement de messages publics. Souvent, ceux-ci vont contacter directement leurs cibles dans des messages privés. Dans ces échanges plus intimes et fermés, ils se présentent comme aidants, disponibles et attentionnés. Ils peuvent notamment répondre à des questions, expliquer comment fonctionne la plateforme d'investissement ou simplement discuter de tout et de rien.

À travers ces échanges, ils cherchent à créer un **lien de confiance personnalisé**, souvent basé sur une **fausse identité** et de **fausses informations** où ils se présentent, entre autres, comme des professionnels bienveillants en cryptomonnaies et parlent de leur vie familiale, de leurs valeurs ou de leurs expériences de vie. Cette stratégie ressemble beaucoup à celle employée dans le cadre des fraudes amoureuses où la relation est construite progressivement pour mieux tromper la victime plus tard.

Ce type de relation est particulièrement **dangereux** puisqu'il donne l'impression que la personne est digne de confiance, ce qui fait **baisser la vigilance** et augmente les chances de croire à l'investissement qui est proposé.

L'exploitation des biais cognitifs

Les escroqueries présentées aux victimes via les plateformes de médias sociaux sont souvent conçues pour exploiter des réflexes mentaux inconscients, appelés biais cognitifs. Voici quelques exemples courants de ces biais :

- La **peur de manquer** une opportunité unique (ex. : une offre disponible seulement pour un certain temps ; une nouvelle monnaie qui vient d'arriver ; une chance de faire des profits qui ne reviendra pas) ;
- Le **sentiment d'urgence** (ex. : un temps limité pour investir ; un programme d'investissement à durée limitée) ;

- La comparaison sociale (ex. : des commentaires positifs en ligne ; des centaines de personnes qui ont déjà fait fortune avec cette méthode) ;
- La **surconfiance** (ex. : croyance qu'on ne fera pas les mêmes erreurs que les autres ; croyance qu'on sera capable d'identifier les signaux d'alerte) ;
- L'**autorité** (ex. : se fier à quelqu'un qui se présente comme un expert ; faire confiance à une personne connue ou une célébrité pour investir).

Ces biais poussent les individus à **prendre des décisions rapides** et peu réfléchies, souvent sans vérifier les faits complètement ou sans poser suffisamment de questions ni demander de second avis.

Est-ce que les facteurs de protection sont suffisants face aux fraudes à l'investissement ?

La littératie financière, c'est quoi ?

La littératie financière, c'est la capacité de comprendre et d'évaluer des informations financières à partir de connaissances, d'expériences et de compétences en lien avec le sujet. Ce **n'est ni le niveau d'éducation ni les connaissances générales ou même l'intelligence qui protègent** contre les fraudes, mais bien le niveau de compréhension des enjeux financiers. Des études^{8,9} démontrent que :

- Les personnes avec une bonne littératie financière sont capables d'**identifier des signaux de fraude** plus facilement ;
- L'amélioration d'un seul point sur l'échelle de mesure du niveau de littératie financière peut **réduire considérablement les risques**, soit d'environ 40% des probabilités d'investir dans une fraude de type Ponzi pour chaque niveau de progression sur l'échelle.

Les limites d'une bonne littératie financière

Même avec de bonnes connaissances et expériences, **personne n'est complètement à l'abri**.

Savoir ne veut pas dire être à l'épreuve de manipulations psychologiques. Par exemple, quelqu'un de bien informé peut devenir trop confiant en ses capacités à reconnaître une arnaque sans se tromper.

Cette **surconfiance peut masquer certains signaux d'alerte** ^{10 11}.

De plus, l'**environnement** actuel des fraudes à l'investissement est **complexe**. Il est difficile, même pour les gens expérimentés, de comprendre toutes les subtilités des investissements numériques, notamment en ce qui concerne :

- Les cryptomonnaies ;
- Les NFT (jetons non fongibles) ;
- Les systèmes de finance décentralisée (DeFi) ;
- Les plateformes non régulées ;
- Les projets de « prévente » de nouveaux tokens (ICO) ;
- Les escroqueries de type « airdrop » ;
- Les faux bots d'investissement automatisé.

Se protéger face à la fraude à l'investissement en ligne : quelques stratégies critiques

Les fraudes à l'investissement sur les plateformes numériques ne reposent pas uniquement sur des promesses trop belles pour être vraies. Elles exploitent également des dynamiques plus profondes comme l'architecture des réseaux sociaux, les interactions humaines, les biais cognitifs et les routines numériques quotidiennes. De ces faits, pour se protéger contre cette fraude, la méfiance seulement ne suffit pas. Il faut aussi **comprendre la manière dont les environnements numériques sont conçus pour nous influencer**, souvent de manière imperceptible. Cela demande donc de développer des stratégies critiques pour reconnaître des signes autres que des promesses de gains élevés. En voici une liste non exhaustive :

1. Gardez l'**esprit ouvert** vis-à-vis de toute information en :

- **Variant délibérément vos sources d'information**, même si vous pensez en avoir trouvé une qui est fiable et crédible.

- **Consultant des ressources indépendantes** non associées à la plateforme, au réseau social ou au groupe en question.
- **Effectuant des recherches inversées** d'images ou de textes pour vérifier si le contenu a déjà été signalé: (<https://www.clinique-cybercriminologie.ca/post/rechgoogle>).

2. Portez une attention particulière à l'**ambiance véhiculée** par l'environnement et le message lui-même :

- Le **ton du message** est-il trop optimiste, urgent ou sensationnaliste ?
- Le fil de commentaires et d'avis est-il **positif et sans contradiction** ?
- Semble-t-il avoir une **mise en scène sociale** (une communauté qui publie des « preuves » des gains obtenus) ?
- Rappelez-vous que le contenu « sponsorisé » indique simplement que quelqu'un a payé la plateforme pour apparaître sur votre fil. Il **n'indique en rien la crédibilité d'une offre**.

Ce ne sont pas nécessairement les promesses elles-mêmes, qui doivent alerter à la fraude, mais aussi le **contexte social et visuel dans lequel elles se réalisent**.

3. Déjouez les **récits émotionnels** et les schémas typiques :

- Demandez-vous **quel intérêt** une personne inconnue aurait à vous écrire en privé et à vous aider à investir ?
- Apprenez à reconnaître les éléments narratifs courants des fraudes comme des **histoires qui sont trop fluides, parfaites ou structurées** de manière à émouvoir ou séduire.

4. Neutralisez les effets des **communautés artificielles** :

- Essayez de retrouver les profils qui commentent ou interagissent dans un groupe et d'identifier des **indicateurs d'un faux compte ou d'un compte automatisé** (compte récent, photo

générique, peu de publications personnelles, etc.) ainsi que s'ils possèdent un historique numérique cohérent.

- **Posez des questions critiques** dans ces groupes et voyez si vos messages sont supprimés ou ignorés.

5. Adoptez une **vérification en plusieurs étapes** avant de prendre une décision :

- **Prenez une pause** : ne répondez pas immédiatement à une offre, et ce, même si une personne veut vous accompagner dans le processus.
- **Posez au moins trois questions** sur la plateforme et trouvez les réponses sans avoir recours à la personne qui vous aide (Depuis combien de temps est-elle créée ? Quels sont ses antécédents légaux ? Existe-t-il des avertissements de régulateurs ? Etc.).
- **Consultez un avis extérieur et indépendant** (une personne de confiance non impliquée, un forum de prévention des fraudes, un site officiel de régulation financière, etc.).

6. Développez une **littératie émotionnelle** en même temps qu'une bonne **littératie financière** :

- Essayez de **nommer vos réactions émotionnelles** face aux annonces d'investissement (excitation, peur, espoir, urgence).
- Demandez-vous si vous êtes en train de prendre une décision dans le but d'**apaiser une émotion ou pour atteindre un objectif rationnel** ?
- Si vous constatez que votre réponse repose sur une émotion, prenez le temps de repenser à l'offre, de poser des questions et de prendre en compte d'autres informations avant de prendre votre décision.

Que pourraient faire les autorités et les plateformes ?

Au-delà des gestes individuels, une partie importante de la solution repose sur l'introduction de changements structurels par les autorités et les différentes plateformes numériques impliquées. En effet, au niveau international, il est de plus en plus reconnu que ces fraudes ne sont pas simplement

des incidents isolés, mais bien des **opérations criminelles organisées, soutenues par des réseaux transnationaux**¹². Ce changement de perspective transforme aussi les besoins. Il ne suffit pas de seulement informer le public, il devient essentiel de doter les autorités et les plateformes d'outils capables d'agir à la même échelle que les fraudeurs. Les recommandations suivantes s'inscrivent dans cette nouvelle approche :

1. Une meilleure régulation de la publicité financière payante :

- **Vérification obligatoire des annonceurs financiers.** Imposer légalement que toute publicité reliée à l'investissement soit préalablement **vérifiée par un régulateur** comme l'AMF ou la FCA. Cela permettrait de limiter l'utilisation des canaux sponsorisés qui sont présentement fortement utilisés par les fraudeurs tout en sanctionnant les plateformes qui diffusent ces publicités illégales.
- **Renforcer le filtrage des plateformes.** Avec toutes les informations collectées par les plateformes et réseaux sociaux, il serait possible **d'interdire ou de forcer une autorisation quelconque pour les annonces** contenant des formulations typiques de fraudes (rendements garantis, gains passifs très élevés, mention de célébrité ou de l'IA).
- **Mentions obligatoires claires** pour aviser les utilisateurs. Afficher de manière visible le statut réglementaire d'un annonceur du type : « non-enregistré auprès d'un régulateur » ainsi que le fait qu'une annonce sponsorisée ne garantit en rien la légitimité de l'offre.

2. Introduire des actions automatiques pour freiner les actions impulsives :

- Mettre en place des « **écrans d'avertissement** » lorsqu'un utilisateur clique sur un lien pour quitter la plateforme vers un site à haut risque. L'IA pourrait être utilisée pour rapidement scanner le lien URL et effectuer quelques recherches pour vérifier sa légitimité.
- **Pop-up de confirmation** si un utilisateur interagit fréquemment avec des contenus d'investissement qui ont été détectés comme à

risques (le pop-up pourrait fournir des conseils et rappeler les techniques courantes utilisées)

3. Agir sur les bulles informationnelles et les algorithmes de recommandation :

- Les algorithmes pourraient être conçus de manière à **suggérer du contenu de littérature financière**, des mises en garde officielles sur les fraudes à l'investissement et des exemples de techniques de fraudes pour les individus qui consomment beaucoup de contenus sur l'investissement.
- Réduction des recommandations automatiques des contenus d'investissement à haut risque ou non régulés.

4. Détection automatisée et réponses rapides :

- Les plateformes pourraient être tenues de déployer des modèles d'intelligence artificielle spécifiquement entraînés pour reconnaître les schémas typiques de fraudes dans les publicités.
- Les plateformes pourraient **collaborer avec les autorités via des canaux de communication sécurisés et prioritaires** (unité de réponse conjointe) plutôt que d'utiliser le signalement classique, souvent très long. Les plateformes pourraient alors fermer un compte ou bloquer certaines annonces frauduleuses beaucoup plus rapidement et sur plusieurs différentes plateformes.
- **Augmenter les exigences des banques** par rapport aux vérifications préalables à l'envoi de fonds vers des plateformes non enregistrées. Les institutions financières pourraient être obligées d'interroger, avant certaines transactions, un service centralisé géré par une autorité compétente qui attribuerait un score de risque aux plateformes via un outil automatique. Si la destination de la transaction est jugée comme risquée, alors un avertissement visuel explicite serait affiché avec des recommandations (recherches à faire, risques, signaux à observer).

5. Augmenter la transparence, la reddition de comptes et les registres publics :

- Obliger les plateformes à **publier régulièrement**

des rapports détaillés sur les fraudes en leur sein. Ce rapport pourrait comprendre le nombre de publicités frauduleuses (spécifique à chaque type), le volume de comptes bannis, les délais moyens de retrait de l'annonce après un signalement et les principales techniques utilisées dans les annonces frauduleuses.

- Créer, avec la collaboration de régulateurs, un **registre consultable et centralisé** qui contient les domaines frauduleux identifiés et les annonceurs exclus pour fraude.

6. Éducation, recherche et prévention :

- Les autorités et les autres plateformes recevant des plaintes ou déclarations de la part de victimes devraient permettre l'accès à ces données après les avoir anonymisées afin de **rendre facilement et rapidement consultables**, par les banques, navigateurs et médias, **les sites frauduleux**, pour faciliter le blocage de ceux-ci.
- Les plateformes pourraient mettre en avant des **campagnes officielles ciblant les publics les plus exposés** (nouveaux investisseurs, personnes recherchant activement à faire des gains rapides, etc.).
- Utiliser les nombreux sites permettant aux victimes de déclarer la fraude subie afin de **mieux répertorier les domaines frauduleux**, les techniques frauduleuses courantes et d'organiser de meilleures campagnes de sensibilisation auprès de la population.

Conclusion

Les fraudes à l'investissement en ligne ne sont pas seulement le produit de quelques individus mal intentionnés : elles s'inscrivent dans un écosystème numérique où les algorithmes, les dynamiques sociales et les failles de vérification publicitaire **travaillent souvent en faveur des fraudeurs**. Les réseaux sociaux, conçus pour capter l'attention plutôt que de garantir la fiabilité des contenus, créent des environnements où les promesses trompeuses peuvent circuler rapidement, sembler crédibles et influencer subtilement les décisions.

Si certains facteurs individuels comme la littératie

nancière ou la vigilance personnelle peuvent offrir une certaine protection, ils ne suffisent pas à eux seuls dans un contexte où les mécanismes technologiques et sociaux amplifient les risques. C'est pourquoi la lutte contre ces fraudes doit aller au-delà des gestes individuels et s'appuyer sur des changements structurels : une meilleure régulation de la publicité numérique, une détection proactive des contenus frauduleux, plus de transparence des plateformes et une collaboration renforcée avec les autorités.

En somme, réduire l'efficacité des fraudes à l'investissement nécessite à la fois une compréhension éclairée des environnements numériques et une action concertée entre citoyens, institutions financières, plateformes et régulateurs. C'est seulement en agissant simultanément sur ces deux fronts qu'il sera possible d'offrir un espace numérique plus sécuritaire et moins propice à la manipulation.

Références

¹ Van Dijck, J., Poell, T. et De Waal, M. (2018). *The Platform Society* (vol. 1). Oxford University Press. [DOI :10.1093/oso/9780190889760.001.0001](https://doi.org/10.1093/oso/9780190889760.001.0001).

² Ramli, R., Muda, S., Kasim, E. S., Md. Zin, N., Ismail, N. et Mohd Padil, H. (2023). Examining the Relationship between Social Media and Intention to Invest in an Investment Scams among Students. *Information Management and Business Review*, 15(4(SI)), 387-393. [DOI : 10.22610/imbr.v15i4\(SI\).L3613](https://doi.org/10.22610/imbr.v15i4(SI).L3613).

³ Kim, H. Y. (2024). What's wrong with relying on targeted advertising ? Targeting the business model of social media platforms. *Critical Review of International Social and Political Philosophy*, 1-21. [DOI : 10.1080/13698230.2024.2309047](https://doi.org/10.1080/13698230.2024.2309047).

⁴ Financial Conduct Authority. (2023). *Response to Ofcom's call for evidence : Third phase of online safety regulation*. <https://www.ofcom.org.uk/siteassets/resources/doc>

[uments/consultations/category-2-6-weeks/281475-third-phase-of-online-safety-regulation/responses/fca.pdf?v=405723](https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-2-6-weeks/281475-third-phase-of-online-safety-regulation/responses/fca.pdf?v=405723).

⁵ McNamara, M.-L., Buzzoni, L., Schmidt, N., Zwolenski, P. et Hansens, P. (2024). Investment scammers slip through cracks in EU Big Tech law. *Investigate Europe*. <https://www.investigate-europe.eu/posts/investment-scammers-slip-through-cracks-in-eu-big-tech-law?>

⁶ Kieffer, C. N. et Mottola, G. R. (2017). *Understanding and Combating Investment Fraud* (vol. 1). Oxford University Press. [DOI : 10.1093/oso/9780198808039.003.0010](https://doi.org/10.1093/oso/9780198808039.003.0010).

⁷ Modic, D. et Lea, S. E. G. (2013). Scam Compliance and the Psychology of Persuasion. *SSRN Electronic Journal*. [DOI : 10.2139/ssrn.2364464](https://doi.org/10.2139/ssrn.2364464)

⁸ Kasim, E. S., Awalludin, N. R., Zainal, N., Ismail, A. et Ahmad Shukri, N. H. (2024). The effect of financial literacy, financial behaviour and financial stress on awareness of investment scams among retirees. [DOI : 10.1108/JFC-04-2023-0080](https://doi.org/10.1108/JFC-04-2023-0080).

⁹ Singh, K. N. et Misra, G. (2023). Victimization of investors from fraudulent investment schemes and their protection through financial education. *Journal of Financial Crime*, 30(5), 1305-1322. [DOI : 10.1108/JFC-07-2022-0167](https://doi.org/10.1108/JFC-07-2022-0167).

¹⁰ Brenner, L. A., Koehler, D. J., Liberman, V. et Tversky, A. (1996). Overconfidence in Probability and Frequency Judgments: A Critical Examination. *Organizational Behavior and Human Decision Processes*, 65(3), 212-219. [DOI : 10.1006/obhd.1996.0021](https://doi.org/10.1006/obhd.1996.0021).

¹¹ Deliema, M., Shadel, D. et Pak, K. (2020). Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors. *Journal of Consumer Research*, 46(5), 904-914. [DOI : 10.1093/jcr/ucz020](https://doi.org/10.1093/jcr/ucz020).

¹² UNODC. (2025). *9th Global Conference on Criminal Finances and Cryptoassets [communication orale]* 9e conférence de l'unodc.