

## Les manipulations psychologiques dans les fraudes à l'investissement : le rôle des biais cognitifs et des émotions viscérales dans la vulnérabilité des victimes

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

Les fraudes à l'investissement en ligne regroupant fausses plateformes d'investissement, cryptomonnaies et fausses opportunités financières se multiplient à une vitesse impressionnante. De plus en plus de personnes perdent leurs économies à cause de stratagèmes soigneusement conçus par les fraudeurs pour **exploiter des réflexes psychologiques** que nous partageons tous. Derrière chaque arnaque réussie se cachent des mécanismes mentaux subtils, appelés **biais cognitifs et biais émotionnels**. Ces deux formes d'erreurs de jugement influencent la façon dont nous pensons, ressentons, et prenons des décisions, souvent sans que nous en ayons conscience <sup>1</sup>. Quant à eux, les fraudeurs savent comment les exploiter pour manipuler les émotions et la perception de leur victime potentielle <sup>2</sup>. Comprendre ces biais, c'est donc apprendre à reconnaître comment des **mécanismes cognitifs tout à fait normaux peuvent être transformés en outils de manipulation**.

Les biais cognitifs sont des raccourcis mentaux que notre cerveau utilise pour aller plus vite dans la prise de décision <sup>3</sup>. Dans la vie quotidienne, ces automatismes sont utiles car ils nous aident à agir de manière efficace sans que nous ayons à analyser chaque détail. Toutefois, dans certaines situations, notamment face à des offres d'investissement attrayantes ou urgentes, ces raccourcis peuvent nous faire prendre de mauvaises décisions <sup>2</sup>. Contrairement à la croyance populaire, **les victimes ne sont ni plus naïves ni moins intelligentes que le reste de la population**. Elles réagissent plutôt à des réflexes psychologiques que les fraudeurs exploitent à leur avantage <sup>1 4 5 6</sup>.

Les biais émotionnels, quant à eux, apparaissent lorsque nos décisions sont influencées par des émotions fortes comme la peur, l'excitation, l'amour, l'amitié, la colère ou le stress <sup>7</sup>. Ces émotions **brouillent notre jugement et nous poussent à agir dans l'instant**. Par exemple, un investisseur pourrait agir avec urgence par peur de manquer une opportunité unique, ou encore avec euphorie face à une promesse de gain rapide. Les fraudeurs reconnaissent ces émotions et créent souvent des contextes émotionnels intenses rassemblant urgences, comptes à rebours, messages rassurants ou inquiétants, et bien d'autres afin de **court-circuiter la réflexion rationnelle** <sup>8 9</sup>.

Ainsi, une victime ne se distingue pas nécessairement d'une non-victime par son intelligence ou son niveau d'éducation <sup>10</sup>. **Chaque biais**, cognitif ou émotionnel, peut à lui seul **affaiblir la vigilance et rendre une personne vulnérable**. Par exemple, une personne peut être amenée à faire confiance à un individu rencontré en ligne qui prend le temps de discuter, de répondre à ses questions et d'offrir des conseils personnalisés sur les investissements. Cette relation crée une impression de proximité et de sincérité qui suffit parfois à désactiver la prudence. Ainsi, même une **personne avertie peut alors tomber sous l'emprise d'une manipulation bien orchestrée** <sup>2</sup>.

Dans les sections qui suivent, nous verrons comment ces biais, souvent combinés, construisent un environnement propice à la manipulation psychologique. D'abord, en favorisant **la construction d'une confiance trompeuse**, puis en **faussant l'évaluation des risques et des gains**, et enfin en **poussant la victime à des décisions impulsives**.

## La construction de la confiance et de la légitimité perçue

Les fraudeurs savent qu'avant de convaincre quelqu'un d'envoyer de l'argent, ils doivent d'abord **gagner sa confiance**. Cela explique pourquoi ils consacrent autant d'efforts à **paraître crédibles et professionnels** <sup>9 11 12</sup>. Pour bâtir cette confiance, les fraudeurs vont **exploiter différents biais cognitifs** qui influencent le jugement <sup>13 14</sup>.

### Le biais d'autorité : quand "l'expert" a toujours raison

Le **biais d'autorité** est l'un des outils les plus puissants utilisés par les fraudeurs, puisqu'il repose sur notre tendance instinctive à **accorder du crédit à ceux qui semblent maîtriser leur sujet** <sup>6 9 15 16 23</sup>. En effet, nous avons tous appris, depuis l'enfance, à suivre les conseils des figures d'autorité, que ce soit des enseignants, des médecins, des conseillers, ou des experts de milieux particuliers. Les fraudeurs misent sur l'influence que des profils de personnes connues, réputées, expertes ou simplement qui en ont l'apparence, ont sur leur niveau de crédibilité apparent <sup>5</sup>.

Les recherches montrent que **plus une personne semble compétente**, plus nous sommes enclins à **croire ce qu'elle dit, même sans preuve** <sup>5 9</sup>. Sur Internet, cette illusion d'expertise peut être **créée de toute pièces** très facilement : une photo en costume, un langage professionnel, un profil LinkedIn bien rempli ou la mention d'une célébrité suffisent souvent à inspirer confiance. Par exemple, un fraudeur se présentant comme un « analyste financier certifié » ou un « spécialiste en cryptomonnaies » peut paraître crédible aux yeux d'une personne qui ne connaît pas bien le domaine.

L'étude de Button et ses collaborateurs (2014) a montré que l'utilisation d'un **langage technique ou spécialisé** augmente de manière significative la **crédibilité perçue** du fraudeur.

Plus précisément, ce langage crée une sorte de **barrière symbolique**, parfois nourrie par un sentiment d'être moins compétent, qui pousse la victime à **s'en remettre au jugement du soi-disant expert** plutôt que d'analyser elle-même les informations <sup>5 9 17</sup>.

Ce phénomène dépasse largement la fraude à l'investissement. **Dans les fraudes amoureuses**, par exemple, certains fraudeurs adoptent aussi des rôles d'autorité comme des médecins, des travailleurs humanitaires, des militaires ou des ingénieurs, pour susciter confiance et respect <sup>6 18</sup>. Ainsi, peu importe le type de fraude, l'apparence de compétence devient un **levier psychologique important** afin d'obtenir la coopération des victimes.

### Le biais de représentativité, de disponibilité et de confiance : quand les apparences trompent

Le biais d'autorité est associé au **biais de représentativité**, soit la tendance à **évaluer une situation en se référant à des modèles familiaux** <sup>19</sup>. Par exemple, lorsqu'on voit une personne en blouse blanche dans un hôpital, on suppose spontanément qu'il s'agit d'un médecin, même si cela pourrait être un technicien ou un stagiaire. Notre cerveau évalue ainsi **la compétence ou la fiabilité** d'une personne en fonction de **son apparence ou de son rôle perçu**. Ce même réflexe s'applique en ligne. La présentation d'une offre d'investissement avec une allure professionnelle, par exemple communiquée sur un site web peaufiné ou via des vidéos explicatives et des certificats d'authenticité, aura plus de chances d'être perçue comme une entreprise légitime <sup>11</sup>. Notre cerveau, habitué à associer la qualité visuelle à une bonne fiabilité, fait alors un raccourci : **si c'est bien présenté, c'est que c'est sérieux**.

La tendance à percevoir ces offres frauduleuses comme crédibles peut également être liée au **biais de confiance** <sup>5 6</sup>. Après tout, la confiance est un élément essentiel de la vie sociale, nous permettant de développer toutes sortes de relations. Ainsi, dans la plupart des situations, **faire confiance est un réflexe humain utile** puisqu'il nous permet d'avancer sans avoir à remettre en question chaque détail. Toutefois, cette tendance à faire confiance peut aussi être **exploitée par des personnes mal intentionnées**.

Ainsi, un individu qui semble **aimable et aidant** peut susciter un sentiment de confiance naturel qui **décourage la vérification**. De plus, en raison de la tendance du cerveau humain à extrapoler certaines situations, la création d'une **apparence de légitimité** peut générer un **niveau de confiance permettant la réussite de la fraude** <sup>20</sup>. Dans une telle situation, les individus n'évaluent pas la crédibilité d'une source d'information sur la base de vérifications concrètes qu'ils ont faites, comme sur des registres officiels ou à l'aide d'indices de fiabilité de plateformes. Ils se basent plutôt sur l'image mentale qu'ils se sont créée du site en question <sup>21</sup>. Autrement dit, ils se **fient à leurs impressions plutôt qu'à des preuves réelles**.

Ce processus est associé au **biais de représentativité** (ou de similitude) et **de disponibilité** <sup>19</sup>. Le premier nous pousse à croire qu'une plateforme est **fiable parce qu'elle "ressemble" à une vraie entreprise** : graphiques de performance, photos de dirigeants, langage technique spécifique à la cryptomonnaie.

Cette forme de raccourci cognitif se combine au deuxième biais, soit celui de disponibilité, où nous évaluons la **fiabilité d'une information selon les exemples similaires que nous avons en tête** <sup>19</sup>. Par exemple, une personne qui vient de voir un reportage sur un crash d'avion peut hésiter à prendre son vol du lendemain, même si le risque réel n'a pas changé. De la même façon, un individu qui a récemment vu une publicité sur une plateforme d'investissement « miracle » peut être plus enclin à y croire. Le simple fait que cette **idée soit récente** ou familière dans sa mémoire **la rend plus crédible** à ses yeux.

De ce fait, dans un environnement numérique avec des possibilités presque illimitées pour modifier l'apparence des interfaces visuelles, ces trois biais forment une **combinaison redoutable**. Ensemble, ils permettent aux fraudeurs de fabriquer de toutes pièces une **illusion de légitimité qui désarme la prudence** et pousse les gens à agir rapidement avant de réfléchir <sup>1</sup>.

### Le biais de preuve sociale : l'influence du groupe

Il a aussi été observé que le comportement d'autrui joue un rôle dans la perception d'offres frauduleuses par les victimes. En effet, plus un **grand nombre de personnes semblent adhérer** à une offre, plus celle-ci **paraît digne de confiance**. Ce phénomène favorise l'imitation, les victimes cherchant à reproduire des comportements dans l'espoir d'accéder aux mêmes avantages ou gains perçus. Dans le contexte des fraudes à l'investissement, le **biais de preuve sociale** joue un rôle majeur. Lorsqu'une plateforme ou un groupe affiche de nombreux « témoignages positifs », un grand nombre d'abonnés ou des promesses de gains partagées par de nombreuses autres personnes, notre cerveau **interprète cela comme un signe de fiabilité** <sup>12 22 23 24</sup>. Ceci nous pousse ensuite à chercher à **imiter ceux qui semblent réussir**.

Ce biais renforce donc la confiance perçue via un mécanisme où plus le nombre de témoignages de tierces parties semble élevé, plus la victime se convainc qu'elle a fait le bon choix <sup>25 26</sup>. Pourtant, dans de nombreuses fraudes, ces « autres » ne sont pas vraiment réels. Les fraudeurs **créent de fausses preuves sociales** via des profils inventés, des commentaires automatisés ou des vidéos d'avis fabriqués, le tout ayant pour but de **simuler une popularité** et de donner l'**impression d'une communauté active et enthousiaste**.

### Le biais (ou effet) d'affinité : quand la confiance vient du sentiment d'appartenance

Le biais de preuve sociale se manifeste souvent en conjonction avec le **biais d'affinité**. Ce dernier repose sur une idée simple, soit que nous faisons **plus facilement confiance à quelqu'un qui nous ressemble**. Qu'il s'agisse d'une proximité religieuse, culturelle, linguistique ou professionnelle, cette similarité crée une illusion de sécurité <sup>27 28</sup>. Les fraudeurs vont exploiter ce principe en se présentant comme des membres d'un groupe familial. Par exemple, comme un « entrepreneur

local », un « membre de la même communauté religieuse » ou le « collègue d'un ami ».

Cette stratégie joue sur l'idée que « **quelqu'un de mon groupe ne me tromperait pas** ». La victime projetterait ainsi ses propres valeurs et croyances sur le groupe de référence <sup>28 29</sup>. Ce phénomène peut **réduire le besoin de vérifier** et même parfois empêcher le signalement de la fraude par loyauté ou par honte <sup>27</sup>. Dans le monde numérique des fraudes à l'investissement, la dynamique entre le biais d'affinité et celui de preuve sociale peut souvent être combinée à travers de **fausses communautés d'investissement**. Ces groupes en ligne rassemblent de supposés investisseurs qui partagent des messages positifs, encouragent les autres à investir et affichent de faux gains. À force de voir ces interactions, les nouveaux venus ont l'impression d'intégrer une communauté bienveillante et soudée. Ce climat d'entraide crée une **illusion de normalité et de succès collectif via des confirmations positives constantes**, ce qui empêche les membres de remettre en question les intentions réelles du groupe. Une telle influence sociale a été démontrée comme un facteur permettant d'expliquer la tendance à faire davantage **confiance à quelque chose qui semble populaire ou validé** par d'autres personnes ou, ici, par d'autres membres d'un même groupe <sup>30</sup>.

## L'influence des distorsions dans l'évaluation du risque et du gain

### Le biais d'optimisme : croire que tout ira bien

Une fois la confiance établie, les fraudeurs exploitent d'autres mécanismes mentaux qui faussent notre manière d'évaluer les risques et les gains. Parmi ceux-ci, **le biais d'optimisme** joue un rôle central. Ce biais réfère à la tendance à **minimiser les risques réels** ou à **croire que nous sommes moins à risque** que les autres de vivre une expérience négative <sup>1 23</sup>. C'est un réflexe courant; toute personne a besoin d'un certain optimisme pour avancer de manière positive dans la vie.

Toutefois, dans un contexte d'investissement, cette pensée peut facilement devenir trompeuse. Par exemple, une personne peut se dire « Plusieurs se font arnaquer, mais moi je suis prudent, ça ne m'arrivera pas ».

Cette confiance excessive que tout ira bien, que le monde est bon, amène à **sous-estimer les dangers réels** des opportunités d'investissement ou à **surestimer la fiabilité d'une offre**, surtout lorsqu'elle semble innovante, moderne ou portée par la technologie <sup>4</sup>. Ce biais influence non seulement la décision d'investir, mais aussi la persistance dans l'erreur. Beaucoup de victimes continuent à verser de l'argent même après des signaux forts de fraude, convaincues que la situation va s'arranger ou que le prochain virement débloquera enfin leurs gains <sup>23</sup>. Cet **espoir** que leur engagement continu finira par produire des profits peut entraîner certaines personnes à **minimiser ou à ignorer les signes problématiques** associés à l'offre d'investissement, même lorsqu'ils sont objectivement apparents <sup>23</sup>.

### Le biais d'escalade d'engagement : continuer pour ne pas perdre

Ensuite, **l'escalade d'engagement**, aussi appelée le biais de « commitment » désigne la tendance à continuer de s'investir dans une décision, même lorsque celle-ci semble mener irrévocablement vers une perte. En effet, une fois que du temps, de l'argent ou des efforts ont été consacrés à une opportunité, il est **psychologiquement difficile de retourner en arrière**. Le fait d'abandonner dans une telle situation peut souvent donner l'impression d'avoir « gaspillé » des ressources, alors que persister permet de conserver une illusion de contrôle ou d'espoir <sup>31</sup>. Ce réflexe est profondément humain puisqu'il découle d'un **besoin de cohérence avec nos choix passés**. Les fraudeurs peuvent ainsi facilement exploiter un tel biais en s'appuyant sur le principe de « commitment and consistency », soit le désir de **rester fidèle à ce qu'on a dit ou fait** <sup>12</sup>. En d'autres mots, une fois qu'une personne a signé un contrat, investi sur un site ou écrit qu'elle croit dans

un projet quelconque, elle est plus encline à agir de manière cohérente avec cet engagement, et ce, même si les informations auxquelles elle a accès changent en cours de route.

Dans les fraudes à l'investissement, ce biais est souvent mis en jeu par les fraudeurs qui vont continuellement **encourager les victimes** à déposer « **un peu plus** » pour « **ne pas tout perdre** » ou encore pour « **sauver l'argent investi** ». Cette pression s'appuie sur deux émotions puissantes, soit **la peur de perdre ce qu'on a déposé** et **l'espoir ou la conviction qu'un dépôt supplémentaire réglera la situation** <sup>31</sup>. Cette spirale émotionnelle peut donc facilement pousser certaines victimes à investir davantage malgré des signes clairs d'une fraude. Un exemple de la vie commune illustre bien le phénomène, soit lorsqu'un joueur de loterie perd plusieurs fois de suite, mais continue d'acheter des billets en se disant que la prochaine fois sera la bonne. Dans une fraude à l'investissement, le principe est sensiblement le même : plus une personne investira et plus il deviendra difficile pour elle d'arrêter et d'abandonner le montant déposé.

#### Le biais de surconfiance : quand on se perçoit plus compétent qu'autrui

Le biais d'optimisme est souvent accompagné par le **biais de surconfiance**. Ce dernier apparaît lorsque nous **surestimons nos compétences**, ou notre capacité à analyser une situation complexe <sup>32</sup>. Autrement dit, c'est lorsque nous pensons que nous sommes parfaitement capables de détecter sans peine une fraude ou une bonne opportunité d'investissement... même si ce n'est pas le cas. Dans une étude de Deliema et ses collaborateurs (2020) comparant des victimes de fraude à l'investissement avec des investisseurs qui n'avaient pas été fraudés, les chercheurs ont observé que les **victimes étaient deux fois plus susceptibles de croire que les investissements risqués**, soit ceux non réglementés, **procuraient plus de revenus**. De plus, plusieurs victimes se montraient plus enclines à effectuer des **transactions fréquentes, à répondre à des offres non sollicitées et à investir dans des produits non réglementés**. En résumé, plusieurs

victimes croyaient être capables de reconnaître une « bonne affaire » et de gérer les risques mieux que les autres. Cette surconfiance les rendait particulièrement **vulnérables aux promesses de rendements exceptionnels** <sup>33</sup>.

Le lien entre le biais de surconfiance et la vulnérabilité à la fraude a aussi été confirmé dans d'autres études, démontrant qu'une perception amplifiée de ses compétences augmente les risques d'être victime de fraude <sup>1 34</sup>. Par exemple, dans une étude portant sur un sondage mené auprès de 3 316 répondants sur un questionnaire du site ScamAdviser, **68 % des participants se disaient « confiants » ou « très confiants »** dans leur capacité à identifier une fraude <sup>21</sup>. Pourtant, malgré cette confiance apparente, ce **même groupe représentait aussi la majorité des individus ayant perdu de l'argent à la fraude (59 %)** <sup>21</sup>.

Un autre élément important est la relation très étroite entre le biais d'optimisme et le biais de surconfiance. Comme le montre la littérature en économie comportementale, ces deux biais se renforcent mutuellement <sup>35</sup>. Plus précisément, **l'optimisme entretient la perception ou l'espoir d'une résolution positive**, alors que la **surconfiance** soutient l'idée que confronté à un problème quelconque, **l'individu sera en mesure d'y faire face et de le régler** <sup>1 32</sup>. Dans le contexte de la fraude à l'investissement, une telle relation présente d'importants risques puisqu'elle interfère avec les mécanismes de vigilance et peut amener les investisseurs à **ignorer des signaux d'alerte ou même rejeter les conseils d'agir avec prudence** <sup>1</sup>.

#### Le biais de confirmation et de cadrage : voir ce qu'on veut voir

Les biais cognitifs fonctionnent rarement de manière isolée. Ils s'influencent les uns les autres et créent une sorte de filtre mental qui change la manière dont nous interprétons l'information. Deux biais jouent fortement sur cette mauvaise interprétation, soit le biais de confirmation et le biais de cadrage. Le **biais de confirmation** nous pousse à chercher ou à croire les informations qui

valident nos propres croyances ou désirs préexistants<sup>36</sup>. Ainsi, une personne qui se voit offrir une opportunité d'investissement rare et prometteuse pourrait se concentrer uniquement sur les signaux qui **confirment son idée d'investir dans l'offre, au détriment des avertissements sur les risques de celle-ci**<sup>37 38</sup>.

Par exemple, elle pourrait seulement prendre en compte les témoignages positifs du groupe en ligne, les messages rassurants du conseiller et les chiffres prometteurs sur le site. **Le biais de cadrage** ou encore le « framing bias » renforce encore cette distorsion. Il désigne le fait que la manière dont une information est diffusée influence grandement la manière dont nous l'interprétons<sup>1</sup>.

Par exemple, en mettant **l'accent sur les gains potentiels et les revenus garantis** plutôt que sur les risques habituels d'un investissement, la **perception** des individus face à ce type de contenu peut être **plus positive**<sup>1</sup>. En effet, lire une offre comme « profits garantis à 30 % » nous semblera souvent plus attrayant que « investissement à haut risque, aucun remboursement possible », même si les deux phrases parlent de la même offre. Lorsque ces deux biais interagissent, la situation qui en découle pourrait être comparée à une sorte de **boucle cognitive** où le **cadrage initial** (promesses de gains, visuels attrayants) dirige la personne **à confirmer ce qu'elle cherche et à ignorer ce qu'elle ne veut pas voir**. Les fraudeurs utilisent très bien ce mécanisme. Ils construisent leurs **annonces d'investissement de façon à forcer un cadrage positif**.

Par exemple, ils peuvent effectuer une présentation fortement positive en utilisant des promesses exagérées, des faux témoignages, des captures d'écran ou des vidéos de profits inventés dans le but de guider l'interprétation de la victime dès le départ<sup>26</sup>. Une fois qu'une personne a été exposée à ce cadrage, le biais de confirmation s'occupe du reste, poussant la victime **à chercher involontairement tout ce qui confirme que l'offre est réelle tout en ignorant les signaux d'alarme**<sup>26</sup>.

### Le biais d'automatisation et l'heuristique de facilité : quand la technologie et la simplicité brouillent notre jugement

À l'ère de l'intelligence artificielle (IA), beaucoup de gens croient que les **technologies** permettent d'éviter les erreurs humaines. Pourtant, bien que ces nouveaux outils soient utiles, une **confiance aveugle** en ceux-ci peut parfois **jouer contre nous**. C'est ce qu'on appelle, plus spécifiquement, le **bias d'automatisation**, soit la tendance à accorder une trop grande **confiance aux outils technologiques**<sup>39</sup>.

Quand il s'agit d'investissement en ligne, cela se manifeste principalement lorsque des personnes s'en remettent entièrement aux algorithmes automatiques d'investissement ou aux plateformes dites « intelligentes », convaincues que la machine est plus fiable et plus efficace qu'eux-mêmes. En effet, il a été démontré que de nombreux investisseurs suivent les recommandations générées par un ordinateur sans les remettre en question, simplement parce qu'elles proviennent d'un système technologique automatisé<sup>39</sup>. Cette dépendance découle de l'attribution d'une valeur objective à la technologie où une personne en vient à croire qu'une **décision prise par une machine est nécessairement rationnelle**<sup>40</sup>. Or, la réalité est souvent bien différente, et ce, encore plus lorsque **les algorithmes derrière la machine « objective » sont en fait manipulés par des fraudeurs**.

Ce biais s'accompagne souvent d'un autre mécanisme psychologique appelé **heuristique d'accessibilité ou encore de facilité**. Il ne s'agit pas d'un biais à proprement parler, mais d'un raccourci mental utilisé pour préserver de l'énergie lorsque notre cerveau doit décider rapidement<sup>41</sup>. Selon Kahneman (2003), nous avons tendance à préférer les informations faciles à comprendre ou à se remémorer, plutôt que celles qui demandent un effort d'analyse complexe. Autrement dit, si nous avons le choix entre deux options, l'une complexe et l'autre plus simple, nous avons **tendance à choisir de manière instinctive l'option la plus simple**<sup>42</sup>. Cette logique s'applique de manière presque parfaite aux fraudes d'investissement modernes. En effet, il a été observé que les victimes étaient particulièrement

attirées par les plateformes qui promettaient des **profits rapides et sans effort requis** de leur part <sup>29</sup>. Le fait que « tout soit déjà fait » donne une **illusion de sécurité**. Par exemple, un individu reçoit un message d'un prétendu conseiller financier lui disant : « Ne vous inquiétez pas, notre système automatise tout pour vous. Je vais investir à votre place. Il vous suffit de déposer l'argent, le reste est pris en charge par notre outil d'intelligence artificielle ». Pour la victime, l'offre semble idéale puisqu'elle n'a **pas besoin d'apprendre le fonctionnement des cryptomonnaies, ni d'analyser le marché, ni encore de prendre des décisions compliquées et stressantes**.

Ce réflexe est expliqué par Shah et Oppenheimer (2009) comme le « chemin de la moindre résistance » où notre cerveau interprète la **facilité d'une solution comme une forme de qualité ou de fiabilité**. Dans les **fraudes**, ce réflexe est souvent **amplifié par des plateformes** qui affichent des graphiques en temps réel et des chiffres précis avec des mentions d'intelligence artificielle un peu partout. En réalité, cette apparente transparence nourrit un **faux sentiment de contrôle** et de fiabilité qui ne cesse de **diminuer la vigilance**, rendant la manipulation plus efficace.

## Le recours heuristique en situation d'incertitude

### Le biais de rareté : la peur de manquer une opportunité

Pour terminer, en addition aux effets considérables des biais précédents, se rajoutent des biais dont le but est de déclencher des réponses rapides sans ou avec peu de réflexion. Bien que chaque biais a la capacité à encourager la prise de décision rapide, le **biais de rareté**, également important dans la fraude à l'investissement, fait référence à la peur de manquer une opportunité unique et souvent « limitée » <sup>22</sup>. Ce biais est souvent activé par des messages qui mettent l'accent sur la chance de l'individu d'être « tombé » sur une offre qui lui permettra d'atteindre ses objectifs d'une manière plus aisée <sup>8</sup>. Ce biais s'active donc lorsqu'une offre

est **présentée comme exceptionnelle**: « Offre réservée à un nombre limité de personnes » ou « Dernière chance d'investir dans cette nouvelle monnaie » ou encore « Vous avez été sélectionné parmi des milliers d'investisseurs pour rejoindre notre groupe VIP ». Confrontée à de tels messages, une personne est plus encline à vouloir s'engager par **crainte que l'opportunité disparaisse** définitivement. Ce biais s'entremêle avec différentes émotions comme le **stress et l'excitation** <sup>4</sup>, ainsi que d'autres biais comme l'optimisme et la surconfiance pour amener l'individu à croire à l'opportunité frauduleuse.

Une personne peut alors se dire : « C'est peut-être risqué, mais une chance comme ça ne revient pas deux fois ». Sous cette pression, l'individu est incité à **poser moins de questions ou à ignorer les doutes** qu'il ressent. Le biais de rareté crée donc un sentiment d'urgence artificielle qui encourage les victimes à agir vite pour ne pas manquer ce qui leur semble être une offre profitable <sup>9</sup>.

## Exploitation des émotions viscérales

Dans le cadre des investissements en ligne, une compréhension des biais cognitifs qui sont exploités ne suffit pas à expliquer la réussite de la fraude. Beaucoup de recherches soulignent le rôle crucial des **émotions viscérales** dans la victimisation en ligne. Ces émotions, qui regroupent principalement **la peur, l'espoir, l'urgence, le désir d'amour ou encore le désir de reconnaissance**, sont couramment utilisées comme leviers par les fraudeurs pour **empêcher le raisonnement critique** de leurs cibles, affaiblir leurs capacités de réguler leurs émotions et les diriger vers des décisions spécifiques <sup>2 9 13 16 43 44</sup>.

L'anticipation d'un gain financier important peut agir comme un puissant incitateur émotionnel, capable d'activer des processus mentaux favorisant la prise de décision rapide <sup>9 29 38</sup>. Face à des promesses de profits rapides et élevés, les individus peuvent entrer dans un état où les émotions prennent le contrôle sur le processus de

prise de décision <sup>29</sup>. Un tel phénomène peut être amplifié par la présence d'une ou de quelques transactions fructueuses au départ de la fraude, laissant place à l'**excitation et à l'euphorie** plutôt qu'à la réflexion et à l'analyse <sup>15 38</sup>. Cette excitation **réduit la vigilance** par rapport aux détails et **limite l'évaluation des risques** tout en augmentant les probabilités d'engagement dans le processus frauduleux <sup>15</sup>.

Le phénomène décrit ci-dessus vient se combiner à un processus plus large où de multiples émotions viscérales sont fréquemment exploitées afin de créer une ouverture permettant le succès de la fraude. Notamment, l'**appât du gain** est nourri par des **promesses irréalistes et un langage suggestif** afin de surpasser les capacités cognitives des individus, et ce, encore plus chez ceux étant peu expérimentés avec les fraudes en ligne <sup>38</sup>. De plus, le potentiel d'un **allègement des pressions financières** relié aux gains promis, soit d'une possibilité de changer sa vie pour le meilleur dans certains cas, contribue activement à l'**affaiblissement des mécanismes de défense** cognitifs <sup>2</sup>. De ce fait, il est possible d'identifier que les émotions positives anticipées fonctionnent comme des régulateurs de la vigilance face aux opportunités risquées <sup>8</sup>.

La manipulation des émotions viscérales ne se limite pas uniquement à l'excitation ou à l'appât du gain. Des **effets plus négatifs** comme le **stress**, l'**inquiétude**, voire la **peur**, sont eux aussi mobilisés de manière stratégique par les fraudeurs <sup>44</sup>. Pour susciter de telles émotions, la création d'une « **urgence** » ou d'un contexte de rareté est souvent employée pour pousser les individus à **prendre des décisions précipitées**. Dans ce contexte, ceux-ci ont alors plus tendance à recourir à des raccourcis mentaux basés sur l'**intuition plutôt que sur l'analyse complète** de la situation <sup>8 16</sup>. Pour continuer, la pression temporelle associée à l'urgence de l'opportunité détourne l'attention portée à l'évaluation de l'offre pour plutôt se concentrer sur une réponse qui reposera sur des actions rapides et émotionnelles <sup>8</sup>. Cette forme de pression est accentuée dans les fraudes par l'implication de nombreux signaux sociaux implicites comme l'idée d'une offre unique qui ne reviendra pas ou encore une sorte de compétition entre

investisseurs où l'on veut montrer notre habileté à faire de bons investissements. Cela renforce le biais de rareté et peut aussi jouer sur la réussite des menaces futures faisant recours à la peur pour inciter la remise de sommes d'argent <sup>9 15</sup>.

Bien que les motivations économiques puissent favoriser des émotions menant à des jugements hâtifs, les fraudes en ligne exploitent aussi des **besoins plus affectifs**, comme le **désir de reconnaissance**, de **connexion**, d'**amour** ou de **valorisation personnelle** <sup>45</sup>. Plus précisément, les fraudeurs construisent des liens relationnels pouvant passer du mentorat à l'amitié, et même à l'amour pour instaurer une **confiance émotionnelle** chez leur cible. Cette stratégie, fréquemment utilisée dans les schémas frauduleux, a pour but de donner l'**illusion** à la victime qu'elle se situe dans une **relation affective plutôt que transactionnelle** <sup>43</sup> <sup>45</sup>. Pour ce faire, un langage empathique et poli, l'appel à des valeurs personnelles et l'offre d'un soutien émotionnel sont mobilisés par les escrocs afin de rendre la victime potentielle plus encline à accepter des propositions risquées qu'elle n'aurait peut-être pas envisagées dans d'autres contextes <sup>15 43</sup>. Les études montrent que les émotions provenant, entre autres, du sentiment d'être **compris, valorisé ou même choisi** peuvent aider à la formation d'un **attachement émotionnel complexe** <sup>22 45</sup>. Ainsi, bien que cette proximité affective soit **construite artificiellement** par les fraudeurs, elle facilite tout de même l'engagement dans la fraude et rend beaucoup plus **difficile le retrait, voire la remise en question de la situation** <sup>9</sup>.

Par la suite, la peur est aussi une émotion très efficace pour inhiber un doute, menant à des choix rapides. Dans le contexte de la fraude à l'investissement, cette **peur** peut être suscitée par une menace de **perte de la somme d'argent investie**, la crainte de **passer à côté d'une opportunité** qui pourrait changer notre vie, ou même parfois de **subir des conséquences légales** <sup>44</sup>. Quand une personne se trouve dans un état émotionnel négatif engageant des émotions comme la panique et l'anxiété, sa capacité à analyser l'information se voit profondément

diminuée, ce qui la rend plus **vulnérable à la persuasion** <sup>44</sup>.

Finalement, l'ensemble des dynamiques émotionnelles est d'autant **plus problématique** lorsqu'il s'accompagne d'une **faible capacité de régulation émotionnelle** <sup>9</sup>. En effet, les recherches montrent que les individus présentant une intelligence émotionnelle plus élevée ou encore une meilleure aptitude à contrôler leurs affects sont moins susceptibles d'adhérer à des scénarios frauduleux <sup>9 13</sup>. À l'inverse, les gens qui se croient intouchables en raison d'une confiance excessive dans leur capacité à prendre une décision réfléchie ou les gens avec moins de contrôle sur leurs émotions (plus impulsifs) sont plus à risque d'être affectés par ces émotions lors de leur décision <sup>22 23</sup>.

## Conclusion

Ce billet de recherche met en évidence que la fraude à l'investissement s'appuie sur l'**activation de biais cognitifs et émotionnels** profondément ancrés dans le fonctionnement humain. Ces mécanismes sont pourtant reconnus comme des **processus normaux, adaptatifs et largement partagés**, qui facilitent habituellement la prise de décision en contexte d'incertitude. Toutefois, lorsqu'ils sont **exploités** de manière intentionnelle par des fraudeurs, ces mécanismes peuvent venir **altérer l'évaluation du risque, renforcer la confiance perçue et favoriser des engagements financiers préjudiciables**, sans que les individus en aient nécessairement conscience.

Dans cette perspective, la vulnérabilité à la fraude à l'investissement ne peut être comprise comme un simple échec individuel de jugement ou de vigilance. Plutôt, les recherches mettent en évidence l'existence d'une **dimension structurelle** de la manipulation, où les fraudeurs conçoivent des **environnements informationnels, relationnels et émotionnels** spécifiquement **adaptés pour activer ces mécanismes psychologiques**. Par conséquent, les approches de prévention gagneraient à s'appuyer sur une compréhension plus poussée du fonctionnement cognitif et émotionnel humain,

plutôt que sur des discours culpabilisants centrés uniquement sur la responsabilité individuelle. Une telle orientation permettrait de mieux reconnaître la nature systémique de la fraude à l'investissement et d'envisager des stratégies de sensibilisation et de protection plus réalistes, fondées sur les **limites ordinaires du raisonnement humain** face au risque, à l'incertitude et à la promesse de gain.

Pour terminer, un tableau résumé des biais cognitifs recensés dans ce billet de recherche et spécifiques à la fraude à l'investissement a été placé ci-dessous.

## Tableau récapitulatif des biais

| Biais                                | Description                                                                              | Effet sur la victime                                                                         | Stratégie du fraudeur                                                                                                                                |
|--------------------------------------|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Biais d'autorité                     | Tendance à croire plus facilement une personne qui paraît experte, légitime ou reconnue. | La victime accorde plus de crédit aux conseils fournis sans vérifier les informations.       | Se présenter comme un "expert". Utiliser titres, jargon, logos d'institutions. Faire référence à des célébrités.                                     |
| Biais de représentativité            | Juger la crédibilité selon la ressemblance à un modèle familial (apparence).             | Confondre une apparence professionnelle avec la légitimité réelle.                           | Soigner l'interface du site d'investissement (site "pro", vidéos, photos des dirigeants, graphiques visuels) pour ressembler à une vraie entreprise. |
| Biais de disponibilité (heuristique) | Juger une situation selon un souvenir récent en mémoire.                                 | Surévaluer la normalité d'une offre ou la fréquence de réussite (souvenir de gains).         | Messages positifs constants. Annonces multiples sur les réseaux sociaux. Témoignages de réussite récents et visibles.                                |
| Biais de confiance                   | Tendance générale à faire confiance spontanément (croire avant de douter).               | Acceptation rapide d'offres ou d'interlocuteurs sympathiques et moins de vérifications.      | Simuler une proximité avec la victime. Bienveillance dans les messages (échanges personnalisés, réponses rapides).                                   |
| Biais de preuve sociale              | Tendance à suivre ce que semblent faire ou penser les autres.                            | Conformité : la victime investit parce que beaucoup y participent.                           | Afficher de faux avis et commentaires positifs. Faux volumes d'utilisateurs ou de transactions.                                                      |
| Biais d'affinité (effet de groupe)   | Faire plus confiance aux personnes perçues comme du "même groupe".                       | Abaisser la vigilance à cause d'une loyauté ou d'une identification au groupe.               | L'exploitation des liens communautaires (religion, origine, profession) et création de faux groupes d'investissement.                                |
| Biais d'optimisme                    | Minimiser la probabilité de rencontrer un événement négatif.                             | Sous-estimer les risques et croire que "ça ira bien pour moi". Faire moins de vérifications. | Présenter l'offre comme inoffensive et sûre. Insister sur l'innovation et le faible risque.                                                          |

|                                                   |                                                                                         |                                                                                                                                      |                                                                                                                                                                           |
|---------------------------------------------------|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Biais de surconfiance                             | Surestimer ses propres compétences pour évaluer / repérer une arnaque ou pour investir. | Ne pas chercher d'avis externes. Ignorer les signaux d'alerte. Continuer plutôt qu'admettre l'erreur.                                | Jouer sur l'ego de la cible (message du type "vous êtes un bon investisseur") ou cibler les profils confiants. Renforcer la confiance via des profits fictifs importants. |
| Escalade d'engagement (commitment)                | Continuer à investir pour "sauver" ce qu'on a déjà mis.                                 | Poursuite des dépôts malgré les pertes. Rationalisation des pertes.                                                                  | Demander de nouveaux versements pour "récupérer" la mise. Promesses de retraits après des dépôts supplémentaires.                                                         |
| Biais de confirmation                             | Chercher les informations qui confirment ce qu'on veut croire.                          | Ignorer ou éviter les preuves contraires. Ne retenir que les éléments rassurants.                                                    | Fournir sélectivement des preuves, faux documents ou chiffres qui vont dans le sens de l'offre proposée. Isoler les victimes dans des faux groupes d'investissement.      |
| Biais de cadrage (framing)                        | La présentation de l'information change son interprétation.                             | Percevoir une offre comme attractive si on met l'accent sur les gains plutôt que les risques.                                        | Mette de l'avant les rendements garantis, la rareté de l'offre, les gains potentiels tout minimisant les informations essentielles d'un vrai investissement.              |
| Biais d'automatisation                            | Confiance excessive dans les systèmes ou algorithmes automatisés.                       | Suivre aveuglément les recommandations "algorithmiques" sans contrôle humain. Faire confiance à une offre qui fait référence à l'IA. | Mettre de l'avant des "bots de trading" et l'IA pour légitimer l'offre. Garantir un taux de succès élevé grâce à la technologie.                                          |
| Biais d'accessibilité / de facilité (heuristique) | Préférence pour les options faciles à comprendre ou à exécuter.                         | Accepter une solution "clé en main" sans vérification. Réduction de la vigilance causée par la simplicité apparente de l'offre.      | Proposer une expérience ultra-simplifiée ("on s'occupe de tout"). Conseiller "tout prêt" qui accompagne de bout en bout. Gestion automatisée via un outil technologique.  |

# Références

- <sup>1</sup> Hidajat, T., Primiana, I., Rahman, S. et Febrian, E. (2020). Why are people trapped in Ponzi and pyramid schemes? *Journal of Financial Crime*, 28(1), 187-203. DOI : [10.1108/JFC-05-2020-0093](https://doi.org/10.1108/JFC-05-2020-0093)
- <sup>2</sup> Fischer, P., Lea, S. et Evans, K. (2009). The psychology of scams: Provoking and committing errors of judgement. Research for the Office of Fair Trading. <https://ore.exeter.ac.uk/repository/bitstream/handle/10871/20958/OfficeOfFairTrading%202009.pdf>
- <sup>3</sup> Berthet, V. (2022). The Impact of Cognitive Biases on Professionals' Decision-Making: A Review of Four Occupational Areas. *Frontiers in Psychology*, 12, 802439. DOI : [10.3389/fpsyg.2021.802439](https://doi.org/10.3389/fpsyg.2021.802439)
- <sup>4</sup> Baddeley, M. (2011). A Behavioural Analysis of Online Privacy and Security. DOI : [10.17863/CAM.1160](https://doi.org/10.17863/CAM.1160)
- <sup>5</sup> Prabowo, H. Y. (2024). When gullibility becomes us: exploring the cultural roots of Indonesians' susceptibility to investment fraud. *Journal of Financial Crime*, 31(1), 14-32. DOI : [10.1108/JFC-11-2022-0271](https://doi.org/10.1108/JFC-11-2022-0271)
- <sup>6</sup> Whitty, M. T. (2015). Mass-Marketing Fraud: A Growing Concern. *IEEE Security & Privacy*, 13(4), 84-87. DOI : [10.1109/MSP.2015.85](https://doi.org/10.1109/MSP.2015.85)
- <sup>7</sup> Loewenstein, G. F., Weber, E. U., Hsee, C. K. et Welch, N. (2001). Risk as feelings. *Psychological Bulletin*, 127(2), 267-286. DOI : [10.1037/0033-2909.127.2.267](https://doi.org/10.1037/0033-2909.127.2.267)
- <sup>8</sup> Stajano, F. et Wilson, P. (2011). Influence: Science and Practice. *Communications of the ACM*, 54(3), 70-75. DOI : [10.1145/1897852.1897872](https://doi.org/10.1145/1897852.1897872)
- <sup>9</sup> Button, M., Nicholls, C. M., Kerr, J. et Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, 47(3), 391-408. DOI : [10.1177/0004865814521224](https://doi.org/10.1177/0004865814521224)
- <sup>10</sup> Knutson, B. et Samanez-Larkin, G. S. (2014). Individual Differences in Susceptibility to Investment Fraud! Research on fraud susceptibility. <https://www.finrafoundation.org/sites/finrafoundation/files/individual-differences-in-susceptibility-to-investment-fraud.pdf>.
- <sup>11</sup> Anderson, M., March, E., Land, L. et Boshuijzen-van Burken, C. (2024). Exploring the roles played by trust and technology in the online investment fraud victimisation process. *Journal of Criminology*, 26338076241248176. DOI : [10.1177/26338076241248176](https://doi.org/10.1177/26338076241248176)
- <sup>12</sup> Rusch, J. J. (2003). The « Social Engineering » of Internet Fraud. *Computer Science, Law and Technology*. <http://taupe.free.fr/book/psycho/social%20engineering/TheSocial%20Engineering%20of%20Internet%20Fraud.pdf>
- <sup>13</sup> Hanoch, Y. et Wood, S. (2021). The Scams Among Us: Who Falls Prey and Why. *Current Directions in Psychological Science*, 30(3), 260-266. DOI : [10.1177/0963721421995489](https://doi.org/10.1177/0963721421995489)
- <sup>14</sup> Junger, M., Koning, L., Hartel, P. et Veldkamp, B. (2023). In their own words: deception detection by victims and near victims of fraud. *Frontiers in Psychology*, 14, 1135369. DOI : [10.3389/fpsyg.2023.1135369](https://doi.org/10.3389/fpsyg.2023.1135369)
- <sup>15</sup> Atkins, B. et Huang, W. (2013). A Study of Social Engineering in Online Frauds. *Open Journal of Social Sciences*, 01(03), 23-32. DOI : [10.4236/jss.2013.13004](https://doi.org/10.4236/jss.2013.13004)
- <sup>16</sup> Chang, J. (2008). An analysis of advance fee fraud on the internet. *Journal of Financial Crime*, 15(1), 71-81. DOI : [10.1108/13590790810841716](https://doi.org/10.1108/13590790810841716)
- <sup>17</sup> Muscanell, N. L., Guadagno, R. E. et Murphy, S. (2014). Weapons of Influence Misused: A Social Influence Analysis of Why People Fall Prey to Internet Scams. *Social and Personality Psychology Compass*, 8(7), 388-396. DOI : [10.1111/spc3.12115](https://doi.org/10.1111/spc3.12115)

- <sup>18</sup> Whitty, M. T. (2013). The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam. *British Journal of Criminology*, 53(4), 665-684. DOI : [10.1093/bjc/azt009](https://doi.org/10.1093/bjc/azt009)
- <sup>19</sup> Tversky, A. et Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science*, 185(4157), 1124-1131.
- <sup>20</sup> Chang, J. et Chong, M. D. (2022). Cognitive heuristics and risk evaluation in crisis fraud. *Journal of Financial Crime*, 29(2), 447-459. DOI : [10.1108/JFC-02-2021-0030](https://doi.org/10.1108/JFC-02-2021-0030)
- <sup>21</sup> Whittaker, J. M., Edwards, M., Cross, C. et Button, M. (2022). "I Have Only Checked after the Event": Consumer Approaches to Safe Online Shopping. *Victims & Offenders*, 18(7), 1259-1281. DOI : [10.1080/15564886.2022.2130486](https://doi.org/10.1080/15564886.2022.2130486)
- <sup>22</sup> 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)
- <sup>23</sup> 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)
- <sup>24</sup> Sari, M. et Nugraha, N. (2016). Cognitive Bias and Risk Preferences Analysis of Ponzi Scheme Investors. 2016 Global Conference on Business, Management and Entrepreneurship, Bandung, Indonesia. DOI : [10.2991/gcbme-16.2016.23](https://doi.org/10.2991/gcbme-16.2016.23)
- <sup>25</sup> 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)I), 387-393. DOI : [10.22610/imbr.v15i4\(SI\)I.3613](https://doi.org/10.22610/imbr.v15i4(SI)I.3613)
- <sup>26</sup> Subburayan, B. (2023). Case Study on Social Media Scam Artists Prey on India's Amateur Investors. *SSRN Electronic Journal*. DOI : [10.2139/ssrn.4405217](https://doi.org/10.2139/ssrn.4405217)
- <sup>27</sup> Fairfax, L. M. (2006). « With Friends Like These... ». Toward a More Efficacious Response to Affinity-Based Securities and Investment Fraud. *FinPlanRN: Consumer Protection Policies & Regulation* (Topic). <https://ssrn.com/abstract=921074>
- <sup>28</sup> Perri, F. S. et Brody, R. G. (2012). The optics of fraud: affiliations that enhance offender credibility. *Journal of Financial Crime*, 19(3), 305-320. DOI : [10.1108/13590791211243147](https://doi.org/10.1108/13590791211243147)
- <sup>29</sup> Ullah, I., Ahmad, W. et Ali, A. (2022). Determinants of investment decision in a Ponzi scheme: Investors' perspective on the Modaraba scam. *Journal of Financial Crime*, 29(4), 1172-1190. DOI : [10.1108/JFC-02-2020-0027](https://doi.org/10.1108/JFC-02-2020-0027)
- <sup>30</sup> Muchnik, L., Aral, S. et Taylor, S. J. (2013). Social Influence Bias: A Randomized Experiment. *Science*, 341(6146), 647-651. DOI : [10.1126/science.1240466](https://doi.org/10.1126/science.1240466)
- <sup>31</sup> Lacey, D., Goode, S., Pawada, J. et Gibson, D. (2020). The application of scam compliance models to investment fraud offending. *Journal of Criminological Research, Policy and Practice*, 6(1), 65-81. DOI : [10.1108/JCRPP-12-2019-0073](https://doi.org/10.1108/JCRPP-12-2019-0073)
- <sup>32</sup> 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)
- <sup>33</sup> 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)
- <sup>34</sup> Whitty, M. T. (2020). Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims. *European Journal on Criminal Policy and Research*, 26(3), 399-409. DOI : [10.1007/s10610-020-09458-z](https://doi.org/10.1007/s10610-020-09458-z)
- <sup>35</sup> Kahneman, D. et Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, 47(2), 263. DOI : [10.2307/1914185](https://doi.org/10.2307/1914185)

<sup>36</sup> Nickerson, R. S. (1998). Confirmation Bias: A Ubiquitous Phenomenon in Many Guises. *Review of General Psychology*, 2(2), 175-220.

[DOI : 10.1037/1089-2680.2.2.175](https://doi.org/10.1037/1089-2680.2.2.175)

<sup>37</sup> Hilton, D. J. (2001). The Psychology of Financial Decision-Making: Applications to Trading, Dealing, and Investment Analysis. *Journal of Psychology and Financial Markets*, 2(1), 37-53.

[DOI : 10.1207/S15327760JPFM0201\\_4](https://doi.org/10.1207/S15327760JPFM0201_4)

<sup>38</sup> Wen, X., Xu, L., Wang, J., Gao, Y., Shi, J., Zhao, K., Tao, F. et Qian, X. (2022). Mental States: A Key Point in Scam Compliance and Warning Compliance in Real Life. *International Journal of Environmental Research and Public Health*, 19(14), 8294. [DOI : 10.3390/ijerph19148294](https://doi.org/10.3390/ijerph19148294)

<sup>39</sup> Shukla, S. et Shukla, S. K. (2023). Impact of Automation Bias and Status Quo Bias on Capital Market Investment Decisions of Indian Investors: An Explanatory Research. *Financial Markets, Institutions and Risks*, 1-11. [DOI : 10.61093/fmir.7\(3\).1-11.2023](https://doi.org/10.61093/fmir.7(3).1-11.2023)

<sup>40</sup> Packin, N. G. (2019). Consumer Finance and AI: The Death of Second Opinions? *New York University Journal of Legislation and Public Policy* (2020). <https://ssrn.com/abstract=3361639>

<sup>41</sup> Kahneman, D. (2003). A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist*, 58(9), 697-720. [DOI : 10.1037/0003-066X.58.9.697](https://doi.org/10.1037/0003-066X.58.9.697)

<sup>42</sup> Shah, A. K. et Oppenheimer, D. M. (2009). The Path of Least Resistance: Using Easy-to-Access Information. *Current Directions in Psychological Science*, 18(4), 232-236. [DOI : 10.1111/j.1467-8721.2009.01642.x](https://doi.org/10.1111/j.1467-8721.2009.01642.x)

<sup>43</sup> Cole, T. (2022). Exploring Online Fraudsters Decision-Making Processes [Georgia State University]. [https://scholarworks.gsu.edu/ayspss\\_dissertations/50](https://scholarworks.gsu.edu/ayspss_dissertations/50)

<sup>44</sup> Norris, G. et Brookes, A. (2021). Personality, emotion and individual differences in response to online fraud. *Personality and Individual Differences*, 169, 109847. [DOI : 10.1016/j.paid.2020.109847](https://doi.org/10.1016/j.paid.2020.109847)

<sup>45</sup> Ross, S. et Smith, R. (2011). Risk factors for advance fee fraud victimisation. *Australian Institute of Criminology*. [DOI : 10.52922/ti268334](https://doi.org/10.52922/ti268334)