

Transformation du paysage de la fraude aux investissements : L'exploitation ciblée du biais cognitif du FOMO par l'Intelligence Artificielle générative.

Auteur : Cols, Quentin

Promoteur(s) : Dantine, Michaël

Faculté : Faculté de Droit, de Science Politique et de Criminologie

Diplôme : Master en criminologie à finalité spécialisée en organisations criminelles et analyse du crime

Année académique : 2025-2026

URI/URL : <http://hdl.handle.net/2268.2/26668>

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.

Transformation du paysage de la fraude aux investissements :
L'exploitation ciblée du biais cognitif du FOMO par
l'Intelligence Artificielle générative.

Quentin COLS

Travail de fin d'études en vue de l'obtention du grade de Master en Criminologie, à finalité
spécialisée en organisations criminelles et analyse du crime.

Année académique 2025-2026

Recherche menée sous la direction de Monsieur Michaël DANTINNE

Professeur à l'Université de Liège.

Remerciements

Tout d'abord, je tiens à remercier chaleureusement mon promoteur, Monsieur Michaël Dantinne, pour son accompagnement assidu et ses conseils avisés tout au long de cette recherche. Ses réflexions et son expertise sur les différentes thématiques ont largement contribué à la configuration et à la mise en œuvre de ce travail. Je lui suis sincèrement reconnaissant pour son appui constant ainsi que pour le temps précieux accordé à la lecture et aux diverses corrections apportées.

Ensuite, je tiens à remercier l'ensemble des personnes ayant contribué, de près ou de loin, à la réalisation de ce travail. Un grand merci au département de criminologie pour l'organisation des séances TFE, ainsi qu'à mes collègues étudiants pour leur soutien et leur écoute durant cette longue étude.

Pour finir, je remercie également mes proches et ma famille pour leur participation active. Que ce soit par de simples encouragements, des conseils avisés ou des relectures attentives de mon travail, leur aide m'a été précieuse. Je souhaite remercier tout particulièrement Lucas et Aurélie pour leur soutien indéfectible.

Table des matières

Abstract.....	5
Partie I : Introduction	6
Partie II : Revue de littérature	7
Chapitre 1 : Les fraudes aux investissements	7
<i>Section 1.1 : Définition et contextualisation</i>	<i>7</i>
<i>Section 1.2 : Fondements théoriques : le triangle de la fraude.....</i>	<i>8</i>
<i>Section 1.3 : L'ingénierie sociale</i>	<i>9</i>
Chapitre 2 : L'intelligence artificielle (IA)	9
<i>Section 2.1 : Définitions et contextualisation</i>	<i>10</i>
<i>Section 2.2 : Fonctionnement de l'IA.....</i>	<i>11</i>
<i>Section 2.3 : Impact sociétal.....</i>	<i>12</i>
Chapitre 3 : Le biais psychologique du FOMO (<i>Fear of Missing Out</i>).....	12
<i>Section 3.1 : Définition et contextualisation</i>	<i>13</i>
<i>Section 3.2 : Cadre théorique : la théorie de l'autodétermination (SDT).....</i>	<i>13</i>
<i>Section 3.3 : Le mécanisme cognitif de Kahneman</i>	<i>14</i>
Chapitre 4 : Convergence technologique (IA) et psychologique (FOMO) dans le monde financier	14
<i>Section 4.1 : Utilisation du langage technique : entre personnalisation et ingénierie sociale</i>	<i>15</i>
<i>Section 4.2 : Pression temporelle : l'extrême exclusivité</i>	<i>15</i>
<i>Section 4.3 : Deepfakes : entre autorité et preuve sociale.....</i>	<i>15</i>
Partie III : Recherche empirique.....	16
Chapitre 1 : Objectifs et hypothèses de recherche	16
H1 : Le langage technique	16
H2 : La pression temporelle	17
H3 : Les deepfakes	17
Chapitre 2 : Méthodologie	17
<i>Section 2.1 : Échantillon.....</i>	<i>18</i>
<i>Section 2.2 : Procédure.....</i>	<i>18</i>
<i>Section 2.3 : Mesures</i>	<i>18</i>
<i>Section 2.4 : Plan d'analyse</i>	<i>19</i>
Chapitre 3 : Résultats	19
<i>Section 3.1 : Analyses statistiques descriptives</i>	<i>19</i>
Profil sociodémographique et habitudes financières	19
Échelle du FOMO : validation et statistiques.....	21
<i>Section 3.2 : Analyse statistique analytique (corrélation)</i>	<i>21</i>
H1 : le langage technique	21

H2 : la pression temporelle	23
H3 : la preuve sociale (<i>deepfakes</i>)	25
Analyses transversales : comparaison inter-scenarii et hiérarchisation des variables	26
Chapitre 4 : Discussion	28
<i>Section 4.1 : Profils socio-démographiques</i>	28
<i>Section 4.2 : Les habitudes financières</i>	29
<i>Section 4.3 : Hypothèse 1 : le langage technique</i>	29
<i>Section 4.4 : Hypothèse 2 : la pression temporelle</i>	30
<i>Section 4.5 : Hypothèse 3 : les deepfakes</i>	32
<i>Section 4.6 : Analyses transversales : comparaison inter-scenarii</i>	33
Chapitre 5 : Limites de l'étude	35
Chapitre 6 : Perspectives de la recherche	36
Partie IV : Conclusion	37
Bibliographie	38
Annexes	43

Abstract

L'année 2026 est marquée par l'explosion de l'Intelligence Artificielle qui, bien que ses fondements théoriques remontent à l'Antiquité, a profondément reconfiguré la cybercriminalité financière et la fraude aux investissements en ligne en Belgique. Cette recherche en criminologie analyse comment l'IA générative s'associe à l'ingénierie sociale pour manipuler le biais psychologique du *FOMO* (*Fear of Missing Out*) afin de neutraliser la vigilance des internautes. Pour ce faire, une méthodologie quantitative et corrélationnelle a été déployée auprès d'un échantillon de la population belge. Trois hypothèses majeures y sont testées : l'influence d'un jargon technico-financier irréprochable généré par les grands modèles de langage (LLM), l'impact d'une pression temporelle accrue, et l'usage de *deepfakes* comme vecteurs d'autorité. Les résultats valident l'ensemble des hypothèses et révèlent une hiérarchisation claire des vulnérabilités : l'utilisation d'un jargon fluide et rigoureux s'avère être le levier de manipulation le plus redoutable. La pression temporelle et les *deepfakes* audiovisuels agissent quant à eux comme des catalyseurs émotionnels secondaires significatifs. En démontrant que l'IAg redéfinit la hiérarchie des vulnérabilités humaines, cette étude offre des clés analytiques indispensables pour orienter les futures stratégies de sensibilisation et de cyber-défense face à la manipulation comportementale automatisée.

Mots-clés : Intelligence Artificielle générative, Fraude aux investissements, FOMO, Ingénierie sociale, Biais cognitifs.

The year 2026 is marked by the explosion of Artificial Intelligence which, although its theoretical foundations date back to Antiquity, has profoundly reconfigured financial cybercrime and online investment fraud in Belgium. This criminological research analyzes how generative AI combines with social engineering to manipulate the psychological bias of FOMO (Fear of Missing Out) in order to bypass internet users' vigilance. To achieve this, a quantitative and correlational methodology was deployed among a sample of the Belgian population. Three major hypotheses are tested: the influence of flawless technical-financial jargon generated by large language models (LLMs), the impact of increased time pressure, and the use of *deepfakes* as vectors of authority. The results validate all hypotheses and reveal a clear hierarchy of vulnerabilities: the use of fluent and rigorous jargon proves to be the most formidable lever of manipulation. Meanwhile, time pressure and audiovisual *deepfakes* act as significant secondary emotional catalysts. By demonstrating that generative AI redefines the hierarchy of human vulnerabilities, this study offers essential analytical keys to guide future awareness and cyber-defense strategies against automated behavioral manipulation.

Keywords: Generative Artificial Intelligence, Investment fraud, FOMO, Social engineering, Cognitive biases.

Partie I : Introduction

L'avènement de la révolution numérique et l'essor fulgurant des technologies ont profondément reconfiguré l'organisation de nos sociétés, ouvrant la voie à des innovations majeures, mais redéfinissant simultanément les opportunités délictueuses. Parmi ces mutations technologiques, l'émergence de l'Intelligence Artificielle générative (IAg) marque un tournant critique. Capable de produire des contenus textuels, audio et visuels d'une cohérence et d'un réalisme autrefois impossibles à automatiser, cette technologie s'est rapidement imposée comme un puissant vecteur d'optimisation pour la cybercriminalité financière (TRM Labs¹, 2024). Parallèlement, le paysage de la finance a vu proliférer des formes de criminalité de masse particulièrement sophistiquées, au premier rang desquelles figurent les fraudes aux investissements. En Belgique, ce phénomène a atteint un seuil d'alarme sans précédent : au cours du seul premier semestre de l'année 2025, les pertes liées aux fraudes en ligne se sont élevées à un montant record de 15 millions d'euros (CCB², 2025).

Pourtant, l'efficacité redoutable de ces escroqueries modernes ne réside pas uniquement dans leur sophistication technique. Elle repose fondamentalement sur l'art de l'ingénierie sociale, discipline psychologique visant à exploiter systématiquement la « faille humaine » pour transformer la victime en un complice involontaire de sa propre spoliation (Vishwanath et al., 2011). À cet égard, les organisations criminelles ne se contentent plus de diffuser des messages d'hameçonnage³ artisanaux. Elles articulent désormais les capacités d'industrialisation et de personnalisation de l'IA générative avec la manipulation ciblée de nos vulnérabilités cognitives individuelles. Au cœur de ces vulnérabilités se trouve un biais psychologique contemporain exacerbé par l'usage des réseaux sociaux : le syndrome du FOMO (*Fear of Missing Out*), ou la peur de manquer une opportunité unique (Przybylski et al., 2013). Ancré dans l'anxiété sociale et le besoin fondamental d'appartenance, le FOMO place les individus dans un état de réceptivité émotionnelle exacerbée. En saturant le « Système 1 » — notre mode de pensée rapide, intuitif et émotionnel théorisé par Daniel Kahneman (2011) — au détriment du « Système 2 » analytique, ce biais court-circuite le raisonnement critique et désarme les réflexes de vigilance. Les fraudeurs exploitent délibérément ce levier en appliquant des stratégies de compression temporelle, de jargon technique hyperréaliste (Wan Fakhruddin et al., 2026) ou d'autorité factice via des *deepfakes* (Vaccari & Chadwick, 2020).

L'intérêt majeur de cette étude réside d'abord dans son actualité et son urgence sociopolitique. Alors que les autorités publiques et les institutions bancaires belges font face à une explosion des plaintes liées aux escroqueries financières en ligne, les modes opératoires évoluent plus vite que les campagnes de prévention traditionnelles. Comprendre la dynamique exacte de cette criminalité de masse constitue un enjeu de sécurité publique crucial pour endiguer des pertes financières qui impactent lourdement l'économie des ménages. Sur le plan scientifique et interdisciplinaire, l'intérêt de ce travail repose sur le décroisement des savoirs. En combinant la criminologie, la psychologie cognitive et l'analyse technologique de l'IAg, cette recherche comble un fossé important de la littérature actuelle. Si la littérature existante traite abondamment de la fraude d'une part, et de l'intelligence artificielle d'autre part, la convergence systémique entre les avancées linguistiques des grands modèles de langage (LLM) et l'exploitation clinique de biais psychologiques comme le FOMO reste encore largement sous-explorée. Enfin, l'intérêt de cette recherche est fondamentalement pratique et préventif. En mettant en lumière le paradoxe cognitif de l'internaute — souvent trop confiant dans ses capacités théoriques à

¹ Entreprise de technologie spécialisée dans l'intelligence blockchain qui fournit des solutions d'investigation criminologique (*blockchain forensics*).

² Centre pour la Cybersécurité Belgique.

³ Fait d'attirer l'internaute sur un faux site pour récupérer ses coordonnées personnelles ou bancaires.

déceler un piège, mais démuni face à l'hyper-réalisme textuel de l'IA (Przybylski et al., 2013) —, cette étude ambitionne de fournir des clés analytiques concrètes. Les conclusions issues de cette analyse ont pour vocation d'orienter les futures stratégies de sensibilisation des cyber-défenseurs et de proposer des pistes de remédiation face à la manipulation comportementale automatisée.

C'est précisément au cœur de ces enjeux que se positionne notre réflexion, guidée par la problématique fondamentale suivante : « *Dans quelle mesure l'utilisation ciblée de l'Intelligence Artificielle générative, à travers l'exploitation des leviers cognitifs et émotionnels liés au biais du FOMO, reconfigure-t-elle le paysage de la fraude aux investissements ?* ». L'objectif principal de cette recherche est de cerner l'articulation entre les capacités techniques d'automatisation des discours persuasifs, via l'IA générative, et la réceptivité psychologique des victimes afin de proposer des clés de lecture actualisées face aux nouvelles dynamiques cybercriminelles.

Pour répondre à cet objectif, ce mémoire adopte une approche méthodologique mixte et se structure en deux grandes parties distinctes. Il se divise d'abord en une phase théorique (revue de littérature) dédiée à l'examen conceptuel des composantes de la fraude, de l'IA générative et du biais du FOMO, suivie d'une étude empirique (approche quantitative par scénarii), dont la synthèse permettra d'établir d'éventuelles convergences entre la recherche théorique et la pratique comportementale observée sur le terrain.

Partie II : Revue de littérature

La revue de littérature est structurée en quatre étapes : après avoir défini successivement les fraudes aux investissements, le rôle de l'IA et le concept psychologique de FOMO, nous aborderons leur interaction systémique au sein de l'ingénierie sociale.

Chapitre 1 : Les fraudes aux investissements

Après une mise en contexte et une définition des fraudes aux investissements, ce chapitre explore les mécanismes du triangle de la fraude (pression, opportunité et rationalisation). Cette approche théorique permet d'introduire l'étude de l'ingénierie sociale, outil central utilisé par les fraudeurs pour contourner la vigilance de leurs victimes.

Section 1.1 : Définition et contextualisation

La fraude est une infraction complexe caractérisée par une intention délibérée de tromper autrui en contournant les cadres légaux (Larousse, s. d.). La littérature académique et juridique s'accorde sur une structure multidimensionnelle reposant sur quatre piliers fondamentaux : l'intention malveillante, le déploiement de manœuvres sophistiquées, l'obtention d'un bénéfice indu et le préjudice subi (Mouton et al., 2016 ; Europol, 2023), une dynamique aujourd'hui optimisée par l'expertise numérique et l'analyse de données (Bädele, 2021 ; Ivan, 2022). Dans le champ financier, la fraude aux investissements amène une victime à effectuer une transaction sur la base d'informations trompeuses — promesses de rendements irréalistes et risques minimisés (Larousse, s. d. ; Quisenberry, 2017) —, un engagement qui contredit pourtant les principes fondamentaux de l'économie de marché (Quisenberry, 2017).

Ce phénomène s'inscrit dans la théorie des activités routinières, où l'acte délictuel émerge de la convergence spatio-temporelle d'un agresseur motivé, d'une cible vulnérable et de l'absence d'un gardien vigilant (Cohen & Felson, 1979). L'expansion technologique a démultiplié ces opportunités en créant de

nouveaux espaces de vulnérabilité numérique (Wolfe & Hermanson, 2004). Les modes opératoires contemporains privilégient une approche multicanale (téléphone, réseaux sociaux, messageries) pour instaurer un climat d'intimité propice à l'hameçonnage (Appel et al., 2020 ; Europol, 2023 ; CVMO⁴, 2025). Séduit par des promesses de gains élevés, l'investisseur consent à une mise de départ modeste — environ 250 € en Belgique (CCB, 2025 ; FSMA⁵, 2025). Ce premier engagement mineur agit comme un catalyseur psychologique (Baumeister & Leary, 1995 ; Beyens et al., 2016) : il cible la « pensée rapide » (Système 1), intuitive et émotionnelle, pour contourner le raisonnement analytique (système 2) (Kahneman, 2011 ; Mouton et al., 2016 ; Ivantchev & Ivantcheva, 2024).

L'année 2025 marque un seuil critique : au premier semestre, les pertes liées aux fraudes en ligne en Belgique ont atteint un record de 15 millions d'euros, dont 12 millions imputables aux cryptomonnaies et plateformes de trading (CCB, 2025 ; FSMA, 2025). Les 1.289 plaintes enregistrées ne constituent que la partie émergée de l'iceberg. Entravées par la honte ou la crainte du jugement social (*victim blaming*), de nombreuses victimes s'enferment dans le mutisme, alimentant le « chiffre noir » de la criminalité (Baumeister & Leary, 1995 ; Kahneman, 2011 ; FINRA⁶ Investor Education Foundation, & AARP, 2022 ; Hock & Button, 2023). Pourtant, le préjudice outrepassa la perte matérielle — moyenne de 37.778 € par individu (CCB, 2025) — pour engendrer des traumatismes cliniques, des états dépressifs et un isolement durable (Hock & Button, 2023 ; OSC & BIT⁷, 2024). À l'échelle macroéconomique, cette recrudescence des fraudes provoque une érosion systémique de la confiance envers les institutions financières et l'innovation technologique. En 2023, environ 70 % des investisseurs exprimaient déjà une vive inquiétude quant à la sécurité de leurs actifs face aux nouvelles capacités de l'intelligence artificielle (Ivan, 2022 ; Sholademi, 2024). En l'absence d'une réponse technologique et éthique rigoureuse, cette méfiance risque de freiner durablement la participation des citoyens aux marchés financiers licites, entravant ainsi le financement de l'économie réelle (Singh Chauhan, 2025 ; Sun et al., 2025). En somme, une population de plus en plus consciente des risques de malversation manifeste une réticence croissante à l'égard de l'acte d'investir.

En conclusion, la fraude aux investissements constitue un défi persistant pour les régulateurs et les épargnants (Europol, 2023 ; CVMO, 2024). Elle impose une vigilance accrue dans l'identification des signaux d'alerte, tels que les promesses de rendements garantis ou l'incitation à une prise de décision hâtive, afin de prévenir des préjudices financiers souvent irréversibles (Przybylski et al., 2013 ; Wan Fakhruddin et al., 2026). Pour se prémunir, les citoyens doivent mobiliser leur raisonnement analytique (Système 2) afin de neutraliser ces biais (Kahneman, 2011), la connaissance des modes opératoires réduisant significativement le risque de victimisation (Vishwanath et al., 2011 ; Whittaker et al., 2025).

Section 1.2 : Fondements théoriques : le triangle de la fraude

Pour analyser le passage à l'acte, la littérature s'est historiquement référée au « Triangle de la fraude » de Cressey (1953), postulant la coexistence de la pression — un besoin financier —, de l'opportunité — une faille perçue dans le système —, et de la rationalisation — la justification mentale de l'acte malhonnête (Pluchart, 2019 ; Sun et al., 2025). Face à la sophistication de la criminalité financière, Wolfe et Hermanson (2004) ont enrichi ce cadre en établissant le « Diamant de la fraude »,

⁴ Commission des valeurs mobilières de l'Ontario.

⁵ Autorité des services et marchés financiers. La FSMA exerce, aux côtés de la Banque Nationale de Belgique (BNB), le contrôle du secteur financier belge.

⁶ Fondation spécialisée sur la victimisation chronique dans le domaine des fraudes financières et les arnaques aux investissements.

⁷ Ontario Securities Commission, & Behavioural Insights Team. Organisme financier officiel de la province de l'Ontario.

qui introduit une quatrième composante : la capacité (traits de personnalité et compétences techniques du fraudeur).

Dans le paysage actuel, l'intelligence artificielle générative agit comme un multiplicateur de cette capacité (Blauth et al., 2022 ; Europol, 2023 ; Whittaker et al., 2025). Elle permet à des acteurs peu qualifiés de déployer des attaques automatisées d'une complexité professionnelle : génération de faux témoignages, publicités ciblées et *deepfakes* de personnalités publiques (Blauth et al., 2022 ; Jia & Li, 2025 ; Whittaker et al., 2025). Ces stimuli techniques sont spécifiquement calibrés pour exploiter le stress lié au syndrome du FOMO en instaurant un sentiment d'exclusivité et d'urgence (Przybylski et al., 2013 ; Milyavskaya et al., 2018), dynamique qui sera approfondie au chapitre 4.

Section 1.3 : L'ingénierie sociale

L'efficacité des fraudes repose sur l'exploitation de la « faille humaine » via l'ingénierie sociale, une stratégie plus rentable et moins coûteuse que le piratage technique (Mouton et al., 2016 ; ESET⁸, 2025 ; Sun et al., 2025). Cette discipline détourne les principes fondamentaux de la psychologie sociale afin d'amener une cible à agir contre ses propres intérêts (Kahneman, 2011 ; Mouton et al., 2016 ; Hock & Button, 2023). Dans cette perspective, la victime peut être considérée comme un « complice involontaire » de sa propre spoliation (CCB, 2025). La technique vise à inciter l'individu à compromettre sa propre sécurité, que ce soit par la divulgation d'informations confidentielles (identifiants, données bancaires), l'exécution d'actions préjudiciables (transferts de fonds) ou l'octroi d'accès non autorisés à des systèmes protégés (Mouton et al., 2016 ; ESET, 2025). Selon le rapport annuel d'ESET (2025), l'ingénierie sociale s'est imposée comme la méthode privilégiée des cybercriminels en raison de ses coûts opérationnels réduits et d'une temporalité d'exécution plus courte par rapport aux tentatives de compromission de systèmes informatiques, dont la sécurité est de plus en plus robuste.

Sa manifestation la plus fréquente est l'hameçonnage (aussi connu sous le nom de *phishing*), dont la crédibilité repose sur une architecture de persuasion en trois axes : une sémiotique visuelle institutionnelle (légitimité graphique), l'invocation d'une autorité feinte (experts ou régulateurs) et l'exploitation de la preuve sociale par de faux témoignages pour stimuler un comportement mimétique (Kahneman, 2011 ; Mouton et al., 2016 ; Wan Fakhruddin et al., 2026). Pour précipiter la décision avant toute vérification (*due diligence*), les fraudeurs emploient des stratégies de compression temporelle (Ye & Chen, 2022, cité dans Wan Fakhruddin et al., 2026). Le langage de l'urgence fonctionne comme un levier réduisant la réflexion critique, articulé autour de « l'évitement de la perte » : l'individu est statistiquement plus motivé par la crainte de manquer une opportunité que par l'espoir d'un profit (Lyu et al., 2025 ; Wan Fakhruddin et al., 2026). Enfin, l'usage des *deepfakes* et la personnalisation des messages par l'IA augmentent drastiquement les taux de conversion en rendant la simulation indiscernable du réel (Blauth et al., 2022 ; Whittaker et al., 2025).

Chapitre 2 : L'intelligence artificielle (IA)

Ce deuxième chapitre propose d'abord une définition et une mise en contexte de l'intelligence artificielle, étayées par une revue des sources académiques de référence. Nous détaillons ensuite les principes fondamentaux de son fonctionnement technique. Enfin, une dernière section s'appuie sur des

⁸ Entreprise mondiale de cybersécurité, d'origine slovaque et fondée en 1992, spécialisée dans le développement de logiciels de protection.

recherches empiriques internationales pour analyser l'impact sociétal de l'IA et les transformations qu'elle engendre.

Section 2.1 : Définitions et contextualisation

L'essor de l'intelligence artificielle (IA) marque une révolution technologique majeure, offrant simultanément des opportunités d'innovation et des outils d'une puissance inédite pour la cybercriminalité financière (Ivan, 2022 ; Singh Chauhan, 2025). Dans ce secteur, elle permet désormais la conception de scénarii d'arnaques ultra-crédibles, personnalisés et déployables à l'échelle mondiale (Blauth et al., 2022). Fondamentalement, l'IA se définit comme la capacité de programmes informatiques à simuler un comportement intelligent (Haiech, 2020 ; Gefen, 2022 ; Hu, 2023 ; Oxford English Dictionary, 2023). Bien que cette technologie sature l'actualité contemporaine, ses racines intellectuelles plongent jusqu'à l'Antiquité à travers les automates de Héron d'Alexandrie⁹, dont les mécanismes reposaient déjà sur des principes de régulation cybernétique (Larousse, s. d. ; Gefen, 2022 ; Haiech, 2020 ; Raulin, 2022). Le tournant scientifique moderne s'opère toutefois en 1950 sous l'impulsion d'Alan Turing¹⁰. Dans son article fondateur, il introduit le « jeu de l'imitation », postulant que l'intelligence réside dans la capacité d'une machine à produire un simulacre de psychologie humaine si abouti qu'un observateur ne peut plus distinguer l'humain de l'automate (Larousse, s. d. ; Haiech, 2020 ; Raulin, 2022 ; Oxford English Dictionary, 2023). Le terme est officiellement consacré en juillet 1956 par John McCarthy¹¹ lors de la conférence de Dartmouth¹² (Haiech, 2020 ; Hu, 2023), avant que la norme ISO de 1995 ne stabilise cette définition comme la faculté d'une unité fonctionnelle à exécuter des fonctions associées à l'intelligence humaine, telles que le raisonnement et l'apprentissage (Raulin, 2022 ; OCDE¹³, 2025). Sur le plan législatif, l'Union européenne a clarifié ce cadre via le *EU AI Act*. Ce texte définit un système d'IA comme un système fondé sur une logique logicielle ou matérielle capable, selon des objectifs fixés par l'humain, de générer des contenus, des prédictions, des recommandations ou des décisions influençant les environnements réels ou virtuels avec lesquels il interagit (European Commission, 2021 ; Europol, 2023 ; Singh Chauhan, 2025 ; OCDE, 2025).

La littérature distingue classiquement deux trajectoires : l'IA faible (ou étroite) et l'IA forte (ou générale). L'IA faible regroupe des systèmes conçus pour accomplir une tâche spécifique, comme la reconnaissance faciale, mais s'avère incapable de transférer ses compétences ou de s'adapter à l'imprévu (Haiech, 2020 ; Raulin, 2022 ; Hu, 2023). Dépourvue de conscience globale, elle constitue à ce jour l'unique forme d'IA opérationnelle (Haiech, 2020 ; Singh Chauhan, 2025). À l'inverse, l'IA forte (AGI) désigne une machine théorique dotée d'une conscience et capable de comprendre n'importe quelle tâche intellectuelle humaine (Gefen, 2022 ; Hu, 2023).

⁹ Ingénieur, mécanicien et mathématicien grec du I^{er} siècle apr. J.-C., célèbre pour ses traités scientifiques novateurs et ses inventions révolutionnaires telles que l'éolipyle (première machine à vapeur) et la fontaine de Héron, jetant ainsi les bases de l'automatisme et de la géométrie appliquée.

¹⁰ Mathématicien, logicien et cryptologue britannique du XX^e siècle, considéré comme l'un des pères fondateurs de l'informatique moderne et de l'intelligence artificielle pour avoir conceptualisé la machine de Turing, décrypté la machine de chiffrement allemande Enigma durant la Seconde Guerre mondiale, et posé les bases théoriques de l'apprentissage automatique (Test de Turing).

¹¹ Informaticien et logicien américain du XX^e siècle, considéré comme l'un des pères fondateurs de l'intelligence artificielle pour avoir inventé le terme lui-même en 1955 et pour avoir organisé la célèbre conférence de Dartmouth en 1956.

¹² Événement scientifique historique considéré comme l'acte de naissance officiel de l'intelligence artificielle en tant que discipline de recherche autonome.

¹³ Organisation de coopération et de développement économiques.

Entre ces deux pôles s'inscrit l'Intelligence Artificielle Générative (IAg), sous-catégorie de l'IA faible capable de créer du contenu nouveau et original plutôt que de simplement classifier des données (Singh Chauhan, 2025). Bien qu'elle surpasse l'humain dans des tâches spécialisées (Gefen, 2022 ; Sholademi, 2024 ; Sun et al., 2025), elle illustre la métaphore de la « chambre chinoise ¹⁴ » de Searle : elle manipule des symboles avec brio sans en saisir le sens profond (Haiech, 2020 ; Gefen, 2022 ; Raulin, 2022). Pour de nombreux experts, l'IA générative actuelle constitue néanmoins un tremplin indispensable vers l'AGI (Europol, 2023 ; Jia & Li, 2025).

Section 2.2 : Fonctionnement de l'IA

L'essor technologique de la dernière décennie est intrinsèquement lié au Machine Learning (ML), ou apprentissage automatique, qui permet aux machines d'identifier des modèles par l'expérience (Bădele, 2021 ; Singh Chauhan, 2025). Un saut qualitatif s'est opéré avec l'avènement du Deep Learning (apprentissage profond), une branche avancée du ML exploitant des réseaux de neurones artificiels multicouches pour analyser des données complexes (Raulin, 2022). Cette évolution a permis l'émergence des réseaux antagonistes génératifs (GANs) en 2014 (Goodfellow et al., 2014 ; Gefen, 2022), puis le tournant majeur de l'IA générative (IAg) via l'introduction des modèles *Generative Pre-trained Transformer* (GPT) en 2018 (Europol, 2023 ; Singh Chauhan, 2025).

Le fonctionnement de l'IAg repose principalement sur deux piliers technologiques. Le premier concerne les Large Language Models (LLM), basés sur l'architecture des *Transformers*. Ces programmes excellent dans le traitement du langage humain en utilisant un mécanisme d'auto-attention qui leur permet de saisir l'importance relative de chaque mot dans une séquence pour en comprendre le contexte global (Hu, 2023 ; Singh Chauhan, 2025). En prédisant statistiquement le mot suivant, les LLM génèrent des discours d'une cohérence humaine, avec une capacité de traitement passée de 2.500 mots à près de 5 millions pour les modèles les plus récents comme Google Gemini (Jia & Li, 2025). Le second pilier repose sur les Réseaux Antagonistes Génératifs (GANs), une architecture mettant en compétition un « générateur » chargé de créer du contenu synthétique et un « discriminateur » chargé d'en évaluer l'authenticité (Goodfellow et al., 2014). Cette lutte itérative permet d'atteindre un tel degré de réalisme que le média produit devient virtuellement indiscernable du réel (Vaccari & Chadwick, 2020).

Cette puissance modifie radicalement le « Diamant de la Fraude » (Wolfe & Hermanson, 2004) en démocratisant la composante de la capacité. Ce qui nécessitait autrefois une expertise rare est accessible au grand public : une imitation vocale crédible ne requiert que deux minutes d'audio, et un hypertrucage (*deepfake*) vidéo se génère en moins de 45 minutes (Sholademi, 2024). Ces contenus synthétiques hyperréalistes sont massivement exploités pour manipuler l'image de célébrités afin de promouvoir des placements fictifs ou exercer une pression psychologique (Emett et al., 2024 ; Whittaker et al., 2025). Bien que certains indices (clignements d'yeux saccadés, voix robotiques) trahissent encore la manipulation (Ivan, 2022 ; Sholademi, 2024), l'augmentation de 1.278% des incidents liés à l'IA entre 2022 et 2023 souligne l'urgence d'un scepticisme accru (OCDE, 2025 ; FSMA, 2025).

¹⁴ Célèbre expérience de pensée philosophique formulée par John Searle en 1980 pour contester l'idée d'une intelligence artificielle « forte », en démontrant qu'une machine capable de manipuler des symboles et de simuler parfaitement la compréhension d'une langue ne possède en réalité aucune conscience ni compréhension réelle du sens de ces symboles.

Section 2.3 : Impact sociétal

L'intégration de l'IA au sein de la société déclenche une mutation des structures de performance et de confiance, documentée par de vastes enquêtes institutionnelles (Ipsos ; CVMO ; EY ; Commission européenne). Bien qu'elle engage des milliards d'investissements stratégiques (Fan et al., 2025 ; OCDE, 2025), son adoption révèle des disparités. En Belgique, 70% des citoyens affirment connaître l'IA, mais cette maîtrise reste superficielle : 41% admettent en savoir peu et 30% n'ont aucune connaissance concrète, ce qui fait craindre l'émergence d'un fossé numérique (Ipsos, 2019). Parallèlement, la Commission européenne (2025) note une forte progression du sentiment d'auto-efficacité numérique, 70% des répondants s'estimant qualifiés pour l'utiliser au quotidien.

L'accueil de la technologie est globalement favorable : 56% des européens jugent son influence bénéfique pour la société et 66% des actifs y voient un impact positif au travail, principalement pour les gains d'efficacité et l'automatisation des tâches répétitives (Distinguin, 2025 ; European Commission, 2025). Pourtant, des freins subsistent : un Belge actif sur cinq redoute la disparition de son poste d'ici dix ans (Ipsos, 2019). De plus, 30% des citoyens s'inquiètent de la protection de leurs données et 82% des européens exigent le respect de la vie privée comme condition essentielle à l'intégration de l'IA (Ipsos, 2019 ; Distinguin, 2025 ; European Commission, 2025).

Au-delà de ces craintes structurelles, l'utilisation détournée de l'IA introduit des risques critiques. En reproduisant des fonctions cognitives supérieures, l'IA permet aux fraudeurs d'élaborer des tactiques de manipulation particulièrement efficaces (Mouton et al., 2016 ; OCDE, 2025). Les attaques d'ingénierie sociale dopées par l'IA ont ainsi explosé au second semestre 2024 (CVMO, 2024), générant des préjudices tant financiers que psychologiques (FINRA & AARP, 2022 ; Hock & Button, 2023). Les *deepfakes* permettent notamment de contourner la sécurité biométrique ou d'usurper l'identité d'experts financiers (Sholademi, 2024), alimentant une crise de confiance où plus de 70 % des investisseurs craignent pour la sécurité de leurs comptes en ligne (Ivan, 2022 ; Sholademi, 2024). Enfin, le stress lié au FOMO, exacerbé par cette hyper-connectivité, dégrade le bien-être émotionnel et peut déclencher anxiété et dépression (Talan et al., 2024) (voir chapitre 3).

En conclusion, l'équilibre entre innovation et sécurité impose un cadre éthique et législatif strict, matérialisé par le Règlement (UE) 2024/1689 (*IA Act*) visant à garantir des systèmes sûrs et respectueux des droits fondamentaux (Parlement européen, 2024 ; Fan et al., 2025). Ce défi majeur nécessitera une éducation continue pour restaurer la confiance numérique (Distinguin, 2025 ; Sun et al., 2025) face à l'avènement de ce que Gefen (2022) qualifie de « machines éternelles et immortelles » (Gefen, 2022, page 4), l'IA incarnant le futur de nos technologies, mais elle soulève également des questions existentielles sur la place de l'humain (Gefen, 2022).

Chapitre 3 : Le biais psychologique du FOMO (*Fear of Missing Out*)

Ce troisième chapitre consacré au FOMO débute par une définition conceptuelle du phénomène, avant d'en explorer les fondements théoriques, notamment à travers la théorie de l'autodétermination. Enfin, nous analysons les mécanismes cognitifs qui sous-tendent l'efficacité de ce biais, en nous appuyant sur le modèle des Systèmes 1 et 2 théorisé par Daniel Kahneman.

Section 3.1 : Définition et contextualisation

Le *Fear Of Missing Out* (FOMO), ou « peur de manquer l'occasion », constitue un construit psychologique dont la portée est devenue critique avec l'omniprésence des technologies numériques (Milyavskaya et al., 2018 ; Talan et al., 2024). Il se définit comme une appréhension constante que d'autres puissent vivre des expériences enrichissantes en notre absence, générant un désir irrésistible de rester continuellement connecté (Przybylski et al., 2013). Ancré dans le besoin fondamental d'appartenance, ce phénomène est exacerbé par les réseaux sociaux qui, en exposant des fragments de vie idéalisés, stimulent une comparaison sociale défavorable et un sentiment d'exclusion (Beyens et al., 2016). Bien que les premières recherches scientifiques sur le sujet remontent à 1996 avec les travaux de Herman¹⁵, le terme n'a été officialisé dans les dictionnaires qu'en 2013, illustrant une accélération technologique qui a décuplé son impact sociétal (Przybylski et al., 2013 ; Merriam-Webster, 2021, cité dans Ivantchev & Ivantcheva, 2024).

Cette dynamique instaure un cercle vicieux où l'inquiétude de rater une interaction ou une opportunité lucrative — un levier central dans les contextes de fraude financière — pousse à une utilisation compulsive des outils numériques, aggravant le malaise psychologique initial (Ivantchev & Ivantcheva, 2024 ; Li, 2024). L'omniprésence des réseaux sociaux agit désormais comme un catalyseur de ce besoin de surveillance d'autrui (Abel et al., 2016, cité dans Ivantchev & Ivantcheva, 2024). Pour les adolescents et jeunes adultes, ces plateformes sont devenues indissociables du quotidien pour maintenir les liens sociaux, mais cette hyper-connexion véhicule des influences délétères sur l'équilibre mental (Beyens et al., 2016).

Le FOMO est ainsi étroitement associé au narcissisme, à l'addiction numérique et à une diminution globale de la qualité de vie, se manifestant par une recrudescence des symptômes anxieux et dépressifs (Li, 2024 ; Talan et al., 2024). Ce biais altère significativement le jugement critique : au lieu d'agir selon son propre profil ou ses besoins réels, l'individu tend à suivre aveuglément la masse, laissant le besoin d'auto-évaluation gouverner ses comportements au détriment de sa sécurité psychologique et financière (Ivantcheva & Ivantchev, 2023). L'impact du FOMO dépasse aujourd'hui la sphère individuelle pour devenir un enjeu de santé publique, une tendance qui a notamment été amplifiée par l'isolement forcé durant la pandémie de COVID-19 (Ivantcheva & Ivantchev, 2023).

Section 3.2 : Cadre théorique : la théorie de l'autodétermination (SDT)

La compréhension psychologique du FOMO s'appuie sur la théorie de l'autodétermination (*Self-Determination Theory* - SDT) de Deci et Ryan (Deci & Ryan, 1985, cité dans Beyens et al., 2016), qui postule que la santé psychologique repose sur la satisfaction de trois besoins fondamentaux : la compétence (agir efficacement), l'autonomie (être auteur de ses choix) et l'appartenance sociale (*relatedness* — se sentir connecté à autrui) (Ryan & Deci, 2000, cité dans Li, 2024 ; Talan et al., 2024). Pour les adolescents et jeunes adultes, le besoin d'appartenance et de popularité est particulièrement saillant, érigeant les réseaux sociaux en outils d'autorégulation et de validation du statut social (Baumeister & Leary, 1995 ; Beyens et al., 2016 ; Talan et al., 2024).

À travers ce prisme, le FOMO est interprété comme un état d'instabilité de l'autorégulation résultant de déficits chroniques ou situationnels dans la satisfaction de ces trois besoins (Przybylski et

¹⁵ Chercheur et expert en marketing qui a conceptualisé pour la première fois le phénomène du FOMO (*Fear Of Missing Out*) dès 1996 à travers des études sur le comportement des consommateurs.

al., 2013 ; Milyavskaya et al., 2018). Lorsque le besoin d'appartenance n'est pas comblé, l'individu développe une sensibilité accrue à la peur de l'exclusion (Przybylski et al., 2013 ; Talan et al., 2024). Il s'agit d'une manifestation d'émotions négatives émergeant dès lors que le lien de proximité avec les pairs est perçu comme menacé (Milyavskaya et al., 2018 ; Gioia et al., 2021, cité dans Ivantcheva & Ivantchev, 2023 ; Li, 2024). Cette fragilité et ce faible bien-être psychologique augmentent la perméabilité aux stimuli externes (Talan et al., 2024). Cette vulnérabilité est alors exploitée par des agents malveillants à l'aide d'offres frauduleuses présentant des opportunités « exclusives » destinées à combler artificiellement ce besoin de validation et d'appartenance (Talan et al., 2024).

Section 3.3 : Le mécanisme cognitif de Kahneman

L'efficacité du FOMO en tant que levier de manipulation repose sur la théorie du double processus de Kahneman (2011). Ce modèle stipule que le traitement de l'information s'articule autour de deux systèmes : le Système 1 (intuitif, rapide et émotionnel) et le Système 2 (analytique, lent et logique). En temps normal, l'activation du Système 2 permet de détecter le caractère suspect d'une offre financière (Pennycook et al., 2020, cité dans Emmett et al., 2024). Cependant, l'être humain se comporte fréquemment comme un « avare cognitif » (Emmett et al., 2024, page 12), privilégiant par défaut le Système 1 afin d'économiser ses ressources mentales (Fiske & Taylor, 2013, cité dans Emmett et al., 2024).

Le FOMO sature le Système 1 en créant un sentiment d'urgence absolue, ce qui a pour effet d'inhiber les capacités d'analyse critique du Système 2 (Stanovich & West, 2000). Les escrocs exploitent délibérément cette faille cognitive en insistant sur l'impératif d'agir immédiatement pour saisir une opportunité lucrative mais limitée dans le temps (Milyavskaya et al., 2018 ; Ivantchev & Ivantcheva, 2024). En cadrant l'offre sous l'angle de l'évitement d'une perte plutôt que du gain simple, ils forcent la victime à prendre une décision instinctive pour échapper au regret futur (Hock & Button, 2023). Ce court-circuitage cognitif est amplifié par la structure des réseaux sociaux qui favorise la diffusion virale et la surcharge informationnelle, transformant le FOMO en un moteur de manipulation systémique (Appel et al., 2020 ; Talan et al., 2024).

Face à la sophistication de ces outils numériques, l'insécurité grandissante des utilisateurs (Sholademi, 2024) souligne l'importance cruciale de cadres législatifs comme l'*AI Act* de l'Union européenne, visant à classer les systèmes d'intelligence artificielle pour protéger les citoyens contre ces formes avancées d'ingénierie sociale (European Commission, 2021 ; Singh Chauhan, 2025).

Chapitre 4 : Convergence technologique (IA) et psychologique (FOMO) dans le monde financier

La fraude financière moderne repose sur une convergence sophistiquée entre l'intelligence artificielle (IA) et le FOMO (*Fear Of Missing Out*). Ce biais, ancré dans l'anxiété sociale et le besoin d'appartenance (Baumeister & Leary, 1995 ; Przybylski et al., 2013), crée une vulnérabilité où l'individu ignore les protocoles de sécurité pour ne pas manquer une opportunité (Beyens et al., 2016 ; Mouton et al., 2016). En exploitant le Système 1, intuitif et émotionnel, cette dynamique court-circuite le raisonnement analytique (Kahneman, 2011 ; Vishwanath et al., 2011).

L'IA générative (IAg) agit comme un catalyseur en offrant aux acteurs malveillants des outils d'industrialisation et de crédibilité inédits (Blauth et al., 2022 ; Ivan, 2022). Cette mutation fait évoluer le cadre traditionnel du « triangle de la fraude » (Cressey, 1953, cité dans Pluchart, 2019) vers le « diamant de la fraude », où l'IA décuple la capacité opérationnelle du fraudeur (Wolfe & Hermanson, 2004) et automatise la tromperie à une échelle systémique (Sun et al., 2025). Selon Europol (2023), cette

technologie est désormais impliquée dans plus de 25 % des cybercrimes financiers en Europe, utilisant notamment des *deepfakes* pour briser la vigilance des victimes (Vaccari & Chadwick, 2020).

Les sections suivantes détaillent les trois techniques fondamentales identifiées dans cette recherche, lesquelles constituent les variables pivots du FOMO. Directement mobilisés dans les processus de fraude, ces leviers gagnent en technicité et en efficacité grâce à l'émergence des nouvelles technologies, et plus particulièrement de l'IA générative.

Section 4.1 : Utilisation du langage technique : entre personnalisation et ingénierie sociale

L'un des impacts majeurs de l'IAg réside dans l'amplification de l'ingénierie sociale via la création d'une complexité factice. Grâce aux grands modèles de langage (LLM), les fraudeurs produisent des contenus d'une précision grammaticale irréprochable, supprimant les fautes d'orthographe qui servaient autrefois de signaux d'alerte (Europol, 2023 ; Wan Fakhruddin et al., 2026). Cette structuration linguistique impeccable renforce la crédibilité perçue des plateformes frauduleuses (Mouton et al., 2016).

Au-delà de la forme, l'IA est utilisée pour saturer la mémoire de travail de la victime par une surcharge cognitive. En bombardant l'investisseur de graphiques complexes et d'un jargon financier pointu, l'escroc provoque une paralysie par analyse (Wan Fakhruddin et al., 2026). Face à cette masse d'informations, le Système 2 capitule au profit du Système 1, accordant une confiance induite à une technologie perçue comme infaillible (Kahneman, 2011 ; Vishwanath et al., 2011). Enfin, l'analyse massive de données permet une hyperpersonnalisation des scénarii sur mesure, ciblant les intérêts spécifiques de chaque individu pour maximiser le taux de réussite (Blauth et al., 2022).

Section 4.2 : Pression temporelle : l'extrême exclusivité

L'exploitation du FOMO constitue le levier émotionnel central permettant de verrouiller la décision de l'investisseur avant toute vérification (*due diligence*). Les fraudeurs utilisent le langage de l'urgence et de l'exclusivité pour activer un mécanisme d'évitement de la perte (Hock & Button, 2023 ; Wan Fakhruddin et al., 2026), conformément à la théorie des perspectives où la crainte de perdre une opportunité l'emporte sur la rationalité du gain (Kahneman, 2011).

En présentant les offres comme des « opportunités uniques » à « accès limités », ils imposent une compression temporelle qui court-circuite le jugement critique (Lyu et al., 2025, cité dans Wan Fakhruddin et al., 2026). Cette stratégie est particulièrement redoutable chez les investisseurs de 18 à 40 ans, plus sensibles à la comparaison sociale sur les réseaux sociaux (Przybylski et al., 2013 ; Beyens et al., 2016). L'IA démultiplie l'efficacité de ces schémas en générant massivement des messages calibrés et des preuves sociales synthétiques pour amplifier cette anxiété de l'opportunité manquée (Blauth et al., 2022 ; Ivantchev & Ivantcheva, 2024).

Section 4.3 : Deepfakes : entre autorité et preuve sociale

L'IA permet de construire une façade de légitimité en simulant une validation sociale artificielle. Les fraudeurs créent de faux témoignages, des compteurs d'utilisateurs fictifs et des communautés de discussions automatisées pour exploiter le biais de preuve sociale et normaliser l'investissement en noyant les doutes dans un consensus simulé (Mouton et al., 2016 ; Blauth et al., 2022 ; Hock & Button, 2023 ; Wan Fakhruddin et al., 2026).

Le sommet de cette sophistication est atteint avec les *deepfakes*, capables de cloner la voix et l'image de personnalités de confiance (PDG, experts ou célébrités) (Ivan, 2022 ; Sholademi, 2024). En Belgique, la FSMA (2025) estime que la moitié des publicités frauduleuses en ligne exploitent déjà ces visages connus pour activer le biais d'autorité. Une étude de Emmett et al. (2024) souligne que le réalisme de ces médias synthétiques influence les investisseurs même lorsqu'ils tentent d'activer leur pensée analytique, illustrant l'érosion de la méfiance traditionnelle face à la perfection technique (Vaccari & Chadwick, 2020). Cette synergie entre l'illusion technologique et le déclencheur émotionnel du FOMO transforme une vulnérabilité psychologique en un risque financier systémique majeur (TRM Labs, 2024 ; CVMO, 2025).

Après cette revue de littérature qui pose les fondements théoriques nécessaires à la compréhension des liens entre fraudes aux investissements, intelligence artificielle et biais de FOMO, la suite de ce travail est consacrée à la phase empirique.

Partie III : Recherche empirique

Après avoir parcouru la théorie académique sur le sujet, passons maintenant au cœur de cette recherche avec la partie pratique. Cette dernière sera divisée en plusieurs chapitres allant du plus abstrait, comme les hypothèses de recherche, au plus concret, tel que les résultats obtenus ainsi que leur discussion, en passant par la méthodologie utilisée.

Chapitre 1 : Objectifs et hypothèses de recherche

L'objectif central de cette étude est de démontrer comment l'intelligence artificielle générative (IAg) agit comme un catalyseur de la fraude aux investissements en exploitant le levier psychologique du *Fear Of Missing Out* (FOMO). En s'appuyant sur la revue de littérature, ce travail analyse la synergie entre sophistication technologique et vulnérabilité humaine afin de valider un modèle où l'IA neutralise les mécanismes de défense de l'investisseur.

H1 : Le langage technique

La première hypothèse postule que l'intégration de l'IA générative, via les grands modèles de langage (LLM), neutralise les indices linguistiques traditionnels de fraude (fautes d'orthographe, syntaxe approximative) qui servaient de heuristiques de défense à l'investisseur (Europol, 2023 ; TRM Labs, 2024). En substituant la méfiance par un jargon technique irréprochable et fluide, l'IA génère une illusion de professionnalisme qui installe une crédibilité immédiate et rend l'hameçonnage indiscernable d'une communication légitime (Singh Chauhan, 2025 ; Wan Fakhruddin et al., 2026).

L'absence de « bruit » linguistique focalise l'attention de la cible exclusivement sur les stimuli émotionnels du FOMO (Mouton et al., 2016). En présentant un projet complexe et formellement parfait, l'IA sature la mémoire de travail de la victime par une surcharge cognitive (Wan Fakhruddin et al., 2026), l'incitant à abandonner son Système 2 analytique au profit du Système 1 intuitif, plus sensible à l'urgence (Kahneman, 2011 ; Vishwanath et al., 2011). Un individu exposé à une fraude utilisant l'IA générative présentera ainsi un taux de vulnérabilité supérieur à celui observé en présence d'une fraude émaillée de fautes.

- **Hypothèse 1 :** *Il existe une corrélation positive entre la sophistication linguistique du message (syntaxe irréprochable, lexique technique spécialisé) et la crédibilité perçue de la fraude.*

H2 : La pression temporelle

La deuxième hypothèse postule que la capacité de l'IA à produire des scénarii d'urgence hyper-personnalisés exacerbe le sentiment de FOMO, provoquant une priorisation du Système 1 au détriment du Système 2. En s'appuyant sur la théorie du double processus (Kahneman, 2011), nous suggérons que l'IA industrialise une compression temporelle qui paralyse le raisonnement délibéré au profit d'une réaction instinctive (Hock & Button, 2023 ; Wan Fakhruddin et al., 2026).

La génération de stimuli de rareté (« places restantes », « opportunité limitée ») active un mécanisme d'évitement de la perte ancré dans l'anxiété sociale (Baumeister & Leary, 1995 ; Przybylski et al., 2013). Contrairement aux messages génériques traditionnels, l'IA calibre cette urgence pour qu'elle soit perçue comme immédiate, créant une surcharge cognitive qui ne laisse pas le temps requis pour effectuer une vérification élémentaire (*due diligence*) auprès des régulateurs (Blauth et al., 2022 ; Vishwanath et al., 2011 ; Lyu et al., 2025). Le court-circuitage cognitif induit par cette pression psychologique démultiplie le taux de réussite de l'escroquerie.

- **Hypothèse 2 :** *Il existe une corrélation positive entre l'intensité du sentiment de pression temporelle induit chez l'individu et sa réceptivité aux fraudes d'investissements.*

H3 : Les deepfakes

La troisième hypothèse avance que l'intégration de contenus synthétiques de type *deepfake* (hypertrucages) génère un biais de crédibilité majeur, où la sophistication visuelle et sonore de l'IA est perçue comme un gage de légitimité financière (Ivan, 2022 ; Sholademi, 2024). Cette capacité à imiter la réalité crée une « vérité synthétique » qui rend la manipulation indétectable pour un utilisateur non averti (Blauth et al., 2022).

En clonant la voix et l'image de personnalités reconnues (experts, dirigeants, célébrités), les fraudeurs mobilisent simultanément les biais d'autorité et de preuve sociale, opérant un transfert de légitimité immédiat vers l'offre (Mouton et al., 2016 ; Vaccari & Chadwick, 2020). Ce processus court-circuite les barrières cognitives car le cerveau accorde une confiance supérieure aux stimuli audiovisuels réalistes qu'aux informations textuelles, confondant réalisme technique et fiabilité institutionnelle (Emett et al., 2024 ; Singh Chauhan, 2025). Renforcée par le FOMO d'une opportunité validée par des experts, la victime s'engage financièrement sans réaliser de vérifications préalables, la technique masquant efficacement l'absence de régulation (FSMA, 2025).

- **Hypothèse 3 :** *Il existe une corrélation positive entre l'intégration de contenus synthétiques de type deepfake et le degré de crédibilité perçu d'une offre d'investissement.*

Chapitre 2 : Méthodologie

Cette recherche adopte une approche quantitative s'appuyant sur une méthode corrélationnelle. Par sa visée principale, cette étude est de nature explicative ; toutefois, elle revêt également une dimension exploratoire en raison du caractère novateur de son objet, à savoir l'analyse simultanée des corrélations entre le syndrome du FOMO, l'usage de l'IA générative et le domaine des fraudes aux investissements. Le recueil des données a été effectué via un questionnaire standardisé numérique¹⁶

¹⁶ Annexe 37

(*Computer-Assisted Web Interviewing — CAWI*), développé et administré sur la plateforme KoboToolbox. Pour minimiser les biais de désirabilité sociale et éviter que les participants ne modifient consciemment leurs réponses, l'enquête a été présentée sous l'intitulé neutre : « Étude sur les habitudes d'investissements financiers au sein de la population belge ». L'outil de collecte était structuré en dix sections thématiques bien distinctes, combinant des questions de contextualisation socio-démographique, des échelles psychométriques standardisées pour évaluer le niveau de FOMO (Przybylski et al., 2013), et des mises en situation concrètes, matérialisées par des scénarii de fraude, intégrant les trois variables pivots testées, à savoir le langage technique des LLM, la compression temporelle et le support synthétique par *deepfakes*.

Section 2.1 : Échantillon

La validité interne et externe de la recherche repose sur une méthode d'échantillonnage non probabiliste par quotas. Les critères retenus visaient à assurer une représentativité de la population belge francophone de plus de 15 ans, principalement ciblée selon des variables clés d'âge, de genre et de niveau d'instruction. Le protocole empirique mis en œuvre a permis de réunir un échantillon final de plus de 150 répondants ($n = 153$), offrant une puissance statistique suffisante pour l'analyse rigoureuse des données. Le recrutement s'est effectué entièrement sur base volontaire et entièrement anonyme, garantissant ainsi un cadre éthique rigoureux, en parfaite conformité avec les exigences de la recherche académique (RGPD¹⁷).

Section 2.2 : Procédure

La procédure de collecte s'est déroulée intégralement en ligne sur la période du 11 Mai 2026 au 6 Juin 2026, permettant de toucher les répondants dans leur environnement numérique habituel. Après avoir cliqué sur le lien de l'étude, les participants étaient accueillis par une note d'information générale rappelant le cadre éthique, la garantie de l'anonymat et l'utilisation exclusive des données à des fins de recherche, sans pour autant dévoiler l'objectif sous-jacent lié à la détection des fraudes afin de préserver la spontanéité des réactions. Les répondants progressaient ensuite de manière séquentielle à travers les dix sections du questionnaire, l'interface KoboToolbox garantissant que chaque question obligatoire soit complétée avant de passer à la suivante. Après avoir commencé par les variables socio-démographiques, les participants étaient confrontés à l'évaluation de leurs traits psychologiques avant d'être exposés aux différents scénarii de simulations de fraudes aux investissements.

Section 2.3 : Mesures

Les instruments de mesure insérés dans le questionnaire se divisent en trois catégories d'outils d'évaluation. Premièrement, le niveau de FOMO (*Fear of Missing Out*) des individus a été quantifié au moyen d'échelles psychométriques standardisées issues de la littérature scientifique - Przybylski et al., 2013 - adaptées pour mesurer précisément l'intensité de cette anxiété sociale et du besoin d'appartenance au sein des écosystèmes numériques. Deuxièmement, la réceptivité et la vulnérabilité comportementale ont été mesurées à travers des indicateurs de crédibilité perçue (évaluée sur des échelles de type Likert) et d'intention d'action face aux scénarii construits. Ces scénarii opérationnalisait les trois stimuli pivots de l'ingénierie sociale assistée par intelligence artificielle : la sophistication sémantique (langage technique des LLM), l'urgence décisionnelle (compression temporelle) et l'autorité visuelle (supports

¹⁷ Règlement général sur la protection des données

synthétiques par *deepfakes*). Enfin, des variables de contrôle socio-démographiques et de profil d'investisseur ont été intégrées pour capter l'expérience financière préalable des répondants.

Section 2.4 : Plan d'analyse

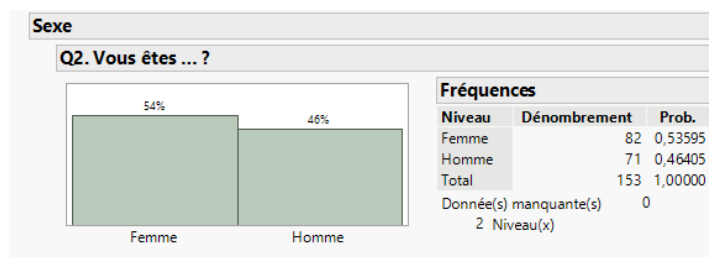
Une fois collectées, les données brutes ont été exportées de la plateforme KoboToolbox et « nettoyées » sur Excel, puis analysées à l'aide du logiciel statistique JMP selon un protocole structuré autour de trois axes principaux. Le premier volet est consacré à la validation des instruments de mesure par le calcul de l'Alpha de Cronbach, un indicateur essentiel pour évaluer la cohérence interne des échelles psychométriques standardisées employées, en particulier celle visant à quantifier l'intensité du syndrome du FOMO chez les répondants. Dans un deuxième temps, le traitement des données s'oriente vers des analyses descriptives globales complétées par la production de matrices de corrélation ; ces outils statistiques permettent d'identifier précisément la force ainsi que le sens des relations existant entre le niveau de FOMO des individus, leur profil d'investisseur et leur degré de réceptivité face aux différents stimuli frauduleux. Enfin, le dernier axe est dédié à la vérification empirique de nos hypothèses de recherche par la réalisation de tests d'analyse de la variance (ANOVA) et de tests *t* de Student. Ces analyses permettent de mesurer de manière statistiquement significative l'impact des différentes modalités des scénarii de fraude, en opposant systématiquement les messages conventionnels aux messages optimisés par l'intelligence artificielle, sur le taux de vulnérabilité et de crédibilité perçus par les participants, offrant ainsi les fondements empiriques indispensables pour valider ou rejeter les hypothèses H1, H2 et H3.

Chapitre 3 : Résultats

Section 3.1 : Analyses statistiques descriptives

Profil sociodémographique et habitudes financières

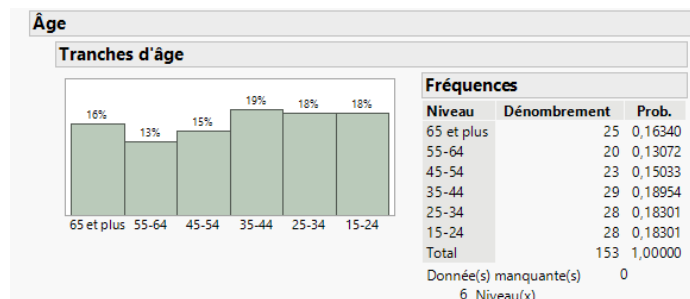
Sexe (Q2)



L'échantillon comprend 153 répondants ($n = 153$) : 54% ($n = 82$) de femmes et 46% ($n = 71$) d'hommes. Confronté aux données de Statbel (2026) (51% de femmes, 49% d'hommes), l'écart maximal n'est que de 3%¹⁸.

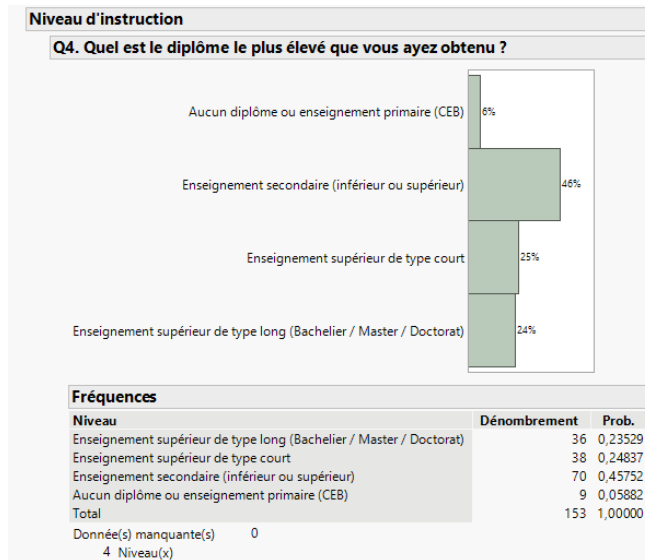
Âge (Q3)

Segmenté en six tranches et comparé à Statbel (2026) (hors moins de 15 ans), l'échantillon se distribue ainsi : 15-24 ans : 18% (+4%) ; 25-34 ans : 18% (+3%) ; 35-44 ans : 19% (+3%) ; 45-54 ans : 15% (parfaite adéquation) ; 55-64 ans : 13% (-3%) ; 65 ans et plus : 16% (-8%)¹⁹.



¹⁸ Annexe 1

¹⁹ Annexe 2



Niveau d'instruction (Q4)

Comparé à Statbel (2025), l'échantillon compte : 6% (n = 9) sans diplôme ou CEB, 46% (n = 70) avec un diplôme secondaire, 25% (n = 38) de diplômés du supérieur de type court et 24% (n = 36) de type long/universitaire. Les diplômés universitaires sont surreprésentés (+5%²⁰) et l'enseignement secondaire sous représenté (-8%).

Auto-évaluation des connaissances financières (Q5²¹)

Une large majorité (69%) admet avoir des compétences limitées : 26% (n = 40) de « novices » et 43% (n = 66) de « débutants ». Le reste se répartit entre « compétents » (22%, n = 33), « avancés » (8%, n = 12) et « experts » (1%, n = 1).

Intérêt pour les opportunités d'investissement en ligne (Q6²²)

L'attrait est très faible. Environ 77% (n = 117) expriment un désintéressement. Seuls 16% (n = 24) se montrent réceptifs (14%, n = 21 « plutôt d'accord » et 2%, n = 3 « totalement d'accord »).

Passé victime face aux arnaques en ligne (Q40²³)

Sur 132 répondants valides, 55% (n = 72) ont déjà été confrontés à une tentative d'arnaque à l'investissement en ligne, et 2% (n = 3) ont subi un préjudice financier direct. Moins de la moitié (43%, n = 57) n'a jamais été confronté à une tentative d'arnaque à l'investissement en ligne.

Auto-évaluation de la capacité de détection des contenus générés par IA (Q42²⁴)

Plus de la moitié de l'échantillon (54%, n = 83) s'estime capable d'identifier une fraude financière en ligne exploitant l'IA. Environ 27% (n = 42) estiment en être incapables et 18% (n = 28) ne sont pas certains.

²⁰ Annexe 3

²¹ Annexe 4

²² Annexe 5

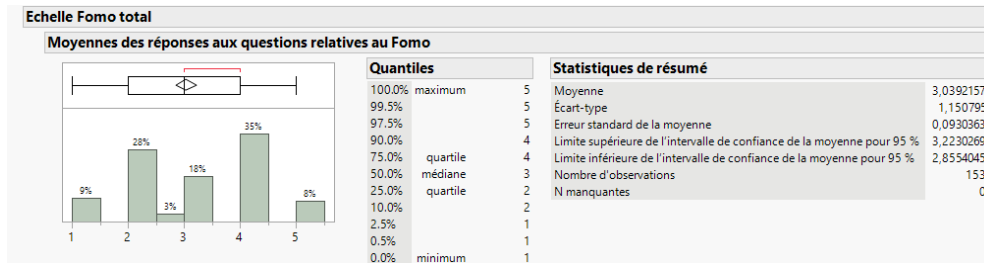
²³ Annexe 6

²⁴ Annexe 7

Échelle du FOMO : validation et statistiques

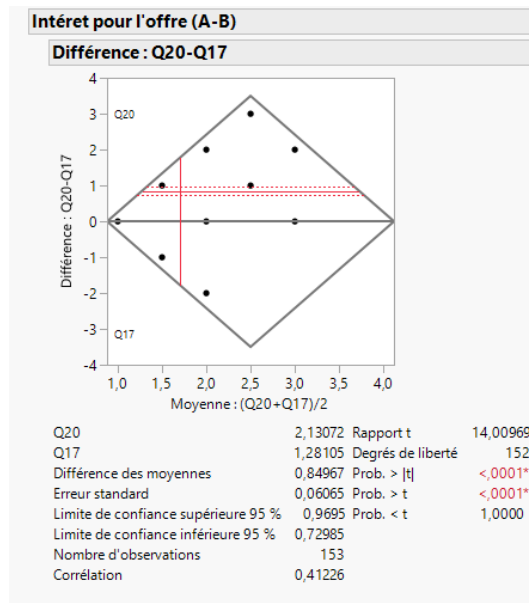
L'échelle de Przybylski et al. (2013) (10 items, Q7 à Q16) présente une cohérence interne satisfaisante avec un Alpha de Cronbach de $\alpha = 0,7599^{25}$. Tous les items ont été conservés.

Le score moyen global est de $M = 3,039$ ($SD = 1,151$), indiquant une dynamique modérée. La structure est toutefois polarisée : 37% ($n = 57$) des répondants affichent un FOMO faible, tandis que 42% ($n = 65$) présentent un FOMO élevé avant toute confrontation aux stimuli.



Section 3.2 : Analyse statistique analytique (corrélation)

H1 : le langage technique



Intérêt subjectif

Pour l'offre A - informelle (Q17²⁶), 75% ($n = 114$) ne sont pas du tout intéressés avec 3% ($n = 4$) de neutres et 0 intéressé. L'offre B (jargon, Q20²⁷) déplace la distribution : 31% ($n = 48$) deviennent neutres et 3% ($n = 4$) intéressés pour seulement 23% ($n = 36$) de pas du tout intéressés.

Le test t apparié confirme ce déplacement significatif : $t(152) = 14,01$; $p < 0,0001$ ($MB = 2,13$ vs $MA = 1,28$).

Il existe donc une différence statistique significative entre le niveau d'intérêt de l'offre A (Q17) et de l'offre B (Q20).

²⁵ Annexe 8

²⁶ Annexe 9

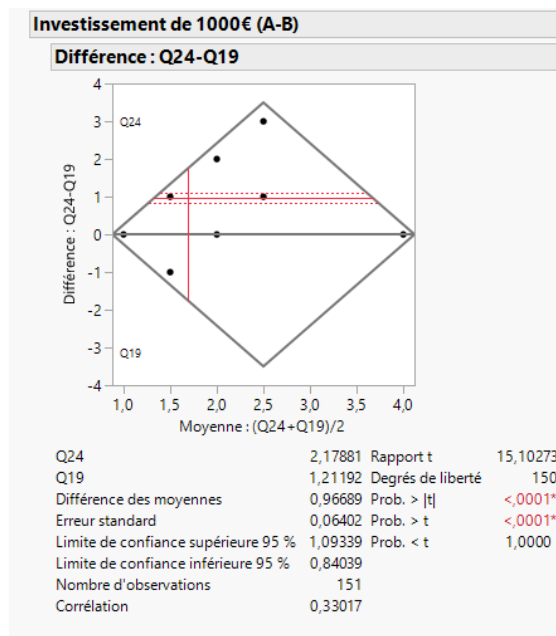
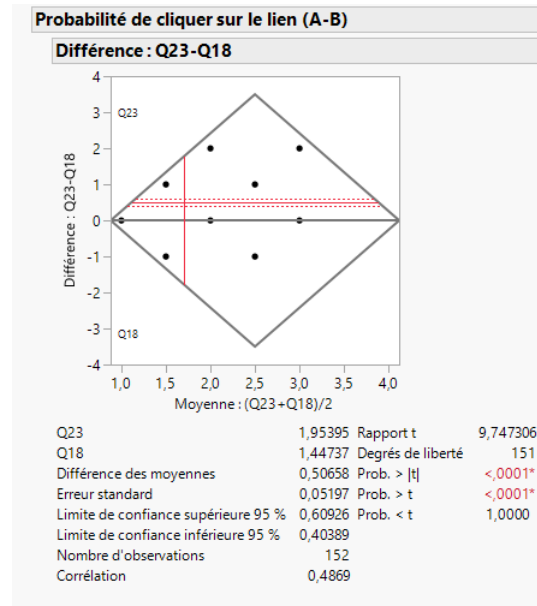
²⁷ Annexe 10

Intention de clic

L'intention de clic augmente significativement entre l'offre A (Q18²⁸) et l'offre B (Q23²⁹) : le pôle « Aucune chance » chute de 57% (n = 86) à 26% (n = 40) au profit de la modalité « Peu probable » (de 42%, n = 64 à 53%, n = 81) et « Peut-être » (de 1%, n = 2 à 20%, n = 31).

Test *t* apparié : $t(151) = 9,75$; $p < 0,0001$ (MB = 1,95 contre MA = 1,45).

Il existe donc une différence statistique significative entre l'intention de clic de l'offre A (Q18) et de l'offre B (Q23).



Prise de risque financier fictif

Face à l'offre A (Q19³⁰), 80% (n = 122) limitent leur placement au palier minimal (1 € - 250 €). Face à l'offre B (Q24³¹), 36% (n = 55) misent entre 251 € et 500 € et 39% (n = 59) choisissent le palier 501 € - 750 € avec plus que 24% (n = 36) pour le palier minimal.

Test *t* apparié : $t(150) = 15,10$; $p < 0,0001$ (MB = 2,18 vs MA = 1,21).

Il existe donc une différence statistique significative entre la prise de risque financier fictive de l'offre A (Q19) et de l'offre B (Q24).

Dynamiques corrélatives³² (offre B)

Le ρ de Spearman montre que l'intention de clic (Q23) et le risque financier (Q24) sont positivement couplés ($\rho = 0,50$; $p < 0,0001$). L'influence perçue des termes techniques (Q21³³) covarie avec l'intention de clic ($\rho = 0,34$; $p < 0,0001$) et le montant placé ($\rho = 0,42$; $p < 0,0001$). Les corrélations entre l'intention de clic, le risque financier et l'influence perçues des termes techniques sont établies.

²⁸ Annexe 11

²⁹ Annexe 12

³⁰ Annexe 13

³¹ Annexe 14

³² Annexe 15

³³ Annexe 16

Traitement heuristique vs analytique

Seuls 19% (n = 29) ont analysé précisément les termes (Q22³⁴). La majorité a adopté une stratégie périphérique (36% sur l'impression globale, 45% sur la fluidité du ton), soit 81% au total. Test χ^2 de Pearson : χ^2 (2, N = 153) = 16,16 ; p = 0,0003. Le test du Chi-deux confirme que la répartition observée est fortement significative.

Crédibilité institutionnelle perçue (Q25³⁵)

Plus de 71% (n = 104) désignent exclusivement l'offre B comme émanant d'une institution régulée, 4% (n = 6) désignent les deux, et 25% (n = 36) répondent « Aucune des deux ». Il n'existe aucune réponse pour l'offre A.

Influence linguistique générale (Q26³⁶)

Environ 59% (n = 90) estiment que la précision du langage influence fortement leur intérêt, et 22% (n = 33) y accordent une influence maximale.

Croyances théoriques (Forme et Jargon)

Environ 97% (n = 148) des répondants s'accordent à dire qu'une institution sérieuse ne fait jamais de fautes d'orthographe (Q34³⁷). De même, 65% (n = 99) assimilent l'usage d'un vocabulaire technique à un signe direct de compétence (Q35³⁸).

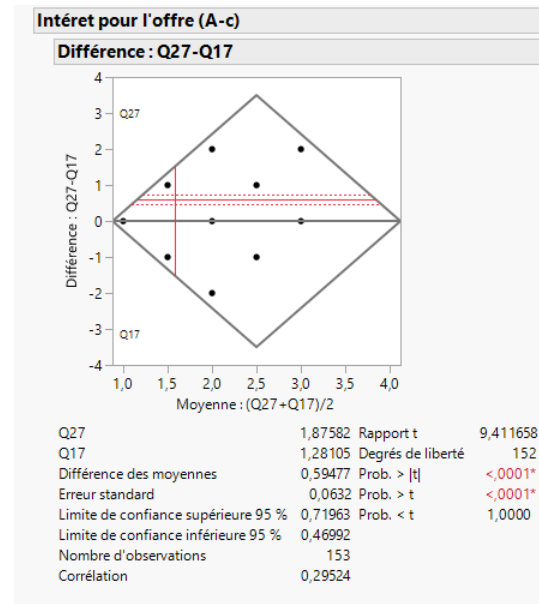
H2 : la pression temporelle

Intérêt subjectif

Le taux de participants « Pas du tout intéressés » passe de 75% (n = 114) pour l'offre A (Q17) à 35% (n = 53) pour l'offre C (urgence, Q27³⁹). Test t apparié significatif : $t(152) = 9,41$; p < 0,0001 (MC = 1,88 vs MA = 1,28).

Il existe donc une différence statistique significative entre le niveau d'intérêt de l'offre A (Q17) et de l'offre C (Q27).

L'ANOVA⁴⁰ est hautement significative : $F(2, 150) = 11,70$; p < 0,0001 ; $R^2 = 0,135$. Le groupe avec un FOMO aigu (groupe 3) se détache avec un intérêt moyen supérieur (M = 2,20) par rapport aux groupes 1 (M = 1,61) et 2 (M = 1,68). La corrélation entre le niveau de FOMO et l'intérêt pour l'offre C est établie.



³⁴ Annexe 17

³⁵ Annexe 18

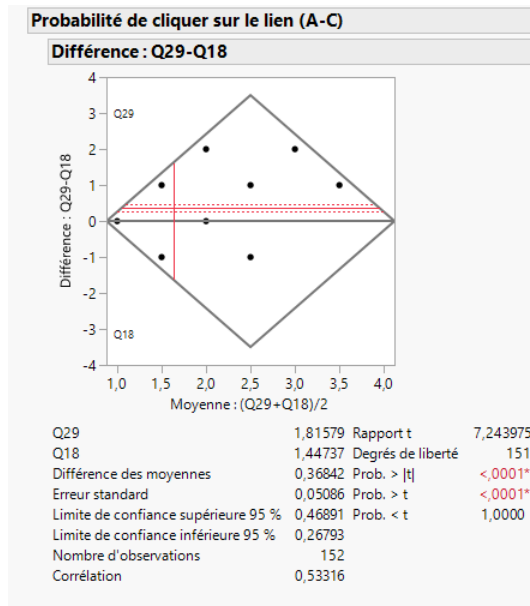
³⁶ Annexe 19

³⁷ Annexe 20

³⁸ Annexe 21

³⁹ Annexe 22

⁴⁰ Annexe 23



Intention de clic

Le pôle « Aucune chance » de cliquer passe de 57% (n = 86) pour l'offre A (Q18) à 36% (n = 55) pour l'offre C (Q29⁴¹). Test *t* apparié : $t(151) = 7,24$; $p < 0,0001$ (MC = 1,82 vs MA = 1,45).

Il existe donc une différence statistique significative entre l'intention de clic de l'offre A (Q18) et de l'offre C (Q29).

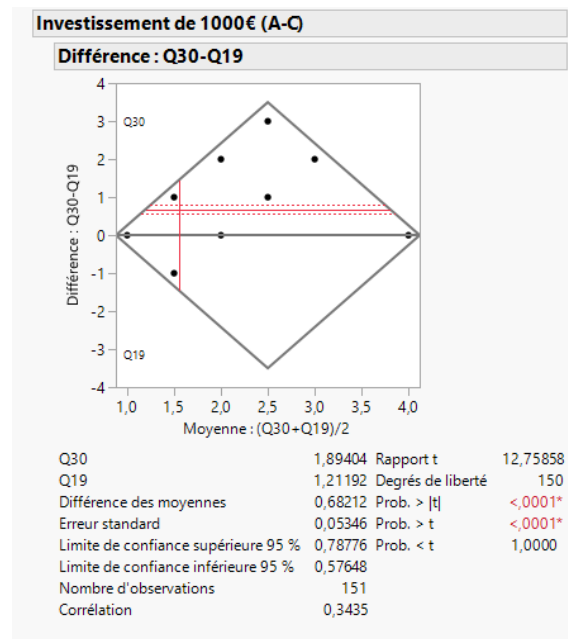
L'ANOVA ⁴²confirme l'effet du FOMO sur le clic : $F(2, 150) = 10,88$; $p < 0,0001$; $R^2 = 0,127$. Le groupe avec un FOMO aigu (groupe 3) se détache avec un intérêt moyen supérieur (M = 2,11) par rapport aux groupes 1 (M = 1,61) et 2 (M = 1,54). La corrélation entre le niveau de FOMO et l'intention de clic est établie.

Prise de risque financier fictif

Face à l'offre C (Q30⁴³), 63% (n = 95) acceptent de risquer entre 251 € et 500 € (contre 80%, n = 122 dans le palier minimal pour l'offre A, Q19). Test *t* apparié : $t(150) = 12,76$; $p < 0,0001$ (MC = 1,89 vs MA = 1,21).

Il existe donc une différence statistique significative entre la prise de risque financier fictive de l'offre A (Q19) et de l'offre C (Q30).

L'ANOVA⁴⁴ valide l'impact du FOMO sur le montant : $F(2, 149) = 5,56$; $p = 0,0047$. Le groupe avec un FOMO aigu (groupe 3) se détache avec un intérêt moyen supérieur (M = 2,09) par rapport aux groupes 1 (M = 1,73) et 2 (M = 1,77). La corrélation entre le niveau de FOMO et le montant investi est établie.



Dynamique d'influence du trait de FOMO

Le score Total FOMO⁴⁵ est faiblement lié à l'offre A ($r = 0,10$), mais s'associe linéairement aux indicateurs de l'offre C : intérêt ($r = 0,3836$), clic ($r = 0,3244$) et montant ($r = 0,3018$). Le ρ de Spearman confirme l'absence de lien significatif avec l'offre A, mais un lien hautement significatif avec l'offre C ($\rho\{\text{intérêt}\} = 0,3747$; $\rho\{\text{clic}\} = 0,3541$; $\rho\{\text{montant}\} = 0,2953$).

⁴¹ Annexe 24

⁴² Annexe 25

⁴³ Annexe 26

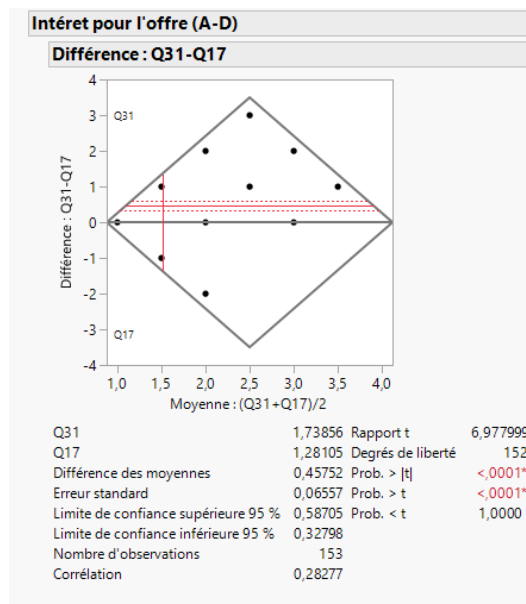
⁴⁴ Annexe 27

⁴⁵ Annexe 28

Tension et croyances théoriques

Seuls 10% ($n = 16$) des sujets rapportent avoir ressenti une tension à la lecture de la contrainte (Q28⁴⁶). Environ 13% ($n = 30$) reconnaissent en théorie que l'exclusivité accélère leur décision (Q36⁴⁷). L'effet théorique d'un minuteur sur la neutralisation des vérifications (Q37⁴⁸) est massivement rejeté (91%, $n = 140$ de désaccord).

H3 : la preuve sociale (*deepfakes*)



Intérêt subjectif

Avec la figure d'autorité (offre D, Q31⁴⁹), le taux de « Pas du tout intéressés » chute de 75% ($n = 114$) pour l'offre A (Q17) à 44% ($n = 68$) pour l'offre D.

Test t apparié significatif : $t(152) = 6,98$; $p < 0,0001$ (MD = 1,74 vs MA = 1,28).

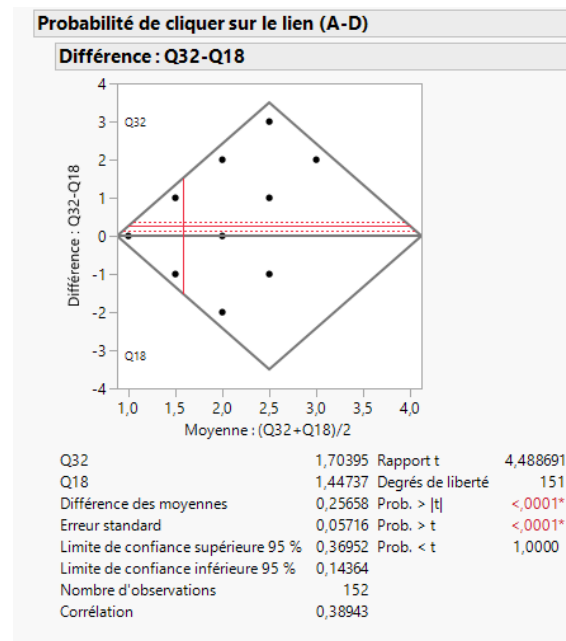
Il existe donc une différence statistique significative entre le niveau d'intérêt de l'offre A (Q17) et de l'offre D (Q31).

Intention de clic

Le pôle « Aucune chance » de cliquer passe de 57% ($n = 86$) pour l'offre A (Q18) à 44% ($n = 67$) pour l'offre D (Q32⁵⁰).

Test t apparié : $t(151) = 4,49$; $p < 0,0001$ (MD = 1,70 vs MA = 1,45).

Il existe donc une différence statistique significative entre l'intention de clic de l'offre A (Q18) et de l'offre D (Q32).



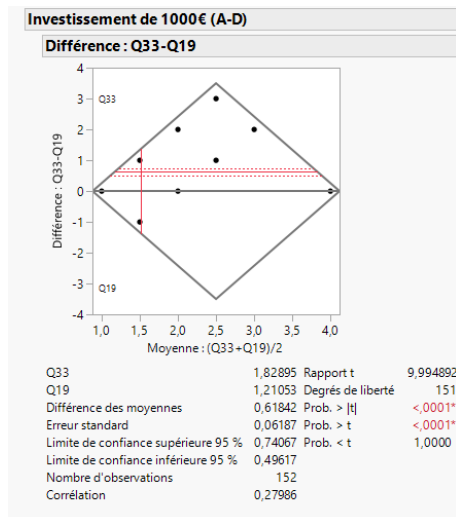
⁴⁶ Annexe 29

⁴⁷ Annexe 30

⁴⁸ Annexe 31

⁴⁹ Annexe 32

⁵⁰ Annexe 33



Prise de risque financier fictif

Environ 46% (n = 71) des répondants acceptent de placer entre 251 € et 500 € sur l'offre D (Q33⁵¹) contre 19% (n = 29) pour l'offre A (Q19) et 17% (n = 26) s'engagent au-delà contre 1% (n = 1) pour l'offre de contrôle.

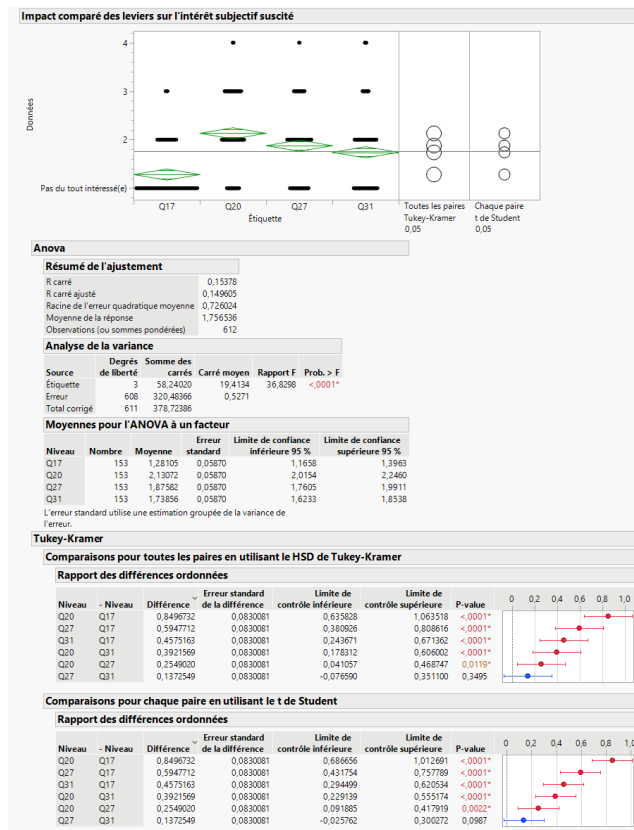
Test *t* apparié : $t(151) = 9,99$; $p < 0,0001$ (MD = 1,83 vs MA = 1,21).

Il existe donc une différence statistique significative entre la prise de risque financière fictive de l'offre A (Q19) et de l'offre D (Q33).

Poids de la preuve sociale et notoriété

Environ 77% (n = 118) des répondants admettent que voir d'autres personnes investir les rassure (Q38⁵²). En revanche, interrogés de manière directe sur l'impact théorique d'une personnalité publique en vidéo (Q39⁵³), 65% (n = 99) rejettent l'idée qu'elle renforce la crédibilité.

Analyses transversales : comparaison inter-scenarii et hiérarchisation des variables



Impact comparé sur l'intérêt subjectif

L'ANOVA est significative : $F(3, 608) = 36,83$; $p < 0,0001$; $R^2 = 0,154$.

Classification : offre B (M = 2,13) > offre C (M = 1,88) > offre D (M = 1,74) > offre A (M = 1,28).

Toutes les offres modifiées augmentent significativement l'intérêt du répondant par rapport à A.

Le jargon (B) surpasse significativement l'autorité/la preuve sociale (C et D), mais l'écart entre l'urgence (C) et la preuve sociale (D) n'est pas significatif ($p = 0,3495$).

⁵¹ Annexe 34

⁵² Annexe 35

⁵³ Annexe 36

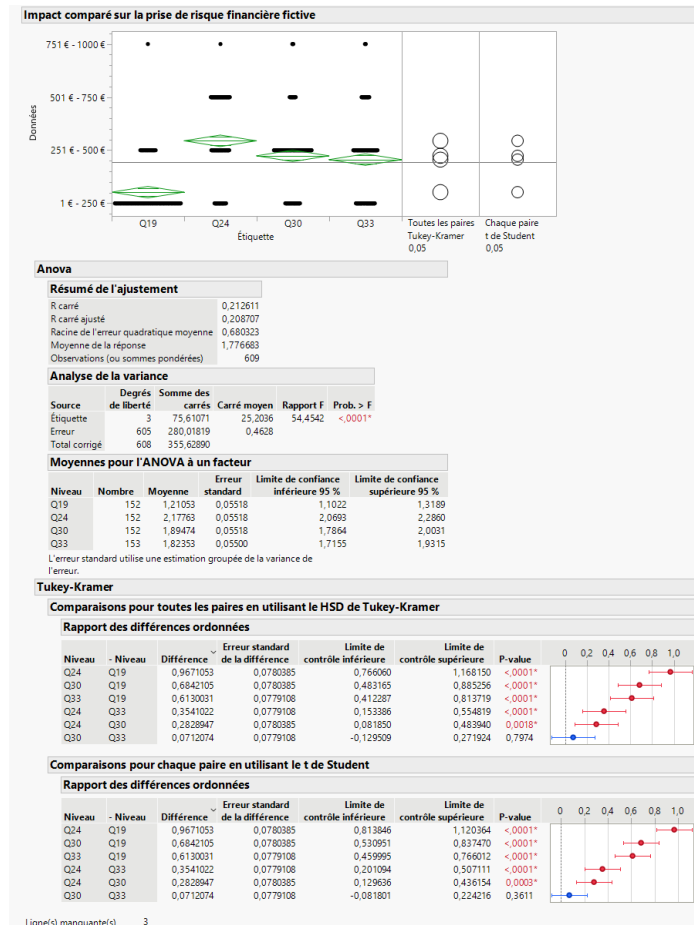
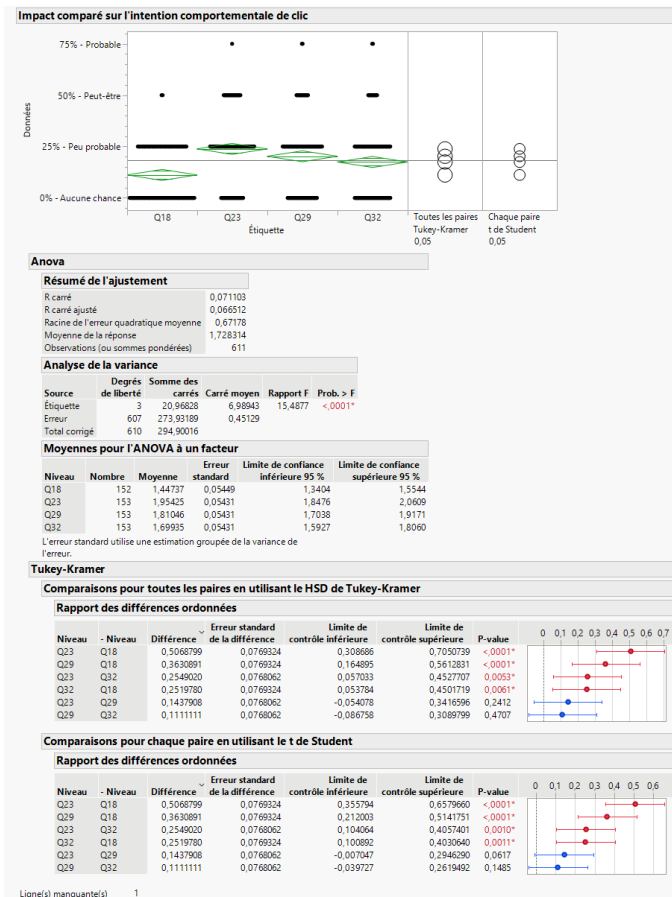
Impact comparé sur l'intention de clic

L'ANOVA est significative : $F(3, 607) = 15,49$; $p < 0,0001$; $R^2 = 0,071$.

Classification : offre B ($M = 1,95$) > offre C ($M = 1,81$) > offre D ($M = 1,70$) > offre A ($M = 1,45$).

Toutes les offres modifiées augmentent significativement le clic par rapport à A.

Le jargon (B) surpasse significativement l'autorité (D), mais son écart avec l'urgence (C) n'est plus significatif ($p = 0,2412$).



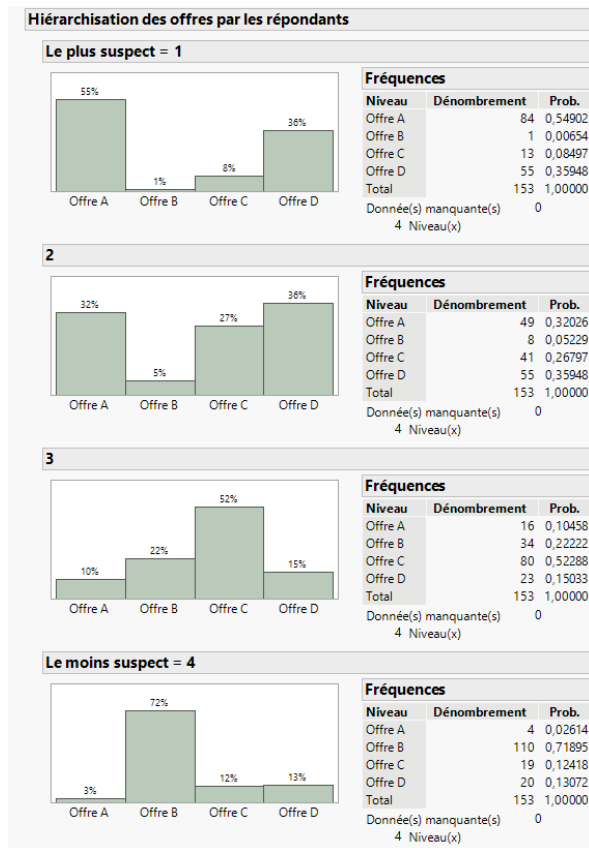
Impact comparé sur la prise de risque financier fictif

L'ANOVA est significative : $F(3, 605) = 54,45$; $p < 0,0001$; $R^2 = 0,213$.

Classification : offre B ($M = 2,18$) > offre C ($M = 1,89$) > offre D ($M = 1,82$) > offre A ($M = 1,21$).

Toutes les offres modifiées augmentent significativement le montant investi par rapport à A.

Le jargon (B) surpasse significativement l'urgence et la preuve sociale (C et D), mais l'écart entre l'urgence (C) et la preuve sociale (D) n'est pas significatif ($p = 0,7974$).



Hiérarchisation des offres par les répondants (Q41)

La tâche de classement final confirme les résultats (1 = plus suspect, 4 = moins suspect) :

L'offre A est jugée la plus suspecte (55%, n = 84 pour le rang 1) ;

L'offre D se positionne aux échelons de suspicion forte à modérée (36%, n = 55 pour le rang 2 et le rang 3) ;

L'offre C se concentre au rang 3 avec une suspicion modérée (52%, n = 80) ;

L'offre B est plébiscitée comme la moins suspecte par 72% (n = 110) des participants (rang 4).

Chapitre 4 : Discussion

Section 4.1 : Profils socio-démographiques

Une analyse rigoureuse de notre échantillon d'étude valide globalement la robustesse de la méthode des quotas appliquée (sexe, âge, niveau d'instruction), tout en révélant des déviations structurelles inhérentes aux enquêtes par questionnaire numérique (*Computer-Assisted Web Interviewing* — CAWI).

D'une part, si la répartition de genre s'avère représentative (avec un écart maximal de seulement 3% par rapport aux données nationales de Statbel, 2026), l'analyse met en évidence une sous-représentation marquée des individus âgés de plus de 65 ans (écart négatif de près de 8% par rapport à Statbel, 2026). Ce phénomène illustre la persistance d'une fracture numérique de second degré (Brotcorne & Valenduc, 2009). Comme le démontrent ces auteurs, les inégalités face au digital ne s'expriment plus en termes d'accès matériel — l'usage d'Internet s'étant démocratisé chez les 65-74 ans (Statbel, 2024) —, mais s'articulent autour d'un fossé d'usages, de compétences cognitives et d'intérêt à interagir avec des protocoles académiques digitalisés.

D'autre part, un biais d'homophilie sociale et académique (Quivy & Van Campenhoudt, 2011) se traduit par une surreprésentation de 11% des profils hautement diplômés (49% de l'échantillon étant issu de l'enseignement supérieur), un effet de réseau direct lié au statut universitaire du chercheur.

Toutefois, d'un point de vue épistémologique, ces biais n'altèrent pas la validité interne de notre recherche. Notre objet d'étude étant structurellement ancré sur Internet (les fraudes financières manipulées par l'IA présupposant une diffusion numérique), il exigeait intrinsèquement d'interroger une

population connectée. Un senior déconnecté ne fait pas partie de la population cible pertinente, puisqu'il se situe hors de portée d'un stimulus frauduleux sur les réseaux sociaux. Notre échantillon ne doit donc pas être lu comme un miroir absolu de la démographie macroéconomique belge, mais comme une photographie fidèle de la population internaute active, cible prioritaire des cyber-fraudeurs.

Section 4.2 : Les habitudes financières

Le premier apport majeur de cette discussion réside dans la mise au jour d'un paradoxe cognitif flagrant entre la compétence financière réelle des participants et leur sentiment de sécurité face aux technologies émergentes. Nos données indiquent que plus des deux tiers des répondants (69%) admettent de sérieuses limites en matière de placement en se qualifiant de « novices » ou « débutants » (Q5). Cette faible littératie financière perçue se traduit logiquement par une posture d'évitement comportemental, 83 % de l'échantillon exprimant un désintéressement massif à l'égard des opportunités d'investissement en ligne (Q6). Pourtant, en totale contradiction avec cette prudence déclarée, 54% des répondants s'estiment tout à fait capables de déceler une fraude financière exploitant l'IA générative (Q42).

Ce décalage caractérise un biais d'excès de confiance (*overconfidence bias*), théorisé par Kahneman (2012) comme une illusion de maîtrise altérant l'évaluation objective des risques. En contexte numérique, cette assurance exagérée s'avère extrêmement délétère : elle désarme la vigilance active de l'internaute. Convaincu de sa capacité de détection, l'individu réduit ses réflexes de vérification.

Or, l'examen du passé victimaire (Q40) démontre que le risque cyber-financier n'a rien d'abstrait : 55% des répondants rapportent avoir déjà été personnellement ciblés par une tentative d'arnaque en ligne. Bien que le taux de conversion effectif (victimes avec préjudice financier direct) ne s'élève qu'à 2%, sa transposition macroéconomique est alarmante. Projeté sur les quelque 11,9 millions de citoyens belges, ce taux de 2% équivaut potentiellement à 240.000 victimes effectives à l'échelle nationale. Cette criminalité de masse permet aux organisations malveillantes de générer des profits se chiffrant en millions d'euros, rentabilisant des campagnes de prospection pourtant rejetées par la majorité.

Section 4.3 : Hypothèse 1 : le langage technique

La première hypothèse (H1) postulait que l'intégration de l'IA générative et des grands modèles de langage (LLM) neutralise les indices linguistiques traditionnels de fraude (fautes d'orthographe, syntaxe approximative) qui servaient historiquement de heuristiques de défense à l'investisseur (Europol, 2023 ; TRM Labs, 2024). En substituant la méfiance instinctive par un jargon technique irréprochable et fluide, l'IA génère une illusion de professionnalisme qui installe une crédibilité immédiate, rendant l'hameçonnage indiscernable d'une communication légitime (Singh Chauhan, 2025 ; Wan Fakhruddin et al., 2026). Nos résultats valident de manière unanime cette hypothèse opérationnelle, consacrant l'existence d'une corrélation positive entre la sophistication linguistique du message et sa crédibilité perçue.

Sur le plan empirique, la comparaison des réactions face à l'énoncé informel et neutre (offre A) et l'énoncé au langage technique expert (offre B) démontre une rupture majeure des défenses psychologiques des participants. L'habillage sémantique sophistiqué déplace significativement l'intérêt subjectif des répondants ($t(152) = 14,01$; $p < 0,0001$), fait s'effondrer le pôle d'évitement au profit d'une intention d'action marquée sur le plan du clic ($t(151) = 9,75$; $p < 0,0001$), et provoque une véritable levée des inhibitions financières. Lors de l'allocation d'un capital fictif de 1.000 €, le test t confirme une

augmentation massive de la prise de risque ($t(150) = 15,10$; $p < 0,0001$), l'investissement conséquent (501 € - 750 €) devenant instantanément la modalité dominante, plébiscitée par 39% de l'échantillon.

Pour expliciter ce court-circuit de la rationalité, nos données valident de manière empirique le Modèle de Probabilité d'Élaboration (ELM ; Petty & Cacioppo, 1986) qui explique les décisions d'une personne suivant son traitement de l'information. Ce cadre théorique modélise la façon dont un individu traite un message persuasif selon deux voies. Un parallèle direct peut être établi avec les Systèmes 1 et 2 de Kahneman (2011) : la route périphérique de l'ELM correspond aux heuristiques du Système 1, tandis que la route centrale exige l'effort cognitif et analytique du Système 2. En présentant un projet complexe et formellement parfait, l'IA sature la mémoire de travail de la victime par une surcharge cognitive (Wan Fakhruddin et al., 2026). Face à cette complexité technique, notre étude démontre que 81% des participants abandonnent la route centrale (traitement analytique) pour adopter une stratégie de traitement périphérique (heuristique), s'en remettant à l'impression globale de professionnalisme (36%) ou au sérieux du ton (45%). Le test d'ajustement du χ^2 de Pearson confirme la nature hautement systémique et non aléatoire de cette préférence pour les indices de surface ($\chi^2(2, N = 153) = 16,16$; $p = 0,0003$). Sous l'effet de cette surcharge, le Système 2 analytique capitule au profit du Système 1 intuitif, structurellement plus sensible aux biais émotionnels et à l'urgence (Kahneman, 2011 ; Vishwanath et al., 2011). En manipulant un vocabulaire spécialisé (ex. : Euronext, arbitrage), le jargon n'est plus analysé pour son contenu, mais est utilisé de manière erronée comme une preuve d'autorité.

Cette dynamique s'appuie sur des représentations mentales profondément ancrées au sein de la population belge étudiée. En effet, 97% des répondants considèrent qu'une institution sérieuse ne commet jamais de fautes d'orthographe (Q34) et 65% assimilent le jargon technique à une preuve directe de compétence (Q35). En répondant point par point à ces croyances, l'offre B est perçue par 71% des sujets comme émanant de manière exclusive d'une institution financière régulée (Q25).

En conclusion, l'absence de « bruit » linguistique focalise l'attention de la cible exclusivement sur les stimuli émotionnels liés au FOMO (*Fear Of Missing Out*) (Mouton et al., 2016). Ces résultats s'inscrivent dès lors parfaitement dans la transition théorique du « triangle de la fraude » (Cressey, 1953) vers le « diamant de la fraude » (Wolfe & Hermanson, 2004). En éliminant les fautes de syntaxe qui servaient historiquement de filtres de sécurité (Europol, 2023), l'IA générative dote les fraudeurs d'une capacité opérationnelle inédite : elle installe une crédibilité immédiate, laissant l'internaute perméable aux suggestions d'exclusivité et maximisant ainsi son taux de vulnérabilité.

Section 4.4 : Hypothèse 2 : la pression temporelle

La deuxième hypothèse (H2) de cette recherche postulait que la capacité de l'IA générative à produire des scénarii d'urgence hyper-personnalisés exacerbe le sentiment de *Fear Of Missing Out* (FOMO), provoquant une priorisation du Système 1 au détriment du Système 2. En s'appuyant sur la théorie du double processus (Kahneman, 2011), nous suggérons que l'IA industrialise une compression temporelle capable de paralyser le raisonnement analytique et délibéré au profit d'une réaction instinctive et impulsive (Hock & Button, 2023 ; Wan Fakhruddin et al., 2026). Sur le plan empirique, nos résultats valident cette hypothèse en démontrant l'existence d'une association directe entre l'intensité du sentiment de contrainte temporelle et la réceptivité aux sollicitations d'investissements frauduleux.

L'analyse de l'offre C révèle le rôle central de la contrainte temporelle comme levier de désengagement des barrières psychologiques des consommateurs. Alors que l'énoncé neutre (offre A) suscitait un désintérêt quasi unanime — marqué par un rejet total de 75% des participants —, l'introduction du facteur d'urgence fait s'effondrer ce pôle d'évitement à seulement 35%. Ce basculement

de l'intérêt général est statistiquement validé par un test t de Student pour échantillons appariés hautement significatif ($t(152) = 9,41$; $p < 0,0001$), matérialisant une progression nette de la moyenne d'intérêt (MA = 1,28 vs MC = 1,88).

Cette levée des défenses cognitives ne se limite pas à une simple attitude déclarative ; elle se traduit par un véritable saut comportemental. Au niveau des intentions de clic (Q29), le refus catégorique recule de 21 points (passant de 57% à 36%), un bond inducteur d'action, lui aussi confirmé par les analyses inférentielles ($t(151) = 7,24$; $p < 0,0001$). L'impact le plus remarquable de cette stratégie d'urgence se cristallise néanmoins dans la prise de risque financière (Q30). Face à l'offre C, les verrous budgétaires cèdent massivement : une nette majorité de répondants (63%) accepte d'allouer une somme intermédiaire non négligeable (entre 251 € et 500 €), une rupture comportementale majeure validée par le test t ($t(150) = 12,76$; $p < 0,0001$). La cohérence interne de ce mécanisme d'engagement est soutenue par de fortes corrélations positives : l'intérêt initial (Q27) se synchronise étroitement avec l'intention de clic ($r = 0,76$; $p < 0,0001$) et avec le montant investi ($r = 0,59$; $p < 0,0001$). L'urgence temporelle agit ainsi comme un puissant catalyseur, capable d'aligner la réceptivité psychologique, l'intention numérique et la mise en danger financière de l'utilisateur.

L'apport majeur de nos analyses réside dans la démonstration que le sentiment d'urgence n'affecte pas les individus de manière uniforme, mais s'appuie sur une prédisposition psychologique sous-jacente. La génération de stimuli de rareté active un mécanisme d'évitement de la perte ancré dans l'anxiété sociale (Baumeister & Leary, 1995 ; Przybylski et al., 2013). Le calcul du coefficient de corrélation linéaire de Pearson (r) montre que le score « Total FOMO » des répondants n'exerce aucune influence sur l'offre neutre ($r = 0,10$), mais s'associe de manière robuste avec l'ensemble des indicateurs de l'offre C : l'intérêt ($r = 0,38$), l'intention de clic ($r = 0,32$) et le montant financier consenti ($r = 0,30$). Ce couplage structurel est réaffirmé par l'analyse non paramétrique de Spearman (ρ), hautement prédictive des comportements face à l'urgence ($\rho = 0,37$; $p < 0,0001$ pour l'intérêt et $\rho = 0,30$; $p = 0,0002$ pour le clic).

L'analyse de variance (ANOVA) vient parachever cette démonstration en scindant l'échantillon selon la sensibilité au FOMO. Pour l'intérêt subjectif ($F(2, 150) = 11,70$; $p < 0,0001$; $R^2 = 0,135$) comme pour l'intention de clic ($F(2, 150) = 10,88$; $p < 0,0001$; $R^2 = 0,127$), les individus manifestant un FOMO aigu (groupe 3) se détachent de manière flagrante en s'exposant à des pertes financières significativement plus élevées ($F(2, 149) = 5,56$; $p = 0,0047$). D'un point de vue cognitif, la pression temporelle impose une compression qui paralyse le Système 2 (analytique, délibéré, lent). Face à la contrainte de temps, les ressources cognitives sont saturées, empêchant l'investisseur d'effectuer les vérifications élémentaires (*due diligence*) auprès des organismes de régulation comme la FSMA (Vishwanath et al., 2011 ; Lyu et al., 2025, cité dans Wan Fakhruddin et al., 2026). L'individu bascule sur son Système 1 (intuitif, rapide), activant les leviers de la théorie des perspectives (Kahneman, 2011) : sous l'effet du FOMO, l'esprit est submergé par une aversion aiguë à la perte. La crainte de « rater » une opportunité financière l'emporte sur l'évaluation objective du risque (Mouton et al., 2016). L'IA générative agit ici comme un multiplicateur de vulnérabilité en calibrant des stimuli d'urgence hyper-personnalisés, maximisant ainsi l'anxiété de la cible (Blauth et al., 2022).

Un dernier enseignement repose sur un paradoxe méthodologique et psychologique remarquable : la déconnexion totale entre l'influence effective des stimuli d'urgence et la perception consciente qu'en ont les répondants. Interrogés sur la tension ressentie à la lecture du minuteur (Q28), seuls 10% des répondants reconnaissent une tension les poussant à agir, tandis que l'écrasante majorité (60%) exprime un rejet formel. De même, l'idée qu'un compte à rebours puisse neutraliser leurs réflexes de vérification (Q37) est massivement rejetée par 92% de l'échantillon. Ce décalage flagrant entre le

refus déclaratif d'être influencé et la réalité des comportements mesurés — où les tests statistiques prouvent que l'urgence fait bondir les investissements — met en évidence l'action subliminale et automatique du Système 1. L'internaute est intimement convaincu d'être imperméable aux techniques grossières du compte à rebours, ce qui renforce l'excès de confiance général. Le piège de la rareté fonctionne à l'insu de sa propre rationalité, neutralisant de fait toute forme de cyber-défense active (Baumeister & Leary, 1995).

Section 4.5 : Hypothèse 3 : les deepfakes

La troisième hypothèse (H3) de cette recherche avançait que l'intégration de contenus synthétiques de type *deepfake* (hypertrucages) génère un biais de crédibilité majeur, où la sophistication visuelle et sonore de l'IA générative est indûment perçue comme un gage de légitimité financière (Ivan, 2022 ; Sholademi, 2024). Cette capacité à imiter parfaitement la réalité crée une « vérité synthétique » (Blauth et al., 2022) capable de rendre la manipulation indétectable pour un utilisateur non averti, court-circuitant ainsi sa vigilance rationnelle. Nos résultats empiriques valident cette hypothèse opérationnelle, confirmant l'existence d'une corrélation positive entre l'intégration de médias synthétiques et le degré de crédibilité accordé à l'offre d'investissement.

Sur le plan descriptif, l'introduction d'un stimulus audiovisuel incarnant une figure de notoriété publique au sein de l'offre D (Q31) transforme radicalement la posture de méfiance absolue observée face à la fraude contrôle (offre A). Le taux de participants se déclarant « Pas du tout intéressés » s'effondre de manière spectaculaire, passant de 75% à 44%. Le test *t* de Student pour échantillons appariés consacre la robustesse statistique de ce déplacement de l'intérêt subjectif : $t(152) = 6,98$; $p < 0,0001$. Cette dynamique de désarmement se transpose de manière identique sur l'intention comportementale de clic (Q32), où le pôle d'évitement strict (« Aucune chance ») recule de près de 13 points, un bond inducteur d'action validé par les analyses inférentielles : $t(151) = 4,49$; $p < 0,0001$.

La conséquence la plus lourde de cette autorité factice se révèle dans la propension des répondants à engager des fonds. Face au *deepfake* (Q33), le palier de prudence minimale (1 € - 250 €), qui verrouillait 80% de l'échantillon sous l'offre A, subit une baisse considérable au profit du montant intermédiaire (251 € - 500 €) qui capte désormais 46% des sujets. Le test *t* apparié pour échantillons dépendants confirme cette levée majeure des barrières de protection économique : $t(151) = 9,99$; $p < 0,0001$ (MD = 1,83 contre MA = 1,21). L'image animée d'une personnalité publique parvient donc à convaincre les internautes d'engager des sommes plus importantes, prouvant que le réalisme technique est confondu avec la fiabilité institutionnelle (Singh Chauhan, 2025).

Pour comprendre les ressorts de cette vulnérabilité, il convient d'analyser la nature des stimuli audiovisuels générés par l'IA (Emett et al., 2024). En clonant la voix et l'image de personnalités reconnues (experts, dirigeants, célébrités), les fraudeurs mobilisent simultanément les biais d'autorité et de preuve sociale, opérant un transfert de légitimité immédiat vers l'offre (Mouton et al., 2016 ; Vaccari & Chadwick, 2020). Nos données confirment que la preuve sociale constitue une faille de sécurité cognitive majeure au sein de la population belge étudiée : 77% des répondants admettent explicitement que voir d'autres personnes (ou des proches) avoir déjà investi les rassure sur la légitimité d'un projet (Q38). En simulant de faux témoignages et des communautés automatisées (Hock & Button, 2023 ; Wan Fakhrudin et al., 2026), l'IA installe l'illusion d'un consensus de marché qui vient renforcer l'effet d'autorité.

D'un point de vue cognitif, ce processus court-circuite les barrières (Emett et al., 2024). Le réalisme des médias générés par IA est si parfait qu'il parvient à saturer les capacités analytiques du Système 2. Même lorsque l'investisseur tente d'activer une pensée critique, la perfection technique du *deepfake* neutralise les indices habituels de suspicion. Le doute est noyé dans l'illusion technologique, ce qui explique pourquoi l'anxiété du FOMO prend le pas sur la prudence réglementaire. Ce phénomène fait directement écho aux constats de la FSMA (2025) et de la CVMO (2025), qui soulignent que les publicités frauduleuses exploitent massivement ces visages connus pour maximiser leur taux de conversion à l'insu de l'absence de régulation réelle.

À l'instar de l'analyse de la pression temporelle, cette section met en exergue un paradoxe méthodologique remarquable, révélant une importante illusion de contrôle chez les répondants. Interrogés de manière directe sur le postulat théorique (Q39 : « L'apparition d'une personnalité publique en vidéo renforce la crédibilité d'un projet »), l'immense majorité des participants (65%) affiche une posture défensive et rejette cette affirmation, seuls 31% admettant y être sensibles en théorie. Ce décalage flagrant entre le refus déclaratif d'être influencé et la réalité des comportements mesurés — où les tests statistiques prouvent que l'urgence visuelle fait bondir les investissements — met en évidence l'action des heuristiques de surface de la route périphérique (ELM ; Petty & Cacioppo, 1986). Consciemment, l'individu applique une norme sociale de vigilance, mais face au stimulus concret, le Système 1, séduit par la fluidité, le réalisme visuel et le sentiment de familiarité face à un visage connu, valide l'offre. Cette vulnérabilité inconsciente rend l'usage des *deepfakes* d'autant plus systémique et dangereux (TRM Labs, 2024) : en exploitant des biais cognitifs qui agissent sous le radar de la conscience, les cybercriminels désarment les réflexes de *due diligence*, transformant la confiance publique en une passerelle directe vers la spoliation financière.

Section 4.6 : Analyses transversales : comparaison inter-scenarii

L'analyse isolée des différentes hypothèses laisse place à une perspective transversale indispensable pour appréhender l'efficacité différentielle des leviers d'ingénierie sociale assistée par IA. Pour mesurer cette réceptivité, trois dimensions décisionnelles ont été modélisées via des analyses de variance (ANOVA) complétées par des tests *post-hoc* de Tukey-Kramer (HSD) : l'intérêt subjectif, l'intention comportementale de clic et l'allocation financière fictive (prise de risque).

Les résultats factuels et les classifications de ces analyses de variance sont synthétisés dans le tableau comparatif ci-dessous.

Tableau 1 : Comparaison transversale de l'impact des stimuli de fraude (n = 153)

Dimensions mesurées	Offre A	Offre B	Offre C	Offre D	Statistiques de l'ANOVA
Intérêt subjectif	1,28 ^c	2,13 ^a	1,88 ^b	1,74 ^b	$F(3, 608) = 36,83$ $p < 0,0001$ $R^2 = 0,154$

Dimensions mesurées	Offre A	Offre B	Offre C	Offre D	Statistiques de l'ANOVA
Intention de clic	1,45 ^c	1,95 ^a	1,81 ^{ab}	1,70 ^b	$F(3, 607) = 15,49$ $p < 0,0001$ R² = 0,071
Prise de risque (Allocation sur 1.000 €)	1,21 ^c	2,18 ^a	1,89 ^b	1,82 ^b	$F(3, 605) = 54,45$ $p < 0,0001$ R² = 0,213

Note : Les moyennes partageant une même lettre en exposant (a, b, c) ne diffèrent pas significativement au seuil de $\alpha = 0,05$ selon le test post-hoc de Tukey-Kramer.

Le test HSD de Tukey-Kramer démontre que l'offre B (jargon technique) suscite un intérêt significativement supérieur à toutes les autres configurations expérimentales, l'écart avec l'offre contrôle étant maximal ($\Delta M = 0,85$; $p < 0,0001$). De surcroît, le jargon surpasse de manière artificielle le levier de l'urgence temporelle (offre C) ($\Delta M = 0,25$; $p = 0,0119$) et l'argument d'autorité (offre D) ($\Delta M = 0,39$; $p < 0,0001$). Bien que l'urgence temporelle présente une moyenne légèrement plus élevée que le *deepfake* de notoriété, leur différence n'est pas statistiquement définie ($p = 0,3495$), marquant une force de captation équivalente à un niveau intermédiaire.

L'intention comportementale de cliquer sur le lien hypertexte varie également de manière significative selon la nature du stimulus ($R^2 = 0,071$). Toutes les offres frauduleuses modifiées provoquent une hausse hautement significative du cliquage par rapport à l'énoncé contrôle A ($p < 0,0001$ pour B et C ; $p = 0,0061$ pour D). Le jargon technico-financier demeure le déclencheur d'action le plus puissant, surpassant significativement l'argument d'autorité ($\Delta M = 0,25$; $p = 0,0053$). En revanche, l'écart d'intention comportementale entre le jargon (offre B) et l'urgence (offre C) s'atténue sous l'effet de la contrainte et perd sa significativité statistique ($p = 0,2412$).

Lorsqu'il s'agit d'allouer un capital théorique de 1.000 €, le type de stimulus détermine plus de 21% de la variance des décisions financières de placement ($F = 54,45$; $p < 0,0001$). Les tests de comparaisons multiples confirment la suprématie absolue de la respectabilité sémantique : l'offre B génère une prise de risque financier maximale, s'élevant de manière hautement significative au-dessus de l'offre contrôle A ($\Delta M = 0,97$), de l'offre D ($\Delta M = 0,35$) et de l'offre C ($\Delta M = 0,28$). Les leviers d'urgence et d'autorité synthétique forment un sous-groupe homogène sans différence statistique ($p = 0,7974$), bien que tous deux induisent une exposition au risque drastiquement supérieure au contrôle.

L'examen final de la tâche de classement post-expérimentale (Q41) parachève cette démonstration. L'offre A est reconnue massivement comme la plus suspecte par 55% des participants (Rang 1), prouvant qu'un message simpliste déclenche immédiatement la méfiance. À l'inverse, l'offre D se positionne aux échelons de suspicion forte à modérée (36% en Rang 1 et Rang 2), tandis que l'offre C se concentre massivement au Rang 3 (52%), s'établissant comme une menace modérée ou faible dans l'esprit collectif. Le résultat le plus spectaculaire concerne l'offre B, plébiscitée de manière écrasante

comme la moins suspecte par 72% de l'échantillon (Rang 4), alors qu'à peine un seul participant (1%) est parvenu à déceler sa nature frauduleuse.

L'analyse croisée de ces résultats transversaux permet de dresser un constat criminologique fondamental : l'ingénierie sociale assistée par Intelligence Artificielle ne se contente pas d'optimiser les techniques de fraude préexistantes, elle redéfinit entièrement la hiérarchie des vulnérabilités humaines en contexte numérique. La convergence des tests ANOVA et *post-hoc* consacre de manière indiscutable la suprématie du jargon technico-financier (offre B). La respectabilité sémantique, débarrassée de ses fautes syntaxiques grâce aux modèles de langage de type LLM, s'impose comme le vecteur de légitimité le plus redoutable. Le fait que près de 72% des répondants aient classé cette offre comme la moins suspecte démontre que la sophistication linguistique est indûment confondue avec l'intégrité réglementaire, plongeant les internautes belges dans un aveuglement cognitif majeur.

Cette suprématie du texte expert éclaire d'un jour nouveau le Modèle de Probabilité d'Élaboration (ELM) et le système 1/2 de Kahneman appliqué à la cybercriminologie. Si l'urgence (offre C) et le *deepfake* d'autorité (offre D) provoquent également une baisse générale de la vigilance, ils agissent principalement comme des catalyseurs émotionnels secondaires. L'urgence temporelle, bien qu'efficace pour induire l'action de clic et l'allocation budgétaire en saturant la mémoire de travail des profils sensibles au FOMO, demeure plus facilement identifiable comme un artifice marketing lors d'un examen posé. De même, la « vérité synthétique » véhiculée par les *deepfakes* audiovisuels suscite encore une relative méfiance, les répondants la classant à un niveau de suspicion supérieur à la manipulation textuelle. Le véritable danger réside donc dans l'action subliminale de la route périphérique face au jargon : l'internaute capitule devant la complexité sémantique et externalise son jugement critique au profit d'une confiance aveugle. Cet impact moins puissant de la pression temporelle et des *deepfakes* via la preuve sociale peut s'expliquer par l'actualité des phénomènes frauduleux qui oblige l'État et ses divers organismes officiels à faire plus de prévention afin de protéger la population. De ce fait, la population est, de manière générale, mieux informée des techniques frauduleuses et risque moins de tomber dans le piège.

Enfin, il est important de garder en tête que cette recherche a analysé l'impact des différentes techniques de manière indépendante. Pourtant, dans la réalité, les fraudeurs utilisent l'ensemble de ces méthodes de façon imbriquée. L'action conjointe de ces trois techniques rend ainsi la fraude potentiellement beaucoup plus redoutable qu'une simple escroquerie classique n'utilisant pas l'IA.

Chapitre 5 : Limites de l'étude

Tout protocole de recherche empirique, aussi rigoureux soit-il, s'inscrit dans des choix méthodologiques et contextuels qui en circonscrivent la portée, et il convient de mettre en lumière les principales limites qui ont jalonné cette étude afin de garantir l'honnêteté scientifique de ce travail.

La première limite majeure tient au biais de représentativité de l'échantillon et à la composition finale du groupe de répondants ; l'enquête ayant été diffusée exclusivement en langue française, elle exclut d'emblée une partie de la population belge, tandis que l'analyse descriptive indique que certains quotas démographiques et socio-économiques n'ont pas été rigoureusement respectés par rapport à la population générale. Néanmoins, ce manque de représentativité stricte s'avère parfaitement cohérent et logique avec le contexte de l'étude, puisque la population ayant massivement répondu présente des caractéristiques d'âge, d'éducation et de connectivité qui correspondent précisément au profil des utilisateurs actifs des réseaux sociaux et des plateformes d'investissement en ligne, faisant d'eux le public

cible prioritaire des organisations criminelles et la population la plus vulnérablement exposée aux stimuli du FOMO (*Fear of Missing Out*) (Przybylski et al., 2013).

Par ailleurs, une seconde limite réside dans le biais de simulation découlant de la nature artificielle des scénarii construits ; bien que les stimuli basés sur l'IA générative (jargon financier complexe, messages d'urgence et *deepfakes*) aient été conçus pour reproduire les modes opératoires actuels, le cadre d'évaluation reste virtuel. Face à un questionnaire universitaire, le participant se trouve dans une posture d'observation consciente, souvent empreinte d'un biais de désirabilité sociale ou d'une vigilance accrue, alors qu'en situation réelle, l'activation du Système 1 de Kahneman (2011) s'opère dans un moment de distraction, de fatigue ou de stress financier aigu. L'absence d'enjeu financier réel et la stativité proposées ne permettent pas de capturer pleinement la charge persuasive et l'interactivité dynamique que déploient les réseaux cybercriminels lors d'un processus d'endoctrinement complet.

De plus, il convient de souligner une limite importante de cette recherche : l'impact de chaque technique a été analysé de manière isolée. Dans la réalité, les fraudeurs combinent habilement ces différents procédés pour maximiser la portée de leur attaque. Par conséquent, une cyberattaque combinant ces trois techniques s'avère potentiellement bien plus redoutable qu'une fraude classique n'exploitant pas l'intelligence artificielle.

Enfin, sur le plan technologique, cette étude se heurte à l'obsolescence rapide de l'Intelligence Artificielle générative (TRM Labs, 2024), dont la vitesse exponentielle d'évolution implique que les conclusions tirées à un instant donné nécessitent une réévaluation continue, même si les mécanismes psychologiques sous-jacents et les structures criminologiques modélisées par le diamant de la fraude de Wolfe et Hermanson (2004) demeurent constants.

Chapitre 6 : Perspectives de la recherche

Les conclusions de cette étude ouvrent plusieurs voies de recherche et d'applications pratiques indispensables pour adapter la lutte contre la cybercriminalité financière aux réalités technologiques contemporaines. Sur le plan de la recherche empirique, une perspective essentielle consisterait à dépasser le cadre des scénarii déclaratifs en concevant des protocoles expérimentaux immersifs — par exemple via des environnements de simulation d'investissement contrôlés mais dynamiques —, afin d'observer en temps réel les réactions comportementales des individus soumis au stress d'une compression temporelle ou face à des agents conversationnels interactifs pilotés par l'IA. De plus, il serait très intéressant pour les recherches futures de créer un protocole expérimental testant non pas les variables de manière isolée, mais un scénario cumulatif (IAG totale) afin de mesurer si l'effet de vulnérabilité est additif ou exponentiel.

Sur le plan pratique et préventif, cette recherche met en évidence l'obsolescence des campagnes de sensibilisation traditionnelles axées sur le repérage d'indices de surface (fautes d'orthographe, syntaxe approximative) que les grands modèles de langage ont désormais totalement gommé. Une perspective d'action majeure réside donc dans le développement de stratégies d'« immunisation cognitive », consistant à éduquer les internautes non pas sur les aspects techniques des messages frauduleux, mais sur leurs propres vulnérabilités psychologiques et sur les mécanismes de manipulation émotionnelle du Système 1. Enfin, du côté de la cyberdéfense, l'industrialisation de la fraude par l'IAG exige une réponse technologique symétrique : la recherche future devra s'articuler autour de la conception d'outils de détection automatisée et d'authentification des contenus en temps réel, capables de restaurer l'écosystème de confiance numérique altéré par la prolifération des médias synthétiques, enrichissant ainsi continuellement les grilles d'analyse du crime face à la reconfiguration permanente de la capacité opérationnelle des délinquants.

Partie IV : Conclusion

Ce travail de fin d'études s'est donné pour mission d'explorer un angle mort mais hautement critique de la cybercriminologie contemporaine : l'exploitation des vulnérabilités humaines par le biais de technologies automatisées de pointe. À la croisée de l'évolution technologique et de la psychologie cognitive, notre recherche s'est structurée autour de la problématique fondamentale suivante : « *Dans quelle mesure l'utilisation ciblée de l'Intelligence Artificielle générative, à travers l'exploitation des leviers cognitifs et émotionnels liés au syndrome du FOMO, reconfigure-t-elle le paysage de la fraude aux investissements ?* ». La thèse défendue tout au long de cette étude soutient que l'Intelligence Artificielle générative ne se limite pas à une simple amélioration technique des outils de communication des fraudeurs. En réalité, elle agit comme un catalyseur clinique capable d'industrialiser l'ingénierie sociale en exploitant de manière sur-mesure des biais comportementaux profondément ancrés, tels que le syndrome du FOMO (Przybylski et al., 2013), neutralisant ainsi les réflexes de vigilance traditionnels des internautes.

L'analyse croisée du cadre théorique et des données empiriques permet de synthétiser les résultats autour de nos trois axes de recherche, révélant comment les cybercriminels saturent les capacités cognitives de leurs cibles pour neutraliser leur vigilance. D'une part, l'utilisation par les grands modèles de langage (LLM) d'un jargon technico-financier complexe et exempt de fautes (H1) sature la mémoire de travail de la victime (Wan Fakhruddin et al., 2026), effaçant les indices d'alerte habituels au profit d'une illusion de légitimité institutionnelle. D'autre part, l'imposition d'une pression temporelle artificielle (H2) active le biais de rareté et le syndrome du FOMO (Przybylski et al., 2013), ce qui sature immédiatement le « Système 1 » instinctif au détriment du « Système 2 » analytique, poussant ainsi à des décisions financières impulsives. Enfin, l'intégration de *deepfakes* (H3) matérialisant des figures d'autorité ou de fausses preuves sociales opère un déplacement perceptif de la confiance (Vaccari & Chadwick, 2020), affaiblissant les postures d'évitement face à une tromperie devenue visuellement indiscutable.

L'analyse transversale de ces éléments révèle un paradoxe cognitif majeur, particulièrement saillant au sein de la population belge : alors qu'une majorité d'individus affiche un excès de confiance en s'estimant capable de détecter une tentative de fraude assistée par IA, la convergence simultanée de ces trois stimuli (technique, temporel et visuel) crée un aveuglement cognitif quasi total. Sur le plan criminologique, cette convergence valide la pertinence du passage du « triangle de la fraude » de Cressey (1953) au « diamant de la fraude » de Wolfe et Hermanson (2004) : l'IA générative vient modifier de manière exponentielle la variable de la capacité opérationnelle du délinquant, lui permettant d'industrialiser une ingénierie sociale sur-mesure autrefois impossible à automatiser à grande échelle.

En guise d'ouverture, les résultats de ce mémoire soulignent l'urgence de repenser structurellement nos paradigmes de cybersécurité et de prévention. Les campagnes de sensibilisation classiques, centrées sur la détection passive d'indices textuels malveillants, apparaissent aujourd'hui obsolètes face à la perfection linguistique de l'IA. Il devient impératif de migrer vers des stratégies d'immunisation cognitive (Vishwanath et al., 2011), visant à éduquer les internautes sur leurs propres biais psychologiques (comme le FOMO) et sur les mécanismes de manipulation émotionnelle. C'est uniquement en renforçant la résilience psychologique des individus et en développant des outils de détection technique de l'IA (solutions d'authentification des contenus, filtres sémantiques avancés) que la société pourra rétablir l'équilibre face à une criminalité financière désormais automatisée et individualisée.

Bibliographie

Articles scientifiques :

- Appel, G., Grewal, L., Hadi, R., & Stephen, A. T. (2020). The future of social media in marketing. *Journal of the Academy of Marketing Science*, 48(1), 79–95. <https://doi.org/10.1007/s11747-019-00695-1>
- Bădele, C. S. (2021). Digital expertise and artificial intelligence in identifying fraud and cybercrime. *Challenges of the Knowledge Society*, 13(2), 793–802. <https://doi.org/10.46337/cks.13.2.14>
- Baumeister, R. F., & Leary, M. R. (1995). The need to belong: Desire for interpersonal attachments as a fundamental human motivation. *Psychological Bulletin*, 117(3), 497–529. <https://doi.org/10.1037/0033-2909.117.3.497>
- Beyens, I., Frison, E., & Eggermont, S. (2016). "I don't want to miss a thing": Adolescents' fear of missing out and its relationship to adolescents' social needs, Facebook use, and Facebook related stress. *Computers in Human Behavior*, 64, 1–8. <https://doi.org/10.1016/j.chb.2016.05.083>
- Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *IEEE Access*, 10, 77110-77122. <https://doi.org/10.1109/ACCESS.2022.3191790>
- Brotcorne, P., & Valenduc, G. (2009). Les compétences numériques et les inégalités dans les usages du numérique. *Les Cahiers du Numérique*, 5(1), 45-68. <https://doi.org/10.3166/lcn.5.1.45-68>
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. <https://doi.org/10.2307/2094589>
- Emett, S., Eulerich, M., Pickerd, J., & Wood, D. A. (2024). *Short and synthetically distort: Investor reactions to deepfake financial news* (Faculty Publications, 8317). BYU ScholarsArchive. <https://doi.org/10.2139/ssrn.4869830>
- Fan, X., Wu, Y., Zhou, Y., & Wu, S. (2025). How does artificial intelligence shock affect labor income distribution? Evidence from China. *Pacific-Basin Finance Journal*, 90, Article 102691. <https://doi.org/10.1016/j.pacfin.2025.102691>
- Gefen, A. (2022). IA : pour une histoire culturelle. *Revue d'histoire culturelle*, (4). <https://doi.org/10.4000/rhc.1204>
- Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems (NIPS)*, 27. <https://doi.org/10.1145/3422622>
- Haiech, J. (2020). Parcourir l'histoire de l'intelligence artificielle, pour mieux la définir et la comprendre. *médecine/sciences*, 36(10), 919–923. <https://doi.org/10.1051/medsci/2020145>

- Hock, B., & Button, M. (2023). Non-ideal victims or offenders? The curious case of pyramid scheme participants. *Victims & Offenders*, 18(7), 1311–1334. <https://doi.org/10.1080/15564886.2023.2186996>
- Ivan, L. (2022). Current and future threats of artificial intelligence (AI) and ways to combat them in cyberspace. *Forensic Science*, 23(4), 253–258. <https://search.proquest.com/openview/11d10b551dc8f01821548f9ff628e564/1.pdf>
- Ivantchev, B., & Ivantcheva, M. (2024). FOMO effect: Social media and online traders. *Journal of Management and Financial Sciences*, (48). <https://doi.org/10.33119/JMFS.2023.48.4>
- Jia, J., & Li, Q. (2025). *AutoTool: Efficient tool selection for large language model agents*. arXiv. <https://doi.org/10.48550/arXiv.2511.14650>
- Li, H. (2024). I cannot miss it for the world: The relationship between fear of missing out (FOMO) and acceptance of ChatGPT. *Basic and Applied Social Psychology*, 46(5), 285–294. <https://doi.org/10.1080/01973533.2024.2365274>
- Milyavskaya, M., Saffran, M., Hope, N., & Koestner, R. (2018). Fear of missing out: Prevalence, dynamics, and consequences of experiencing FOMO. *Motivation and Emotion*, 42(5), 725–737. <https://doi.org/10.1007/s11031-018-9683-5>
- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Information and Computer Security*, 22(5), 389–408. <https://doi.org/10.1016/j.cose.2016.03.004>
- Pluchart, J.-J. (2019). Le triangle de la fraude. *Vie & sciences de l'entreprise*, 207(1), 83–97. <https://doi.org/10.3917/vse.207.0083>
- Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior*, 29(4), 1841–1848. <https://doi.org/10.1016/j.chb.2013.02.014>
- Quisenberry, W. L. (2017). Ponzi of all Ponzis: Critical analysis of the Bernie Madoff scheme. *International Journal of Econometrics and Financial Management*, 5(1), 1–6. <https://doi.org/10.12691/ijefm-5-1-1>
- Raulin, A. (2022). L'intelligence artificielle dans la gestion et la valorisation de l'information : clés de repérage (histoire et analyse). *I2D — Information, données & documents*, 59(1), 14–21. <https://doi.org/10.3917/i2d.221.0014>
- Sholademi, D. B. (2024). Leveraging AI for detecting deep fakes and combating financial fraudulent identity schemes. *International Journal of Research Publication and Reviews*, 5(12), 4096–4111. <https://doi.org/10.55248/gengpi.5.1224.250131>
- Singh Chauhan, K. D. (2025). ChatGPT for good? Taking 'beneficence' seriously in the regulation of generative artificial intelligence. *International Review of Law, Computers & Technology*, 39(2), 152–174. <https://doi.org/10.1080/13600869.2024.2364989>

- Stanovich, K. E., & West, R. F. (2000). Individual differences in reasoning: implications for the rationality debate? *The Behavioral and Brain Sciences*, 23(5), 645–726. <https://doi.org/10.1017/s0140525x00003435>
- Sun, G., Ling, Z., Li, Y., & Xie, C. (2025). Artificial intelligence and financial fraud. *Pacific-Basin Finance Journal*, 93(C), Article 102830. <https://doi.org/10.1016/j.pacfin.2025.102830>
- Talan, T., Doğan, Y., & Kalinkara, Y. (2024). Effects of smartphone addiction, social media addiction and fear of missing out on university students' phubbing: A structural equation model. *Deviant Behavior*, 45(1), 1–14. <https://doi.org/10.1080/01639625.2023.2235870>
- Tenenbaum, A. (2012). Retombées de l'affaire Madoff sur la Convention de Lugano : La localisation du dommage financier. *Revue critique de droit international privé*, 1(1), 45-60. <https://doi.org/10.3917/rcdip.121.0045>
- Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society*, 6(1). <https://doi.org/10.1177/2056305120903408>
- Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability. *Decision Support Systems*, 51(3), 576–586. <https://doi.org/10.1016/j.dss.2011.03.002>
- Wan Fakhrudin, W. F. W., Wan Adnan, W. N. A., Zaid, Y. H., & Abu Bakar, F. (2026). Linguistic strategies in investment fraud: A case study of language structuring in cryptocurrency investment website. *International Journal of Research and Innovation in Social Science (IJRISS)*, 10(1). <https://doi.org/10.47772/IJRISS.2026.10100079>
- Whittaker, L., Mulcahy, R., Russell-Bennett, R., Letheren, K., & Kietzmann, J. (2025). Examining consumer appraisals of deepfake advertising and disclosure: Show deepfakes as “real life” or say they are fake? *Journal of Advertising*. Publication en ligne avancée. <https://doi.org/10.1080/00218499.2025.2498830>
- Wolfe, D. T., & Hermanson, D. R. (2004). The Fraud Diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42.

Rapports et comptes rendus :

- Autorité des services et marchés financiers (FSMA). (2025, 3 octobre). *Fraudes à l'investissement et offres illicites - Dashboard 1er semestre 2025*. https://www.fsma.be/sites/default/files/media/files/2025-10/20251003_dashboard_fraudes_investissement_2025_q1_q2.pdf
- European Commission. (2025). *Special Eurobarometer 554: Artificial Intelligence and the future of work*. Publications Office of the European Union. <https://europa.eu/eurobarometer/surveys/detail/3222>

Europol. (2023). *ChatGPT - The impact of Large Language Models on Law Enforcement*. Office des publications de l'Union européenne. <https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement>

FINRA Investor Education Foundation, & AARP. (2022). *Blame and shame in the context of financial fraud*. <https://www.finrafoundation.org/sites/finrafoundation/files/Blame-and-Shame-in-the-Context-of-Financial-Fraud.pdf>

Ontario Securities Commission, & Behavioural Insights Team. (2024, 25 septembre). *Artificial intelligence and retail investing: Scams and effective countermeasures* (Rapport de recherche). OSC. <https://www.osc.ca/en/investors/artificial-intelligence-and-retail-investing-scams-and-effective-countermeasures>

Ouvrages (Livres):

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Petty, R. E., & Cacioppo, J. T. (1986). The Elaboration Likelihood Model of persuasion. In *Communication and persuasion: Central and peripheral routes to attitude change* (pp. 1-24). Springer. https://doi.org/10.1007/978-1-4612-4964-1_1

Quivy, R., & Van Campenhoudt, L. (2011). *Manuel de recherche en sciences sociales* (4e éd.). Dunod.

Consultation de pages web et articles de presse :

Centre pour la Cybersécurité Belgique. (2025, 3 octobre). *Safeonweb launches national prevention campaign against investment fraud today: €15 million already stolen*. CCB Safeonweb. <http://ccb.belgium.be/news/safeonweb-launches-national-prevention-campaign-against-investment-fraud-today-eu15-million>

Commission des valeurs mobilières de l'Ontario. (2024, 22 mai). *Une étude de la CVMO révèle que les escroqueries renforcées par l'IA représentent un risque important pour les investisseurs*. <https://www.osc.ca/fr/nouvelles-evenements/nouvelles/une-etude-de-la-cvmo-revele-que-les-escroqueries-renforcees-par-lia-representent-un-risque-important>

Commission des valeurs mobilières de l'Ontario (CVMO). (2025, 29 mai). *Escroqueries liées à l'IA : risques et mesures de protection*. GetSmarterAboutMoney.ca. <https://www.gerezmieuxvotreargent.ca/chemin-dapprentissage/recherches-et-rapports/escroqueries-liees-a-lia-risques-et-mesures-de-protection/>

Distinguin, S. (2025, 25 juillet). *Baromètre européen de l'intelligence artificielle 2025*. EY. https://www.ey.com/fr_fr/insights/tmt/barometre-europeen-de-l-intelligence-artificielle-2025

Éditions Larousse. (s. d.-a). *Fraude*. Dans *Dictionnaire de français Larousse*. Consulté le 26 janvier 2026 sur <https://www.larousse.fr/dictionnaires/francais/fraude/35120>

- Éditions Larousse. (s. d.-b). Intelligence artificielle. Dans *Encyclopédie Larousse en ligne*. Consulté le 26 janvier 2026 sur https://www.larousse.fr/encyclopedia/divers/intelligence_artificielle/187257
- ESET. (2025). *Ingénierie sociale (dans le domaine de la cybersécurité)*. Consulté le 26 janvier 2026 sur <https://www.eset.com/be-fr/social-engineering-business/>
- Hu, C. (2023, 5 février). *What is AI? An artificial intelligence definition*. Popular Science. <https://www.popsci.com/technology/artificial-intelligence-definition/>
- Ipsos. (2019). *Perception de l'intelligence artificielle (IA) par les Belges*. SPF Économie. <https://economie.fgov.be/fr/publications/perception-de-lintelligence>
- Organisation de coopération et de développement économiques. (2025). *Intelligence artificielle*. Consulté le 26 janvier 2026 sur <https://www.oecd.org/fr/themes/intelligence-artificielle.html>
- Oxford English Dictionary. (2023). Artificial intelligence, n. Dans *OED*. Consulté le 26 janvier 2026 sur https://www.oed.com/dictionary/artificial-intelligence_n
- Parlement européen et Conseil de l'Union européenne. (2024, 13 juin). Règlement (UE) 2024/1689 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 715/2007, (CE) n° 400/2008, (CE) n° 1217/2009, (UE) n° 679/2016 et (UE) 2018/1725 et la directive 2002/58/CE (règlement sur l'intelligence artificielle). *Journal officiel de l'Union européenne*, L, 2024/1689. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- Statbel. (s. d.). *Population*. SPF Économie, P.M.E., Classes moyennes et Énergie. Consulté le 10 mai 2026, à l'adresse <https://statbel.fgov.be/fr/themes/population>
- TRM Labs. (2024, 25 avril). *Fraude par l'IA : Comment les escrocs exploitent l'IA générative*. TRM Blog. <https://www.trmlabs.com/post/ai-fraud-how-scammers-are-exploiting-generative-ai>

Annexes

Annexe 1

Vous êtes ...	Données brutes	Données relatives	Population Belge réelle (Statbel)	Variation
Un homme	71	46%	49%	-3%
Une femme	82	54%	51%	3%
Total général	153	100%	100%	

Hommes et femmes	Hommes et femmes	Hommes et femmes
Sexe	Femmes	Hommes
Population au 01 janvier 2025	5.995.529	5.830.022
		11.825.551

Source: Statbel (Direction générale Statistique - Statistics Belgium)

Annexe 2

Age en 2026 (basé sur l'année de naissance)	Données brutes	Données relatives	Population Belge réelle (sans les moins de 15 ans)	Variation
15-24 ans	28	18,30%	14,01%	4,29%
25-34 ans	28	18,30%	15,22%	3,09%
35-44 ans	29	18,95%	15,58%	3,38%
45-54 ans	23	15,03%	15,32%	-0,29%
55-64 ans	20	13,07%	15,63%	-2,56%
65 ans et plus	25	16,34%	24,24%	-7,91%
Total général	153	100,00%	100,00%	

Calcul du pourcentage sans les moins de 15 ans			
Age population belge (statbel)	Données brutes (Statbel)	Données relatives	Regroupement sans les moins de 15 ans
Moins de 5 ans	577823	4,89%	
5-9 ans	633654	5,36%	15-24 ans 1390357
10-14 ans	687908	5,82%	25-34 ans 1509515
15-19 ans	699349	5,91%	35-44 ans 1545589
20-24 ans	691008	5,84%	45-54 ans 1519732
25-29 ans	730126	6,17%	55-64 ans 1550411
30-34 ans	779389	6,59%	65 ans et plus 2405315
35-39 ans	773866	6,54%	
40-44 ans	771723	6,53%	Total 9920919
45-49 ans	749945	6,34%	
50-54 ans	769787	6,51%	
55-59 ans	780624	6,60%	
60-64 ans	775034	6,55%	
65-69 ans	683784	5,78%	
70-74 ans	574709	4,86%	
75-79 ans	483443	4,09%	
80-84 ans	306697	2,59%	
85-89 ans	220483	1,86%	
90-94 ans	106770	0,90%	
95-99 ans	26257	0,22%	
100 et plus	3172	0,03%	
Total	11825551	100,00%	

Tous les âges	Classe d'âges	Population au 01 janvier 2025
	Moins de 5 ans	577.823
	De 5 à 9 ans	633.654
	De 10 à 14 ans	687.908
	De 15 à 19 ans	699.349
	De 20 à 24 ans	691.008
	De 25 à 29 ans	730.126
	De 30 à 34 ans	779.389
	De 35 à 39 ans	773.866
	De 40 à 44 ans	771.723
	De 45 à 49 ans	749.945
	De 50 à 54 ans	769.787
	De 55 à 59 ans	780.624
	De 60 à 64 ans	775.034
	De 65 à 69 ans	683.784
	De 70 à 74 ans	574.709
	De 75 à 79 ans	483.443
	De 80 à 84 ans	306.697
	De 85 à 89 ans	220.483
	De 90 à 94 ans	106.770
	De 95 à 99 ans	26.257
	100 ans et plus	3.172
Tous les âges		11.825.551

Source: Statbel (Direction générale Statistique - Statistics Belgium)

Annexe 3

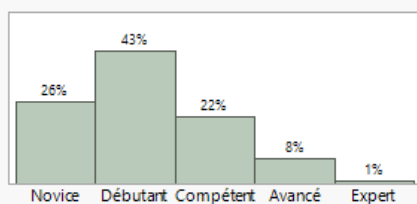
Quel est le diplôme le plus élevé que vous ayez obtenu ?	Données brutes	Données relatives	Population Belge réelle (Statbel)	Variation
Aucun diplôme ou enseignement primaire (CEB)	9	5,88%	8,50%	-2,62%
Enseignement secondaire (inférieur ou supérieur)	70	45,75%	54%	-8,25%
Enseignement supérieur de type court	38	24,84%	18,90%	5,94%
Enseignement supérieur de type long (Bachelier / Master / Doctorat)	36	23,53%	18,60%	4,93%
Total général	153	100,00%	100,00%	

Niveau d'instruction de la population de 15 ans et plus^(f) - en pourcentage (1987-2025)

Diplôme obtenu	2022	2023	2024	2025
Total	100,0%	100,0%	100,0%	100,0%
Primaire ou sans diplôme	9,6%	10,0%	9,8%	8,5%
Secondaire inférieur	17,5%	17,5%	17,5%	16,7%
Secondaire supérieur	36,3%	36,9%	37,2%	37,3%
Niveau non universitaire type court / formation professionnalisante ou de transition (à orientation professionnelle)	18,8%	18,5%	18,5%	18,9%
Niveau non universitaire type long / Niveau universitaire / Bachelier académique ou Master	17,8%	17,1%	17,1%	18,6%

Auto-évaluation des connaissances financières

Q5. Comment évaluez-vous votre niveau de connaissances en produits financiers?



Fréquences

Niveau	Dénombrement	Prob.
Novice	40	0,26316
Débutant	66	0,43421
Compétent	33	0,21711
Avancé	12	0,07895
Expert	1	0,00658
Total	152	1,00000

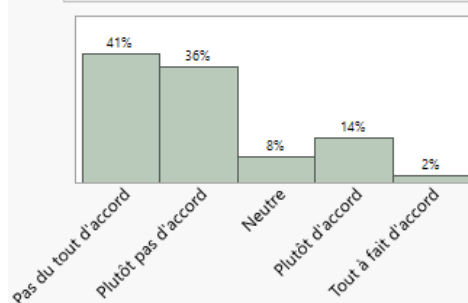
Donnée(s) manquante(s) 1
5 Niveau(x)

Annexe 4

Annexe 5

Intérêt pour les opportunités d'investissement en ligne

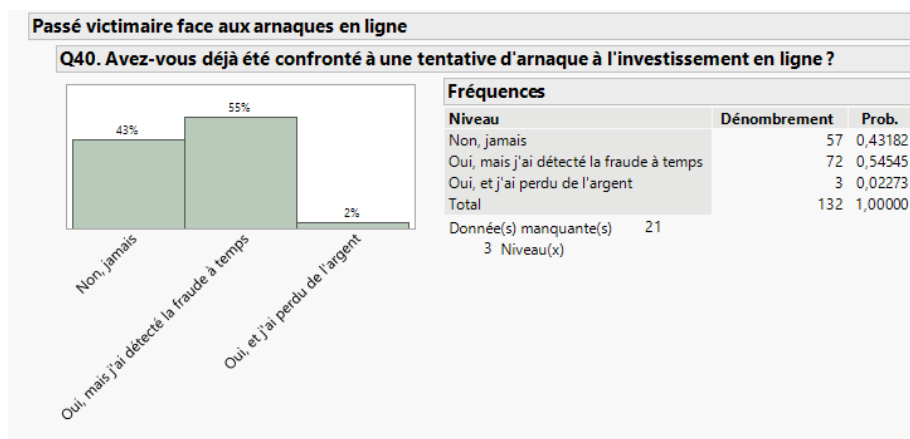
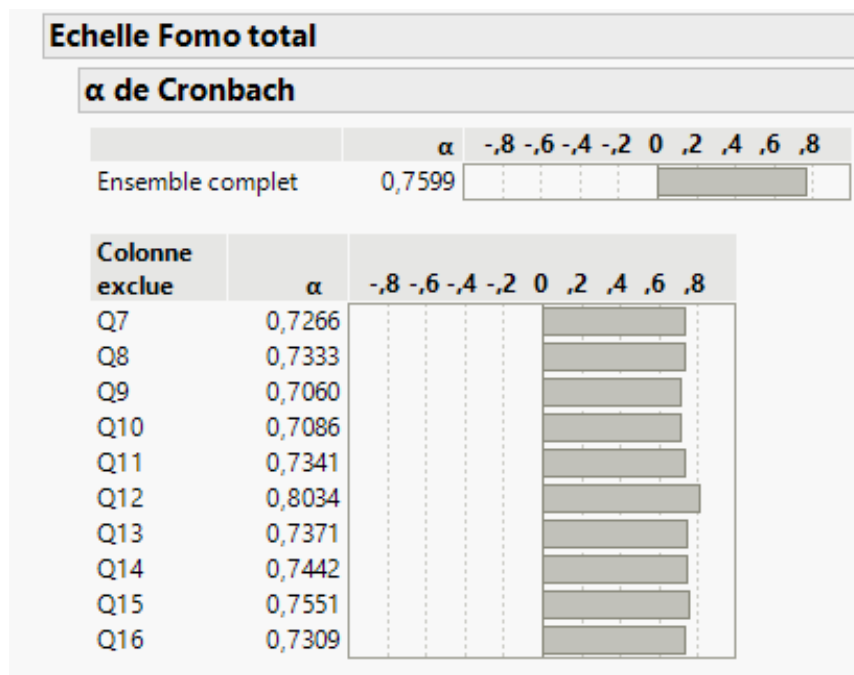
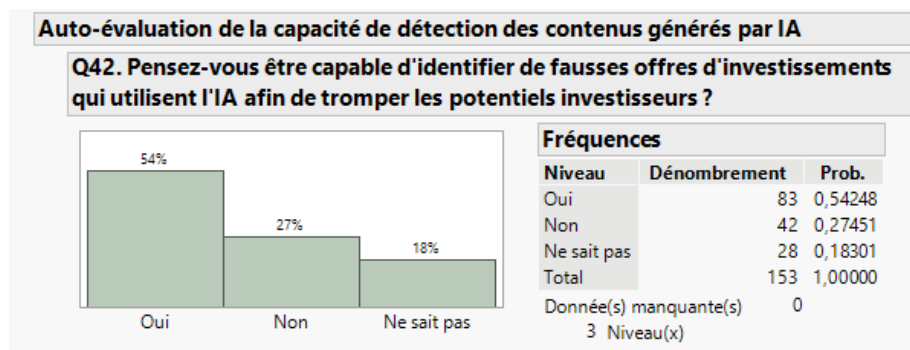
Q6. « De manière générale, je suis intrigué(e) ou intéressé(e) par les opportunités d'investissement que je vois passer sur Internet. »

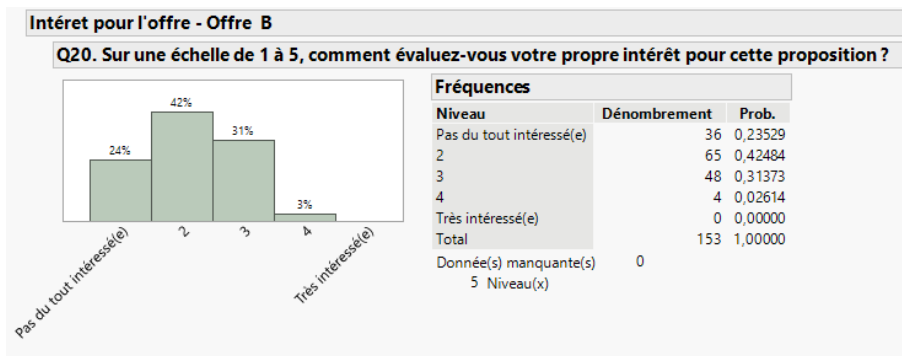
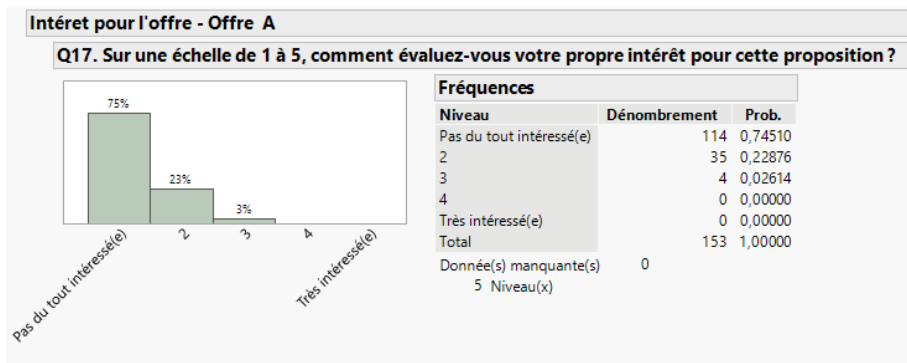
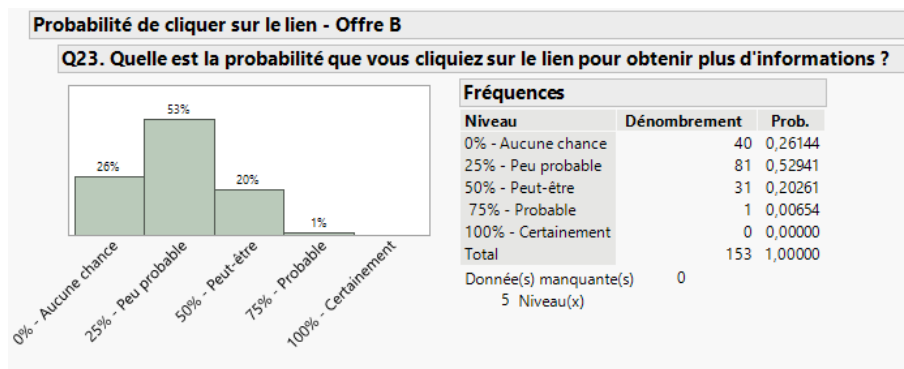
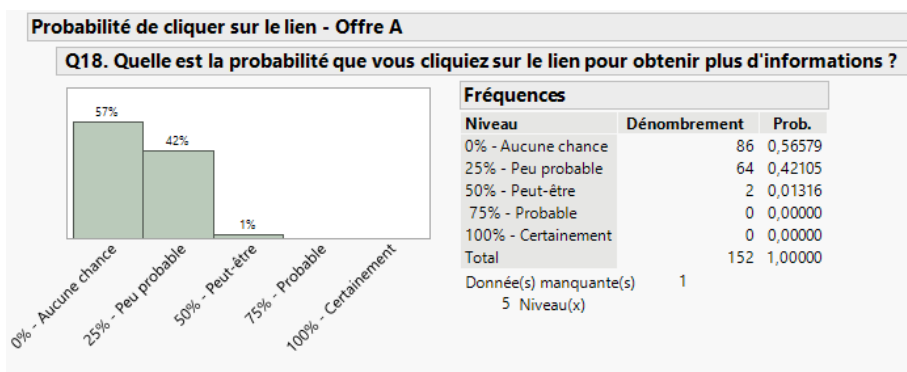


Fréquences

Niveau	Dénombrement	Prob.
Pas du tout d'accord	62	0,40523
Plutôt pas d'accord	55	0,35948
Neutre	12	0,07843
Plutôt d'accord	21	0,13725
Tout à fait d'accord	3	0,01961
Total	153	1,00000

Donnée(s) manquante(s) 0
5 Niveau(x)

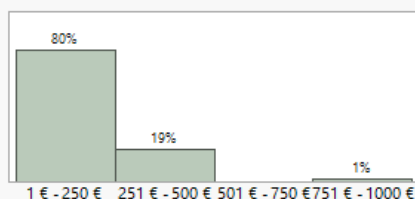
Annexe 6Annexe 7Annexe 8

Annexe 9Annexe 10Annexe 11Annexe 12

Annexe 13

Investissement de 1000€ - Offre A

Q19. En imaginant que vous soyez intéressé par l'offre, si vous aviez 1000 € à investir aujourd'hui, quelle somme seriez-vous prêt(e) à placer dans cette offre ?



Fréquences

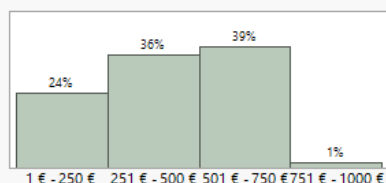
Niveau	Dénombrement	Prob.
1 € - 250 €	122	0,80263
251 € - 500 €	29	0,19079
501 € - 750 €	0	0,00000
751 € - 1000 €	1	0,00658
Total	152	1,00000

Donnée(s) manquante(s) 1

4 Niveau(x)

Investissement de 1000€ - Offre B

Q24. Scénario fictif : En imaginant que vous soyez intéressé par l'offre, si vous aviez 1000 € à investir aujourd'hui, quelle somme seriez-vous prêt(e) à placer dans cette offre ?



Fréquences

Niveau	Dénombrement	Prob.
1 € - 250 €	36	0,23684
251 € - 500 €	55	0,36184
501 € - 750 €	59	0,38816
751 € - 1000 €	2	0,01316
Total	152	1,00000

Donnée(s) manquante(s) 1

4 Niveau(x)

Annexe 14

Impact de l'influence perçue du jargon financier (Q21) sur la probabilité de clic (Q23) et le montant de l'investissement consenti (Q24)

Corrélations

	Q21	Q23	Q24
Q21	1,0000	0,3457	0,4470
Q23	0,3457	1,0000	0,5034
Q24	0,4470	0,5034	1,0000

Il y a 2 valeurs manquantes. Les corrélations sont estimées par la méthode REML.

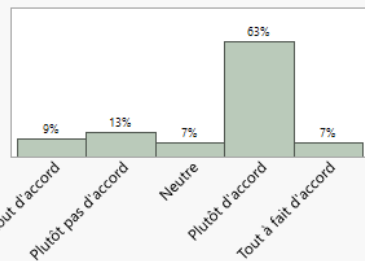
Non paramétrique : p de Spearman

Variable	par variable	p de Spearman	Prob.> p	
Q23	Q21	0,3427	<,0001*	
Q24	Q21	0,4201	<,0001*	
Q24	Q23	0,4971	<,0001*	

Annexe 15

Influence des termes techniques

Q21. Dans quelle mesure êtes-vous d'accord avec l'affirmation suivante : «L'usage de termes techniques (ex : ratio de Sharpe, arbitrage) renforce mon intérêt vis-à-vis de l'offre.» ?



Fréquences

Niveau	Dénombrement	Prob.
Pas du tout d'accord	14	0,09211
Plutôt pas d'accord	20	0,13158
Neutre	11	0,07237
Plutôt d'accord	96	0,63158
Tout à fait d'accord	11	0,07237
Total	152	1,00000

Donnée(s) manquante(s) 1

5 Niveau(x)

Annexe 16

Répartition des stratégies de traitement cognitif de l'information chez les répondants face à une offre à jargon technique (Q22)

Q22. Lors de votre lecture, comment avez-vous traité les informations techniques ?

La fluidité et le sérieux du ton m'ont permis de comprendre l'opportunité sans effort.

45%

Je me suis fié à l'impression globale de professionnalisme.

36%

J'ai analysé précisément chaque terme avant de juger.

19%

Test de probabilités

Niveau	Prob. estimée.	Prob. de référence
J'ai analysé précisément chaque terme avant de juger.	0,18954	0,333333333
Je me suis fié à l'impression globale de professionnalisme.	0,35948	0,333333333
La fluidité et le sérieux du ton m'ont permis de comprendre l'opportunité sans effort.	0,45098	0,333333333

Test	Khi deux	Degrés de liberté	Prob. > khi deux
Rapport de vraisemblance	17,2779	2	0,0002*
Pearson	16,1569	2	0,0003*

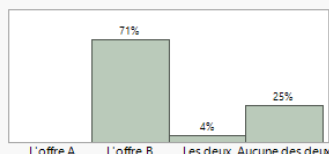
Méthode : Fixer les valeurs de référence et réajuster l'échelle des omissions.

Remarque : La somme des probabilités de référence n'est pas égale à 1. Les probabilités ont été réajustées à l'échelle.

Annexe 17

Crédibilité institutionnelle perçue

Q25. Entre les deux offres présentées, laquelle vous semble provenir d'une institution financière régulée ?



Fréquences

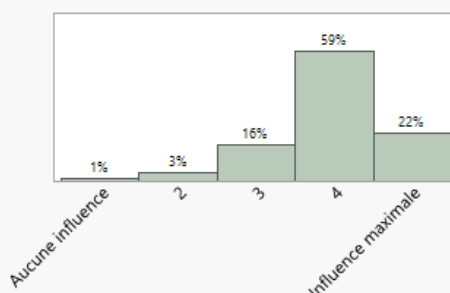
Niveau	Dénombrement	Prob.
L'offre A ("Salut ! Vu que...")	0	0,00000
L'offre B ("Suite aux fluctuations...")	104	0,71233
Les deux	6	0,04110
Aucune des deux	36	0,24658
Total	146	1,00000

Donnée(s) manquante(s) 7
4 Niveau(x)

Annexe 18

Influence linguistique générale

Q26. À quel point l'absence de fautes d'orthographe et la précision du langage influencent-elles votre intérêt envers une publicité en ligne ?

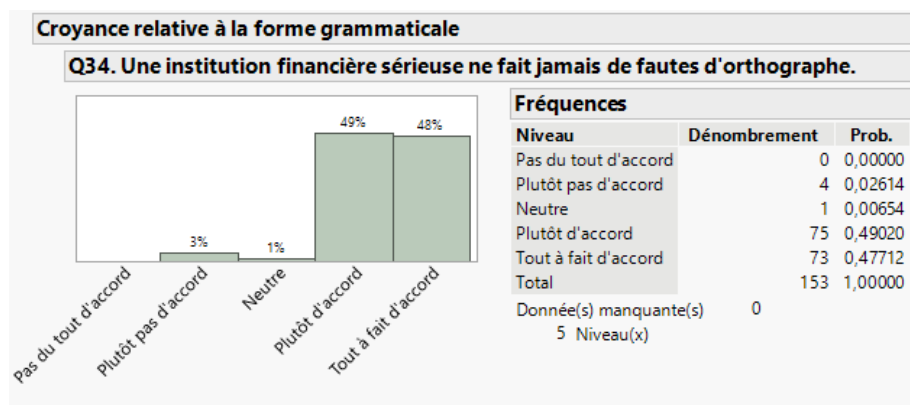
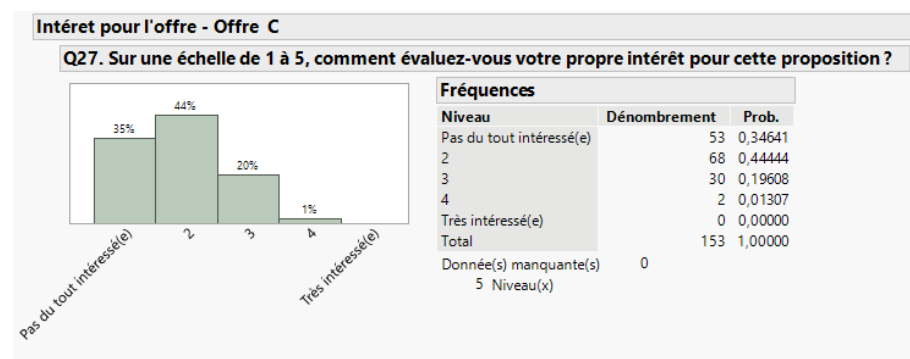
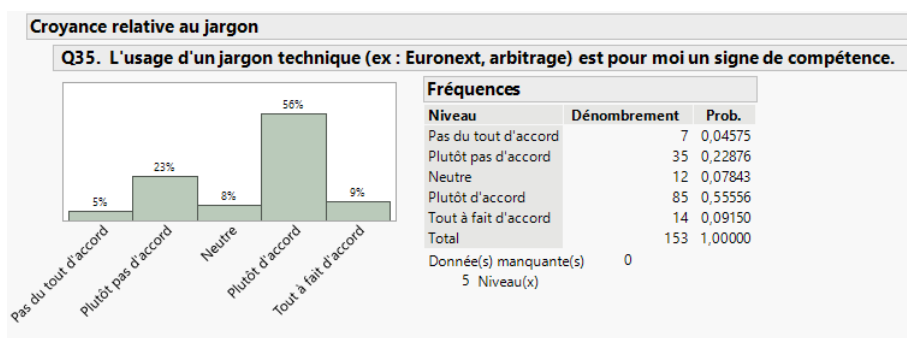


Fréquences

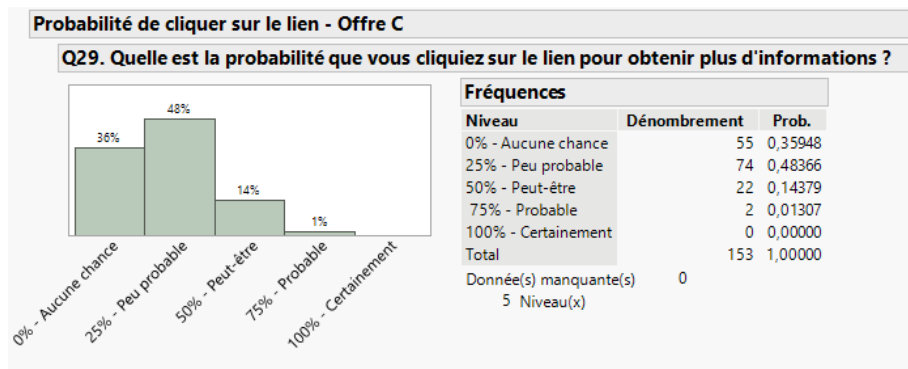
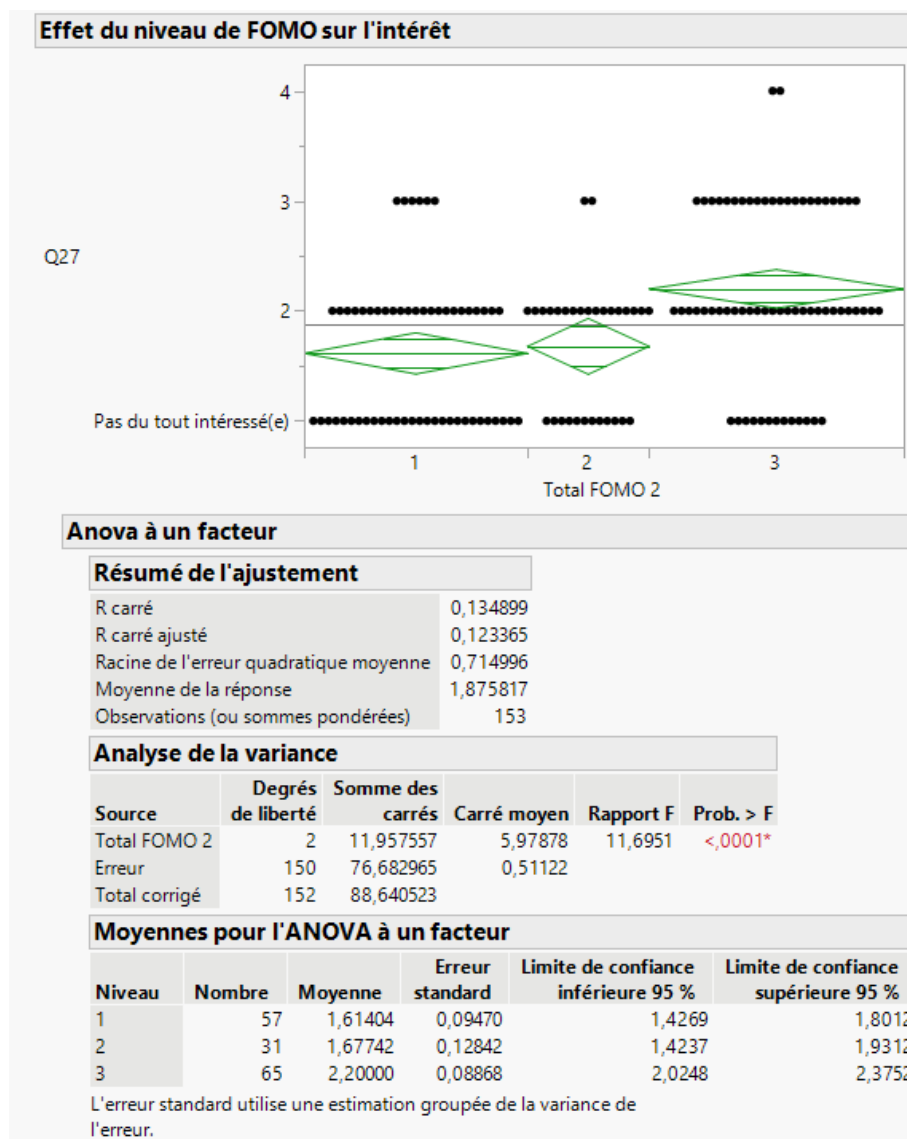
Niveau	Dénombrement	Prob.
Aucune influence	1	0,00654
2	5	0,03268
3	24	0,15686
4	90	0,58824
Influence maximale	33	0,21569
Total	153	1,00000

Donnée(s) manquante(s) 0
5 Niveau(x)

Annexe 19

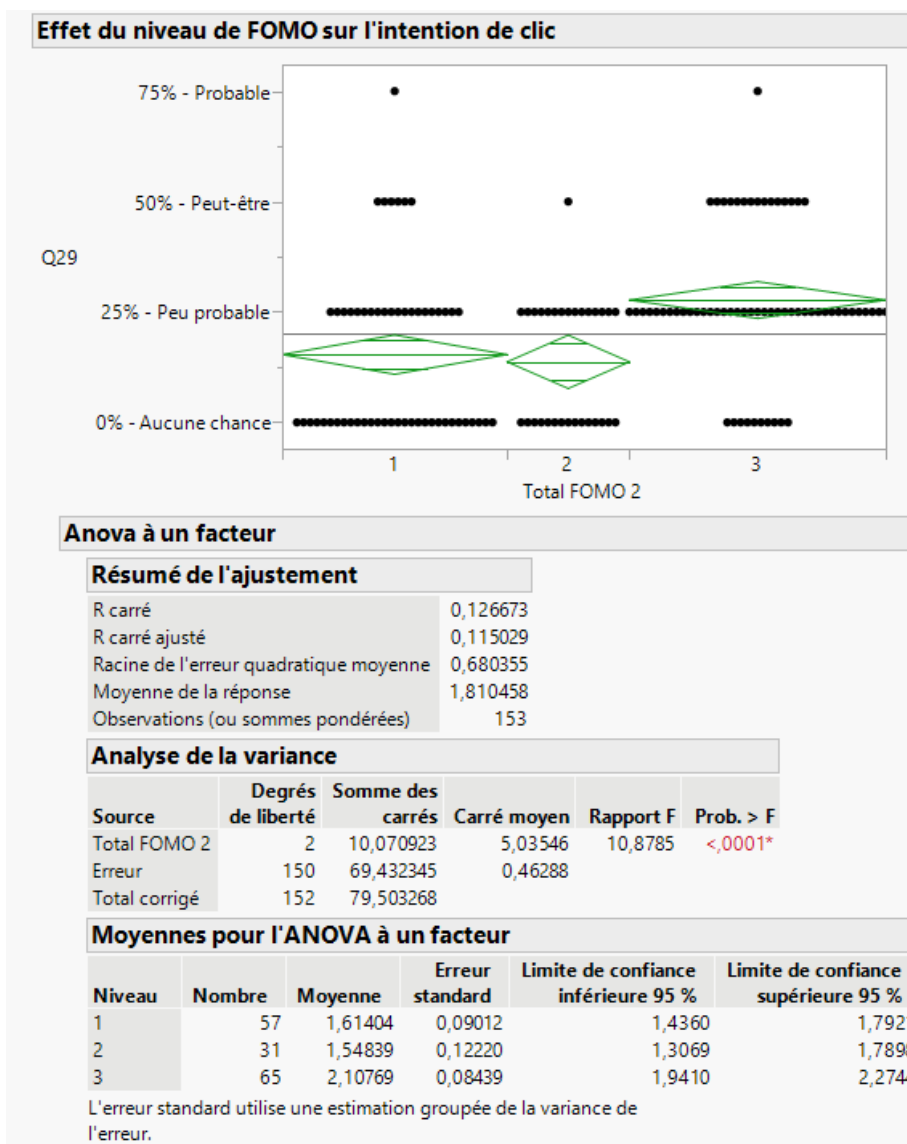
Annexe 20Annexe 21Annexe 22

Annexe 23



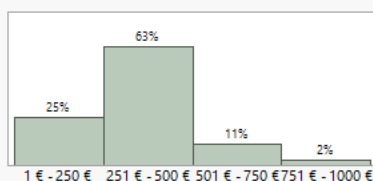
Annexe 24

Annexe 25



Investissement de 1000€ - Offre C

Q30. Scénario fictif : En imaginant que vous soyez intéressé par l'offre, si vous aviez 1000 € à investir aujourd'hui, quelle somme seriez-vous prêt(e) à placer dans cette offre ?



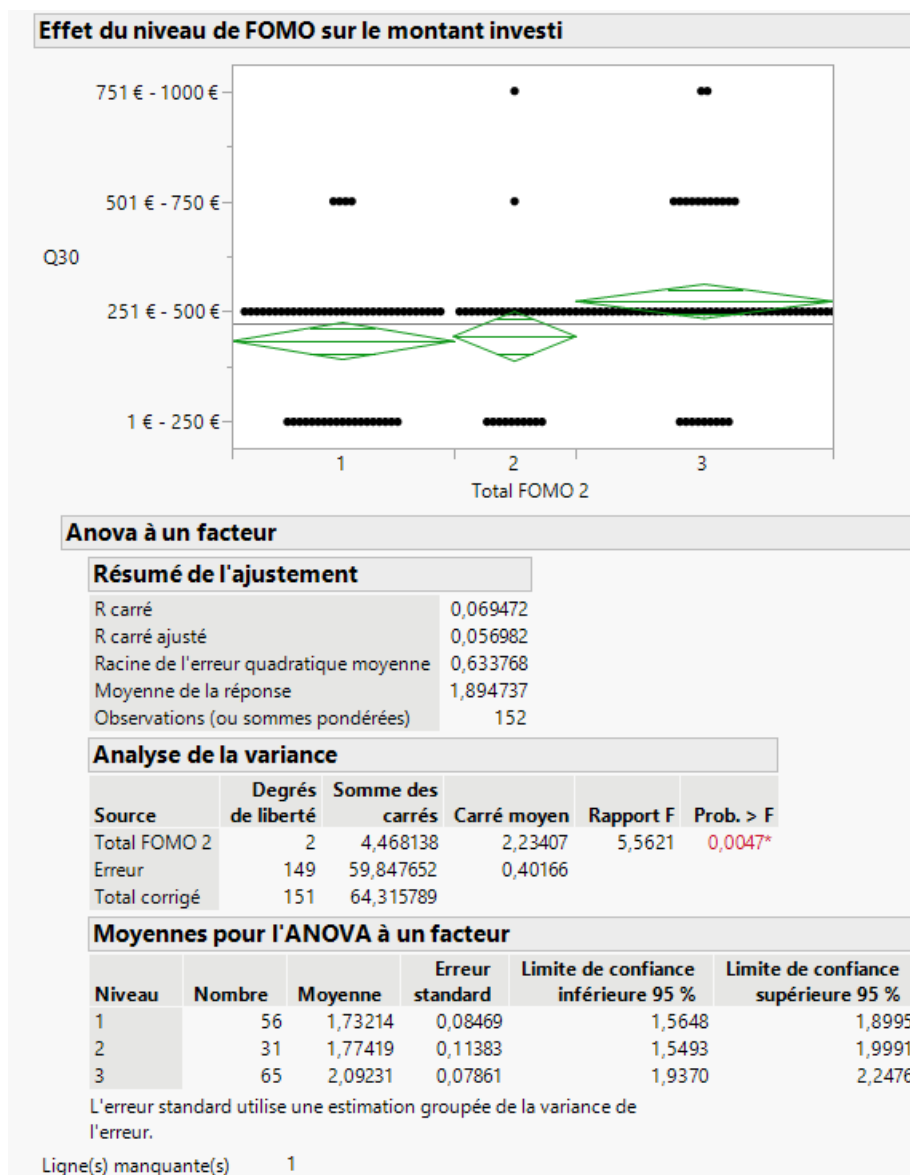
Fréquences

Niveau	Dénombrement	Prob.
1 € - 250 €	38	0,25000
251 € - 500 €	95	0,62500
501 € - 750 €	16	0,10526
751 € - 1000 €	3	0,01974
Total	152	1,00000

Donnée(s) manquante(s)
4 Niveau(x)

Annexe 26

Annexe 27



Dynamique d'influence du trait de FOMO**Corrélations**

	Total FOMO	Q17	Q18	Q19	Q27	Q29	Q30
Total FOMO	1,0000	0,0996	0,2593	0,0391	0,3836	0,3244	0,3018
Q17	0,0996	1,0000	0,5553	0,0846	0,2952	0,3443	0,0765
Q18	0,2593	0,5553	1,0000	0,0981	0,3750	0,5259	0,1913
Q19	0,0391	0,0846	0,0981	1,0000	0,0378	0,1020	0,3436
Q27	0,3836	0,2952	0,3750	0,0378	1,0000	0,7314	0,5763
Q29	0,3244	0,3443	0,5259	0,1020	0,7314	1,0000	0,5098
Q30	0,3018	0,0765	0,1913	0,3436	0,5763	0,5098	1,0000

Il y a 3 valeurs manquantes. Les corrélations sont estimées par la méthode REML.

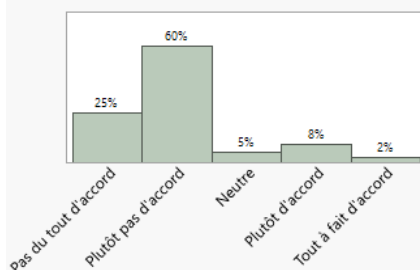
Non paramétrique : ρ de Spearman

Variable	par variable	ρ de Spearman	Prob.> ρ	
Q17	Total FOMO	0,1442	0,0753	
Q18	Total FOMO	0,2814	0,0004*	
Q18	Q17	0,5244	<,0001*	
Q19	Total FOMO	0,0479	0,5575	
Q19	Q17	0,0936	0,2514	
Q19	Q18	0,1326	0,1046	
Q27	Total FOMO	0,3747	<,0001*	
Q27	Q17	0,3005	0,0002*	
Q27	Q18	0,3947	<,0001*	
Q27	Q19	0,0727	0,3736	
Q29	Total FOMO	0,3541	<,0001*	
Q29	Q17	0,3230	<,0001*	
Q29	Q18	0,5292	<,0001*	
Q29	Q19	0,1302	0,1099	
Q29	Q27	0,7556	<,0001*	
Q30	Total FOMO	0,2953	0,0002*	
Q30	Q17	0,0981	0,2291	
Q30	Q18	0,2611	0,0012*	
Q30	Q19	0,2799	0,0005*	
Q30	Q27	0,5944	<,0001*	
Q30	Q29	0,5467	<,0001*	

Annexe 28

Tension ressentie à la lecture

Q28. Dans quelle mesure êtes-vous d'accord avec l'affirmation suivante : « Face à l'indication "Plus que 15 minutes", j'ai ressenti une tension me poussant à agir rapidement. »

**Fréquences**

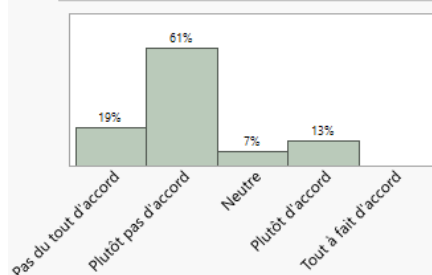
Niveau	Dénombrement	Prob.
Pas du tout d'accord	38	0,24837
Plutôt pas d'accord	92	0,60131
Neutre	7	0,04575
Plutôt d'accord	13	0,08497
Tout à fait d'accord	3	0,01961
Total	153	1,00000

Donnée(s) manquante(s) 0
5 Niveau(x)

Annexe 29

Croyances théoriques liées à l'exclusivité

Q36. Le sentiment de pouvoir rater une offre exclusive me pousse à décider plus rapidement



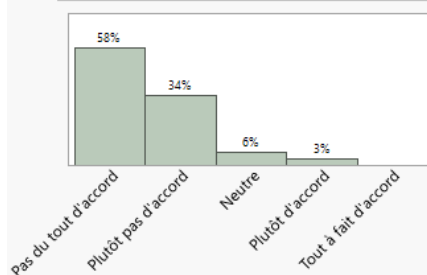
Fréquences

Niveau	Dénombrement	Prob.
Pas du tout d'accord	29	0,19079
Plutôt pas d'accord	93	0,61184
Neutre	11	0,07237
Plutôt d'accord	19	0,12500
Tout à fait d'accord	0	0,00000
Total	152	1,00000
Donnée(s) manquante(s)	1	
5 Niveau(x)		

Annexe 30

Croyances théoriques liées au compte à rebours

Q37. Un compte à rebours m'incite à prendre une décision sans vérification supplémentaire



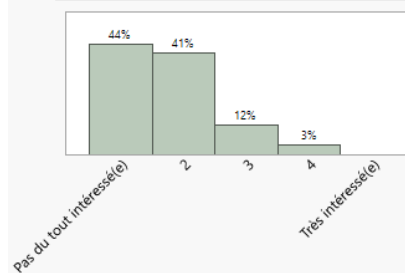
Fréquences

Niveau	Dénombrement	Prob.
Pas du tout d'accord	88	0,57516
Plutôt pas d'accord	52	0,33987
Neutre	9	0,05882
Plutôt d'accord	4	0,02614
Tout à fait d'accord	0	0,00000
Total	153	1,00000
Donnée(s) manquante(s)	0	
5 Niveau(x)		

Annexe 31

Intérêt pour l'offre - Offre D

Q31. Sur une échelle de 1 à 5, comment évaluez-vous votre propre intérêt pour cette proposition ?



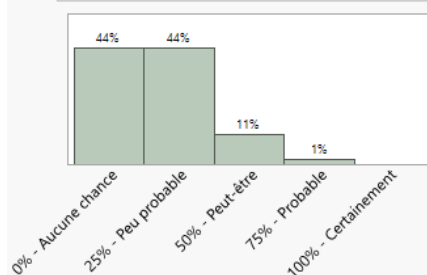
Fréquences

Niveau	Dénombrement	Prob.
Pas du tout intéressé(e)	68	0,44444
2	62	0,40523
3	18	0,11765
4	5	0,03268
Très intéressé(e)	0	0,00000
Total	153	1,00000
Donnée(s) manquante(s)	0	
5 Niveau(x)		

Annexe 32

Probabilité de cliquer sur le lien - Offre D

Q32. Quelle est la probabilité que vous cliquiez sur le lien pour obtenir plus d'informations ?



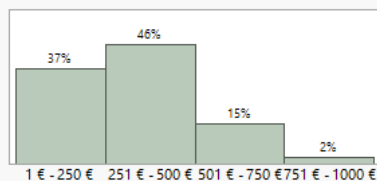
Fréquences

Niveau	Dénombrement	Prob.
0% - Aucune chance	67	0,43791
25% - Peu probable	67	0,43791
50% - Peut-être	17	0,11111
75% - Probable	2	0,01307
100% - Certainement	0	0,00000
Total	153	1,00000
Donnée(s) manquante(s)	0	
5 Niveau(x)		

Annexe 33

Investissement de 1000€ - Offre D

Q33. Scénario fictif : En imaginant que vous soyez intéressé par l'offre, si vous aviez 1000 € à investir aujourd'hui, quelle somme seriez-vous prêt(e) à placer dans cette offre ?

**Fréquences**

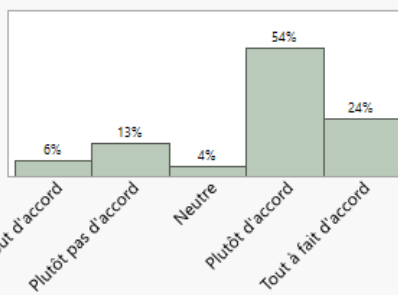
Niveau	Dénombrement	Prob.
1 € - 250 €	56	0,36601
251 € - 500 €	71	0,46405
501 € - 750 €	23	0,15033
751 € - 1000 €	3	0,01961
Total	153	1,00000

Donnée(s) manquante(s) 0

4 Niveau(x)

Annexe 34**Le poids de la preuve sociale**

Q38. Voir que d'autres personnes ont déjà investi (des amis par exemple) me rassure sur la légitimité d'un projet

**Fréquences**

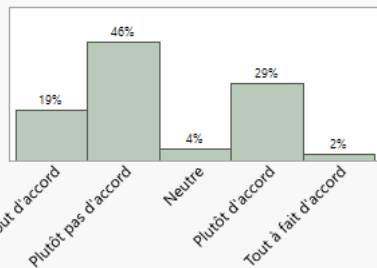
Niveau	Dénombrement	Prob.
Pas du tout d'accord	9	0,05882
Plutôt pas d'accord	20	0,13072
Neutre	6	0,03922
Plutôt d'accord	82	0,53595
Tout à fait d'accord	36	0,23529
Total	153	1,00000

Donnée(s) manquante(s) 0

5 Niveau(x)

Annexe 35**L'impact de la notoriété publique en ligne**

Q39. L'apparition d'une personnalité publique en vidéo renforce la crédibilité d'un projet

**Fréquences**

Niveau	Dénombrement	Prob.
Pas du tout d'accord	29	0,18954
Plutôt pas d'accord	70	0,45752
Neutre	6	0,03922
Plutôt d'accord	45	0,29412
Tout à fait d'accord	3	0,01961
Total	153	1,00000

Donnée(s) manquante(s) 0

5 Niveau(x)

Annexe 36

Annexe 37**Enquête sur les habitudes d'investissement financier à l'ère numérique****Introduction**

Madame, Monsieur,

Dans le cadre de mon travail de fin d'études en Criminologie à l'Université de Liège, je mène une recherche académique visant à analyser les habitudes d'investissement financier de la population belge.

Votre participation à cette recherche est entièrement volontaire : vous êtes libre de ne pas y prendre part ou d'interrompre votre réponse à tout moment en fermant simplement la fenêtre de votre navigateur, et ce, sans aucun préjudice. Le temps nécessaire pour compléter ce questionnaire est estimé à environ quinze minutes.

Conformément au Règlement Général sur la Protection des Données (RGPD), vos réponses sont strictement anonymes et seront traitées de manière confidentielle sous le sceau du secret professionnel. Les renseignements recueillis seront utilisés exclusivement à des fins de recherche statistique et de manière agrégée. Une fois l'étude finalisée, les données seront codées et stockées ; dès cet instant, leur caractère anonyme rendra impossible tout retrait individuel de la base de données.

Cette étude est réalisée par Quentin Cols (Qcols@student.uliege.be).

En cliquant sur le bouton ci-dessous, j'affirme avoir pris connaissance des modalités de traitement de mes données à caractère personnel et marque mon accord sur ceux-ci.

Je vous remercie chaleureusement pour votre précieuse collaboration.

Avez-vous lu et accepté les conditions ci-dessus pour participer à cette étude ?

- ☐ Oui, je participe
- ☐ Non, je ne souhaite pas participer

Section 1: Profilage

Q1. Résidez-vous actuellement en Belgique ?

Lieu de résidence principal

- ☐ Oui
- ☐ Non

Q2. Vous êtes ...?

- ☐ Un homme
- ☐ Une femme
- ☐ Autre
- *Si autre, veuillez préciser :* _____

Q3. Quelle est votre année de naissance ?

Pour répondre à ce questionnaire, vous devez être âgé de 15 ans au minimum

- [_____]

Q4. Quel est le diplôme le plus élevé que vous ayez obtenu ?

- [] Aucun diplôme ou enseignement primaire (CEB)
- [] Enseignement secondaire (inférieur ou supérieur)
- [] Enseignement supérieur de type court
- [] Enseignement supérieur de type long (Bachelier / Master / Doctorat)
- [] Autre
- *Si autre, veuillez préciser :* _____

Section 2: Habitudes financières

Q5. Comment évaluez-vous votre niveau de connaissances en produits financiers (actions, cryptomonnaies, épargne, ...) ?

- [] Novice : Je n'y connais presque rien
- [] Débutant : Je connais les concepts de base (ex : ce qu'est une action)
- [] Compétent : J'ai une bonne compréhension globale des mécanismes
- [] Avancé : Je sais analyser des produits et adapter ma stratégie
- [] Expert : J'ai une maîtrise technique approfondie
- [] Ne sait pas / Ne souhaite pas répondre

Q6. Dans quelle mesure êtes-vous d'accord avec l'affirmation suivante : « De manière générale, je suis intrigué(e) ou intéressé(e) par les opportunités d'investissement que je vois passer sur Internet. » ?

- [] Pas du tout d'accord
- [] Plutôt pas d'accord
- [] Neutre
- [] Plutôt d'accord
- [] Tout à fait d'accord

Section 3

Vous trouverez ci-dessous une série d'affirmations concernant vos expériences quotidiennes. En utilisant l'échelle fournie, veuillez indiquer à quel point chaque affirmation reflète vos expériences générales. Veuillez répondre en fonction de ce qui correspond réellement à votre vécu, plutôt que de ce que vous pensez que vos expériences devraient être. Veuillez traiter chaque point indépendamment des autres.

Affirmations	Pas du tout d'accord	Plutôt pas d'accord	Neutre	Plutôt d'accord	Tout à fait d'accord
Q7. Je crains que les autres aient des expériences plus gratifiantes que les miennes.	[]	[]	[]	[]	[]
Q8. Je crains que mes amis aient des expériences plus gratifiantes que les miennes.	[]	[]	[]	[]	[]
Q9. Cela me préoccupe de savoir que mes amis s'amusent sans moi.	[]	[]	[]	[]	[]
Q10. Cela m'angoisse de ne pas savoir ce que mes amis sont en train de faire.	[]	[]	[]	[]	[]
Q11. Il est important pour moi de comprendre les allusions et blagues que mes amis partagent.	[]	[]	[]	[]	[]
Q12. Parfois, je me demande si je passe trop de temps à suivre ce qu'il se passe autour de moi.	[]	[]	[]	[]	[]
Q13. Cela m'ennuie de rater une occasion de fréquenter mes amis.	[]	[]	[]	[]	[]

Affirmations	Pas du tout d'accord	Plutôt pas d'accord	Neutre	Plutôt d'accord	Tout à fait d'accord
Q14. Lorsque je passe un bon moment, il est important pour moi de le partager en ligne (ex: Facebook, Instagram).	☐	☐	☐	☐	☐
Q15. Cela m'ennuie de rater un événement planifié avec d'autres personnes.	☐	☐	☐	☐	☐
Q16. Lorsque je pars en vacances, je garde un œil sur ce que mes amis sont en train de faire.	☐	☐	☐	☐	☐

Section 4: Offre A

Considérez l'offre suivante reçue par message ou via une publicité:

« Salut ! Vu que le marché bouge beaucoup en ce moment, on a un super plan pour vous. Nos robots ont trouvés une faille pour gagné de l'argent facile. C'est une oportunity de dingue avec un rendement garantie et très élevé. »

Q17. Sur une échelle de 1 à 5, comment évaluez-vous votre propre intérêt pour cette proposition ?

- ☐ 1 - Pas du tout intéressé(e)
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5 - Très intéressé(e)

Q18. Quelle est la probabilité que vous cliquiez sur le lien pour obtenir plus d'informations ?

- ☐ 0% Aucune chance
- ☐ 25% Peu probable
- ☐ 50% Peut-être

- ☐ 75% Probable
- ☐ 100% Certainement

Q19. Scénario fictif : En imaginant que vous soyez intéressé par l'offre, si vous aviez 1000 € à investir aujourd'hui, quelle somme seriez-vous prêt(e) à placer dans cette offre ?

- ☐ 1 € - 250 €
- ☐ 251 € - 500 €
- ☐ 501 € - 750 €
- ☐ 751 € - 1000 €

Section 5: Offre B

Considérez maintenant cette seconde offre:

« Suite aux récentes fluctuations de la volatilité sur les marchés financiers, nos modèles prédictifs ont identifié une opportunité d'arbitrage structurelle. Ce protocole vise à capturer les inefficiences de prix temporaires pour générer un rendement décorrélié des indices traditionnels. Le ratio de Sharpe est estimé à 2.5. »

Q20. Sur une échelle de 1 à 5, comment évaluez-vous votre propre intérêt pour cette proposition ?

- ☐ 1 - Pas du tout intéressé(e)
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5 - Très intéressé(e)

Q21. Dans quelle mesure êtes-vous d'accord avec l'affirmation suivante : « L'usage de termes techniques (ex : ratio de Sharpe, arbitrage) renforce mon intérêt vis-à-vis de l'offre. » ?

- ☐ Pas du tout d'accord
- ☐ Plutôt pas d'accord
- ☐ Neutre
- ☐ Plutôt d'accord
- ☐ Tout à fait d'accord

Q22. Lors de votre lecture, comment avez-vous traité les informations techniques ?

- ☐ J'ai analysé précisément chaque terme avant de juger.
- ☐ La fluidité et le sérieux du ton m'ont permis de comprendre l'opportunité sans effort.
- ☐ Je me suis fié à l'impression globale de professionnalisme.

Q23. Quelle est la probabilité que vous cliquiez sur le lien pour obtenir plus d'informations ?

- ☐ 0% Aucune chance
- ☐ 25% - Peu probable
- ☐ 50% Peut-être
- ☐ 75% Probable
- ☐ 100% Certainement

Q24. Scénario fictif : En imaginant que vous soyez intéressé par l'offre, si vous aviez 1000 € à investir aujourd'hui, quelle somme seriez-vous prêt(e) à placer dans cette offre ?

- ☐ 1 € - 250 €
- ☐ 251 € - 500 €
- ☐ 501 € - 750 €
- ☐ 751 € - 1000 €

Q25. Entre les deux offres présentées, laquelle vous semble provenir d'une institution financière régulée ?

- ☐ L'offre A ("Salut ! Vu que...")
- ☐ L'offre B ("Suite aux fluctuations...")
- ☐ Aucune des deux
- ☐ Les deux
- ☐ Ne sait pas / Ne souhaite pas répondre

Q26. À quel point l'absence de fautes d'orthographe et la précision du langage influencent-elles votre intérêt envers une publicité en ligne ?

- ☐ 1 - Aucune influence
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5 - Influence maximale

Section 6: Offre C

Veuillez lire attentivement cette autre offre:

« ALERTE MARCHÉ : Nos systèmes viennent de détecter une inefficience critique sur l'arbitrage de volatilité. Accès restreint : plus que 3 places disponibles pour ce cycle. Cette fenêtre d'opportunité expirera automatiquement dans 15 minutes pour garantir le taux de rendement. Cliquez ici pour sécuriser votre allocation avant clôture immédiate. »

Q27. Sur une échelle de 1 à 5, comment évaluez-vous votre propre intérêt pour cette proposition ?

- ☐ 1 - Pas du tout intéressé(e)
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5 - Très intéressé(e)

Q28. Dans quelle mesure êtes-vous d'accord avec l'affirmation suivante : « Face à l'indication "Plus que 15 minutes", j'ai ressenti une tension me poussant à agir rapidement. » ?

- ☐ Pas du tout d'accord
- ☐ Plutôt pas d'accord
- ☐ Neutre
- ☐ Plutôt d'accord
- ☐ Tout à fait d'accord

Q29. Quelle est la probabilité que vous cliquiez sur le lien pour obtenir plus d'informations ?

- ☐ 0% Aucune chance
- ☐ 25% Peu probable
- ☐ 50% Peut-être
- ☐ 75% Probable
- ☐ 100% Certainement

Q30. Scénario fictif : En imaginant que vous soyez intéressé par l'offre, si vous aviez 1000 € à investir aujourd'hui, quelle somme seriez-vous prêt(e) à placer dans cette offre ?

- ☐ 1 € - 250 €

- ☐ 251 € - 500 €
 - ☐ 501 € - 750 €
 - ☐ 751 € - 1000 €
-

Section 7: Offre D

Imaginez que vous voyez une offre d'investissement accompagnée d'une vidéo avec un individu décrivant l'offre:

« Bonjour, ici Jeff Bezos. J'ai personnellement analysé ce nouveau protocole d'arbitrage. Les résultats sont sans appel : c'est l'une des architectures les plus robustes que j'ai pu observer cette année. Je recommande vivement cette opportunité à ceux qui cherchent à diversifier leur portefeuille avec sérieux. »

Q31. Sur une échelle de 1 à 5, comment évaluez-vous votre propre intérêt pour cette proposition ?

- ☐ 1 - Pas du tout intéressé(e)
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5 - Très intéressé(e)

Q32. Quelle est la probabilité que vous cliquiez sur le lien pour obtenir plus d'informations ?

- ☐ 0% Aucune chance
- ☐ 25% - Peu probable
- ☐ 50% Peut-être
- ☐ 75% Probable
- ☐ 100% Certainement

Q33. Scénario fictif : En imaginant que vous soyez intéressé par l'offre, si vous aviez 1000 € à investir aujourd'hui, quelle somme seriez-vous prêt(e) à placer dans cette offre ?

- ☐ 1 € - 250 €
- ☐ 251 € - 500 €
- ☐ 501 € - 750 €
- ☐ 751 € - 1000 €

Section 8: Critères spécifiques

Pour chaque affirmation, indiquez votre niveau d'accord sur une échelle allant de « Pas du tout d'accord » à « Tout à fait d'accord ».

Affirmations	Pas du tout d'accord	Plutôt pas d'accord	Neutre	Plutôt d'accord	Tout à fait d'accord
Q34. Une institution financière sérieuse ne fait jamais de fautes d'orthographe.	[]	[]	[]	[]	[]
Q35. L'usage d'un jargon technique (ex: Euronext, arbitrage) est pour moi un signe de compétence.	[]	[]	[]	[]	[]
Q36. Le sentiment de pouvoir rater une offre exclusive me pousse à décider plus rapidement.	[]	[]	[]	[]	[]
Q37. Un compte à rebours m'incite à prendre une décision sans vérification supplémentaire.	[]	[]	[]	[]	[]
Q38. Voir que d'autres personnes ont déjà investi (des amis par exemple) me rassure sur la légitimité d'un projet.	[]	[]	[]	[]	[]
Q39. L'apparition d'une personnalité publique en vidéo renforce la crédibilité d'un projet.	[]	[]	[]	[]	[]

Section 9: Dernières questions

Q40. Avez-vous déjà été confronté à une tentative d'arnaque à l'investissement en ligne ?

- ☐ Oui, et j'ai perdu de l'argent
- ☐ Oui, mais j'ai détecté la fraude à temps
- ☐ Non, jamais
- ☐ Ne sait pas / Ne souhaite pas répondre

Q41. Selon vous, quelle offre parmi celles présentées aujourd'hui vous a semblé la plus « suspecte » après réflexion ? Veuillez classer dans l'ordre du plus suspect (1) au moins suspect (4).

- **1 (Le plus suspect) :** ☐ **Offre A** (« Salut ! Vu que le marché bouge beaucoup... ») ☐ **Offre B** (« Suite aux récentes fluctuations... ») ☐ **Offre C** (« ALERTE MARCHÉ : Nos systèmes... ») ☐ **Offre D** (« Bonjour, ici Jeff Bezos... »)
- **2 :** ☐ **Offre A** (« Salut ! Vu que le marché bouge beaucoup... ») ☐ **Offre B** (« Suite aux récentes fluctuations... ») ☐ **Offre C** (« ALERTE MARCHÉ : Nos systèmes... ») ☐ **Offre D** (« Bonjour, ici Jeff Bezos... »)
- **3 :** ☐ **Offre A** (« Salut ! Vu que le marché bouge beaucoup... ») ☐ **Offre B** (« Suite aux récentes fluctuations... ») ☐ **Offre C** (« ALERTE MARCHÉ : Nos systèmes... ») ☐ **Offre D** (« Bonjour, ici Jeff Bezos... »)
- **4 (Le moins suspect) :** ☐ **Offre A** (« Salut ! Vu que le marché bouge beaucoup... ») ☐ **Offre B** (« Suite aux récentes fluctuations... ») ☐ **Offre C** (« ALERTE MARCHÉ : Nos systèmes... ») ☐ **Offre D** (« Bonjour, ici Jeff Bezos... »)

Q42. Pensez-vous être capable d'identifier de fausses offres d'investissements qui utilisent l'IA afin de tromper les potentiels investisseurs ?

- ☐ Oui
- ☐ Non
- ☐ Ne sait pas / Ne souhaite pas répondre

Fin - Merci !

Merci pour votre participation !

Cette étude s'inscrit dans le cadre d'un mémoire en Criminologie à l'Université de Liège. Certaines offres présentées au cours de ce questionnaire étaient fictives et créées uniquement pour les besoins de la recherche. L'objectif est d'analyser comment certains leviers (jargon technique, sentiment d'urgence, utilisation de l'image de célébrités et de l'intelligence artificielle) peuvent influencer la perception de légitimité d'une offre.

Méfiez-vous des offres trop belles pour être vraies, même si elles semblent relayées par des personnalités connues.

Vos données restent anonymes et ne seront utilisées qu'à des fins statistiques académiques.