



MINISTÈRE
DE LA TRANSFORMATION
ET DE LA FONCTION
PUBLIQUES

*Liberté
Égalité
Fraternité*



SCIENCES COMPORTEMENTALES APPLIQUÉES

Mieux protéger le consommateur
en ligne

DÉCEMBRE
2021



Direction interministérielle
de la transformation publique

RÉSUMÉ

L'enjeu

Chaque année, 780 000 personnes âgées de 14 ans ou plus résidant en France métropolitaine - soit 1,6% de la population adulte - achètent un produit ou un service qui n'est pas ensuite livré, ne correspond pas aux qualités ou quantités attendues, ou déclenche un coût supplémentaire imprévu pour le consommateur.

Avec la croissance du cybercommerce, un pourcentage toujours plus important de ces personnes peut être classé comme **victimes de fraudes à l'achat en ligne**. Dans près de la moitié des cas, une fraude à l'achat entraîne une perte de plus de 100€ pour le consommateur, tandis que 11% des cas mènent à une perte de plus de 1 000€.

La montée en popularité du commerce en ligne a, en effet, multiplié les possibilités pour les escrocs : alors qu'auparavant, les arnaqueurs devaient contacter eux-mêmes leurs victimes, ils peuvent maintenant les laisser venir vers eux. De plus, les progrès réalisés dans la conception des interfaces utilisateurs (tels que l'émergence de « dark patterns ») a donné aux escrocs plus d'occasions d'attirer l'attention sur de fausses offres alléchantes.

Il est donc essentiel de trouver des solutions pour aider les consommateurs à se protéger des fraudes à l'achat en ligne.

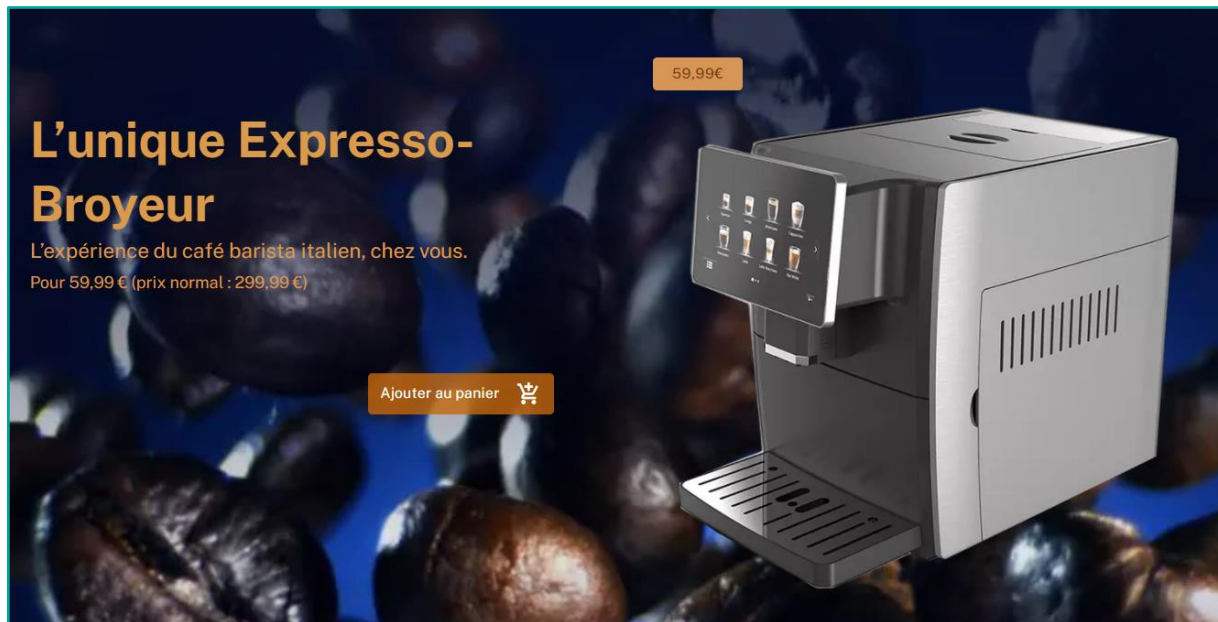
La solution testée

Afin d'essayer de réduire la vulnérabilité des consommateurs aux fraudes à l'achat en ligne, nous avons développé une intervention cherchant à générer **une prise de conscience** chez les consommateurs sans qu'ils aient à subir des pertes. Le fait d'être « arnaqué » sert alors à créer un « *moment d'apprentissage* », au cours duquel les consommateurs sont plus susceptibles d'être réceptifs à un message de prévention.¹

Pour ce faire, nous avons mis en place une simulation de site de vente de produits en ligne - DiBartolo.fr, un fabricant de machines à café - que nous avons promue à travers des publicités Facebook. Le site mobilise plusieurs pratiques manipulatrices communément utilisées par les fraudeurs pour influencer l'achat des consommateurs (vente privée, faux descriptif, pas d'adresse/contact du vendeur, faux avis, faux état de stock, un prix anormalement bas, un compte à rebours, ...). Ces allégations s'apparentent à ce que la littérature appelle des « dark patterns »².

¹ Lawson PJ, Flocke SA. Teachable moments for health behavior change: A concept analysis. Patient Educ Couns. 2009; 76(1): 25-30.

² Mathur, A., Acar, G., Friedman, M., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. Proceedings of the



Une fois le « pot aux roses révélé », les consommateurs étaient informés qu'ils avaient failli être escroqués, et encouragés à adopter de nouveaux réflexes lors de leurs achats en ligne.

Nous avons également développé un module de formation en ligne (ou « **formation intégrée** ») pour donner des clés aux consommateurs pour se protéger. Cette formation était proposée aux consommateurs, juste après la révélation de la supercherie - l'idée étant de les cibler durant ce « moment d'apprentissage » et de s'assurer que la formation était offerte à des personnes véritablement vulnérables.

L'expérimentation

Pour déterminer le potentiel d'impact de cette intervention, nous avons mené un essai contrôlé randomisé durant lequel nous avons proposé une deuxième série de fausses offres aux personnes qui avaient « acheté » la première machine à café. Nous avons ensuite comparé le taux de « re-victimation » entre les groupes tests pour identifier l'impact de la **prise de conscience** et de la **formation intégrée**.

L'expérimentation s'est déroulée en deux temps. Dans un **premier temps**, lors de l'achat de la machine à café, le site répartissait de façon aléatoire les consommateurs dans l'un de trois groupes tests :

1. **Groupe de contrôle** : les consommateurs ont été remerciés pour leur commande et informés qu'ils seraient contactés le jour de son expédition afin

que leur paiement soit recueilli (ce groupe n'a été averti de la supercherie qu'à la fin de l'expérimentation).

2. **Prise de conscience** : les consommateurs ont été informés qu'ils avaient été exposés à une fausse annonce, encouragés à faire plus attention et redirigés vers des ressources consultables sur le site de la DGCCRF.
3. **Prise de conscience + formation intégrée** : en plus d'être exposé à la « prise de conscience », les consommateurs ont pu suivre la formation intégrée.

Dans un second temps, **nous avons proposé le deuxième ensemble de fausses offres à tous les participants à l'étude**, les invitant à acheter un nouveau produit sur un deuxième site de vente en ligne factice afin de mesurer l'impact de la prise de conscience et de la formation sur la vulnérabilité aux fraudes à l'achat en ligne.³ Enfin, tous les participants ont été invités à remplir une enquête de fin d'expérimentation afin de mesurer leur perception de l'acceptabilité de cette approche. L'expérimentation (comprenant la première et la deuxième offre) s'est déroulée sur une période d'un mois et demi, entre le 25 mai 2021 et le 5 juillet 2021.

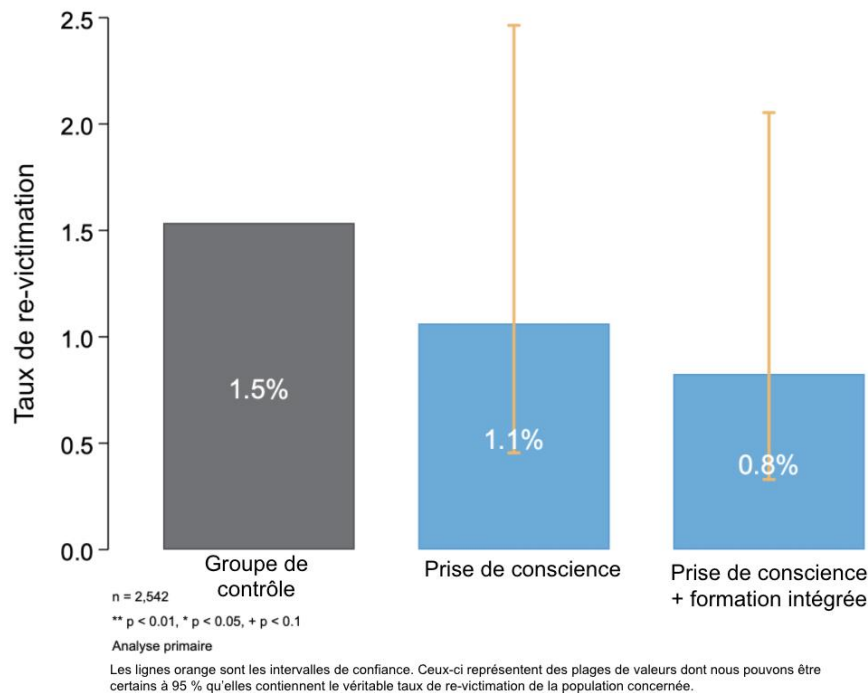
Les résultats principaux

L'intervention s'est avérée très mobilisatrice, démontrant à quel point les consommateurs sont vulnérables à ce type d'arnaque. Au total, 2 542 consommateurs ont « acheté » la machine à café. S'il s'était agi d'une vraie escroquerie, les préjudices subis par les consommateurs auraient été conséquents : la fausse offre aurait en effet généré plus de 150 000 € de revenus en moins de quatre semaines.

L'intervention montre un potentiel d'impact notable sur la vulnérabilité des consommateurs aux fraudes à l'achat en ligne. Néanmoins, malgré ce potentiel, **les résultats ne sont pas statistiquement significatifs** (probablement du fait de la taille de l'échantillon), et ne restent donc à ce jour que des indications.⁴ Nous ne pouvons pas conclure (avec un niveau de confiance de 95 %) que l'exposition à une "prise de conscience" et à une "formation intégrée" réduit la susceptibilité aux fraudes à l'achat.

³ <https://harrisontech.fr/tele4k>, <https://harrisontech.fr/platine>, <https://harrisontech.fr/enceinte-bt>

⁴ Nombre de personnes revictimisées: 13 - groupe de contrôle, 9 - groupe prise de conscience, 7 - groupe prise de conscience + formation intégrée



Néanmoins :

- Le message de « *prise de conscience* » montre une diminution de 0,4 points de pourcentage du taux de re-victimation par rapport au groupe de contrôle, soit une réduction de 27% en termes relatifs, comparé aux personnes n'ayant rien reçu (groupe contrôle).
- La combinaison du message de « *prise de conscience* » et de formation intégrée (groupe 3) est quant à elle liée à une diminution du taux de re-victimation encore plus notable (même si toujours non statistiquement significative) : 0.7 point de pourcentage, soit une diminution de 47% en termes relatifs, comparé au groupe de contrôle.
- Toutefois, ces résultats sont à considérer avec prudence, compte tenu de l'incertitude statistique qui entoure leur mesure (cf. précisions de lecture en légende du graphique précédent).
- La tendance positive est telle que cette intervention mérite néanmoins d'être testée à nouveau.

Une enquête de fin d'expérimentation a été faite auprès des 2 542 consommateurs qui ont acheté la machine à café et ont donc participé à l'étude. **Plus de 9 sur 10 répondants (n = 61) ont considéré l'approche appropriée pour une campagne de sensibilisation.**

Suites possibles

Les résultats de ce rapport sont encourageants : **une fausse offre dans un environnement sécurisé, suivie d'un message de prise de conscience et d'exercices, peut mobiliser un grand nombre de consommateurs, est perçue comme acceptable et utile par les répondants à notre enquête de fin d'expérimentation, et pourrait potentiellement réduire la vulnérabilité des consommateurs aux fraudes en ligne.**

Ce mécanisme a donc un potentiel d'impact qui mériterait d'être testé et approfondi à nouveau. Dans cette optique, nous explorons avec la DGCCRF et la DITP si cette intervention peut être appliquée à d'autres situations et testée à nouveau.

En outre, ces travaux sont une démonstration des apports potentiels des sciences comportementales et des méthodes expérimentales pour innover dans le domaine de la protection des consommateurs.

Grâce à un diagnostic rigoureux des risques posés pour les consommateurs par certaines pratiques commerciales, l'approche comportementale permet en effet de développer des innovations ciblées, et de les pré-tester afin d'identifier les futurs éléments clés des politiques de protection des consommateurs.

A l'heure où la Commission européenne, l'OCDE et la commission fédérale américaine du commerce (FTC) réfléchissent à leur position sur les « dark patterns », des études expérimentales de ce type peuvent ainsi fournir des compléments importants aux études de juristes, d'économistes ou universitaires, plaçant le consommateur, sa cognition, ses limitations et ses préférences au centre de la réflexion.

SOMMAIRE

Résumé	2
Sommaire	7
1. Contexte	8
2. Pourquoi un focus sur les fraudes à l'achat en ligne ?	10
3. Qu'est-ce qui nous rend vulnérables aux fraudes à l'achat en ligne ?	13
3.1. Barrières pouvant expliquant la vulnérabilité face aux fraudes à l'achat en ligne	13
3.2. Leviers pour réduire la vulnérabilité aux fraudes à l'achat en ligne	14
4. Solution testée : encourager une prise de conscience pour inciter les consommateurs à la prudence	17
4.2. Prise de conscience	22
4.3. Formation intégrée et règles heuristiques	23
5. Résultats : cette intervention peut-elle réduire la vulnérabilité aux fraudes en ligne ?	26
5.1. Design expérimental et questions de recherche	26
5.2. Ce type d'intervention mobilise-t-il ?	30
5.3. Ce type d'intervention est-il perçu comme étant acceptable ?	35
5.4. Ce type d'intervention fonctionne-t-il ?	36
6. Suites possibles	45
Annexe méthodologique	48

1. Contexte

La **Direction interministérielle de la transformation publique (DITP)** a lancé en 2018 un appel à manifestation d'intérêt auprès des administrations centrales et opérateurs sociaux visant à mobiliser les enseignements et méthodes des sciences comportementales afin d'améliorer l'efficacité des politiques publiques. Cette démarche participe d'une triple conviction quant à la nécessité de :

- Comprendre finement les comportements réels des parties prenantes de l'action publique ;
- Promouvoir des modes d'interventions publiques plus incitatifs ;
- Et tester selon des standards scientifiques robustes les solutions identifiées, afin de déployer à terme des interventions fondées sur des études et des preuves concrètes.

L'appel à manifestation d'intérêt (AMI),⁵ rendu possible par un financement du Programme d'Investissements d'Avenir,⁶ incluait cinq critères d'appréciation. La DITP a encouragé les problématiques suivantes :

1. À fort impact ou du moins à fort potentiel de répliquabilité ;
2. À dominante comportementale (et non d'ordre technique, financier, etc.) ;
3. Faisant l'objet d'un consensus éthique ;
4. Permettant un accès à des données et donc une mesure d'efficacité ;
5. Et faisant l'objet d'un portage institutionnel robuste.

La **Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF)** a été l'un des lauréats de cet AMI avec une candidature portant sur la protection des consommateurs contre les fraudes. Afin de répondre à cet enjeu, la DITP a sollicité l'appui et l'expertise du Behavioural Insights Team (BIT)⁷ pour appliquer les leçons des sciences comportementales à ce domaine.

Au cours de la phase de ciblage du projet, le périmètre du travail a été précisé : il a ainsi été décidé que le projet se focaliserait sur **l'amélioration de la protection des**

⁵

https://www.modernisation.gouv.fr/sites/default/files/fichiersattaches/appel_a_manifestation_dinteret_valide_sciences_comportementales.pdf

⁶ <https://www.gouvernement.fr/le-programme-d-investissements-d-avenir>

⁷ Le BIT est un organisme de conseil indépendant qui se consacre à l'application des sciences du comportement et à l'évaluation systématique des politiques publiques. Pour plus d'informations: <https://www.bi.team/>

consommateurs contre les fraudes à l'achat en ligne, qui constitue une des priorités actuelles de la DGCCRF. L'objectif de ce projet était donc de :

Développer une intervention ayant le potentiel de réduire les achats en ligne causés par les fraudes, qui peuvent s'identifier par les conséquences suivantes :

- produit ou service non livré ou non rendu
- qualité ou quantité non conformes
- coût supplémentaire imprévu pour le consommateur

2. Pourquoi un focus sur les fraudes à l'achat en ligne ?

Chaque année, plus de 780 000 personnes âgées de 14 ans ou plus résidant en France métropolitaine - soit 1,6% de la population adulte - achètent un produit ou un service qui n'est pas ensuite livré, ne correspond pas aux qualités ou quantités attendues, ou déclenche un coût supplémentaire imprévu pour le consommateur.⁸

Avec la croissance du cybercommerce, un pourcentage toujours plus important de ces personnes peut être classé comme victimes de fraudes à l'achat en ligne. En 2018, plus de la moitié des victimes d'escroqueries (51%) s'était fait piéger sur Internet, loin devant le téléphone (21%) et le démarchage à domicile (8%).⁹

La montée en popularité du commerce en ligne a, en effet, changé les règles du jeu et multiplié les possibilités pour les escrocs : alors qu'auparavant, les arnaqueurs devaient contacter eux-mêmes leurs victimes, ils peuvent maintenant les laisser venir vers eux.

Aucun groupe n'est exclu de cette menace : le taux de victimisation aux arnaques semble globalement uniforme, et être indépendant du sexe, de l'âge, la catégorie socioprofessionnelle de la victime et la régularité avec laquelle il effectue des achats en ligne.¹⁰

Lorsque des fraudes à l'achat en ligne se produisent, elles peuvent avoir de graves conséquences financières et psychologiques pour les victimes. Dans un peu moins de la moitié des cas, une fraude à l'achat entraîne une perte de plus de 100€ pour le consommateur, tandis que 11% des cas mènent à une perte de plus de 1 000€.¹¹ Étant donné que 40% des Français épargnent moins de 1 000€ par an, ce niveau de préjudice est très important.

Il est donc essentiel de trouver des solutions pour aider les consommateurs, au sens le plus large du terme, à se protéger des fraudes à l'achat en ligne.

⁸ Données de 2018. Source: Rapport d'enquête Cadre de vie et sécurité 2019, SSMSI. Disponible sur : <https://www.interieur.gouv.fr/Interstats/L-enquete-Cadre-de-vie-et-securite-CVS/Rapport-d-enquete-Cadre-de-vie-et-securite-2019>

⁹ L'Observatoire national de la délinquance. Une arnaque sur deux a lieu sur internet. Disponible sur : <https://www.vie-publique.fr/en-bref/276265-une-arnaque-sur-deux-lieu-sur-internet>

¹⁰ SSMSI. (2019). Chiffres sur la victimation 2019. Disponible sur : <https://www.interieur.gouv.fr/Interstats/Actualites/Rapport-d-enquete-Cadre-de-vie-et-securite-2019>

¹¹ SSMSI. (2019). Chiffres sur la victimation 2019. Disponible sur : <https://www.interieur.gouv.fr/Interstats/Actualites/Rapport-d-enquete-Cadre-de-vie-et-securite-2019>

Quelles techniques utilisent les escrocs ?

Lors de la promotion d'une fausse offre en ligne, les escrocs incluent des éléments faux et/ou omettent des détails essentiels afin d'inciter le consommateur à prendre une décision commerciale qu'il n'aurait pas prise en d'autres circonstances. Il s'agit par exemple de faux rabais, de frais cachés, de fausses descriptions de produits et de faux avis.

Les progrès réalisés dans la conception des interfaces utilisateurs ont donné aux escrocs plus d'occasions d'attirer l'attention des utilisateurs vers ces faux éléments, ou de cacher des informations essentielles, dans l'espoir de générer des achats. Ces dernières années ont vu l'émergence de « **dark patterns** » - des éléments de l'interface qui poussent les consommateurs à faire des achats, tels que les comptes à rebours, les notifications d'activités et les messages de commandes en cours.

Nous présentons ci-dessous une sélection des pratiques frauduleuses les plus répandues sur les marchés en ligne :

Exemples de pratiques frauduleuses affirmant la popularité ou qualité d'un produit



Commandes en cours - Ce message montre le nombre en cours - même dans les cas des commandes anciennes

Faux avis - le même avis apparaît plusieurs fois sur ce site, avec des noms de clients différents

Notification d'activité - Ce message indique le nombre d'individus qui ont ajouté le produit au panier dans les dernières 72 heures

Exemples de pratiques frauduleuses soulignant la nature limitée d'une offre



Compte à rebours - L'offre est disponible même après l'expiration de la minuterie

Offre limitée - Ces sites Web affirment que les ventes se termineront « bientôt » sans indiquer de date limite.

Exemples d'offre frauduleuse cachant des informations essentielles



Abonnement caché - Cette publicité promet un iPhone à un prix imbattable, mais ne met pas en évidence le fait que le consommateur s'inscrit aussi à un abonnement de 89 € / mois

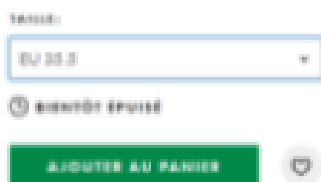
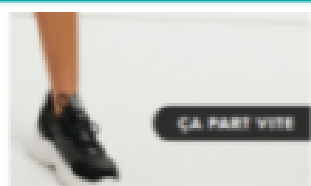
Exemples de pratiques frauduleuses utilisant des « simulateurs de confiance »



Faux sceaux et certificats - Ce faux label a été utilisé pour tromper les consommateurs en leur faisant croire qu'un produit conforme aux standards Européens, alors qu'il signifie « China Export » (20 minutes, 2019)

Faux logos et marques - ce site Web a utilisé un faux logo de la Fondation du patrimoine pour encourager les utilisateurs à faire un don à un faux site Web pour soutenir la reconstruction de Notre-Dame (Europe1, 2019).

Exemples de pratiques frauduleuses indiquant qu'une offre est rare



Forte demande - ce message apparaît pour tous les produits dans le panier

Bas niveau de stock - Ce message apparaît pour tous les produits

L'utilisation des « *dark patterns* » est de plus en plus commune, à la fois sur les sites légitimes et illégitimes. Une étude des 11 000 marchés en ligne les plus populaires dans le monde a trouvé que 11 % d'entre eux les utilisent.¹² Les sites web frauduleux, quant à eux, mobilisent des versions agressives des « *dark patterns* », falsifiant par exemple les informations présentées au consommateur et employant une interface utilisateur coercitive pour influencer le comportement des consommateurs.

Cette tendance risque d'aggraver encore le problème des fraudes à l'achat en ligne : des études pionnières ont montré que les « *dark patterns* » peuvent avoir un impact considérable sur le comportement d'achat d'une personne, tout en passant souvent complètement inaperçus par celle-ci.^{13 14} Il est donc important que les initiatives visant à protéger les consommateurs contre les fraudes à l'achat en ligne les éduquent également sur les techniques que les fraudeurs utilisent pour les tromper, y compris les « *dark patterns* ».

¹² Mathur, A., Acar, G., Friedman, M., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. Proceedings of the ACM on Human-Computer Interaction. ArXiv. Disponible sur : <https://arxiv.org/pdf/1907.07032.pdf>

¹³ Idem

¹⁴ Luguri, J., Strahilevitz, L. 2019. Shining a light on dark patterns. University of Chicago, Public Law Working Paper. No. 719. Disponible sur : <https://static1.squarespace.com/static/5d96a88b1171fc55023ea912/t/5e2548bd3e92f9543996238e/1579501761768/Shining+a+Light+on+Dark+Patterns.pdf>

3. Qu'est-ce qui nous rend vulnérables aux fraudes à l'achat en ligne ?

Nous avons mené un ensemble d'activités de recherche afin d'identifier les facteurs pouvant expliquer et potentiellement accroître ou diminuer la vulnérabilité face aux pratiques commerciales trompeuses en ligne. Parmi ces activités de recherche nous identifions une revue de la littérature, ainsi qu'une série d'entretiens avec les experts de la DGCCRF, des associations de consommateurs et enfin avec des consommateurs qui avaient signalé de telles pratiques par le passé.

Les conclusions de cette phase d'exploration sont détaillées dans un rapport de diagnostic du projet, qui propose une synthèse des obstacles et leviers identifiés, ainsi qu'une série d'options de solutions fondées sur les sciences comportementales.

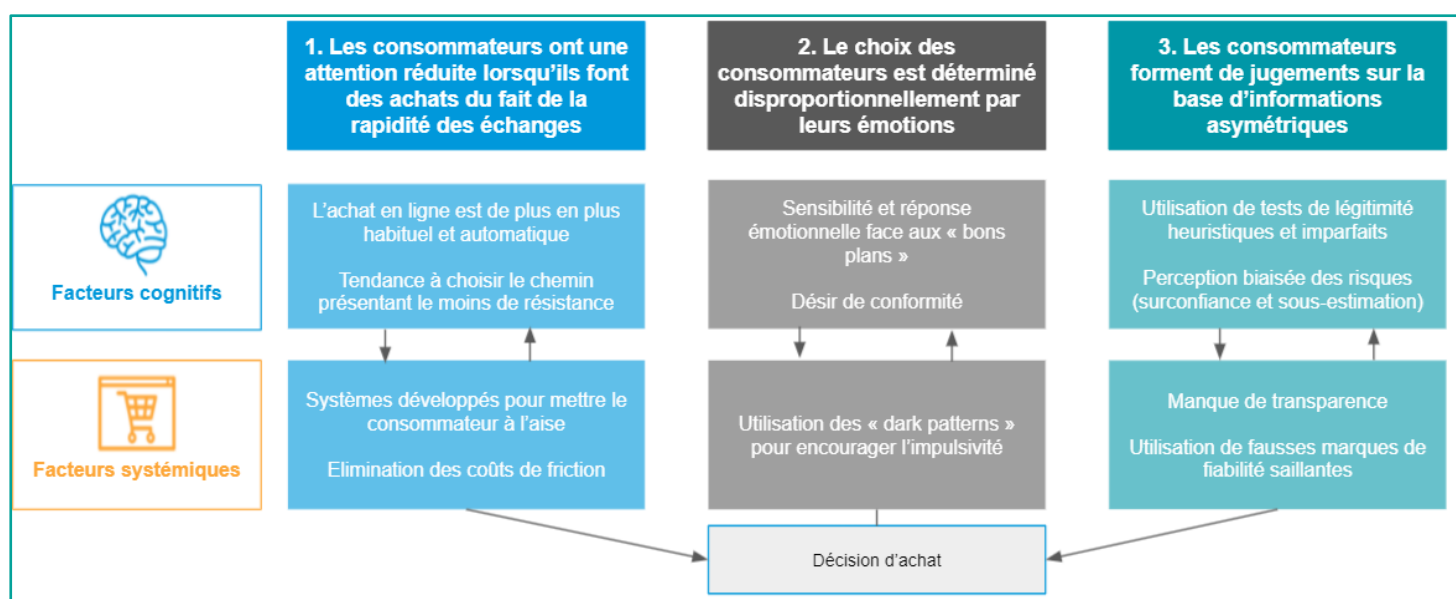
3.1. Barrières pouvant expliquant la vulnérabilité face aux fraudes à l'achat en ligne

Nous avons identifié trois grandes barrières (figure 1 ci-après) expliquant la vulnérabilité aux fraudes à l'achat en ligne, liées à :

1. Une attention réduite des consommateurs ;
2. Des choix déterminés disproportionnellement par les émotions ;
3. Des jugements formés sur la base d'informations asymétriques.


Il est par ailleurs rapidement devenu clair que la vulnérabilité aux pratiques commerciales trompeuses est entraînée à la fois par les biais cognitifs des consommateurs, mais aussi par les techniques employées par les vendeurs en ligne pour les duper ou pour déclencher des achats. Ces facteurs cognitifs et systémiques se combinent et se nourrissent mutuellement, incitant ainsi les consommateurs à prendre une décision qu'ils n'auraient pas prise en d'autres circonstances.



Figure 1 : Barrières expliquant la vulnérabilité aux fraudes à l'achat en ligne



3.2. Leviers pour réduire la vulnérabilité aux fraudes à l'achat en ligne

Nous avons proposé une série de leviers (ou pistes de solutions) afin de répondre « en miroir » aux barrières identifiées. Ceux-ci sont résumés ci-dessous et détaillés dans leur intégralité dans le rapport de diagnostic.

Barrière	Levier
Attention réduite 	Pour capter l'attention des consommateurs : <ol style="list-style-type: none"> 1. Concentrer leur attention, grâce à des amorces affichées pendant le parcours d'achat et qui demandent aux consommateurs d'effectuer certaines vérifications avant de pouvoir confirmer l'achat 2. Protéger par défaut, à travers un plug-in intelligent qui est capable de détecter la présence de « <i>dark patterns</i> » et qui notifie le consommateur quand un marché en ligne paraît risqué
Détermination émotionnelle du choix	Pour aider les consommateurs à faire des choix en pleine conscience de leur réponse émotionnelle : <ol style="list-style-type: none"> 3. Créer des opportunités de réflexion, à travers (a) des exercices de délibération introduits au moment de la vente, qui demandent au consommateur par exemple d'expliquer pourquoi il souhaite effectuer l'achat ou

	<p>d'effectuer un quiz sur les dark patterns ou bien (b) un « <i>ami numérique</i> » intégré dans une application de banque mobile, qui permettra aux consommateurs d'établir des restrictions sur les achats sur des sites Web inconnus et à des moments particuliers</p> <p>4. Créer des moments de prise de conscience, grâce à la mise en place d'une simulation d'une fraude à l'achat, divulguée en ligne, et qui incorpore une « <i>formation intégrée</i> qui éduque les consommateurs au moment où ils se font avoir.</p>
<p>Formation imparfaite de jugements</p> 	<p>Pour guider les consommateurs afin qu'ils puissent mieux évaluer les risques :</p> <p>5. Développer des règles heuristiques (des règles simplificatrices permettant d'aboutir à une solution satisfaisante dans des situations complexes), applicables à une large gamme de situations, que les consommateurs peuvent mettre en place pour se protéger lors des achats en ligne</p> <p>6. Fournir des outils de vérification, tel qu'un score, symbole ou label de confiance, qui peut permettre au conseiller de vérifier la légitimité d'un site d'un coup d'œil.</p>

Zoom : Méthodologie employée lors de la phase de diagnostic

Afin de mieux comprendre notre population-cible et son contexte, nous avons mené les activités de recherche suivantes :

- ❖ **Entretiens avec des consommateurs.** Quinze entretiens semi-directifs ont été conduits avec des consommateurs qui avaient été victimes d'une pratique commerciale trompeuse ou signalé une de ces pratiques à la DGCCRF. Le choix des consommateurs a été fait de façon à ce que nous obtenions un échantillon varié sur des critères tels que : le niveau de confiance en ligne ; la raison de la plainte (victime ou investigateur) ; l'âge ; le lieu de résidence ; et le nombre d'achats en ligne dans les trois derniers mois afin de couvrir différents contextes et comportements lors de ces entretiens.
- ❖ **Entretiens avec les associations de consommateurs.** Trois entretiens avec des organisations consoméristes afin de comprendre leur point de vue sur les barrières et potentiels leviers pour améliorer la protection du consommateur en ligne. Nous avons parlé avec des représentants de : Familles Rurales ; l'INC (Institut National de la Consommation) ; et CLCV (Consommation, Logement,

Cadre de Vie)

- ❖ **Entretiens avec des experts de la DGCCRF.** Cinq entretiens ont été menés avec différentes équipes de la DGCCRF, afin de faire une cartographie des outils employés pour protéger les consommateurs de pratiques commerciales trompeuses et de comprendre le fonctionnement de ses services. Nous avons parlé avec des représentants : du processus d'accueil des publics ; de la veille économique ; de SignalConso ; de la communication ; et de l'équipe gérant les relations avec les organisations de consommateurs

Nous remercions tous ceux qui ont participé aux entretiens pour leur aide.

En parallèle à ces activités de recherche, nous avons aussi effectué :

- ❖ **Une revue de la littérature** prenant en compte la recherche académique, la littérature grise (documentation parallèle non académique) y compris les rapports produits par la DGCCRF et autres agences publiques, les travaux du BIT, et les études menées en France ou à l'étranger - en nous concentrant tout particulièrement sur les pratiques commerciales trompeuses.
- ❖ **Une synthèse des leçons en barrières et leviers comportementaux**, qui empêchent ou aident les consommateurs à se protéger en ligne. L'identification de ces barrières et leviers nous a permis de proposer des pistes de solutions initiales pour réduire la vulnérabilité des consommateurs aux pratiques commerciales trompeuses en ligne.

4. Solution testée : encourager une prise de conscience pour inciter les consommateurs à la prudence

À partir de cette longue liste de solutions potentielles, nous avons décidé de développer une intervention visant en priorité à répondre au fait que les consommateurs ne cherchent à en savoir plus sur la protection contre les fraudes qu'une fois qu'ils se sont fait arnaquer - et donc trop tard.

Nous avons développé une intervention cherchant à générer une **prise de conscience chez les consommateurs** (levier 4 ci-dessus) sans qu'ils aient à subir des pertes. Le fait d'être « arnaqué » sert alors à créer un « *moment d'apprentissage* », au cours duquel les consommateurs sont plus susceptibles d'être réceptifs à un message de prévention.¹⁵

Pour ce faire, nous avons mis en place une simulation de site de vente en ligne - DiBartolo.fr, que nous avons promue à travers des publicités Facebook. Le site mobilise plusieurs des pratiques frauduleuses évoquées ci-dessus pour inciter les consommateurs à faire un achat.

Une fois le « pot aux roses » révélé, les consommateurs étaient informés qu'ils avaient failli être escroqués, et encouragés à adopter de nouveaux réflexes lors de leurs achats en ligne.

Nous avons également développé un module de formation en ligne (ou « **formation intégrée** ») pour donner des clés aux consommateurs pour se protéger des fraudes à l'achat en ligne. Cette formation était proposée aux consommateurs à l'issue de la révélation de l'arnaque - l'idée étant de les cibler durant ce « *moment d'apprentissage* », et de s'assurer que la formation était offerte à des personnes véritablement vulnérables. La formation intégrée comprend trois éléments :

1. Une série de règles heuristiques (levier 5 ci-dessus), ou réflexes d'achat à suivre pour se protéger lors d'achats en ligne.
2. Un exercice de « *mise en pratique* », qui invite les consommateurs à déterminer si une offre est légitime.
3. Un exercice « *bonus* » permettant aux consommateurs de calculer le point auquel leurs décisions d'achat sont influencées par leurs émotions et la

¹⁵ Lawson PJ, Flocke SA. Teachable moments for health behavior change: A concept analysis. Patient Educ Couns. 2009; 76(1): 25-30.

présence de « *dark patterns* ». L'objectif de cet exercice final était d'encore accentuer la prise de conscience.

Le diagramme ci-dessous résume le parcours suivi par un consommateur prenant part à cette intervention.

Figure 2 : Parcours usager de l'intervention

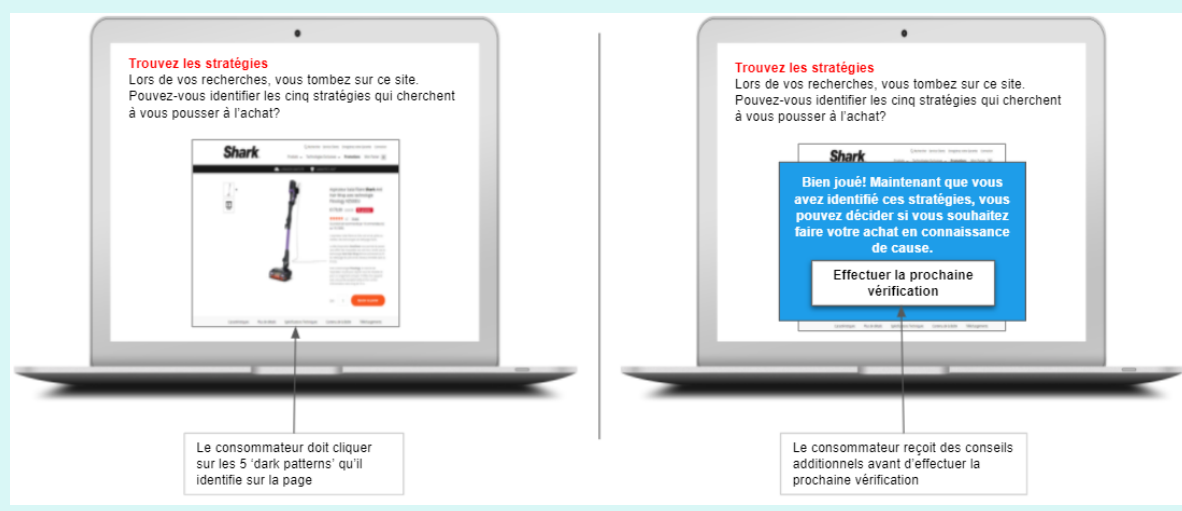


Zoom : intelligence collective et processus de co-construction

Suite à la publication de notre rapport de diagnostic, nous avons organisé une réunion qui a rassemblé des représentants de différentes équipes de la DGCCRF, au cours de laquelle les participants ont discuté et choisi parmi six pistes d'intervention différentes. Après une discussion en plénière sur chaque piste d'intervention, les participants ont noté les interventions potentielles en fonction de différents critères de faisabilité : impact, mise en place, mesurabilité et mise à l'échelle. Ce processus de co-sélection a conduit à une priorisation des différentes options et à la décision, validée en comité de pilotage, de développer une formation intégrée.

Idée	Scores combinés			
	Faisabilité - mise en oeuvre	Faisabilité - évaluation	Mise à l'échelle	Score total
Formation intégrée L'utilisation d'une formation intégrée pourrait aider à créer ces moments de changement en simulant l'erreur sans pour autant faire encourir de risques au consommateur. En pratique : Une fausse offre pourrait être divulguée en ligne. Les consommateurs seraient informés de la nature frauduleuse de l'offre, du risque qu'ils ont pris, et recevraient des informations pratiques pour se protéger en ligne. Evaluation : Test en ligne sur les clics / comportements faisant partie de la formation	14	12	13	53

Par la suite, nous avons formé deux groupes de travail composés d'experts pertinents de la DGCCRF dont la mission était de développer des prototypes de l'intervention. Un groupe s'est concentré sur le faux marché en ligne, tandis que l'autre s'est concentré sur la formation intégrée. Chaque groupe de travail s'est réuni tous les quinze jours sur une période de deux mois, travaillant ensemble pour créer des prototypes fonctionnels. Ceux-ci constituent la base des matériels d'intervention finaux.



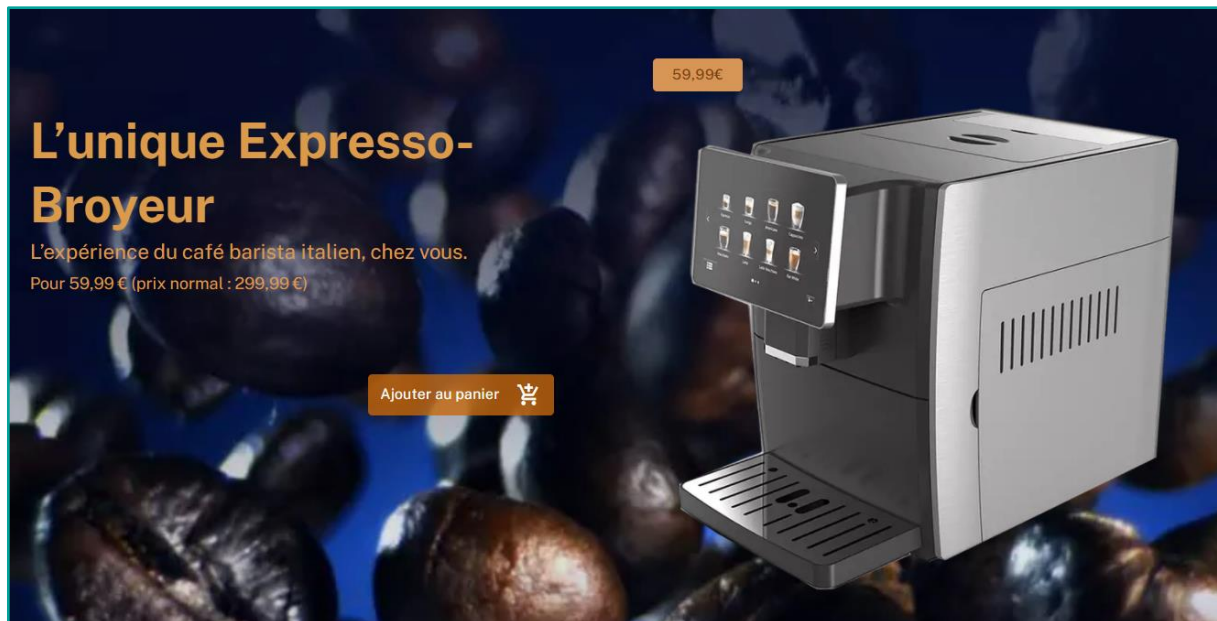
4.1. Di Bartolo.fr : un site de vente en ligne mobilisant des techniques communes pour encourager l'achat

Afin de pouvoir générer cette prise de conscience chez les consommateurs, il était important que nous puissions créer un site de vente en ligne aussi réaliste que possible ; de ce fait, de nombreuses tactiques d'incitation à l'achat ont été mobilisés à l'occasion de ce travail de co-création.

Parmi ces tactiques nous retrouvons des « dark patterns », fréquents même sur des sites légitimes (comptes à rebours, notifications de l'activité d'autres utilisateurs, faux

avis), jusqu'à des pratiques déloyales utilisées par des sites frauduleux (faux rabais, labels et accréditations).

C'est ainsi qu'est né dibartolo.fr - un site de vente en ligne offrant à l'achat une machine à café haut de gamme pour un prix drastiquement réduit.¹⁶



Un survol du site révèle la présence de plusieurs éléments frauduleux, notamment :

- Des fausses notifications sur l'activité d'autres consommateurs (*une commande vient d'être passée*) et des faux avis, qui jouent sur notre désir de **preuve sociale**, selon lequel nous déterminons nos choix en examinant les actions des autres.¹⁷



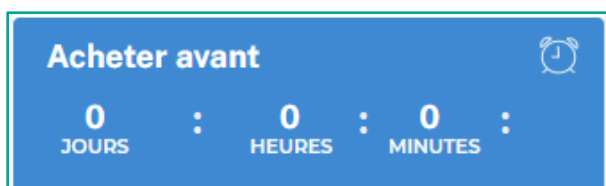
- Des faux stocks et des faux comptes à rebours. Ces informations soulignent le caractère limité d'une offre, en s'appuyant sur notre tendance à accorder plus de valeur aux choses qui apparaissent rares (**biais de rareté**)¹⁸ et à agir impulsivement lorsqu'on estime qu'une situation est **urgente**.¹⁹

¹⁶ Nous avons décidé de faire la promotion d'une machine à café suite à la réalisation d'une série de « tests de conversion », décrits à la page 25.

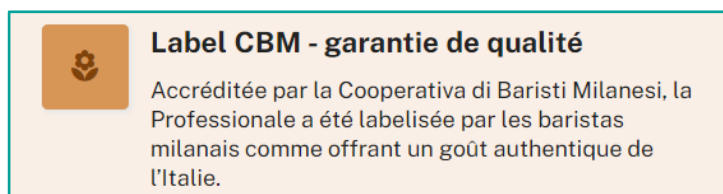
¹⁷ Cialdini, R. (2009). Influence: Science and practice. Vol. 4. Pearson education Boston

¹⁸ Mittone, L., & Savadori, L. (2009). The scarcity bias. Applied Psychology: An International Review, 58, 453–468.

¹⁹ Fischer P, Lea SEG, Evans KM. Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. Journal of Applied Social Psychology 2013; 43:2060–2072.



- Des faux descriptifs, labels et accréditations, manipulant la tendance des consommateurs à appliquer des critères imparfaits pour juger de la légitimité d'une offre, ainsi que leur tendance à faire confiance à des messagers d'autorité dans des situations d'asymétrie d'information.



Garantie de 3 ans - Di Bartolo Professionale est garantie trois ans. Au moindre problème avec la machine, nous vous rembourserons intégralement - sans que vous n'ayez de justification à apporter.

Afin de générer du trafic et des « achats » sur ce faux site de vente en ligne, une page business et des publicités ont été mises en ligne sur Facebook. Celles-ci soulignaient la durée limitée de l'offre et incitaient les consommateurs à se diriger vers DiBartolo.fr.

Figure 3 : Exemple de publicités publiées sur Facebook



Avant de lancer les fausses offres, nous avons effectué une série de tests de conversion (qui mesurent la *conversion* entre le visionnage d'une publicité et le fait de cliquer sur cette publicité, taux conversion que nous avons ensuite comparé pour chaque produit) pour s'assurer que nos offres pourraient attirer un grand nombre de participants (voir la page 25 pour plus de détails). Sur de nombreux points, nous avons donc utilisé les mêmes techniques marketings que celles utilisées habituellement par les sites de vente en ligne.

4.2. Prise de conscience

Pour le groupe **prise de conscience**, le « *parcours d'achat* » sur DiBartolo.fr était interrompu au moment de la validation de la commande : un consommateur arrivant à ce point se voyait alors informé qu'il avait failli « se faire avoir » et était invité à faire plus attention.

Comme évoqué précédemment, l'objectif est ici de provoquer une « prise de conscience » chez le consommateur sur les risques des achats en ligne. Celle-ci vise à susciter un choc et donner lieu à un « moment d'apprentissage » permettant d'éviter qu'il ne subisse un vrai préjudice financier. Ce message met également en contexte l'étendue du problème des fraudes à l'achat en ligne et dirige les consommateurs vers des ressources mises en ligne par la DGCCRF pour les protéger.

Figure 4 : Exemple de message de prise de conscience

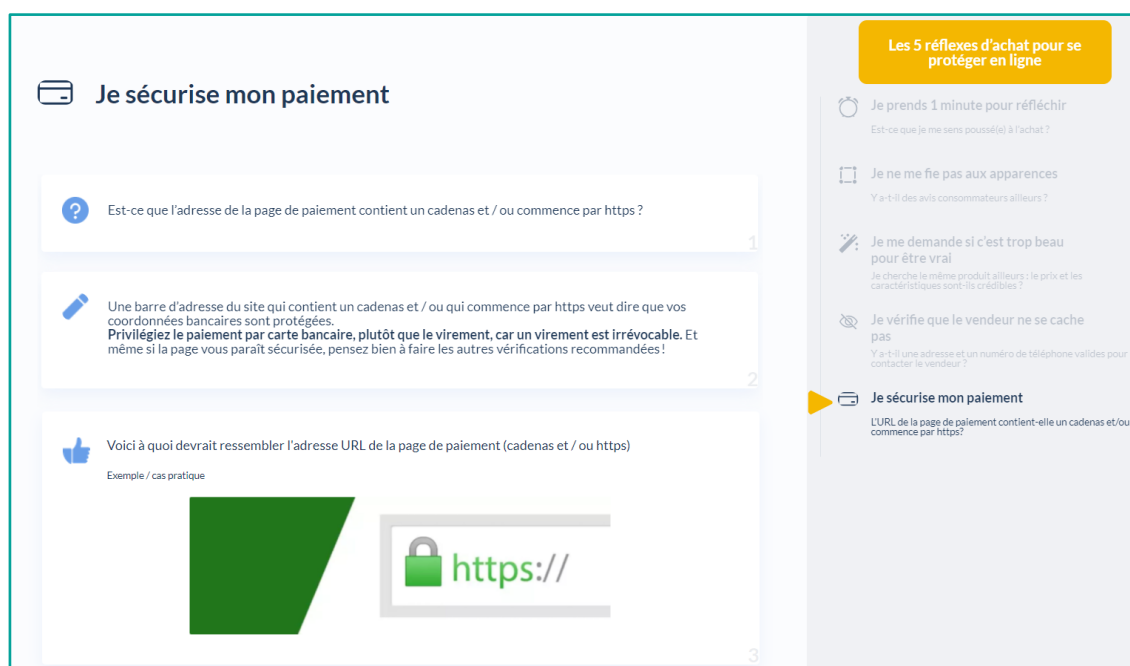


4.3. Formation intégrée et règles heuristiques

Pour les consommateurs tombant dans le troisième groupe d'expérimentation, en plus de partager le message de « prise de conscience », nous avons également testé le fait d'offrir la possibilité de suivre une « formation intégrée » gratuite. Cette formation comportait trois éléments, présentés aux utilisateurs dans une séquence linéaire :

1. Une série de **règles heuristiques** (les « *réflexes d'achat* »), applicables à un large éventail de situations et à suivre pour se protéger lors d'achats en ligne.²⁰ Notre travail de diagnostic a montré que les consommateurs mettaient en place des stratégies rudimentaires et souvent imparfaites pour se protéger en ligne. En développant des « *réflexes d'achat* », nous visions à proposer aux consommateurs un ensemble de règles plus efficaces que celles utilisées habituellement, offertes en format « aide-mémoire » pour une plus grande efficacité.

Figure 5 : Exemple de règles heuristiques



2. Un exercice de « ***mise en pratique*** » pendant lequel les consommateurs étaient confrontés à une série de fausses offres et invités à appliquer les règles heuristiques pour déterminer si l'offre était légitime ou non. Cet exercice applique plusieurs principes des sciences de l'apprentissage : un processus d'apprentissage par la pratique, un retour d'information immédiat, un cadrage conceptuel (par ex : sur les dark patterns), et une « trace » permettant de garder un souvenir des éléments clés (réflexes d'achat téléchargeables).

Figure 6 : Exemple d'un exercice de mise en pratique

Je prends 1 minute pour réfléchir

Voici le site sur lequel vous arrivez. Êtes-vous capable d'identifier les 3 stratégies utilisées pour vous pousser à l'achat ? Cliquez sur les éléments du site qui vous semblent être là pour vous pousser à l'achat.

Meilleure mini-site Plus que 24h à ce prix

Djerba - Choix Flex
Tunisie, Djerba

Vols et transferts inclus
Tout compris
Dates disponibles : 7 à 21 nuits

Y'a-t-il des avis consommateurs ailleurs ?

457€

Vite ! 5 réservations faites dans l'heure

Club Relax Djerba Mare
Tunisie, Djerba

Vols et transferts inclus
Tout compris
Dates disponibles : 7 à 10 nuits ou plus

8 jours 7 nuits dès 499€

Prix spécial ! En exclusivité pour nos clients

Suivant

1 — 2 — 3 — 4 — 5

Les 5 réflexes d'achat pour se protéger en ligne

Je prends 1 minute pour réfléchir
Est-ce que je me sens poussé(e) à l'achat ?

☐ **Je ne me fie pas aux apparences**
Y'a-t-il des avis consommateurs ailleurs ?

Je me demande si c'est trop beau pour être vrai
Je cherche le même produit ailleurs : le prix et les caractéristiques sont-ils crédibles ?

Je vérifie que le vendeur ne se cache pas
Y'a-t-il une adresse et un numéro de téléphone valides pour contacter le vendeur ?

Je sécurise mon paiement
L'URL de la page de paiement contient-elle un cadenas et/ou commence par https ?

- Un exercice offrant la possibilité pour les consommateurs de déterminer dans quelle mesure leurs décisions d'achat sont influencées par des « *dark patterns* » et leurs propres émotions. Dans cet exercice, l'individu voit plusieurs variations de la même offre et indique comment l'inclusion ou l'omission de certaines informations et « *dark patterns* » affecte son désir d'acheter le produit offert. Cet exercice répond à un constat selon lequel un individu est plus à même de se sentir concerné lorsqu'il perçoit le point auquel un conseil s'applique à son cas personnel. En montrant aux consommateurs à quel point leurs choix sont concrètement affectés par l'insertion de ces « *dark patterns* », nous espérons donc provoquer une prise de conscience supplémentaire sur le rôle que les émotions jouent sur les achats.

Figure 7 : Exemple de l'exercice « émotions »

Quiz: Quels sont les facteurs qui influencent vos décisions d'achats ?

37.5%

Dè Bartolo Professional
★★★★★ (nouveau)

Couleur: Noir

Stock disponibles
17%

Offre de lancement
149,99 € (prix unitaire à partir de votre recommandation)

Ajouter au panier

Livraison sous 2 JOURS en France

Déplacez le curseur pour indiquer à quel point cette annonce vous donne envie d'acheter cette cafetière

Ce produit ne me tente pas du tout

Je suis très tenté par ce produit

Suivant

Zoom : Ethique et Confidentialité

Un soin particulier a été porté au respect des règles d'éthique et de confidentialité des données (notamment en matière de RGDP) lors de cette expérimentation.

Considérations éthiques

Le protocole de recherche a été revu et validé par le comité éthique du Behavioural Insights Team, nos considérations principales pour l'éthique de cette recherche étaient les suivantes :

1. Nous n'avons pas demandé aux participants de partager leurs coordonnées bancaires lorsqu'ils effectuaient leur achat sur Di Bartolo (en préférant une simulation de paiement à la livraison), afin de limiter le stress potentiel lié au partage de ces données
2. Au moment où les participants étaient informés de la supercherie nous leur donnions aussi l'occasion d'agir immédiatement pour mieux se protéger à l'avenir, en leur partageant à minima les informations disponibles sur le site de la DGCCRF, et *a maxima* la formation intégrée. À la fin de l'expérimentation, tous les participants se sont aussi vus donner l'accès à la formation intégrée et aux réflexes d'achat. Ainsi, nous souhaitions éviter les sentiments d'impuissance ou de confusion qui peuvent suivre un moment de prise de conscience d'une fraude
3. À la fin de l'expérimentation, nous avons invité tous les participants à partager leurs retours sur cette approche, afin d'en comprendre l'acceptabilité
4. À ce même moment, nous avons également offert des possibilités de débriefing aux participants si ceux-ci en ressentaient le besoin à la suite de l'intervention, en les redirigeant vers des sources de soutien indépendantes, telles que le numéro de soutien France Victimes.

Protection des données et participation informée

Lors de sa visite sur le site Di Bartolo, si le consommateur cliquait sur le lien « politique de confidentialité » présent sur le site il était informé qu'il participait à une expérimentation scientifique, précisant dans quel cadre ses données pouvaient être récoltées et pour quel usage. Certains des commentaires laissés sur la page Facebook suggèrent que certains consommateurs ont lu la politique de confidentialité, et se sont rendu compte de la supercherie de cette manière.

5. Résultats : cette intervention peut-elle réduire la vulnérabilité aux fraudes en ligne ?

Afin d'évaluer l'efficacité de cette intervention, nous avons mis en place un essai contrôlé randomisé (ECR). Celui-ci s'est déroulé du 25 mai au 5 juillet 2021.

5.1. Design expérimental et questions de recherche

L'expérimentation s'est déroulée en deux temps. Dans un **premier temps**, les consommateurs ont « acheté » une machine à café sur le premier faux marché en ligne - dibartolo.fr. Lors de l'achat du produit, le site répartissait de façon aléatoire les consommateurs dans l'un de trois groupes tests :

4. **Groupe de contrôle** : les consommateurs ont été remerciés pour leur commande et informés qu'ils seraient contactés le jour de son expédition afin que leur paiement soit recueilli.
5. **Prise de conscience** : les consommateurs ont été informés qu'ils avaient été exposés à une fausse annonce frauduleuse, encouragés à faire plus attention et redirigés vers des ressources consultables sur le site de la DGCCRF.²¹
6. **Prise de conscience + formation intégrée** : en plus d'être exposé à la « prise de conscience », les consommateurs ont pu suivre la formation intégrée.

Dans un second temps, **nous avons proposé un deuxième ensemble de fausses offres à tous les participants à l'étude**, par l'intermédiaire d'une seconde campagne publicitaire publiée sur Facebook et partagée par courriel, les invitant à acheter un nouveau produit sur un deuxième marché en ligne factice.²²

Nous avons enfin mesuré les taux d'achat des seconds produits (ce que nous appelons les taux de « re-victimation »), et envoyé à tous les participants une enquête finale par courriel.

Zoom : la « re-victimation »


Afin de pouvoir mesurer les effets des interventions sur la vulnérabilité face aux fraudes à l'achat en ligne, nous avons tenté de recontacter tous les participants à l'étude pour leur soumettre une deuxième série de fausses offres, distincte de la première. Cette seconde série de fausses offres a été lancée un mois après la première offre.

²¹ <https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Pratiques-commerciales-trompeuses>

²² <https://harrisontech.fr/tele4k>, <https://harrisontech.fr/platine>, <https://harrisontech.fr/enceinte-bt>

Contrairement à la première fausse offre, qui proposait une machine à café, la deuxième fausse offre faisait la promotion de trois produits : une platine vinyle, un téléviseur 4K et une enceinte Bluetooth. Nous avons décidé d'utiliser cette approche au vu du fait qu'il n'y avait pas de moyen de savoir quels produits intéresseraient les acheteurs d'une machine à café en amont. Cette stratégie nous a permis d'accroître la chance d'intéresser les participants et donc de déterminer si l'intervention pouvait réduire la vulnérabilité des consommateurs face à des offres trompeuses.

La [platine vinyle](#), le [téléviseur 4K](#) et l'[enceinte Bluetooth](#) ont tous obtenu de bons résultats lors de nos tests de conversion (décrits à la page 25).



OLED 4K TV

169,99 €

Harrison OLED 4K



Réf. : EA873810

★★★★☆ 456 avis : 4.8/5

OLED 4K Ultra HD TV






Réf. : OLED4K721

Taille : 47 pouces

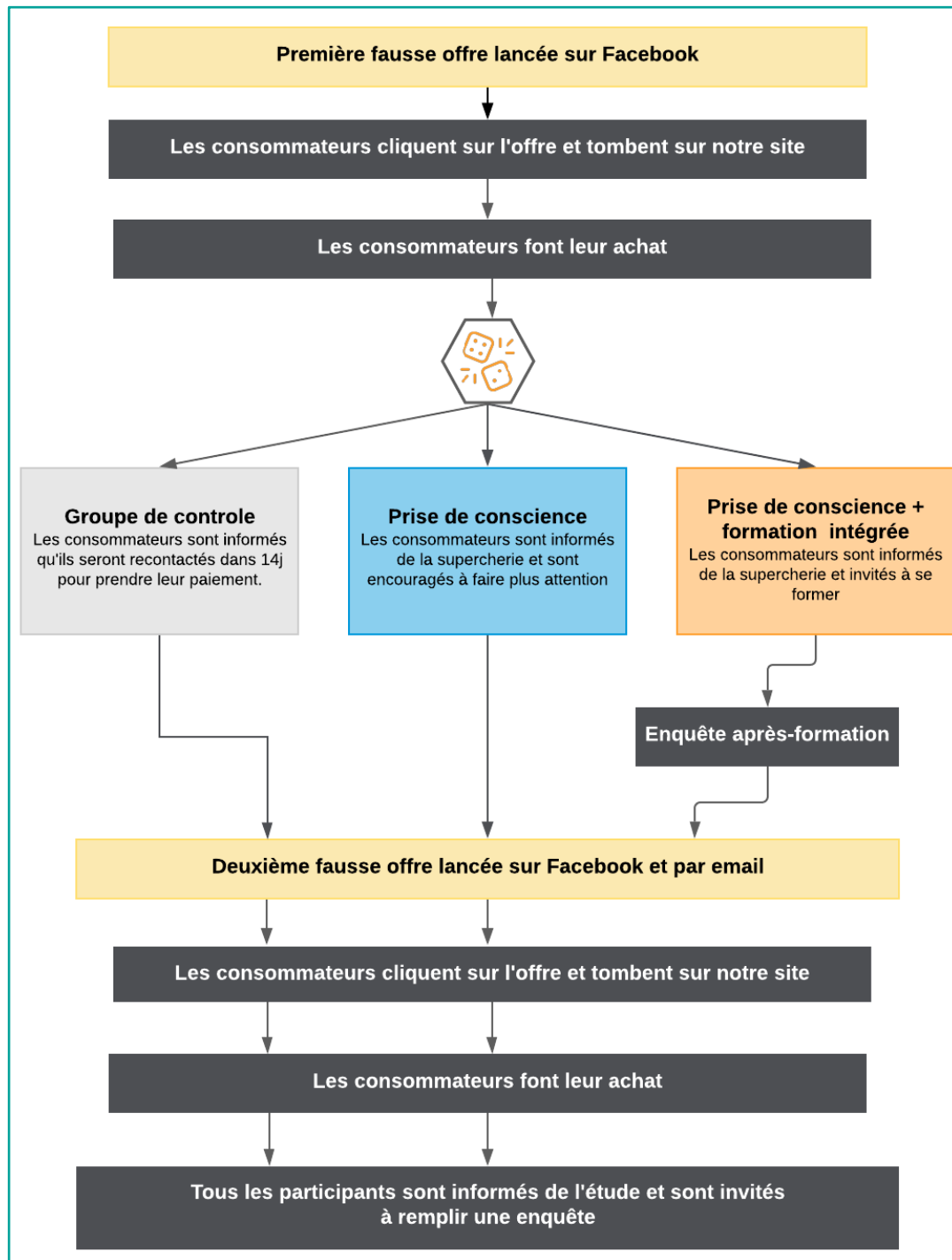
Caractéristiques

- 47 pouces
- Ecran ultra HD et ultra fin
- TV connectée Wifi
- Comprend un support mural ultraplat
- Compatible HDMI 2.1



Une synthèse du parcours des participants est présentée ci-dessous :

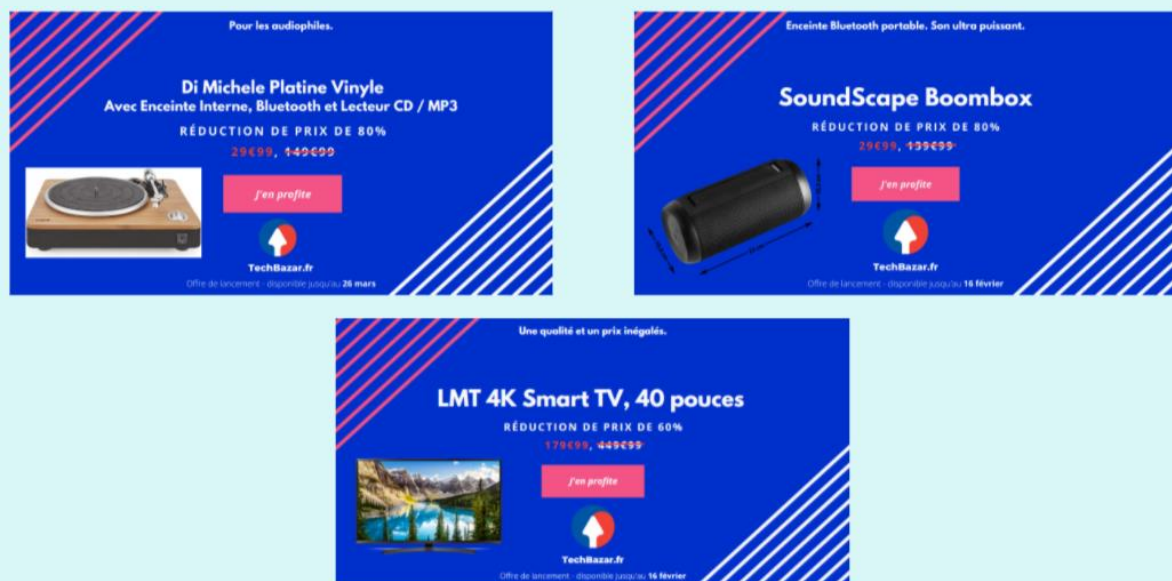
Figure 8 : Synthèse du parcours des participants



Zoom : tests de conversion

Nous avons réalisé une série de tests de conversion afin d'identifier les produits et les publicités ayant le plus grand potentiel d'attirer un maximum de clics et « d'achats ».

Dans la période précédant le lancement de l'étude, nous avons lancé 22 annonces depuis une page Facebook business pour différents produits à bas prix et observé quels produits généraient le coût par clic le plus bas. Nous avons utilisé la même charte graphique pour chaque annonce, en ne manipulant que le produit et certains détails liés à l'offre pour maintenir un niveau de comparabilité entre les publicités.



Une fois les produits sélectionnés, nous avons testé une série de publicités différentes, chacune avec sa propre charte graphique, en sélectionnant à nouveau celles associées au coût par clic le plus bas.

Enfin, nous avons lancé un test de conversion « approfondi », au cours duquel nous avons testé le parcours du consommateur complet sur une version bêta de notre premier faux marché en ligne. Cet exercice nous a permis de nous assurer, avant le lancement de l'étude, que l'expérimentation pourrait attirer un nombre important de participants.

Ce design expérimental nous permet d'établir le potentiel d'impact de ce type d'intervention en offrant des réponses à trois questions de recherche principales :

1. **Ce type d'intervention mobilise-t-il les consommateurs ?** Il est en effet essentiel, pour la DGCCRF, de savoir si ce type d'intervention peut atteindre sa cible. Pour y répondre, nous analysons :
 - le nombre et le profil démographique des personnes qui ont vu ou cliqué sur l'une des publicités autour de la première fausse offre (la machine à café)
 - le nombre de personnes qui ont visité le premier faux marché en ligne, ajouté la machine à café au panier et passé une commande (et qui, ce faisant, sont devenus participants à l'étude)
 - la mesure dans laquelle les participants ont interagi avec les messages de « prise de conscience » et/ou la « formation intégrée ».
 - la quantité et la nature des commentaires laissés par les consommateurs sur nos publicités Facebook et envoyés par courriel.
2. **Ce type d'intervention est-il perçu comme étant acceptable par les consommateurs ?** En effet, la question se pose lorsque les pouvoirs publics mettent en place un protocole visant à « tromper » les consommateurs. Pour y répondre, nous analysons :
 - les réponses à une enquête envoyée à tous les participants de l'étude à la fin de l'expérience
3. **Ce type d'intervention fonctionne-t-il ?** Ou autrement dit : les participants sont-ils moins à même de « se faire avoir » une seconde fois après avoir été soumis à la prise de conscience et/ou reçu la formation ? Pour y répondre, nous analysons :
 - la fraction de participants ayant acheté un second produit (les taux de re-victimation) dans les différents groupes expérimentaux

5.2. Ce type d'intervention mobilise-t-il ?

Enseignement principal : l'intervention a touché un public large pour un budget pourtant limité. Si l'engagement envers le message « *prise de conscience* » était élevé, le niveau d'interaction avec la formation reste plus mitigé.

L'intervention a touché un public important et varié

Notre [première fausse offre](#), active du 25 mai au 21 juin 2021, a obtenu un taux de conversion élevé, démontrant que (a) l'approche utilisée peut mobiliser un nombre

important de consommateurs et (b) qu'un grand nombre de personnes restent vulnérables aux fraudes de ce type hébergées sur les réseaux sociaux.

Au total :

- **467 000** consommateurs uniques ont **vu** une de nos publicités
- **20 000** (4,3%) d'entre eux ont **cliqué** sur l'une de nos publicités. Ce taux de clics est supérieur à la moyenne sur Facebook, qui est de 0,89% tous secteurs confondus.²³
- **6 000** (1,3%) d'entre eux ont **ajouté** la machine à café à **leur panier**.
- **2 542** (0,5%) d'entre eux ont **« acheté » la machine à café** et sont devenus des participants de l'étude.²⁴

S'il s'agissait d'une vraie escroquerie, les préjudices subis par les consommateurs auraient été conséquents. En effet, si nous avons collecté les paiements des consommateurs, notre fausse offre aurait généré **plus de 150 000 € de revenus** en moins de quatre semaines, alors que nous n'avions investi que 6 650 € sur la conception et la diffusion des annonces.

Cette méthode semble donc prometteuse, car : 1) elle permet d'atteindre un public large à un coût raisonnable, et 2) elle permet de cibler ce budget sur des personnes vulnérables aux fraudes à l'achat en ligne. Cette méthode permet donc de créer un lien direct avec un public susceptible de tomber victime d'une fraude utilisant les mêmes pratiques, et donc de cibler efficacement ces communications.

L'audience atteinte par les publicités pour la première fausse offre était par ailleurs relativement variée en termes d'âge et de genre :

- **Sexe (H/F) : 62% / 38%**
- **Catégorie d'âge :**
 - **18-24 : 2%**
 - **25-34 : 15%**
 - **35-44 : 28%**
 - **45-54 : 29%**
 - **55-64 : 17%**
 - **65+ : 8%**

²³ Wordstream. (2019). Facebook ad benchmarks for your industry. Disponible sur : <https://www.wordstream.com/blog/ws/2019/11/12/facebook-ad-benchmarks>

²⁴ 12,7% des visiteurs de dibartolo.fr ont donc acheté la machine à café. Le taux de conversion moyen est de 9,21%, tous secteurs confondus. Source: Wordstream - <https://www.wordstream.com/blog/ws/2019/11/12/facebook-ad-benchmarks>

Néanmoins, ce public est en moyenne plus âgé et plus masculin, ce qui correspond à la moyenne des utilisateurs de Facebook, même si ce biais est légèrement plus marqué dans notre échantillon que la moyenne des utilisateurs de Facebook.²⁵ Ceci est une conséquence du choix de la machine à café et du ciblage automatique effectué par l'algorithme de Facebook. En effet, nous avons ciblé nos publicités aux utilisateurs de Facebook âgés de plus de 18 ans et résidant en France. Nous avons ensuite laissé l'algorithme publicitaire de Facebook déterminer quels utilisateurs devaient voir l'une de nos publicités, ce qui explique certains déséquilibres entre sexe et catégorie d'âge. Le fait de choisir un autre produit ou service permettrait donc d'atteindre une audience différente. Cependant, celle-ci correspondra toujours à une population vulnérable à l'offre en question.²⁶

Les consommateurs semblent avoir interagi avec le message « prise de conscience »

Sur les 2 542 participants, 847 ont été attribués au groupe « prise de conscience ». Ces consommateurs ont passé en moyenne 50 secondes devant le message d'alerte.

Bien que nous ne puissions pas voir combien de temps chaque utilisateur a passé sur cette page, une durée moyenne de 50 secondes suggère que beaucoup ont pris le temps de lire le message, qui comptait 106 mots.

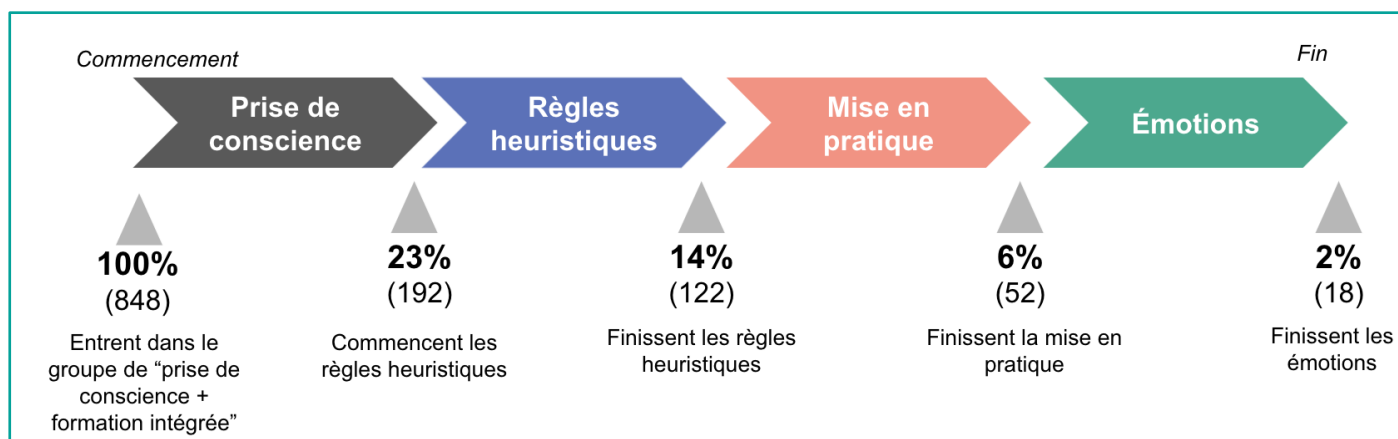
L'interaction avec la formation était quant à elle moins concluante

848 participants ont quant à eux été attribués au groupe « prise de conscience + formation intégrée ». Après avoir vu le message « prise de conscience » :

- **23%** (192 personnes) de ces participants ont **commencé** l'exercice « **règles heuristiques** »
- **14%** (122 personnes) ont **fini** l'exercice « **règles heuristiques** »
- **6%** (52 personnes) ont **fini** les exercices « **règles heuristiques** » et « **mise en pratique** »
- **2%** (18 personnes) ont **fini** les exercices « **règles heuristiques** », « **mise en pratique** » et « **émotions** »

²⁵ Digimind (2021). Facebook les chiffres essentiels en 2021 en France et dans le Monde. Disponible sur : <https://blog.digimind.com/fr/agences/facebook-chiffres-essentiels>

²⁶ Lors de nos tests de conversion, nous avons observé que le fait de manipuler le produit offert modifie le type de public que l'annonce atteint. En effet, l'algorithme de Facebook cible des individus qui ont un profil qui leur rend plus susceptible d'acheter le produit proposé. Cela signifie par exemple que pour certains produits, les hommes étaient plus susceptibles de voir la publicité que les femmes et vice-versa.

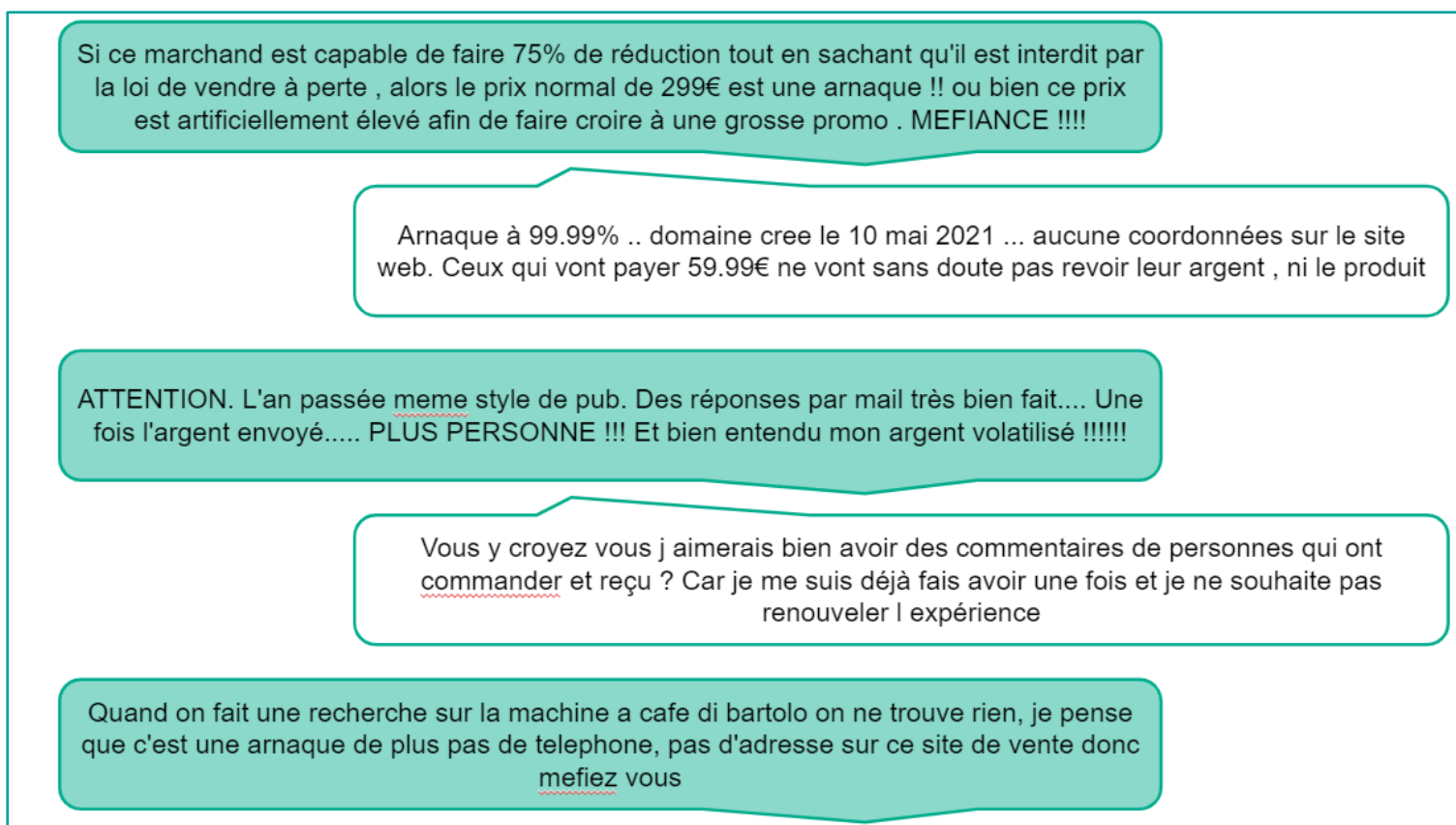


Dans la section « *perspectives d'avenir* », nous discutons de pistes potentielles pour accroître l'engagement avec cet élément de l'intervention (page 37).

L'annonce a suscité un grand nombre de commentaires sur Facebook et de courriels, qui oscillaient entre la suspicion et la curiosité

Un grand nombre de commentaires ont été laissés par des consommateurs sur la page Facebook de notre fausse offre (plus de 220 ont été enregistrés). La grande majorité de ces commentaires semble avoir eu pour but d'informer d'autres consommateurs d'une potentielle fraude. Les caractéristiques de l'offre et du site internet (prix cassé, potentiel abonnement caché, manque de mentions légales, de coordonnées de contact, etc.) étaient soulignées par les consommateurs comme des signes d'une potentielle fraude. De plus, certains consommateurs ont mentionné s'être fait arnaquer dans le passé par des offres similaires, ce qui suggère qu'ils ont fait appel à leur expérience personnelle pour se faire cette opinion. Enfin, certains consommateurs disaient aussi avoir effectué des vérifications additionnelles, qui avaient confirmé leur suspicion : certains avaient cherché des avis de clients sur internet, d'autres avaient entrepris des recherches sur l'entreprise sur internet, et certains s'étaient même rendu compte de la supercherie.

Figure 9 : Exemple de commentaire reçu sur la page Facebook de l'offre



Le formulaire de contact sur le site internet de nos offres a lui aussi été rempli un grand nombre de fois (plus de 175), mais le type de commentaire laissé par les consommateurs qui pensaient contacter le vendeur directement (à travers notre formulaire de contact) diffère de celui observé sur la page Facebook. En effet, certains des courriels comprenaient des questions *habituelles* de service après-vente (sur les délais de livraison, ou les modalités de paiement par exemple, voir image ci-dessous), venant de consommateurs qui ne paraissaient pas être suspicieux envers l'offre proposée.

Message : Bonjour j'ai commandé une machine le 12/06/2021 et je n'ai toujours pas reçu pourriez-vous me recontacter aux [redacted] en vous remerciant

Message : Bonjour merci de me contacter car je suis intéressé par votre produit mais par contre je préfère payer en espèces à réception du colis est-ce que cette démarche est-il possible car j'ai déjà commandé sur Internet et j'ai du changer ma carte à deux reprises donc je ne voudrais pas commander avec ma carte bleue mais payer en espèces une fois que le colis sera arrivé à mon adresse est-ce que c'est possible ! [redacted]

Figure 10 : Exemple de courriels reçus qui ne dénotent pas de suspicions

D'autres consommateurs ont utilisé le formulaire de contact pour partager leurs suspicions sur cette offre, mais paraissaient moins efficaces dans leurs comportements de vérification de ces suspicions : par exemple, ils demandaient

directement au vendeur de les rassurer plutôt que d'effectuer des vérifications plus poussées eux-mêmes (voir image ci-dessous).

Figure 11 : Exemple de courriel reçu qui souligne des suspicions

Message : Bonjour, j'ai commandé une machine mais j'ai commencé à regarder sur internet et aucun site ne parle de cette marque ou de cette machine... C'est pas rassurant et j'ai peur de l'arnaque.
Pouvez vous me rassurer svp ?

5.3. Ce type d'intervention est-il perçu comme étant acceptable ?

Principales conclusions : Une grande majorité des participants ont considéré que l'approche était appropriée, et plusieurs d'entre eux ont communiqué leur appréciation.

Les utilisateurs ont exprimé un haut degré de satisfaction à l'égard de l'intervention

A la fin de l'expérimentation, les participants ont tous été informés de l'étude et une enquête leur a été envoyée pour explorer, entre autres, l'acceptabilité de l'intervention.

Nous tenons à souligner que compte tenu de la petite taille de l'échantillon, les résultats présentés ci-dessous ne sont donnés qu'à titre indicatif.

Parmi les répondants à l'enquête, l'acceptabilité de cette intervention apparaît très élevée. Lorsque interrogés sur l'approche de l'intervention, plus de 9 sur 10 répondants ($n = 61$) ont considéré l'approche appropriée pour une campagne de sensibilisation. En outre, la popularité de l'approche était comparable entre les groupes d'intervention (93% et 94%) et le groupe de contrôle (90%).

De nombreux commentaires positifs ont enfin été laissés par les participants à l'étude en fin d'expérimentation, dont certains sont énumérés ci-dessous :

“Campagne très bien réalisée. Je voulais montrer à ma fille que parfois il y a de grosses arnaques sur le net et grâce à vous elle est + méfiante sur le net. Un grand merci à vous”

“Une très bonne initiative de votre part, cette action nous permet de nous sensibiliser sur les arnaques en ligne. Merci à vous.”

“Je trouve cette campagne de sensibilisation bien ayant déjà été victime de fraude sur internet...”

“Il faudrait que cette campagne soit reconduite plus souvent”

“Ravi de voir que la DGCCRF s'intéresse à ce type d'approche frauduleuse sur Facebook.”

Aucun courriel négatif n'a été reçu pendant ou après l'expérimentation concernant les actions de la DGCCRF (que ce soit sur les sites de vente en ligne ou par l'intermédiaire du mail de contact mis à disposition sur les pages de formation) et aucune critique médiatique (négative) n'a été générée à ce jour.

5.4. Ce type d'intervention fonctionne-t-il ?

Principales conclusions : L'intervention a montré un potentiel prometteur pour réduire la vulnérabilité des consommateurs face aux fraudes en ligne. Si cette tendance positive venait à être confirmée, les outils testés ici pourraient représenter une addition importante aux outils déjà employés par les instances de protection du consommateur.

Pour déterminer si notre intervention avait le potentiel de réduire la vulnérabilité des consommateurs face aux fraudes à l'achat en ligne, nous avons proposé une deuxième série de fausses offres aux participants à l'étude (voir page 22). Nous avons ensuite comparé le taux de « re-victimation »²⁷ entre les trois groupes tests.

Nous avons utilisé deux canaux de communication pour cibler les participants qui avaient « acheté » la machine à café, afin de maximiser la portée de nos publicités et

²⁷ Le taux de « re-victimation » correspond au taux d'achat des seconds produits par les personnes qui ont acheté le premier produit (la machine à café).

donc de minimiser le risque que nos résultats soient biaisés par le fait que les participants n'aient simplement pas vu la deuxième publicité :

- **Facebook** : les fonctionnalités de Facebook²⁸ nous ont permis de cibler à nouveau les utilisateurs qui avaient commandé une machine à café sur dibartolo.fr. avec nos publicités pour la deuxième série de fausses offres.
- **Email** : les consommateurs qui ont commandé sur dibartolo.fr ont été invités à fournir leur adresse électronique lors de la commande de leur machine à café. Nous avons envoyé un e-mail promotionnel à ces adresses concernant notre deuxième série de fausses offres.

Figure 12 : Exemple de courriel envoyé aux participants concernant la deuxième fausse offre



²⁸ Facebook. (2021). *The Facebook Pixel*. <https://www.facebook.com/business/learn/facebook-ads-pixel>

Cette stratégie s'est avérée relativement efficace. Comme indiqué ci-dessous, bien que le ciblage soit imparfait, la majorité des participants (n = 2 542) ont vu au moins une des secondes publicités et ont reçu un courriel promotionnel :

Reciblage - Facebook		
Nombre de personnes et pourcentage de l'échantillon ayant vu une de nos publicités	1 616	63,5%
Nombre de clics	238	9,3%

Reciblage - Courriel		
Nombre de personnes et pourcentage de l'échantillon ayant reçu un des courriels	2 059	81,0%
Parmi ceux l'ayant reçu, nombre de personnes et pourcentage de l'échantillon ayant ouvert un courriel	1 364	66%
Parmi ceux l'ayant ouvert, nombre de personnes et pourcentage de l'échantillon ayant cliqué sur le lien de redirection vers le site de vente en ligne	61	2,3%

Les facteurs suivants sont susceptibles d'avoir limité le ciblage de participants : la non-connexion de participants à Facebook, les rebonds de courriels lorsque les participants ont mal saisi leur adresse mail, l'utilisation d'adresses mails secondaires, des restrictions sur la capacité de Facebook Pixel de re-cibler les utilisateurs de l'iOS 14 d'Apple, la concurrence d'autres acteurs pour les espaces publicitaires.

Nous avons observé un niveau d'interaction élevé avec la deuxième série de publicités sur Facebook et le courriel promotionnel. Le taux de clics de 9,3 % sur nos publicités Facebook est supérieur à la moyenne globale de 0,9 %, ²⁹ et le taux de clics de 2,3 % sur les courriels a été conforme à la moyenne globale de 2,6 % et a dépassé la moyenne de 1,1 % pour le secteur du commerce. ³⁰

Ce niveau élevé d'interaction avec une série de publicités et de courriels non sollicités suggère qu'une proportion non négligeable de victimes de fraudes à l'achat risque

²⁹ Wordstream. (2019). *Facebook ad benchmarks for your industry*
<https://www.wordstream.com/blog/ws/2019/11/12/facebook-ad-benchmarks>

³⁰ Campaign Monitor. (2021). *Ultimate Email Marketing Benchmarks for 2021: By Industry and Day*.
<https://www.campaignmonitor.com/resources/guides/email-marketing-benchmarks/>

d'être de nouveau exposée à l'avenir, et renforce l'idée que cette intervention touche directement un public particulièrement vulnérable. Si un taux de clics élevé ne se traduit pas toujours par des achats et peut s'expliquer en partie par le faible prix des produits proposés, il n'en reste pas moins qu'une proportion importante de participants (dont beaucoup avaient récemment été informés qu'ils avaient été escroqués) ont cliqué sur des publicités provenant d'une entreprise avec laquelle ils n'avaient aucun lien préalable et dont la page Facebook ne comptait aucun contenu historique.³¹

Nous avons observé un taux de re-victimation conforme à nos attentes

29 consommateurs (représentant 1,1% de l'échantillon) ayant acheté la machine à café ont acheté la platine vinyle, la TV ou l'enceinte Bluetooth et ont donc été victimes d'une deuxième fausse offre moins d'un mois après la première fausse offre.

Même s'il est difficile de trouver des références avec lesquelles comparer ce taux vu la spécificité de la seconde offre et la définition unique à ce projet du taux de re-victimation, ce taux nous semblait raisonnable, d'autant plus que :

- il n'y avait pas de moyen de connaître a priori les préférences de produits des consommateurs qui ont acheté une machine à café ³² ;
- le reciblage des participants était imparfait ;
- les consommateurs ont été contactés par une entreprise avec laquelle ils n'avaient jamais été associés et qui n'avait aucun profil historique sur les réseaux sociaux ou sur internet (Di Bartolo ayant été créé spécifiquement pour ce projet).

Tout comme le taux de clics élevé sur les publicités de la deuxième série de fausses offres, ce taux de re-victimation suggère qu'il pourrait exister un groupe de consommateurs particulièrement à risque, susceptibles d'être à nouveau victimes d'escroqueries de la même nature

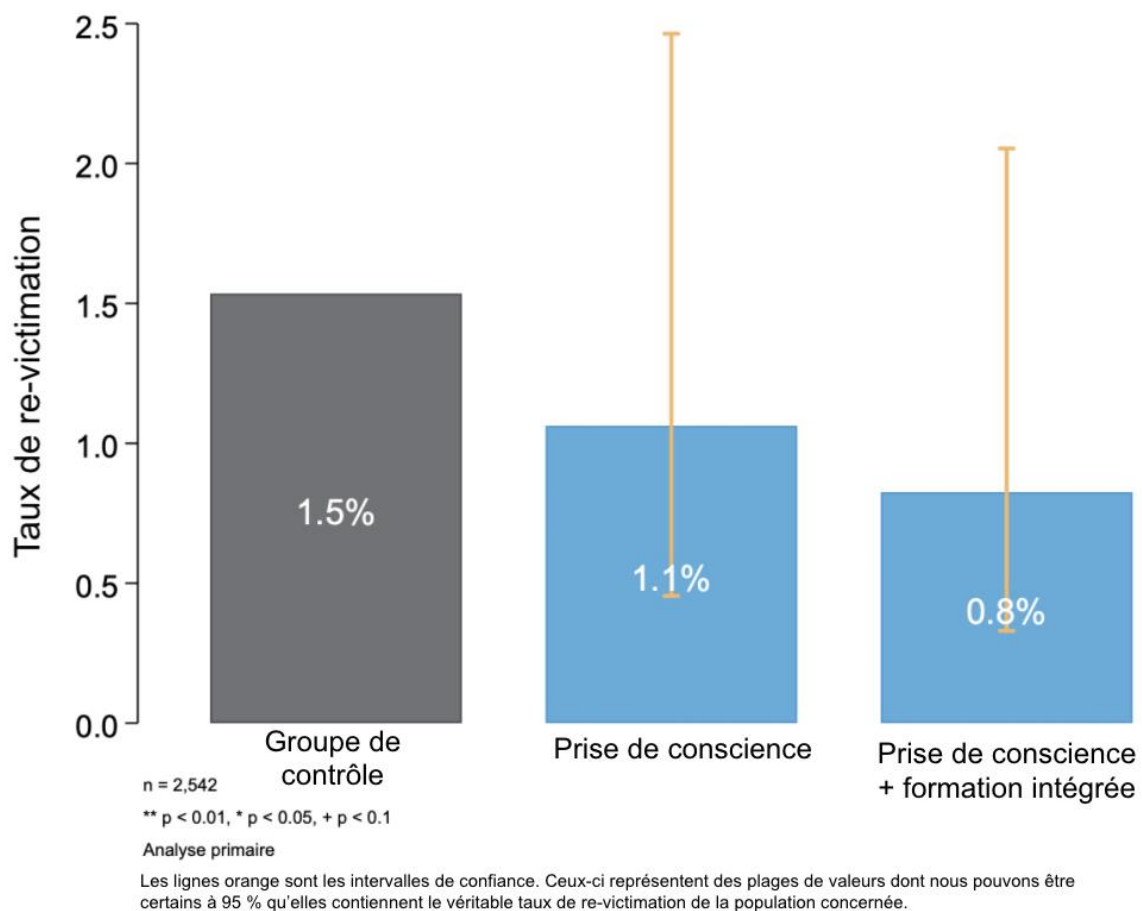
Même si les résultats ne sont pas statistiquement significatifs, l'intervention a montré un potentiel pour réduire la vulnérabilité aux fraudes, et mérite d'être testée davantage

³¹ Tech Bazar x Harrison Technologie - <https://www.facebook.com/Tech-Bazar-x-Harrison-Technologie-101608578853667>

³² Pour contrer cela, nous avons fait la promotion de trois produits différents, qui ont tous obtenu de bons résultats lors des tests de conversion.

Comparer les taux de re-victimation entre les trois groupes tests permet d'observer une tendance positive qui suggère que ce mécanisme à un potentiel d'impact fort qui mérite d'être testé à nouveau et approfondi.

Figure 13 : Taux de « re-victimation » par groupe d'intervention



Malgré cette tendance positive, les résultats ne sont pas statistiquement significatifs, potentiellement à cause de la petite taille de notre échantillon qui ne nous permet de détecter que des effets statistiquement significatifs supérieurs à 1,6 point de pourcentage. Nous ne pouvons pas conclure (avec un niveau de confiance de 95 %) que l'exposition à une "prise de conscience" et à une "formation intégrée" réduit la susceptibilité aux fraudes à l'achat.

Néanmoins, cette tendance positive aurait potentiellement pu être confirmée avec un échantillon plus large.

Le message de « *prise de conscience* » a permis une diminution de 0,4 point de pourcentage du taux de re-victimation, soit une réduction de 27% en termes relatifs, comparé à ne rien recevoir (groupe de contrôle).

La combinaison du message de « *prise de conscience* » et de formation intégrée (groupe 2) a, quant à elle, permis une diminution du taux de re-victimation encore plus notable : 0,7 point de pourcentage, soit une diminution de 47% en termes relatifs, comparé au groupe contrôle.

Bien qu'un résultat statistiquement significatif n'ait pas été obtenu, ces résultats encouragent à approfondir l'expérience et suggèrent que les solutions proposées pourraient réduire la vulnérabilité des consommateurs aux offres frauduleuses.

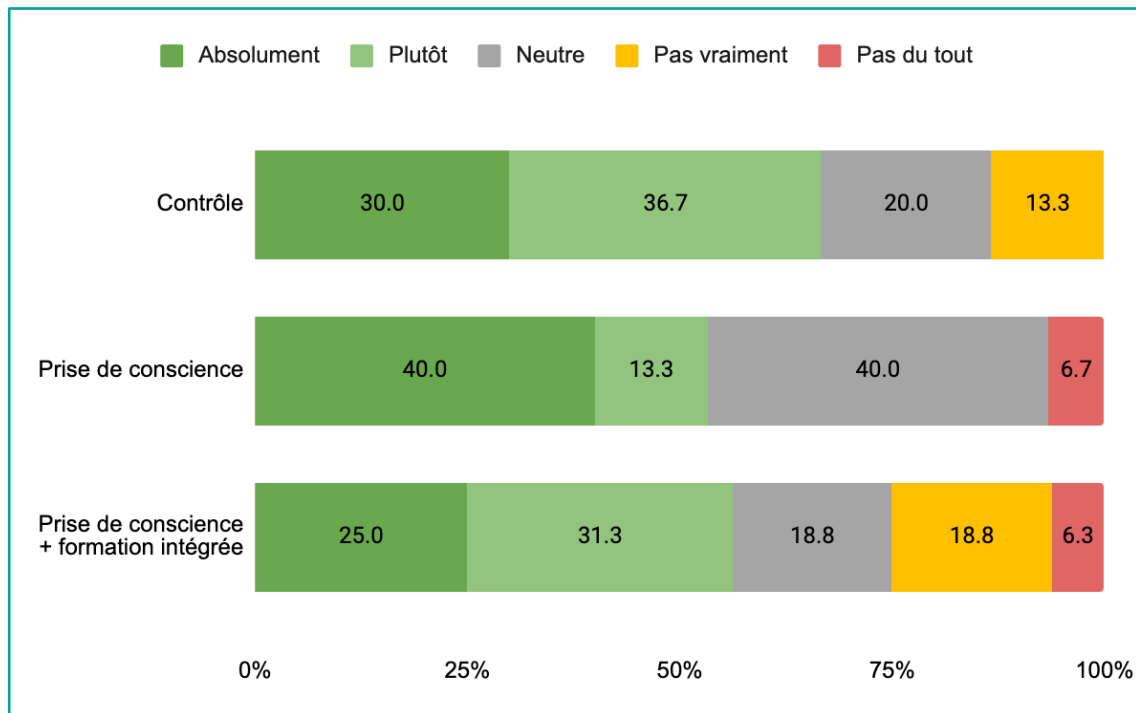
Si cette réduction du taux de re-victimation peut être confirmée à l'avenir, cette intervention pourrait avoir le potentiel de réduire de manière significative la vulnérabilité aux fraudes en ligne, ainsi que les dommages financiers subis par les consommateurs. Par exemple, dans le cas de l'offre de la machine à café, une réduction de 27% du taux de victimation aurait pu éviter à près de 700 consommateurs de se faire avoir, et 37 500€ de revenus en moins pour le fraudeur.

La prise de conscience semble réduire la confiance des consommateurs dans leur capacité à se protéger, mais suivre la formation intégrée semble l'augmenter.

Dans l'enquête envoyée en fin d'expérimentation, nous avons demandé aux participants s'ils pensaient savoir comment se protéger lors d'achats en ligne. Nous présentons les résultats descriptifs ci-dessous sur le petit échantillon de 61 individus qui ont répondu à cette enquête. Vu la taille modeste de cet échantillon, les résultats présentés ci-dessous ne sont donnés qu'à titre indicatif.

Parmi les répondants, nous observons que ceux faisant partie des groupes d'intervention semblent être moins sûrs de leur capacité à se protéger que ceux du groupe contrôle (voir figure 14 et annexe 2). Ce résultat pourrait sembler paradoxal de prime abord, la sensibilisation et la formation surtout visant justement à apporter des clefs de réponse aux consommateurs. Toutefois, elle pourrait en fait être considérée comme encourageante, en ayant constitué des déclics et une véritable prise de conscience chez les consommateurs. Plus précisément, le mécanisme de « prise de conscience » visait, en partie, à lutter contre un excès de confiance et une sous-estimation de risque que nous avons identifiés chez certains consommateurs lors de notre phase de diagnostic, tandis que la formation visait à doter les consommateurs de connaissances susceptibles de les aider à se protéger en ligne. Au vu des résultats mis en évidence à la figure 14, il semble bien que ces deux objectifs soient atteints, même s'ils mériteraient confirmation avec un échantillon de plus grande taille, permettant d'en tirer des conclusions statistiquement plus robustes.

Figure 14 : Confiance des individus à se protéger contre les fraudes en ligne, par groupe d'intervention (N=61)



L'intervention menée ne semble pas influencer sur le nombre de règles connues, mais connaître des règles heuristiques semble aider les consommateurs à mieux se protéger

Nous avons également demandé, dans le questionnaire final, aux participants d'identifier les bons « réflexes d'achat » parmi une longue liste. Nous étudions ici le nombre de « bonnes » règles identifiées par les participants.

En moyenne, les participants sont parvenus à identifier en moyenne 3 règles heuristiques, sur les 5 habituellement listées.³³ Ce chiffre est cependant identique dans les trois groupes d'expérimentation (voir détails au tableau en annexe 3), suggérant que parmi les participants à l'enquête, les interventions n'ont pas affecté le nombre de règles connues. Il convient néanmoins de souligner que les participants à l'enquête ne sont probablement pas représentatifs de la population dans son ensemble - nous ne pouvons donc pas conclure avec certitude que l'intervention n'a aucun effet sur les connaissances.

Enfin, nous comparons les personnes ayant été re-victimées ou non. Sans grande surprise, ceux qui ont été re-victimés étaient aussi ceux qui connaissaient le moins de règles heuristiques (2,25, vs 3,07). Cela suggère que malgré l'effet limité des exercices

³³ Les règles qui ont été le plus identifiées sont les suivantes : « je sécurise mon paiement » (85%), « je ne me fie pas aux apparences » (70%) et « je me demande si c'est trop beau pour être vrai » (60%)

tels qu'ils ont été testés ici, il peut être utile de continuer à explorer des modes de formation autour de bons réflexes d'achat.

Zoom : règles heuristiques (« réflexes d'achat ») élaborés par les experts de la DGCCRF, la DITP et le BIT



Je prends une minute pour réfléchir – « Certains sites de vente en ligne utilisent des stratégies pour accélérer l'achat, comme des comptes à rebours, des mentions de stocks limités ou des appels à l'action immédiats. Ces stratégies visent à nous rendre impulsifs, mais ne sont pas toujours illégales. Au mieux, c'est pour encourager les ventes ; au pire, pour dissimuler une arnaque. Prenez le temps de la réflexion pour être sûr(e) que votre achat n'est pas juste une décision impulsive.



Je ne me fie pas aux apparences – « Un site ayant un historique de ventes aura habituellement des avis de consommateurs. Si possible, pensez à vérifier au moins 2 sources d'avis ou de commentaires différentes, pour avoir accès à un plus grand nombre d'avis de consommateurs. Les faux avis sont communs sur internet, c'est pourquoi une recherche ciblée sur les "arnaques" peut mieux porter ses fruits ! Si votre recherche ne retourne pas d'avis, ou retourne des mentions d'arnaques, fraudes, ou des mauvaises expériences, soyez vigilant(e) »



Je me demande si c'est trop beau pour être vrai – « Si l'article ou service est proposé à un prix beaucoup plus bas que sur les autres sites, vérifiez bien que les caractéristiques sont bien les mêmes : parfois, un prix anormalement bas peut servir à cacher d'autres problèmes. Pensez par exemple à vérifier :

- que le vendeur n'utilise pas de faux gages de qualité (tel que le terme artisan, des logos d'organismes publics, ou un faux label),
- les délais de livraison ou d'intervention,
- si le produit est vendu neuf ou d'occasion,
- que votre achat n'inclut pas une souscription à un abonnement caché, pour éviter des frais additionnels.



Je vérifie que le vendeur ne se cache pas – « Un site de vente en ligne fiable devrait vous donner un moyen de le contacter en cas de besoin, pour toutes remarques ou demande : cherchez dans le site si ces informations vous sont données, par exemple dans un onglet

“mentions légales” ou dans les conditions générales de vente. Privilégiez les sites ayant une adresse physique en France ou dans l'Union Européenne sinon les recours seront quasiment impossibles. Attention : un formulaire de contact ou une adresse email peuvent ne pas être suffisants !



Je sécurise mon paiement - Une barre d'adresse du site qui contient un cadenas et / ou qui commence par https veut dire que vos coordonnées bancaires sont protégées. Privilégiez le paiement par carte bancaire, plutôt que le virement, car un virement est irrévocable. Et même si la page vous paraît sécurisée, pensez bien à faire les autres vérifications recommandées !

6. Suites possibles

Le développement du e-commerce entraîne une augmentation quotidienne du nombre de fraudes ainsi qu'un affinement de techniques d'escroquerie. Néanmoins, les résultats de ce rapport sont encourageants. **Une fausse offre dans un environnement sécurisé, suivie d'un message de prise de conscience et d'exercices : peut mobiliser un grand nombre de consommateurs ; a été perçue comme acceptable et utile par les répondants à notre enquête de fin d'expérimentation ; et pourrait potentiellement réduire la vulnérabilité des consommateurs aux fraudes en ligne.**

Ce mécanisme a donc un potentiel d'impact qui mériterait d'être testé et approfondi à nouveau. Dans cette optique, la DITP et le BIT explorent avec la DGCCRF comment et si cette intervention peut être appliquée à d'autres situations et testée à nouveau.

La DITP et le BIT présentent ci-après des pistes de réflexions et de recommandations à considérer si cette initiative devait être relancée, avant d'offrir une perspective plus large sur l'application de la science comportementale à la protection des consommateurs. Ces propositions sont non engageantes pour la DGCCRF, sous réserve d'un approfondissement ultérieur de ces pistes.

Dans un premier temps, lancer une version « allégée » de l'intervention qui utilise uniquement le mécanisme de prise de conscience

Des discussions sont en cours concernant la reproduction de cette intervention.

Au vu de l'engagement que nous avons observé avec la formation telle qu'elle a été développée aujourd'hui, la DITP et le BIT recommandent dans un premier temps de répliquer uniquement le mécanisme de « prise de conscience » en excluant la « formation intégrée ».

Envisager de retravailler la formation intégrée à un stade ultérieur

Bien que l'interaction des consommateurs avec la formation intégrée ait été modeste dans cette expérimentation, la DITP et le BIT considèrent que (a) le niveau d'engagement pourrait être accru en apportant certaines modifications à son design et (b) qu'une formation de ce type a un potentiel de réduire la vulnérabilité des consommateurs aux escroqueries en ligne.

Pour accroître l'interaction avec la formation, il serait possible de :

- **Ajuster le texte que les consommateurs voient sur le page d'accueil pour mitiger l'effet de choc / la confusion ressenti** - Parmi les 848 utilisateurs attribués au groupe « prise de conscience + formation intégrée », 320 (38%) ont immédiatement quitté la page d'accueil après avoir été informés qu'ils allaient être escroqués. Bien qu'il faille s'attendre à un certain degré d'attrition lié au

choc, il est possible que la proportion d'utilisateurs qui quittent immédiatement la page puisse être réduite en utilisant un ton moins alarmiste ou plus humoristique. Les commentaires laissés sur les annonces Facebook suggèrent que certains utilisateurs ont mal interprété le message « prise de conscience », croyant que l'offre était en fait réelle plutôt qu'une simulation, et que la DGCCRF avait interdit le site web en conséquence. Simplifier et adoucir le texte pourrait réduire ces erreurs d'interprétation et de ce fait, augmenter l'interaction avec la formation.

- **Rendre la formation plus attrayante visuellement**, par exemple en réduisant considérablement la quantité de texte, en utilisant un design plus vif et en incluant des images et des illustrations de meilleure qualité.
- **Réduire la quantité de contenu** - notre formation comprenait trois modules différents. Si un nombre raisonnable de consommateurs ont commencé le premier module, très peu ont terminé la formation dans son intégralité. Nous recommandons que toute version future de la formation ne comprenne qu'un seul module - la « mise en pratique » - et que les efforts soient concentrés sur la création d'une expérience d'apprentissage qui soit aussi pratique, appliquée et engageante que possible, sans dépasser cinq minutes en durée.

Bien que les résultats de l'expérimentation manquent de robustesse sur ce point, la DITP et le BIT considèrent que la « formation intégrée » représente une méthode prometteuse pour réduire la vulnérabilité des consommateurs aux pratiques frauduleuses. Le [Google phishing quiz](#) fournit un exemple de formation courte et engageante. Il s'agit d'un quiz qui présente aux utilisateurs 8 courriels différents et leur demande d'identifier s'ils sont légitimes ou non. Le quiz utilise plusieurs des principes que notre formation intégrée cherchait à mobiliser : par exemple, les participants reçoivent un retour immédiat sur leurs réponses, et se voient proposer des réflexes à appliquer (par ex : « *en passant la souris sur ce lien... vous verrez qu'il ouvre le domaine non sécurisé « drive--google--.com », qui n'appartient pas à Google* »).

Chaque mois, environ 100 000 utilisateurs accèdent à ce quiz³⁴, et une étude à petite échelle a indiqué qu'il pouvait améliorer la capacité des utilisateurs à repérer les tentatives de phishing.³⁵ En outre, une « formation intégrée » que nous avons mise en place en partenariat avec la police de Londres a réduit de 21 % la probabilité qu'un policier partage ses informations de connexion en réponse à un e-mail de phishing.³⁶

³⁴ <https://www.similarweb.com/website/phishingquiz.withgoogle.com/>

³⁵ Weaver BW, Braly AM, Lane DM. Training Users to Identify Phishing Emails. Journal of Educational Computing Research. February 2021. doi:10.1177/0735633121992516

³⁶ BIT. (2020). *Strengthening the Metropolitan Police against cyber attacks*. <https://www.bi.team/case-studies/strengthening-the-metropolitan-police-against-cyber-attacks>

Utiliser une version revisitée des réflexes d'achat dans des campagnes de sensibilisation qui ciblent les consommateurs avertis

L'analyse des commentaires des consommateurs, ainsi que celle des résultats au questionnaire de fin d'expérimentation, ont montré que les consommateurs semblent avoir déjà intégré certains des réflexes d'achat. Plus de 85% des consommateurs ayant rempli le questionnaire savaient qu'il est important de vérifier que la page de paiement est sécurisée ; et environ 70% vérifiaient les avis d'autres consommateurs. De plus, les commentaires laissés par les consommateurs sur les publicités DiBartolo suggèrent que ces consommateurs étaient prêts à effectuer, ou avaient effectué des vérifications rapides pour s'assurer du bien-fondé (ou non) de l'offre.

Au vu de ces résultats, il pourrait être utile de revoir les réflexes d'achat afin de prioriser ceux qui ne sont pas encore acquis par les consommateurs, et de continuer à les communiquer aux consommateurs lors de campagnes de sensibilisation.

Identifier d'autres occasions d'appliquer les méthodes des sciences comportementales à la protection des consommateurs

La conclusion la plus importante de ces travaux est qu'ils démontrent les apports potentiels des sciences comportementales et des méthodes expérimentales pour innover dans le domaine de la protection des consommateurs.

Grâce à un diagnostic rigoureux des risques posés pour les consommateurs par certaines pratiques commerciales, l'approche comportementale permet en effet de développer des innovations ciblées, et de les pré-tester afin d'identifier les futurs éléments clés des politiques de protection des consommateurs.

A l'heure où la Commission européenne et la commission fédérale américaine du commerce (FTC) réfléchissent à leur position sur les « dark patterns » et leur éventuelle régulation, des études expérimentales de ce type peuvent ainsi fournir des compléments importants aux études de juristes ou économistes, plaçant le consommateur, sa cognition, ses limitations et ses préférences au centre de la réflexion.

Bien que le recours à l'approche comportementale reste pour l'instant limité, la tendance est pourtant à un recours croissant à ces méthodes. Étant donnée la nature profondément comportementale du processus décisionnel d'achat, la DITP et le BIT s'attendent à ce que cette tendance se poursuive et s'accélère dans les années à venir, offrant de nouvelles perspectives importantes dans le domaine de la protection du consommateur.

L'équipe projet

Nous tenons enfin à remercier les équipes de la DGCCRF ayant collaboré avec nous tout au long de ce projet et ayant permis sa mise en place et son succès.

DGCCRF : Philippe d'Authier de Sisgau, Agnès Mayanobe, Cédric Pelletier, Charlotte Ferreyros, Florian N'Guyen, Hélène Merrien, Jérémy Ferrain, Marianne Lefort, Sylvie Becam, Guillaume Defillon, Marie-Astrid Philippart

DITP : El Ghali Lamrani Alaoui, Mariam Chammat, Stéphan Giraud

BIT : Anysia Nguyen, Laura Litvine, Tom McMinigal, Violette Gadenne

Annexe méthodologique

Tableau annexe 1 : Taux d'acceptabilité de notre approche selon le groupe d'expérimentation, le nombre d'exercices et le statut de re-victimation

Acceptabilité : « Je trouve que cette approche est appropriée pour une campagne de sensibilisation »*

Échantillon	Catégorie	Tout à fait (%)	Plutôt (%)	Neutre (%)	Pas vraiment (%)	Pas du tout (%)
Tous les participants ayant répondu au questionnaire	Contrôle (30)	60.00	30.00	3.33	3.33	3.33
	Prise de conscience (15)	73.33	20.00	0.00	6.67	0.00
	Prise de conscience + formation intégrée (16)	75.00	18.75	0.00	0.00	6.25
Tous les participants du groupe « prise de conscience + formation intégrée » ayant répondu au questionnaire *	Aucun exercice (12)	66.67	25.00	0.00	0.00	8.33
	Au moins un exercice (4)	100.00	0.00	0.00	0.00	0.00
Tous les participants ayant répondu au questionnaire	Pas re-victimé (57)	64.91	26.32	1.75	3.51	3.51
	Re-victimé (4)	100.00	0.00	0.00	0.00	0.00

*Nous avons réalisé des tables de fréquences pour montrer la répartition des avis sur l'acceptabilité de l'approche selon plusieurs critères : le groupe d'expérimentation, le nombre d'exercices complétés, et le statut de re-victimation. Les échantillons ne nous permettent pas de faire des tests de significativité et aucune des différences ne sont à interpréter comme causales.

**Seulement 16 personnes sur les 61 qui ont répondu à notre questionnaire de fin d'expérimentation sont dans le groupe « prise de conscience + formation intégrée » et ont donc eu la possibilité de faire les exercices. Seulement ceux-là sont donc inclus dans les catégories : aucun exercice, au moins un exercice

Tableau annexe 2 : Taux de confiance en la capacité de se protéger contre les fraudes en ligne selon le groupe d'expérimentation, le nombre d'exercices et le statut de re-victimation

Impact perçu : « Je sais comment me protéger contre les fraudes lorsque j'effectue des achats en ligne »*

Échantillon	Catégorie	Tout à fait (%)	Plutôt (%)	Neutre (%)	Pas vraiment (%)	Pas du tout (%)
Tous les participants ayant répondu au questionnaire	Contrôle (30)	30.00	36.67	20.00	13.33	0.00
	Prise de conscience (15)	40.00	13.33	40.00	0.00	6.67
	Prise de conscience + formation intégrée (16)	25.00	31.25	18.75	18.75	6.25
Tous les participants du groupe « prise de conscience + formation intégrée » ayant répondu au questionnaire**	Aucun exercice (12)*	16.67	33.33	16.67	25.00	8.33
	Au moins un exercice (4)	50.00	25.00	25.00	0.00	0.00
Tous les participants ayant répondu au questionnaire	Pas re-victimé (57)	29.82	29.82	24.56	12.28	3.51
	Re-victimé (4)	50.00	25.00	25.00	0.00	0.00

*Nous avons réalisé des tables de fréquences pour montrer la répartition de la confiance qu'ont les individus en leur capacité de se protéger selon plusieurs critères : le groupe d'expérimentation, le nombre d'exercices complétés, et le statut de re-victimation. Les échantillons ne nous permettent pas de faire des tests de significativité et aucune des différences ne sont à interpréter comme causales.

**Voir astérisque dans le tableau annexe 1

Tableau annexe 3 : Nombre de règles heuristiques (sur cinq) trouvées selon le groupe d'expérimentation, le nombre d'exercices et le statut de re-victimation

Échantillon	Catégorie	Nombre moyen de règles heuristiques trouvées
Tous les participants ayant répondu au questionnaire	Contrôle (30)	3.00
	Prise de conscience (15)	3.00
	Prise de conscience + formation intégrée (16)	3.06
Tous les participants du groupe « <i>prise de conscience + formation intégrée</i> » ayant répondu au questionnaire*	Aucun exercice (12)	3.00
	Au moins un exercice (4)	3.25
Tous les participants ayant répondu au questionnaire	Pas re-victimé (57)	3.07
	Re-victimé (4)	2.25

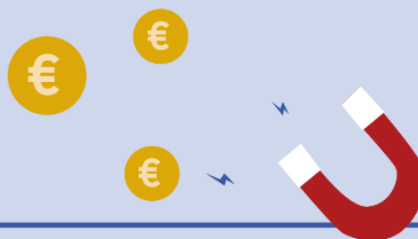
*Nous avons réalisé des tables de fréquences pour montrer le nombre de règles heuristiques trouvées selon plusieurs critères : le groupe d'expérimentation, le nombre d'exercices complétés, et le statut de re-victimation. Les échantillons ne nous permettent pas de faire des tests de significativité et aucune des différences ne sont à interpréter comme causales.

*Voir astérisque dans le tableau annexe 1



MINISTÈRE
DE LA TRANSFORMATION
ET DE LA FONCTION
PUBLIQUES

*Liberté
Égalité
Fraternité*



Ce rapport a été réalisé par les équipes de la
Direction interministérielle de la transformation publique
www.modernisation.gouv.fr

Décembre 2021