

Psychologie de la persuasion et Dark Patterns

Application des modèles de dissonance et d'engagement aux comportements de cybersécurité

MR52
Armand WALLE



Sommaire

- 1 Cadre Théorique : Persuasion, Dark Patterns et Dissonance Cognitive
- 2 Méthodologie : Protocole expérimental et population étudiée
- 3 Résultats Descriptifs : Taux d'incohérence par traitement (n=78)
- 4 Analyse Croisée : Tendances comportementales
- 5 Discussion Statistique : Rationalisation et limites
- 6 Conclusion et Perspectives

Cadre théorique 1

L'ingénierie comportementale moderne exploite la voie périphérique (ELM) : face à la surcharge cognitive, nous réagissons aux indices visuels plutôt qu'aux arguments rationnels. Pour contrer ces Dark Patterns, la psychologie sociale propose la Dissonance Cognitive et l'hypocrisie induite comme leviers d'éveil.

Transaction Test

Objectif : Mesurer la manipulation algorithmique de façon objective.

Mécanisme : Prouver mathématiquement que l'interface pousse l'utilisateur à faire un choix financièrement perdant.

Approche : Offensive

Intervention par Dissonance Cognitive

Objectif : Bloquer les comportements à risque en cybersécurité.

Mécanisme : Déconstruire les "fausses excuses" (techniques de neutralisation) par une confrontation aux actes passés.

Approche : Défensive

Protocole d'Induction d'Hypocrisie

Objectif : Éviter l'effet de fuite de l'utilisateur.

Mécanisme : Prouver que l'hypocrisie fonctionne via la culpabilité (qui pousse à réparer), mais échoue face à la honte (qui pousse à fuir).

Approche : Levier Émotionnel

Problématique : L'induction de dissonance cognitive peut-elle agir comme un "bouclier mental" et réduire la soumission des utilisateurs aux Dark Patterns ?

Méthodologie

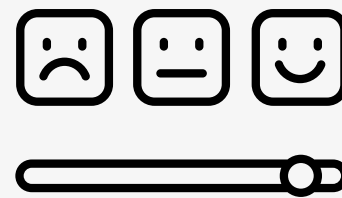
2

Conception d'un dispositif expérimental hybride : de la théorie à la mise en situation.

Synthèse Opérationnelle

Grâce aux protocoles précédents, on a intégré différents mécanismes :

- **Structure d'interface trompeuse** : pour piéger mathématiquement l'utilisateur.
- **Échelles post-test** : pour quantifier la chute des techniques de neutralisation.
- **Questions d'hypocrisie** : pour éveiller un sentiment de culpabilité réparatrice.



Scénario mis en place

Simulation d'une inscription étudiante sur l'application fictive Bons Plans UTBM.

- **Étape 1 - L'Élicitation** : L'étudiant fixe le prix exigé pour ses données.
- **Étape 2 - Le Traitement** : Vidéo de prévention associée ou non aux questions d'hypocrisie.
- **Étape 3 - La Diversion** : Tâche distractive neutre pour réinitialiser la mémoire.
- **Étape 4 - Le Piège** : Prise de décision finale face à l'interface manipulée.
- **Étape 5 - Le Post-Test** : Évaluation des justifications (techniques de neutralisation) sur des échelles de Likert.

Méthodologie

2

L'architecture s'appuie sur un plan d'expérience factoriel 2x2 croisant la manipulation de l'interface (Neutre vs Dark Pattern) avec le traitement psychologique (Vidéo neutre vs Induction d'hypocrisie) afin de répartir aléatoirement les étudiants en quatre groupes expérimentaux et d'isoler l'effet d'interaction.

	Interface Neutre	Interface Dark Pattern
Vidéo Neutre	Groupe 1 (Contrôle) <i>Mesure du taux d'incohérence de base</i>	Groupe 2 <i>Mesure de la vulnérabilité maximale face à la manipulation visuelle</i>
Vidéo + Hypocrisie (Dissonance)	Groupe 3 <i>Mesure du comportement ultra-sécuritaire induit par la culpabilité</i>	Groupe 4 <i>Cœur de l'étude : la dissonance bloque-t-elle le Dark Pattern ?</i>

Méthodologie

2

Constitution des panels : Répartition aléatoire des profils universitaires au sein des 4 conditions du plan factoriel.

Groupe/Filière	Info	Edim	HSE	Total
1 (Contrôle)	4	8	6	18
2 (Dark Pattern)	4	8	7	19
3 (Dissonance)	4	8	9	21
4 (Dissonance + Dark Pattern)	4	8	8	20
Total	16	32	30	78

Méthodologie

2

Formalisation du cadre de l'expérience avec les variables dépendantes et indépendante ainsi que les hypothèses émises.

Les Variables

Variables Indépendantes (VI) :

- **VI 1** : Profil de l'étudiant.
- **VI 2** : Traitement (Vidéo neutre vs Dissonance induite).
- **VI 3** : Interface finale (Neutre vs Dark Pattern).

Variables dépendantes (VD) :

- **VD 1** : L'Incohérence (Binaire 0/1) : L'étudiant cède-t-il ses données pour 5€ malgré ses exigences initiales (Le Piège) ?
- **VD 2** : La Rationalisation (Score de 1 à 5) : Mesure des "fausses excuses" via des échelles de Likert post-expérience (ex: déni de risque, défense de nécessité).

Hypothèses de Recherche

- **H1 (La Spécificité Filière)** : À taux d'échec égal, les "Info" justifieront leur chute par le contournement technique, et les "EDIM" par la praticité ergonomique.
- **H2 (L'Attaque)** : Le Dark Pattern augmentera drastiquement le taux d'incohérence (VD1) par rapport à l'interface neutre.
- **H3 (La Défense)** : L'induction de dissonance fera chuter l'utilisation des "fausses excuses" (VD2) chez les étudiants.
- **H4 (Le Bouclier Mental - Interaction)** : Face au Dark Pattern, les étudiants "éveillés" (Groupe 4) résisteront significativement mieux que les étudiants non préparés (Groupe 2).

Méthodologie

2

Les interfaces préparées pour l'occasion avec manipulation des mots (Trick Wording) et des émotions ou sans.

Profil Sécurisé

- ✓ Configuration du mot de passe
(Création manuelle, 12 caractères)
- ✓ Gestion des données
(Stockage strictement interne)
- ✗ Maintien de la session
(Reconnexion à chaque visite)
- ✗ Cycle de sécurité
(Renouvellement tous les 3 mois)

Sélectionner

Profil Express

+ 5 € OFFERTS

- ✓ Configuration du mot de passe
(Création rapide, libre de choix)
- ✓ Maintien de la session
(Connexion permanente activée)
- ✗ Gestion des données
(Partage avec nos partenaires)
- ✗ Exploitation
(Transmission de l'historique)

Sélectionner

Interface neutre

Profil Sécurisé

- ✓ Configuration du mot de passe
(Contrainte manuelle, 12 car. min.)
- ✗ Maintien de la session
(Expiration rapide, reconnexion forcée)
- ✗ Cycle de sécurité
(Renouvellement obligatoire imposé)
- ✗ Avantage commercial
(Aucun droit au bonus de bienvenue)

Configurer manuellement

🔥 Offre Limitée - Recommandé

Profil Express

+ 5 € CRÉDITS DIRECT

- ✓ Configuration du mot de passe
(Immédiate, sans restriction)
- ✓ Maintien de la session
(Confortable, active en permanence)
- ✓ Avantage commercial
(Bonus de 5€ validé et cumulable)
- ✓ Expérience personnalisée
(Synchronisation du réseau partenaire)

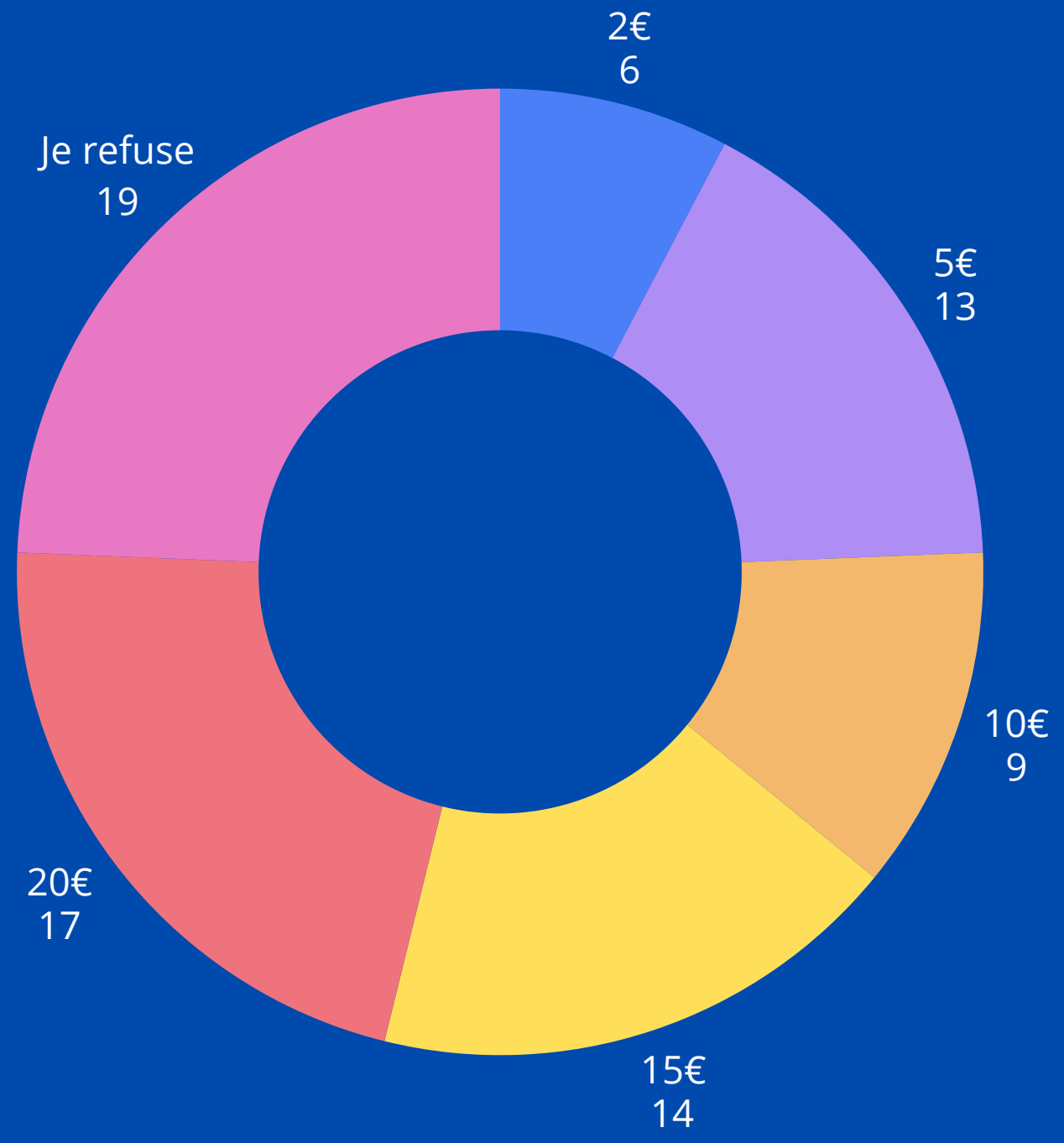
Activer mon offre Express

Interface avec Dark Patterns

Résultats Descriptifs

3

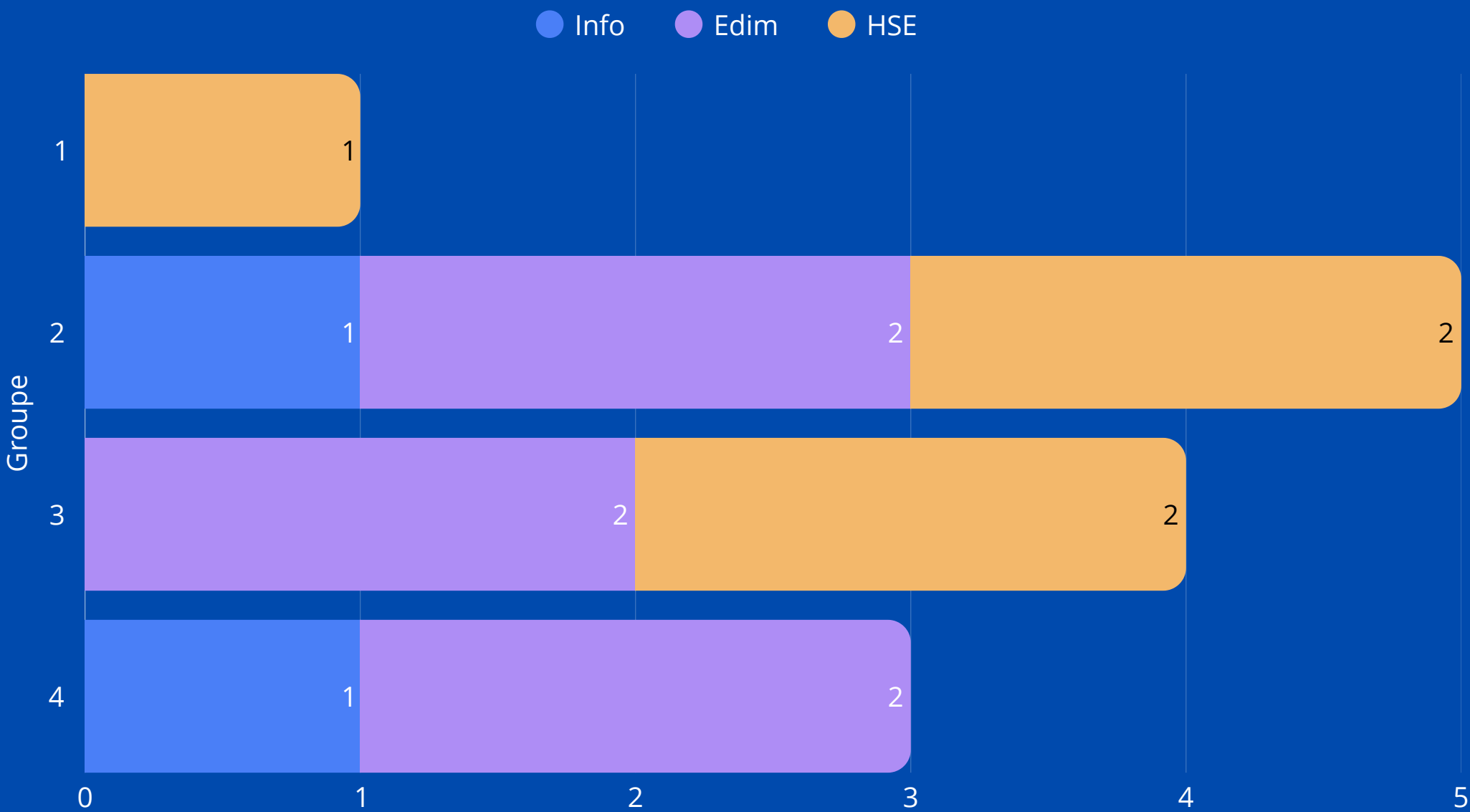
La valeur accordée aux données personnelles (Pré-test) sur le panel 78 personnes.



Résultats Descriptifs

3

Taux d'incohérence (soumission au piège) selon la condition expérimentale.



Bilan descriptif

Incohérence Groupe 1 : **5.6%**

Incohérence Groupe 2 : **26.3%**

Incohérence Groupe 3 : **19%**

Incohérence Groupe 4 : **15%**

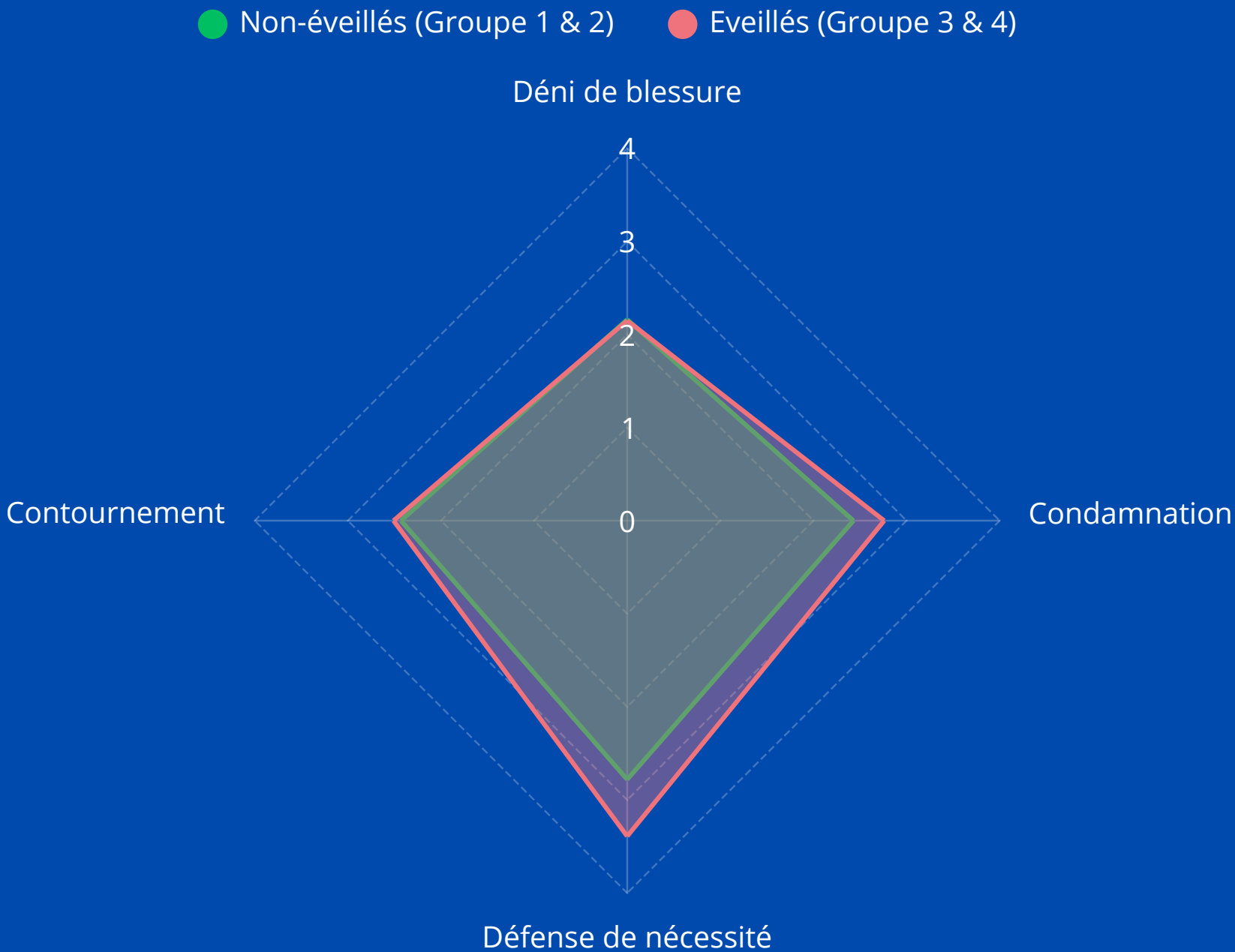
Efficacité de l'interface : Le Dark Pattern (G2) multiplie par 5 le taux d'erreur par rapport à l'interface neutre (G1).

L'effet Bouclier : L'induction de dissonance avant le Dark Pattern (G4) permet de réduire le taux de soumission de 11 points par rapport à l'attaque seule (G2).

Résultats Descriptifs

3

Scores moyens d'adhésion aux techniques de neutralisation (Échelles de Likert 1-5 sur l'intensité des justifications).



Observation

L'excuse dominante : La Défense de nécessité (le manque de temps) est l'argument le plus mobilisé par tous les étudiants. Dans les groupes 3 et 4 cela monte même à 3.39 points sur 5.

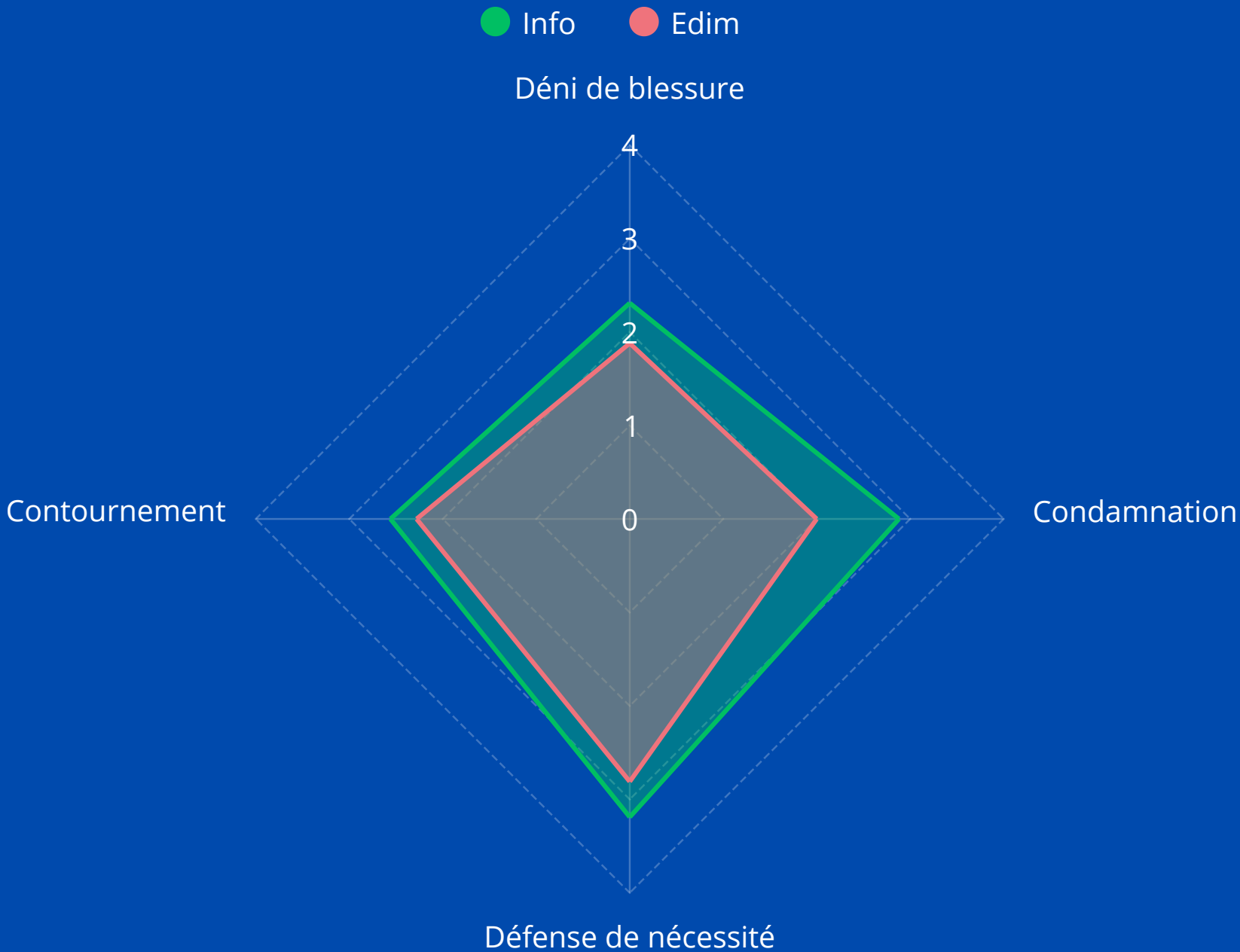
Un résultat contre-intuitif : Contrairement à ce que j'avais postulé dans l'Hypothèse 3, l'induction d'hypocrisie n'a pas fait chuter les justifications. Au contraire, les groupes "éveillés" ont augmenté leur rationalisation.

Piste d'interprétation : L'inconfort psychologique généré a probablement été trop fort, déclenchant un mécanisme de défense de l'ego.

Analyse Croisée

4

Différences de rationalisation entre les experts techniques (Info) et les experts en usages (EDIM).



Stratégies de rationalisation asymétriques

La prédominance Informatique : Les experts techniques (Info) rationalisent globalement beaucoup plus que les experts en design (EDIM) sur tous les critères.

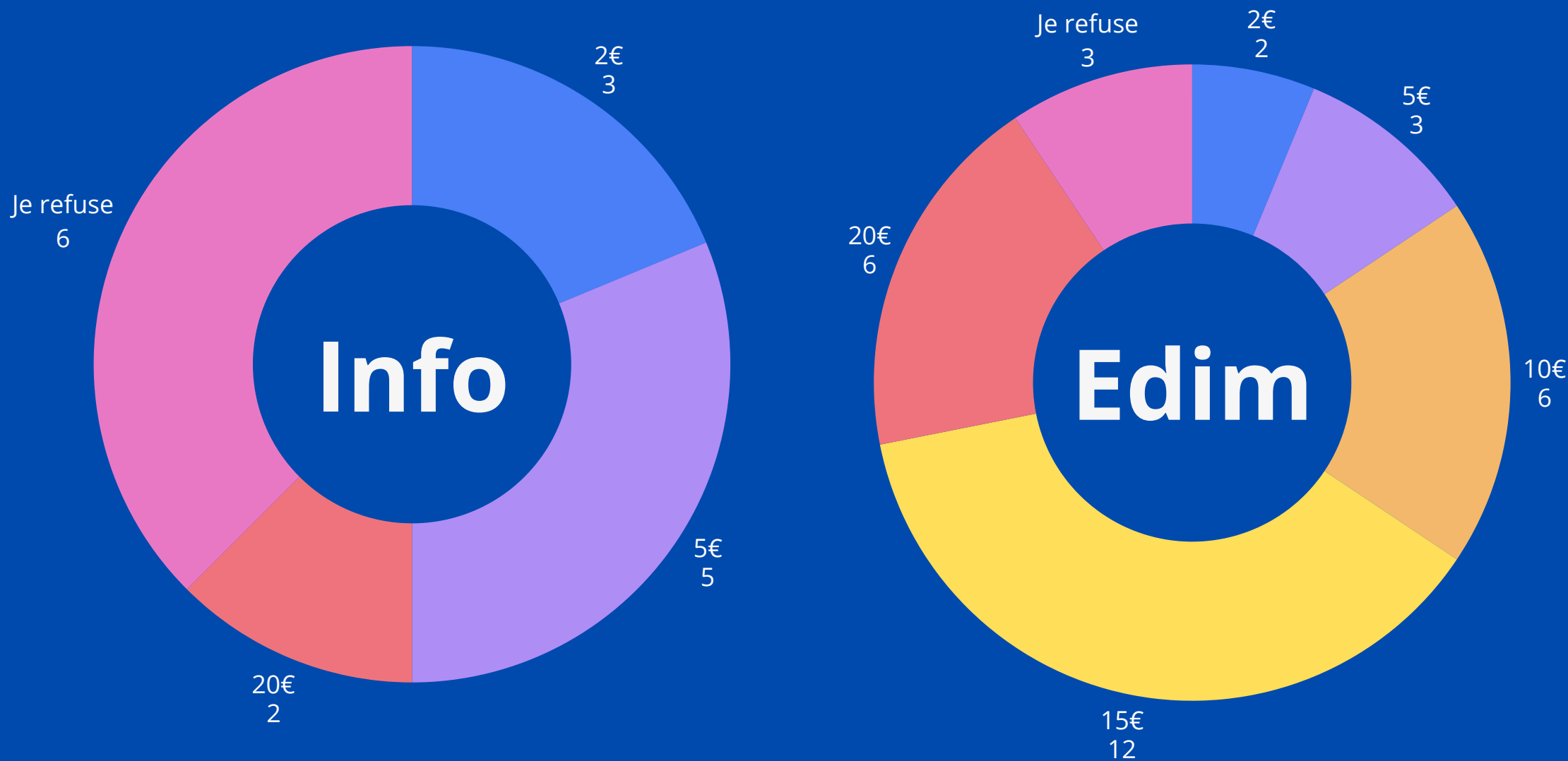
Le Contournement assumé : Comme postuler (H1), la filière Info assume davantage le recours au "mot de passe poubelle" (2,56 contre 2,28) justifiant la prise de risque par une maîtrise technique de la faille.

L'hégémonie de la Nécessité : L'argument du manque de temps et de la friction ergonomique reste l'excuse n°1 pour les deux profils (pics respectifs à 3,19 et 2,81).

Analyse Croisée

4

La donnée comme monnaie d'échange : une perception radicalement différente entre experts techniques et experts en usages.



La dualité de la valeur

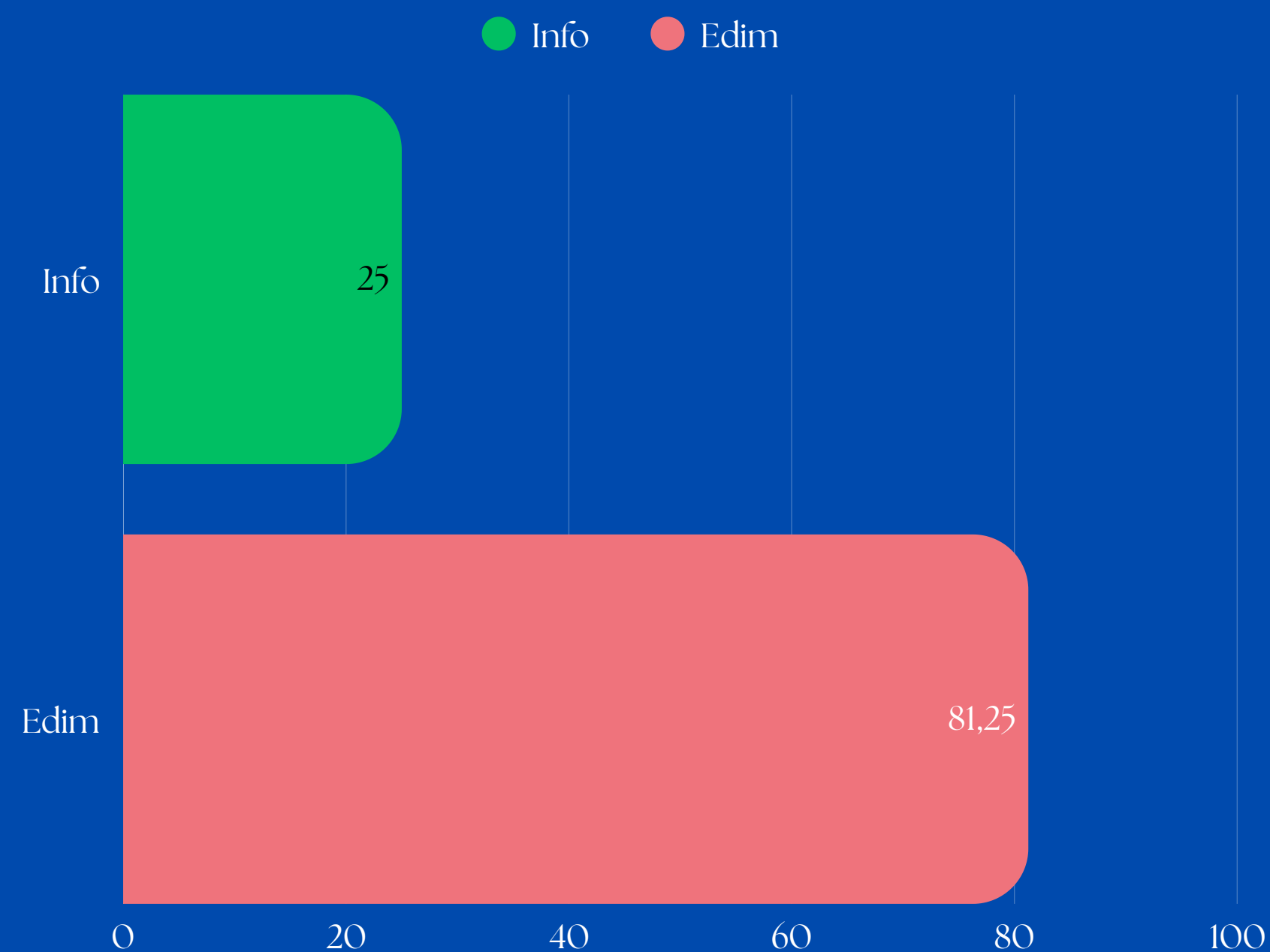
Le fatalisme pragmatique (Info) : Une polarisation marquée ; les étudiants en informatique tendent soit à protéger radicalement leurs données (37,5% de refus), soit à les "brader" (pour 2 ou 5€) en utilisant des stratégies de contournement technique.

La négociation marchande (EDIM) : Les designers abordent la donnée comme une ressource de valeur, exigeant une compensation élevée (le mode "prix fort" à 15-20€ est majoritaire) avant d'accepter le partage.

Analyse Croisée

4

Analyse de l'hygiène numérique : la réutilisation des mots de passe comme révélateur de la vulnérabilité.



Une faille de sécurité structurelle

L'alibi technique (Info) : 75% des étudiants en informatique séparent leurs comptes, confirmant une meilleure hygiène numérique, bien que 25% restent exposés.

La faille ergonomique (EDIM) : Une porosité alarmante (81,25% de réutilisation) révèle que, pour ces profils, la fluidité d'usage et la mémoire cognitive priment sur la sécurité des accès universitaires (ENT/Mail).

Enjeu de prévention : Le besoin d'interfaces sécurisées mais "sans friction" est un levier critique pour les profils non-techniques.

Discussion Statistique

5

Interprétation critique des résultats statistiques et validité méthodologique.

Bilan des Hypothèses

H1 : Influence de la filière	 Partiellement validée	Profils de rationalisation distincts, mais dépendance commune à la "Nécessité".
H2 : Effet du Dark Pattern	 Validée	Effet puissant du Dark Pattern sur l'incohérence des choix (VD1).
H3 : Réductions des Fausses Excuses	 Invalidée	Effet boomerang : la dissonance a augmenté la rationalisation au lieu de la réduire.
H4 : Bouclier Mental	 Validée (tendance)	Réduction de 11 points du taux d'incohérence malgré l'effet boomerang.

Discussion Statistique



Interprétation de l'effet tendanciel sur le taux d'incohérence.

Synthèse des analyses

Parmi l'ensemble des analyses effectuées, seules les tendances liées au taux d'incohérence (VD1) et aux profils de rationalisation (VD2) ont révélé des écarts comportementaux tendanciels.

Comparaison	Statistique Khi2	p-valeur	Significatif (p < 0.05) ?
Groupe 1 vs Groupe 2	2,932104006	0,08683425891	Non

Test du Khi² (VD1) : Observation d'un effet tendanciel fort (N=78). Bien que la valeur p soit > 0,05, l'écart de 21 points entre le groupe contrôle et le groupe manipulé suggère un impact réel de l'effet d'attaque du Dark Pattern.

Les limites majeures :

- **Puissance Statistique :** La taille de l'échantillon (N=78) limite la significativité statistique globale.
- **Validité Écologique :** Le caractère simulé de l'expérience (application fictive) peut différer d'une prise de décision réelle.
- **Biais de désirabilité :** Tendance naturelle à rationaliser ses choix à posteriori lors du remplissage des échelles de Likert.

Conclusion et Perspectives

6

Vers une cybersécurité fondée sur la psychologie humaine

Synthèse des acquis

Preuve de l'attaque : Confirmation de la puissance manipulatoire des Dark Patterns (incohérence x5).

L'effet "Bouclier" : L'éveil à l'éthique réduit significativement la soumission, malgré l'effet de réactance.

Profilage psychologique : Validation de stratégies de défense distinctes entre experts techniques (Info) et experts en usages (EDIM).

Perspectives et ouvertures

Design Éthique : Développer des Bright Patterns qui favorisent la réflexion sans imposer de friction excessive.

Échelle et validité : Déployer le protocole sur un échantillon plus large et hétérogène pour renforcer la puissance statistique.

Prévention adaptative : Concevoir des interfaces qui s'adaptent au "profil de défense" de l'utilisateur (ex: sensibilisation technique vs sensibilisation ergonomique).

Bibliographie

- BOGLIACINO, Francesco, PEJSACHOWICZ, Leonardo, LIVA, Giovanni et al. Testing for Manipulation: Experimental Evidence on Dark Patterns. In: SocArXiv [en ligne]. Disponible sur : https://doi.org/10.31235/osf.io/sqt3j_v1 (consulté le 9 avril 2026)
- SIPONEN, Mikko, PUHAKAINEN, Petri, VANCE, Anthony. Can individuals' neutralization techniques be overcome? A field experiment on password policy. In: Computers & Security [en ligne]. 2020, vol. 88, p.101617. Disponible sur : https://jyx.jyu.fi/jyx/Record/jyx_123456789_65920 (consulté le 12 avril 2026)
- RYOO, Yuhosua, KIM, Woojin. Approach versus avoidance: A self-regulatory perspective on hypocrisy induction in anti-cyberbullying CSR campaigns. In: Journal of Business Ethics [en ligne]. 2024, vol. 189, n° 2, p. 345-364. Disponible sur : https://www.researchgate.net/publication/368926901_Approach_versus_Avoidance_A_Self-Regulatory_Perspective_on_Hypocrisy_Induction_in_Anti-Cyberbullying_CSR_Campaigns (consulté le 18 avril 2026)