CRPC | Chaire de recherche en prévention de la cybercriminalité

Notes *de synthèse*

Vol. 4, Num. 6
2024

Le rôle des biais cognitifs sur la prise de décision en cybersécurité

Maya Dubord, candidate à la maîtrise en criminologie

Introduction

La théorie du choix rationnel soutient que les individus cherchent, avant tout, à satisfaire leurs besoins en produisant le moins d'effort possible [1]. L'analyse de coûts et bénéfices d'agir (ou non) est largement influencée par les informations dont l'individu dispose au moment de prendre sa décision. Sans des informations justes et complètes à sa disposition, il est possible de faire des choix irrationnels par inadvertance [2].

La recherche sur les biais cognitifs et les heuristiques, amorcée dans les années 1970, découle de la théorie du choix rationnel [3]. **Les heuristiques sont des stratégies employées pour prendre des décisions le plus efficacement possible** [4]. Elles demandent d'inférer des informations et d'employer des raccourcis mentaux dans le but d'économiser des efforts cognitifs [3, 5, 6]. **Les biais cognitifs sont la conséquence d'erreurs dans l'utilisation de ces raccourcis mentaux** [7]. Ils sont constitués d'erreurs de jugement inconscientes menant à des prises de décisions irrationnelles [5, 7].

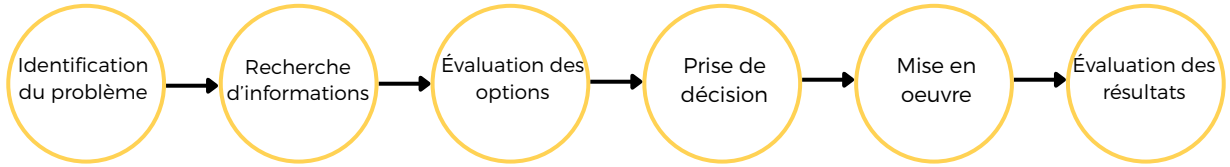
Selon les pionniers de la recherche sur les biais cognitifs, **une décision serait prise non seulement en fonction des informations disponibles, mais aussi en fonction de l'interprétation qu'en font les individus**. L'utilisation de son jugement en se basant sur des processus de réflexions erronés peut mener un individu à évaluer inadéquatement les conséquences de ses gestes [3].

Travailler en cybersécurité, ou encore le simple fait de devoir tenir compte de celle-ci dans ses tâches quotidiennes, implique la prise d'une multitude de décisions complexes quotidiennement. Ainsi, **une vigilance accrue à ses propres biais cognitifs peut limiter l'avènement d'incidents de sécurité** [8]. Cette note de synthèse brosse un portrait du processus de prise de décision selon les fondements de la psychologie sociale, des heuristiques et biais cognitifs, de leurs impacts en matière de cybersécurité, et des interventions possibles pour limiter leurs conséquences négatives.

Les principaux concepts

La prise de décision

Prendre une décision dans le but de résoudre un problème est **un processus qui implique de faire une analyse d'une situation et d'y trouver une solution** [9]. Ce processus peut être séparé en six étapes : **l'identification d'un problème**, **la recherche d'informations**, **l'évaluation des options**, **la prise de décision**, **la mise en œuvre et l'évaluation des résultats** [10]. La figure 1 représente ce processus.



Processus de prise de décision [11]

Il existe deux manières différentes de prendre une décision [11, 12]. La première, appelée **"Système 1" est rapide, instinctive, et se traduit par des réflexions faites par automatismes** [12]. La deuxième, appelée **"Système 2" est plus lente et délibérée, incluant des réflexions approfondies qui demandent du temps et ayant but de peser le pour et le contre** [12]. La combinaison des deux systèmes permet de distinguer les informations pouvant être traitées efficacement de celles qui demandent une attention accrue avant de pouvoir prendre une décision [12].

Ces deux systèmes présentent des avantages et des inconvénients. Le **Système 1** permet de prendre des décisions rapidement et efficacement [11]. **Il permet de s'adapter à des situations imprévues sans en faire une analyse approfondie**. Cette capacité d'adaptation fondée sur l'intuition peut aider à réagir à des situations dangereuses ou créant une forte réaction émotionnelle [11]. Aussi, **le Système 1 permet d'automatiser certaines décisions en se basant sur les connaissances acquises lors d'expériences antérieures** [11]. Toutefois, le Système 1 présente aussi plusieurs inconvénients. **Il peut mener à des réponses émotionnelles excessives et à des simplifications exagérées d'une situation** [11] et il est **sensible aux stéréotypes et peut mener à des jugements discriminatoires**. En raison de sa rapidité, le Système 1 peut susciter un sentiment exagéré de confiance par rapport à la capacité de juger précisément d'une situation [11].

Le Système 2 présente aussi plusieurs avantages. incluant **la possibilité de faire une analyse approfondie d'une situation**, **la correction des biais cognitifs du premier système, la résolu-tion de problèmes plus complexes** et **la prise de décisions informées fondées sur une évaluation rationnelle des risques et avantages d'une situation** [11]. En contrepartie, le Système 2 présente des inconvénients quant à **sa lenteur, l'importance des efforts cognitifs exigés, la vulnérabilité à surévaluer une situation et le risque de négliger des signaux émotionnels** [11]. Les biais cognitifs peuvent donc être engendrés par le Système 1 et remédié par le Système 2 [11]. La prochaine section présentera un portrait plus approfondi des heuristiques et des biais cognitifs qui en découlent.

Heuristiques et biais cognitifs

Les heuristiques sont définies comme étant des approximations effectuées dans le but de prendre une décision [4]. Les heuristiques demandent de faire de l'inférence et d'employer des raccourcis mentaux dont le but est de faire le moins d'efforts cognitifs possible pour arriver à la meilleure décision [3, 5, 6]. Une partie des informations disponibles pour la prise de décision est donc ignorée pour prendre une décision de manière efficace [4]. L'emploi de raccourcis cognitifs n'est pas nécessairement néfaste, certains contextes ne permettant pas la prise en considération exhaustive d'un grand nombre de facteurs, par exemple, dû à l'urgence de la situation [3, 6, 12, 13]. Ils peuvent toutefois devenir problématiques lorsqu'ils mènent à une appréciation erronée de la décision à prendre. **Les erreurs potentielles que peuvent engendrer les heuristiques s'appellent les biais cognitifs** [3].

Un biais cognitif est défini comme **une erreur de jugement identifiable et classifiable engendrant des comportements s'éloignant de l'action la plus rationnelle à adopter [5].** Les biais cognitifs sont involontaires et inconscients et

dérivent d'une erreur de jugement effectuée de bonne foi [7]. Par exemple, un individu pourrait faire un choix X alors que la situation semble mener à faire le choix Y si son jugement des événements est erroné en raison de ses biais cognitifs.

Les biais cognitifs peuvent être classés en fonction des quatre familles d'heuristiques sur lesquels ils se fondent. La première famille est constituée des **biais découlant de l'heuristique de disponibilité**. Cette dernière consiste à **évaluer la probabilité d'un événement en fonction de la facilité avec laquelle on peut penser à des exemples de situations similaires qui se sont déjà produites** [3, 11]. Plus la situation est facile à envisager, plus l'événement sera perçu comme probable. Par exemple, il peut être difficile de trouver plusieurs exemples d'événements où tous les serveurs informatiques d'une institution sont tombés en panne simultanément, mettant à risque leurs infrastructures de sécurité. La situation pourrait être perçue comme peu probable alors qu'elle représente un risque réel.

La deuxième famille inclut les **biais issus de l'heuristique de représentativité**. Celle-ci implique d'**estimer la probabilité qu'une situation se produise en fonction de sa similarité avec d'autres événements connus** [3, 11]. Plus un événement est similaire à un autre, plus les conséquences de l'événement antérieur sont jugées comme plus probable de se reproduire. Par exemple, une institution n'ayant pas été victime de rançongiciel par le passé pourrait ne pas mettre en place des mesures de formation et de protection en estimant que cela n'arrivera pas non plus dans le futur, malgré un changement du profil des risques.

La troisième famille découle quant à elle, de **l'heuristique d'ajustement et d'ancrage**, définie par l'**évaluation d'une situation en fonction d'un point de référence acquis antérieurement** [3, 11], c'est-à-dire que la gravité d'une situation peut être évaluée en fonction de la gravité d'une autre. Par exemple, une fuite de données concernant un seul usager pourrait être perçue comme étant modérément grave (voir pas grave du tout) si l'organisation concernée a été confrontée à une fuite de données de 200 ou 2000 usagers par le passé.

La dernière famille est issue de **l'heuristique émotionnelle**, soit **la prise de décision faisant appel aux émotions plutôt qu'à un processus rationnel d'évaluation d'une situation** [3, 11]. Par exemple, un employé pourrait transmettre des documents à un cybercriminel parce que ce dernier se fait passer pour un collègue et le presse d'agir rapidement. Des exemples de biais cognitifs découlant de ces familles d'heuristiques seront présentés dans la prochaine section.

Biais cognitifs et prise de décision en matière de cybersécurité

Types de biais

La prochaine sous-section présente quelques biais cognitifs identifiés dans la littérature scientifique sur la cybersécurité.

Effet de cadrage

L'effet de cadrage consiste à présenter deux choix susceptibles de produire le même résultat, mais en modifiant la présentation des énoncés pour inciter à prendre une décision spécifique [14]. Le premier choix suggère par exemple un résultat sûr ou générant un gain pour la personne prenant la décision, tandis que le deuxième se caractérise par une formulation impliquant un niveau d'incertitude plus marqué [14, 15]. Généralement, la décision qui ne suscite pas de sentiment de risque est préférée bien que les résultats des deux choix soient identiques [14]. Par exemple, une étude visant à évaluer la probabilité pour un employé, d'être victime d'une cyberattaque en utilisant des messages de sensibilisation mettait en avant soit un potentiel de perte, soit un potentiel de gain. Les résultats de la recherche démontrent que l'utilisation de messages de sensibilisation axés sur des pertes

potentielles mène à des comportements plus sécuritaires [15]. **Le cadrage peut aussi être employé pour présenter des résultats sous un angle favorable ou défavorable**. Par exemple, affirmer que 18% des entreprises canadiennes ont été victimes d'un incident de cybersécurité en 2021 n'évoque pas la même réaction qu'affirmer que 82% des entreprises canadiennes n'ont pas été affectées par ces incidents pour la même année[16]. La formulation ainsi changée soutient le même propos, mais ne dirige pas vers la même évaluation de la situation.

Effet d'ancrage

L'effet d'ancrage est « […] un jugement […] fortement influencé par l'exposition préalable de celui qui juge, à une « valeur de référence », laquelle agit comme une « ancre » pour l'esprit humain. » [17] Par exemple, lorsqu'un gestionnaire décide de donner une priorité plus élevée à une menace à la cybersécurité spécifique, les employés se concentrent alors sur cette menace précise au lieu d'évaluer l'ensemble des risques qui peuvent accompagner l'incident principal [18]. Les informations sont donc tenues pour acquises sans une remise en question de leur validité ou fiabilité.

Illusion du contrôle

L'illusion du contrôle consiste pour une personne à croire qu'elle peut influencer exagérément une situation même si les issues possibles sont en réalité complètement aléatoires [19, 20]. **Plus l'illusion de contrôler une situation augmente, plus la perception du risque diminue** [20]. Par exemple, un employé désirant accéder à des documents corporatifs sur son téléphone cellulaire personnel peut avoir l'impression qu'il est entièrement protégé grâce à l'authentification à deux facteurs. En revanche, cette illusion de contrôle diminue sa sensibilité aux failles de sécurité causées par sa connexion internet sur un réseau non sécurisé ou le manque de mise à jour de ses applications. Il en va de même pour les employés qui ont suivi des modules de formation introductifs à la cybersé-curité qui peuvent surestimer leurs capacités à détecter et à éviter les risques en ligne.

Théorie d'un monde juste

Le biais de la théorie d'un monde juste repose sur le besoin humain de croire que des principes de justice régissent le monde et que les individus obtiennent ce qu'ils méritent, c'est-à-dire que les actes sont alignés avec les conséquences [21, 22]. Par exemple, il pourrait s'agir de la perception de tierces parties qu'un employé victime de piratage informatique, soit responsable de sa situation, malgré les mesures de protection exemplaires qu'il a mises en place sans prendre en compte le déséquilibre d'expertise entre lui et un fraudeur. Blâmer la victime permet ainsi de maintenir le sentiment que le monde est juste, bien que les probabilités de se faire attaquer soient dans la plupart des cas hors de son contrôle.

Effet de Barnum

L'effet de Barnum reflète la tendance des êtres humains à accepter des descriptions vagues et générales de traits de caractère comme étant des descriptions précises et justes de leur personnalité [23, 24]. Ceci augmenterait la confiance qu'une personne accorde à son interlocuteur ou à la plateforme de communication qu'elle emploie en créant une apparence de validité et de crédibilité [24]. Une étude a d'ailleurs démontré que plus une tentative d'hameçonnage est perçue comme étant réaliste, moins elle a de chance d'être détectée et déclarée comme un incident de cybersécurité [25]. La recherche démontre aussi que plus un courriel malicieux est convaincant, moins les erreurs techniques (erreurs dans le nom de domaine ou le nom de la compagnie) sont détectées [25]. Bien que cette étude ne vienne pas directement évaluer l'effet de Barnum, elle démontre l'impact que peut avoir une perception erronée du réalisme d'une situation en matière de cybersécurité.

Biais des coûts irrécupérables

Le biais des coûts irrécupérables consiste pour une personne à décider de continuer à investir des ressources dans une action bien que les bénéfices soient inférieurs aux efforts déjà investis. Les investissements antérieurs qui ne peuvent plus être récupérés et réinvestis ailleurs sont pris en considération de manières disproportionnées dans l'évaluation d'une situation [26, 27, 28]. En cybersécurité, cela se traduit par exemple par le fait de continuer à employer un antivirus désuet et inefficace à cause de l'argent dépensé antérieurement pour renouveler les licences de celui-ci année après année.

Impacts des biais cognitifs

Les biais cognitifs peuvent influencer négativement les risques de cybervictimisation et la réponse déployée face aux incidents. Les études recensées ne permettent pas de déterminer les coûts financiers qu'engendrent les biais cognitifs en matière de sécurité. L'analyse des impacts des biais a plutôt été effectuée dans des laboratoires et leurs résultats sont difficilement généralisables dans un contexte d'entreprise. Malgré tout, quelques études de cas ont produit des résultats applicables à la cybersécurité.

Risque de cybervictimisation

Les biais cognitifs peuvent affecter négativement les entreprises en favorisant la prise de mauvaises décisions mettant à risque leur cybersécurité [29]. Les biais cognitifs des victimes potentielles peuvent être exploités par les cybercriminels à travers l'utilisation de techniques d'ingénierie sociale. L'ingénierie sociale est caractérisée par l'utilisation de techniques de manipulation par un attaquant pour tenter d'obtenir l'aide de la victime dans la perpétration d'une opération d'utilisation malveillante d'un ordinateur [30]. Elle peut prendre la forme d'appels téléphoniques, de courriels, de message texte ou de rencontres face à face [31]. En manipulant une conversation avec la victime, le cybercriminel peut arriver à la mettre en confiance et à lui soutirer des informations. Une étude néerlandaise a démontré l'impact de l'ingénierie sociale sur les biais cognitifs par des individus malveillants. Les chercheurs y ont évalué la différence entre l'intention de respecter les protocoles de sécurité et les comportements réels face à une demande d'installation d'un logiciel provenant d'une source non fiable [32]. Sur les 49 participants, aucun individu n'a admis vouloir télécharger le logiciel suspects. Dans la réalité, 40% des répondants ont téléchargé le logiciel [32]. Sans une prise de conscience accrue de ses propres vulnérabilités, il est possible que la victime ne se rende pas compte de la situation et que l'incident ne soit pas signalé aux services informatiques [30].

Réponse aux incidents de cybersécurité

Lors d'incidents de cybersécurité, l**es biais cognitifs peuvent mener à une mauvaise prise de décision pour y répondre** [29]. Ils peuvent mener à une mauvaise évaluation des risques présents au sein d'une organisation [33]. **L'illusion de contrôle que peuvent avoir les gestionnaires sur l'atténuation des risques de cybersécurité peut mener à l'implantation de protocoles de protection non adaptés à la réalité de l'entreprise** [33]. Des facteurs organisationnels, tels que le désir d'économiser sur les coûts d'implantation de mesures de protection et une culture organisationnelle ne valorisant pas la prévention, peuvent contribuer à l'établissement de pratiques de cybersécurité défaillantes [33]. Une étude sur quatre attaques par déni de service distribué (DDoS) dont ont été victime le Bureau australien de la Statistique en 2016 a démontré que les cyberattaques sont inévitables et que les gestionnaires se doivent d'être prêts pour y répondre avant qu'elles n'arrivent. Les biais cognitifs présents chez les gestionnaires du Bureau auraient mené à une sous-évaluation des risques présents au sein des infrastructures de cybersécurité [33]. Les chercheurs ont également démontré qu'une trop

grande confiance accordée aux partenaires organisationnels en matière de cybersécurité peut mener une institution à oublier d'adapter les pratiques de prévention à ses besoins spécifiques. Dans le cas du Bureau, les techniques de prévention mises en place par IBM n'ont pas été remises en question et ne se sont pas montrées efficaces lors des attaques [33].

Interventions sur les biais

Volet des employés et des gestionnaires

Peu d'études ont été effectuées uniquement sur les méthodes d'intervention sur les biais cognitifs en matière de prévention des incidents de cybersécurité. **Les études ayant porté sur les biais cognitifs et la victimisation ont démontré qu'une prise de conscience par rapport aux biais cognitifs par des modules de formation peut venir diminuer les risques de victimisation** [31, 34]. Pour les gestionnaires, une prise de conscience de leurs propres biais ainsi que de ceux de leurs équipes peut être favorable au développement de pratiques plus sécuritaires [34]. **Toutefois, les effets de cette prise de conscience tendent à diminuer avec le temps** [35]. De plus amples recherches sont nécessaires pour tenter de comprendre comment faire perdurer son effet [31]. Par exemple, une étude a démontré que l'utilisation de plusieurs rappels des protocoles de réponses aux incidents de cybersécurité sous différentes formes serait une manière adéquate d'augmenter la sensibilité des employés aux risques [36].

Volet organisationnel

Puisque chaque organisation fait face à des menaces propres à son domaine d'affaires et ses caractéristiques, il est impossible de développer une liste de mesures de prévention universelles [33]. **Les organisations se doivent d'être proactives dans le développement et l'entretien de leurs protocoles de cybersécurité** [33]. Il est possible d'atténuer les impacts des biais cognitifs lors de la création de ces protocoles. Ceux-ci doivent être soumis à un processus rigoureux d'évaluation par un comité jouant le rôle de l'avocat du diable [33]. Par ce processus, il est attendu que tous les membres du comité doivent tenter de trouver le meilleur plan possible pour arriver aux résultats inverses de ceux désirés et il y a donc la responsabilité de trouver comment faire échouer les protocoles pour en déceler les failles [33]. Ce processus permet d'identifier les vulnérabilités oubliées lors de l'élaboration initiale du projet, de mettre en place les mesures de révision appropriées et d'augmenter la robustesse du protocole final [33].

Conclusion

En conclusion, **les biais cognitifs peuvent engendrer et amplifier les risques de cybersécurité dans les organisations et parmi les individus** [29, 34, 36]. Ils sont causés par des erreurs de jugement dans le processus décisionnel basé sur une mauvaise approximation et interprétation des informations disponibles [11, 14]. Ils peuvent mener à une mauvaise évaluation des caractéristiques d'un événement ou encourager les individus à répondre inadéquatement à une situation [29]. Plusieurs types de biais cognitifs tels que les biais d'effet de cadrage et d'ancrage ont été présentés ci-haut [14, 37]. En revanche, plusieurs autres biais non abordés tels que les biais de confirmation ou de complaisance pourraient être étudiés pour mieux comprendre les risques auxquels font face les organisations.

Malgré les conséquences potentiellement graves des biais, il est possible d'intervenir pour tenter de prévenir leurs impacts négatifs [33]. **Des modules de formation permettant une prise de conscience des biais par les employées et les gestionnaires et des mises en situation concrètes peuvent aider à favoriser une culture de cybersécurité positive et efficace** [31, 34]. De plus amples recherches sur les techniques de sensibilisation aux biais cognitifs par la ludification pourraient être intéressantes.

Références

[1] Hirschi, T. (2014). On the Compatibility of Rational Choice and Social Control Theories of Crime. Dans D. B. Cornish et R. V. Clarke (dir.), *The Reasoning Criminal: Rational Choice Perspectives on Offending* (p. 105-118). Londres: Routledge.

[2] Simon, H. A. (1991). Bounded Rationality and Organizational Learning. *Organization Science*, *2*(1), 125–134. https://doi.org/10.1287/orsc.2.1.125

[3] Kahneman, D. et Tversky, A. (1982). Judgment under uncertainty: Heuristics and biases. Dans D. Kahneman, P. Slovic et A. Tversky (dir.), *Judgment under Uncertainty: Heuristics and Biases* (p. 3–20). Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511809477.002

[4] Gigerenzer, G. et Gaissmaier, W. (2011). Heuristic decision making. *Annual Review of Psychology*, *62*, 451–482. https://doi.org/10.1146/annurev-psych-120709-145346

[5] Hilbert, M. (2012). Toward a synthesis of cognitive biases: How noisy information processing can bias human decision making. *Psychological Bulletin*, *138*(2), 211–237. https://doi.org/10.1037/a0025940

[6] Thomas, O. (2018). Two decades of cognitive bias research in entrepreneurship: What do we know and where do we go from here? *Management Review Quarterly*, *68*(2), 107–143. https://doi.org/10.1007/s11301-018-0135-9

[7] Pohl, R. (2022). Cognitive illusions: Intriguing phenomena in thinking, judgment, and memory. Londres: Routledge.

[8] Keh, H. T., Der Foo, M. et Lim, B. C. (2002). Opportunity Evaluation under Risky Conditions: The Cognitive Processes of Entrepreneurs. Entrepreneurship *Theory and Practice*, *27*(2), 125–148. https://doi.org/10.1111/1540-8520.00003

[9] Driver, M. J., Brousseau, K. R. et Hunsaker, P. L. (1998). *The Dynamic Decision Maker: Five Decision Styles for Executive and Business Success*. iUniverse.

[10] Simon, H. A., Dantzig, G. B., Hogarth, R., Plott, C. R., Raiffa, H., Schelling, T. C. et coll. (1987). Decision Making and Problem Solving. *Interfaces*, *17*(5), 11–31.

[11] Kahneman, D. (2011). *Thinking, Fast and Slow*. Doubleday Canada.

[12] Ehrlinger, J., Readinger, W. O. et Kim, B. (2016). Decision-making and cognitive biases. *Encyclopedia of Mental Health*, *12*(3), 83–87.

[13] Busenitz, L. W. et Barney, J. B. (1997). Differences between entrepreneurs and managers in large organizations: Biases and heuristics in strategic decision-making. *Journal of Business Venturing*, *12*(1), 9–30. https://doi.org/10.1016/S0883-9026(96)00003-1

[14] Tversky, A. et Kahneman, D. (1981). The Framing of Decisions and the Psychology of Choice. *Science*, *211*(4481), 453–458.https://doi.org/10.1126/science.7455683

[15] Rodríguez-Priego, N., van Bavel, R., Vila, J. et Briggs, P. (2020). Framing Effects on Online Security Behavior. *Frontiers in Psychology*, 11.

[16] Gouvernement du Canada, S. C. (2022, October 18). *Le Quotidien—L'incidence du cybercrime sur les entreprises canadiennes*, 2021.

[17] Goldszlagier, J. (2015). L'effet d'ancrage ou l'apport de la psychologie cognitive à l'étude de la décision judiciaire. *Les Cahiers de la Justice*, *4*(4), 507–531. https://doi.org/10.3917/cdlj.1504.0507

[18] Durbin, S. (2022). 10 cognitive biases that can derail cybersecurity programs. *Security Magazine*.

[19] Hoorens, V. (1996). Self-favoring biases for positive and negative characteristics: Independent phenomena? *Journal of Social and Clinical Psychology*, *15*(1), 53–67. https://doi.org/10.1521/jscp.1996.15.1.53

[20] Rhee, H.-S., Ryu, Y. et Kim, C. (2005). I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security.

[21] Lerner, M. J. et Simmons, C. H. (1966). Observer's reaction to the "innocent victim": Compassion or rejection? *Journal of Personality and Social Psychology*, *4*(2), 203–210.

[22] Hafer, C. L. et Bègue, L. (2005). Experimental Research on Just-World Theory: Problems, Developments, and Future Challenges. *Psychological Bulletin*, *131*(1), 128–167. https://doi.org/10.1037/0033-2909.131.1.128

[23] Dickson, D. H. et Kelly, I. W. (1985). The 'Barnum Effect' in Personality Assessment: A Review of the Literature. *Psychological Reports*, *57*(2), 367–382. https://doi.org/10.2466/pr0.1985.57.2.367

[24] Snyder, C. et Shenkel, R. (1976). Effects of "favorability," modality, and relevance on acceptance of general personality interpretations prior to and after receiving diagnostic feedback. *Journal of Consulting and Clinical Psychology*, *44*, 34–41. https://doi.org/10.1037/0022-006X.44.1.34

[25] Kersten, L., Burda, P., Allodi, L. et Zannone, N. (2022). Investigating the Effect of Phishing Believability on Phishing Reporting. *2022 IEEE European Symposium on Security and Privacy Workshops*, 117–128. https://doi.org/10.1109/EuroSPW55150.2022.00018

[26] Thaler, R. (1980). Toward a positive theory of consumer choice. *Journal of Economic Behavior & Organization*, *1*(1), 39–60. https://doi.org/10.1016/0167-2681(80)90051-7

[27] Kahneman, D. et Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263–291. https://doi.org/10.2307/1914185

[28] Johnson, C. K., Gutzwiller, R. S., Gervais, J. et Ferguson-Walter, K. J. (2021). Decision-Making Biases and Cyber Attackers. *2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW)*, 140–144.

[29] Lemay, A. et Leblanc, S. (2018, March 10). *Cognitive Biases in Cyber Decision-Making*.

[30] Abraham, S. et Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183–196. https://doi.org/10.1016/j.techsoc.2010.07.001

[31] Bullée, J.-W. et Junger, M. (2020). Social Engineering. Dans T. J. Holt et A. M. Bossler (dir.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (p. 849–875). Springer International Publishing.

[32] Bullee, J.-W. (2017). Experimental social engineering: Investigation and prevention. https://doi.org/10.3990/1.9789036543972

[33] Ceric, A. et Holland, P. (2019). The role of cognitive biases in anticipating and responding to cyberattacks. *Information Technology & People*, *32*(1), 171–188. https://doi.org/10.1108/ITP-11-2017-0390

[34] White, C. A. (2023). Mixed Method Exploration of Cybersecurity Executive Decisions and Cognitive Bias [Thèse, Marymount University]. In ProQuest Dissertations and Theses (2822137641). ProQuest Dissertations & Theses Global Closed Collection.

[35] Bullée, J.-W., Montoya, L., Junger, M. et Hartel, P. (2016, January 14). *Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention*. https://doi.org/10.3233/978-1-61499-617-0-107

[36] Moustafa, A. A., Bello, A. et Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology*, 12.

[37] Tsohou, A., Karyda, M. et Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, *52*, 128–141. https://doi.org/10.1016/j.cose.2015.04.006