Université de Montréal

CRPC | Chaire de recherche en prévention de la cybercriminalité

# Résumé *de recherche*

# Entre perception et réalité : étude de la cyber-hygiène au sein d'une université québécoise

Shanna Auger-Drolet, M.Sc.

## Introduction

L'étude de Shanna Auger-Drolet intitulé « **Entre perception et réalité : Étude de la cyber-hygiène au sein d'une université québécoise** » le cadre de sa maîtrise en criminologie a porté sur les enjeux de cyber-hygiène dans un contexte universitaire. Cette étude s'intéresse à **la différence entre les perceptions et les comportements réels en matière de cybersécurité**, avec pour objectif d'améliorer les programmes de sensibilisation dans ce domaine.

## Problématique

La technologie joue un rôle central dans nos sociétés modernes, mais elle expose aussi les infrastructures à des cyberattaques, qui peuvent entraîner des conséquences financières et sociétales majeures (Ncubukezi & Mwansa, 2021 ; Singh et al., 2020). Bien que des solutions technologiques soient mises en place pour contrer ces menaces, **le comportement humain reste une faille critique** (McCormac et al., 2017). Selon plusieurs études, jusqu'à 95 % des violations de cybersécurité résultent d'erreurs humaines (Tempestini et al., 2023). En 2023, le coût moyen d'un incident de cybersécurité au Canada était estimé à 6,94 millions de dollars (Stephenson, 2023). Ces données soulignent **la nécessité d'améliorer la cyber-hygiène à travers des initiatives ciblées et efficaces**.

La cyber-hygiène englobe les pratiques individuelles et organisationnelles visant à protéger les systèmes d'information et les données contre les cyberattaques. **Elle inclut plusieurs dimensions, telles que la gestion des courriels, le stockage des appareils, la transmission des données, l'utilisation des médias sociaux et les méthodes d'authentification** (Vishwanath et al., 2020). Malgré ces bonnes pratiques, de nombreux utilisateurs ne les adoptent pas systématiquement, ce qui les rend vulnérables.

Les universités, avec leurs multiples utilisateurs et volumes importants de données sensibles, sont particulièrement exposées aux cyberattaques. **La culture universitaire, valorisant la libre circulation de l'information, peut entraîner une moindre priorisation de la cybersécurité** (Borgman, 2018). Peu d'études ont exploré ce sujet dans un contexte québécois, ce qui rend cette recherche innovante.

## Question de recherche

L'étude vise à répondre à la question suivante : **comment la perception de la cyber-hygiène au sein de la communauté universitaire influence-t-elle les comportements réels en matière de cybersécurité ?** Les objectifs incluent l'évaluation des connaissances et attitudes des participants vis-à-vis des politiques de cybersécurité, l'identification des divergences entre perceptions et pratiques et la formulation de recommandations pour améliorer les programmes de sensibilisation.

## Méthodologie

Pour mener cette recherche, une approche quantitative a été adoptée, basée sur **un questionnaire inspiré du modèle HAIS-Q** (Parsons et al., 2014). Les participants incluaient 127 étudiants et 139 employés d'une université québécoise. En complément, **un test d'hameçonnage a permis d'évaluer les comportements réels face à des courriels frauduleux**. Les données ont été analysées avec Excel et SPSS pour déterminer les tendances et différences significatives entre les groupes.

Le questionnaire comportait 69 questions réparties en neuf catégories : gestion des mots de passe, utilisation des courriels, utilisation d'Internet, utilisation des médias sociaux, dispositifs mobiles, traitement de l'information, rapports d'incident, messages frauduleux et renseignements personnels. Les réponses étaient recueillies sur une échelle de Likert. Plus de 3658 personnes ont été sollicitées, mais seulement 266 questionnaires ont été entièrement remplis et retenus pour l'analyse.

## Résultats

Les résultats montrent que **les employés ont une meilleure cyber-hygiène que les étudiants**, notamment en ce qui concerne la gestion des mots de passe et la vigilance face aux courriels frauduleux. Toutefois, certains écarts entre perception et pratique subsistent dans les deux groupes. Par exemple, **bien que la majorité des répondants déclarent utiliser des mots de passe sécurisés et ne pas les partager, les tests d'hameçonnage ont révélé que certains comportements ne sont pas toujours cohérents avec ces déclarations**.

L'étude met également en lumière plusieurs discordances entre perception et pratique. **Les employés, bien que plus sensibilisés, n'appliquent pas toujours les bonnes pratiques de manière constante**. Les étudiants, de leur côté, souffrent d'un manque de sensibilisation et de connaissances suffisantes.

## Recommandations

Pour améliorer la cyber-hygiène dans les milieux universitaires, il est recommandé d'adapter les programmes de formation **en intégrant des théories comportementales comme le modèle KAB** (Maennel et al., 2018). Il est essentiel de promouvoir une culture organisationnelle qui encourage les bonnes pratiques, en impliquant davantage les gestionnaires et en favorisant des campagnes de sensi-

-bilisation innovantes et interactives (Reeves et al., 2021). De plus, **la réalisation de tests réguliers, comme des simulations d'hameçonnage, permettrait d'évaluer les progrès et d'identifier les domaines à améliorer**.

En conclusion, cette recherche met en évidence les défis liés à la cyber-hygiène dans les milieux universitaires et propose des pistes pour renforcer la cybersécurité. Les universités doivent prioriser la protection des données tout en sensibilisant efficacement leurs communautés. En adoptant des approches équilibrées entre technologie et facteur humain, il est possible de réduire les risques liés aux cyberattaques et de créer un environnement plus sécurisé pour tous (Chapman, 2019 ; Cheng & Wang, 2022).

## Le modèle KAB (Knowledge-Attitude-Behavior)

Le modèle KAB (*Knowledge-Attitude-Behavior*), ou modèle Connaissances-Attitudes-Comportements, est un cadre théorique utilisé pour **analyser et expliquer la relation entre les connaissances d'un individu, ses attitudes et ses comportements**. Il est souvent appliqué dans des domaines comme la santé publique, la cybersécurité et l'éducation pour comprendre comment les connaissances influencent les actions des individus.

Composantes du modèle KAB :

- **Connaissances** (*Knowledge*): ce qu'un individu sait sur un sujet donné. Par exemple, en cybersécurité, cela inclut la compréhension des menaces comme l'hameçonnage ou l'importance des mots de passe sécurisés.
- **Attitudes** (*Attitude)*: l'état d'esprit ou les croyances qu'un individu développe à partir de ses connaissances. Par exemple, quelqu'un qui sait que les cyberattaques sont fréquentes peut développer une attitude de méfiance vis-à-vis des courriels inconnus.
- **Comportements** (*Behavior*): les actions concrètes prises par un individu en fonction de ses connaissances et attitudes. Dans le cas de la cybersécurité, cela peut se traduire par l'adoption de mots de passe forts, l'utilisation d'un VPN ou la vérification des expéditeurs de courriels.

Le modèle KAB permet d'identifier **où se situent les blocages entre la sensibilisation et l'action**. Si les connaissances existent mais que les comportements ne suivent pas, cela peut indiquer un problème d'attitude (ex. perception d'un faible risque) ou des obstacles pratiques (ex. manque d'outils). Il est donc utilisé pour concevoir des campagnes de sensibilisation plus efficaces en cybersécurité.

## Références

Borgman, C. L. (2018). Open Data, Grey Data, and Stewardship: Universities at the Privacy Frontier. B*erkeley Technology Law Journal*, *33*(2), 365–412

Chapman, J. (2019). How safe is your data? Cyber-security in higher education. *HEPI Policy Note 12*. Higher Education Policy Institute.

Cheng, E. C. K. & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information Technologies in Education, Research and Innovation*, *13*(4), 1-14.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151-156.

Ncubukezi, T. & Mwansa, L. (2021). Best Practices Used by Businesses to Maintain Good Cyber Hygiene During Covid19 Pandemic. *Journal of Internet Technology and Secured Transactions*, *9*(1), 714–721.

Reeves, A., Delfabbro, P. & Calic, D. (2021). Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *Sage Open*, *11*(1), 21582440211000050.

Singh, D., Mohanty, N. P., Swagatika, S. & Kumar, S. (2020). Cyber-hygiene: The key concept for cyber security in cyberspace. *Test Engineering and Management*, *83*, 8145-8152.

Stephenson, A. (2023, 24 juillet). Cybercrime costs Canadian companies millions even as awareness grows: report. *Global News*.

Tempestini, G., Rovira, E., Pyke, A. & Di Nocera, F. (2023). The Cybersecurity Awareness INventory (CAIN) : Early Phases of Development of a Tool for Assessing Cybersecurity Knowledge Based on the ISO/IEC 27032. *Journal of Cybersecurity and Privacy*, *3*(1), 61-75.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G. & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, 128.

Le travail dirigé complet est disponible à la demande. Contactez info@prevention-cybercrime.ca