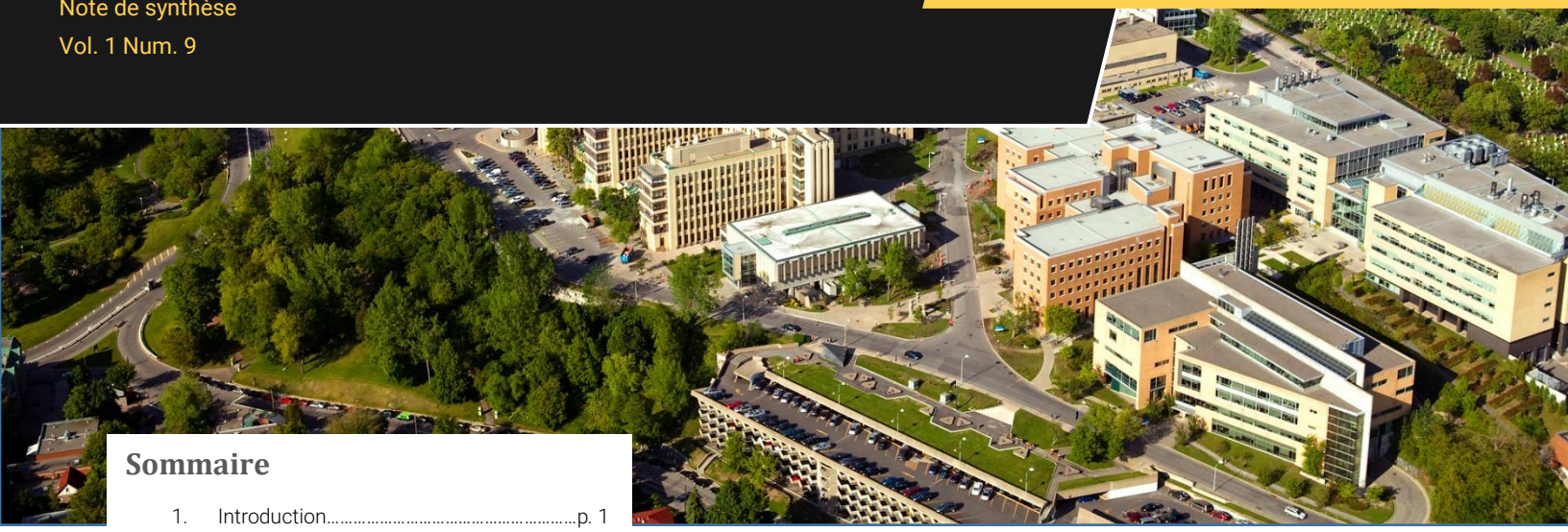
# Sensibilisation à la cybersécurité et facteurs sociodémographiques

Fyscillia Ream

Note de synthèse
Vol. 1 Num. 9

CRPC | Chaire de recherche en prévention de la cybercriminalité



## Sommaire



## Introduction

Les organisations et gouvernements s'appuient de plus en plus sur les nouvelles technologies et, le besoin de protéger adéquatement leurs informations et données est devenu un enjeu critique, créant une augmentation importante des dépenses en outils et innovation technologiques. Cependant, ils occultent souvent l'un des principaux facteurs de risque pesant sur la sécurité de l'information: les utilisateurs. Au sein des organisations, les employés sont souvent perçus comme étant le maillon faible de la chaîne de sécurité[1]. Cependant, cette désignation occulte le fait que les employés d'une entreprise peuvent être la ressource la plus importante pour lutter contre les cybermenaces, ce qui amène à penser la sécurité de l'information comme un problème humain - avec une solution humaine - plutôt que technologique[1].

À la fin de l'année 2019, la main d'œuvre canadienne représentait environ **19 000 000 personnes** en emploi soit **47% de femmes** et **53% d'hommes**. **13% étaient âgés de 15 à 24 ans, 65% de 25 à 54 ans et 22% de 55 ans et plus**[2].

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.


Il est important de considérer **le potentiel impact des facteurs sociodémographiques sur la sensibilisation à la cybersécurité** car cela peut mettre en lumière les mécanismes sous-jacents pouvant se répercuter la responsabilisation de l'utilisateur en regard de la sécurité de l'information.

**Le genre et l'âge** sont les principales caractéristiques individuelles définissant l'appartenance des individus à un groupe et, qui est susceptible **d'avoir une influence profonde sur les perceptions, les attitudes et les performances individuelles**[3].

D'autres caractéristiques telles que le niveau d'éducation le revenu annuel moyen, la position hiérarchique dans l'organisation peuvent aussi apparaître comme des facteurs individuels déterminants quant à la sensibilisation à la cybersécurité.

Cependant la majorité des études qui ont prêté attention aux facteurs sociodémographiques ne s'est intéressée qu'au genre et à l'âge. Il y a plus d'études sur ces deux facteurs.

## L'âge

Le milieu du travail s'appuie de plus en plus sur les outils technologiques et les organisations demandent de plus en plus à ce que leurs employés puissent maitriser l'informatique ou du moins, soient capables d'utiliser un ordinateur.

**L'âge est un facteur démographique d'intérêt dans les études sur le comportement des employés vis-à-vis des nouvelles technologies**. Les employés les plus jeunes ont souvent eu plus l'opportunité de développer des compétences informatiques que ceux plus âgés (par exemple à l'école). Les changements physiologiques et psychologiques peuvent aussi désavantager les plus âgés quant à leur capacité à utiliser les outils informatiques (par exemple, porter des verres bifocaux peut rendre difficile l'utilisation d'un clavier combiné avec un écran)[4].

Les études sur la cybersécurité s'intéressant aux différences d'âge sont de diverses natures. En ce qui concerne la **victimisation en ligne**, certaines études montrent que **les utilisateurs plus âgés (+ de 50 ans) sont moins aptes à prévenir et à éviter des incidents de cybersécurité** suivi par les plus jeunes (- de 21 ans)[5]. Une autre étude[6] montre quant à elle **qu'il n'existe pas de différence significative entre les catégories âges** en ce qui concerne le vol d'identité, alors qu'une autre[7] montre que les plus jeunes sont plus susceptible d'en être victime. Concernant l'hameçonnage, les **18-25 ans** seraient plus susceptibles d'en être victime que les groupes plus âgés[8].

En ce qui concerne **le comportement en ligne**, **les plus jeunes auraient plus tendance à partager leurs mots de passe** et ce, parce qu'ils accéderaient à moins d'informations confidentielles en ligne (par exemple, un compte bancaire, un compte chez un fournisseur d'électricité ou d'internet, etc.)[9] [10].

Certaines études sur **le comportement des employés** montrent que les adultes plus âgés sont plus interpellés par les campagnes de sensibilisation à la cybersécurité que les jeunes adultes[11]. En outre, **plus les individus prennent de l'âge, plus ils étaient sensibilisés**. Cela peut s'expliquer par le fait que les personnes plus âgées sont davantage conscientes des risques et des limites de leurs capacités à assurer leur sécurité[12]. De même, **les employés plus jeunes ont des comportements plus risqués en ligne**[13] **alors que les employés les plus âgés se conforment plus aux politiques de sécurité**[14]. Les personnes plus jeunes sont davantage familières avec les outils et le maniement informatique et font peut-être preuve de plus d'insouciance face à leur protection ou surestiment leur capacité à identifier et éviter les risques en ligne.

## Le genre

**Le genre est l'un des facteurs sociodémographiques qui a probablement le plus d'influence sur les perceptions, les attitudes et la performance d'un individu**[15]. Néanmoins, cette influence peut être modérée par d'autres facteurs (par exemple, la classe sociale ou l'ethnicité)[16].

En ce qui concerne la **victimisation en ligne**, les hommes seraient plus à risque d'être victime de vol d'identité[7] et les femmes seraient principalement victimes de cyber harcèlement[17]. Une étude sur l'hameçonnage a montré que **les femmes seraient plus susceptibles de cliquer sur des liens ou ouvrir des courriels frauduleux**[8] alors qu'une autre étude[18] a déterminé qu'**il n'existe pas de différence de genre**.

De manière générale, les études sur la victimisation en relation avec le genre varient, certains auteurs estimant qu'il n'y a aucun impact[19] tandis que d'autres estiment qu'il existe une corrélation entre le genre la susceptibilité d'être victime- les femmes seraient plus à même de cliquer sur des liens douteux[8]. Une étude ayant étudié l'effet de genre dans une population démontre quant à elle **que la susceptibilité d'être victime est inversement proportionnelle**[20]**, c'est-à-dire que plus le pourcentage de femmes dans la population augmente, plus la susceptibilité d'être victime diminue**. Comme on le voit, il n'existe pas de certitudes sur l'influence que le genre exerce dans ce domaine et les résultats restent contradictoires.

Concernant **la perception du risque en ligne**, **les femmes seraient plus préoccupées** par ce dernier[21]. Les femmes et les hommes peuvent percevoir les mêmes risques différemment ou percevoir différents risques[16].

Pour ce qui est **des pratiques de sécurité en ligne**, **les hommes déclarent avoir un comportement plus sécurisé comparativement aux femmes** mais ce résultat doit être tempéré par le fait que les hommes font souvent trop confiance en leurs capacités. En effet, **les hommes ont de plus faibles intentions de conformité à la sécurité car ils s'estimeraient plus aptes à bien se protéger par eux-mêmes**[23], ce qui peut en soi constituer un facteur de risque non négligeable.

En outre, **les femmes expriment plus d'inquiétude face au maintien de la vie privée en ligne**[24] car elles voient leurs actions plus à risques et elles ont tendance à suivre avec plus de rigueur les recommandations de sécurité[25].

De même, dans une étude sur **la sensibilisation à la sécurité de l'information**, les résultats ont montré **une légère différence entre les hommes et les femmes, ces dernières étant plus sensibilisée aux mesures de sécurité que les hommes**[11]. Par contre, les femmes font moins de mises à jour des logiciels et adoptent des mots de passe moins sûrs[9].

En revanche, **d'autres études n'ont pas trouvé de différence entre les hommes et les femmes au niveau des pratiques de sécurité en ligne**[26] **ou au niveau du respect de politiques de sécurité**[27]. Ces différences de résultats peuvent s'expliquer par les méthodologies employées dans ces études. En ce qui concerne les études sur les mises à jour et l'adoption de mots de passe sûrs, ces études se sont appuyées sur des données auto-rapportées, c'est-à-dire que les participants ont eu à remplir un sondage et à évaluer eux-mêmes leurs capacités et

leurs habitudes en ligne[9] [26]. Par contre, l'étude sur le respect des politiques de sécurité s'est quant à elle appuyée sur des scénarios hypothétiques. Les participants ont été confrontés à plusieurs scénarios de violation des politiques de sécurité et ils ont eu à évaluer leur conformité en regard de ces scénarios[27].

## Autres facteurs

Parmi les autres facteurs sociodémographiques pour lesquels nous disposons d'études, on peut noter le **niveau d'éducation** et **la position hiérarchique dans l'organisation**.

Dans une étude sur les comportements de sécurité auto-rapportés, les résultats ont montré qu'il **n'existe pas de différence de comportements selon le niveau d'éducation des employés**[13].

En ce qui concerne **la position hiérarchique** au sein de l'organisation, **le niveau de sensibilisation à la cybersécurité décroit selon la position hiérarchique des employés**. Les gestionnaires les plus haut placés auraient un niveau moyen de sensibilisation et effectueraient les actions de base de sécurité. **Plus le niveau hiérarchique descend, plus le niveau de sensibilisation baisse avec des employés tout en bas de l'échelle qui négligent les actions de base**. Cette étude conclut qu'il existe des problèmes de communication de l'information entre les gestionnaires et les employés et ce, parce que les gestionnaires occultent le facteur humain de la sécurité de l'information (c'est-à-dire ne prennent pas en considération les employés qui doivent appliquer les mesures de sécurité)[28].

## Conclusion et recommandations

Les études empiriques qui tiennent compte des facteurs sociodémographiques **ne sont pas concluantes, ayant souvent des résultats divergents**.

Toutefois, ces études recommandent de **continuer à prendre en compte les différences individuelles lors de la mise en œuvre de programmes de sensibilisation**. En effet, lors de l'évaluation de ces programmes, il se peut que des différences apparaissent selon les caractéristiques individuelles et cela est important pour comprendre comment et pourquoi les utilisateurs font des choix différents en ce qui a trait à la sécurité de l'information. **La formation et les interventions devraient être ciblées de manière appropriée pour garantir la conformité de tous les groupes d'utilisateurs aux politiques de sécurité**. Les programmes de formation pourraient être adaptés pour mettre l'accent sur les facteurs qui sont importants pour chaque groupe[3].

En outre, **les programmes de sensibilisation devraient prendre en compte la position hiérarchique et les connaissances des utilisateurs**. Il existe plusieurs niveaux hiérarchiques dans une organisation et avec eux, des tâches et responsabilités différentes. Certaines de positions ne requièrent pas de gérer des informations qui peuvent s'avérer cruciales pour l'organisation. Ces utilisateurs n'ont donc pas besoin d'une formation approfondie. De plus, les utilisateurs doivent être regroupés en fonction de leurs connaissances techniques. Les utilisateurs ayant des connaissances techniques avancées devraient être formés en profondeur, tandis que les autres devraient d'abord suivre une formation de base [28].

## Références

[1] Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S. Chen, Q. et Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior*, *84*, 375-382.

[2] Statistique Canada. Tableau 14-10-0287-01 *Caractéristiques de la population active, données mensuelles désaisonnalisées et la tendance-cycle, 5 derniers mois.*

[3] Morris, M. G., Venkatesh V. et Ackerman, P. L. (2005). Gender and Age Differences in Employee Decisions About New Technology: An Extension to the Theory of Planned Behavior. *IEEE Transactions on Engineering Management*, *52*(1), 69-84.

[4] Westerman, S. J et Davies, D. R. (2000). Acquisition and application of new technology skills: the influence of age. *Occup. Med.*, *50*(7), 478-482.

[5] Koyuncu, M. et Pusatli, T. (2019). Security awareness level of smartphone users: An exploratory case study. *Mobile Information Systems*, 2019, 1-11.

[6] Pratt, T. C., Holtfreter, K. et Reisig, M. D. (2010). Routine online activity and Internet fraud targeting: Extending the generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

[7] Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238.

[8] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F. et Downs, J. (2010). Who Falls For Phish?: A Demographic Analysis Of Phishing Susceptibility

And Effectiveness Of Interventions. *Proceedings Of The Sigchi Conference On Human Factors In Computing Systems*, 373-382.

[9] Gratian, M., Bandi, S., Cukier, M., Dykstra, J. et Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345-358.

[10] Whitty, M., Doodson, J., Creese, S. et Hodges, D. (2015). Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3-7.

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

[12] Williams, F. P., McShane, M. D. et Akers, R. L. (2000). Worry About Victimization: An Alternative and Reliable Measure for Fear of Crime. *Western Criminology Review*, *2*(2), 1-26.

[13] Pattinson, M., Butavicius, M. Parsons, K., McCormac, A. et Calic, D. (2015). Factors that Influence Information Security Behavior: An Australian Web-Based Study. Dans, I. Askoxylakis et T. Tryfonas (dir.), *Human Aspects of Information Security, Privacy, and Trust* (p. 231-241). Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015.

[14] D'Arcy, J. et Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Inf. Manage. Comput. Secur.*, *22*(5), 474–489.

[15] Nosek, B. A., Banaji, M. et Greenwald, A. G. (2002). Harvesting implicit group attitudes and beliefs from a demonstration web site. *Group Dynamics: Theory, Research, and Practice*, *6*(1), 101.

[16] Gustafson, P. E. (1998). Gender Differences in Risk Perception: Theoretical and Methodological Perspectives. *Risk Analysis*, *18*(6), 805-811.

[17] Li, Q. (2007). New bottle but old wine: A research of cyberbulling in schools. *Computers in Human Behavior*, *23*(4), 1777-1791.

[18] Butavicius, M., Parsons, K., Pattinson, M., McCormac, A., Calic, D. et Lillie, M. (2017). Understanding susceptibility to phishing emails: assessing the impact of individual differences and culture. *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security and Assurance*, 12–23.

[19] Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin E. et Wagner, D. (2012). Android Permissions: User Attention, Comprehension, and Behavior. *Symposium on Usable Privacy and Security (SOUPS)*, July 11-13 2012, Washington, DC, USA.

[20] Garg, V. et Niliadeh, S. (2013). Craigslist Scams and Community Composition: Investigating Online Fraud Victimization. *2013 EEE Security and Privacy Workshops*, 123-126.

[21] Eckel, C. C. et Grossman, P. J. (2008). Men, Women And Risk Aversion: Experimental Evidence. *Handbook Of Experimental Economics Results*, *1*(1), 1061-73.

[22] Anwar, M., He, W., Ash, I., Yuan, X. Li, L. et Xu, L. (2017). Gender Difference and Employees' Cybersecurity Behaviors. *Information Technology & Decision Sciences Faculty Publications*, 13.

[23] Ifinedo, P. (2012). Understand information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

[24] Hoy, M. G. et Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, *10*(2), 28-45.

[25] Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

[26] Ngo, T. F. et Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational-level factors. *International Journal of Cyber Criminology*, *5*(1), 773-793.

[27] Vance, A., Siponen, M. et Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*, 190-198.

[28] Papagiannakis, K. (2011). *An overview of the current level of Security Awareness in Greek companies* (Mémoire de maitrise, Erasmus University of Rotterdam). Rotterdam, Pays-Bas.