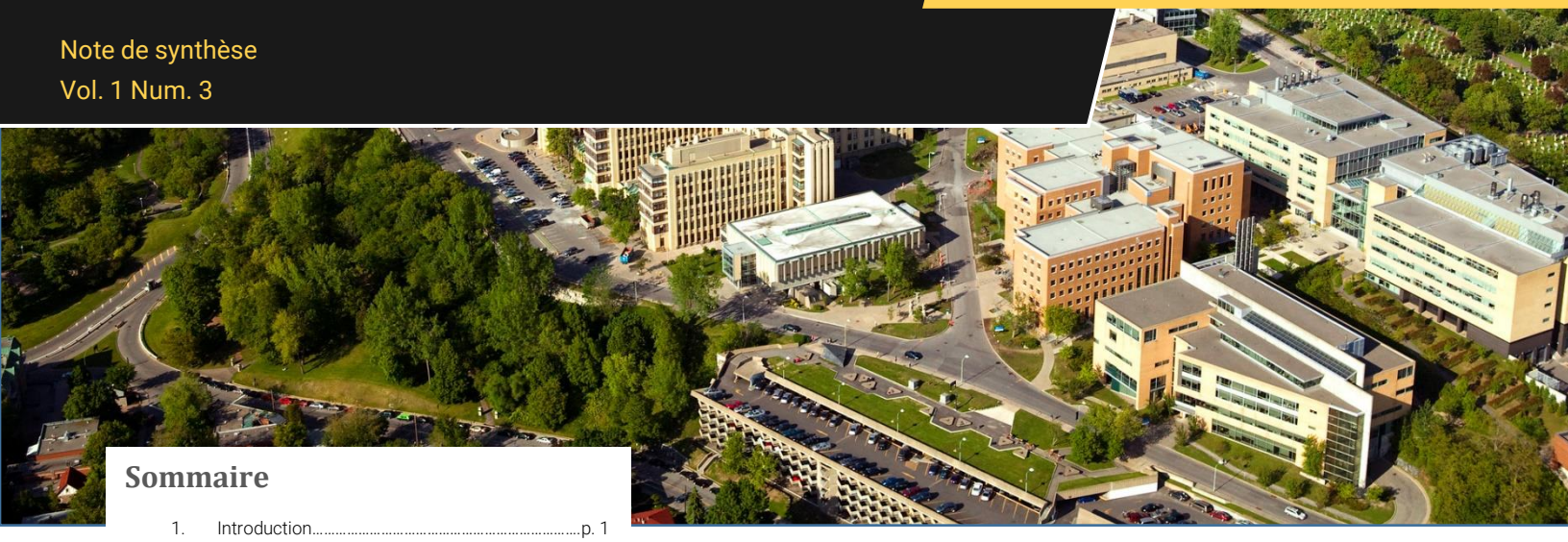
Les programmes de formation en cybersécurité

Adeline Veyrinas, candidate à la maîtrise

CRPC | Chaire de recherche en prévention de la cybercriminalité

Note de synthèse
Vol. 1 Num. 3



Sommaire

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.

Introduction

Selon Statistique Canada[1], **21% des entreprises canadiennes ont été touchées par un incident de cybersécurité en 2017, dont 23% concernaient un vol ou une tentative de vol de données personnelles ou financières**[2]. Ce type de cybercriminalité entraîne des pertes monétaires et réputationnelles majeures[3]. Par exemple, les entreprises de services monétaires ont rapporté des répercussions en termes de contretemps sur les activités quotidiennes des employés (71%) ou sur l'utilisation de ressources (75%), voire une perte de revenus (51%).

Le facteur humain dans la prévention des menaces virtuelles est un défi important pour les entreprises canadiennes. En 2018, 34% des brèches de données seraient dues à des acteurs internes aux entreprises et 33% d'entre elles avaient été menées via des attaques d'ingénierie sociale qui visaient des employés[4 5 6].

Il convient alors de se pencher sur les besoins des entreprises en prévention des pertes de données : quelles sont leurs priorités quant au facteur humain, élément central de certains cyber-incidents ? Cette note de synthèse établit un cadre concret de la situation actuelle des entreprises afin de dégager les principales solutions proposées dans la littérature tout en exposant les améliorations qui pourraient être apportées. Finalement, des implications pratiques applicables aux entreprises seront proposées.

Les besoins des entreprises en prévention des pertes de données

Bien que les entreprises privilégient les solutions techniques pour sécuriser leurs systèmes, il semblerait que le principal facteur des fuites de données confidentielles en leur sein soit humain, c'est-à-dire le comportement de leurs employés[7]. Ainsi, en 2019, l'hameçonnage serait le principal responsable des brèches de données d'entreprises américaines[6 8 9].

Un problème majeur en matière de prévention de ce type d'incident est que, bien que les règles internes soient connues des employés, ces derniers ne les appliquent que très rarement, voire pas du tout[10 11 12 13].

Deux principales méthodes ont été mises en avant afin de permettre aux individus d'adopter des comportements sains en gestion de l'information : **la sensibilisation** et **la formation**[14]. Bien qu'elle permette d'éveiller l'attention et la responsabilisation des individus aux cyber-risques, la sensibilisation ne suffirait pas à elle seule à leur faire adopter des comportements sécuritaires en la matière[7]. La formation, quant à elle, fournit des compétences particulières afin d'être capable de prévenir les menaces lorsqu'elles surviennent[55] Cette méthode est souvent considérée comme la meilleure mesure préventive des menaces en sécurité de l'information en raison de sa dimension implicative[15 16].

Les formations en sécurité de l'information se différencient principalement selon leurs approches individuelles ou collectives[17], chacune d'entre elle ayant démontré des intérêts différents mais complémentaires en sensibilisation et adoption de comportements sécuritaires de l'information.

Les méthodes de formation en prévention de la sécurité de l'information

Une approche collective : le groupe de collaboration

Le groupe de collaboration est un type de formation pertinent en matière de sensibilisation et de changement de comportement. Il s'agit d'ateliers de petite taille et de courte durée à un niveau local (par exemple, des employés de même statut/rôle dans l'entreprise). Ces ateliers sont généralement dispensés par un instructeur « expert » sur un sujet et impliquent des échanges entre collègues à travers des modules de réflexion collectifs sur un thème donné[18 19 21].

Le groupe de collaboration est considéré comme un type de formation des plus efficaces parmi les différentes méthodes de sensibilisation et de formation à la sécurité de l'information et ce, en raison de l'intégration de théories psychologiques de changement comportemental[20] telles que les **normes subjectives** et la **participation active**.

Susciter l'implication et la motivation des individus : la participation active

Les groupes de collaboration incluant des ateliers de réflexion collective favorisent l'**implication des participants**.

Cet élément est important dans l'adoption de comportements selon plusieurs théories telles que la **Buy-in Theory of Participation** et la **Théorie de la Participation**. Selon ces théories, plus le niveau d'engagement et d'influence d'un individu sur un phénomène est élevé, plus il le perçoit comme étant personnellement important et pertinent. L'individu aurait ainsi tendance à adopter des attitudes et comportements en accord avec ce phénomène et à augmenter sa participation dans des activités reliées[3 21].

Ainsi, les dimensions participatives de ces groupes (partage de connaissances, collaboration/réflexion collective, intervention) permettraient :

- D'**adopter des solutions efficaces** à travers la réflexion collective active en se basant sur les éléments de l'espace mental (MINDSPACE) [22] [23] [24];

- **D'augmenter sa compréhension et la perception de sa responsabilité** en prévention des risques par le biais de l'expérience de réflexion personnelle et de recherche de solutions en la matière[30];

- D'amener à un **changement d'attitude** et de comportement vis-à-vis de la sécurité de l'information en raison de l'investissement demandé[7] [33].

Susciter une attitude positive : confiance relationnelle

À travers les échanges et la réflexion collective, les groupes de collaboration amèneraient les employés à adopter une attitude positive envers les comportements sécuritaires. Le **respect des normes sociales**[25] serait l'élément qui contribuerait à cette adhésion collective. Plusieurs théories de changement comportemental évoquent cette notion telles que :

- La **Théorie du Lien Social** qui explique le comportement des individus à travers les relations qu'ils entretiennent avec leurs pairs : plus ils s'impliquent dans des activités et comportements définis avec ceux-ci, moins ils ont tendance à déroger[3];

- La **Théorie du Comportement Planifié** qui s'appuie sur la notion de normes subjectives/personnelles[26] afin d'expliquer comment un individu détermine son intention d'adopter un comportement désigné[27] [28] [29];

- La théorie du **Modèle de la Probabilité d'Elaboration** qui s'appuie sur l'existence d'arguments persuasifs afin de faire intégrer et accepter certaines informations à des individus[13].

L'échange des différents points de vue entre les employés, l'analyse des attentes de tous et chacun, ainsi que la transmission des connaissances via les interactions tendent à la création d'un **lien social** ou de confiance, qui est une base pour l'adoption de comportement spécifique[30].

Ce lien social permettrait notamment :

- **D'accroître sa compréhension** sur un sujet donné grâce à un échange actif entre des individus présentant un niveau semblable de connaissances[30] [31];

- **D'intensifier sa sensibilisation et ses connaissances** à travers le transfert de connaissances par les échanges entre collègues et avec l'instructeur[30] [32];

- **De motiver les individus à modifier leurs comportements** en étant impliqués dans un processus collectif de promotion de comportements sécuritaires de l'information[30].

En somme, à travers le concept d'**interdépendance positive**[32], le groupe de collaboration s'appuie principalement sur le principe d'**apprentissage collaboratif** selon lequel les individus travaillant ensemble à la réalisation d'une activité commune bénéficient d'un soutien social pour comprendre, intégrer (se responsabiliser) et se motiver à atteindre les objectifs de celle-ci[33] [34] [40].

Cette approche présente toutefois certaines limites qu'il convient de ne pas oublier dans l'hypothèse d'une opérationnalisation. Ce type de formation :

- Est **coûteux** en termes de ressources temporelles[18] [19], financières et humaines et nécessite une importante préparation quant à l'identification des besoins prioritaires de l'entreprise en matière de prévention de la cybercriminalité. Il faudrait que des analyses soient réalisées en amont afin de faire ressortir les points sur lesquels les formations devraient porter.

- Nécessite d'être mis en place de manière pérenne et répétée sur le temps afin d'être intégrée par les utilisateurs et permettre le(s)

changement(s) d'attitude et/ou comportement souhaité(s);

- Est difficile à évaluer en termes d'efficacité en raison de l'aspect qualitatif de la formation, ce qui nécessite des outils de mesure adaptés et dont les effets doivent être mesurés sur la durée[19 35].

Une approche individuelle : la formation sur ordinateur

La deuxième méthode d'apprentissage est la **formation sur ordinateur (FSO)** (*computer-based training*) qui présente l'avantage de permettre aux utilisateurs de suivre un apprentissage interactif adapté à leurs besoins et à leur rythme et ce, à faibles coûts[36].

La ludification pour obtenir l'attention des individus

Les FSO, s'inspirant des principes du jeu, sont considérées comme étant particulièrement pertinentes dans l'éveil de l'intérêt chez les individus (en termes de socialisation, d'objectif à atteindre, de système de récompenses et de punitions, d'identification de comportements «vitaux»[37], etc.). Les «jeux sérieux»[38] permettraient d'impliquer les employés dans les formations qu'ils suivent en les plongeant dans monde virtuel engageant[39 40 41 42].

Ce type d'apprentissage trouve son origine dans les théories de la motivation, dont la **Théorie de l'Auto-Détermination**. Cette théorie se fonde sur la notion de **motivation intrinsèque** pour expliquer les agissements des individus largement dirigés par le plaisir et la satisfaction personnelle. Elle permet d'expliquer comment le jeu entraînerait une attitude favorable et l'intention d'adopter un comportement particulier[43 44].

Augmenter la perception de sa capacité de réussite à travers la simulation

Les FSO s'appuient également sur la simulation de scénarios de cybercriminalité en mettant en avant l'engagement et l'implication à travers l'interactivité avec des situations réalistes.

Cela permet notamment aux utilisateurs d'évaluer leurs aptitudes en la matière tout en :

- **Améliorant leurs connaissances et compétences** en s'entraînant à reconnaître les indices d'un cas de cybercriminalité[45];
- **Comprenant l'impact de leurs décisions** à travers le retour rapide sur l'expérience et donc les résultats de leur apprentissage[46];
- **Améliorant la perception de leur auto-efficacité**[47] à travers l'expérience de situations réalistes de prévention des risques d'une menace désignée.

La simulation repose sur des théories liées à la notion d'auto-efficacité, telles que :

- La **Théorie Sociale Cognitive** qui s'appuie sur des expériences réussies de résolution de problèmes. Ainsi, l'intention d'adopter un comportement serait influencée par les conséquences perçues des actions passées en la matière (impact positif pour l'individu, difficultés rencontrées, etc.)[48];
- La **Théorie de la Protection-Motivation** qui se base sur l'analyse d'une situation de menace afin de déterminer son intention d'engager une action. L'individu va évaluer sa capacité à éviter l'occurrence de ladite menace (auto-efficacité) et effectuer un calcul coûts-bénéfices des résultats du comportement qu'il aura à adopter pour cela[49 50]. En somme, il doit pouvoir estimer qu'il est capable de remédier à ce danger et qu'il y gagnera plus qu'il n'y perdra à le faire.

Les FSO sont pertinentes car elles permettent aux utilisateurs de se placer dans une situation réelle de cybercriminalité, de prendre position, de connaître les conséquences de leurs actions et de savoir s'ils ont la capacité d'adopter les comportements demandés. Ces avantages s'expliquent par la perception du sentiment contrôle face aux menaces[24].

Une formation adaptable aux différents profils d'individus

La FSO est une méthode qui présente l'avantage de permettre aux utilisateurs de suivre un apprentissage individualisé à travers :

- Le **contrôle de la durée des sessions** de formation[23];
- Les **différents scénarios/sujets proposés** en fonction de la position hiérarchique de l'utilisateur dans l'entreprise et de ses connaissances pré-acquises[15];
- L'**élaboration de ses propres scénarios** de cyberattaque/cybersécurité pour coïncider avec ses besoins personnels[51];
- L'**accès à de l'information en de multiples formats** (texte, audio, vidéo) simultanément et facilement commutables pour s'adapter aux différents types de réceptivité[52 53].

Cependant, la FSO présente des limites qui doivent être considérées dans l'éventualité de sa mise en oeuvre:

- Il s'agit d'une **approche auto-formatrice** qui ne permet pas aux utilisateurs de communiquer avec un instructeur pour poser des questions ou obtenir des informations supplémentaires[47 51 54 55];
- Le **support informationnel riche** et le **format complexe** peuvent entraîner une surcharge cognitive[56] et annuler l'effet désiré, c'est-à-dire la rétention durable de ce qui aura été appris durant la formation[45 46 53];
- Les **« jeux sérieux », adaptés à une clientèle adulte** et/ou d'employés d'entreprises et assez élaborés pour fournir le niveau d'apprentissage nécessaire sans être trop complexes sont plutôt **rares**[57];
- Ce type de formation nécessite des **mises à jour régulières** en fonction de l'évolution des technologies et donc des menaces en cybercriminalité[58].

Implication pratiques pour la prévention des pertes de données

Les deux méthodes présentées ici proposent des éléments permettant aux entreprises de sensibiliser leurs employés à la sécurité de l'information et de leur faire adopter des comportements sécuritaires et respectueux des politiques de sécurité (cf. tableau en annexe pour un récapitulatif).

Plusieurs points importants sont à retenir pour la promotion de l'adoption de comportements sécuritaires de l'information:

- S'assurer que les employés comprennent la nécessité de l'adoption de tels comportements, par exemple en leur montrant les conséquences de leurs actions[13 59 60 61];
- Combiner les formations avec des campagnes de sensibilisation continues afin que les employés puissent se souvenir des grandes lignes de ce qu'ils ont appris lors des formations[30 62];
- Proposer du matériel visuel, des phrases courtes et du contenu simple afin que cela soit facile à comprendre et à retenir[31 63 64];
- Motiver les employés à réaliser une tâche/activité plutôt que de l'imposer, afin de faciliter l'intégration des comportements encouragés lors de celle-ci[3 13 31];
- Fournir un soutien organisationnel à ces formations en encourageant les comportements mis en avant par celles-ci, par exemple via un communiqué sur l'intranet de l'entreprise ou l'adoption visible de ces comportements par les gestionnaires[3 13];
- Fournir un retour immédiat aux employés sur leur processus d'apprentissage afin qu'ils puissent ajuster leurs conduites et connaissances à cet égard[23 31 60].

Améliorer l'évaluation des programmes de formation et de sensibilisation

Malgré les informations précédemment mentionnées, en raison d'un manque de données empiriques sur la performance de ces programmes de formation, il est difficile d'établir des résultats pertinents en termes d'efficacité de ces programmes. Il existe de nombreuses propositions de méthodes de formation mais rares sont les études qui ont réalisé une analyse.

En outre, il existe un déficit concernant l'évaluation même de ces programmes et de l'impact de leur mise en place sur les destinataires (les employés et leurs entreprises), permettant d'évaluer l'effet sur la sensibilisation et les comportements des individus visés notamment sur leur efficacité à long terme et à leur conformité aux objectifs initiaux[8] [65] [66].

Ces formations manquent d'analyses quant à leurs effets et leur opérationnalisation concrète dans les entreprises[27] [67] [68] [69].

Les rares études qui évoquent l'évaluation des programmes sur lesquels elles portent se cantonnent à une présentation des retours d'expérience de la part des utilisateurs, c'est-à-dire une évaluation subjective à court terme. Il y a donc encore beaucoup d'améliorations à apporter dans l'évaluation des programmes de sensibilisation à la cybersécurité[27].

Références

[1] Parmi les entreprises ayant répondu à une enquête réalisée par Statistique Canada en 2017.
[2] Statistique Canada. (2017). L'incidence du cybercrime sur les entreprises canadiennes, 2017.
[3] Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. *Computers & Security*, *56*, 70-82.
[4] Technique visant à tromper un individu afin de l'amener à transmettre des données confidentielles.
[5] Parmi les entreprises ayant transmis leurs données en matière d'incidents de données à Verizon en 2018.
[6] Verizon. (2019). 2019 Data Breach Investigations Report.
[7] Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133.
[8] Fait d'envoyer un courriel frauduleux à un individu pour l'inciter à cliquer sur un lien.
[9] Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2013). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, *12*(1), 28-38.

[10] Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, *26*(4), 276-289.

[11] Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, *68*, 145-159.

[12] Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, *61*, 46-58.

[13] Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133.

[14] Voir les programmes « Security Education Training and Awareness » (SETA).

[15] Aldawood, H., & Skinner, G. (2018, December). Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)* (pp. 62-68).

[16] Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS quarterly*, 757-778.

[17] McIlwraith, A. (2016). *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Routledge.

[18] Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, *29*(4), 432-445.

[19] Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies–A case study. *Information security technical report*, *14*(4), 223-229.

[20] Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862-10868.
[21] Ottis, R. (2014). Light weight tabletop exercise for cybersecurity education. *Journal of Homeland Security and Emergency Management*, *11*(4), 579-592.

[22] Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014, June). Scene: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In *International conference of design, user experience, and usability* (pp. 229-239). Springer, Cham.

[23] Dolan, P., Hallsworth, M., Halpern, D., King, D., & Vlaev, I. (2010). MINDSPACE: influencing behaviour for public policy. *Institute for Government*.

[24] Turland, J., Coventry, L., Jeske, D., Briggs, P., & van Moorsel, A. (2015, July). Nudging towards security: Developing an application for wireless network selection for android phones. In *Proceedings of the 2015 British HCI conference* (pp. 193-201). ACM.

[25] Conduites à adopter dans un groupe donné.

[26] Croyances d'un individu quant aux normes sociales et aux attentes de ses pairs relativement à l'adoption du comportement.

[27] Banfield, J. M. (2016). *A study of information security awareness program effectiveness in predicting end-user security behavior* (Doctoral Dissertation).

[28] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

[29] Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

[30] Konak, A., & Bartolacci, M. R. (2016). Using a virtual computing laboratory to foster collaborative learning for information security and information technology education. *Journal of Cybersecurity Education, Research and Practice*, *2016*(1), Article 2.

[31] Inayat, I., ul Amin, R., Inayat, Z., & Salim, S. S. (2013). Effects of collaborative web based vocational education and training (VET) on learning outcomes. *Computers & Education, 68, 153-166*

[32] Principe selon lequel pour succéder de manière individuelle, les individus doivent réussir en groupe.

[33] Laal, M., & Ghodsi, S. M. (2012). Benefits of collaborative learning. *Procedia-social and behavioral sciences*, *31*, 486-490.

[34] Laal, M. (2013). Positive interdependence in collaborative learning. *Procedia-Social and Behavioral Sciences*, *93*, 1433-1437

[35] Roberts, T. S. (Ed.). (2004). *Online collaborative learning: Theory and practice*. IGI Global.

[36] Furnell, S., Warren, A., & Dowland, P. S. (2004, July). Improving security awareness and training through computer-based training. In *Proceedings of the 3rd World Conference on Information Security Education* (WISE 2004). California: Monterey

[37] Holdsworth, J., & Apeh, E. (2017, September). An effective immersive cyber security awareness learning platform for businesses in the hospitality sector. In *2017 IEEE 25th International Requirements Engineering Conference Workshops* (REW) (pp. 111-117). IEEE.

[38] Jeux qui ont d'autres buts que le simple divertissement, comme l'éducation.

[39] Beckers, K., & Pape, S. (2016, September). A serious game for eliciting social engineering security requirements. In *2016 IEEE 24th International Requirements Engineering Conference* (pp.16-25). IEEE.

[40] Hendrix, M., Al-Sherbaz, A., & Victoria, B. (2016). Game based cyber security training: are serious games suitable for cyber security training? *International Journal of Serious Games*, *3*(1), 53-61.

[41] Kulkarni, V. K. (2019). *Basic Cybersecurity Awareness Through Gaming*.

[42] Raman, R., Lal, A., & Achuthan, K. (2014, March). Serious games based approach to cyber security concept learning: Indian context. In *2014 International Conference on Green Computing Communication and Electrical Engineering* (ICGCCEE) (pp. 1-5). IEEE.

[43] Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203-1230.

[44] Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442-451.

[45] George, J. F., Biros, D. P., Adkins, M., Burgoon, J. K., & Nunamaker, J. F. (2004, June). Testing various modes of computer-based training for deception detection. In *International Conference on Intelligence and Security Informatics* (pp. 411-417). Springer, Berlin, Heidelberg.

[46] Cao, J., Lin, M., Deokar, A., Burgoon, J. K., Crews, J. M., & Adkins, M. (2004, June). Computer-based training for deception detection: What users want? In *International Conference on Intelligence and Security Informatics* (pp. 163-175). Springer, Berlin, Heidelberg.

[47] Capacité d'adopter une conduite désignée.

[48] Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816-826.

[49] Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

[50] Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human Behavior*, *24*(6), 2799-2816.

[51] Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*(1), 63-72.

[52] Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2017). Managing information security awareness at an Australian bank: a comparative study. *Information & Computer Security*, *25*(2), 181-189.

[53] Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92-100.

[54] Jacoby, R. (2005). Computer based training: Yes or no. *Journal of Health Care Compliance*, *7*(3), 45-48.

[55] Hannum, W. (2001). *Web-based training: advantages and limitations*. Web-based traigning, Educational Technology Publications. New Jersey, 13-20.

[56] État mental d'un individu qui reçoit un volume trop important d'informations en ce qu'il n'aurait pas la capacité cognitive d'en traiter autant dans le temps qui lui est imparti, amenant ainsi à un échec de la mémorisation à long terme de ces informations.

[57] Pour en savoir plus sur le programme CyberCIEGE : https://my.nps.edu/web/c3o/cyberciege

[58] Roepke, R., & Schroeder, U. (2019). The Problem with Teaching Defence against the Dark Arts—a Review of Game-based Learning Applications and Serious Games for Cyber Security Education. In *11th International Conference on Computer Supported Education*. Heraklion, Crete, Greece.

[59] Ayyagari, R., & Figueroa, N. (2017). Is seeing believing? Training users on information security: Evidence from Java Applets. *Journal of Information Systems Education*, *28*(2), 115-122.

[60] Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*, *15*(5/6), 352-357.

[61] Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information management & computer security*, *6*(4), 167-173.

[62] Kim, P., & Homan, J. V. (2012). Measuring the effectiveness of information security training: A comparative analysis of computer-based training and instructor-based training. *Issues in Information Systems*, *13*(1), 215-224.

[63] Chatzoglou, P. D., Sarigiannidis, L., Vraimaki, E., & Diamantidis, A. (2009). Investigating Greek employees' intention to use web-based training. *Computers & Education*, *53*(3), 877-889.

[64] Mansurov, A. (2016). A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching Students at Altai State University, Russia. *Modern Applied Science*, *10*(11), 159.

[65] Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289-296.

[66] Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication*, *800*(50), 1-39.

[67] Cf. notion de validité externe : généralisation des résultats d'une étude aux groupes/contextes auxquels ils sont censés s'appliquer.

[68] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008, October). Lessons from a real world evaluation of anti-phishing training. In *2008 eCrime Researchers Summit* (pp. 1-12). IEEE.

[69] Tioh, J. N., Mina, M., & Jacobson, D. W. (2017, October). Cyber security training a survey of serious games in cyber security. In *2017 IEEE Frontiers in Education Conference* (FIE) (pp. 1-5). IEEE.

[70] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248.

Annexe

Critères de performance	Groupe de collaboration		Formation assistée par ordinateur	
	Inclus	Éléments moteurs	Inclus	Éléments moteurs
Sensibilisation	✓	Participation Identification Responsabilisation	✓	Multi-supports/formats Efficacité de la réponse Auto-efficacité
Modification comportement	✓	Discussion active Réflexion collective Interaction avec instructeur	✓	Expérience avec ordinateur/internet Simulation
Conformité aux politiques de l'entreprise	✓	Partage de connaissances et expériences Engagement Normes sociales	✓	Simulation situationnelle Retours Auto-efficacité
Acquisition de connaissances	✓	Acquisition d'informations via les échanges	✓	Acquisition d'informations via la simulation
Satisfaction des utilisateurs	✓	Socialisation collègues et instructeur	✓	Ludification motivante et engageante
Avantages	✓	Influence sociale Culture organisationnelle Partage de connaissances et expériences	✓	Rentabilité Contrôle du rythme Personnalisable Diffusion large