CRPC | Chaire de recherche en prévention de la cybercriminalité

Notes *de synthèse*

Vol. 4, Num. 2
2024

Ludification en cybersécurité : conditions de réussite et défis actuels

Mélanie Théorêt, candidate à la maîtrise en criminologie

Introduction

La présente note de synthèse constitue une revue de littérature sur **l'utilisation des approches ludiques et des jeux dans le domaine de la cybersécurité**. La ludification (ou gamification) incorpore plusieurs mécanismes clés pour engager et motiver les participants, parmi lesquels les plus communs sont l'attribution de points, de badges et l'utilisation de tableaux de bord pour classer les participants en fonction de leur performance, le recours à des logiques de défis et de quêtes pour insuffler un élément d'aventure, l'utilisation de systèmes de rétroaction en temps réel et de récompenses pour renforcer les comportements positifs, ainsi que la valorisation des dynamiques d'interaction sociales où la collaboration et la compétition renforcent l'engagement. Pour concevoir un jeu éducatif sur la cybersécurité efficace et adapté, il est impératif de **comprendre ce qui fonctionne**, d'**identifier les conditions de réussite** et de **combler les lacunes existantes dans les travaux antérieurs**. La structure de cette note se divise en trois sections principales qui résument les thèmes majeurs tirés de la littérature scientifique : les avantages de la gamification en cybersécurité, les lacunes observées dans les jeux de cybersécurité existants, et les éléments essentiels d'un jeu efficace. La deuxième section conclut la note par une synthèse brève, mettant en lumière les points essentiels à retenir, les interrogations qui demeurent sans réponse et les recommandations pratiques.

Les avantages de la ludification en cybersécurité

La ludification présente des avantages significatifs en matière de sensibilisation à la sécurité de l'information [1]. Plusieurs jeux ont déjà été développés pour sensibiliser un large éventail d'utilisateurs aux problématiques de cybersécurité, ciblant la population générale, les enfants, les adolescents, et même les professionnels [1]. Parmi ces jeux, **les jeux sérieux sont les plus couramment utilisés pour la sensibilisation à la cybersécurité** [1]. Les jeux sérieux sont des jeux spécialement conçus dans le but de **transmettre un message éducatif préétabli** [2]. Contrairement à la ludification qui ne possède aucune sophistication particulière, les jeux sérieux intègrent des éléments de jeu à diverses fins dans des contextes généralement non ludiques [2]. Il est important de noter que les définitions de ces concepts ne font pas l'objet d'un consensus universel dans la littérature et qu'il arrive parfois que ces termes soient utilisés de manière interchangeable [2].

Les effets positifs de la ludification en éducation sont mentionnés dans plusieurs méta-analyses à grande échelle [3, 4, 5, 6, 7]. L'une des clés de son succès réside dans sa capacité à **engager activement les apprenants et à établir des liens émotionnels avec le contenu** [3, 4]. L'apprentissage par les jeux permet également de stimuler la motivation des apprenants à participer à des formations tout en améliorant

considérablement leurs performances d'apprentissage [1]. De plus, une étude menée sur une période de 6 mois [6], dans le cadre d'un projet de gamification en sécurité de l'information organisationnelle, a démontré que la ludification peut être utilisée pour **mieux intégrer des formations dans les routines quotidiennes des employés**, pour **susciter une motivation intrinsèque** chez ces derniers à appliquer les mesures de sécurité, et pour qu'ils **se conforment réellement aux pratiques de cybersécurité** [8].

En outre, les approches éducationnelles basées sur les jeux ont la capacité de **rendre la cybersécurité plus accessible**, en particulier pour des groupes d'apprenants sous-représentés tels que les femmes et les personnes issues de minorités ethniques [9]. En effet, l'apprentissage par les jeux peut **servir d'alternative aux méthodes d'apprentissage traditionnelles qui peuvent entraîner un désengagement** [10] et qui ne conviennent pas nécessairement à tous les individus [11]. Selon les conclusions d'une méta-analyse [6], les jeux **génèrent des gains cognitifs plus élevés que les méthodes d'enseignement traditionnelles**. La gamification se révèle ainsi efficace pour familiariser les joueurs avec des concepts tel que ceux que l'on retrouve en cybersécurité, qui peuvent être moins accessibles par les méthodes d'apprentissage classiques [11, 12]. Elle offre donc une approche innovante pour rendre la cybersécurité plus compréhensible et accessible pour un large public [9].

Ainsi, il est évident que l'apprentissage par les jeux offre des avantages indéniables en matière de sensibilisation à la cybersécurité. Cependant, il est important de noter que certains jeux de cybersécurité développés présentent des lacunes pouvant potentiellement réduire leur efficacité en matière de sensibilisation.

Les lacunes des jeux de cybersécurité existants

Bien que les études concluent que la gamification en cybersécurité produit des résultats positifs, des lacunes et des limites subsistent, en particulier en ce qui concerne l'**absence d'une structure claire pour orienter le développement des jeux de cybersécurité** [1]. En effet, certains jeux s'avèrent souvent **trop complexes ou peu adaptés aux besoins des employés**, et il semble que les jeux existants se soient principalement concentrés sur des enjeux généraux de cybersécurité, en mettant l'accent sur la sensibilisation face aux menaces internes à la sécurité [1]. Ainsi, il est proposé de simplifier le développement des jeux en créant des projets axés sur les menaces à la sécurité les plus courantes, tout en tenant compte de la diversité des besoins en matière de formation [1]. Cependant, cette simplification ne doit pas mener à une réduction excessive de la complexité, car de nombreux jeux abordent la cybersécurité de manière superficielle, en se limitant à une gamification de surface ou même en se présentant simplement comme un quiz ludo-éducatif, sans réellement prendre en compte les mécanismes d'attraction et d'engagement des joueurs [9].

À travers une revue systématique, des chercheurs ont examiné les caractéristiques principales de 181 jeux de cybersécurité à l'échelle mondiale et ont constaté que **les jeux actuels mettent davantage l'accent sur les aspects techniques de la cybersécurité**, semblant parfois négliger l'aspect social du domaine (par exemple, tous les enjeux liés aux interactions sociales) [9]. En intégrant cette dimension sociale, souvent oubliée en cybersécurité, il serait possible d'encourager une participation plus large et ainsi de sensibiliser un public plus vaste aux enjeux de cybersécurité à travers les jeux [9]. Cela dit, tous les joueurs ne seront pas attirés par un même jeu et **des éléments tels que l'âge, le genre et les préférences personnelles peuvent influencer la manière dont une personne s'intéresse ou réagit à un jeu** [2].

Malgré les efforts de certains concepteurs de jeux à intégrer des personnages féminins et des représentations ethniques diverses dans leurs projets ludiques, de nombreux jeux continuent de refléter les inégalités de genre et de race présentes dans le domaine de la cybersécurité [9]. Cela pourrait compromettre l'engagement de certains joueurs appartenant à ces groupes minoritaires [13].

Par ailleurs, contrairement aux jeux de divertissement qui n'ont généralement pas pour objectif premier d'instruire les joueurs, **les jeux sérieux sont souvent développés avec des budgets nettement plus restreints**, ce qui peut influencer leur capacité à motiver et à éduquer les joueurs de manière efficace [2]. De plus, même si les jeux de sensibilisation à la cybersécurité peuvent avoir des effets positifs en augmentant la conscientisation à la sécurité de l'information, **ces effets peuvent ne pas persister dans le temps** [14]. À titre d'exemple, l'évaluation de l'application mobile NoPhish, un jeu de cybersécurité visant à identifier les menaces d'hameçonnage, a montré une amélioration de la capacité des participants à détecter ces menaces après avoir utilisé l'application [15]. Cependant, une étude de suivi menée 5 mois plus tard, suggère que bien que les participants obtiennent toujours de bons résultats aux questions sur l'hameçonnage, leurs performances globales avaient diminué, ce qui soulève des préoccupations quant à la rétention des compétences acquises et à la fréquence de recours aux jeux [14, 15]. Il est donc primordial de prendre en considération ces limitations dans l'élaboration des jeux de sensibilisation efficaces.

Les caractéristiques essentielles d'un jeu sérieux

Lors de la phase de conception du jeu, il est impératif de **mener une recherche approfondie pour définir clairement les objectifs du projet** et réfléchir attentivement aux connaissances à transmettre aux joueurs [2]. Il est important que le contenu éducatif fasse partie intégrante du jeu [2]. Les jeux qui offrent des expériences d'apprentissage actives plutôt que passives, ainsi que ceux offrant un accès illimité, se sont révélés plus efficaces [5]. Par exemple, les joueurs peuvent être immergés dans le jeu en jouant le rôle d'une victime ou d'un acteur malveillant, leur permettant ainsi de prendre des actions influençant le déroulement du jeu [2]. Pour une efficacité maximale de l'apprentissage, le jeu doit **encourager la pensée critique**, laissant aux joueurs la possibilité de tirer leurs propres conclusions plutôt que de leur dicter ce qui est bien ou mal [2]. L'efficacité d'un jeu dépend ainsi de sa **capacité à se rapprocher de l'expérience personnelle du joueur**, à **établir une connexion entre le sujet du jeu et l'apprenant**, à **fournir des opportunités d'action au sein du jeu**, ainsi qu'à **s'adapter à l'environnement dans lequel le joueur interagit avec le jeu** [16].

Il est également essentiel que **le jeu soit en adéquation avec le groupe cible**, en prenant en compte des caractéristiques telles que l'âge et le sexe [2]. En effet, les jeux qui permettent aux utilisateurs de créer des avatars en accord avec leur identité peuvent stimuler l'engagement des joueurs et augmenter leur motivation à y participer [13]. Par conséquent, il est crucial que les personnages du jeu reflètent le public visé [2].

Par ailleurs, **les jeux sérieux s'avèrent plus efficaces lorsqu'ils sont accompagnés d'instructions et lorsqu'ils sont complétés par d'autres activités éducatives**, telles que des discussions en groupe ou l'utilisation de matériel écrit supplémentaire [2, 5, 7]. De même, leur efficacité est accrue lorsque l'apprentissage est réparti sur plusieurs sessions et que les joueurs ont l'opportunité de travailler en groupe [7]. Il est donc judicieux d'intégrer les jeux sérieux dans des interventions plus larges, pouvant se dérouler dans un contexte de formation ou professionnel, afin de garantir que le public cible y participe activement [2].

Enfin, il est crucial de **ne pas réduire un jeu sérieux à un simple projet de ludification** qui n'offre pas de véritable processus d'apprentissage, car cela est moins susceptible

d'entraîner un changement de comportement [2]. Les joueurs risquent d'adopter le comportement désiré uniquement pour obtenir des récompenses ou des points en retour [2]. Cependant, les stratégies de ludification qui stimulent les motivations intrinsèques et qui ont une approche plus globale peuvent être efficaces [2]. Une étude portant sur un jeu sérieux d'évasion destiné à l'éducation en matière de sécurité matérielle a identifié **trois éléments essentiels pour la conception de ce type de jeu sérieux** [17] : la nécessité d'un **scénario captivant**, l'**implication de l'enseignant dans la planification et la supervision du jeu** et la tenue d'une **séance de rétroaction** pour garantir que les étudiants ont pleinement assimilé les concepts abordés.

Conclusion et recommandations

Pour conclure, cette note de synthèse a permis d'examiner **les conditions de réussite des jeux de cybersécurité**, mettant en lumière les avantages de la gamification dans ce domaine, les lacunes des jeux existants et les éléments essentiels pour la conception de jeux sérieux efficaces. La gamification s'avère prometteuse **en favorisant l'engagement actif des apprenants**, **l'établissement de liens émotionnels avec le contenu**, et **la stimulation de la motivation en cybersécurité**. Cependant, des lacunes subsistent dans les jeux actuels, notamment leur **inadéquation vis-à-vis des besoins des utilisateurs** et leur **manque de diversité des représentations identitaires**. Pour garantir l'efficacité des futurs jeux de cybersécurité, il est essentiel de prendre en compte ces avantages et lacunes, tout en respectant les principes fondamentaux d'un bon jeu, notamment **la compréhension des besoins du public cible**, **la promotion de la représentation inclusive** et **la stimulation de l'engagement actif des joueurs**.

En suivant ces orientations, les jeux de cybersécurité peuvent jouer un rôle significatif dans la formation et la sensibilisation des individus. Enfin, des évaluations approfondies sont nécessaires pour **mieux comprendre l'efficacité à long terme des jeux en cybersécurité** et pour **assurer leur déploiement à grande échelle**. Ce processus continu d'évaluation et d'amélioration est crucial pour maximiser l'impact des programmes de ludification.

Références

[1] Sharif, K. H. et Ameen, S. Y. (2021). A Review on Gamification for Information Security Training, *International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI)*, Sana'a, Yemen, 2021, pp. 1-8.

[2] Aerts, S. (2019). Boîte à outils du REPC N°15. Prévenir la victimisation des mineurs à l'ère du numérique : sensibilisation et changement de comportement. *European Crime Prevention Network (EUCPN)*.

[3] Clark, D. B., Tanner-Smith, E. E., et Killingsworth, S. S. (2016). Digital games, design, and learning: A systematic review and meta-analysis. *Review of educational research*, *86*(1), 79-122.

[4] Connolly, T. M., Boyle, E. A., MacArthur, E., Hainey, T. et Boyle, J. M. (2012). A systematic literature review of empirical evidence on computer games and serious games. *Computers & education*, *59*(2), 661-686.

[5] Sitzmann, T. (2011). A meta-analytic examination of the instructional effectiveness of computer-based simulation games. *Personnel psychology*, *64*(2), 489-528,

[6] Vogel, J. J., Vogel, D. S., Cannon-Bowers, J., Bowers, C. A., Muse, K. et Wright, M. (2006). Computer gaming and interactive simulations for learning: A meta-analysis. *Journal of educational computing research*, *34*(3), 229-243.

[7] Wouters, P., van Nimwegen, C., van Oostendorp, H. et van der Spek, E. D. (2013). A meta-analysis of the cognitive and motivational effects of serious games. *Journal of Educational Psychology*, *105*(2), 249–265.

[8] Silic, M., et Lowry, P. B. (2020). Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. *Journal of Management Information Systems*, *37*(1), 129–161.

[9] Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J. et Weintrop, D. (2020). Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. *Simulation & Gaming*, *51*(5), 586–611.

[10] Siala H., Kutsch E. et Jagger S. (2019). Cultural influences moderating learners' adoption of serious 3d games for managerial learning. *Information Technology & People*. *33*(2), 424-455.

[11] Gee, J. P. (2003). What video games have to teach us about learning and literacy. *Computers in entertainment (CIE)*, *1*(1), 20-20.

[12] Ketelhut, D. J. (2007). The impact of student self-efficacy on scientific inquiry skills: An exploratory investigation in River City, a multi-user virtual environment. *Journal of science education and technology*, *16*, 99-111.

[13] Birk M. V., Atkins C., Bowey J. T. et Mandryk R. L. (2016). Fostering intrinsic motivation through avatar identification in digital games. *In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pp. 2982–2995.

[14] Scholefield, S. et Shepherd, L.A. (2019). Gamification Techniques for Raising Cyber Security Awareness. In: Moallem, A. (eds) *HCI for Cybersecurity, Privacy and Trust. HCII 2019. Lecture Notes in Computer Science*, vol 11594. Springer, Cham.

[15] Canova, G., Volkamer, M., Bergmann, C. et Reinheimer, B. (2015). NoPhish app evaluation: lab and retention study. In *NDSS workshop on usable security*.

[16] Squire, K. (2011). *Video Games and Learning: Teaching and Participatory Culture in the Digital Age. Technology, Education--Connections (the TEC Series)*. Teachers College Press. 1234 Amsterdam Avenue, New York, NY 10027.

[17] Bruguier, F., Lecointre, E., Pradarelli, B., Dalmasso, L., Benoit, P. et Torres, L. (2019). Teaching Hardware Security: Earnings of an Introduction Proposed as an Escape Game. *The Review*.