CRPC | Chaire de recherche en prévention de la cybercriminalité

Notes *de synthèse*

Vol. 4, Num. 5
2024

Inventaire des outils de communication en sensibilisation à la cybersécurité en entreprise

Isabelle Chadic, candidate à la maîtrise en criminologie

Introduction

Les activités opérationnelles des entreprises dépendent désormais en grande partie des nouvelles technologies [1]. Avec la gestion des données clients via des systèmes informatiques, les employés deviennent des cibles potentielles pour les cybercriminels. Par ailleurs, 74% des cyberincidents sont causés par des erreurs humaines [2, 3, 4, 5]. Ces vulnérabilités ont des conséquences économiques, réputationnelles et sociales importantes pour les entreprises et leurs clients [6, 7, 8]. **Afin d'assurer la protection des systèmes et des données sensibles, les entreprises déploient des programmes de formation et de sensibilisation à la cybersécurité (SETA) afin d'améliorer les connaissances, les attitudes et comportement des employés vis-à-vis de la sécurité de l'information** [4, 8, 3, 9]. Ces programmes s'appuient sur une diversité d'outils de communication permettant d'atteindre les objectifs de sensibilisation de l'organisation.

La communication et ses outils: puissant moteur de sensibilisation

Les études en santé publique mettent en évidence l'influence de la communication sur les connaissances, les croyances, les attitudes et les comportements individuels [10, 11]. Plus précisément, **la communication visant au changement de comportement représente une mesure en soi d'intervention ayant le pouvoir prévenir diverses problématiques de santé** [11].

Les outils de communication revêtent une importance particulière, ayant **pour but de diffuser des messages actionnables auprès d'un public cible** [10, 11]. Par exemple, l'analyse des campagnes de prévention liées à des problématiques telles que l'alcoolisme, le VIH et la consommation de tabac indique que l**e choix des outils de communication influence la portée de la sensibilisation, lesquels doivent être adaptés au contexte et au dit public** [10, 11]. En effet, chaque outil de communication est doté de mécanismes spécifiques offrant la possibilité d'atteindre les destinataires du message de sensibilisation. Par exemple, les études portant sur la prévention du tabagisme suggèrent que les avertissements visuels sont plus efficaces que les avertissements uniquement textuels chez les jeunes, car ils permettent de renforcer la compréhension des risques tout en suscitant des réactions émotionnelles afin de dissuader la consommation [12].

La sélection des outils de communication est donc cruciale dans le domaine de la sensibilisation à la cybersécurité, dont les objectifs sont similaires à celui de la santé, à savoir influencer les décisions personnelles en améliorant les connaissances [11].

Les outils de communication en sensibilisation à la cybersécurité

Il existe une variété d'outils de communication qui peuvent être déployés numériquement ou physiquement. La littérature scientifique examine certains de ces outils dans un contexte organisationnel, dont voici un inventaire synthétique :

Les outils physiques

Sous la conduite d'un expert, les **ateliers et séminaires** permettent aux employés d'interagir entre eux afin se familiariser avec des sujets liés à la cybersécurité ainsi que de partager leurs réflexions et leurs expériences [12]. Les **conférences** sont quant à elles, plutôt menées par des experts internes ou externes à l'organisation et transmettent de manière interactive ou non des informations détaillées sur diverses thématiques de cybersécurité [13, 14].

Préparés par un expert et mis à la disposition des apprenants, les **documents textuels papier** (ex. dépliants, rapports, politiques de sécurité de l'information, etc.) transmettent des connaissances sur différents sujets liés à la cybersécurité [2, 15, 16]. Les **affiches papier** mettent en lumière des problèmes pressants ou rappelant des actions spécifiques à entreprendre pour renforcer la sécurité de l'organisation. Dans l'ensemble, elles cherchent à attirer l'attention des employés en transmettant des messages brefs et informatifs sur la cybersécurité [14, 17].

Puis, regroupant une gamme variée de produits (ex. autocollants, tasses, tapis de souris, etc.), le **matériel promotionnel** permet d'attirer l'attention des employés sur les pratiques de cyberhygiène ainsi que de créer un effet de rappel [13, 18].

Les outils numériques

Tout comme leur version papier, les **documents textuels numériques** (ex. rapports, politiques de sécurité de l'information, etc.) diffusent des connaissances sur divers sujets de cybersécurité, mais dans un format numérique qui s'intègre mieux dans l'environnement de travail informatisé des employés [2, 15, 16]. Plus créatives, les **infographies numériques** sont des représentations visuelles d'informations ou de données, utilisées pour illustrer des concepts liés à la cybersécurité et faciliter leur compréhension par les employés [19, 20].

Les **courriels et les infolettres** sont des moyens de communication électroniques permettant de diffuser des informations liées à la cybersécurité, notamment pour mettre en évidence des problèmes urgents concernant la sécurité de l'information [14, 21]. De plus, intégrées aux courriels, les **bannières d'avertissement** constituent des alertes textuelles numériques utilisées pour informer les employés que certaines communications externes pourraient présenter un risque pour la cybersécurité de l'organisation, tout en leur prodiguant des conseils à cet égard (par exemple, ne pas cliquer sur les liens, ne pas télécharger de pièces jointes, etc.) [22].

Les **modules d'apprentissage** en ligne sont des regroupements multimédias organisés permettant de diffuser des informations sur la cybersécurité de manière séquentielle, à travers divers supports tels que des vidéos d'experts, des animations et du contenu textuel. Ces modules offrent ainsi une gamme d'informations, allant du concis au détaillé, et peuvent inclure des composantes interactives ou non [15, 23, 24].

Soulignés par la littérature scientifique comme étant prometteurs, les **jeux sérieux** sont des conceptions numériques permettant d'évaluer à la fois la compréhension théorique et les compétences pratiques des employés en les plongeant dans des environnements ludiques reproduisant des situations réelles [24]. Les jeux sérieux impliquent un but ainsi qu'une compétition et des règles spécifiques, contrairement aux simulations [26]. (*Voir la note de synthèse 2 du volume 4, "Ludification en cybersécurité: conditions de réussite et défis actuels" pour en savoir plus sur les jeux sérieux*).

Trois types de simulations sont particulièrement discutées dans la littérature. Les **simulations d'attaques**, telles que les tests d'hameçonnage, sont des environnements numériques reconstituant la réalité de façon simplifiée permettant aux employés de vivre des scénarios d'attaques récurrents portant atteinte à la cybersécurité d'une organisation [25]. Les **simulations d'incidents inhabituels** se concentrent quant à elles sur la détection et la réponse à des incidents non courants liés à la cybersécurité, permettant ainsi aux utilisateurs d'apprendre à réagir sans risques réels [25]. Enfin, les **exercices sur table** (***Table Top Exercises* ou TTX en anglais**) sont des exercices où les gestionnaires, le personnel de gestion d'urgence et les professionnels TI discutent de scénarios de risque pour évaluer et renforcer les protocoles de gestion des crises [26, 27].

La communication vidéo

La communication vidéo regroupe tout un ensemble d'outils au format distinct les uns des autres. D'une part, les **vidéos éducatives** permettent de transmettre de l'information sur différents sujets liés à la cybersécurité offrant un apprentissage visuel et audio aux participants [14, 28].

D'autre part, certains outils représentent le produit virtuel d'initiatives physiques. Ainsi, les **webinaires** sont des présentations en ligne animées par un expert, permettant de transmettre des connaissances sur divers sujets de cybersécurité tout en stimulant la participation des employés [29]. Également offertes de manière synchrone, les **présentations en direct** transmettent quant à elle, de manière audiovisuelle une conférence ou une présentation physique aux employés [30, 31].

Parallèlement, la diffusion du contenu vidéo du programme de cybersécurité des entreprises peut s'effectuer via divers outils préparés en amont, en mode asynchrone. Par exemple, les **présentations différées** (***Talking Head***) permettent à un expert de transmettre des infor-mations pertinentes sur la cybersécurité. Ces présentations sont souvent accompagnées de quelques lignes de texte superposé, d'images fixes ou de courtes séquences vidéo pour appuyer la narration [30, 31]. Au contraire, les **diapositives animées** combinent des images avec une narration vocale ou une vidéo réduite de l'expert, souvent affichées dans un coin de la diapositive [30, 31]. Les **entrevues différées** transmettent des connaissances aux employés en présentant une ou plusieurs personnes répondant à des questions sur la cybersécurité, et ce, sans établir un contact direct avec la caméra [30, 31]. Enfin, les **animations** utilisent de courtes séquences d'images pour présenter, à travers des techniques comme le dessin et d'autres méthodes numériques, des sujets liés à la cybersécurité créant l'illusion de mouvement [24, 32]. Également de brève durée, les **courts-métrages** illustrent des scénarios simulés d'incidents de cybersécurité dans le but de conscientiser les utilisateurs aux dangers potentiels et aux mesures de sécurité à adopter [16, 24].

Efficacité des outils de communication en sensibilisation à la cybersécurité

Les évaluations empiriques dénotent que **peu importe l'outil, les programmes de sensibilisation ont un impact positif sur les connaissances en cybersécurité** [7, 9, 14]. Cependant, il existe un débat dans la littérature concernant l'efficacité des outils de communication à provoquer des changements de comportement au sein de l'audience visée.

Certaines études indiquent que **l'utilisation de présentations en personne est inefficace, provoquant l'ennui des participants** [33]. Cependant, d'autres études sont plus nuancées et indiquent que l**a réussite de ces outils dépend fortement de l'expertise du professionnel dans le domaine et de ses compétences en communication**. Ces éléments sont cruciaux pour une transmission efficace de l'information et pour susciter l'intérêt des participants [33, 34]. En effet, d'autres chercheurs ont obtenu des résultats démontrant que ce mo-

-de était préférable en termes de satisfaction utilisateur, d'efficacité et d'auto-efficacité [35], où ces compétences ont pu être mieux valorisées.

En ce qui concerne les **outils basés sur la vidéo**, la littérature scientifique souligne que **l'environnement sensoriel créé par leur intégration multimédia (voix, image, texte, etc.) est efficace en termes de transfert d'apprentissages**, **favorisant ainsi la compréhension et la rétention de l'information** chez les apprenants [36, 37]. Cependant, d'autres études ont plutôt conclu à des **améliorations limitées où les vidéos de sensibilisation n'ont pas eu d'effet statistiquement significatif sur les comportements autodéclarés des participants** (ex. se connecter à des réseaux Wi-Fi inconnus) [38]. Ces résultats pourraient être attribués au **manque d'attention aux facteurs liés à l'apprentissage**, en copiant simplement un format papier sans proposer de réelle adaptation à l'outil [39]. D'autre part, des chercheurs ont observé des **changements significatifs dans les capacités des participants à identifier des courriels d'hameçonnage après avoir été exposés à un outil de sensibilisation textuel** [14]. Ces résultats s'expliquent par une clarté et concision de l'information, facile à suivre pour les apprenants [14]. Néanmoins, la nature moins stimulante d'un texte et le fait de privilégier la mémorisation plutôt que la compréhension peuvent compromettre l'intérêt et l'apprentissage [14].

Certains auteurs mettent plutôt l'accent sur l'aspect visuel d'autres outils tels que **les bandes dessinées, qui ont montré de meilleurs résultats en termes de sensibilisation**. Ils soulignent que le cerveau humain traite l'information visuelle plus promptement que celle de nature textuelle, améliorant ainsi la compréhension des concepts [8]. Cependant, **une utilisation excessive peut nuire à la sensibilisation en raison d'une surcharge cognitive** [41].

En ce qui concerne **la simulation**, **ses effets positifs en matière d'apprentissage ont été démontrés** [33]. En effet, des études portant sur les simulations d'hameçonnage ont révélé une **augmentation de la perception du risque et du degré de traitement systématique**, des **changements de comportement**, des **réactions plus confiantes face aux menaces**, ainsi que des **taux améliorés quant à la probabilité d'adopter un comportement sécuritaire** [42, 43]. Ces études démontrent d'ailleurs une double utilité agissant à la fois comme **mécanisme de formation**, mais également de **validation des connaissances et compétences acquises durant l'exercice** [42]. Ces avantages proviennent de divers mécanismes, tels qu'une conception réaliste appropriée garantissant l'apprentissage, l'utilisation d'heuristiques comme la disponibilité, la répétition des exercices, ainsi qu'un retour d'information sur les résultats. [15, 33, 43]. Or, les chercheurs relèvent également **certains inconvénients incluant le risque de développement d'une résistance excessive chez les apprenants** (ex. en ignorant des demandes légitimes en les croyant frauduleuses), ainsi que **des délais et boucles de rétroaction entre un événement de cybersécurité et la réponse de l'utilisateur** [33, 42].

De plus en plus discutés, les outils ludiques ont prouvé leur efficacité en sensibilisant les apprenants aux risques liés à la cybersécurité, aux meilleures pratiques en termes de cyberhygiène, ainsi qu'en développant les compétences pour identifier les vulnérabilités organisationnelles [44, 45]. La littérature scientifique dans le domaine de l'apprentissage souligne que le jeu est l'une des méthodes les plus efficaces. En effet, **le jeu possède la capacité à motiver les apprenants, particulièrement lorsque les fondements du concept de jeu sont respectés** (règles, but, etc.) et que certains principes tels que la narration et l'histoire sont pris en compte, suscitant ainsi l'intérêt et le désir d'apprendre chez les participants [11, 47]. Cependant, tout comme les autres outils, les jeux risquent de **perdre de leur**

efficacité s'ils sont utilisés de manière inappropriée, mal élaborés, ou s'ils ne correspondent tout simplement pas aux particularités individuelles de l'utilisateur (*Voir la note de synthèse 2 du volume 4, "Ludification en cybersécurité: conditions de réussite et défis actuels*).

Conclusion

Pour renforcer les connaissances et les compétences en matière de cybersécurité, les entreprises disposent d'une gamme variée d'outils de communication dédiés à la sensibilisation. Comme mis en évidence dans cet inventaire et les résultats en termes d'efficacité, **un même outil peut être utilisé de différentes manières, modulant ainsi ses capacités de sensibilisation**. Bien que certains auteurs suggèrent qu'une stratégie optimale consiste à **diversifier les canaux de communication, la configuration optimale reste encore indéterminée, notamment en raison des spécificités individuelles et organisationnelles**. En effet, les préférences des employés pour certains outils de communication semblent influencer la capacité des programmes de sensibilisation [14, 40]. Ce constat soulève des interrogations sur la pertinence d'un cadre de contrôle de cybersécurité adaptable, où les programmes de sensibilisation seraient modulés par les caractéristiques organisationnelles et personnelles [40].

Néanmoins, certains auteurs soulignent que la personnalisation systématique n'est pas toujours réalisable en raison des contraintes de temps et d'investissement [14] bien que d'autres auteurs avancent que la personnalisation offre des avantages pour optimiser les investissements en cybersécurité, proposant ainsi une solution efficace tout en évitant de consacrer du temps et de gaspiller des ressources à la création de contenu peu performant [9, 40].

Recommandations

Une approche équilibrée combinant différentes méthodes de communication en fonction du contexte et des besoins des apprenants peut maximiser l'efficacité des programmes de sensibilisation à la cybersécurité.

Évaluer les besoins de son entreprise
Il est primordial de bien connaître son public cible ainsi que ses ressources humaines et financières disponibles afin d'exploiter efficacement l'outil sélectionné.

Favoriser des éléments captivants
Pour maximiser le transfert d'apprentissage, l'intégration d'éléments audio-visuels s'avère bénéfique pour maintenir l'attention des participants. De plus, l'utilisation d'outils tels que les jeux sérieux ou les simulations se distingue par une plus grande efficacité afin de susciter l'intérêt des apprenants, accroître leur sensibilisation, et induire des modifications comportementales.

Multiplier les outils
Sans avoir à calibrer l'outil préféré de chaque employé, la combinaison de plusieurs outils peut être bénéfique puisqu'elle permet de s'adapter aux préférences individuelles des apprenants. Cela permet de maximiser les chances de rejoindre l'employé avec un canal qui capte son intérêt.

Porter une attention particulière au contenu présenté par les outils
Quel que soit l'outil choisi, il est crucial de considérer l'impact du contenu diffusé par cet outil. Par exemple, une présentation excessive d'informations dans un langage complexe peut influencer la capacité de sensibilisation en compromettant l'attention, le caractère stimulant, ou la compréhension des informations.

Tableau récapitulatif sur l'efficacité des outils de communication

Outils	Avantages	Limites	Critères de réussite
Présentation en personne	• Transmission directe de l'information; • Interaction avec les participants suscitant l'intérêt; • Préférable en termes de satisfaction utilisateur et auto-efficacité (selon certaines études).	• Risque d'ennui chez les participants; • Efficacité dépendante du communicateur.	• Engagement des participants; • Clarté et pertinence du contenu présenté; • Nécessite un certain degré d'expertise du professionnel et d'excellentes compétences en communication
Multimédia/vidéo	• Stimulation du transfert d'apprentissage; • Amélioration de la compréhension et de la rétention de l'information; • Traitement de l'information visuelle rapide permettant la compréhension des concepts.	• Si exploité inadéquatement, risque d'effets limités sur les comportements; • Risque de surcharge cognitive lors d'une utilisation excessive	• Qualité de la production; • Pertinence et clarté du message.
Texte	• Facile de suivre le contenu présenté; • Acquisition de connaissances et de compétences.	• Présentation de l'information axée sur la mémorisation plutôt que la compréhension peut nuire à l'intérêt et l'apprentissage; • Risque d'une diminution de l'intérêt en raison d'un manque de stimulation dans le texte.	• Présentation de l'information de manière claire et concise; • Limitation de la longueur des informations présentées pour éviter l'excès.
Simulation	• Stimulation du transfert d'apprentissage; • Accroissement de la perception du risque et du degré de traitement systématique; • Réactions plus confiantes face aux menaces; • Double utilité : mécanisme de formation & validation.	• Risque de développement d'une résistance excessive chez les apprenants posant obstacle à l'emploi; • Délai et boucles de rétroaction entre un événement de cybersécurité et la réponse de l'utilisateur.	• Conception selon un niveau de réalisme adéquat afin d'assurer les apprentissages; • Usage d'heuristiques dont la disponibilité; • Répétition des simulations et rétroaction sur les résultats
Jeux	• Capacité à enseigner de manière interactive et à rendre l'apprentissage plus agréable; • Motivation à apprendre et intérêt; • Développement des compétences et compréhension des risques et des meilleurs pratiques.	• Besoin d'une conception soigneuse pour garantir la pertinence et l'efficacité pédagogique.	• Conception de jeux attrayants, tenant compte des fondements du concept de jeu (règles, but, etc.) et des principes efficaces tels que la narration et l'histoire; • Adaptabilité du contenu ludique aux objectifs de sensibilisation et aux besoins spécifiques des utilisateurs.

Références

[1] Dupont, B. (2019). La cyberrésilience des institutions financières : importance et applicabilité. *Journal de cybersécurité*, *5*(1), tyz013.

[2] Bauer, S., Bernroider, E. W. et 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.

[3] Campbell, C. C. (2019). Solutions for counteracting human deception in social engineering attacks. *Information Technology & People*, *32*(5), 1130-1152.

[4] Kweon, E., Lee, H., Chai, S. et Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: an empirical evidence. *Information Systems Frontiers*, *23*, 361-373.

[5] Verizon. (2023). *2013 Verizon Data Breach Investigations Report*.

[6] Confente, I., Siciliano, G. G., Gaudenzi, B. et Eickhoff, M. (2019). Effects of data breaches from user-generated content: A corporate reputation analysis. *European Management Journal*, *37*(4), 492-504.

[7] He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L. et Tian, X. (2020). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, *21*(2), 203-213.

[8] Dincelli, E. et Chengalur-Smith, I. (2020). Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems*, *29*(6), 669-687.

[9] Alkhazi, B., Alshaikh, M., Alkhezi, S. et Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, *10*, 132132-132143.

[10] LaCroix, J. M., Snyder, L. B., Huedo-Medina, T. B. et Johnson, B. T. (2014). Effectiveness of mass media interventions for HIV prevention, 1986–2013: a meta-analysis. *JAIDS Journal of Acquired Immune Deficiency Syndromes*, 66, S329-S340.

[11] Ngigi, S., Busolo, D. N. (2018). Behaviour change communication in health promotion: Appropriate practices and promising approaches. International *Journal of Innovative Research and Development*, *7*(9), 84-93.

[47] Hammond, D. (2011). Health warning messages on tobacco products: a review. *Tobacco control*, *20*(5), 327-337.

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

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

[15] Kävrestad, J., Hagberg, A., Nohlberg, M., Rambusch, J., Roos, R., & Furnell, S. (2022). Evaluation of contextual and game-based training for phishing detection. *Future Internet*, *14*(4), 104.

[16] Alhashmi, A. A., Darem, A. et Abawajy, J. (2021). *Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats*.

[17] Bada, M., Sasse, A. M. et Nurse, J. R. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?*

[18] Abawajy, J. et Kim, T. H. (2010, November). Performance analysis of cyber security awareness delivery methods. In *Security Technology, Disaster Recovery and Business Continuity: International Conferences, SecTech and DRBC 2010, Proceedings* (pp. 142-148). Berlin, Heidelberg: Springer Berlin Heidelberg.

[19] Zhang-Kennedy, L., Chiasson, S. et Biddle, R. (2014). Arrêtez de cliquer sur « mettre à jour plus tard » : persuader les utilisateurs qu'ils ont besoin d'une protection antivirus à jour. In Persuasive Technology : 9th International Conference, *PERSUASIVE 2014*, Padoue, Italie, 21-23 mai 2014. Délibérations 9 (p. 302-322). Éditions Springer International.

[20] Risch, J. S. (2008). *On the role of metaphor in information visualization*.

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

[22] Moul, K. A. (2019). Avoid phishing traps. *Paper presented at the ACM SIGUCCS User Services Conference*.

[23] Ruiz, J. G., Mintzer, M. J. et Leipzig, R. M. (2006). The impact of e-learning in medical education. Academic medicine, 81(3), 207-212.

[24] Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, *54*(1), 1-39.

[25] Sauvé, L. et Kaufman, D. (2010). *Jeux et Simulations éducatifs: Études de Cas et leçons Apprises*. PUQ.

[26] Angafor, G. N., Yevseyeva, I. et Maglaras, L. (2023). Scenario-based incident response training: lessons learnt from conducting an experiential learning virtual incident response tabletop exercise. *Information & Computer Security*.

[27] Wendelboe, A. M., Miller, A., Drevets, D., Salinas, L., Miller, E. J., Jackson, D., ... et Public Health Working Group. (2020). Tabletop exercise to prepare institutions of higher education for an outbreak of COVID-19. *Journal of Emergency Management*, *18*(2), 1-20.

[28] Aldawood, H. et Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73.

[29] Forrester, J., Lopez, M. L., & Valentina, M. D. (2022). Marketing a cybersecurity Awareness Solution in LPA Contexts. In *Cybersecurity Awareness* (pp. 161-181). Cham: Springer International Publishing.

[30] Santos-Espino, J. M., Afonso-Suárez, M. D. et Guerra-Artal, C. (2016). Speakers and boards: A survey of instructional video styles in MOOCs. *Technical Communication*, *63*(2), 101-115.

[31] Hansch, A., Hillers, L., McConachie, K., Newman, C., Schildhauer, T. et Schmidt, J. P. (2015). Video and online learning: Critical reflections and findings from the field.

[32] Mayer, R. E. et Moreno, R. (2002). Animation as an aid to multimedia learning. *Educational psychology review*, 14, 87-99.

[33] Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S. et Wasim, M. (2023). Exploring cybersecurity education and training techniques: a comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry*, *15*(12), 2175.

[34] Corradini, I. et Corradini, I. (2020). Training methods. Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology, 115-133.

[35] Stockhardt, S., Reinheimer, B., Volkamer, M., Mayer, P., Kunz, A., Rack, P. et Lehmann, D. (2016). Teaching phishing-security: which way is best?. In *ICT Systems Security and Privacy Protection: 31st IFIP TC 11 International Conference*, SEC 2016, Ghent, Belgium, May 30-June 1, 2016, Proceedings 31 (pp. 135-149). Springer International Publishing.

[36] Stonebraker, P. W. et Hazeltine, J. E. (2004). Virtual learning effectiveness: An examination of the process. *The Learning Organization*, *11*(3), 209-225.

[37] Fern, A., Givan, R. et Siskind, J. M. (2002). Specific-to-general learning for temporal events with application to learning event definitions from video. *Journal of Artificial Intelligence Research*, 17, 379-449.

[38] Chin, A. G., Etudo, U. et Harris, M. A. (2016). On mobile device security practices and training efficacy: An empirical study. *Informatics in Education*, *15*(2), 235.

[39] Mbarika, V. W., Sankar, C. S., Raju, P. K. et Raymond, J. (2000). Importance of learning-driven constructs on perceived skill development when using multimedia instructional materials. *Journal of Educational Technology Systems*, *29*(1), 67-87.

[40] Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, D. et McCormac, A. (2020). Matching training to individual learning styles improves information security awareness. *Information & Computer Security*, *28*(1), 1-14.

[41] Liu, D., Santhanam, R. et Webster, J. (2017). Toward meaningful engagement: A framework for design and research of gamified information systems. *MIS Quarterly*, *41*(4), 1011–1034.

[42] Jansson, K. et von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & information technology*, *32*(6), 584-593.

[43] Baillon, A., De Bruin, J., Emirmahmutoglu, A., Van De Veer, E. et Van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. *PloS one*, *14*(12), e0224216.

[44] Alotaibi, F. F. G. (2019). Evaluation and enhancement of public cyber security awareness (Doctoral dissertation, University of Plymouth).

[45] Fatima, R., Yasin, A., Liu, L. et Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. *Journal of Computer Security*, *27*(6), 581-612.

[46] Quinn, C. N. (2005). *Engaging learning: Designing e-learning simulation games*. John Wiley & Sons.

[47] Kapp, K. M. (2012). *The gamification of learning and instruction: game-based methods and strategies for training and education*. John Wiley & Sons.