Université de Montréal

CRPC | Chaire de recherche en prévention de la cybercriminalité

Notes *de synthèse*

Vol. 5, Num. 2
2025

Appliquer la roue des changements de comportement en cybersécurité

Mélina Girard, M.Sc

Introduction

Dans le domaine de la cybersécurité, l'idée que l'être humain constitue le maillon faible du système reste au cœur de nombreux débats [1]. Cette perception s'explique par le fait que de nombreuses cyberattaques exploitent des erreurs humaines, telles que l'ouverture de liens d'hameçonnage ou le partage accidentel d'informations sensibles [2]. Malgré des systèmes de sécurité de plus en plus sophistiqués, **les vulnérabilités humaines continuent d'offrir une voie d'accès privilégiée aux cybercriminels**.

Face à cette réalité, les approches traditionnelles de sensibilisation et de formation en cybersécurité visent à informer les utilisateurs des menaces et à leur inculquer des pratiques sécuritaires [3, 4]. Toutefois, ces initiatives montrent des limites importantes : **rien ne prouve que la simple sensibilisation mène systématiquement à des comportements plus sécurisés**. Les compétences acquises tendent à s'éroder avec le temps [5], les rappels par courriel peuvent parfois créer un faux sentiment de sécurité, laissant entrevoir des limites importantes à ces stratégies [6] et la charge de vigilance imposée aux employés ne prend pas toujours en compte les contraintes organisationnelles qui influencent leurs comportements [7].

Plutôt que de se concentrer uniquement sur la responsabilisation individuelle, une approche plus globale et fondée sur la psychologie comportementale pourrait permettre d'améliorer l'efficacité des interventions en cybersécurité. La roue des changements de comportement (RCC) (*Behavior Change Wheel* en anglais) [8], un cadre théorique largement utilisé dans d'autres domaines comme la santé publique, pourrait fournir une alternative aux stratégies actuelles. **En tenant compte des facteurs individuels, environnementaux et organisationnels, elle propose des interventions adaptées aux sources réelles des comportements à risque**. Contrairement aux approches traditionnelles qui se limitent souvent à informer les individus des menaces et des bonnes pratiques à adopter [5, 6], **la RCC vise à modifier les comportements en profondeur en identifiant et en ciblant les leviers d'action les plus efficaces** [8]. En combinant des stratégies d'intervention variées, allant de l'éducation à la restructuration de l'environnement, elle permet non seulement d'encourager l'adoption de comportements sécuritaires, mais aussi de s'assurer qu'ils deviennent des habitudes durables plutôt que de simples réactions ponctuelles aux formations reçues.

Cette note de synthèse explore l'applicabilité de la RCC dans le domaine de la cybersécurité, en mettant en évidence ses avantages par rapport

aux approches traditionnelles et en illustrant son utilisation à travers un exemple d'intervention visant à réduire les incidents d'hameçonnage dans une entreprise.

Développement de la RCC

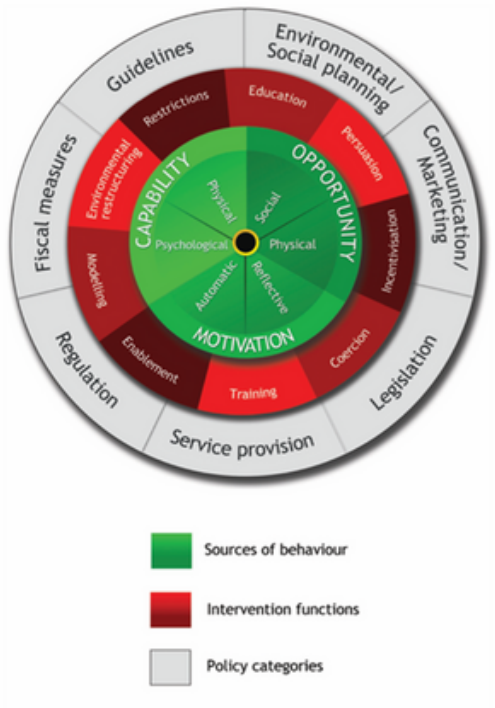
La roue des changements de comportement (RCC) a été développée en 2011 par Michie et ses collègues, un groupe de chercheurs spécialisés dans le domaine de la psychologie. **Ce modèle a été conçu pour aider les professionnels de la santé publique, de la psychologie et d'autres domaines à développer et à évaluer des interventions visant à changer les comportements** et est utilisable par tout individu de diverses disciplines avec des niveaux d'expertise variables [8].

La RCC a été développée à partir d'une analyse systématique de 19 cadres de changement de comportement existants [8]. Ces cadres ont été jugés comme incomplets et conceptuellement incohérents et la RCC visait à pallier ces limites. **L'objectif était de synthétiser les caractéristiques communes des cadres existants en les reliant à un modèle de comportement suffisamment large pour pouvoir être appliqué à n'importe quel comportement dans n'importe quel contexte**. Grâce à cette flexibilité et à sa capacité à structurer des interventions fondées sur des mécanismes éprouvés, la RCC constitue un outil particulièrement précieux pour les programmes de cybersécurité, qui peinent encore à produire des changements de comportement durables.

Développement de la RCC

Tel que le montre la **Figure 1**, la RCC se compose de trois couches principales : **les sources du comportement** (en vert), **les fonctions d'intervention** (en rouge) et **les catégories de politique** (en gris) [8].

Figure 1. La roue des changements de comportement [8]



La première couche (en vert) repose sur le modèle COM-B*, qui identifie les points d'intervention pour modifier un comportement [8]. Ce modèle se concentre sur trois dimensions essentielles:

- **La capacité** *(capability)*: désigne les aptitudes physiques et psychologiques nécessaires pour adopter un comportement, comme les connaissances ou la force.
- **L'opportunité** *(opportunity)*: réfère à l'environnement physique et social qui permet ou favorise l'accomplissement du comportement.
- **La motivation** *(motivation)*: se divise en **motivation automatique** (liée aux habitudes) et **motivation réflexive** (qui repose sur des décisions conscientes).

---

* Le modèle COM-B (*Capability, Opportunity, Motivation - Behavior*) est un cadre utilisé pour analyser et influencer les comportements. Il postule que pour qu'un individu adopte un comportement donné, il doit en avoir la capacité (connaissances et compétences), l'opportunité (facteurs externes facilitant ou contraignant le comportement) et la motivation (facteurs internes influençant l'adoption du comportement) [8].

La deuxième couche de la RCC (en rouge) présente **neuf fonctions d'intervention, soit les actions spécifiques ou stratégies directes à mettre en œuvre pour provoquer un changement comportemental**. Ces fonctions incluent :

- **L'éducation** *(education)*: accroître les connaissances ou la compréhension.
- **La persuasion** *(persuasion)*: susciter des sentiments positifs ou négatifs ou stimuler l'action.
- **L'incitation** *(incentivisation)*: créer une attente de récompense.
- **La coercition** *(coercion)*: créer une attente de punition ou de coût.
- **La formation** *(training)*: transmettre des compétences.
- **L'habilitation** *(enablement)*: augmenter les moyens/réduire les obstacles pour accroître les capacités.
- **La modélisation** *(modelling)*: fournir un exemple auquel les gens peuvent aspirer ou qu'ils peuvent imiter.
- **La restructuration environnementale** *(environnemental restructuring)*: changer le contexte physique ou social.
- **Les restrictions** *(restrictions)*: utiliser des règles pour réduire la possibilité d'adopter le comportement cible ou pour augmenter le comportement cible en réduisant la possibilité d'adopter des comportements concurrents.

Enfin, la dernière couche (en gris) propose **sept catégories de politique, qui représentent les mécanismes ou approches de gouvernance pour faciliter ou soutenir la mise en œuvre des interventions**. Ces catégories incluent :

- **Les lignes directrices** *(guidelines)*: créer des documents qui recommandent ou imposent la pratique. Cela inclut toutes les modifications apportées à la prestation de services.
- **La planification environnementale et sociale** *(environnemental/social planning)*: concevoir et/ou contrôler l'environnement physique ou social.
- **La communication et marketing** *(communication and marketing)*: utiliser des médias imprimés, électroniques, téléphoniques ou audiovisuels.
- **La législation** *(legislation)*: faire ou modifier des lois.
- **La prestation de services** *(service provision)*: fournir un service.
- **Les règlements** *(régulation)*: établir des règles ou des principes de comportement ou de pratique.
- **Les mesures fiscales** *(fiscal measures)*: utiliser le système fiscal pour réduire ou augmenter le coût financier des comportements désirables ou indésirables.

Cette structure permet d'**aborder le changement à travers une approche à la fois comportementale, environnementale et politique**, assurant ainsi une couverture complète des facteurs influençant le comportement humain [8].

Utilisation de la RCC

La RCC a été largement testée et utilisée dans divers domaines de la santé, où elle a montré son efficacité. Elle a notamment servi à concevoir des interventions visant à réduire le temps passé assis au travail [9], à améliorer la qualité des conversations sur l'activité physique dans les soins de santé [10], à renforcer la maîtrise de soi dans les comportements de santé [11], à développer des interventions basées sur la technologie pour les personnes âgées [12] et à concevoir des programmes de sevrage de la consommation de tabac [13]. Ces exemples montrent **la flexibilité et l'efficacité du modèle RCC pour influencer et modifier les comportements humains dans des contextes variés**.

Dans le domaine de la cybersécurité, la RCC n'a pas encore été pleinement exploitée ni testée de manière systématique. Les recherches actuelles se sont principalement concentrées sur son application potentielle dans le développement de campagnes et de programmes de sensibilisa-

-tion, sans toutefois l'utiliser pour changer concrètement les comportements ou évaluer son efficacité sur le terrain.

Par exemple, des chercheurs néerlandais ont analysé des campagnes gouvernementales de cybersécurité et ont observé que celles-ci se focalisent principalement sur l'éducation et la sensibilisation, sans tirer parti de l'ensemble des techniques de changement de comportement proposées par la RCC [14]. Les auteurs soulignent également l'absence d'études mesurant l'impact direct de ces campagnes sur les comportements des citoyens. Selon eux, **bien que les campagnes actuelles visent à accroître la sensibilisation, elles ne parviennent pas à provoquer un véritable changement de comportement**. Informer les utilisateurs sur les menaces ne suffit pas, car **il n'existe pas de preuve que la simple sensibilisation mène à des comportements plus sécurisés**. Le manque de diversité dans les techniques d'intervention employées est mis en avant, les campagnes se limitant souvent à l'éducation et à la persuasion. Pour remédier à cette situation, il est essentiel d'intégrer des théories et techniques de changement de comportement, comme celles identifiées par la RCC. **Les auteurs recommandent donc d'adopter des approches plus structurées et spécifiques aux comportements en cybersécurité, en ciblant des groupes particuliers de la population et en intégrant une plus grande variété de techniques issues de la RCC** afin de maximiser l'impact de ces campagnes.

D'autres chercheurs ont également souligné **le manque de fondement théorique dans les programmes de formation à la cybersécurité en milieu organisationnel** [15, 16]. Ce déficit théorique limite leur capacité à provoquer des changements de comportement durables. Il est donc recommandé d'utiliser la RCC pour structurer les programmes de sensibilisation et de formation à la cybersécurité afin de les rendre plus efficaces [15]. Il est également nécessaire d'élaborer des programmes de cybersécurité fondés sur la RCC afin de renforcer la conformité proactive des employés aux politiques de sécurité [16].

Enfin, d'autres chercheurs ont proposé quant à eux, un cadre fondé sur la RCC et le modèle COM-B pour concevoir des programmes de formation plus efficaces, notamment en **se concentrant sur l'analyse des écarts comportementaux et sur la révision des politiques existantes** [17].

Ces études s'accordent sur le fait que les programmes de cybersécurité ne reposent pas suffisamment sur des bases théoriques solides [14, 15, 16]. Elles soulignent aussi que la sensibilisation seule ne suffit pas à changer durablement les comportements. De plus, la plupart des études évaluent l'efficacité des formations immédiatement après leur mise en œuvre, sans prendre en compte la diminution progressive de la rétention des compétences au fil du temps [7].

Étapes de son utilisation

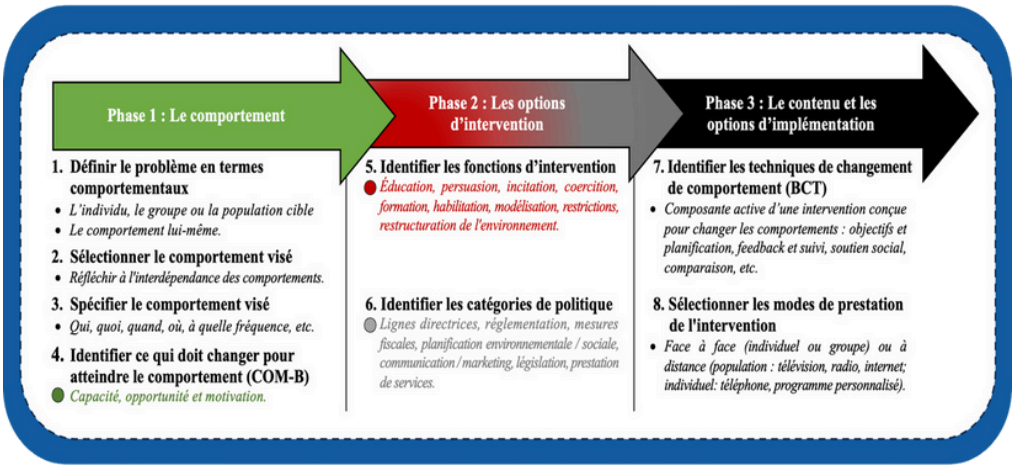
La RCC n'ayant pas encore été systématiquement testée dans le domaine de la cybersécurité, voici un exemple fictif de son application pour développer une intervention, en suivant les huit étapes réparties en trois phases principales présentes à la **Figure 2**.

Exemple : Une entreprise en pleine croissance avec 300 employés fait face à une augmentation des incidents d'hameçonnage. Bien que la cybersécurité soit valorisée, le comportement attendu – signaler les courriels suspects et éviter de cliquer sur les liens ou pièces jointes – n'est pas toujours adopté. Les employés sont surchargés et l'équipe TI, composée de seulement deux professionnels, est limitée en termes de disponibilité.

Phase 1

La première phase de l'utilisation de la RCC consiste à **comprendre le comportement**. Tout d'abord, il est essentiel de définir précisément le problème en identifiant le niveau d'intervention

Figure 2. Schéma des phases et étapes de l'utilisation de la RCC



qu'il soit individuel, de groupe ou à l'échelle de l'entreprise et de spécifier clairement le comportement à modifier (étape 1) [8]. Par exemple, **plutôt que de viser un objectif vague comme réduire l'impact de l'hameçonnage, il est préférable de se concentrer sur des actions spécifiques comme identifier les courriels suspects, ne pas cliquer sur les liens, les signaler et les supprimer** [15].

Cependant, ce comportement est influencé par de nombreux facteurs contextuels et environnementaux. L'étape suivante consiste donc à **sélectionner le comportement cible en tenant compte des interdépendances possibles et en évaluant les comportements potentiels selon leur impact, leur facilité de changement et leur centralité** (étape 2) [8]. Dans ce cas précis, cela pourrait inclure la pression liée à la productivité [18], le volume de courriels reçus quotidiennement [19] ou encore la disponibilité de l'équipe TI [20].

Une fois le comportement cible identifié, **il est crucial de le spécifier en détail** (étape 3) : qui doit adopter ce comportement, ce qui doit être fait, quand, où, à quelle fréquence et avec qui (voir **Tableau 1**).

Enfin, il est nécessaire **d'identifier les changements à apporter chez les individus ou dans l'environnement pour encourager ce comportement** (étape 4). En utilisant le modèle COM-B, on peut déterminer les sources du comportement. Les principales sources problématiques sont :

- **Opportunité physique**: les outils et infrastructures pour signaler les courriels suspects sont insuffisants et l'environnement de travail ne permet pas de signaler ces courriels sans ressentir une pression de temps.
- **Motivation automatique**: le signalement des courriels suspects n'est pas encore une habitude intégrée dans les pratiques des employés.

En revanche, **certains facteurs favorisent déjà l'adoption du comportement souhaité**. Les employés ont les capacités nécessaires pour identifier et signaler les courriels suspects, car ils possèdent les compétences cognitives et techniques requises (capacité psychologique et physique). De plus, l'environnement social semble favorable, c'est-à-dire que l'organisation valorise la cybersécurité et encourage ces bonnes pratiques (opportunité sociale). Enfin, leur motivation réflexive est présente, ce qui signifie qu'ils comprennent l'importance de signaler les tentatives d'hameçonnage et qu'ils sont prêts à le faire lorsque les conditions le permettent.

Ainsi, **le problème ne réside pas tant dans un manque de compétences ou de volonté, mais plutôt dans des obstacles structurels et contextuels**, comme l'absence d'outils facilitant le signalement ou un environnement de travail qui impose une charge cognitive trop élevée

pour que cette action devienne une habitude.

Tableau 1. Spécification du comportement identifié

Qui	Les employés du bureau
Quoi	Reconnaître un courriel d'hameçonnage, ne pas cliquer sur les liens ou pièces jointes et signaler ce courriel via un bouton signaler le courriel.
Quand	Chaque fois qu'ils reçoivent un courriel qui contient des signes typiques d'hameçonnage (ex. : demande urgente d'informations sensibles, fautes d'orthographe, expéditeur inconnu).
Où	Dans leur messagerie professionnelle, à la fois sur leur ordinateur de bureau et sur leurs appareils mobiles utilisés pour le travail.
À quelle fréquence	Chaque fois qu'ils reçoivent un courriel suspect.

Phase 2

La phase 2 consiste à **identifier les options d'intervention**. Elle commence par l'étape 5, qui exige de **choisir les fonctions d'intervention en s'appuyant sur les éléments du modèle COM-B** identifiés à l'étape 4. Comme le montre le **Tableau 2**, toutes les interventions ne sont pas pertinentes selon la source du comportement identifié. Dans notre exemple, pour résoudre les problèmes liés à l'opportunité physique, seules la formation, les restrictions, les restructurations environnementales et l'habilitation seraient pertinentes. En revanche, pour aborder la motivation automatique, les fonctions d'intervention incluraient la persuasion, l'incitation, la coercition, la formation, la modélisation, ainsi que la restructuration environnementale et l'habilitation.

En prenant cette étape en considération, il devient évident que **les résultats mitigés des formations anti-hameçonnage pourraient être dus à une inadéquation entre l'intervention choisie et la source du problème**. Des chercheurs ont souligné que, malgré des ateliers répétés, les employés stagnent dans leur capacité à détecter les tentatives d'hameçonnage [21].

Même avec des formations en ligne spécifiquement axées sur l'hameçonnage, ceux qui cliquent fréquemment sur des courriels d'hameçonnage ne montrent qu'une amélioration marginale, suggérant ainsi un rendement décroissant des méthodes de formation traditionnelles. Cela indique que, **bien que les employés possèdent les compétences requises, d'autres facteurs contextuels influencent leur comportement**. Par exemple, face à une charge de travail élevée, un employé peut lire ses courriels en diagonale. De plus, si le service informatique est difficilement accessible – avec seulement deux techniciens pour 300 employés – ou si les questions sont perçues comme dérangeantes, cela dissuade les employés de demander de l'aide [20]. La crainte du jugement en cas d'erreur peut également limiter leur volonté de poser des questions [22], réduisant ainsi l'efficacité des formations.

Une fois les fonctions d'intervention identifiées, **il faut les évaluer selon les critères APEASE**:

Tableau 2. Matrice des liens entre les sources COM-B et les fonctions d'intervention

Sources COM-B	Fonctions d'intervention								
	Éducation	Persuasion	Incitation	Coercition	Formation	Restriction	Restructuration environnementale	Modélisation	Habilitation
Capacité physique					x				x
Capacité psychologique	x				x				x
Opportunité physique					x	x	x		x
Opportunité social						x	x	x	x
Motivation automatique		x	x	x	x		x	x	x
Motivation réflective	x	x	x	x					

acceptabilité, praticabilité, efficacité/coût-efficacité, abordabilité, effets secondaires/sécurité et équité (***A****cceptability*, ***P****racticability*, ***E****ffectiveness*, ***A****ffordability*, ***S****pill-over effects*, ***E****quity*, en anglais) [8]. Après cette évaluation, seules la restructuration environnementale et l'habilitation sont retenues, les autres interventions (formation, sensibilisation, modélisation, persuasion, incitation) étant jugées non pertinentes ou non souhaitables (coercition, restriction).

À l'étape 6, il s'agit d'identifier les catégories de politiques en fonction des interventions retenues à l'étape 5. Comme le montre le **Tableau 3**, toutes les catégories de politiques ne sont pas adaptées à chaque intervention [8]. Dans cet exemple, les politiques identifiées incluent les mesures fiscales, la réglementation, les lignes directrices, la planification environnementale et sociale, la législation, ainsi que la prestation de services.

Toutefois, **la capacité d'une organisation à mettre en œuvre ces politiques dépend de son niveau d'influence et de ses ressources**. Par exemple, une entreprise de 300 employés ne pourra pas modifier une législation, une action qui relève plutôt des gouvernements et des instances réglementaires lorsqu'ils souhaitent induire des changements de comportement à grande échelle. En revanche, elle peut mettre en place des lignes directrices internes, restructurer l'environnement de travail, adapter ses politiques de cybersécurité ou investir dans des solutions techniques favorisant le signalement des courriels suspects. Ainsi, **la sélection des catégories de politiques doit être réaliste et alignée sur les capacités et le champ d'action de l'organisation concernée**.

Comme pour l'étape précédente, il est nécessaire d'évaluer si ces catégories de politiques répondent aux critères APEASE [8]. Après cette évaluation, seules la réglementation, les lignes directrices, la planification environnementale et sociale et la prestation de services sont retenues.

Phase 3

La phase 3 consiste à définir le contenu et les options d'implémentation à travers deux étapes : identifier les techniques de changement de comportement (TCC) (*Behavior Change Technique* en anglais) (étape 7) et choisir le mode de livraison (étape 8) [8]. Une TCC est défi-

Tableau 3. Matrice de liens entre les fonctions d'intervention et les catégories de politique

Catégories de politique	Fonctions d'intervention								
	Éducation	Persuasion	Incitation	Coercition	Formation	Restriction	Restructuration environnementale	Modélisation	Habilitation
Communication/ marketing	x	x	x	x	x	x	x		x
Lignes directrices			x	x	x		x		x
Mesures fiscales	x	x	x	x	x	x	x		x
Réglementations	x	x	x	x	x	x	x		x
Législation	x	x	x	x	x	x	x	x	x
Planification environnementale / sociale							x		x
Prestation de services	x	x	x	x	x			x	x

-nie comme « **une composante active d'une intervention conçue pour modifier les comportements** » [8]. Cette composante doit être observable, reproductible et constituer une partie irréductible d'une intervention, servant ainsi d'ingrédient actif dans le changement de comportement. Les TCCs peuvent inclure des éléments tels que la fixation d'objectifs et la planification, la rétroaction et le suivi, le soutien social ou encore la comparaison des comportements. Il existe une liste de 16 groupes de BCTs disponibles à cet effet.

En évaluant ces TCCs selon les critères APEASE, on identifie des techniques mieux adaptées telles que :

- **La restructuration de l'environnement physique et social**: par exemple, l'ajout d'un bouton de signalement intégré directement dans la messagerie des employés pour faciliter le signalement des courriels suspects [7].
- **L'invitation ou l'utilisation de signaux**: l'affichage de rappels visuels , comme une bannière dans un courriel indiquant les signes caractéristiques d'un courriel d'hameçonnage
- **Le soutien social**: la mise en place de groupes d'entraide ou de référents en cybersécurité au sein des équipes pour encourager le partage des bonnes pratiques et réduire l'hésitation à poser des questions.
- **La planification d'actions**: l'intégration d'un processus standardisé où chaque employé, lors de la réception d'un courriel suspect, suit une procédure claire et préétablie (ex. : vérifier l'expéditeur, signaler, supprimer).

Ces stratégies, en facilitant l'adoption des comportements sécuritaires au quotidien, augmentent les chances que ces derniers deviennent des habitudes durables au sein de l'organisation.

Enfin, à l'étape 8, il est essentiel de déterminer le ou les modes de prestation de l'intervention. Cela peut se faire en face à face (en individuel ou en groupe) ou à distance, que ce soit à l'échelle de la population (par la télévision, la radio, internet, etc.) ou de manière individualisée (via le téléphone, un programme personnalisé, etc.) [8]

Conclusion

En conclusion, bien que l'humain soit souvent perçu comme le maillon faible en cybersécurité, cette vision simplifie excessivement un problème complexe [7]. Se concentrer exclusivement sur la formation et la responsabilisation individuelle revient à négliger des facteurs contextuels et organisationnels qui limitent l'efficacité des interventions [23]. **La roue des changements de comportements propose une approche plus globale, en tenant compte non seulement des comportements individuels, mais aussi des environnements physique et social, ainsi que des réformes structurelles nécessaires** [8]. Son application, encore peu explorée dans le domaine de la cybersécurité, pourrait offrir des solutions plus durables, en équilibrant sensibilisation, soutien organisationnel et infrastructures adaptées [14, 15, 16, 17]. Ce cadre, déjà éprouvé dans d'autres domaines, montre un potentiel important pour transformer les stratégies de prévention des cyberattaques et répondre plus efficacement aux vulnérabilités humaines.

Il est essentiel que **les interventions en cybersécurité soient alignées avec les véritables sources de comportement**, comme le suggère le modèle COM-B. Insister sur des solutions inappropriées, comme la formation ou la sensibilisation, lorsqu'elles ne ciblent pas les obstacles réels, revient à enfoncer un clou déjà planté, laissant d'autres aspects cruciaux, qui soutiennent un comportement sécurisé, de côté.

Pour que les comportements souhaités soient réellement adoptés, il est crucial de diversifier les approches et d'utiliser les bonnes interventions au bon moment. Cela nécessite une compréhension fine des facteurs influençant le comportement et l'application de techniques et de politiques adaptées au contexte, comme le recommande la RCC. Ce n'est qu'en adoptant cette approche holistique et stratégique que les organisations pourront espérer renforcer durablement la sécurité numérique de leurs employés [24].

Références

[1] Branley-Bell, D., Coventry, L. et Sillence, E. (2021). Promoting Cybersecurity Culture Change in Healthcare. *Proceedings of the 14th PErvasive Technologies Related to Assistive Environments Conference*, 544-549.

[2] Alshaikh, M., Maynard, S. B. et Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computer & Security*, *100*.

[3] Tsohou, A., Karyda, M., Kokolakis, S. et Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24*(1), 38-58.

[4] Posey, C., Roberts, T. L. et Lowry, P. B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems*, *32*(4), 179-214.

[5] Reinheimer, B., Aldag, L., Mayer, P. et Mossano, M. (2020). *An investigation of phishing awareness and education over time : When and how to best remind users*.

[6] Lain, D., Kostiainen, K. et Capkun, S. (2021). Phishing in Organizations : Findings from a Large-Scale and Long-Term Study (arXiv:2112.07498). arXiv.

[7] Bergeron, A. (2024, avril 26). Maximizing Employee Protection by Rethinking Expectations of Phishing Awareness and Email Security. *GoSecure*.

[8] Michie, S., van Stralen, M.M. et West, R.(2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Sci*, *6*(42).

[9] Munir, F., Biddle, S. J. H., Davies, M. J., Dunstan, D., Esliger, D., Gray, L. J., Jackson, B. R., O'Connell, S. E., Yates, T. et Edwardson, C. L. (2018). Stand More AT Work (SMArT Work) : Using the behaviour change wheel to develop an intervention to reduce sitting time in the workplace. *BMC Public Health*, *18*(1), 319.

[10] Reid, H., Smith, R., Williamson, W., Baldock, J., Caterson, J., Kluzek, S., Jones, N. et Copeland, R. (2022). Use of the behaviour change wheel to improve everyday person-centred conversations on physical activity across healthcare. *BMC Public Health*, *22*(1), 1784.

[11] Aldulaimi, saeed H., Abdeldayem, M. M. et Abdelhakim, M. N. A. (2020). Developing a Planned Intervention Using the Behavior Change Model to Improve Self-control of Healthcare Employees : A Longitudinal Study. *Research Square*.

[12] Direito, A., Michie, S., Lefevre, C. E. et Collins, E. I. M. (2017). Application of the behaviour change wheel framework to the development of interventions within the City4Age project. 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 1-6.

13] Gould, G. S., Bar-Zeev, Y., Bovill, M., Atkins, L., Gruppetta, M., Clarke, M. J. et Bonevski, B. (2017). Designing an implementation intervention with the Behaviour Change Wheel for health provider smoking cessation care for Australian Indigenous pregnant women. *Implementation Science*, *12*(1), 114.

[14] van Steen, T., Norris, E., Atha, K. et Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity*, *6*(1).

[15] Alshaikh, M., Maynard, S., & Ahmad, A. (2019, juin 8). *Toward sustainable behaviour change : an approach for cyber security education training and awareness*.

[16] Zheng, R., Cowan, G., Rong, R., Xinjing, L., Yanjun, W. et Ping, H. (2024). Cybersecurity Crafting Intervention Model Based on Behaviors Change Wheel. Dans H. Jahankhani, G. Bowen, M. S. Sharif, et O. Hussien (Éds.), *Cybersecurity and Artificial Intelligence : Transformational Strategies and Disruptive Innovation* (p. 281-307). Springer Nature Switzerland.

[17] Thamae, R., Abdullah, H. et Mujinga, M. (2024). Toward a Framework to Improve Employees' Compliance with Cybersecurity Policy in Organizations. Dans X.-S. Yang, R. S. Sherratt, N. Dey, et A. Joshi (Éds.), *Proceedings of Eighth International Congress on Information and Communication Technology* (p. 359-369). Springer Nature.

[18] Jalali, M. S., Bruckes, M., Westmattelmann, D. et Schewe, G. (2019). Why Employees (Still) Click on Phishing Links : An Investigation in Hospitals (SSRN Scholarly Paper 3317498). *Social Science Research Network*.

[19] Sarno, D. M. et Neider, M. B. (2022). So Many Phish, So Little Time : Exploring Email Task Factors and Phishing Susceptibility. *Human Factors*, *64*(8), 1379-1403.

[20] Brenner, P. S. (2019). Can Phishing Tank Survey Response Rates? Evidence from a Natural Experiment. *Field Methods*, *31*(4), 295-308.

[21] Nwankpa, J., Shan, (Jay) Zhe, Merhout, J., Benamati, J. et Weese, M. (2023). A Social Engineering Research Partnership in Higher Education to Improve Information Security Education, Training, and Awareness (SETA) Programs. *AMCIS 2023 Proceedings*.

[22] Lee, F. (2002). The Social Costs of Seeking Help. *The Journal of Applied Behavioral Science*, *38*(1), 17-35

[23] Simonet, J. et Teufel, S. (2019). The Influence of Organizational, Social and Personal Factors on Cybersecurity Awareness and Behavior of Home Computer Users. Dans G. Dhillon, F. Karlsson, K. Hedström et A. Zúquete (Éds.), *ICT Systems Security and Privacy Protection* (p. 194-208). Springer International Publishing.

[24] Alotaibi, F., Clarke, N. et Furnell, S. (2017). An analysis of home user security awareness & education. *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, 116-122.

.