CRPC | Chaire de recherche en prévention de la cybercriminalité

Notes *de synthèse*

Vol. 4, Num. 8
2024

Les coups de pouces (*nudges*) appliqués à la cybersécurité

Jade Philibert, candidate à la maîtrise en criminologie

Introduction

En 2008, Thaler et Sunstein ont écrit le livre *Nudge: Improving decisions about health, wealth, and happiness* [1] portant sur les coups de pouce (*nudges*), **ces interventions douces qui visent à modifier les comportements des individus sans toutefois leur enlever leur liberté de choix**. Thaler et Sunstein décrivent chacune des étapes qui influencent les choix d'un individu, et proposent donc de modifier l'architecture des choix pour influencer positivement la prise de décision [1]. Plus précisément, le terme NUDGES fonctionne également comme un acronyme permettant de se rappeler aisément les six principes essentiels guidant ce type d'intervention : « **iNcentives, Understand mappings, Defaults, Give feedback, Expect errors, Saliency/Structuring complex choices** » [1]. Ces principes pourraient être traduits ainsi : **Incitatifs**, **compréhension de l'effet des choix sur les résultats**, **options par défaut**, **donner une rétroaction**, **anticiper les erreurs** et **aider l'individu à faire des choix complexes**. Les coups de pouce sont principalement utilisés pour aider les individus à faire les bons choix, dans leur propre intérêt ou pour celui de la société, même si leur efficacité est controversée, en plus des enjeux éthiques qui y sont associés et qui ont donné lieu à des débats importants*****.

Les coups de pouce sont utilisés et appliqués, depuis une quinzaine d'années dans divers domaines tels que la santé, les assurances, les régimes de retraite et la sécurité routière [1, 2, 3]. Dans tous ces domaines, **les coups de pouce ont pour objectif de limiter les impacts négatifs des biais cognitifs** dans la prise de décisions** [5]. Plutôt que d'espérer vainement supprimer les biais cognitifs, l'originalité de l'approche par coups de pouce réside dans le fait qu'**elle va plutôt exploiter ces biais cognitifs pour améliorer différents aspects sociaux de la vie des individus et de la société**. La cybersécurité et la prévention de la cybercriminalité n'y font pas exception. Depuis quelques années, la technique des coups de pouce a été adoptée dans ces deux domaines [5]. En effet, le maintien de la sécurité numérique des individus et des entreprises est directement lié aux choix et actions des citoyens et travailleurs, justifiant ainsi l'application de coups de pouce dans ces domaines [6].

Cette note de synthèse propose une revue des connaissances actuelles sur les coups de pouce dans le domaine de la cybersécurité. Plus précisément, les caractéristiques de ceux-ci et les différents mécanismes d'interventions dans

***** Voir par exemple cet article dans la revue de l'INSERM

****** Pour en savoir plus sur les biais cognitifs, consultez la note de synthèse vol. 4, num. 6

lesquelles ces coups de pouce s'insèrent seront abordés. Pour finir, la conclusion discutera des implications éthiques et des limites des coups de pouce, et formulera quelques recommandations.

Caractéristiques et éléments essentiels d'un coup de pouce

Plusieurs termes sont utilisés dans la littérature pour aborder ce type d'intervention : *nudge*, *nudging* [5], ou *digital nudging* [7], pour ne nommer que les principaux. Un coup de pouce peut prendre la forme d'un message mentionnant la possibilité d'être infecté par un virus si la navigation internet ne se fait pas de manière sécuritaire [8], d'un message invitant à la création d'un mot de passe plus robuste [9], ou encore d'avertissements indiquant s'il est judicieux ou non de télécharger un logiciel de sécurité via un site internet ou une application mobile [10, 11, 12].

Les **principales caractéristiques** partagées par la majorité des coups de pouce, quels que soient les domaines d'application, sont les suivantes :

Premièrement, pour qu'un coup de pouce soit efficace, **les avantages et les intentions derrière son application doivent être clairement établis et transparents** [4, 5, 10, 12]. En effet, lorsque le but qui soutient sa mise en place est manifeste, les individus ne vont pas suivre aveuglément les directives ou les choix qui leur sont proposés et vont ainsi mieux comprendre ce qui est visé par le coup de pouce [5, 11, 13]. Bien évidemment, **pour qu'un coup de pouce soit plus efficace, l'individu qui y est exposé doit en comprendre le fonctionnement et l'objectif** [4, 7]. Si l'individu comprend son utilité, il sera plus en mesure de prendre les décisions adéquates et de mieux comprendre comment ses actions vont améliorer la cybersécurité [5]. Également, les coups de pouce ne doivent pas être utilisés de manière excessive. Ils doivent apparaître de manière occasionnelle, et ils doivent être ajustés aux besoins de l'entreprise ou des systèmes pour lesquels il y a un désir d'améliorer la cybersécurité [11].

De surcroît, **l'apparence visuelle du coup de pouce** pourrait avoir un impact sur la prise de décision de l'individu. En effet, l'apparence que l'on donne aux messages ou à l'énoncé qui apparaîtra comme rappel des conséquences de la mesure ou du comportement adéquat à adopter est cruciale pour l'efficacité du coup de pouce. Par exemple, la couleur, la forme et l'ajout de symboles pourraient avoir un impact sur les précautions de cybersécurité prises par l'individu [5, 13]. De plus, **le contenu d'un message** pourrait également avoir un impact sur l'efficacité du coup de pouce, tel que des messages de rappel de mises à jour d'un système non intrusif et succincts [14] ou des suggestions et conseils pratiques pour la création d'un mot de passe [15, 16].

Un coup de pouce peut s'appuyer principalement sur l'aspect visuel du message devant être véhiculé aux usagers [11]. **La structure de la présentation du coup de pouce pourrait avoir un impact sur la diminution des effets négatifs des biais cognitifs**, tels que le biais de simplification* et le biais de représentativité** [11, 17]. Dans la littérature scientifique actuelle, plusieurs chercheurs ont abordé la présentation des coups de pouce. Par exemple, une étude réalisée en 2020 a examiné le taux de comparution à la Cour des accusés après leur remise en liberté, alors qu'ils attendaient leur audience. Les auteurs ont observé que, simplement en modifiant l'ordre des informations présentées aux accusés dans les formulaires qui leur sont remis lors de leur libération, le taux de non-comparution des accusés avait diminué de 13% à 21% [20]. Un autre chercheur ajoute que **pour qu'un coup de pouce soit compris de tous, la présentation doit être simple et la navigation**

---

* Le biais de simplification se produit lorsque des individus simplifient les informations ou les décisions complexes en utilisant des raccourcis. Ces raccourcis permettent de réduire la complexité de la prise de décision.

** Le biais de représentativité se produit lorsque des individus jugent la probabilité d'un événement en se basant sur la ressemblance de cet événement à un autre existant, plutôt que sur des faits ou données probantes.

à travers le coup de pouce (messages, programmes, courriel) **doit être intuitive** [4]. Généralement, pour maximiser l'effet souhaité, le coup de pouce s'appuiera sur d'autres mécanismes d'interventions, en plus d'avoir une présentation attrayante.

Un autre aspect très important à prendre en compte dans la mise en place d'un coup de pouce est **l'élément temporel** [17]. En effet, **le moment choisi pour déclencher un coup de pouce aurait un effet sur l'influence qu'il pourrait avoir sur la prise de décision de l'individu** pour améliorer sa sécurité personnelle ou celle de l'entreprise [17]. Par exemple, des chercheurs ont tenté de tester la temporalité du coup de pouce pour la création d'un mot de passe dans un jeu en ligne dans lequel les participants pouvaient choisir ou non d'utiliser cette fonction de sécurité. Certains participants ont reçu un coup de pouce les invitant à créer un mot de passe dès le début du jeu alors que d'autres participants ne recevaient ce coup de pouce que plus tard dans le jeu, après avoir choisi les caractéristiques de leur personnage. Ces chercheurs ont conclu que pour les participants ayant reçu le coup de pouce après avoir commencé le jeu, le message de rappel aurait davantage d'effets sur la mesure de sécurité prise (mise en place d'un mot de passe pour accéder au jeu plutôt que ne pas créer un mot de passe). Les résultats de cette étude pourraient être transposés à d'autres contextes de sécurité. Ceci n'est néanmoins qu'un exemple et **les résultats de la littérature ne sont pas unanimes**. Certains chercheurs estiment qu'une pause dans les actions effectuées par les individus, induite par un coup de pouce, pourrait être bénéfique [18], tandis que d'autres mentionnent plutôt que l'interruption pourrait être défavorable et les mesures de sécurité préconisées pourraient être ignorées [17, 19].

Après ce rapide survol des caractéristiques essentielles d'un coup de pouce, nous allons passer en revue les éléments sur lesquels interviennent les coups de pouce pour la prise de décision.

Mécanismes d'intervention

Cadrage

Le domaine de la cybersécurité ne fait pas exception à l'application d'un coup de pouce mettant de l'avant un mécanisme de cadrage. Celui-ci consiste à **sélectionner judicieusement et à ordonner les avantages et les risques reliés aux choix à prendre par l'usager** [11]. L'individu sera ainsi plus en mesure d'évaluer l'ensemble des options qui s'offrent à lui. Toutefois, **cette présentation pourrait être perçue comme positive ou négative par l'individu** [10]. Des chercheurs ont mené en 2021 une étude portant sur l'acceptation des témoins de connexion (les fameux *cookies*), qui sont directement liés à la vie privée des usagers [20]. Ces chercheurs ont trouvé qu'**en termes de sécurité, l'ajout d'une barre de couleurs représentant le nombre de témoins de connexion acceptés par l'utilisateur lors de la navigation sur le web** (vert – aucun témoin -, jaune, orange, rouge – tous les témoins) **serait efficace en aidant l'individu à mieux définir ses préférences sur le nombre de témoins de connexion accumulés lors de sa navigation et exercerait une influence positive sur ses choix** [20]. La présentation et l'ordre dans lequel les informations sont exposées à l'individu pourraient alors exercer une influence quant à l'adéquation du coup de pouce. Ceci n'est toutefois pas confirmé par l'ensemble des études [6, 11]. **D'après d'autres études, présenter un coup de pouce avec un cadrage positif** (soulignant les avantages) **comparativement à un coup de pouce avec un cadrage négatif** (mettant en avant les risques, comme la perte ou le vol de données et la réduction de la performance de l'appareil) **pourrait ne pas occasionner de différence sur l'efficacité de celui-ci, et ce, peu importe la situation** [10, 12]. Il y aurait alors matière à continuer les recherches en cybersécurité sur les effets d'un coup de pouce à cadrage positif ou négatif.

Information

Le coup de pouce peut viser à informer et à éduquer les individus sur les choix judicieux à prendre [5, 11]. En plus d'un cadrage adéquat du problème faisant l'objet du coup de pouce, une portion de celui-ci peut porter sur l'éducation de l'individu pour activer sa prise de décision [5]. Ce type d'information jumelée à un cadrage adéquat du coup de pouce contribuerait aux changements de comportements et de décisions des individus [8]. Toutefois, bien que le coup de pouce communique une information pertinente, il n'y a pas de garantie que l'utilisateur répondra adéquatement à la technique [11].

Une stratégie adoptée pour surmonter ce défi est **la personnalisation du coup de pouce selon les caractéristiques et biais cognitifs des individus** [5, 15]. Il y aurait toutefois une modération des effets des coups de pouce personnalisés, selon les différents styles de prise de décisions des individus [15]. Le domaine de prédilection pour l'utilisation des coups de pouce en cybersécurité est actuellement lié aux mots de passe. En effet, une grande partie de la littérature scientifique portant sur les coups de pouce en cybersécurité est liée à l'évaluation du choix de mots de passe [9, 14, 15, 16, 21]. Par exemple, **des chercheurs ont évalué la personnalisation des coups de pouce aux différents styles de prise de décisions**, soient : « le style général de prise de décision (General Decision-Making Style [GDMS]***** ; le besoin de cognition (need for cognition [NFC])****** ; la prise en compte des conséquences futures (Consideration for Future Consequences [CFC])******* et la numératie********». Ces chercheurs ont constaté qu'**un coup de pouce personnalisé au style de prise de décision d'un individu le conduirait à créer un mot de passe plus robuste que lorsqu'un coup de pouce non personnalisé lui est présenté** [15, 16].

Les études qui portent sur la création de mots de passe plus robustes établissent quelques résultats pertinents. Premièrement, **plusieurs coups de pouce liés aux mots de passe ont été testés**, par exemple « le compteur de mots de passe » et « le temps de craquage » [11, 15, 16]. Ces coups de pouce peuvent être efficaces pour aider les usagers à améliorer leurs mots de passe [11, 15, 16]. Deuxièmement, **les coups de pouce en lien avec le mot de passe seraient plus efficaces en raison de la rétroaction** (*feedback*) **immédiate après la création celui-ci** [11, 15, 16].

Défaut

Le coup de pouce qui suit un modèle par défaut consiste à ce que l'usager suive les paramètres déjà établis, sans avoir à se poser de questions [11, 21]. Par exemple, par défaut, l'option de chiffrement des conversations des téléphones intelligents est activée par tous les fournisseurs de services, plutôt que de laisser aux consommateurs le choix de recourir à cette fonctionnalité [5]. Ainsi, l**a prise de décision est réduite et ne requiert pas d'efforts cognitifs pour l'individu** [4, 5, 11, 21]. L'option par défaut sera proposée à l'utilisateur si le comportement qui est adéquat et recommandé est trop complexe et demande trop d'efforts et de concentration [22].

Ainsi, comparativement à la personnalisation du coup de pouce, **l'option par défaut est une solution unique et identique pour l'ensemble des individus** [23]. Concrètement, en cybersécurité, le coup de pouce par défaut peut être lié aux paramètres de vie privée d'un site internet [22]. De plus, pour tous domaines confondus, l'option par défaut est privilégiée par les individus dans la majorité des cas et s'avère une stratégie d'intervention relativement efficace [4, 23]. Il est donc utile de créer des coups de pouce par défaut qui sont alignés avec le comportement recherché [4]. Plusieurs raisons peuvent expliquer que les individus souscrivent à l'option par défaut, telles que la peur de perdre quelque chose ou encore le manque d'informations sur les alternatives possibles qui poussent les utilisateurs à suivre le coup de pouce par défaut, par exemple, en disposant d'une explication incomplète quant aux conséquences d'adhérer ou non à une configura-

-tion privée plus élevée [1, 21, 23]. De surcroît, si les individus n'ont pas beaucoup de connaissances ou ne sont pas familiers avec le choix à faire, ils se tourneront vers l'option par défaut, qui les informe suffisamment et représente un risque d'erreur réduit [23].

Incitation

L'incitation est reliée aux avantages et aux conséquences qui peuvent découler d'un choix, et qui visent à inciter les gens à agir [8, 11, 24, 25, 26]. L'incitation est souvent utilisée en combinaison avec d'autres mécanismes d'intervention, puisqu'elle est souvent **sous-jacente à l'ensemble des coups de pouce**. Plus particulièrement, **l'incitation est liée au coup de pouce de cadrage positif et négatif** [11, 12]. Dans le cadrage, le corps du texte incite l'individu à prendre une décision adéquate alors que la disposition de l'information est plutôt liée à la présentation du coup de pouce [26].

Un exemple d'utilisation de l'incitation est l'apparition de fenêtres contextuelles (*pop-up*) contenant des messages d'encouragement ou des messages plus « menaçant » [27]. Ce deuxième type de message viserait à inciter à un comportement plus sécuritaire par le recours à la peur [27]. Néanmoins, les messages d'encouragement produiraient de meilleurs résultats au niveau de la modification des comportements que les messages reposant sur la peur [27].

De plus, **la technique de l'élimination est un coup de pouce lié à l'incitation qui est jugée relativement efficace** par certains chercheurs [17]. Celle-ci consiste à **mettre en place un message de type fenêtre contextuelle et d'inciter l'individu à prendre une décision dans le but d'éliminer les risques visés par le contenu du message**. La technique de l'élimination pourrait, par exemple, consister en un message incitant les utilisateurs d'un jeu vidéo à créer un mot de passe pour éliminer les risques d'usurpation d'identité de leur profil [17]. Cette technique conduirait les utilisateurs à por-ter une attention particulière à l'avertissement de sécurité et donc à créer un mot de passe plus robuste [17].

Influence sociale

L'influence sociale est un mécanisme d'intervention par coup de pouce qui est régulièrement évalué dans la littérature et qui serait le plus efficace [4, 16, 28, 29]. **Un coup de pouce qui relève de l'influence sociale utilisera les normes sociales dominantes et la comparaison sociale pour encourager une prise de décision et/ou un geste adéquat de la part de l'individu** [6, 25]. En cybersécurité, les coups de pouce s'appuyant sur l'influence sociale ont pour but de rendre les comportements souhaitables plus visibles en informant un utilisateur des actions entreprises par ses pairs. **L'influence sociale peut être positive ou négative**. Dans le premier cas, **on parle d'influence positive lorsqu'elle sert à motiver les utilisateurs à adopter des pratiques de sécurité plus strictes en les informant que « la plupart des gens utilisent des mots de passe forts » ou que « votre mot de passe est plus fort que celui de X % des utilisateurs »** [16]. Ce type de rétroaction peut encourager les individus à améliorer leurs propres comportements en matière de sécurité, car ils peuvent ressentir un sentiment d'appartenance ou de compétition avec leurs pairs. Par exemple, des chercheurs ont trouvé que 37% de leur échantillon (sur 50 000 utilisateurs de Facebook) était plus enclin à s'informer des dispositifs de sécurité disponibles (notifications de connexion à un nouvel appareil ; authentification à deux facteurs ; dispositif de sécurité par contacts de confiance) lorsqu'ils étaient informés du nombre d'amis Facebook qui utilisaient un dispositif de sécurité similaire [29]. **L'influence sociale négative se produit plutôt lorsque les utilisateurs sont informés que « de nombreuses personnes ont des mots de passe faibles » ou qu'« un pourcentage significatif d'utilisateurs a été compromis »**.

Comme mentionné dans la section *Information* de cette note de synthèse, plusieurs études en

cybersécurité portent sur les coups de pouce liés aux mots de passe. Tel est le cas dans une étude évaluant l'influence sociale sur la prise de décision de créer un mot de passe plus robuste [30]. Dans leur étude, les chercheurs ont démontré que **les participants qui recevaient une rétroaction sur la robustesse de leurs mots de passe en comparaison avec ceux de leurs pairs étaient plus enclins à générer des mots de passe plus forts**. D'autres chercheurs se sont également intéressés à l'efficacité des coups de pouce reposant sur l'influence sociale. Dans leur étude, les participants étaient invités à créer un mot de passe pour un faux compte sur le site d'une institution financière. L'objectif des chercheurs était d'évaluer l'efficacité de la recommandation de mots de passe, de l'influence sociale positive et négative. Les résultats de leur étude ont démontré que **l'influence sociale positive est plus efficace**, par exemple lorsque les utilisateurs reçoivent un message de type: « Votre mot de passe est plus fort que celui de 19.9% des utilisateurs » [16].

De surcroît, l'influence sociale a été utilisée pour évaluer les comportements de sécurité des employés à la suite d'une fausse fuite de données [28]. Les chercheurs ont effectué une expérimentation en envoyant un courriel à 76 employés, et ce, pour évaluer si un coup de pouce reposant sur une technique d'influence sociale aurait un impact sur la mise à jour sécuritaire des appareils électroniques de l'entreprise. Les résultats semblent indiquer que l'influence sociale aurait un effet sur la décision de l'employé d'effectuer les mises à jour [28]. Toutefois, **le coup de pouce était plus efficace lorsqu'il s'appuyait sur une norme sociale individuelle** (X% des employés ont déjà fait les mises à jour) **plutôt qu'un courriel de norme sociale d'équipe** (X% des employés dans votre équipe ont déjà fait les mises à jour) [28]. Les auteurs expliquent ce résultat par le fait que l**es individus perçoivent leur cyberhygiène de manière adéquate, et donc qu'il y aurait une certaine motivation associée à la comparaison avec les autres individus de l'entreprise** [28]. Au contraire, dans les cas de la norme sociale d'équipe, les individus comptaient sur la réception de plus d'informations sur la marche à suivre de la part de leurs collègues immédiats, retardant ainsi l'accomplissement des tâches liées à la cybersécurité [28].

Conclusion

Les coups de pouce faciliteraient la prise de décision vertueuse, tout en respectant l'autonomie des individus [31, 32]. Il y aurait néanmoins **des enjeux en lien avec le respect et l'intégrité des choix individuels et la responsabilité de créer des coups de pouce adéquats et nécessaires** [31]. Un autre enjeu important est que **les coups de pouce peuvent être utilisés de manière abusive ou porter atteinte à l'éthique qui est sous-jacente à ces interventions douces** [33]. Par exemple, une compagnie de sécurité pourrait utiliser des coups de pouce pour vendre son logiciel de protection, bien qu'il en existe des meilleurs sur le marché, rendant ainsi son acte non-éthique [31]. De plus, **si le coup de pouce n'est pas créé de manière à ce que les intentions derrière sa mise en application soient transparentes, cela pourrait brimer le droit de l'individu d'avoir toutes les informations nécessaires pour prendre une décision et favoriser ainsi sa manipulation** [31, 34]. Par exemple le concepteur d'un site internet qui, au lieu d'utiliser une barre mesurant la force du mot de passe de l'utilisateur, emploie plutôt un arrière-plan effrayant pour pousser l'individu à appliquer un mot de passe plus robuste sur ce site, créera de la confusion chez l'utilisateur quant à la sécurité dudit site [31]. Le but derrière les deux coups de pouce est le même, soit la mise en place d'un mot de passe robuste, mais dans le premier cas, l'intention derrière le coup de pouce est visuellement plus perceptible.

Bien que des chercheurs aient trouvé que les coups de pouce puissent être efficaces, il n'y a aucune garantie que **les comportements de sécurité des individus lors des expérimentations dans des études scientifiques soient les mêmes lorsque ceux-ci prennent des décisions au quotidien ou**

au travail [5, 13]. En effet, dans les expérimentations, les risques ne sont pas réels [16, 36]. Il est donc pertinent de se demander si l'ensemble des coups de pouce exercent une influence significative dans la modification de comportements inadéquats dans le cadre de la cybersécurité « réelle ».

De plus, plusieurs études dans le domaine de la cybersécurité portent sur les mots de passe et la force de ceux-ci [9, 14, 15, 16, 21]. Toutefois, **il existe plusieurs autres éléments qui sont liés à la sécurité et ceux-ci sont peu évalués**. Ainsi, une limite à la littérature scientifique actuelle est qu'il est impossible de confirmer que les résultats trouvés dans le cadre d'une étude peuvent s'appliquer à une autre pratique de cybersécurité [16].

Une dernière limite des coups de pouce est l'évaluation des changements de comportements dans le temps [25]. Il a été trouvé que **l'effet des coups de pouce liés aux comportements de cybersécurité diminue graduellement à travers le temps** [5]. Toutefois, l'étude qui rapporte ce résultat a évalué les effets pour un écart de seulement deux semaines entre la première expérimentation et la seconde [5]. Des recherches plus approfondies sur cet aspect seraient pertinentes.

Recommandations

- La **personnalisation des coups de pouce selon les besoins et préoccupation du milieu est à privilégier** [35]. En effet, plus les coups de pouce se rapprochent des besoins en termes de cybersécurité de l'entreprise ou du milieu, plus il sera simple et facile pour les individus de comprendre les raisons derrière de telles techniques. De plus, des coups de pouce qui ciblent les besoins des milieux permettent de **ne pas engorger le système avec des coups de pouce non essentiels** et de se concentrer sur des difficultés rencontrées par les milieux. Cependant, pour augmenter l'efficacité de coups de pouce, il faut que les besoins de l'utilisateur/individu soient également pris en compte [9, 13].
- **Le coup de pouce hybride** (coup de pouce simple jumelé à celui d'information) **est à privilégier** [5] plus particulièrement dans le domaine de la cybersécurité, puisqu'il pousse l'individu à prendre conscience des effets d'une telle technique sur ses comportements en cybersécurité. Il y a ainsi une décision active qui est prise de la part de l'individu qui permet que le comportement se poursuive dans le temps même lorsque le coup de pouce est retiré de l'environnement. Cette approche créerait alors un automatisme chez les individus [5, 13].
- **Davantage d'études portant sur l'effet à long terme des coups de pouce sont nécessaires afin de mieux comprendre leur impact**. À long terme, ce qui est recherché est d'encourager des gestes de protection plus réguliers et automatiques chez l'individu. Des études longitudinales dans un milieu de travail et sur une période de plus d'un an, permettraient d'obtenir de tels résultats [5, 24]. Cette meilleure compréhension permettrait d'ailleurs de mettre en place des coups de pouce beaucoup plus rapidement, et ce, dans l'objectif d'améliorer la cybersécurité.

Tableau résumé des différents types de contrôle/mesure de cybersécurité activé par un coup de pouce

Type de contrôle ou mesure	Description	Mécanisme utilisé	Efficacité	Références
Changement de mot de passe pour un choix plus robuste	• Encourager les utilisateurs à améliorer la sécurité de leurs mots de passe (selon des critères préétablis) • Exemples: ◦ Compteur de mots de passe communs ◦ Graphique radar de la force du mot de passe ◦ Temps de craquage d'un mot de passe	• Cadrage • Information • Incitation • Influence sociale	• Augmenter la robustesse du mot de passe • Aspect visuel du coup de pouce (par ex. le graphique radar) • Informatif (par ex. compteur de mot de passe communs)	[5, 9, 13, 14, 15, 16, 17 26, 30, 36]
Paramétrages des critères de vie privée	• Influencer les décisions des utilisateurs concernant leurs paramètres de confidentialité, par l'introduction des options ou configuration par défaut. • Exemples: ◦ Acceptation des témoins de connexions ◦ Paramètres de confidentialité par défaut ◦ Cadre d'acception (*opt-in*) *versus* cadre de refus (*opt-out*)	• Défaut • Cadrage	• Partage d'informations plus sélectif de la part de l'utilisateur grâce aux paramètres par défaut plus stricts et restrictifs	[11, 20, 37, 38, 39, 40]
Navigation sécuritaire	• Influencer positivement le comportement des utilisateurs afin d'adopter des pratiques de navigation sécuritaires • Exemples: ◦ Message d'avertissement d'infection potentielle à un virus ◦ Message d'avertissement lors de téléchargement de logiciels ◦ Avertissement intégré sur le navigateur web	• Information • Cadrage	• Message d'encouragement ou d'avertissement influence l'utilisateur à des pratiques sécuritaires	[8, 10, 12, 18, 19, 27, 41]

Type de contrôle ou mesure	Description	Mécanisme utilisé	Efficacité	Références

Contrôle de sécurité proactif	• Anticiper les risque de cybersécurité et les cybermenaces potentielles
	• Stratégies préventives plutôt que réactives
	• Exemples:
	  ◦ Choix d'un réseau sans fil (WiFi) (sécurisé ou non)
	  ◦ Choix d'un fournisseur de services infonuagique
	  ◦ Chiffrage du téléphone intelligent
		• Information
		• Incitation
			• Se base sur l'information pour inciter l'utilisateur à faire des choix préventifs sécuritaires.	[5, 42, 43]

Comportement en matière de sécurité des systèmes	• Encourager les utilisateurs à mettre en oeuvre des comportements réguliers en matière de sécurité et de performance des systèmes et appareils électroniques
	• Exemples:
	  ◦ Incitation à effectuer les mises à jour d'un appareil électronique
	  ◦ Suggestions de bonnes pratiques
	  ◦ Authentification à double facteur
		• Influence sociale
		• Incitation
			• Messages de rappel avec incitation ou suggestions réduisent l'évitement (le fait d'ignorer les mesures de sécurité à mettre en place)	[28, 29, 35, 44, 45]

Références

[1] Thaler, R. H. et Sunstein, C. R. (2008). *Nudge : improving decisions about health, wealth, and happiness*. Yale University Press.

[2] Segerståhl, K. et Oinas-Kukkonen, H. (2007). Distributed User Experience in Persuasive Technology Environments. Dans, Y. de Kort, W. IJsselsteijn, C. Midden, B. Eggen, B.J. Fogg (dir.), *Persuasive Technology (vol 4744)*. Springer: Berlin, Heidelberg.

[3] Madrian, B. C. et Shea, D. F. (2001). The power of suggestion: Inertia in 401(K) participation and savings behavior. *Quart. J. Econ.*, *116*(4), 1149–1187.

[4] Sunstein, C. R. (2014). Nudging: a very short guide. *Journal of Consumer Policy*, 37, 583-588.

[5] Zimmermann, V. et Renaud, K. (2021). The nudge puzzle: Matching nudge interventions to cybersecurity decisions. *ACM Transactions on Computer-Human Interaction*, *28*(1).

[6] Turland J., Van Moorsel A., Coventry L., Jeske D. et Briggs P. (2015). Nudging towards security: Developing an application for wireless network selection for android phones. *ACM International Conference Proceeding Series*, 193–201.

[7] Weinmann, M., Schneider, C. et Brocke, J. V. (2016). Digital nudging. *Business & Information. Systems Engineering*, *58*(6), 433–436.

[8] van Bavel, R. et Rodríguez-Priego, N. (2016). Nudging Online Security Behaviour with Warning Messages: Results from an online experiment. *JRC Technical Reports*. EUR 28197.

[9] Kennison, S. M., Jones, I. T., Spooner, V. H. et Chan-Tin, D. E. (2021). Who creates strong passwords when nudging fails. *Computers in Human Behavior Reports*, *4*, 100132.

[10] Sharma, K., Zhan, X., Nah, F. F. H., Siau, K. et Cheng, M. X. (2021). Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity. *Organizational Cybersecurity Journal: Practice, Process and People*, *1*(1), 69-91.

[11] Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S. et Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, *50*(3), 1-41.

[12] Rosoff, H., Cui, J. et John, R. S. (2013). Heuristics and biases in cyber security dilemmas. *Environment Systems and Decisions*, *33*, 517-529.

[13] Hartwig, K. et Reuter, C. (2021). Nudge or Restraint: How do People Assess Nudging in Cybersecurity-A Representative Study in Germany. Dans *Proceedings of the 2021 European Symposium on Usable Security*.

[14] Frik, A., Malkin, N., Harbach, M., Peer, E. et Egelman, S. (2019). A promise is a promise: The effect of commitment devices on computer security intentions. Dans *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*.

[15] Peer, E., Egelman, S., Harbach, M., Malkin, N., Mathur, A. et Frik, A. (2020). Nudge me right: Personalizing online security nudges to people's decision-making styles. *Computers in Human Behavior*, *109*, 106347.

[16] Qu, L., Xiao, R., Shi, W., Huang, K., Qin, B. et Liang, B. (2022). Your behaviors reveal what you need: a practical scheme based on user behaviors for personalized security nudges. *Computers & Security*, *122*, 102891.

[17] Qu, L., Xiao, R. et Shi, W. (2023). Interactions of Framing and Timing in Nudging Online Game Security. *Computers & Security*, 124.

[18] Egelman, S., Cranor, L.F., Hong, J. (2008). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. Dans, *Proceedings of the SIGCHI conference on human factors in computing systems*.

[19] Reeder, R.W., Felt, A.P., Consolvo, S., Malkin, N., Thompson, C., Egelman, S. (2018). An Experience Sampling Study of User Reactions to Browser Warnings in the Field. Dans, *Proceedings of the 2018 CHI conference on human factors in computing systems*.

[20] Bermejo Fernandez, C., Chatzopoulos, D., Papadopoulos, D. et Hui, P. (2021). This website uses nudging: Mturk workers' behaviour on cookie consent notices. *Proceedings of the ACM on human-computer interaction*, *5*(CSCW2), 1-22.

[21] Kankane, S., DiRusso, C. et Buckley, C. (2018, April). Can we nudge users toward better password management? an initial study. Dans, *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*.

[22] van Steen, T. (2022). When choice is (not) an option: nudging and techno-regulation approaches to behavioural cybersecurity. Dans D. D., Schmorrow, et C. M., Fidopiastis (dir.), *Augmented Cognition (vol 13310, p. 120-130)*. Cham: Springer International Publishing.

[23] Dhingra, N., Gorn, Z., Kener, A. et Dana, J. (2012). The default pull: An experimental demonstration of subtle default effects on preferences. *Judgment and Decision Making*, *7*(1), 69-76.

[24] Lin, Y., Osman, M. et Ashcroft, R. (2017). Nudge: concept, effectiveness, and ethics. *Basic and Applied Social Psychology*, *39*(6), 293-306.

[25] Caraban, A., Karapanos, E., Gonçalves, D. et Campos, P. (2019, May). 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. Dans, *Proceedings of the 2019 CHI conference on human factors in computing systems*.

[26] Kankane, S., DiRusso, C. et Buckley, C. (2018, April). Can we nudge users toward better password management? an initial study. Dans, *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*.

[27] Van Bavel, R., Rodríguez-Priego, N., Vila, J. et Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29-39.

[28] Inaba, M. et Terada, T. (2023). Nudge to Promote Employees' Information Security Compliance Behavior: A Field Study. Dans, *2023 IEEE International Conference on Cyber Security and Resilience (CSR) (p. 335-340)*. IEEE

[29] Das, S., Kramer, A. D., Dabbish, L. A. et Hong, J. I. (2014). Increasing security sensitivity with social proof: A large-scale experimental confirmation. Dans, *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*.

[30] Dupuis, M. et Khan, F. (2018). Effects of peer feedback on password strength. Dans. *2018 APWG Symposium on Electronic Crime Research (eCrime)* (p. 1-9). IEEE.

[31] Renaud, K. et Zimmermann, V. (2018). Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies*, *120*, 22-35.

[32] Sunstein, C. R. (2015). Nudges do not undermine human agency. Journal of consumer policy, 38, 207-210.

[33] Sunstein, C. R. (2015). The ethics of nudging. *Yale J. on Reg.*, *32*, 413.

[34] Wilkinson, T. M. (2013). Nudging and manipulation. *Political Studies*, *61*(2), 341-355.

[35] Coventry, L., Briggs, P., Jeske, D. et Van Moorsel, A. (2014). SCENE: A structured means for creating and evaluating behavioral nudges in a cyber security environment. Dans, *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience: Third International Conference, DUXU 2014, Held as Part of HCI International 2014*, Heraklion, Crete, Greece, June 22-27, 2014, Proceedings, Part I 3 (vol. 8517, p. 229-239). Springer International Publishing.

[36] Zibaei, S., Malapaya, D. R., Mercier, B., Salehi-Abari, A. et Thorpe, J. (2022). Do password managers nudge secure (random) passwords? Dans, *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*.

[37] Tschersich, M. (2015, Janvier). Comparing the configuration of privacy settings on social network sites based on different default options. Dans, 2015 48th Hawaii International Conference on System Sciences (p. 3453-3462). IEEE.

[38] Baek, Y. M., Bae, Y., Jeong, I., Kim, E. et Rhee, J. W. (2014). Changing the default setting for information privacy protection: What and whose personal information can be better protected? *The Social Science Journal*, *51*(4), 523-533.

[39] Johnson, E. J., Bellman, S. et Lohse, G. L. (2002). Defaults, framing and privacy: Why opting in-opting out. *Marketing letters*, *13*, 5-15.

[40] Balebako, R., Leon, P. G., Almuhimedi, H., Kelley, P. G., Mugan, J., Acquisti, A., Cranor, L.F. et Sadeh, N. (2011). Nudging users towards privacy on mobile devices. Dans, *2nd International Workshop on Persuasion, Nudge, Influence, and Coercion Through Mobile Devices*.

[41] Petrykina, Y., Schwartz-Chassidim, H. et Toch, E. (2021). Nudging users towards online safety using gamified environments. *Computers & Security*, *108*, 102270.