MASTER EN SCIENCES INFORMATIQUES À FINALITÉ SPÉCIALISÉE EN SOFTWARE ENGINEERING

Conception, développement et évaluation d'un outil de sensibilisation à la cybersécurité

Hallaert, Elise

Award date:
2021

Awarding institution:
Universite de Namur

Université de Namur
Faculté d'informatique
Année académique 2020–2021

Conception, développement et évaluation d'un outil de sensibilisation à la cybersécurité

Elise Hallaert

Maître de stage : Jean-Noël Colin

Promoteur : _____ (Signature pour approbation du dépôt - REE art. 40)
Jean-Noël Colin

Co-promotrices : Fanny Boraita et Julie Henry

Mémoire présenté en vue de l'obtention du grade de
Master en Sciences Informatiques

Table des matières

Table des figures

Liste d'abréviations

La table suivante reprend les abréviations et acronymes utilisés dans le document.

DDos	distributed denial of service attack
SSL	Secure Sockets Layer protocol
GDPR	General Data Protection Regulation
ENISA	Agence de l'Union Européenne pour la cybersécurité
UE	Union Européenne
NIS	Directive on Security of Network and Information Systems
cPPP	contractual Public-Private Partnership
CIRB	Centre d'Informatique pour la Région Bruxelloise
CERT	Cyber emergency team fédéral
FCCU	Federal Computer Crime Unit
RCCU	Regional ComputerCrime Units
ARES	Académie de Recherche et d'Enseignement supérieur
QCM	Questionnaire à choix multiple

Résumé

La cybersécurité est influencée par de nombreux facteurs, tous ayant une grande importance. Parmi eux, le facteur humain est central et complexe à traiter. Afin d'agir sur celui-ci, un outil d'aide à la sensibilisation a été développé afin de proposer une activité de sensibilisation à la cybersécurité aux élèves du secondaire. Celui-ci est inspiré par les jeux de point and click, un type de jeu d'enquête sur ordinateur permattant de gamifier l'activité et améliorer l'attention de l'élève ainsi que son implication. L'activité amène l'élève à se confronter à un ordinateur ayant été attaqué, son objectif étant de retrouver des documents apparemment perdus. Après les recherches qui ont été réalisée au préalable, une analyse des besoin a mené à la conception, au développement, et enfin à l'évaluation via une méthode d'évaluation de campagne de sensibilisation en trois axes, de l'outil qui a été testé auprès d'élèves du secondaire.

Remerciements

Je tiens à remercier toutes les personnes qui ont contribué au succès de mes études et l'accomplissement de mes objectifs de formation jusqu'à aujourd'hui, et en particulier l'ensemble du personnel de l'Université de Namur qui m'a permis de suivre cinq années de formation incroyablement enrichissantes.

Ensuite, je tiens à remercier en particulier mon promoteur J-N. Colin, pour son encadrement, son expertise, et pour avoir proposé un sujet passionnant. Je tiens également à remercier particulièrement mes deux co-promotrice, J. Henry et F. Boraita pour avoir apporté un soutien, un encadrement et une grande clarté.

Enfin, je souhaite remercier les professeurs du secondaire ayant collaboré avec moi dans le cadre de ma recherche et tous les élèves ayant pris part à celle-ci.

Chapitre 1

Introduction

La cybersécurité est au coeur des préoccupations et son importance est grandissante. Le domaine grandit et nécessite de plus en plus d'efforts. Si les états et les entreprises prennent des mesures pour se protéger ou encore améliorer la résilience des systèmes, le facteur humain reste un maillon difficile à renforcer. Afin d'approcher ce dernier, la présente étude aborde un travail de conception et de développement d'un outil de sensibilisation à la cybersécurité gamifié par son support, un logiciel point and click de type escape game. L'évaluation de cet outil a été réalisée via l'évaluation de son impact en utilisant une méthode basée sur deux théories, l'une abordant la sensibilisation via trois axes, et l'autre proposant une méthodologie éprouvée permettant d'évaluer ces mêmes axes.

Ce mémoire est constitué de 12 chapitres relatant les étapes qui ont été suivies pour la recherche réalisée.

En premier lieu, l'introduction reprend un résumé du mémoire et une définition préalable de la cybersécurité, c'est-à-dire le thème principal du mémoire, afin de correctement situer le domaine.

Ensuite, le chapitre deux abordera la cybercriminalité en Belgique. La cybercriminalité est la raison d'être de la cybersécurité, elle la façonne et influence son évolution. Il est fondamental de bien connaître la menace afin de se sécuriser en prévision et en conséquence et de comprendre les raisons pour lesquelles certaines pratiques sont en place.

Les stratégies en matière de cybersécurité au niveau européen et belge seront ensuite expliquées. Cela passera par les plans en place, les positionnements vis-à-vis de la cybersécurité, et les mesures en pratique. Cela placera le contexte politique et législatif dans lequel les plans de sensibilisation prennent place et posera les bases nécessaires à aborder le sujet central de ce mémoire qu'est l'influence du facteur humain sur la cybersécurité.

En effet, si les stratégies en place permettent de protéger des cybermenaces, le facteur humain, de grande importance, est souvent laissé pour compte mal-

gré son importance capitale. Les formations existantes et à venir en Fédération Wallonie-Bruxelles pemettront de bien se représenter les connaissances et lacunes qui introduiront à la problématique des intentions car les enjeux de la sensibilisation à la cybersécurité sont directement liés aux **intentions** de l'individu qui sont façonnées, notamment, et principalement, par son expérience et sa formation. L'explicitation des enjeux permettra également d'encadrer l'objectif en explicitant où commence et où se termine la sensibilisation telle qu'abordée dans cette recherche.

Dès lors, le contexte dans lequel la sensibilisation prend place ainsi que son intérêt auront été caractérisés et celle-ci pourra être bien définie, décrite et expliquée.

Afin de découvrir les facteurs aidant à la sensibilisation qui ont guidé la conception et le développement d'un outil d'aide à la sensibilisation à la cybersécurité, le cadre d'évaluation de la sensibilisation sera expliqué afin de lier les lignes directrices aux facteurs qui guident la sensibilisation pour mieux les comprendre.

Avant d'aborder l'analyse préalable réalisée pour la conception de l'outil, toutes les lignes directrices liées à la sensibilisation à la cybersécurité, en particulier, qui ont guidé la conception seront relatés.

Ensuite, les apports de la recherche seront amorcés, d'abord par l'analyse détaillée des besoins auxquels l'outil veut répondre en définissant précisément l'objectif et les composants de celui-ci ; le public visé, les sujets à aborder, les contraintes et besoins, et le support.

Le développement et l'implémentation de l'outil seront alors développés afin de mener à l'étape d'évaluation de celui-ci.

En commençant par le cadre théorique, la méthode d'évaluation sera explicitée par le procédé suivi et l'analyse des données obtenues.

Les résultats seront alors communiqués et commentés.

Enfin, un résumé des contributions, des limites et perspectives induites par cette recherche sera exprimé avant de proposer une conclusion à celle-ci.

1.1 Définition

Le domaine de la cybersécurité a subi de grands changements ces dernières années, et prévoit d'en subir encore dans les années à venir. Elle a beaucoup évolué tant en tant que domaine que dans sa définition. D'abord en raison de sa relative récence, mais également en raison de sa complexité. Plusieurs désaccords quant à sa définition sont encore débattus aujourd'hui au sein de la communauté de la sécurité. La section suivante reprend ses définitions récentes.

Une recherche de 2014 a recensé des articles et mené des discussions autour de la définition de la cybersécurité [1]. La définition qui en a résulté est la suivante :

" La cybersécurité est l'organisation et la collection de ressources, processus et de structures utilisées pour protéger le cyberespace et les systèmes liés à ce cyberespace de la survenance d'évènements qui ne respectent pas, de manière juridique, les droits de la propriété. "

Il s'agit d'une définition qui est très ouverte, mais elle peut ainsi être utilisée plus facilement dans le cadre de l'interdisciplinarité à laquelle elle est sujette.

Selon l'ANSSI, *"Les risques liés à la négligence humaine sont pris en compte par la sûreté de fonctionnement alors que ceux liés à la malveillance sont traités par la cybersécurité. Néanmoins, les mesures de cybersécurité permettent de couvrir certains risques liés à la négligence."* [2].

Chapitre 2

Cybercriminalité en Belgique

2.1 Introduction

Si les chiffres de la criminalité au sens large semblent diminuer en Belgique et dans tous les pays limitrophes, la cybercriminalité quant à elle, atteint des chiffres sans précédents. Ceci est symptomatique des opportunités créées par l'informatisation des processus et systèmes et par l'évolution de ceux-ci. Ce chapitre s'appliquera à en donner une représentation claire et à en retracer l'historique. L'objectif est d'en apprendre plus sur la menace à laquelle répond la cybersécurité et de mieux connaître l'influent principal de la cybersécurité qu'est la cybercriminalité, car c'est cette dernière qui la façonne.

2.2 La cybercriminalité

Dans cette section, les données clés de la cybercriminalité seront exposées.

Les chiffres de la police fédérale belge indiquent une augmentation de plus de 29% de la cybercriminalité entre 2018 et 2019 avec une hausse de plus de 80% pour le phishing. Or, les cybercriminels ont aussi profité de la crise et de la situation sanitaire pour déployer encore plus d'attaques, les chiffres ont donc atteint des valeurs sans précédents ces deux dernières années [3].

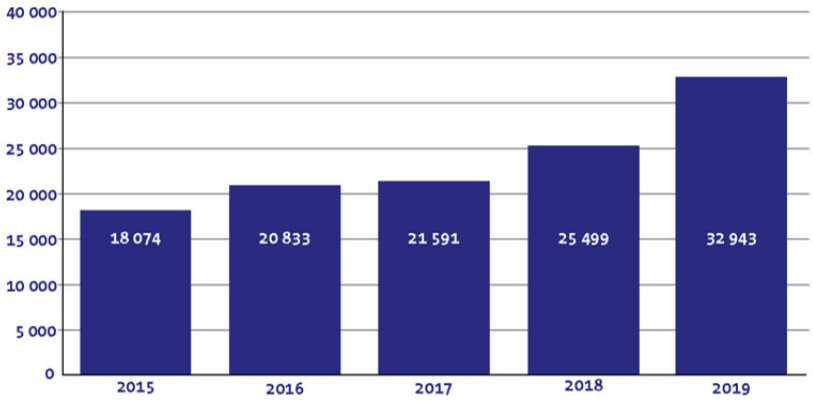

FIGURE 2.1 – Evolution du nombre de cas de criminalité informatique en Belgique par année [4].

Il semble que les cas sont également de plus en plus déclarés à la police, même si ces déclarations n'atteignent pas le quart des attaques ayant lieu en Belgique [4].

L'Europe est également la cible privilégiée des cyberattaques venant du monde entier [5].

"Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19." Jürgen Stock, INTERPOL Secretary General

En effet, les nouvelles attaques de phishing exploitent maintenant la situation sanitaire en se faisant passer pour des autorités gouvernementales ou du domaine de la santé afin d'obtenir des informations personnelles, profitant encore du télétravail pour élargir leur nombre de cibles.

Avec l'avènement des vaccins, le nombre d'attaques a encore augmenté, créant des campagnes qui tirent profit des inquiétudes de la population.

2.3 Historique

L'histoire de la cybersécurité est intimement liée à l'histoire des vulnérabilités en informatique. Souvent, c'est en réaction à ces dernières que la cybersécurité évolue. Elle a traversé plusieurs âges et a vraiment commencé dans les années 70 dans le milieu universitaire avant de s'institutionnaliser dans les années 90. Depuis ces 10 dernières années, les attaques prenant de plus en plus d'ampleur, les réglementations évoluent aussi.

2.3.1 1940 : avant la cybersécurité

Les débuts de la communication à distance

Avant la création du cyberespace [1] , le télégraphe a permis d'augmenter le nombre de communication, les distances auxquelles nous pouvions communiquer ainsi que la rapidité avec laquelle nous communiquions. Avec cette innovation sont apparues les premières vulnérabilités et la première idée de la confidentialité dans les communications [6].

Selon John Packer, conservateur au musée du télégraphe, c'est durant cette période que les utilisateurs ont commencé à demander des communications privées et sécurisées. Ainsi, les distributeurs du service ont tenu à assurer que tout était sécurisé. Ce fut une surprise étant donné que le prix des communications devait empêcher les messages à caractère trop personnel selon eux.

Afin d'effectivement permettre une certaine sécurité, les conversations ont commencé à être chiffrées et l'utilisation de câbles sous-marins devait également éviter l'accès aux messages échangés.

En revanche, le concept même de confidentialité des communications n'est entré dans le vocabulaire que lorsque d'autres technologies de communications sont apparues, comme la télégraphie sans fil inventée par Guglielmo Marconi.

Le premier pirate électronique

C'est après le travail de ce dernier qu'une entreprise de Télégraphie, la Eastern Telegraph Company, a essayé de le perturber, et y est parvenue. Nevil Maskelyne, magicien et grand habitué de la technologie sans fil, a été engagé dans le but d'intercepter des messages et d'en envoyer de non désirés, pour démontrer, devant le grand public, les failles de sécurité de la technologie de Marconi. Dès lors, l'intérêt du filaire ainsi qu'une sorte de standard de confidentialité ont été apportés sur le devant de la scène par le télégraphe [7].

2.3.2 Définition du terme

Le terme "*cybersécurité*" trouve son origine dans la définition du mot "*cybernétique*", créé par Norbert Wiener, professeur au MIT, en 1948. A l'origine, il a été utilisé pour décrire les systèmes d'information complexes, décrivant "*le champ de la théorie de la commande et de la communication*". Il proviendrait du grec "*kuberneïn*", signifiant "*diriger*" [8].

C'est après avoir été utilisé dans un roman de William Gibson traitant du vol de données que le terme, et son préfixe "*cyber*" ont peu à peu été utilisés par la communauté scientifique, désignant ce qui est relatif aux communications et aux échanges d'informations de manière générale.

1. Espace de communication créé par l'interconnexion mondiale des ordinateurs (Internet) ; espace, milieu dans lequel naviguent les internautes. (LeRobert)

2.3.3 Années 70 et l'expérimentation

La particularité qui sous-tend le concept de virus réside dans son abilité à se répliquer pour infecter un appareil. Le principe de "*self-replicating automata*" ou encore "*automate auto-reproducteur*" peut être retracé jusqu'à l'année 1949, créé par le visionnaire John Van Neumann [9].

Le premier virus tel que défini aujourd'hui n'est pas connu, mais le premier ver, c'est-à-dire premier virus capable de se répliquer sur un réseau, a été créé par l'ingénieur Robert H. Thomas en 1971. L'objectif n'était pas de créer des dommages mais bien de démontrer l'application d'un tel programme. Il développa ainsi *Creeper* en assembleur PDP-10 sur *Tenex*, et placé sur l'*arpanet*, *Creeper* infecta des systèmes en affichant "*I'M THE CREEPER : CATCH ME IF YOU CAN*" [10], [11].

L'année suivante, poussé par la création du premier virus, l'ingénieur Ray Tomlinson a non seulement amélioré le *Creeper*, mais a également développé le premier programme considéré comme étant un antivirus, *Reaper*, permettant d'arrêter le *Creeper*.

Dans les années qui ont suivi, la sécurité informatique s'est limitée au milieu universitaire, puis internet s'est développé, augmentant les communications ainsi que les cibles potentielles.

2.3.4 Années 80 : le commencement du piratage black hat

Durant les années 80 ont commencé les attaques dites "*black hat*", c'est-à-dire conduites avec des intentions malveillantes.

En 1988, Robert Morris, fils d'un cryptographe, souhaitait connaître l'ampleur du réseau constitué des appareils connectés à internet. Pour ce faire, il mit en place un programme qui pouvait voyager sur le réseau en demandant à chaque appareil, un à un, d'envoyer une réponse permettant de les compter.

Malheureusement, le programme n'avait pas prévu le dépassement de certaines limites. De grandes parties d'internet furent ainsi bouchées en raison du trafic beaucoup trop important généré par le programme. Ceci marqua la première prise de conscience face aux risques des attaques DDoS ainsi que des opportunités générées par l'Internet of Things [12].

Dans les années 80 et 90, la lutte contre les mauvaises pratiques s'est principalement concentrée sur les jeux et autres produits piratés.

2.3.5 Les premiers virus (années 1990)

Avec l'avènement du commerce en ligne, la question de sécurité a commencé à se poser à plus large échelle. Pour permettre des paiements sécurisés, un cryptographe égyptien, Taher Elgamal, a créé SSL, pour *Secure Sockets Layer protocol*. Ayant quelques problèmes dûs vraisemblablement à une idée mal développée

dans les faits, la version 2.0 améliorée et utilisable fit ses débuts en 1995 et devint ensuite le coeur du protocole HTTPS [13].

Bien que le piratage éthique selon sa définition actuelle existait déjà avant, c'est en 1995 que le terme a été utilisé pour la première fois par John Patrick, vice-président au MIT. Il s'agit d'un concept intéressant dans le sens où certaines sources pensent qu'il s'agit de l'objectif principal de la plupart des hackers tandis que les médias ont tendance à représenter les hackers comme de grands criminels. En réalité, le terme "*hacker*" voulait désigner des experts en informatique qui souhaitaient trouver des moyens d'améliorer des systèmes de manière créative. Ensuite, la montée des moyens de communication ont fait apparaître des comportements permettant de contourner des limitations. C'est ainsi que les distributeurs de service ont engagé des experts dans le but de trouver leurs propres failles avant qu'elles ne soient exploitées. La montée des vols de données et des intrusions a valu au terme "*hacker*" la connotation qu'il a aujourd'hui. Pour plus de précision, la littérature les décrit souvent comme les "*hackers black hat*". Dès lors, par opposition à ce type de piratage, les entreprises investissent dans le piratage éthique, ou "*piratage white hat*", qui est en fait un moyen de lutte contre le piratage criminel [14].

L'infection par un virus la plus rapide du vingtième siècle fut effectuée par David L. Smith en 1999 avec un programme appelé Melissa. En seulement quelques heures, le virus a atteint plus de dix mille machines dans le monde. Les réparations ont coûté plus de 80 millions de dollars, et l'attaque a duré plus d'une semaine.

Il s'agissait d'un mail contenant un document word infecté. Le mail avait été créé sur base des suggestions de l'ingénierie sociale, utilisant l'adresse mail d'un proche pour demander de télécharger la pièce jointe, et envoyant ensuite des mails à partir de la nouvelle adresse infectée.

L'année suivante, le virus *I love You* créé par Onel de Guzman s'est propagé de la même manière, effaçant des fichier, volant des mots de passe et faisant encore plus de victimes [15]. L'objectif était en fait de parvenir à accéder à internet gratuitement, et étant donné que les philippines n'avaient à l'époque aucune législation sur le piratage, il n'a pas été poursuivi.

2.3.6 Années 2000 : institutionnalisation des cybermenaces et de la cybersécurité

Le mouvement anonymous s'est fortement fait connaître après les attentats de ce siècle tels que ceux du 13 novembre 2015 à Paris ou encore ceux de Bruxelles ou de Nice. La naissance de ce mouvement remonte à 2003, avec la création d'un site d'images dont les pseudos étaient "anonymous" par défaut. C'est quelques années plus tard, en 2007, qu'ils commencèrent à attaquer l'église scientologique puis toute mesure liberticide empêchant la révolte du peuple selon eux [16].

Il s'agit également de la décennie qui a vu une montée des mesures de cybersécurité, comme la création d'une *Division nationale de la cybersécurité* aux Etats-Unis en 2003, ou encore la *Convention sur la cybercriminalité* du Conseil de l'Europe, visant l'harmonisation des lois de criminalité pour les 67 pays qui l'ont signée en 2004.

En 2007, le Royaume-Uni fait entrer en vigueur une loi sur la fraude qui permet de catégoriser les délits ainsi que d'en avoir une définition [17].

Ces mesures ont évidemment fait écho aux attaques qui montaient en puissance ; des plans de lanceurs spaciaux américains ont été volés, la Défense américaine a subi des attaques sur ses messageries, la China Aerospace Science & Industry corporation a trouvé des logiciels espions dans ses ordinateurs pour ne citer que quelques faits entre 2006 et 2007. Ainsi, les attaques étaient bien plus ciblées, et les entreprises ont commencé, doucement, à s'équiper pour lutter contre les attaques.

2.3.7 De nos jours

Les attaques ont aujourd'hui pris une autre forme à force d'évoluer. Les "*script-kiddies*" n'ont aujourd'hui que peu d'incidence en raison des protections et de la sensibilisation de la population, en revanche, d'autres conflits sont maintenant passés au virtuel, prenant beaucoup d'ampleur.

Par exemple, en 2010, Google fut victime de l'opération *Aurora*, dont les révélations de WikiLeaks ont confirmé l'implication du gouvernement chinois [18].

Les vols d'identité atteignent des niveaux sans précédents, faisant plusieurs millions de victimes et des attaques de grande envergure se suivent sans avoir d'objectif défini. Les hackers black hat sont de mieux en mieux organisés.

En 2010 le gouvernement britannique a assigné un statut "*Tier One*" au cybercrime.

En mai 2018, le RGPD entre en vigueur pour réguler l'utilisation des données des citoyens européens et l'Europe fait preuve d'impérialisme afin de contrôler l'utilisation des services étrangers en son sein.

Les attaques se font de plus en plus courantes, et encore plus depuis le commencement du télétravail en masse dans le monde. Plusieurs pays mettent à jour leurs lois mais sont limités par leur propre fracture numérique dans la lutte contre les cybercriminels. Il arrive également que les gouvernements eux-mêmes ne respectent pas les lois en vigueur, comme en Belgique où l'utilisation des données des citoyens dans le cadre du programme de vaccination a posé question.

Selon plusieurs experts, l'utilisation de l'intelligence artificielle ainsi que la montée de l'Internet Of Things tendent à faciliter les attaques et augmenter les cibles possibles, rendant le défi de la protection de plus en plus difficile.

Télétravail : une nouvelle tendance

Une nouvelle tendance dans les secteurs d'apparition est apparue dans le courant de l'année 2020. Tandis que les secteurs de la finance et des institutions sont proportionellement moins attaqué chaque année, [19] les utilisateurs particuliers ont été moins touchés proportionnellement par des attaques que les années précédentes et l'industrie a été presque trois fois plus touchée. Cette tendance pourrait être une conséquence du télétravail et aura peut-être de grandes conséquences sur le domaine de la cybersécurité [19].

Chapitre 3

Cybersécurité : les deux niveaux de stratégie

3.1 Introduction

Dans les chapitres précédents, la cybersécurité a été définie. L'importance de celle-ci a ensuite été exposée dans le chapitre 2 en abordant la cybercriminalité à laquelle elle fait face, qui la fait évoluer et constitue sa raison d'être. Ce chapitre va maintenant exposer les mesures en place pour lutter contre les menaces maintenant connues et aborder les facteurs critiques dans le domaine. Il abordera d'abord l'influence de l'Europe avant de se concentrer sur la Belgique, ses plans mis en place et la mise en oeuvre des directives européennes. Ainsi, le contexte juridique et politique de la cybersécurité, constituant le décor dans lequel évoluent les individus, permettra de comprendre l'importance de la prise en compte du facteur humain, via les formation en place, dans ces mesures.

3.2 En Europe

Le conseil européen a déjà pris conscience de l'importance de la cybersécurité. Il multiplie les mesures et sait communiquer et distiller des informations primordiales [20].

Ces dernières années, plusieurs mesures importantes ont été mises en place comme la mise à jour de la stratégie contre la cybersécurité ou l'imposition des sanctions aux cyberattaques [20].

Depuis le 20 avril 2021, un centre de compétences en cybersécurité à Bucarest visant la mise en commun des compétences des états membres, entreprises, universités ou autres parties prenantes européennes a reçu un nouvel élan grâce à l'établissement de son règlement qui devra ensuite être adopté par le Parlement

européen. Au-delà de la mise en commun des fonds investis dans la recherche et le développement de technologies liées à la cybersécurité, le centre s'occupera des affectations des financements européens. Via une coopération avec l'ENISA (Agence de l'Union européenne pour la cybersécurité), le centre servira à renforcer la sécurisation des infrastructures ainsi que la compétitivité mondiale du secteur et l'autonomie de l'UE dans le domaine [1]. L'UE distingue 6 pôles de sécurité sur lesquels elle travaille tout en cherchant à conforter les citoyens [20] :

— Renforcement de la cyberrésilience
— Lutte contre la cybercriminalité
— Stimulation de la cyberdiplomatie
— Renforcement des cyberdéfenses
— Stimulation de la recherche et de l'innovation
— Protection des infrastructures critiques

Tout repose principalement sur deux textes : le GDPR et le NIS (législation sur la sécurité des réseaux et des systèmes d'informations des Etats membres).

3.2.1 La stratégie européenne

Depuis 2020, l'UE mise sur une stratégie de renforcement de la résilience des citoyens et des infrastructures situées en Europe face à la menace cyber afin d'obtenir des outils et des services fiables. Pour cela, plusieurs objectifs ont été fixés comme la fixation d'un cadre uni et autonome, l'adoption de nouvelles normes et le soutien du développement, ou encore, la création de groupes de travail ou de "*boîtes à outils*" liés à des sujets précis.

Le renforcement régulier des règles liées aux services permettant la cybercriminalité est aussi une voie privilégiée, par l'ajustement permettant une meilleure détection des crimes et un accès aux preuves, facilitant les poursuites, notamment pour les crimes sur mineurs. Plusieurs négociations avec d'autres pays sont en cours pour cette raison.

En plus du centre de lutte contre la cybercriminalité au sein d'*Europol*, une plateforme, *Empact*, sert à lutter contre les menaces par l'identification et le répertoriage de celles-ci.

Les lois entourant les données sont toujours mises à jour, renforcées et ajustées, permettant aussi d'alimenter les débats cyberdiplomatiques et de faire preuve d'impérialisme [21].

1. Mariana Vieira da Silva, ministre d'État portugaise de la présidence du Conseil des ministres, présidence du Conseil

3.2.1.1 Les grands plans d'investissement européens

Suite à la crise sanitaire mondiale, un plan de relance augmentant les mesures a été lancé pour soutenir ceux déjà en place [21].

Ceux-ci sont principalement divisés en trois grandes catégories : les plans de recherche et innovation tels que *Horizon* ou *cPPP* [22] , les supports au déploiement, qui servent à placer ou moderniser les infrastructures, et enfin les investissements de compétence, qui soutiennent des projets en particulier.

3.2.1.2 Le facteur humain selon l'UE

L'UE discerne deux types de facteurs humains, appelés compétence et sensibilisation (awareness). La compétence représente les experts, dont l'UE manque. Un objectif important est donc de stimuler le domaine pour augmenter le nombre d'experts.

Le facteur humain dans le sens de la conséquence du manque de sensibilisation est vu comme une grande faiblesse de la cybersécurité en Europe. Peu de mesures y sont liées, mais chaque année l'ENISA organise le mois de la cybersécurité, profitant de la campagne pour sensibiliser entreprises, institutions et citoyens.

3.2.1.3 L'avenir de la cybersécurité dans l'UE

Plusieurs projets sont toujours d'actualité et de nouvelles mesures arrivent à grands pas telles que le renforcement de la cyberrésilience ou le soutien de jeunes entreprises et de PME. L'UE s'intéresse actuellement à la législation autour des réseaux et systèmes d'information et sur un schéma européen visant un système de certification spécifique à l'union européenne. Bien entendu, la mise en place du centre de compétences en cybersécurité aura, lui aussi, de nouvelles missions.

3.3 En Belgique

3.3.1 Cadre juridique

La Belgique transpose d'abord les directives européennes puis s'assure que ces lois sont respectées. Comme pour tout autre état européen, le RGPD donne un cadre clair qui permet une protection.

Au niveau national, des analyses de risques sont souvent demandées pour juger de la nécessité de nouvelles mesures. La Belgique peut aussi profiter des audits et certifications faits au niveau européen [23].

Du point de vue de la sensibilisation, la Belgique propose des campagnes chaque année, sur différents médias, notamment en collaboration avec le centre

de cybersécurité Belgique. Ce centre a d'ailleurs publié que "*en l'espace d'un an et demi, notre pays est passé de la 11ème à la 5ème place dans le classement des pays européens les plus sûrs en termes de cybersécurité*".

Il propose en outre des guides, des webinaires et autres campagnes et transpose les directives pour le droit national.

3.3.2 La stratégie belge

La Belgique base en partie sa stratégie de lutte contre le cybercrime sur la coopération internationale. Les plans sont formés au niveau régional, mais ils ne peuvent être mis en place sans une collaboration.

Un plan fédéral avec des autorités sectorielles a été approuvé mais n'est, à ce jour, pas encore mis en place. Dans le cadre de la conformation à la règlementation européenne, des adaptations législatives sont notamment renforcées par une aide à l'information, et des diagnostics de maturité grâce au CIRB [24].

Quatre acteurs sont visibles dans le paysage de la cybersécurité en Belgique. Il s'agit :

— Le Centre pour la Cybersécurité Belgique

— la Cyber emergency team fédérale (CERT)

— la Federal Computer Crime Unit (FCCU) et les cinq Regional Computer Crime Units (RCCU) au sein de la Police fédérale belge

— l'asbl Cyber Security Coalition

Qui se partagent rôles et responsabilités.

Dans chaque région, plusieurs entités gèrent encore différentes missions et activités basées sur des plans spécifiques à chacune.

3.3.3 Sensibilisation en entreprise

Une étude a tout de même trouvé un bon niveau de sensibilisation dans les PME en Wallonie [25]. Les résultats de l'étude ont montré que l'information au sujet du RGPD a bien circulé et que des effets ont effectivement été observés, avec de plus en plus de requêtes pour la sécurisation des entreprises. Aussi, tous les participants à cette étude ont obtenu un score au-delà de 80% au test auquel ils ont été soumis.

Chapitre 4

Sujet d'étude : Le facteur humain

4.1 Introduction

Les chapitres précédents ont permis d'avoir une idée claire de l'évolution de la cybercriminalité ainsi que de la cybersécurité l'ayant suivie de près, tant au niveau européen que belge. Le facteur humain étant le point critique de ces mesures en place, ce chapitre abordera d'abord les mesures de formation en Fédération Wallonie-Bruxelles pour obtenir une vue d'ensemble de ce qui existe déjà. Ensuite, l'importance du facteur humain sera explicité plus amplement via ses enjeux réels et la raison pour laquelle ce facteur est si complexe en termes d'intention. L'objectif de ce chapitre est donc d'introduire au sujet principal de la recherche réalisée, le facteur humain, grand oublié des mesures en place dans la législation et les mesures connues.

L'impact du facteur humain dans la sécurité d'un système est très largement reconnu, qu'il s'agisse d'éviter un processus malveillant ou tout simplement de mauvais comportements côté utilisateur [26]. Son importance est capitale lorsqu'il s'agit de protéger un système, [27] d'abord parce qu'oublier de le prendre en compte dans le design d'un système informatique peut réduire à néant les efforts de sécurisation mis en place, jusqu'à devenir une faiblesse à part entière pouvant être facilement et rapidement exploitée. La montée des attaques de type *phishing* et *ransomware* témoignent de ce maillon faible. Jusqu'ici, la plupart des approches sont tournées vers les produits eux-mêmes, par exemple en réduisant le contrôle utilisateur, et non pas tournées vers l'utilisateur final [28].

Les entreprises mettent aujourd'hui en place des entraînements de "*security awareness*[1]" basées sur une définition de l'"*information security awareness*" qui est "*la mesure dans laquelle chaque membre du personnel comprend*

1. *l'importance de la sécurité des informations*
2. *Le niveau de sécurité approprié à l'organisation*
3. *leurs responsabilités individuelles*

et agissent en conséquence" [29],

mais le facteur humain reste un problème considéré non résolu.

4.2 Formation du facteur humain en Fédération Wallonie-Bruxelles

4.2.1 Les programmes aujourd'hui

La dernière circulaire faisant état des programmes d'étude est la n°4777 et date du premier mars 2014 [30].

Aujourd'hui, les programmes de l'enseignement primaire en fédération Wallonie-Bruxelles ne prévoient pas de formation à l'informatique mais des activités d'éducation aux médias qui consistent à déchiffrer des éléments, reconnaître une image ou une URL. En revanche, il est à noter que plusieurs écoles proposent tout de même des activités dirigées, comme des introductions à la dactylographie ou aux bonnes pratiques sur internet par exemple.

Les programmes du secondaire, quant à eux, proposent des cours d'informatique dès le premier degré. Une activité au choix pour le premier degré propose de la dactylographie, du traitement de texte et de la bureautique. Une autre activité complémentaire d'initiation à l'informatique pour le premier degré commun reprend des activités mises au programme à partir du premier septembre 2008. Il s'agit du programme 378/2008/240 qui propose au premier degré une introduction à la maîtrise de l'ordinateur, de la production de documents et de messages électroniques et de l'exploitation des sources d'informations numériques. En revanche, il n'y a pas d'activité similaire pour le premier degré différencié.

Le programme cité précédemment reprend une activité pouvant être proposée en activité au choix d'une formation optionnelle groupée au deuxième degré. Celui-ci se compose de traitement de texte, de contact avec un tableur et un logiciel de présentation. Il s'agit de la seule activité proposée au deuxième degré.

Pour l'enseignement général et technique de transition du troisième degré, il existe une activité de formation optionnelle groupée qui reprend un cours de science informatique décrit par le programme 477/2016/248A. Celui-ci est

1. sensibilité à la sécurité

bien plus fourni et propose 13 modules allant des fondamentaux de l'informatique à la conduite d'un projet de programmation. Par contre, aucun module ne fait état de la sécurité en ligne. Pour ce qui est de l'activité au choix proposée par le programme 378/2008/240 au troisième degré, le traitement de texte et l'exploitation d'un tableur sont suivis par un module de traitement d'image et d'utilisation d'une suite bureautique. Le programme d'informatique de gestion entré en vigueur en 2001 pour le secondaire général du troisième degré est composé de notions d'application et de TIC, d'utilisation de tableurs et de bases de données. Il existe aussi un programme de dactylographie pour le troisième degré.

Enfin, une orientation de technicien ou technicienne en informatique est proposée par le programme 358/2008/248B, entré en vigueur en 2011. Celui-ci contient sept fonctions allant de l'assurance d'une veille technologique à l'intégration professionnelle en passant par l'installation et le maintien d'un parc informatique, la sécurité de celui-ci, l'exploitation des ressources d'un PC et le respect de normes. Ce programme dispose de compétences très variées et est le seul à aborder des notions de cybersécurité à ce jour.

Ainsi, aucun cours abordant la cybersécurité n'est obligatoire dans l'enseignement obligatoire en Fédération Wallonie-Bruxelles. Ce manquement est ressenti vis-à-vis de la cybersécurité mais aussi de l'informatique en général.

4.2.2 Le pacte d'excellence

Le pacte d'excellence [31], dont la construction a officiellement commencé en 2015 et prévoit de modifier complètement le visage de l'enseignement, n'a pas oublié le numérique. La formation menant à maîtriser les outils numériques devrait apparaître dès le primaire. Trois axes avaient été discutés avant la publication : l'utilisation des outils dans le but d'apprendre d'autres choses, la littératie numérique qui consiste en la responsabilisation et la sensibilisation des internautes et la science du numérique [32].

Une version provisoire a été publiée le 26 mars 2021 sur le site d'ARES. Il soutien une ouverture au monde selon quatre pôles qui sont les pôles manuel, technique, technologique et numérique.

Les compétences liées à l'information et aux données sont prévues en troisième et quatrième primaire ainsi qu'en première et deuxième secondaire, et les notions de sécurité en sixième et en première secondaire. Ceci est motivé par l'idée que l'élève doit d'abord maîtriser les outils et être autonome avant d'en apprendre la sécurité.

Le programme de sécurité de la sixième primaire est consitué de vocabulaire quant à la sécurité des personnes et des données, des savoir-faire quant à la sécurité des mots de passes, des traces personnelles et aux situation de danger en ligne, et enfin des compétences de prévention de risques vis-à-vis des données et de l'équilibre social et psychologique.

Le programme de première secondaire reprend ces mêmes constituants ainsi que du savoir-faire de paramétrage et d'encodage de données personnelles et des notions plus avancées d'identité numérique et de navigation sécurisée.

A cela s'ajoute une vision plus large du domaine, avec une prise en compte du croisement entre les disciplines. Des contenus combinés permettraient donc d'aborder plusieurs compétences à la fois ainsi qu'élargir le champ des possibles pour le corps enseignant.

4.3 Enjeux de la sensibilisation à la cybersécurité

Plusieurs études viennent à la conclusion que le facteur humain est le plus important avec des facteurs soit liés au management et le fait que les personnes sont attitrées à des responsabilités inadéquates ou n'ont pas la possibilité de travailler dans de bonnes conditions, soit liés directement à l'utilisateur final avec des problèmes de comportements, de croyances, de motivation, de conscience des risques, et enfin, d'utilisation des technologies. [33] Un grand nombre de brèches de sécurité surviennent à cause de la réticence de l'utilisateur à se conformer à certains comportements [34].

Du point de vue des intentions, même un utilisateur qui pense être conscient des risques aurait tendance à entreprendre des actions risquées [35]. Il s'agit souvent de l'utilisateur qui crée des brèches de sécurité dans un système de matériel et de logiciels très bien conçu, surtout lorsqu'il n'a pas été bien informé [26], avec des chiffres allant jusqu'à 86% des faiblesses en 2009.

Sensibiliser l'utilisateur final serait la clé pour résoudre les risques liés à ce facteur. Pour ce faire, il doit être conscient du danger et connaître les comportements adéquats afin d'amener une sorte de "*culture de la responsabilité*" [27].

La vulnérabilité principale liée au facteur humain serait l'ingénierie sociale avec des utilisateurs qui seraient plus d'un tiers à cliquer sur un lien proposé venant d'un courrier spécifiquement suspicieux [26].

Chapitre 5

Sensibilisation

5.1 Introduction

Maintenant que le facteur humain a été explicité en termes d'enjeux et de problématiques, il est maintenant important de chercher des solutions. Ce chapitre va s'intéresser à la sensibilisation en abordant sa définition précise et en expliquant la méthodologie d'évaluation qui mènera alors à comprendre les lignes directrices dans le cadre d'une campagne de sensibilisation, c'est-à-dire au travail de sensibilisation au domaine.

5.2 Définition

"*Sensibilisation : Fait de susciter l'intérêt d'une personne, d'un groupe.*", LeRobert.

La sensibilisation est un concept souvent confondu avec la conscientisation et l'information. Cette confusion provient tant des définitions floues et variant d'une source à l'autre que de la difficulté à traduire avec précision "*awareness-raising*" de l'anglais selon le contexte dans la littérature.

Le tableau synthétique ci-dessous, réalisé par Francis Tilman de l'asbl le GRAIN permet de distinguer ces trois concepts [36].

	Information	Sensibilisation	Conscientisation
Données	Transmission de données et de grilles d'analyse	Transmission de données et de grilles d'analyse Présentation de questions éthiques et politiques. + intentions du chercheur et le problème qui le préoccupe Souci de partage de ce dernier.	Interpellation éthique et politique. Recherche de participation des destinataires à l'analyse et à la recherche de solutions.
Implication	Réception intellectuelle	Ouverture intellectuelle sur des enjeux et sur les responsabilités qui en découlent	Idem information et sensibilisation + formalisation de l'implication, concernant la domination et l'émancipation.

5.3 Évaluation de la sensibilisation

Pour évaluer la sensibilisation d'un individu, il faut trouver les facteurs qui la déterminent, c'est-à-dire ce qui peut être mesurable afin de comparer les mesures avant et après une campagne de sensibilisation.

Une étude de 2015 [34] a relevé des caractéristiques pertinentes issues des théories du comportement planifié, du modèle tripartite et la théorie de la conscience dans le but de former un modèle de théorie de sensibilisation à la sécurité de l'information.

L'étude a donné des résultats intéressants mais n'a pas permis d'établir un cadre concret ou un modèle d'évaluation. Il n'apporte pas non plus de nuance selon le profil du public et n'a pas été éprouvé. Dès lors, d'autres méthode, similaires mais plus tournées vers l'individu, ont inspiré la recherche.

5.3.1 Evaluation d'une campagne de sensibilisation

Plusieurs méthodes sont utilisées pour évaluer l'impact d'une campagne de sensibilisation. L'une d'entre elles, proposée par Wavestone, s'intéresse plus particulièrement aux campagnes liées à la cybersécurité [37].

Leur méthode trouve sa place dans un modèle de maturité, c'est-à-dire une échelle qui permettra d'évaluer l'avancement de la culture que l'on veut mettre en place au travers de la campagne de sensibilisation. Elle détermine aussi à partir de quel niveau certaines activités peuvent être mises en place comme la mesure quantitative des résultats par exemple.

En ce qui concerne la mesure du niveau de maturité en cybersécurité, ils distinguent 3 axes à évaluer.

— La sensibilité qui se réfère à la perception de l'importance de la sécurité,
— la connaissance qui se réfère au niveau de connaissance des utilisateurs vis-à-vis des enjeux et des bonnes pratiques de la sécurité,
— et enfin les comportements, qui, quant à eux, se réfèrent au niveau de respect des bonnes pratiques des utilisateurs.

Plusieurs méthodes sont possibles pour évaluer chaque axe, allant du QCM à l'observation. L'objectif est de visualiser, pour chaque axe, l'évolution quantitative en tant qu'indicateur [38].

5.3.2 La théorie du comportement planifié

Cette théorie permet d'étailler l'évaluation du comportement tel que décrit dans le cadre de wavestone cité précédemment. La théorie du comportement planifié s'appuie sur plusieurs variables pour prédire des conduites humaines [39]. L'adoption d'un comportement serait régit par l'intention de l'adopter ou non, permettant ainsi de prédire si une personne, selon son intention, exécutera ou non une action. Cette intention serait en fait influencée par trois facteurs par une relation causale.

1. L'attitude de l'individu vis-à-vis du comportement attendu,
2. sa perception des normes sociales entourant le comportement attendu,
3. sa perception du contrôle qu'il a sur le comportement attendu.

Ces trois dernières sont indépendantes, mais des relations de corrélation peuvent tout de même être observées. Les influences sont représentées sur le schéma suivant.

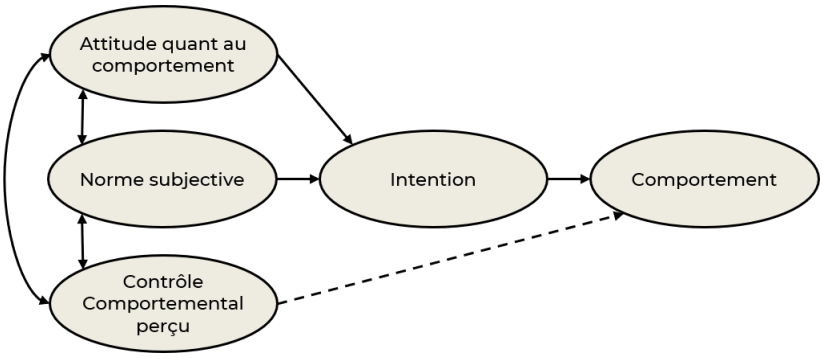

FIGURE 5.1 – Schéma de la théorie du comportement planifié [40]

Mathématiquement, cela peut être formulé comme suit :

$$C = \vec{u}(I) = \vec{u}(A, N, O)$$

avec C le comportement attendu, I l'intention de l'adopter, A l'attitude envers le comportement, N la perception de la norme et O la perception du contrôle sur le comportement.

L'intention est ainsi l'intermédiaire entre la complexité des concepts d'attitude, de norme et de contrôle et l'adoption du comportement attendu.

5.3.2.1 Les mesures des facteurs de la théorie du comportement planifié

Le **comportement** est "*...la réponse manifeste, observable par rapport à une cible donnée dans un situation donnée.*" [39] C'est l'élément qu'il faut clairement définir pour déduire l'intention. Il devrait être considéré selon ses quatre composantes, à savoir : l'action, la cible du comportement, le contexte de l'action et le temps de mise en oeuvre.

L'exemple qui suit représente un comportement par ses composantes.

Action	Une personne se lave les mains
Cible	Une personne peut se laver les mains au gel hydroalcoolique ou au savon
Contexte	Une personne peut se laver les mains chez lui ou dans un magasin
Temps	Une personne peut se désinfecter les mains avant de rentrer dans un magasin ou toutes les heures

L'**intention**, permet donc d'estimer à quel point un individu prévoit d'adopter le comportement déterminé plus tôt. C'est le facteur de motivation qui indique à quel point un individu est disposé à avoir un comportement ou à faire des efforts pour y parvenir. Elle serait directement proportionnelle aux chances de suivre un comportement.

Pour la mesurer précisément, le facteur de temps est à prendre en compte, car, si le temps n'est pas censé avoir des effets sur l'intention, il permet quand même à des évènements d'avoir lieu qui, eux, pourraient avoir des effets et modifier l'intention. Ainsi, certaines intentions ont de plus grandes ou de plus basses stabilités, rendant l'évaluation plus ou moins précise selon le temps. En revanche, si évaluer l'intention proche d'un comportement dans le temps améliore sa précision, l'évaluer juste avant n'aura souvent que peu d'intérêt.

Si l'on veut directement mesurer l'intention, on utilisera souvent des questions directes visant le comportement et des échelles de Likert [1]. Par exemple :

> *J'ai l'intention de me laver les mains régulièrement chez moi au cours des six prochains mois.*

Avec une échelle allant de *entièrement d'accord* à *entièrement en désaccord.*

L'**attitude**, qui est la "*...prédisposition affective ou évaluative.*" [39] et représente la sensibilité vis-à-vis de quelque chose, est une disposition dirigée vers une cible qui est influencée par des évènements vécus ou les connaissances acquises par un individu.

Dans le cas de l'influence sur un comportement, l'attitude serait en particulier le jugement en mal ou en bien du comportement, ce qui est donc bon ou mauvais à faire, une évaluation positive ou négative qui détermine si l'individu est personnellement favorable ou défavorable. C'est donc un jugement subjectif qui est sujet aux variations de croyances telles que les légendes urbaines ou les préjugés. En particulier, l'attitude consisterait bien à associer un jugement à la conséquence du comportement [42].

Cette composante peut être évaluée de manière directe ou indirecte. Les mesures directes sont effectuées par des échelles bipolaires à sept échelons pouvant aller d'agréable à désagréable ou de désirable à indésirable par exemple. La mesure indirecte, quant à elle, repose sur l' "*expectancy-value model*" qui suggère que l'attitude dépend de l'évaluation de la conséquence de l'action et du degré auquel l'individu croit que l'action entraînera la conséquence.

Mathématiquement, on obtiendrait la formule suivante qui décrit le score d'attitude envers un comportement.

$$A = \sum_{i=1}^{n} c_i \times e_i$$

1. Une échelle de Likert est une échelle d'attitude comprenant le plus souvent 5 à 7 degrés par laquelle on demande à l'individu d'exprimer son degré d'accord ou de désaccord relatif à une affirmation. Les échelles de Likert sont le plus souvent utilisées dans le cadre d'études quantitatives réalisées par le biais de questionnaires [41].

avec A le score d'attitude, c_i la croyance de survenue de la conséquence i en cas d'adoption du comportement, e_i l'évaluation de l'attitude envers la conséquence i et n le nombre de conséquences évaluées.

La **perception des normes sociales** représente la façon dont l'individu ressent le pression sociale et les influences de son entourage importantes tel que ses parents, amis, collègues ou supérieurs. Sa vision de leurs attentes, c'est-à-dire de leur potentielle approbation ou désapprobation, ou de leur attitude concernant le comportement, influence ses intentions de produire le comportement. Il s'agit encore d'une composante basée sur des croyances, une estimation évoluant dans le temps selon les connaissances et évènements vécus. Informer sur les tendances des personnes importantes peut donc modifier cette composante, de même que l'importance de l'entourage.

Cette composante peut également être évaluée de manière directe ou indirecte. La mesure directe consiste à demander à l'individu à quel point il pense que les personnes importantes pour lui approuvent ou désapprouvent le comportement ou à quel point ces personnes s'attendent à ce qu'il entreprenne l'action. La réponse à ces questions serait de préférence avec une échelle de Likert à sept échelons. La mesure indirecte repose sur le même "*expectancy-value model*" que pour la dernière composante. Il est attendu de l'individu qu'il réponde, sur une échelle de Likert, à quel point il est probable que l'adoption du comportement donné sera approuvée ou désapprouvée par la personne ou les personnes citées puis d'indiquer à quel point il compte se conformer à cette attente, toujours sur une échelle de Likert.

Mathématiquement, on obtient alors

$$P = \sum_{i=1}^{n} c_i \times o_{c_i}$$

avec P le score de perception de la norme sociale, c_i la croyance que la personne i approuve ou désapprouve le comportement i, o_{c_i} le degré auquel l'individu compte se conformer à l'attente et n le nombre de personnes citées.

La **perception du contrôle sur le comportement**, représente la perception du degré de contrôle sur le comportement évalué. En d'autres termes, il s'agit de la facilité avec laquelle l'individu se voit entreprendre le comportement. Un très grand nombre de facteurs peuvent influencer cette composante.

En particulier, deux facteurs sont représentés par les concepts de *locus de contrôle* et de *sentiment d'efficacité*. Le premier est la croyance d'un individu de ses possibilités d'influencer ou non le cours de sa vie. On distingue alors deux types de locus : le locus interne signifie que l'individu pense qu'il est responsable pour ce qui lui arrive et que les évènements sont liés à son comportement, tandis que le locus externe signifie qu'il attribuera le cours des évènements à des concepts comme le destin, la chance, ou en tous cas des concepts externes à lui. Le sentiment d'efficacité, ou d'auto-efficacité, reposerait sur des facteurs

amenant l'individu à penser qu'il est capable de performer ou non. Cela peut influencer ses compétences ou les efforts qu'il est prêt à fournir, voire ses réactions face à des obstacles. Ainsi, plus une personne se croit capable d'entreprendre une action, plus elle aura de chances de parvenir à l'entreprendre effectivement, que le sentiment soit réaliste ou non. Cela résulte donc encore de croyances vis-à-vis de ses capacités, de ses ressources, de la favorabilité du contexte ou d'autres éléments pouvant influencer la réussite de l'entreprise.

Il est à noter que ces facteurs n'ont pas de lien direct avec l'intention, influencée par les connaissances et les évènements vécu ; la perception peut changer sans que l'intention ne soit modifiée.

Deux types de mesures directes sont utilisées pour cette composante. La première consiste à demander à quel point l'individu à confiance en ses capacités ou à quel point il croit contrôler le comportement. L'autre manière repose sur des interviews préalables permettant d'éliciter des obstacles potentiels et de demander à quel point ceux-ci peuvent empêcher la bonne réalisation du comportement.

5.3.2.2 Méthodologie

Afin de comparer les intentions d'individus, qui sont l'antécédent direct du comportement, grâce à un score, la théorie est accompagnée de méthodes de construction de questionnaires [43].

La première étape consiste à définir le comportement. Il s'agit donc bien ici de définir la cible, l'action, le contexte et les éléments de temps.

Ensuite, il faut définir la population de recherche, c'est-à-dire, les personnes auxquelles le questionnaire sera adressé. Cette définition peut mener à faire des modifications dans le questionnaire pour s'adapter.

Subséquemment, six éléments sont formulés pour évaluer les composantes de la théorie, à savoir : l'attitude, la norme perçue, le contrôle perçu et l'intention.

Un questionnaire doit alors être proposé à des personnes représentant la population de recherche pour éliciter les éléments qui constitueront le questionnaire, c'est-à-dire les référents, les facteurs de contrôle et les conséquences. Le questionnement doit être fait individuellement. La construction dudit questionnaire consiste en plusieurs questions à adapter à la construction.

Cela permet alors de construire le questionnaire standard qui permettra de relever des mesures directes, avec des échelles de Likert.

Il est recommandé d'ajouter au questionnaire des éléments questionnant des facteurs démographiques, mais aussi d'autres types de questions directement liées au sujet analysé. Elles sont appelés "*background factors*" par l'auteur.

5.3.2.3 Validité de la thèse

Avec les années, la théorie du comportement planifié est devenue un modèle de référence dans le domaine de la psychologie sociale [44]. Ceci en raison du fait qu'elle a été éprouvée et qu'elle s'accorde bien à des études comparatives, mais également car elle s'avère ne pas nécessiter un grand nombre de variables à mesurer.

5.3.2.4 Applications

La thèse du comportement planifié est utilisable totalement indépendamment d'un domaine d'application [44], permettant de l'appliquer à n'importe quel domaine tant que celui-ci est maîtrisé. En revanche, il est recommandé de l'utiliser pour des comportements pouvant être identifiés, classifiés et exprimés correctement et avec précision. Celle-ci est considérée exploitable dans toutes les étapes d'un programme, c'est-à-dire autant dans l'analyse préalable des comportements que dans l'évaluation de la campagne.

Les domaines ayant utilisé la théorie du comportement planifié sont nombreux, allant de la promotion de la santé à la protection de l'environnement, en passant par la sécurité routière, l'acceptation d'un système informatique ou encore le partage de contenu sur les réseaux sociaux [45]-[47].

Chapitre 6

Lignes directrices pour la sensibilisation à la cybersécurité

6.1 Introduction

Maintenant que le contexte de la cybersécurité a été explicité que les axes par lesquels la sensibilisation au sujet est évaluée, les facteurs permettant de sensibiliser, et donc d'influencer ces axes, peuvent être abordés. Ce chapitre reprend toutes les lignes directrices trouvées dans la littérature liées à la recherche réalisée dans le cadre de ce mémoire, c'est-à-dire qu'elle est orientée vers la sensibilisation des jeunes.

La mobilisation, ou a fortiori l'introduction de changements dans les comportements individuels, peuvent être facilement adressés à un public déjà informé et prêt à agir. Pour les publics qui n'ont pas encore identifié le problème ou dont la prise de conscience n'est pas encore collective, la sensibilisation permet de faire naître la réflexion ou encore de favoriser la prise en compte de solutions ou de nouveaux comportements selon les activités.

L'exercice de la sensibilisation est complexe et dépend d'un grand nombre de variables. En particulier, en cybersécurité, un obstacle connu des campagnes de sensibilisation réside dans le fait que les solutions proposées n'ont pas toujours l'air faciles à mettre en place. Il faut montrer que les nouveaux comportements sont possibles [26]. Responsabilité, confiance, communication et coopération sont les bases de la culture de la sécurité [28].

La sensibilisation est considérée comme étant très complexe en raison des facteurs à prendre en compte pour la réussir, mais également parce que ceux-ci dépendent du contexte, de l'objectif et du public visé.

6.2 Les facteurs de sensibilisation généraux

En premier lieu, la compréhensibilité de la campagne a évidemment un impact sur sa réussite. Cela peut sembler évident mais il reste important de prendre le facteur en compte pendant le développement de la campagne. Le sentiment d'engagement a également un grand impact dans les campagnes de sensibilisation en général [26], [28].

Il est important, également, que la source de la campagne ait autorité dans le domaine, et que la campagne soit proposée à l'échelle de l'utilisateur, c'est-à-dire bien adaptée à lui. Aussi, les processus participatifs tendent à avoir de meilleurs résultats, en particulier lorsqu'ils stimulent la responsabilisation.

Enfin, des règles simples permettent de donner une impression de contrôle aux participants, et améliorent les interactions [28]. Il est important, quand même, d'éviter les conseils généraux répétitifs et ayant peu de sens [48]. Il faut se concentrer sur ce que l'on veut communiquer et l'objectif visé en donnant les bons comportements plutôt que de citer ce qui ne doit pas être fait [49].

La stratégie globale doit comporter plusieurs étapes qui sont, la définition de l'objectif, de la cible et des moyens à utiliser, le développement et le déploiement du matériel nécessaire. Ensuite, l'implémentation et la supervision permettent de vérifier l'efficacité du programme de sensibilisation [25].

De manière générale, la sensibilisation est sensible à différents facteurs et répond à un schéma qui permet de théoriser les composants d'une campagne de sensibilisation.

6.2.1 Le cadre MINDSPACE

Le cadre MINDSPACE [50] offre une particularisation des facteurs à prendre en compte dans une campagne de sensibilisation et permet de théoriser la formalisation des composants de cette dernière. Les facteurs sont représentés par chaque lettre du nom du cadre.

Le Messager représente l'importance d'avoir de la crédibilité vis-à-vis de ce que l'on veut communiquer.

L'Incitatif précise que l'utilisateur doit être incité à avoir de bons comportements en étant reconnu et récompensé.

Les Normes sont des normes sociales qui, contrairement à des comportements exceptionnels, rendront les bonnes pratiques durables.

Le Défaut signifie qu'un utilisateur s'écartera rarement de ce qui est déjà en place. Modifier des paramètres ou des configurations rendant de mauvais comportements plus complexes à avoir permettrait tout simplement de les éviter.

L'effet de Saillance est observé lorsque plusieurs informations sont visibles en même temps. Seul le plus important sera retenu.

L'effet de Priming exprime le fait qu'un utilisateur adoptera le comportement qui lui vient le plus spontanément. La mise en situation ou l'illustration des bonnes pratiques permet d'ancrer un comportement afin qu'il soit le premier venant à l'esprit.

L'Affect reprend certaines caractéristiques générales des campagnes de sensibilisation, comme la pertinence du matériel ou sa bonne planification.

La Consistance demande que l'utilisateur puisse sentir que son comportement est bien celui attendu.

Enfin, l'Ego de l'utilisateur est à prendre en compte, car il doit avant tout se sentir compétent pour conserver les comportements qui lui sont demandés.

6.3 Dans le cadre scolaire

Plusieurs recommandations ont été faites dans la littérature au sujet de la sensibilisation effectuée dans un contexte scolaire. En effet, au-delà des recommandations autour des programmes, de l'implantation ou du suivi, il est d'abord recommandé de bien informer les professeurs au préalable et d'essayer d'atteindre les parents et proches [51].

6.4 Principaux influenceurs en matière de cybersécurité

Si les facteurs influents pour les personnes adultes peuvent être très variés et plutôt constants, les adolescents, souvent très influencés par leur environnement et leurs contacts tendent à trouver difficilement des facteurs motivationnels. En particulier, ils tendent à réévaluer leurs compétences scolaires durant le passage au supérieur, avec souvent une tendance à la baisse dans certains domaines. Le domaine de l'informatique, en particulier, est souvent délaissé et principalement par les jeunes filles [52].

Un cadre théorique recommandé par les auteurs de [52] permet de visualiser les influences de différents composants dans les pratiques des adolescentes [53].

FIGURE 6.1 – Principaux facteurs d'influence chez les adolescents [53]

L'étude note aussi qu'il est important d'apporter des facteurs d'influence tôt afin d'intéresser les jeunes filles avant que leur intérêt ne décline, souvent vers 15 ans, car il n'aurait pas du tout tendance à pouvoir remonter [52]. Cela permettrait alors de pouvoir intéresser la moitié de la population qui risquerait d'avoir un sentiment d'efficacité particulièrement bas.

Les principaux influenceurs, selon l'étude, seraient la famille, l'école et les groupes ou communautés. La famille serait l'influenceur principal, comprenant parents, fratterie et famille étendue. L'école influencerait surtout via les personnalités rencontrées parmi le personnel. Les figures servant d'exemple peuvent parfois devenir le plus grand influenceur. Les groupes sociaux, quant à eux, influenceraient principalement les activités pratiquées. Cette tendance peut être mise en regard avec une étude réalisée en Italie sur plus de 2000 professeurs du secondaire [54]. Une grande sensibilité aux problèmes du numérique a été observée, mais la plupart déclarent qu'ils ne savent pas comment supporter des activités liées à ce domaine, démontrant une fois de plus l'importance cruciale d'en proposer.

6.5 Le réalisme

Les études s'accordent à dire qu'une approche efficace repose sur le réalisme des problèmes montrés aux personnes formées. Ainsi, l'individu peut véritablement avoir l'impression d'utiliser ses capacités techniques. Des problèmes physiques ou de simulation comme des jeux vidéos ou des exercices basés sur des scénarios ou encore des activités virtuelles sont cités comme exemples pour introduire le réalisme [55].

L'utilisation d'escape game a été testée, proposant un environnement immersif dans lequel les énigmes reposent sur des concepts de cybersécurité [56]. Il en a été déduit qu'il s'agit d'un bon outil d'éducation à la cybersécurité qui, en plus, encourage la compétition qui serait un bon moteur d'apprentissage.

6.6 Gamification

Étant donné que le processus d'intégration de nouvelles notions requiert de la participation et de la motivation de la part des participants, les expériences de jeu sont de plus en plus privilégiées dans l'enseignement de la cybersécurité [55], [57], [58].

La gamification consiste à ajouter des éléments de game design dans un contexte particulier pour permettre d'améliorer une expérience et ajouter de la valeur au contexte. C'est à ne pas confondre avec la ludification qui représente l'interaction lors du jeu.

Plusieurs mécanismes peuvent être utilisés pour gamifier quelque chose : la notion de progrès, de contrôle d'un avatar, des récompenses, des résolutions de problèmes en collaboration, des histoires et de la compétition. Cela aligne en fait l'activité avec ce que l'individu recherche, à savoir le succès, la réussite, la distinction et la récompense [57]. A ce sujet, la collaboration semble être le principal facteur de réussite pour les adultes [58]. D'autres compétences peuvent également être améliorée par le jeu, menant par exemple un participant à mener une résolution de problème qu'il pourra reproduire.

Aussi, des études montrent que l'on peut multiplier par 4 la quantité d'informations retenues lorsqu'elles ont été pratiquées plutôt qu'étudiées [58].

Attention en revanche, l'apprentissage par le jeu doit proposer des actions dont les conséquences peuvent être expérimentées par l'apprenant, apprenant par l'expérimentation et les erreurs [58].

Les jeux vidéo, activités virtuelles ou escape games [56] sont ainsi de bons outils selon ce facteur. De manière générale, la gamification promeut l'apprentissage actif et augmente la rétention d'informations en comparaison avec des méthodes plus traditionnelles [57].

Des alternatives, telles que l'utilisation d'outils visuels comme avec l'outil Roboscape [59] permet d'apprendre des concepts différemment et ont de très bons résultats chez les plus jeunes.

6.6.1 L'escape game en particulier

Un escape game, ou jeu d'évasion, est un jeu thématisé basé sur des énigmes scénarisées se passant dans un environnement immersif [60]. Inspiré des jeux de type "*point and click*" dans lesquels il fallait cliquer sur des éléments d'une pièce pour résoudre des énigmes et sortir de la pièce, ce type de jeu a beaucoup gagné en popularité depuis 2007. Ses composantes sont :

— Des énigmes,

— Un scénario immersif,

— Un game master servant à initier le scénario et mener l'histoire.

6.7 Compétition

La compétition permettrait d'améliorer l'engagement envers les activités d'apprentissage de la cybersécurité, d'augmenter la motivation et d'aider à évaluer les compétences [61]. Il s'agit souvent d'un élément qui peut être apporté par la gamification car il s'agit d'ajouter une notion liée au jeu dans un contexte qui n'est pas un jeu.

6.8 Recommandations spécifiques aux cours en ligne

En ce qui concerne les cours en ligne comme les MOOC, plusieurs points d'attention sont proposés par [62]. Le choix du sujet est d'une grande importance car nombreuses sont les lacunes dans les cours en ligne car les professeurs peinent à savoir quoi enseigner. Ensuite, les niveaux sont importants. En effet, les cours pour un niveau débutant sont très rares. L'adaptation aux commentaires, à l'âge et aux genres, si mal effectuée, peut également devenir un obstacle pour les apprenants. Les cours qui promeuvent l'interaction ont aussi de meilleurs résultats. Offrir des cours avec un rôle actif est recommandé, de même que d'offrir des moyens d'évaluer l'évolution dans l'apprentissage.

6.9 Facteurs inefficaces

De l'autre côté du spectre, plusieurs éléments sont à proscrire. Parmi eux, les cours en classe qui n'ont pas ou peu d'influence sur la sensibilisation à la

cybersécurité, les conseils prodigués en ligne de manière ponctuelle car ils ne sont pas du tout immersifs, les cours en ligne, les évènements thématiques autour de la cybersécurité, ou encore l'envoi de mails informatifs [57].

Chapitre 7

Analyse des besoins

7.1 Introduction

Dans les sections précédentes, nous avons pu déterminer quelles voies ont déjà été empruntées et quels aspects étaient encore à découvrir. Nous avons donc conscience de l'historique de la cybersécurité et des mesures déjà mises en place liées au facteur humain. Les recommandations peuvent maintenant être utilisées d'un point de vue pratique dans une analyse des besoins liés à l'outil de sensibilisation qui a été réalisé.

Dans ce chapitre, nous allons étayer l'étude qui a été réalisée et expliciter son intérêt en proposant une analyse des besoins qui reprendra d'abord l'objectif en détails, puis abordera le choix du public cible, le cadre thématique lié au domaine, les contraintes et besoins non fonctionnels élicités et enfin le support choisi.

7.2 Détermination de l'objectif

La piste d'étude choisie est le développement d'un outil de sensibilisation à la cybersécurité pour les étudiants du premier degré du secondaire.

L'outil développé sera conçu dans le but de remplir l'objectif de sensibilisation à la cybersécurité. Selon la théorie développée dans les chapitres précédents, celui-ci devrait, afin de poursuivre un objectif d'efficacité, respecter certaines caractéristiques relatives à sa nature, notamment, la génération d'un sentiment d'engagement, de responsabilité, de contrôle, amener à la coopération et la communication, apporter du réalisme, de compétition, une part de gamification et, si possible, des pistes de réponse.

Afin de répondre à une grande part des recommandations données dans la littérature, l'escape game a été retenu en tant qu'outil. Celui-ci permet, en

plus, d'apporter beaucoup de liberté dans son développement et dans les sujets abordés.

Ainsi, l'objectif de cette étude est bien de sensibiliser une population en proposant des données pertinentes vis-à-vis du problème qui nous préoccupe, c'est-à-dire la sécurité. Le public ne doit pas être amené à analyser le problème pour chercher de nouvelles solutions.

7.3 Choix du public

Le public visé au lors du développement de l'outil devait être les élèves du premier degré. Celui-ci a été choisi selon les recommandations trouvées dans la littérature ainsi que la maturité technologique des élèves en Belgique.

Les utilisateurs finaux étant souvent oubliés dans la gestion du facteur humain dans la cybersécurité, une intégration de ceux-ci via l'utilisation de personas a été proposée par [28]. En représentant les types utilisateurs, les personas permettent d'éviter d'oublier certains utilisateurs ainsi que d'identifier les risques, vulnérabilités et faiblesses de ceux-ci afin de proposer des outils de sensibilisation adéquats en termes de contenu et de support voire même d'incorporer le persona lui-même dans l'outil ou dans d'autres mesures de sécurité.

7.3.1 Personas

Pour être réussi, un persona devrait être construit avec des informations pertinentes et fabriqué avec des méthodes de design coopératif. Utiliser des scénarios basés sur des histoires permettent d'avoir plus d'engagement vis-à-vis de l'utilisateur [28]. Le processus de création de ces personas et de leur mise en oeuvre dans le cadre d'une campagne de sensibilisation, en 6 étape, est constitué d'une étape préliminaire liée à l'entreprise si la création du personas y est liée, puis d'une étape d'interviews de personnes représentant le public cible, l'analyse du contenu de ces interviews est la troisième étape, elle mène au design et au développement de la campagne, puis à son implémentation, et enfin, à son évaluation.

Les interviews ont mené à la création de deux personas. Les détails du suivi du processus vont maintenant être décrits.

Etape préliminaire

L'étape préliminaire convient à une démarche située au sein d'une entreprise. Le choix de ne pas la suivre a été fait pour cette raison.

Première étape : besoins et objectif

La première étape consiste à réunir les besoins qui motivent la démarche. Celle-ci se termine avec le choix du public.

Ainsi, l'objectif est la sensibilisation à la cybersécurité. Celle-ci se veut tournée vers les risques principaux auxquels un utilisateur peut être confronté.

En prenant en considération l'âge auquel les personnes sont les plus réceptives ainsi que les mesures prévues dans le pacte d'excellence en Fédération Wallonie-Bruxelles, l'objectif de conscientisation se dirigeait naturellement vers des élèves âgés d'environ 12 ans. Le pacte d'excellence prévoit d'ailleurs une approche de l'informatique dès 8 ans, mais il n'a pas encore été mis en place. Or, étant donné que le public âgé entre 8 et 12 n'est pas encore forcément accoutumé à la technologie, le choix a été fait de diriger l'outil vers un public plus âgé.

Le public d'élèves du premier degré de l'enseignement supérieur est âgé d'environ 11 à 15 ans et suit des cours d'informatique au sens large. Cela permet donc de ne pas avoir de problèmes liés au fait que le pacte n'est pas encore mis en application tout en ayant un public assez jeune pour être réceptif. Proposer l'outil à un public d'élèves de primaire nécessiterait de nouvelles adaptations vis-à-vis de leur âge et de leur formation.

Deuxième étape : Personas

Cette étape consiste à interviewer des personnes afin d'éliciter des informations qui permettent de créer l'archétype de l'utilisateur.

Dans ce cas, 4 élèves du secondaire, âgés de 13 à 15 ans, ont été interviewés.

Le questionnaire qui leur a été proposé a permis d'obtenir les personas mais ont également servi à la mise en place de l'évaluation en suivant les recommandations de la théorie du comportement planifié, reprenant chaque composant du comportement afin d'obtenir des résultats qualitatifs.

Le questionnaire des interviews reprenait les questions suivantes :

Q1	Quel âge as-tu ?
Q2	Quelles études fais-tu ?
Q3	Comment se passe l'école ?
Q4	Comment te sens-tu vis-à-vis de l'informatique et de la cybersécurité ?
Q5	Décris ton utilisation d'internet en général.
Q6	Aimerais-tu en savoir plus sur la cybersécurité ?
Q7	Que penses-tu de la cybersécurité ?
Q8	Quels sont les avantages de faire attention à son empreinte numérique ?
Q9	Quels sont les avantages de faire attention à ses mots de passe ?
Q10	Quels sont les avantages de faire des sauvegardes de ses fichiers ?
Q11	Quels sont les avantages de faire attention aux mails qu'on reçoit ?
Q12	Quels sont les inconvénients faire attention à son empreinte numérique ?
Q13	Quels sont les inconvénients faire attention à ses mots de passe ?
Q14	Quels sont les inconvénients faire des sauvegardes de ses fichiers ?
Q15	Quels sont les inconvénients faire attention aux mails qu'on reçoit ?
Q16	A quoi penses-tu en premier lorsque l'on te dit de faire attention à son empreinte numérique ?
Q17	A quoi penses-tu en premier lorsque l'on te dit de attention à ses mots de passe ?
Q18	A quoi penses-tu en premier lorsque l'on te dit de faire des sauvegardes de ses fichiers ?
Q19	A quoi penses-tu en premier lorsque l'on te dit de faire attention aux mails qu'on reçoit ?

Q20	Enumère les personnes ou groupes de personnes qui approuvent ou pensent que tu dois faire attention à ton empreinte numérique.
Q21	Enumère les personnes ou groupes de personnes qui approuvent ou pensent que tu dois faire attention à ses mots de passe ?
Q22	Enumère les personnes ou groupes de personnes qui approuvent ou pensent que tu dois faire des sauvegardes de ses fichiers ?
Q23	Enumère les personnes ou groupes de personnes qui approuvent ou pensent que tu dois faire attention aux mails qu'on reçoit ?
Q24	Enumère les personnes ou groupes de personnes qui désapprouvent ou pensent que tu ne devrais pas faire attention à ton empreinte numérique.
Q25	Enumère les personnes ou groupes de personnes qui désapprouvent ou pensent que tu ne devrais pas faire attention à ses mots de passe ?
Q26	Enumère les personnes ou groupes de personnes qui désapprouvent ou pensent que tu ne devrais pas faire des sauvegardes de ses fichiers ?
Q27	Enumère les personnes ou groupes de personnes qui désapprouvent ou pensent que tu ne devrais pas faire attention aux mails qu'on reçoit ?
Q28-29	Enumère les personnes ou groupes de personnes les plus/moins susceptibles de faire attention à ton empreinte numérique.
Q30-31	Enumère les personnes ou groupes de personnes les plus/moins susceptibles de faire attention à ses mots de passe ?
Q32-33	Enumère les personnes ou groupes de personnes les plus/moins susceptibles de faire des sauvegardes de ses fichiers ?
Q34-35	Enumère les personnes ou groupes de personnes les plus/moins susceptibles de faire attention aux mails qu'on reçoit ?
Q36-37	Enumère les personnes ou groupes de personnes les plus/moins susceptibles de faire attention à ton empreinte numérique.
Q38-39	Enumère les personnes ou groupes de personnes les plus/moins susceptibles de faire attention à ses mots de passe ?
Q40-41	Enumère les personnes ou groupes de personnes les plus/moins susceptibles de faire des sauvegardes de ses fichiers ?
Q42-43	Enumère les personnes ou groupes de personnes les plus/moins susceptibles de faire attention aux mails qu'on reçoit ?
Q44-45	Enumère ce qui faciliterait/rendrait difficile de faire attention à ton empreinte numérique.
Q46-47	Enumère ce qui faciliterait/rendrait difficile de faire attention à ses mots de passe ?
Q48-49	Enumère ce qui faciliterait/rendrait difficile de faire des sauvegardes de ses fichiers ?
Q50-51	Enumère ce qui faciliterait/rendrait difficile de faire attention aux mails qu'on reçoit ?

Une discussion ouverte a suivi les interviews, permettant de récolter plus

d'informations. Une analyse de contenu a mené à une élicitation des idées des interviewés et d'une retrancription sous forme d'expressions ou de mots. L'analyse des réponses a été réalisée selon un codage ouvert, sans grille d'analyse réalisée au préalable.

Ce travail a mené à la création des deux personas ci-contre et à l'écriture du questionnaire comparatif utilisé pour l'évaluation de l'outil développé.

Lucas	Aptitudes	Lucas est étudiant en section technique du secondaire. Il aime apprendre par la pratique et se renseigner par lui-même sur internet à propos de sujets qui l'intéressent.
14 ans	Compétences	Lucas est habitué à toucher à l'informatique. C'est à lui que sa famille se réfère lorsqu'il y a un problème et il n'a pas peur de toucher à tout pour trouver des solutions en cas de problème, mais il n'a pas une maîtrise profonde des concepts.
Section technique secondaire	Activités	Il passe beaucoup de temps sur son ordinateur. Il joue à des jeux vidéo et regarde beaucoup de vidéos sur Twitch. Il lui arrive d'aller sur des sites de téléchargement illégaux.
Célibataire, sans enfant	Motivations	Lucas a très envie d'en apprendre plus pour se sentir encore plus compétent dans le domaine. Il n'a pas l'impression d'avoir besoin d'apprendre à se protéger sur internet ou de changer ses pratiques sur son ordinateur.
	Attitude	Lucas pense que ses connaissances sont avancées. Il se sent à l'aise avec les concepts dont il connait le nom. Le domaine ne lui paraît pas particulièrement complexe et il a l'impression d'être compétent dans celui-ci.

Léa	Aptitudes	Léa est élève en général en secondaire. Elle est assez studieuse et n'apprend presque qu'exclusivement à l'école.
15 ans	Compétences	Léa ne s'y connait pas beaucoup en informatique ou dans le domaine de la cybersécurité. Elle connait quelques notions, principalement grâce à ce qu'elle a vu à la télé ou ce que ses parents et amis ont pu lui dire. Elle n'a rien appris à l'école à ce sujet.
Section générale secondaire	Activités	Elle regarde beaucoup de films et de séries en streaming. Elle poste beaucoup de contenu sur ses réseaux, c'est-à-dire plusieurs fois par semaine.
Célibataire, sans enfant	Motivations	Léa aimerait beaucoup en savoir plus pour pouvoir se protéger. Elle sait qu'il peut il y avoir des dangers mais elle ne sait pas lesquels. Elle pense qu'il est important d'être renseigné.
	Attitude	Léa pense que le domaine de l'informatique est difficile d'accès et que sa protection vient principalement des mesures mises en place dans les logiciels. Elle a souvent peur de mal faire et prend vite peur lorsque quelque chose ne fonctionne pas comme elle le voudrait, mais se sent sereine de manière générale.

FIGURE 7.1 – Personas développés pour cette étude

En raison de la quantité limitée d'informations car ceux-ci ont été développés à partir de 4 interviews, il n'y avait pas suffisamment d'informations pour former des distinction entre motivations internes ou externes ou encore des distinctions d'attitude.

Troisième étape : analyse

La troisième étape consiste à éliciter les besoins pertinents en analysant chacun des personas. Le contenu des interviews a également été retenu afin d'enrichir la réflexion. En considérant comment chaque persona réagirait à des scénarios inspirés des statistiques relatives à l'objectif, les plus grandes faiblesses ont été identifiées.

— Les métiers de la cybersécurité

— L'empreinte numérique

— Les mots de passe
— L'anonymat sur internet
— Les menaces sur internet
— Principe du chiffrement et processus de sécurité

Le détail sera donné dans la section 7.4 Détermination des sujets à aborder.

Quatrième étape : design et développement

La quatrième étape sert à sélectionner les canaux de communications de sensibilisation.

Le choix s'est porté sur un escape game scénarisé dont l'objectif est d'incarner un expert en cybersécurité devant sauver le directeur de la perte des bulletins des élèves. Aucun service n'offre un support suffisant, celui-ci a été entièrement développé pour cette étude. Plusieurs itérations ont été prévues, notamment pour équilibrer la difficulté et le travail en collaboration pour l'utilisateur, ainsi que pour ajouter des aspects de compétition. Dans les faits, seule une itération a été possible en raison des difficultés à tester la première version.

Aucun autre canal, ni primaire, ni secondaire, n'a été prévu en complément même si cela est proposé dans la théorie.

Cinquième étape : Implémentation

La cinquième étape consiste à former une stratégie de développement permettant de respecter les ressources de temps et de personnel allouées.

L'implémentation a été planifiée sur un mois, suivie d'environ 20 jours de tests et d'itérations, en parallèle avec le développement d'un système de mesures pour tester l'efficacité de l'outil.

Sixième étape : révision

Cette dernière étape fournit du contenu pour de futures itérations. Elle sert à identifier l'efficacité, les bons et les mauvais côtés de la campagne de sensibilisation. Ceux-ci seront abordés dans le chapitre 11 Contributions, limites et perspectives.

L'évaluation de l'outil n'a donné lieu qu'à une évaluation, sans itération.

7.4 Détermination des sujets à aborder

7.4.1 Introduction

Le domaine étant très large, il est évident que certains sujets seulement ont été retenus. Ceux-ci ont été choisis en fonction des plus pertinents selon les

statistiques de vulnérabilités vis-à-vis du public, c'est-à-dire le facteur humain, qui a été choisi au préalable, ainsi que vis-à-vis des capacités et de la formation numérique de ceux-ci. Il a également été influencé par le contenu des interviews réalisées pour la création des personas.

7.4.2 Les menaces sur internet

Les menaces sur internet ont été choisies car il s'agit de l'enjeu principal de la cybersécurité. Celles-ci ont été restreintes aux menaces les plus répandues dans le cyberespace chez les particuliers, à savoir l'ingénierie sociale sous forme de phishing et le malware. Il s'agit aussi des deux vulnérabilités principales auxquelles les personas peuvent être confrontés [63].

7.4.3 Les pratiques de mots de passe

Parmi les bonnes pratiques ayant le plus d'impact sur la protection des données, les pratiques de mots de passe sont parmi les plus faciles à mettre en place.

L'utilisation de mots de passe n'ayant pas ou peu de sémantique permet d'éviter que certains logiciels générateurs de mot de passe utilisés dans les attaques *brute force* puissent utiliser des dictionnaires afin de trouver le mot de passe plus rapidement.

Varier les mots de passe permet également d'éviter que plus de données personnelles fuitent dans le cas où un mot de passe est obtenu par une personne malveillante, d'une manière ou d'une autre.

Ainsi, ces deux pratiques sont retenues.

7.4.4 L'empreinte numérique et l'anonymat sur internet

Une difficulté, lors de la sensibilisation d'un public à un sujet, est de proposer une ouverture sur les problématiques liées au domaine auquel le public va être sensibilisé. L'empreinte numérique et l'anonymat sont des problématiques très liées à l'âge du public visé, et celles-ci ont récemment évolué avec des des générations d'utilisateurs ayant une empreinte numérique de plus en plus grande et commençant de plus en plus jeune.

Il s'agit aussi de problèmes liés aux comportements des jeunes ayant certains accès sans avoir la maturité numérique suffisante pour se protéger ou tout simplement pour comprendre le problème auquel ils sont confrontés.

7.4.5 Les métiers de la cybersécurité

L'incarnation d'un expert en cybersécurité a été choisi dans le but de permettre d'obtenir plus d'implication de la part du public. Sachant que la théorie

du comportement planifié nous informe que le contrôle perçu permet d'augmenter les chances de suivre un comportement, il s'agit d'un moyen de donner à l'utilisateur l'impression d'avoir un grand contrôle en incarnant un expert.

7.4.6 Principe du chiffrement et processus de sécurité

Ce thème n'a d'abord été motivé ni par les données de personas ni par les lignes directrices. Il a été motivé par la nature de l'outil lui-même afin d'ajouter en gamification car le thème se prêtait bien au développement d'énigmes de difficultés variées et adaptables au public cible.

Ainsi, l'étude suivante s'intéressera à la **conception, au développement et à l'évaluation d'un escape game visant la sensibilisation aux métiers de la cybersécurité, à l'empreinte numérique, aux bonnes pratiques de mots de passe, à l'anonymat et aux menaces sur internet et aux principes de chiffrement et de processus de sécurité**.

7.5 Détermination des contraintes et besoins non-fonctionnels

Les contraintes non fonctionnelles ont été prises en compte afin de respecter le contexte de test envisagé à cette étape, c'est-à-dire dans un contexte scolaire ou dans le cadre d'évènements ponctuels à destination des élèves du secondaire.

De manière préventive, cinq contraintes on été retenues.

— Respect des données des joueurs
— Désinfection totale possible
— Minimisation des outils nécessaires en plus de l'outil proposé
— Tout élément produit/proposé sera justifié
— Durée limitée à 50 minutes

Respect des données des joueurs

Le respect des données est directement lié au RGPD, il est évident qu'il fallait que l'outil de sensibilisation ainsi que ceux d'évaluation de l'outil respectent toutes les mesures.

Désinfection totale possible

Étant donné le contexte sanitaire dans lequel le développement de l'outil a eu lieu, il était important que tout outil produit puisse être entièrement désinfectable ou jetable.

Minimisation des outils nécessaires en plus de l'outil proposé

Afin d'obtenir un outil simple à mettre en place et motivant son utilisation, la minimisation des accessoires utiles à l'outil est une contrainte qui a été maintenue. Le public prévu étant des élèves du secondaire, il était possible que la mise en place soit réalisée par les professeurs et pas par une personne impliquée dans le développement ou le processus de test de l'outil. Sa bonne réalisation pouvait ainsi être assurée.

Tout élément produit/proposé sera justifié

Cette contrainte est liée au contexte scolaire dans lequel l'outil pourra être utilisé. En effet, l'encadrement ne pouvant se faire entièrement par une personne compétente dans le domaine de la cybersécurité, il était important que toute notion puisse être explicitée et que l'outil en lui-même ait un cadre le justifiant et qu'il soit entièrement utilisable en autonomie.

Durée limitée à 50 minutes

Cette contrainte a été fixée afin d'assurer le bon déroulement du test de l'outil ainsi que son utilisation dans un contexte scolaire. Étant donné que la durée des cours dans le secondaire est fixée à 50 minutes, cette durée simplifie sa mise en place.

7.6 Choix du support

La nature de l'outil fut l'objet d'un choix dirigé par le souhait d'avoir un support suivant les lignes directrices énoncées plus tôt en section 7.3.1, respectant les contraintes non fonctionnelles et adapté au public cible.

Ainsi, l'escape game réalisé sur un logiciel immersif permet d'avoir un seul support qui n'a pas besoin d'être désinfecté, et allie aussi les possibilités de jeu en collaboration tout en offrant de très vastes possibilités et un support approprié au domaine de la cybersécurité pour l'immersion.

Chapitre 8

Développement et implémentation

Le chapitre précédent a décrit l'analyse des besoins qui a été réalisée en amont afin de déterminer en quoi consistera l'outil de sensibilisation. Ce chapitre va maintenant expliciter les étapes de développement et d'implémentation qui ont été suivies en abordant le prototypage et l'implémentation qui ont mené à la formation de l'outil pédagogique en détails.

8.1 Prototype

Prototyper un logiciel consiste à organiser des activités qui permettent d'orienter le développement d'un logiciel encore incomplet en formant des artéfacts différents du produit final.

Ici, les prorotypes ont permis de représenter un OS fictif auquel les joueurs ont été confronté afin d'agir en tant qu'expert en cybersécurité pour résoudre l'activité.

8.1.1 Inspirations

Gameplay et design

La première étape du prototypage du produit est de trouver des sources d'inspiration. Ainsi, l'escape game devant pouvoir être fait sur ordinateur majoritairement, son activité précurseure, le jeu "*point and click*", fut une grande inspiration. En particulier, un jeu vidéo de type "*point and click*" sorti en 2020 reprend une partie de gameplay qui inspira grandement l'outil développé.

FIGURE 8.1 – Capture d'écran du jeu There is No game

Il s'agissait d'un faux OS intégré dans le jeu "There is No game" demandant à l'utilisateur de naviguer dessus et d'effectuer certaines actions afin de passer à la suite de l'aventure.

8.1.1.1 Design graphique

Plusieurs designs ont inspiré les différents composants de l'OS fictif.

Corbeille :

La corbeille a été inspirée de la corbeille Windows, avec des options visibles sur de grandes icônes dans les paramètres de la corbeille.

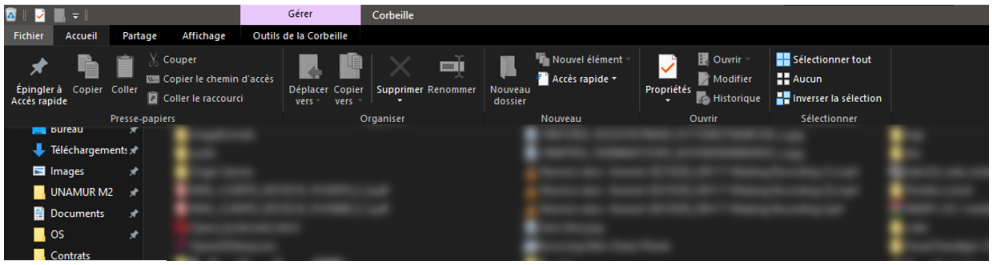

FIGURE 8.2 – Capture d'une corbeille Windows

Instagram et Facebook :

Il s'agit des deux réseaux sociaux les plus utilisés [64] **sur ordinateur** chez les 12-15 ans. Leur interface web a été reprise afin d'être reconnaissable.

FIGURE 8.3 – Capture du site Instagram

FIGURE 8.4 – Capture du site Facebook

Message électronique Un message électronique malveillant est affiché durant le jeu d'escape game. Celui-ci est directement inspiré d'un mail de phishing publié par Bpost sur leur compte Twitter.

FIGURE 8.5 – Mail malveillant publié par par bpost [65]

8.1.2 Wireframe

Sur base des inspirations, le prototypage peut consister, comme première étape, en l'élaboration de wireframes. Ceux-ci permettent de visualiser les composants de l'écran ou encore les comportements.

Dans ce cas-ci, les comportements sont principalement calqués sur ceux d'un OS classique, ne justifiant donc pas de les modéliser avec des wireframes. En ce qui concerne les composants, étant donné que plusieurs écrans seront grandement inspirés de logiciels existants, seul un écran a été représenté via wireframe.

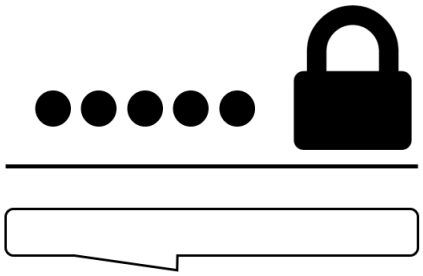

FIGURE 8.6 – Wireframe d'une page de connexion réalisé pour cette étude

Ce wireframe a été designé afin de répondre à une interrogation quant au placement du message accompagnant le scénario. Il est placé dans le fond de l'écran sur cette représentation et a subi des modifications depuis.

8.2 Implémentation

8.2.1 Scénario

Plusieurs itérations sur le scénario de l'escape game ont mené à la réalisation d'un scénario basé sur une histoire voulant lier l'incarnation d'un expert en cybersécurité afin de simuler l'impression de contrôle des utilisateurs et une situation proche d'eux afin d'obtenir une histoire qui soit bien adaptée et simple à appréhender. Le scénario est composé de plusieurs énigmes et actions à effectuer, basées sur les sujets élicités selon les lignes directrices et les personas réalisés précédemment.

La formation d'un scénario doit suivre quelques étapes. D'abord la détermination de l'objectif pédagogique, qui a été fait dans les sections précédentes, ensuite l'écriture du début et de la fin du scénario, la conception des énigmes,

des aides éventuelles, et enfin, le test et l'adaptation et la remise à zéro si besoin [66]

Le tableau suivant reprend les différentes étapes à suivre dans la narration et avec les indices disponibles à chacune de ces étapes.

n°	Etat	Indice	Action à réaliser
1	L'écran affiche les informations d'un message électronique : date, adresse email de l'expéditeur, objet et contenu du mail	Un indice reformulant l'action à réaliser est disponible	L'objectif est de cliquer sur les trois éléments typiques du mail de phishing. Dans ce cas, il s'agit d'une adresse mail n'appartenant pas à l'expéditeur présumé, d'un objet avec un message poussant à l'action, et d'un problème soulevé dans le mail invraisemblable.
2	L'écran affiche un cadenas avec un espace pour introduire un mot de passe. L'assistant informe les joueurs que plusieurs techniques existent pour se souvenir de son mot de passe.	L'indice indique que l'on peut utiliser un mot de passe facile ou écrire son mot de passe quelque part pour ne pas l'oublier, même si c'est une mauvaise idée	Un post it avec le mot de passe est placé près de l'ordinateur. Il faut l'entrer pour ouvrir la session de l'ordinateur.
3	Le bureau de l'ordinateur affiche une corbeille, un navigateur et un dossier de bulletins	NA	Les joueurs doivent cliquer sur les bulletins pour découvrir qu'ils ont été cryptés et qu'ils ont besoin d'un code. L'assistant suggère que l'on fouille la corbeille.
4	Dans la corbeille, aucun fichier n'est visible. Trois icônes sont apparents pour vider la corbeille, restaurer des fichiers et retrouver des fichiers sur le disque	NA	En restaurant les fichiers supprimés, une note apparaît.
5	Une note est contenue dans la corbeille.	NA	En cliquant sur la note une énigme donnant la composition du code pour décrypter les fichiers apparaît. Il s'agit du nom de son chat et un mot de passe simple à 5 chiffres, le tout crypté avec un chiffrement de César. A la fin de la note, le nom du hacker apparaît en tant qu'auteur du fichier.

6	Les joueurs savent maintenant quel est le pseudo du hacker. L'assistant propose de le chercher sur internet.	Un indice permet de comprendre où était situé le pseudonyme du hacker ainsi que où l'utiliser.	Les joueurs doivent chercher le pseudo du hacker sur insta-gram afin d'obtenir son vrai nom, situé dans la description.
7	Les joueurs connaissent maintenant le vrai nom du hacker.	L'indice dit qu'il est possible de voir le vrai nom du hacker quelque part.	En recherchant le nom trouvé, la page facebook laisse apparaître un compte dont les publications révèlent le nom du chat du hacker.
8	Les joueurs ont maintenant toutes les informations qui permettent de trouver le code. L'assistant explique comment effectuer un chiffrement de César.	L'indice explique qu'il existe des mots de passe simples à 4 chiffres qui sont 1234.	Pour déchiffrer le dossier, le nom du chat et le mot de passe simple à 5 chiffres, c'est à dire 12345, doivent être chiffrés de manière à obtenir le code à appliquer.
9	Le dossier est finalement vide. En revanche, une sauvegarde a été faite et permet de récupérer une ancienne version	NA	Les joueurs doivent obtenir l'ancienne sauvegarde en cliquant sur l'icône puis cliquer sur le fichier ainsi retrouvé.
10	Un terminal apparaît, expliquant que le fichier était en fait infecté par un virus. Les joueurs ont deux minutes pour mettre en place des actions de protection.	NA	Les joueurs doivent changer les mots de passe en proposant trois mots de passe différents et suffisamment longs, faire une analyse des fichiers de l'ordinateur et effectuer un backup.

Le scénario demandant aux joueurs de mettre en place les solutions qui sont suggérées, il montre la faisabilité de ces solutions et d'avoir son Ego pris en compte comme le suggère le cadre MINDSPACE, augmentant les chances que le comportement soit adopté, de même que le processus participatif induit notamment par la complexité de certaines énigmes, par exemple grâce au chiffrement. La ligne directrice recommandant de donner les bons comportements au lieu de citer ce qui ne doit pas être fait a également été suivi en offrant les bons comportements résumés et explicités à mettre en oeuvre en pratique.

Pour reprendre le cadre MINDSPACE, le Messager manque de crédibilité, mais les bons comportements sont bien récompensés à la fin de l'escape game. Aussi, l'effet de Saillance induit de retenir les éléments les plus frappants. Dans ce cas, les risques de cybermenaces seront retenues par les participants. L'effet de Priming, quant à lui, utilise l'illustration des bons comportements, dans ce cas les bonnes pratiques à mettre en oeuvre, pour permettre à l'utilisateur de s'en souvenir et de les faire spontanément lorsqu'il en aura besoin. La Consistance, directement intégrée grâce à l'utilisation d'un scénario, garanti à l'utilisateur de savoir qu'il a le comportement attendu.

Le scénario a été gamifié mais reprend beaucoup d'éléments existants afin

de paraître vraisemblable et ne pas tomber dans un gameplay manquant de réalisme comme suggéré dans les lignes directrices.

8.2.2 Développement

Après obtention d'un scénario suffisamment avancé, le développement du logiciel a commencé. Celui-ci a suivi un modèle par incréments, c'est-à-dire par décomposition en composants qui ont été développés en parallèle ou en séquence selon l'architecture prévue.

Ce développement se prêtait particulièrement à la technologie utilisée pour le développement, *electron*. La technologie et ce modèle de développement privilégient tous deux un noyau principal développé en amont, puis des incréments avec une reconception et des tests.

8.2.3 Architecture

La structure du logiciel est reflétée dans l'arborescence des fichiers. Il s'agit d'un noyau principal, situé à la base de l'arborescence, puis de composants.

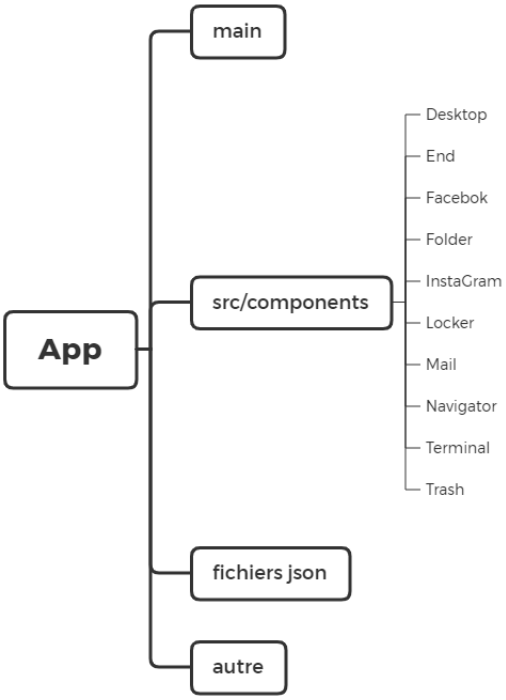

FIGURE 8.7 – Arborescence de fichiers du logiciel développé pour l'escape game

Les différents composants sont :

— Desktop est le composant gérant le bureau, ses interactions avec les autres composants et son interface.
— End est le composant des interfaces de fin et de leur affichage.
— Facebok est le composant du site Facebok, gérant son affichage et les interactions avec l'utilisateur.
— Folder gère l'archivage fictif des fichiers.
— InstaGram correspond au composant du site Insta-Gram, qui gère l'affichage et l'interface.
— Locker est le composant du verrouillage de la session.
— Mail est le composant d'analyse du mail malveillant, qui gère son utilisation et les interactions.

— Navigator est le composant précédant celui de Facebok et de Insta-Gram, qui permet d'y accéder en tant que navigateur.

— Terminal est le dernier composant utilisé dans le déroulement de l'escape game. Il gère l'étape chronométrée qui suit l'infection par un virus dans le scénario.

— Trash est le composant chargé de l'interface et des interactions de la fausse corbeille.

8.2.4 Interface

Deux problèmes principaux ont dû être résolus du point de vue de l'utilisabilité.

8.2.4.1 Interventions de l'assistant

Durant les tests sur utilisateur, ces derniers ont rencontré des difficultés à comprendre l'intention du message de l'assistant. Le design de l'interface ne leur permettait pas de comprendre qu'il s'agissait d'un élément externe à la fausse interface d'ordinateur ou de voir le changement de message, les menant à manquer certaines informations pendant des étapes cruciales.

Pour y remédier, plusieurs éléments ont été mis en place. D'abord, une coloration derrière la bulle de message pour lui donner du relief et donner l'impression qu'il ne s'agît bien que d'une surcouche sur l'interface. Ensuite, une barre verticale clignotante, c'est-à-dire un caractère ascii 124 | , servant à sous-entendre qu'il s'agit d'une discussion en cours, que l'assistant vient d'écrire, pour que l'utilisateur le lise. Enfin, des petits visages avec une expression, colorés et clignotants ont été ajoutés. Cela permet de faire varier l'expression et la couleur pour que le joueur voie un changement dans le message de l'assistant.

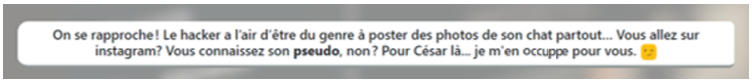

FIGURE 8.8 – Exemple de message reçu de l'assistant dans le jeu

8.2.4.2 Orientation de l'utilisateur

L'escape game est basé sur un scénario permettant de récolter des informations afin de résoudre des énigmes. Le suivi de ce scénario est une condition nécessaire à la compréhension des énigmes et de l'histoire. En évitant certaines étapes, le suivi est impossible et donc l'objectif de sensibilisation est altéré.

Pour orienter le joueur, et sur les conseils de la co-promotrice à ce mémoire, Julie Henry, des pop-up ont été ajoutés, contenant le message " *Vous n'avez pas assez d'indice pour vous rendre ici.*".

8.2.5 Livret explicatif

Un livret explicatif et d'accompagnement a été produit pour permettre aux enseignants du secondaire de mettre en place l'activité, l'animer, et effectuer un suivi ensuite.

Il contient une présentation de l'escape game, les explications nécessaires à la mise en place ainsi que les réponses à des questions potentielles ou des difficultés rencontrées durant les tests qui requièrent des informations supplémentaires.

Le scénario illustré avec la résolution de l'escape game est fourni, avec, pour chaque étape, les objectifs suivis. Enfin, un résumé des notions abordées propose des explications afin de répondre aux questions potentielles des joueurs.

8.2.6 Artéfacts produits

En résumé, trois artéfacts ont été produits à destination des professeurs :

— Un logiciel d'escape game

— Un livret explicatif et d'accompagnement

— Une courte vidéo d'aide à l'installation

Le logiciel et le livret explicatif sont disponibles au lien suivant : `https://drive.google.com/drive/folders/1HkFJfGtIBI8i3yO3dvhMz93A3L78i78L?usp=sharing`

Chapitre 9

Méthode d'évaluation

9.1 Introduction

Les chapitre précédents ont mené à connaître l'état d'avancement du domaine afin de trouver les lignes directrices pour la conception et le développement de l'outil d'aide à la sensibilisation à la cybersécurité ainsi que les méthodologies à suivre pour son évaluation. Le chapitre suivant abordera cette dernière en faisant suite à la description de la conception et du développement.

Celui-ci reprendra le cadre théorique qui a été suivi puis explicitera les étapes de construction du questionnaire qui a été mis au point afin d'évaluer l'impact de l'outil de sensibilisation dans cette étude comparative. Le procédé d'évaluation et ses contraintes ainsi que l'analyse et ses limitations seront aussi explicités dans ce chapitre.

9.2 Cadre théorique

Afin d'évaluer la sensibilisation opérée par une campagne, wavestone préconise [38], comme expliqué dans les chapitres précédents, de baser l'évaluation de l'efficacité de la campagne sur des questionnaires abordant trois axes : la sensibilité, la connaissance et les comportements. Plusieurs méthodes sont alors possibles, sans aucune préconisée en particulier. Des études ont récemment tenté de proposer un vrai cadre d'évaluation sans encore parvenir à une méthode concrète. Celles-ci tendent à s'inspirer de plusieurs modèle, dont, en particulier, celle du comportement planifié [67] , [68], [34].

L'évaluation de la sensibilisation opérée grâce à l'outil développé pour cette recherche s'est ainsi inspirée de ces travaux. Elle a été réalisée via des questionnaires basés sur les trois axes cités précédemment, suivant les recommandations

de la théorie du comportement planifié afin de construire le questionnaire et d'orienter les questions de l'axe comportemental.

Le même questionnaire a été proposé à des élèves du secondaire n'ayant pas passé l'escape game ainsi qu'à des élèves après avoir participé à l'activité d'escape game. Initialement, le public devait être des élèves du premier degré du secondaire mais la situation sanitaire n'a pas permis de réaliser des interventions en classe telles que prévues. Ainsi, pour éviter un nombre de testeur trop réduit, le public a été finalement âgé de 12 à 18 ans, c'est-à-dire limité au secondaire.

9.3 Construction du questionnaire

La construction du questionnaire a été réalisée en suivant les étapes recommandées de la théorie du comportement planifié [43].

9.3.1 Définition du comportement

Le comportement a été défini selon sa cible, l'action, le contexte et les éléments de temps. Étant donné que plusieurs comportements ont été sélectionnés, on considère qu'il s'agit en réalité d'un comportement défensif constitué de plusieurs éléments : les pratiques de mot de passe, les sauvegardes de sécurité, l'empreinte numérique et le phishing. Ceux-ci correspondent aux bonnes pratiques abordées dans l'activité.

Dès lors, le comportement consiste en la considération de bonnes pratiques de mots de passe lors de leur création et de leur maintien, la réalisation de sauvegardes de sécurité régulières, l'attention au contenu posté en ligne, et aux mails reçus lors de leur consultation.

9.3.2 Définition de la population de recherche

La population de recherche a été définie en tant que les élèves du premier degré du secondaire ayant accès à internet sur n'importe quel appareil.

9.3.3 Interviews d'individus représentatifs de la population de recherche

La construction du questionnaire s'est ainsi basée sur les interviews préalables décrites en section *7.3.1 Personas* afin de déterminer quelles sont les conséquences perçus des comportements, les référents normatifs et les facteurs de contrôle spécifiques à la population de recherche.

9.3.4 Rédaction du questionnaire

La rédaction du questionnaire a suivi les recommandations de Icek Ajzen [43].

D'abord, 5 à 6 questions sont formulées afin de rencontrer les constructions principales de la théorie : l'attitude, la norme subjective, le contrôle perçu et l'intention. Ensuite, sur base des interviews réalisées décrites dans la section 7.3.1, le questionnaire est étendu, questionnant maintenant les conséquences, les référents et croyances normatives, les facteurs de contrôle, et les questions additionnelles, comme des questions démographiques ou relatives à l'axe sensibilité et connaissance dans ce cas-ci.

En plus des directives de Ajzen [43], le questionnaire a été inspiré de l'application de la théorie à d'autres études comme sur l'intention de boire et conduire [69].

La liste des questions posées est décrite dans le tableau suivant.

— b : axe comportement
— s : axe sensibilité
— k : connaissance
— d : mesure démographique
— a : autre
— A : attitude
— N : norme subjective
— P : contrôle perçu
— I : intention
— C : comportement passé
— 1 : conséquence élicitée du comportement
— 2 : référent normatif
— 3 : facteur de contrôle

QO question ouverte QR question orientée QA question alternative QF question fermée

n°	Question	type	sujet
1	Quel âge as-tu ? Par exemple, si tu as 12 ans, écris 12.	QR	d
2	De quel genre es-tu ?	QR	d
3	A quels appareils as-tu accès à la maison ? Coche ceux auxquels tu peux avoir accès	QA	d
4	As-tu accès à internet ?	QF	d
5	Peux-tu raconter une expérience qui t'a fait vraiment peur alors que tu étais sur ton smartphone ou un ordinateur (perte de fichier, perte d'informations, non fonctionnement, contact avec quelqu'un, ...)	QO	a
6	As-tu déjà participé à l'escape game sur la cybersécurité	QF	d
7	Peux-tu citer des risques liés à l'utilisation de l'ordinateur et d'internet ? Tu peux citer des mots si tu ne sais pas	QO	k
8	As-tu déjà fait des choses pour te protéger sur un ordinateur ou sur internet ? Tu peux citer des mots si tu ne sais pas.	QO	a
	Pour chaque activité, dis à quel point tu trouves ça important.	QA échelle 4	s
9	[Faire attention à mes mots de passe serait]		
10	[Faire des sauvegardes de sécurité de ce qu'il y a sur mon ordinateur serait]		
11	[Faire attention à ce que je mets en ligne serait]		
12	[Faire attention aux mails que je reçois serait]		
	Pour chaque activité, dis à quel point tu trouves ça facile ou difficile. Il n'existe pas de mauvaise réponse !	QA échelle 4	b A
13	[Faire attention à mes mots de passe serait]		
14	[Faire des sauvegardes de sécurité de ce qu'il y a sur mon ordinateur serait]		
15	[Faire attention à ce que je mets en ligne serait]		
16	[Faire attention aux mails que je reçois serait]		
17	Mettre en place ce qui a été cité (mots de passe, sauvegardes, posts, mails) serait, selon toi :	QA échelle 4	bA
	Dis, pour chaque ligne, à quel point tu es d'accord avec la phrase.	QA échelle 4	bN
18	[La plupart des gens importants pour moi trouve ça bien de faire attention à ses mots de passe]		
19	[La plupart des gens importants pour moi trouve que c'est bien de faire attention à ce que l'on poste en ligne		
20	[La plupart des gens importants pour moi trouve que c'est bien de faire des sauvegardes de sécurité]		
21	[La plupart des gens importants pour moi trouve que c'est bien de faire attention aux mails que l'on reçoit		
	Dis, pour chaque ligne, à quel point tu es d'accord avec la phrase.	QA échelle 4	bN
22	[La plupart des gens comme moi trouve ça bien de faire attention à ses mots de passe]		
23	[La plupart des gens comme moi trouve que c'est bien de faire attention à ce que l'on poste en ligne]		
24	[La plupart des gens comme moi trouve que c'est bien de faire des sauvegardes de sécurité]		
25	[La plupart des gens comme moi trouve que c'est bien de faire attention aux mails que l'on reçoit]		

	Dis, pour chaque ligne, à quel point tu es d'accord avec la phrase.	QA échelle 4	bP
26	[Je sais que je peux faire attention à mes mots de passe]		
27	[Je sais que je peux faire des sauvegardes de sécurité]		
28	[je sais que je peux faire attention aux mails que je reçois]		
29	[Je sais que je peux faire attention à ce que je poste en ligne]		
	Dis, pour chaque ligne, à quel point tu es d'accord avec la phras	QA échelle 4	bI
30	[Je compte faire attention à mes mots de passe]		
31	[Je compte faire des sauvegardes de sécurité]		
32	[Je compte faire attention aux mails que je reçois]		
33	[Je compte faire attention à ce que je poste en ligne]		
34	As-tu déjà fait des sauvegardes de fichiers pour les retrouver en cas de perte ? (Backup, time machine, disque dur, clé usb, ...)	QF	bC
35	Utilises-tu le même mot de passe pour plusieurs choses sur internet ?	QF	bC
36	Quelles informations as-tu, ou mettrais-tu sur ton profil d'un réseau social, en visible pour les autres ? Cela inclus tes posts et ce qui n'est pas directement lié à ton profil.	QA	bC
	Dis, pour chaque ligne, à quel point tu es d'accord avec la phrase.	QA échelle 4	b1
37	[Faire attention à son empreinte numérique permet d'éviter que mes informations soient divulgées]		
38	[Faire attention à ses mots de passe permet d'éviter que des gens l'obtiennent]		
39	[Faire des sauvegardes de sécurité me permet d'éviter de perdre des fichiers importants]		
40	[Faire attention aux mails que je reçois permet d'éviter d'attraper des virus sur l'ordinateur]		
	Dis, pour chaque ligne, à quel point tu es d'accord avec la phrase.	QA échelle 4	
41	[Mes parents pensent que je devrais faire attention à mes mots de passe, à ce que je poste en ligne, aux mails que je reçois et aux sauvegardes de sécurité]	QA échelle 4	b1
42	[Mes amis pensent que je devrais faire attention à mes mots de passe, à ce que je poste en ligne, aux mails que je reçois et aux sauvegardes de sécurité]	QA échelle 4	b1
43	[J'aimerais avoir conscience des risques que j'encours sur internet et sur l'ordinateur en général]	QA échelle 4	b3
44	[Avoir conscience des risques que j'encours me permettrait de faire attention à mes comportements sur l'ordinateur et internet.]	QA échelle 4	b3

45	Selon toi, qu'est-ce que le phishing ?	QO	k
46	Selon toi, qu'est-ce qu'un réseau social ?	QO	k
47	Selon toi, qu'est-ce que le chiffrement en informatique ?	QO	k
48	Selon toi, qu'est-ce qu'un expert en cybersécurité ?	QO	k
49	Selon toi, qu'est-ce que l'empreinte numérique sur internet ?	QO	k
50	Peux tu décrire une mauvaise pratique liée aux mots de passe ? Quelque chose qu'il ne faut surtout pas faire.	QO	k
51	Selon toi, quel est le mot de passe le plus fort ?	QA	k
52	Selon toi, quel est le mot de passe le plus faible ?	QA	k
53	Selon toi, ce mail est-il véritable ou est-ce un mail malveillant	QF	k

Etant donné que la théorie du comportement planifié ne donne pas de recommandations concernant l'ordre dans lequel les questions doivent être posées, celles-ci ont été proposées dans l'ordre dans lequel elles ont été construites afin de conserver la cohérence lorsque les élèves remplissent le questionnaire malgré la perception potentiellement biaisée du questionnaire.

Les échelles de Likert réduites à 4 points évitaient la neutralité lors des réponses. De plus, étant donné l'âge des participants, et malgré le support visuel de réponse, une échelle à 6 points pouvait nécessiter un effort plus élevé lors de la mémorisation nécessaire à la réponse.

9.4 Procédé d'évaluation

Initialement, l'évaluation devait se dérouler en classe. Des enseignants du secondaire ont accepté de soumettre leurs élèves au questionnaire avant et après l'activité à laquelle ils s'étaient inscrits. L'encadrement de cette étape de réponse au questionnaire ne pouvait donc pas être réalisé. Le déroulement de l'escape game, quant à lui, pouvait partiellement être encadré selon les enseignants inscrits à l'activité. Finalement, étant donné le contexte sanitaire et le passage au code rouge, aucun encadrement n'a été possible. Les réponses aux questionnaires avant et après l'activité ainsi que l'activité elle-même n'ont été encadré que par les enseignants, aidés par le manuel d'accompagnement.

9.5 Analyse des résultats

Le questionnaire étant constitué de questions ouvertes mais l'étude devant être quantitative car nous voulions des données concrètes permettant de tirer des conclusions, un travail d'analyse a été réalisé avant l'étude statistique.

Ainsi, les questions 7 et 36 ont d'abord été codées selon une échelle à 4 point afin de conserver la cohérence des échelles du questionnaire. Ceci a été réalisé en fonction du nombre de réponses données selon le quartile dans lequel il se trouvait.

Les questions 8, 34, 35, 45 à 53 ont été remplacées par des valeurs booléennes car il s'agissait de savoir si la réponse était correcte ou non, ou si le participant avait répondu positivement à une question ouverte.

Par exemple, à la question : "Selon toi, qu'est-ce que le chiffrement en informatique ?", la réponse "*raport avec le binnère (1 ou 0)*" a été considérée fausse avec une valeur de 1 sur l'échelle, tandis que "*c'est un code permettant de chiffrer des données privées que l'on ne veut pas partager, plusieurs sortes de chiffrement son possible, tels que le chiffrement césar, le ROT13 et bien d'autres*" a été considérée vraie avec une valeur de 4 sur l'échelle.

Ensuite, une analyse factorielle a permis d'obtenir des valeurs unidimensionnelles pour chaque axe analysé.

Les analyses statistiques ont été réalisées sur excel.

9.6 Biais potentiels sur l'évaluation de la sensibilisation

Le processus d'évaluation ainsi que son déroulement a pu générer plusieurs biais. En premier lieu, lors de l'analyse des résultats des participants, les réponses s'étant révélées être de la triche, c'est-à-dire des réponses trouvées sur internet pour les questions ouvertes ou des doublons dans le questionnaire avec pour seule différence la participation ou la non participation à l'activité n'ont pas été comptabilisés et ont été simplement écartés. L'analyse des questions ouvertes peut également avoir été orientée par le correcteur l'ayant réalisée.

Aussi, les statistiques ont été réalisées sur les résultats sans tri des questions selon un quelconque indice de cohérence interne. Sans forcément éviter un biais, un tri de ce genre aurait pu permettre des résultats plus parlants.

La taille des groupes, c'est-à-dire la population témoin n'ayant pas participé à l'activité était de 29 personnes tandis que seulement 20 personnes ont répondu au questionnaire après l'activité, il est tout-à-fait possible qu'un biais dû au déséquilibre d'effectif soit présent, et que la population ayant participé à l'étude soit trop petite pour que les résultats soient sérieux.

La plupart des questions ne proposait pas la possibilité de répondre "ne sais pas" ou "ne répond pas", ce qui est déconseillé lorsque l'on mesure des croyances ou des constructions cognitives telles que mesurées dans cette étude.

Il est également possible que la question 6 : "*As-tu déjà participé à l'escape game sur la cybersécurité ?*" ait induit une confusion selon leur participation à l'étude ou à l'activité.

Deux grands problèmes sont également à prendre en compte ; la plupart du temps, les participants ont dû répondre au questionnaire juste après la participation à l'escape game, donc en général moins d'une heure après y avoir déjà répondu la première fois. Il est à considérer que l'effort peut avoir été difficile ou

désagréable pour les participants, et peu soutenable. Aussi, la méthode d'évaluation recommande de laisser du temps entre deux réponses au questionnaire. Cela a d'ailleurs été confirmé dans les résultats obtenus que les participants ayant répondu la deuxième fois avec un minimum de deux jours depuis leur participation avaient un score général plus élevé.

Chapitre 10

Résultats

Ce chapitre présente les résultats de la recherche qui permettent de discuter de l'effet de l'exposition à l'outil de sensibilisation à la cybersécurité développé. Celui-ci est divisé en six parties afin d'aborder les indicateurs démographiques de nos résultats permettant d'en savoir plus sur la population ayant pris part à l'étude, puis d'aborder les effets sur chaque axe repris par l'étude, et ensuite, commentera les résultats et abordera des informations notables qui ont été trouvées dans les résultats.

10.1 Indicateurs démographiques

Le questionnaire a été répondu 49 fois par des élèves du secondaire âgés de 13 à 19 ans. Le nombre exact de personnes différentes est inconnu car une majorité des participants a répondu deux fois.

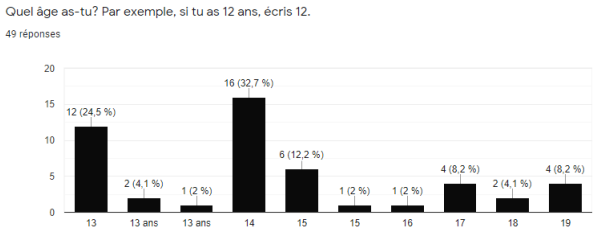

FIGURE 10.1 – Répartition de l'âge des participants

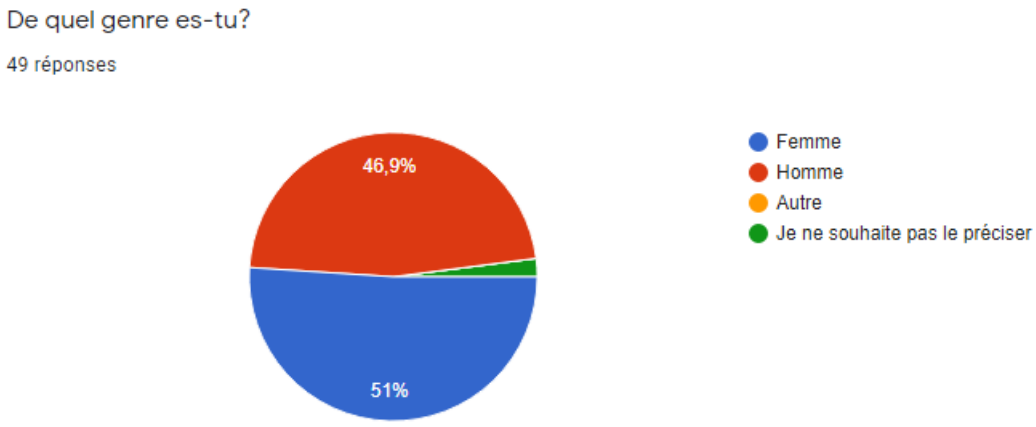

FIGURE 10.2 – Répartition des genre des participants

Parmi les participants, la répartition en fonction des genres était équilibrée avec 51% de femmes et 46,9% d'hommes.

La grande majorité (>90%) des participants ont quotidiennement accès à un smartphone et une télévision, et plus de 80% à un ordinateur. La totalité des participants a accès à internet chez elle.

10.2 Effets de l'activité sur la connaissance

En moyenne, les participants ont obtenu un score de 68,33% avec un minimum possible de 25% et un maximum de 100%.

A participé	Score de connaissance
Non	66.81%
Oui	70.66%
Moyenne	68.33%

On observe une différence de 3,85%, donc une augmentation positive du score moyen de connaissance. L'écart type du score des participants n'ayant pas suivi l'activité est légèrement plus bas (0.129) que celui de ceux qui l'ont suivie (0.142), il est donc possible que l'activité d'escape game ait eu plus d'effet sur certaines personnes, mais on peut en déduire une amélioration.

10.3 Effets de l'activité sur le comportement

Le comportement est l'axe ayant eu la plus légère amélioration dans le score (1,15), mais ayant eu le score moyen le plus élevé comme le montre le tableau suivant.

A participé	Score de comportement
Non	76.95%
Oui	78.10%
Moyenne	77.40%

Aussi, l'écart type pour chaque échantillon est très bas avec 0.08 pour les participants n'ayant pas suivi l'activité et 0.09 pour ceux l'ayant réalisée. Il semble donc que cet axe est le plus stable.

10.4 Effets de l'activité sur la sensibilité

L'axe de la sensibilité est celui ayant subit la plus grande différence de score comme l'indique le tableau suivant.

A participé	Score de sensibilité
Non	50.65%
Oui	78.29%
Moyenne	61.59%

Les deux échantillons ont des écarts-types similaires d'environ 0.11.

Le graphique suivant reprend tous les résultats énoncés ci-dessus.

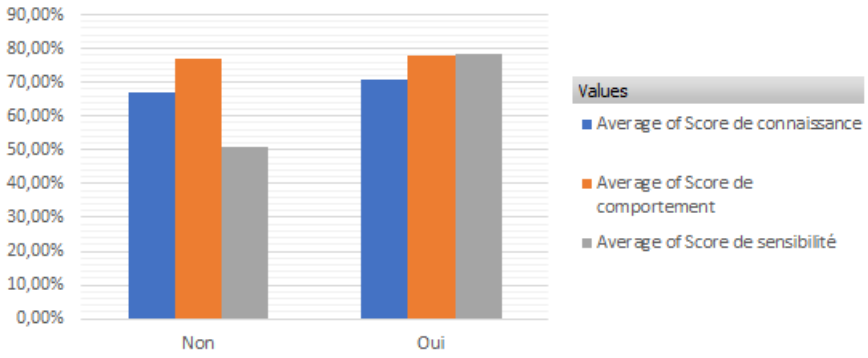

FIGURE 10.3 – Répartition des scores moyens pour chaque axe évalué

10.5 Analyse des résultats

L'activité de sensibilisation a eu une influence positive sur les trois axes évaluant la sensibilité des participants, et en particulier sur celui de la sensibilité. Cela peut s'expliquer par le fait que les participants ont ainsi été effectivement confronté aux cybermenaces durant l'activité, démontrant l'importance d'une cybersécurité efficace et sérieuse.

En revanche, l'axe des comportements, le plus stable selon les résultats, pourrait démontrer la difficulté de faire changer les comportements des individus, ou être symptomatique des erreurs qui ont été réalisée durant cette recherche. L'écart-type très bas pour les deux populations peut être questionné, car cette caractéristique démontre tout de même une tendance très affermie dans la population.

L'axe de connaissance a eu une amélioration moyenne parmi les trois axes. L'écart-type plus petit chez la population ayant participé à l'escape game est expliquée par le fait qu'un individu ayant déjà une certaine connaissance ne peut plus l'améliorer, car celle-ci est définie par une valeur binaire : sait ou ne sait pas.

10.6 Informations notables

Plusieurs sujets semblaient au coeur des préoccupations des participants n'ayant pas participé à l'activité. Ceux-ci sont ressortis dans les réponses aux questions ouvertes. Parmi leur préoccupations se trouvait principalement la peur de l'enlèvement et du catfishing [1]

L'activité semble aussi avoir généré du doute chez les participants, qui ne sont pas certains qu'un mail malveillant le soit après l'avoir suivie tandis que tous en sont certains avant de l'avoir réalisée.

Les scores pour l'axe de connaissance, et indépendamment de la participation ou non à l'activité, ont également une tendance à augmenter avec l'âge. Ce n'est pas le cas pour l'axe comportemental ou de sensibilité.

1. Le catfishing est une activité trompeuse par laquelle une personne crée un personnage fictif ou une fausse identité sur un réseau social, en ciblant généralement une victime spécifique, Wikipédia

Chapitre 11

Contributions, limites et perspectives

11.1 Les contributions de la recherche

La présente recherche a permis d'observer l'application de la théorie du comportement planifié [39] alliée aux trois axes de la méthode proposée par wavestone [37]. Cette contribution pourrait permettre d'ouvrir la voie à son utilisation non éprouvée mais déjà considérée dans la littérature.

La campagne réalisée dans le cadre de cette étude a également permis d'améliorer la sensibilité des participants à la cybersécurité.

Par ailleurs, l'étude a surtout mis en évidence la nécessité de prendre en compte un grand nombre de facteurs liés au domaine de la cybersécurité dans le cadre de campagnes de sensibilisation et dans l'utilisation de la gamification par l'escape game.

11.2 Les limites de la recherche

Bien que les résultats de la recherche soient positifs, leur validité peut être remise en question. En plus des erreurs potentielles déjà énoncées, la mise en oeuvre a été laborieuse et soumise à de grands changements liés au contexte sanitaire.

Aussi, il a été mis en évidence que l'outil pédagogique était plus adapté à un public de fin de secondaire plutôt que du premier degré comme prévu initialement. La quantité d'informations a semblé être trop élevée également, car des confusions parmi les concepts ont été observées. La compréhensibilité de la campagne résidait aussi dans la compréhensibilité de ces solutions. Ce facteur étant complexe à aborder, il est à noter qu'il aurait pu être mieux réalisé.

Le fait que l'activité ait été proposée par un professeur et non une personne ayant autorité dans le domaine de la cybersécurité a aussi pu réduire l'impact de la campagne, de même que le manque de compétition entre les participants en raison de l'encadrement réalisé par un professeur qui n'a pas pu être contrôlé ou observé.

Afin de s'ancrer plus profondément dans l'actualité, la question de la santé et de la désinformation aurait pu être abordées dans la campagne. Aussi, des canaux secondaires, en complément de l'activité auraient pu être développés pour renforcer l'effet de la sensibilisation.

11.3 Les perspectives

Une adaptation de l'outil au public permettrait d'obtenir une difficulté plus adéquate ainsi que l'ajout d'une temporalité dans l'escape game qui semble être un facteur important dans une gamification par escape game et qui n'a pas été introduite dans l'outil [70].

Les données récoltées pourraient en outre permettre d'observer les facteurs significatifs dans l'évaluation de la sensibilisation au domaine de la cybersécurité.

Chapitre 12

Conclusion

A l'issue de cette recherche, nous pouvons déterminer l'influence positive de la campagne de sensibilisation à la cybersécurité effectuée via un escape game thématique. Selon les scores obtenus, la sensibilité à ce sujet a été la plus influencée par l'approche adoptée. Par ailleurs, il convient de rappeler que seuls certains sujets ont été abordés par cette campagne.

Pour réaliser celle-ci, nous avons commencé par réaliser une analyse de la littérature sur le sujet afin de déterminer l'avancement dans le domaine de la sensibilisation à la cybersécurité, les facteurs déterminants dans la création d'un outil et d'une campagne associée ainsi que les pistes de méthodologie pour réaliser l'évaluation d'un outil.

Ainsi, les contributions ont été :

— L'utilisation d'une méthodologie mixte basée sur les propositions récentes de la littérature dans le domaine

— La création d'un outil de sensibilisation à la cybersécurité pour le secondaire, d'un manuel associé et d'une vidéo de présentation pour son installation

— La gamification par un escape game de différents sujets liés à la cybersécurité

— La mise en évidence de facteurs critiques à prendre en compte dans la méthodologie adoptée

Enfin, il a été clairement exposé que des ajustements dans le design et la méthodologie permettraient d'obtenir des résultats démontrant l'intérêt de l'outil dans la sensibilisation au domaine de la cybersécurité.

Bibliographie

[1] D. Craigen, N. Diakun-Thibault et R. Purse, « Defining cybersecurity, » *Technology Innovation Management Review*, t. 4, n° 10, 2014.

[2] ANSSI. (2014). « Méthode de classification et mesures principales, » adresse : https://www.ssi.gouv.fr/uploads/IMG/pdf/securite_industrielle_GT_methode_classification-principales_mesures.pdf (visité le 10/10/2020).

[3] L. Paoli, E. V. Hellemont, C. Verstraete, J. Visschers, K. Leuven, R. D. Wolf, M. Martens, L. D. Marez et P. Verdegem, « Belgian Cost of Cybercrime : Measuring cost and impact of cybercrime in Belgium. (English), » *Annalen der Physik*, t. 322, p. 891-921, 2017.

[4] P. fédérale. (2020). « Statistiques de criminalité 2019 : nouvelle hausse marquée de la cybercriminalité, le total reste stable, » adresse : https://www.police.be/5998/fr/actualites/statistiques-de-criminalite-2019-nouvelle-hausse-marquee-de-la-cybercriminalite-le-total (visité le 20/06/2021).

[5] INTERPOL. (2020). « INTERPOL report shows alarming rate of cyberattacks during COVID-19, » adresse : https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (visité le 23/06/2021).

[6] T. McMullan. (2015). « The world's first hack : the telegraph and the invention of privacy, » (visité le 17/06/2021).

[7] S. Hong, *Wireless : From Marconi's Black-Box to the Audion*. MIT Press, 2019.

[8] P. R. Masani, *Norbert Wiener*. Birkhäuser, 2012.

[9] G. Dalakov. (2021). « The first computer virus of Bob Thomas, » adresse : https://history-computer.com/the-first-computer-virus-of-bob-thomas-complete-history/ (visité le 18/06/2021).

[10] Thales. (2019). « Arrête-moi si tu peux : histoire de la cybersécurité, » (visité le 27/04/2021).

[11] J. S. Cunningham. (2016). « Interview with Ray Tomlinson on Creeper/Reaper, » (visité le 06/05/2021).

[12] C. Witchalls. (2018). « 30 years ago, the world's first cyberattack set the stage for modern cybersecurity challenges, » (visité le 02/07/2021).

[13] M. James. (2016). « A history of ethical hacking, » (visité le 16/04/2021).

[14] A. B. Association, *ABA Journal*. American Bar Association, 1999, p. 108.

[15] R. A. Hudson, *The ILOVEYOU Virus and Its Impact on the U.S. Financial Services Industry*. U.S. Government Printing Office, 2000, p. 48.

[16] G. Coleman, *Hacker, Hoaxer, Whistleblower, Spy : The Many Faces of Anonymous*. Verso Books, 2014, p. 256.

[17] OTAN. (2013). « Les cyberattaques - repères chronologiques, » adresse : `https://www.nato.int/docu/review/2013/Cyber/timeline/FR/index.htm` (visité le 16/05/2021).

[18] S. Shane et A. W. Lehren, « Leaked Cables Offer Raw Look at U.S. Diplomacy, » *The New York Times*, p. 1-1, 2010.

[19] FEDIL. (2020). « CYBERSECURITY CHECKLIST, » adresse : `https://www.fedil.lu/fr/publications/cybersecurity-checklist/` (visité le 12/06/2021).

[20] C. européen. (2021). « Cybersécurité : comment l'UE lutte contre les cybermenaces, » adresse : `https://www.consilium.europa.eu/fr/policies/cybersecurity/` (visité le 17/06/2021).

[21] ——, (2020). « Cybersecurity Policies, » adresse : `https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies` (visité le 08/04/2021).

[22] E. Commission. (2021). « Overview of funding programmes, » adresse : `https://ec.europa.eu/info/overview-funding-programmes_en` (visité le 16/05/2021).

[23] F. Fanuël, *Quelles armes pour faire face aux cyber-attaques ?* Centre Jean Gol, 2019, p. 1-20.

[24] H. Feuillien, R. Herzeele et J. Araoud, « Vers un plan régional de cybersécurité, » *Bruxelles Prévention Sécurité*, p. 1-60, 2017.

[25] C. Ponsard, J. Grandclaudon et S. Bal, *Survey and Lessons Learned on Raising SME Awareness about Cybersecurity*. Prague, Czech Republic : SCITEPRESS - Science et Technology Publications, 2019, p. 558-563.

[26] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas et G. Giannakopoulos, « The Human Factor of Information Security : Unintentional Damage Perspective, » *Procedia - Social and Behavioral Sciences*, p. 5, 2014.

[27] P. Kearney, *Security : The Human Factor*. IT Governance, 2010.

[28] D. Ki-Aries et S. Faily, « Persona-centred information security awareness, » *Computers & Security*, t. 70, p. 663-674, 2017.

[29] E. S. Forum, « Implementation Guide : How to make your organization aware of IT Security, » *European Security Forum, London*, 1993.

[30] D. LETURCQ, « Circulaire n°4777 du 17/03/2014, » *Fédération Wallonie-Bruxelles*, p. 1-57, 2014.

[31] F. W.-B. /. M. /. A. générale de l'Enseignement. (2021). « Référentiel de formation manuelle, technique, technologique et numérique, » adresse : http://www.ares-ac.be/images/FIE/Referentiels/Referentiel-FMTTN.pdf (visité le 03/05/2021).

[32] H. Maquet. (2017). « Les élèves de primaire vont-ils apprendre le codage informatique ? » Adresse : https://www.rtbf.be/info/medias/detail_les-eleves-de-primaire-vont-ils-apprendre-le-codage-informatique?id=9780674 (visité le 23/06/2021).

[33] N. Badie et A. Habibi Lashkari, « A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP, » *Journal of Basic and Applied Scientific Research, 2, 9, 9331-9347.*, t. 2, jan. 2012.

[34] A. R. Ahlan, M. Lubis et A. R. Lubis, « Information security awareness at the knowledge-based institution : its antecedents and measures, » *Procedia Computer Science*, t. 72, p. 361-373, 2015.

[35] L. González-Manzano et J. M. de Fuentes, « Design recommendations for online cybersecurity courses, » *Computers Security*, t. 80, p. 238-256, 2019.

[36] F. Tilman. (2005). « Information – sensibilisation – conscientisation Quelle communication pour l'émancipation ? » Adresse : http://www.legrainasbl.org/index.php?option=com_content&view=article&id=117:information-sensibilisation-conscientisation-quelle-communication-pour-lemancipation-&catid=54:analyses (visité le 03/05/2021).

[37] Hapsis. (). « Comment mesurer l'impact des campagnes de sensibilisation ? » Adresse : https://www.riskinsight-wavestone.com/2015/06/comment-mesurer-limpact-des-campagnes-de-sensibilisation/ (visité le 18/04/2021).

[38] ——, (2015). « Comment mesurer les impacts des campagne de sensibilisation, » adresse : https://www.riskinsight-wavestone.com/2015/06/comment-mesurer-limpact-des-campagnes-de-sensibilisation/ (visité le 26/03/2021).

[39] I. Ajzen, « From Intentions to Actions : A Theory of Planned Behavior, » p. 11-39, 1985.

[40] *Théorie du comportement planifié*, fr, Page Version ID : 177414645, déc. 2020. adresse : https://fr.wikipedia.org/w/index.php?title=Th%5C%C3%5C%A9orie_du_comportement_planifi%5C%C3%5C%A9&oldid=177414645%5C%7D (visité le 17/08/2021).

[41] BOITMOBILE, *Echelle de Likert - Définitions Marketing » L'encyclopédie illustrée du marketing*, FR. adresse : https://www.definitions-marketing.com/definition/echelle-de-likert/%5C%7D (visité le 17/08/2021).

[42] I. Ajzen et M. Fishbein, « A Bayesian analysis of attribution processes, » *Psychological Bulletin*, t. 82, p. 261-277, 1975.

[43] I. Ajzen, « Constructing a theory of planned behavior questionnaire, » p. 1-7, 2006.

[44] J. Cestac et T. Meyer, *Des attitudes à la prédiction du comportement : le modèle du comportement planifié*, P. Morchain et A. Somat, éd., sér. Psychologies. Rennes : Presses universitaires de Rennes, mai 2019, p. 55-86, Code : La psychologie sociale : applicabilité et applications, isbn : 978-2-7535-6412-1.

[45] T. Sommestad et J. Hallberg, *A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance*. juil. 2013, t. 405, p. 257-271.

[46] T. Teo et C. Beng Lee, « Explaining the intention to use technology among student teachers : An application of the Theory of Planned Behavior (TPB), » *Campus-Wide Information Systems*, t. 27, p. 60-67, 2010.

[47] W. Hardeman, M. Johnston, D. Johnston, D. Bonetti, N. Wareham et A. L. Kinmonth, « Application of the Theory of Planned Behaviour in Behaviour Change Interventions : A Systematic Review, » *Psychology & Health*, t. 17, p. 123-158, 2002.

[48] M. Beyer, S. Ahmed, K. Doerlemann, S. Arnell, S. Parkin et A. S. et al., « Awareness is only the first step : A framework for progressive engagement of staff in cyber security, techreport, » *Hewlett Packard Enterprise*, p. 1-12, 2015.

[49] S. Manke et I. Winkler, « The Habits of Highly Successful Security Awareness Programs : A Cross-Company Comparison, » *secure mentem*, p. 33, 2012.

[50] (). « Les 9 facteurs d'influence en sensibilisation à la cybersécurité, » adresse : `https://terranovasecurity.com/fr/9-elements-qui-influencent-le-facteur-humain/`.

[51] E. Kritzinger, M. Bada et J. R. C. Nurse, *A Study into the Cybersecurity Awareness Initiatives for School Learners in South Africa and the UK*, M. Bishop, L. Futcher, N. Miloslavskaya et M. Theocharidou, éd. Cham : Springer International Publishing, 2017, p. 110-120.

[52] P. Rowland et C. B. Noteboom, « Adolescent Girls' Influencers in Cybersecurity Education and Activities, » *MWAIS 2019 Proceedings*, p. 7, 2019.

[53] P. Rowland, « The CybHER Program supported by CISSE Framework to Engage and Anchor Middle-school Girls in Cybersecurity and Anchor Middle-school Girls in Cybersecurity, » *Dakota State University*, p. 1-83, 2018.

[54] I. Corradini et E. Nardelli, *Developing Digital Awareness at School : A Fundamental Step for Cybersecurity Education*, I. Corradini, E. Nardelli et T. Ahram, éd., sér. Advances in Intelligent Systems and Computing. Cham : Springer International Publishing, 2020, p. 102-110.

[55] J. Sánchez, A. Mallorquí, A. Briones, A. Zaballos et G. Corral, « An Integral Pedagogical Strategy for Teaching and Learning IoT Cybersecurity, » *Sensors*, t. 20, p. 3970, jan. 2020.

[56] C. J. Cornel, D. C. Rowe et C. M. Cornel, « Starships and Cybersecurity : Teaching Security Concepts through Immersive Gaming Experiences, » p. 27-32, 2017.

[57] M. Adams et M. Makramalla, « Cybersecurity Skills Training : An Attacker-Centric Gamified Approach, » *Technology Innovation Management Review*, t. 5, p. 5-14, 2015.

[58] G. Jin, M. Tu, T.-H. Kim, J. Heffron et J. White, « Evaluation of Game-Based Learning in Cybersecurity Education for High School Students, » *Journal of Education and Learning (EduLearn)*, t. 12, p. 150, 1er fév. 2018.

[59] Netsblox. (2019). « Cybersecurity Education with RoboScape, » adresse : `https://netsblox.org/cybersecurity` (visité le 20/05/2021).

[60] R. Prieur. (2015). « Tout savoir sur l'escape game, » adresse : `https://www.escapegame.fr/quest-ce-quun-escape-game/` (visité le 04/03/2021).

[61] S. Fouché et A. H. Mangle, *Code hunt as platform for gamification of cybersecurity training*, sér. CHESE 2015. New York, NY, USA : Association for Computing Machinery, 14 juil. 2015, p. 9-11.

[62] L. González-Manzano et J. M. de Fuentes, « Design recommendations for online cybersecurity courses, » *Computers Security*, t. 80, p. 238-256, 1er jan. 2019.

[63] (). « Quelles sont les 6 cyberattaques les plus courantes ? » fr-BE, adresse : `https://allianz.be/fr/particuliers/blog/quelles-sont-les-6-cyberattaques-les-plus-courantes.html` (visité le 17/08/2021).

[64] (2021). « Étude sur les jeunes et les réseaux sociaux : 72 % des 16-18 ans n'utilisent pas Facebook, » adresse : `https://www.blogdumoderateur.com/etude-jeunes-reseaux-sociaux/` (visité le 03/05/2021).

[65] *Tweet bpost*, fr. adresse : `https://twitter.com/bpost_fr/status/1255157698603159553` (visité le 17/08/2021).

[66] M. Baudier et I. Nathalie. (). « Escape Game Pedagogique Ludicio (SU2IP), » adresse : `https://www.calameo.com/read/00014017315e91f927694?page=9` (visité le 17/08/2021).

[67] V. Lombardi, S. Ortiz, J. Phifer, T. Cerny et D. Shin, *Behavior Control-Based Approach to Influencing User's Cybersecurity Actions Using Mobile News App*, sér. SAC '21. Virtual Event, Republic of Korea : Association for Computing Machinery, 2021, p. 912-915.

[68] Y. Hong et S. Furnell, « Understanding cybersecurity behavioral habits : Insights from situational support, » *Journal of Information Security and Applications*, t. 57, p. 102 710, 2021.

[69] D. C. Chan, A. M. Wu et E. P. Hung, « Invulnerability and the intention to drink and drive : An application of the theory of planned behavior, » *Accident Analysis Prevention*, t. 42, p. 1549-1555, 2010.

[70] M. Baudier et I. Nathalie. (). « Escape Game Pedagogique Ludicio (SU2IP), » adresse : `https://www.calameo.com/read/00014017315e91f927694?page=9` (visité le 17/08/2021).