”Stop Hackers”, un jeu de rôle pour éduquer les enfants à la cybersécurité de manière critique

Julie Henry, Alyson Hernalesteen, Anne-Sophie Collard

“Stop Hackers”, un jeu de rôle pour éduquer les enfants à la cybersécurité de manière critique*

Henry, Julie[0000−0003−4354−9848], Hernalesteen, Alyson, and Collard, Anne-Sophie[0000−0003−3457−6908]

Namur Digital Institute (NADI), Université de Namur, Belgique
prénom.nom@unamur.be

Abstract. Le jeu de rôles “Stop Hackers” a pour objectif d'éduquer les enfants de 10-14 ans à la cybersécurité. Basé sur un modèle théorique d'éducation au numérique critique et citoyenne, ce dispositif questionne l'intention humaine derrière une cyberattaque, les conditions de son succès, ainsi que la valeur des données visées. D'une part, il s'agit de réfléchir à la forme d'une éducation à la cybersécurité qui entraînerait un changement de représentation de ce concept informatique et un questionnement critique chez les jeunes. D'autre part, il s'agit de déterminer si les enseignants se sentent capables de mettre en œuvre une telle éducation critique, au-delà des aspects techniques. “Stop Hackers” a été conçu à partir d'une démarche de type recherche orientée par la conception. Des données ont été collectées lors des phases d'expérimentation, par observations et via des interviews, auprès de quatre enseignants et 107 élèves. Les résultats obtenus montrent : 1) que les enseignants sont en mesure de mettre en place le dispositif au sein de leur classe, 2) que le dispositif permet d'atteindre, partiellement, les objectifs d'apprentissage, et 3) que la contextualisation et l'expérience de jeu peuvent servir de base à un questionnement critique.

Keywords: Éducation au numérique · Éducation aux médias · Enseignement de l'informatique · Activité débranchée

Si les jeunes utilisent, de plus en plus tôt, Internet et ses outils de communication (médias sociaux, jeux en ligne, courrier électronique et messagerie instantanée), il est interpellant de constater qu'un grand nombre d'entre eux n'ont jamais entendu parler du phishing et de ses dérivés[1].

Prendre conscience des risques auxquels ils sont exposés sur Internet est une étape importante pour que les jeunes naviguent en toute sécurité et comprennent les différentes cyber-menaces auxquels ils pourraient être confrontés. Cela peut se faire à travers des campagnes de sensibilisation et des initiatives ponctuelles, mais la solution la plus efficace pour toucher un maximum de jeunes reste d'organiser une éducation à la cybersécurité à l'école.

* Supported by organization x.

[1] 30% des jeunes Belges, selon le rapport de Febelfin (2021). There is plenty of ‘phish’ in the sea., consulté en ligne le 23/12/2021

Cette recherche vise à développer un dispositif éducatif pour les 10-14 ans croisant l'enseignement de l'informatique et l'éducation aux médias (EAM) et questionnant l'intention humaine derrière une cyberattaque, les conditions de son succès, ainsi que la valeur des données visées. D'une part, il s'agit de réfléchir à la forme d'une éducation à la cybersécurité qui entraînerait un changement de représentation de ce concept informatique et un questionnement critique chez les jeunes. D'autre part, il s'agit de déterminer si les enseignants se sentent capables de mettre en œuvre une telle éducation critique, au-delà des aspects techniques.

Les principaux apports de cet article sont :

- la validation d'un modèle théorique d'éducation citoyenne critique à la technologie qui intègre les approches de l'enseignement de l'informatique, ici dans le domaine de la cybersécurité, et de l'EAM [X,X] ;
- la conception d'un dispositif éducatif questionnant l'intention humaine à l'origine d'une cyberattaque, les conditions de son succès, ainsi que la valeur des données visées, et pouvant être mis en place par un enseignant ;
- la formulation de pistes pour d'autres concepteurs et chercheurs afin de créer des activités éducatives critiques en cybersécurité pour les enfants, s'appuyant sur l'analyse des données préliminaires recueillies.

1 L'éducation à la cybersécurité : intérêt et défis

Accélérée par la crise du covid, la numérisation de la vie quotidienne se poursuit et augmente les cyber-risques. Une éducation à la cybersécurité apparait, dès lors, essentielle pour faire prendre conscience aux jeunes internautes de leur vulnérabilité lorsqu'ils utilisent des médias sociaux (en opposition à leur sentiment d'invincibilité [19]), mais aussi leur apprendre à prévenir certaines cyberattaques [1]. En outre, il apparait que cette éducation devrait se faire dès le plus jeune âge. En effet, les enfants ne sachant pas encore lire ni écrire, couraient un risque beaucoup plus élevé que leurs aînés face aux menaces et aux dangers du cyberespace parce qu'ils ne possèdent pas les connaissances pour se protéger [22]. L'intérêt pour une telle éducation est partagé par les enseignants, conscients que leurs élèves doivent être préparés à identifier les risques qu'ils encourent lorsqu'ils utilisent les technologies numériques [4].

Si l'aspect essentiel d'une éducation à la cybersécurité n'est donc plus à discuter, sa mise en œuvre rencontre plusieurs défis : le manque de compétences des enseignants et l'insuffisance de ressources pour les soutenir, mais aussi un manque de diversité dans le choix des thèmes à aborder.

Si, de façon générale, les enseignants ont la volonté d'enseigner la cybersécurité, ils déclarent ne pas avoir les connaissances suffisantes pour le faire. Le manque de ressources et de soutien pour les y aider ne favorise pas la mise en place d'une telle éducation [4,16,19] : très peu de ressources s'adressent aux jeunes enfants [22], les approches proposées manquent de rigueur dans l'évaluation de leurs effets [18] et n'ont pas toujours le succès escompté [12,13,10,9].

Concernant les thèmes composant cette éducation, cyberintimidation, protection des données personnelles et fiabilité des informations sur les médias sociaux sont ceux qui sont les plus couramment évoqués par les enseignants [4]. Ces thèmes sont également parmi les plus étudiés au niveau de la recherche [18], avec la vie privée et les données personnelles, les problèmes des cyberprédateurs utilisant les médias sociaux et les jeux, les sextos [11,15,25,8], ainsi que le phishing (reconnaissance d'un e-mail frauduleux) [9]. Les compétences plus techniques, telles que le maintien de la sécurité des comptes (gestion des mots de passe et craquage de ceux-ci), des logiciels et des appareils (mises à jour), d'un réseau, ou encore la connaissance des techniques possibles de cyberattaque, sont peu présentes [7,15] ou réalisées par des experts [14].

2 Un modèle théorique d'éducation au numérique critique et citoyenne

Compte tenu de l'âge des élèves, Corradini et Nardelli trouvent excessif de parler d'éducation à la cybersécurité à l'école primaire et secondaire. Pour eux, il s'agit avant tout de conscience numérique (*digital awareness*) : apprendre aux élèves à comprendre le concept de risque numérique et souligner l'importance du comportement en ligne [4]. Cela passe, selon eux par l'apprentissage d'une utilisation responsable des technologies numériques.

Cette vision s'inscrit dans dans une approche de l'éducation au numérique qui vise les compétences permettant d'utiliser, de comprendre et d'évaluer les technologies [23,24]. Avec le développement de technologies complexes, dont le fonctionnement devient de plus en plus opaque pour le grand public, la compréhension des aspects techniques est un enjeu fondamental. Cette dimension technique est prise en charge, au niveau de l'éducation, par l'enseignement de l'informatique qui soutient l'acquisition de compétences suffisamment avancées pour comprendre les concepts fondamentaux et identifier les logiques de ces technologies [5].

Cependant, enseigner les aspects techniques ne suffit pas pour amener les usagers à questionner la place des technologies dans la société et la manière dont elles s'inscrivent dans des pratiques qu'elles façonnent en même temps. Faire appel aux cadres de l'EAM permet d'envisager une éducation aux technologies qui soit critique par rapport aux problématiques éthiques et sociétales, et réflexive par rapport aux pratiques de chacun. C'est une approche qui envisage les risques mais aussi les opportunités que représente l'évolution du numérique dans la société. Concernant la cybersécurité, il ne s'agit donc pas seulement d'alerter sur les problèmes liés aux attaques mais aussi d'envisager de continuer à utiliser les technologiques numériques tout en étant conscient des risques. L'EAM vise en effet à développer les compétences nécessaires pour être critique, créatif, autonome et socialisé dans l'environnement médiatique contemporain, en prenant en compte la dimension technique des médias numériques mais également leurs dimensions informationnelle (sémiotique) et sociale (pragmatique) [6].

Pour répondre aux exigences de la formation de citoyens critiques et autonomes en cybersécurité, le modèle théorique sur lequel nous nous appuyons croise les perspectives de l'enseignement de l'informatique et de l'EAM [X]. Il s'inscrit dans la proposition d'une éducation critique à la technologie formulée par Saariketo [20,21], qui vise à prendre en compte de manière réflexive le rôle de la technologie dans la société et la vie quotidienne. Il s'agit donc non seulement de soutenir une compréhension des aspects de la cybersécurité au niveau de son fonctionnement informatique réel et actuel, mais aussi d'en développer une compréhension qui s'inscrit dans un contexte d'usage des technologies numériques, mettant en jeu des intérêts et des intentions humaines, prenant place au sein de relations sociales et s'inscrivant dans la compréhension que nous pouvons avoir d'une situation. En d'autres termes, cela consiste à ouvrir la "boîte noire" pour saisir les failles et les stratégies mises au point techniquement, mais aussi à la "déplier" dans un contexte médiatique et social pour mettre au jour la manière dont est envisagée la sécurité numérique en tant que construction sociale. Cette approche intégrée permet de développer une réflexivité (1) sur notre compréhension technique de la cybersécurité et des risques dans lesquels nos usages évoluent, et (2) sur le rôle du contexte médiatique et social dans lequel elle prend place, au sein duquel s'entremêlent les risques et les opportunités liés à nos usages des technologies numériques.

3 Méthodologie de recherche

S'appuyant sur ce modèle théorique de l'éducation au numérique critique et citoyenne, la recherche mise en place vise, d'une part, à concevoir une activité d'éducation à la cybersécurité pour les 10-14 ans et, d'autre part, à répondre aux deux questions suivantes :

- L'activité "Stop Hackers" est-elle réalisable en classe par un enseignant ? Est-ce que le dispositif fonctionne tant que jeu éducatif ? Comment les enseignants se l'approprient-ils ?
- L'activité permet-elle de remplir ses objectifs éducatifs ? Quels sont les apprentissages développés par les élèves, au niveau technique et au niveau critique ?

Après avoir expliqué le contexte et la démarche de recherche, nous présentons le dispositif éducatif "Stop Hackers" puis la méthode de collecte et d'analyse des données.

3.1 Contexte

Le dispositif "Stop Hackers" accompagne la mise en œuvre d'une réforme de l'enseignement en Belgique francophone[2] et vise à outiller les enseignants pour la mise en place d'un nouveau référentiel de compétences incluant une éducation

[2] Le Pacte pour un Enseignement d'Excellence, consulté le 11 janvier 2022.

au numérique, le référentiel “Formation Manuelle Technique, Technologique et Numérique” (FMTTN)[3]. En ce qui concerne l'éducation à la cybersécurité, le référentiel FMTTN annonce deux compétences à développer chez les enfants de 11 à 13 ans (élèves de 6e primaire et de début de secondaire) : “adopter un comportement responsable face à des situations de cyberattaque” et “réagir de manière responsable face aux risques de cyberattaque”. Les savoirs associés à ces compétences consistent principalement en du vocabulaire, utilisé de façon adéquate et en contexte (hameçonnage, virus, routeur, pirates, attaque en ligne, etc.). Les savoir-faire énoncés sont “reconnaitre des situations de cyberattaque” et “proposer et mettre en place des pistes d'actions pour faire face à des situations de cyberattaque”.

3.2 Une recherche orientée par la conception

Le dispositif “Stop Hackers” a été développé selon une approche de type recherche orientée par la conception (RoC) [2,3]. Cette approche consiste à mener un processus itératif qui articule des phases de conception, d'expérimentation dans différents contextes (dans le cas de cette étude, dans des écoles mais également dans d'autres contextes d'éducation non formelle), et d'analyse des données collectées durant ces expérimentations en vue d'améliorer le dispositif. Dans le cadre de cette recherche, la phase de conception repose sur une collaboration entre les chercheurs, les praticiens (enseignants) et des experts en cybersécurité (l'expertise en EAM est déjà représentée au sein de l'équipe de recherche) [3]. Elle est structurée en quatre étapes, les trois dernières étant itératives et suivant un processus de “recherche par les erreurs” [2] :

- les chercheurs **s'approprient** le sujet à partir de ressources validées par les experts ;
- ils **prennent du recul** par rapport à la connaissance experte et sélectionnent les concepts pertinents à aborder suivant le modèle théorique suivi (Section 2) et les compétences numériques visées (Section 3.1) ; il s'agit plus précisément de développer une connaissance des attaques possibles et de pouvoir identifier le rôle du contexte social dans la compréhension des risques liés à ces attaques ;
- les chercheurs **définissent la séquence** de l'activité qu'ils soumettent ensuite aux experts pour une première validation ;
- ils **créent du matériel pédagogique**.

L'activité est **séquencée** en trois temps : la contextualisation, l'expérience de jeu et le débriefing. La **contextualisation** part des représentations des enfants et de leurs pratiques médiatiques. Ensuite, à la manière d'un jeu de rôles, les enfants vivent une **expérience** tangible dans une situation définie. Enfin, le **débriefing** consiste en un retour sur le contexte, sur les représentations initiales et sur l'expérience de jeu. Il s'agit aussi d'élargir le questionnement à des problématiques sociétales contemporaines.

[3] Le référentiel FMTTN, version provisoire consultée le 11 janvier 2022

Les données collectées au fur et à mesure des expérimentations menées avec les enseignants permettent de consolider l'activité ainsi que le matériel éducatif **créé**, y compris la documentation pour les aider à mettre en œuvre l'activité au niveau pédagogique, didactique ou organisationnel. Cette approche a déjà été éprouvée dans une autre recherche visant le développement de dispositifs d'éducation critique au numérique [X] : un dispositif éduquant à l'intelligence artificielle [X,X].

3.3 Le dispositif "Stop Hackers"

"Stop Hackers" est un jeu de rôle débranché, inspiré du jeu "Les loups-garous de Thiercelieux". Ce dispositif vise à faire prendre conscience aux élèves que :

- Il existe différentes menaces sur Internet.
- Ces menaces sont mises en oeuvre par des personnes (et non des machines) qui ont des intentions.
- Les données volées ou endommagées ont une certaine valeur.
- Pour que ces menaces réussissent et deviennent des cyberattaques, il faut des conditions et un contexte social qui les rendent plausibles. Dans le cas contraire, elles échoueront.

Le temps de **contextualisation** de l'activité se réfère aux pratiques médiatiques de partage d'informations, en particulier sur les réseaux sociaux et via les applications de communication. La consigne donnée pour le temps du jeu est de partager le plus d'informations avec ses amis, afin que les cyberattaques s'inscrivent dans des pratiques et un contexte social familiers aux enfants.

Lors du jeu (**expérience**), les élèves sont répartis en groupes de 6 à 10 joueurs. Trois rôles sont disponibles : les amis, les pirates et les routeurs. Chaque groupe doit être composé des trois rôles, dans des proportions définies : de 3 à 5 amis, de 2 à 3 pirates et de 1 à 2 routeurs. Au sein d'un même groupe, amis et pirates s'affrontent.

Les amis ont pour mission de s'envoyer des messages et du contenu (photos et vidéos à visionner, contenu à télécharger). Chaque ami a une personnalité (six disponibles : Alice, Bob, Carole, David, Greg et Fanny) et un lot de cartes "messages" à sa disposition(cfr Figure 1) et un plateau pour les disposer (cfr Figure 2). Chaque ami est représenté par une couleur que l'on retrouve également en bordure de ses cartes : par exemple, Bob est "rouge" et Alice, "violet". Pour chaque message reçu, un ami doit décider s'il souhaite en consulter le contenu (à savoir le déposer sur son plateau, d'après la pré-visualisation sur la carte) ou le jeter. Dans les deux cas, il lui est demandé de justifier par écrit sa décision. Chaque contenu consulté (c'est-à-dire visionné ou téléchargé) permet de gagner un point au groupe d'amis à condition qu'il soit sécurisé, sinon il en fait perdre. Les amis ne découvrent qu'en fin de partie les contenus qui n'étaient pas sécurisés.

Les routeurs sont neutres. Chaque groupe en possède au moins un. Ils sont les maîtres du temps dans le jeu : ils gèrent les tours d'échanges de messages entre amis. À chaque tour, le routeur collecte les messages des amis de son groupe,

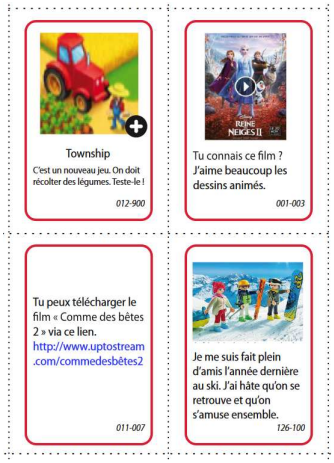

Fig. 1. Cartes “messages” de Bob

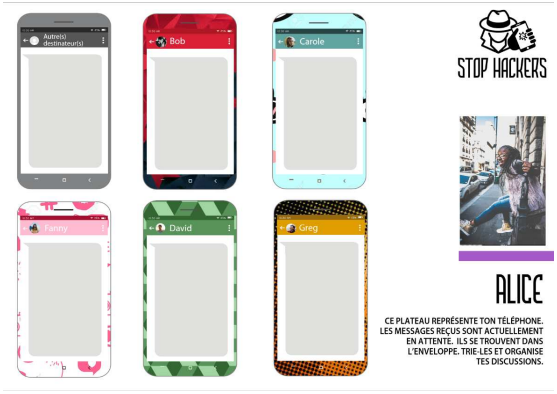

Fig. 2. Plateau de jeu d’Alice

les trie et les transfère aux bons destinataires. Il peut y ajouter des publicités, représentées par des cartes “messages” disposant d’une bordure grise. Chaque plateau dispose d’un emplacement pour déposer ces messages sans expéditeur précis.

Les pirates doivent lancer des menaces. Les trois profils de pirate représentent trois menaces différentes, avec des missions précises. Eve est une écouteuse externe (*eavesdropper*) et a pour mission de relever, dans les échanges entre amis, un maximum d’informations personnelles. Elle ne dispose pas de cartes “messages”. Oscar peut usurper l’identité d’un ami et substituer les messages de ce dernier par les siens qui sont infectés de virus. Pour se faire, ses cartes messages sont les copies conformes des messages des amis, couleurs comprises. Enfin, Peggy pratique le *phishing* : à travers ses messages qui ressemblent à de la publicité (de couleur grise), elle tente de manipuler les amis pour récupérer leurs données personnelles. Chaque menace réussie, et donc devenue cyberattaque, permet de faire gagner un point aux pirates. Pour éviter que les amis identifient les pirates, ceux-ci sont décrits comme des techniciens aidant les routeurs dans leurs tâches.

Dépendant du temps prévu par l’enseignant, le jeu peut prendre fin après sept tours, à savoir que chaque ami a, au minimum, envoyé sept messages. Le comptage des points va permettre de déterminer les vainqueurs dans chaque groupe, mais surtout de lancer le **débriefing**. Il est intéressant de ne pas dévoiler directement l’existence des pirates mais de prendre le temps, d’abord, de recueillir le ressenti des élèves : ont-ils ou non perçu les menaces ? font-ils des liens avec des situations déjà vécues ? Ensuite, des discussions pourront être menées concernant les intentions des pirates, la valeur des données piratées, la “forme” des menaces, les conditions de succès de celles-ci, etc.

La documentation créée à l’intention des enseignants comprend les règles du jeu, mais aussi un dossier pédagogique dans lequel se retrouvent, entre autres,

une clé de répartition des rôles, des connaissances théoriques en cybersécurité, des commentaires d'enseignants ayant testé le dispositif et des suggestions de thèmes à aborder durant le débriefing.

3.4 Phases d'expérimentation et d'analyse

Dans un premier cycle de l'itération, la phase d'expérimentation a été réalisée avec des experts en informatique et des enseignants, en vue de récolter leur évaluation sur la faisabilité du jeu avec le public-cible et la pertinence des concepts en lien avec les objectifs visés. Six chercheurs en informatique ont d'abord été impliqués ; ensuite, une vingtaine d'enseignants issus de l'enseignement primaire, secondaire et spécialisé. Durant ces tests, des observations ont été consignées par l'équipe de recherche et des discussions informelles ont été menées avec les participants.

Dans les cycles suivants, la phase d'expérimentation a pris place dans des écoles, en contexte réel. De février à juin 2021, le dispositif "Stop Hackers" a été testé auprès de quatre enseignants et 107 élèves : 21 en 5e primaire (P5), 44 en en 6e primaire (P6 - deux expérimentations) et 42 en 1re secondaire (S1 - deux expérimentations). Le matériel a évolué entre les différentes itérations, sur le fond et sur la forme. L'activité a été menée par les enseignants, en présence d'un membre de l'équipe de recherche qui intervenait principalement lors du débriefing. Pour chaque test, la collecte de données s'est déroulée en plusieurs étapes. Avant et après le test, des entretiens ont été menés avec les enseignants concernant leurs besoins avant le jeu, mais aussi leur vécu durant celui-ci et leur ressenti du vécu des élèves. Il leur a également été demandé d'évaluer, d'un point de vue pédagogique, le dispositif et de formuler quelques recommandations. Durant le test, des observations ont été réalisées par le chercheur afin de valider la jouabilité du dispositif dans un contexte réel et de vérifier la compréhension du jeu lui-même et des enjeux liés à la cybersécurité par les participants. Afin d'enrichir ces observations, des entretiens individuels ont été menés avec six élèves de P6.

4 Résultats et discussion

L'analyse et la discussion des résultats, illustrés par des verbatims, permet de répondre aux deux questions de recherche : d'une part, la question de la faisabilité de l'activité en classe et, d'autre part, la question des apprentissages.

4.1 Le dispositif éducatif "Stop Hackers"

Si les quatre enseignants ayant testé le dispositif soulignent à l'unanimité le côté ludique de l'activité et l'intérêt d'aborder la thématique de la cybersécurité en classe, ils ne semblent pas toujours au clair avec les objectifs d'apprentissage. Ainsi, lors de la phase de débriefing, les enseignants éprouvent des difficultés à structurer la discussion avec les élèves et ne savent pas toujours comment réagir

face à leurs propos. Ils souffrent d'un manque de maîtrise des enjeux liés à la cybersécurité. Bien que l'enseignant de S1 paraisse mieux connaitre le sujet et structurer, de ce fait, le débriefing, il éprouve tout de même des difficultés à gérer les échanges.

Concernant les élèves, certains semblent en difficulté avec leur rôle durant l'activité. Deux raisons pourraient l'expliquer. La première est un manque de précisions dans les consignes données par l'enseignant au début de l'activité et dans les réponses aux questions des élèves à propos de ces consignes. Un enseignant de P6 témoigne : *"Au début de l'activité j'étais vraiment énervé car je n'arrivais pas à gérer toutes les questions tout en continuant à donner les consignes."*. En outre, les élèves ne parviennent pas toujours à faire le lien entre un rôle et son matériel spécifique. Une évolution des supports a été rapidement proposée. Ainsi, l'enseignant de S1 a bénéficié, lors de sa deuxième expérimentation, d'une version améliorée du matériel pour les pirates mentionnant clairement ce qu'ils pouvaient ou ne pouvaient pas faire. Cette adaptation a notamment rendu les élèves jouant ce rôle plus autonomes, ce qui a eu comme effet direct de soulager l'enseignant en début d'activité. Toutefois, malgré la confusion des enseignants quant aux consignes, les observations ont montré que les élèves étaient capables, en fin d'activité, d'expliquer les règles du jeu et les diférents rôles proposés. Cela a été confirmé dans les entretiens : *"c'est un jeu avec plusieurs rôles. Chaque personne a un rôle spécial : six amis, le routeur qui est une machine qui ne peut pas parler qui fait passer les messages aux amis et les techniciens qui sont censés aider le routeur mais qui sont en fait des pirates. Le but du jeu c'est de s'envoyer des messages entre amis pour cumuler des points sans se faire pirater et perdre des points"* (élève de P6). La seconde raison est relative à un manque d'adaptation du dispositif à la réalité de la classe : les élèves circulent beaucoup durant l'activité, une grande quantité de matériel est nécessaire et celui-ci est très vite dispersé sur les bancs, des confusions sont possibles entre les cartes des amis et des pirates, le timing de l'activité est serré, entre autres. Concernant ce dernier point, la contextualisation (les références aux pratiques médiatiques des élèves, les consignes et la distribution du matériel) est chronophage, durant en moyenne 20 minutes. Il est conseillé d'accorder au moins 30 minutes au débriefing. L'enseignant doit donc gérer le temps de jeu et adapter, en temps réel, le nombre de tours au rythme des élèves.

Enfin, selon le niveau des élèves, l'activité n'a pas été vécue de la même manière. En secondaire, le rôle "ami" semble trop simpliste et les élèves s'ennuient comme le souligne l'enseignant : *"il faut trouver une occupation pour les amis qui attendent que le routeur et les pirates agissent."*. Une solution est proposée par cet enseignant : demander aux "amis" de prendre notes des critères sur lesquels ils reposent leur choix de consulter ou non un message. Lors du débriefing, ces notes alimenteront les discussions. Cet élément n'a pas été relevé dans les classes de primaire. Au-délà de ces quelques moments creux, que ce soit en primaire ou en secondaire, les élèves sont absorbés par l'activité et les tâches à réaliser. Ils ne cherchent pas à gagner mais plutôt à comprendre les rôles et stratégies. Un élève

de P6 résume parfaitement ces observations : *"il n'y a pas vraiment de gagnant. L'objectif, c'est de comprendre ce que sont les hackers et comment ça se passe"*.

4.2 Les apprentissages

Il apparait que les élèves s'inspirent surtout de ce qu'ils vivent au quotidien pour se poser des questions. Lors du débriefing, ils sont nombreux à signaler qu'eux-mêmes ou un membre de leur entourage ont déjà été piratés ou ont subi une tentative de piratage par phishing : *"on reçoit des messages quand on joue comme - si tu mets ton âge, ton nom, ton adresse, tu peux gagner 2000 ou 3000 €- mais c'est pas du tout ça"* (élève de P5) ; *"une amie à mes parents a reçu un message qui disait qu'elle devait retirer de l'argent d'un compte pour mettre sur un autre, mais en fait ils lui ont volé 4000 €"* (élèves de P5). La thématique fait donc sens dans cette tranche d'âges et les élèves semblent avoir compris qu'il existe différentes attaques en ligne et qu'il est possible de les éviter (mais pas forcément comment les éviter). Ainsi, ils comprennent que les publicités peuvent être piégées et qu'il existe des pirates qui espionnent ce qu'ils s'envoient : *"certains tournaient autour de nous et ils notaient des choses sur une feuille."* (élève de P6). Les élèves incarnant les pirates perçoivent mieux que le contexte d'un message est important à analyser : *"Si je savais que le personnage aimait la nourriture, je mettais des publicités sur la nourriture"*. À l'opposé, un élève (P6) qui a joué le rôle d'un ami explique, durant l'entretien, la stratégie qu'il a adoptée pour éviter les pirates. Il confie s'être rendu compte, à la fin de l'activité, que sa stratégie n'était pas la bonne, mais il ne sait pas expliquer pourquoi : *"j'ai tout de suite eu un tilt pour les hackers, donc je me suis dit que je ne devais pas prendre les cartes grises. Je n'ai pris que ceux qui venaient des amis, mais j'ai eu tort de faire comme ça"*.

Ils n'ont donc pas toujours une vision correcte de ce qu'ont représententé les différents rôles joués durant l'activité et des menaces présentes, même s'ils prennent bien conscience de leur existence lors du débriefing. Par exemple, les élèves (P6) interviewés associent, à l'unanimité, les publicités sans expéditeur connu à du piratage, mais jamais les contenus envoyés par des amis. Pourtant, le pirate Oscar usurpe l'identité des amis pour leur transférer des contenus malveillants. De plus, ces mêmes élèves lient majoritairement les intentions des pirates au vol d'argent et ne donnent de la valeur qu'à des données personnelles non illustrées dans l'activité : *"certaines sont plus importantes, non ? Ce serait des codes de banque ou de téléphone, mais dans le jeu, il n'y en avait pas trop"* ; *"Je ne sais pas trop. Je dirais que les informations intimes comme des photos, c'est ce qu'on pourrait voler"* ; *"Certaines données sont plus importantes, comme savoir ce que tu aimes bien... [il se reprend] non, savoir des codes VISA et tout ça"* ; *"Je n'ai pas beaucoup de données importantes, donc je ne sais pas ce qu'on pourrait me voler"*. Dès lors, ils ne savent pas toujours identifier les données qu'eux-mêmes transmettent et la valeur qu'elles peuvent avoir pour les pirates.

Ces différents résultats montrent que la contextualisation permet d'ancrer la problématique de la cybersécurité dans les pratiques et le vécu des élèves, tout en introduisant l'expérience du jeu. Lors de celui-ci, les élèves se rendent compte

de certains aspects, ils se posent des questions, sans que le jeu leur apporte toutes les réponses, ce qui permet de nourrir le temps de débriefing. Celui-ci est donc un moment essentiel pour approfondir les questions et asseoir les apprentissages. Or les résultats montrent que ce troisième temps du dispositif comporte certaines limites. Durant le débriefing, les enseignants de primaire, par manque de connaissances, se sont principalement focalisés sur les témoignages des élèves ou se sont référés à leur propre vécu, sans gagner en généralisation au niveau du questionnement et sans revenir sur les différents types de menace en ligne. De manière générale, les aspects techniques (notamment, comment éviter une attaque) ont peu été abordés, les enseignants étant moins à l'aise pour en discuter. Seul l'enseignant du secondaire, professeur d'informatique, y a introduit des notions techniques. Renforcer les thèmes plus techniques dans la documentation servant au débriefing semble nécessaire, celle-ci étant plutôt orientée sur la dimension critique. Ces thèmes devront être accompagnés de notions théoriques pour donner une base minimale de connaissances aux enseignants.

5 Conclusion

A partir du modèle d'une éducation au numérique critique et citoyenne, le dispositif "Stop Hackers" a pour objectif d'éduquer les enfants de 10-14 ans à la cybersécurité. Le projet de recherche a montré que l'activité, conçue à partir d'une démarche de type recherche orientée par la conception, peut être menée par des enseignants dans leur classe et permet de rencontrer, partiellement, les objectifs d'apprentissage. La contextualisation et l'expérience de jeu permettent de développer un questionnement critique, même s'il pourrait davantage monter en généralisation au cours du débriefing. Les aspects liés à la perspective de l'éducation à l'informatique doivent encore être renforcés, notamment à partir de la documentation fournie. Une autre possibilité serait de poursuivre l'activité par une leçon spécifique sur les notions plus techniques. Les enseignants seraient également plus confiants s'ils pouvaient bénéficier d'une formation sur la thématique.

References

1. Amankwa, E.: Relevance of Cybersecurity Education at Pedagogy Levels in Schools. Journal of Information Security, 12(4), 233-249. (2021)
2. Anderson, T., & Shattuck, J.: Design-based research: A decade of progress in education research?. Educational researcher, 41(1), 16-25. (2012)
3. Cobb, P., Confrey, J., DiSessa, A., Lehrer, R., & Schauble, L.: Design experiments in educational research. Educational researcher, 32(1), 9-13. (2003)
4. Corradini, I., & Nardelli, E.: Developing digital awareness at school: a fundamental step for cybersecurity education. In International Conference on Applied Human Factors and Ergonomics (pp. 102-110). Springer, Cham. (2020, July)
5. De la Higuera, C.: A l'ecole, doit-on enseigner l'informatique ou le coding ?Retrieved from http://www.slate.fr/story/110897/ecole-enseigner-informatique-coding, accessed December 7, 2021. (2015)

6. Fastrez, P.: Quelles compétences le concept de littératie médiatique englobe-t-il ? Une proposition de définition matricielle. Recherches en communication, 33, 35-52. (2010)
7. James, C., Weinstein, E., & Mendoza, K.: Teaching digital citizens in today's world: Research and insights behind the common sense K–12 digital citizenship curriculum. Common Sense Media. (2019)
8. Kumar, P., Vitak, J., Chetty, M., Clegg, T. L., Yang, J., McNally, B., & Bonsignore, E.: Co-designing online privacy-related games and stories with children. In Proceedings of the 17th ACM Conference IDC (pp. 67-79). (2018)
9. Lastdrager, E., Gallardo, I. C., Hartel, P., & Junger, M.: How effective is anti-phishing training for children?. In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017) (pp. 229-239). (2017)
10. Maqsood, S., Biddle, R., Maqsood, S., & Chiasson, S.: An exploratory study of children's online password behaviours. In Proceedings of the 17th ACM Conference on Interaction Design and Children (pp. 539-544). (2018)
11. Martin, F., Gezer, T., & Wang, C.: Educators' perceptions of student digital citizenship practices. Computers in the Schools, 36(4), 238-254. (2019)
12. Martin, F., Gezer, T., Wang, W. C., Petty, T., & Wang, C.: Examining K-12 educator experiences from digital citizenship professional development. Journal of Research on Technology in Education, 1-18. (2020)
13. Nicholson, J., Javed, Y., Dixon, M., Coventry, L., Ajayi, O. D., & Anderson, P.: Investigating teenagers' ability to detect phishing messages. In 2020 EuroSPW (pp. 140-149). IEEE. (2020)
14. Nicholson, J., Terry, J., Beckett, H., & Kumar, P.: Understanding Young People's Experiences of Cybersecurity. In European Symposium on Usable Security 2021 (pp. 200-210). (2021)
15. Orlando, J.: Kids need to learn about cybersecurity, but teachers only have so much time in the day. The Conversation. Retrieved January 10, 2022 from http://theconversation.com/kids-need-to-learn-about-cybersecurity-but-teachers-only-have-so-much-time-in-the-day-112136 (2019)
16. Pencheva, D., Hallett, J., & Rashid, A.: Bringing cyber to school: Integrating cybersecurity into secondary school education. IEEE Security & Privacy, 18(2), 68-74. (2020)
17. Putnam, C.: Teaching in a Digital Age: Internet Safety Education. (2019)
18. Quayyum, F., Cruzes, D. S., & Jaccheri, L.: Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, 100343. (2021)
19. Rahman, A., Sairi, I. H., Zizi, N. A. M., & Khalid, F.: The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10(5), 378-382. (2020)
20. Saariketo, M.: Imagining alternative agency in techno-society: outlining the basis of critical technology education (en). Media practice and everyday agency in Europe, 129-138. (2014)
21. Saariketo, M.: Reflections on the question of technology in media literacy education. In Reflections on media education futures: contributions to the Conference Media Education Futures in Tampere, Finland (pp. 51-61). (2014)
22. Snyman, D. P., Drevin, G. R., Kruger, H. A., Drevin, L., & Allers, J.: A Wolf, Hyena, and Fox Game to Raise Cybersecurity Awareness Among Pre-school Children. In International Symposium on Human Aspects of Information Security and Assurance (pp. 91-101). Springer, Cham. (2021, July)

23. Voogt, J., & Roblin, N. P.; A comparative analysis of international frameworks for 21st century competences: Implications for national curriculum policies. Journal of curriculum studies, 44(3), 299-321. (2012)
24. Vuorikari, R., Punie, Y., Gomez, S. C., & Van Den Brande, G.: DigComp 2.0: The digital competence framework for citizens. Update phase 1: The conceptual reference model (No. JRC101254). Joint Research Centre (Seville site). (2016)
25. Zhao, J., Wang, G., Dally, C., Slovak, P., Edbrooke-Childs, J., Van Kleek, M., & Shadbolt, N.: I make up a silly name' Understanding Children's Perception of Privacy Risks Online. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-13). (2019)