Une expérience d'éducation à la cybersécurité en Guadeloupe : le projet TiNum

par Lamprini Chartofylaka

Les outils numériques, qui font désormais partie intégrante du quotidien des jeunes enfants, en particulier depuis le début de la crise sanitaire de Covid 19, sont l'objet de nombreux travaux de recherche. Cet article présente un travail de recherche-action portant sur la cybersécurité en lien avec l'éducation aux médias et à l'information (EMI). Mené en Guadeloupe, il interroge les conceptions des élèves du primaire sur la notion de « robustesse d'un mot de passe » dans le cadre d'un projet, intitulé TiNum. Ce projet relève du domaine de l'éducation aux médias et à l'information et, plus précisément, du champ de l'éducation numérique.

Introduction

Les outils numériques font de plus en plus partie du quotidien des jeunes enfants, en particulier depuis le début de la crise sanitaire, et sont l'objet de nombreux travaux de recherche. Les questions relatives aux enjeux cachés de ces usages (à titre indicatif voir Capelle, 2020) et à la sensibilisation de ce jeune public aux bonnes pratiques numériques sont plus que jamais incontournables. Au-delà des usages des outils numériques, ces questions sont également en lien avec leur éducation à la citoyenneté.

Dans cet article, nous présentons un travail de recherche-action portant sur la cybersécurité, mené en Guadeloupe. Nous nous interrogeons sur les conceptions des élèves du primaire à propos de la notion de la robustesse d'un mot de passe dans le cadre d'un projet, intitulé *TiNum*. Ce projet relève du domaine de l'éducation aux médias et à l'information (EMI) et plus précisément du champ de l'éducation numérique (voir Joubaire, 2017).

1. Cadre conceptuel

La Guadeloupe est un département-région ultramarin français, où les fragilités à l'égard du numérique sont plus sensibles que dans le reste du territoire national, à la fois en raison de la vulnérabilité des infrastructures face aux risques naturels et de la situation socioéconomique de la population. Les enjeux relatifs au numérique y sont d'autant plus considérables, notamment pour réduire les fractures éducatives, sociales et économiques (Artano et al., 2020). En matière d'accès à l'information, peu d'études se sont intéressées aux pratiques relatives aux médias sur ce territoire. Les données, parfois lacunaires (Médiamétrie, 2018, 2022), montrent la faiblesse de la presse

classique, la prédominance d'une radio, qui réalise à elle seule environ 50% de parts de marché. Ces données permettent peu de retracer les audiences de télévision, faute d'adhésion de chaînes locales aux systèmes de mesure. Par ailleurs, peu de travaux portent sur les usages du numérique aux Antilles – en particulier ceux des jeunes enfants – et sur les questions de cybersécurité.

Pourtant, la sensibilisation de ce public sur la protection de ses données personnelles et de sa vie privée en ligne est indispensable (Commission Nationale de l'Informatique et des Libertés - CNIL, 2022), d'autant plus que c'est à partir de l'âge de 15 ans que « […] les mineurs peuvent consentir seuls à certaines utilisations de leurs données en France » (CNIL, 2021, p. 38).

Au niveau international, plusieurs travaux s'intéressent aux connaissances et aux compétences des jeunes enfants à propos de l'éducation à la cybersécurité. Certains auteurs (Kumar et al. 2017) se sont interrogés sur la compréhension par les jeunes enfants des notions de confidentialité et de sécurité en ligne. Ces auteurs, en même temps qu'ils fournissent des recommandations, soulignent l'importance de la création de ressources pédagogiques devant aider les parents à aborder ces sujets avec leurs enfants dès le plus jeune âge. D'autres auteurs (Choong et al., 2019; Lamond et al., 2022) mettent l'accent sur la prise en compte du développement progressif des capacités langagières et cognitives des individus, afin qu'ils puissent comprendre et adopter de bons réflexes à propos de leur cybersécurité.

Concernant la création de mots de passe, les jeunes enfants ont tendance à inclure des informations personnelles (Maqsood et al., 2018) ou à utiliser des mots de passe insuffisamment robustes (Choong et al., 2019). Cela s'explique, d'après ces auteurs, par le fait que les enfants « [...] are either unaware of what constitutes a strong password or are unable to generate one[1] » (Ibid.,p.10). Ces auteurs donnent l'exemple de la non-inclusion de caractères spéciaux dans les mots de passe générés par les enfants.

2. Projet TiNum : brève description et méthodologie

Le projet *TiNum* s'inscrit dans une dimension transversale entre le numérique et l'oralité. Il s'adresse aux élèves du primaire (niveau CM1 et CM2) et vise à les sensibiliser aux enjeux de la sécurité informatique à travers l'exemple du choix de mots de passe sécurisés. Dans la continuité d'une première étude menée en Guadeloupe en 2018 qui a montré des résultats prometteurs (Chartofylaka et Delcroix, 2018), nous avons conduit avec ce projet des tests à plus grande échelle. Les activités réalisées dans le cadre de *TiNum* sont en lien avec les directives de l'Éducation Nationale française concernant les apprentissages fondamentaux des élèves relatifs à l'EMI et portant sur :

[1] [...] ignorent ce qui constitue un mot de passe fort ou sont incapables d'en générer un (Traduction libre : L.Chartofylaka)

- « Le développement des aptitudes au discernement et à la réflexion critique prend appui sur l'éducation aux médias et à l'information (EMI) et sur la discussion réglée. » (ministère de l'Éducation Nationale, France, 2020, p. 66);
- Le développement des compétences de « Connaître ses droits et responsabilités dans l'usage des médias (citoyenneté et capacité à agir). » (ministère de l'Éducation Nationale, 2022, p. 4).

Les activités du projet se déroulent en deux phases de deux heures chacune, durant deux jours consécutifs. La première phase consiste en une présentation des enjeux de la sécurité informatique d'une façon ludique et interactive. La seconde est la phase d'activité des élèves proprement dite. À partir d'un mot de passe « simple », chaque enfant imagine une histoire dont il déduit un mot de passe plus robuste. L'histoire peut servir de moyen mnémotechnique. Diverses données ont été recueillies tout au long du projet portant sur les conceptions des élèves autour du concept de mot de passe. Ces données sont aussi relatives à la création d'un mot de passe robuste à partir de ce dispositif. Une description plus détaillée de ces deux phases est disponible dans Chartofylaka et al. (2022).

Les expérimentations se sont déroulées de novembre 2020 à mai 2021 dans la Région académique de la Guadeloupe, en incluant des classes des îles de l'Archipel (La Désirade, Les Saintes). Elles ont concerné six classes du primaire, représentant 114 élèves.

3. Méthodologie de collecte de données

Dans cette étude, nous traitons une partie des données recueillies pendant les activités menées dans la première phase de l'activité.

Étant donné que les élèves ont tendance à utiliser des informations personnelles pour générer un mot de passe (Maqsood et al., 2018), nous avons questionné les connaissances des participants sur la robustesse d'un mot de passe à travers l'activité suivante :

Nous avons fourni un prénom composé de 8 lettres (par exemple : nathalie), écrit en minuscule et une date de naissance (par exemple :16081997) en chiffres, sans inclure des signes de ponctuation comme la barre oblique (« / ») ou le point («.»). À partir de ces deux informations dites « personnelles », les participants sont invités à écrire sur un post-it des propositions de mots de passe robustes.

Pour évaluer les propositions (items) faites par les participants, nous avons défini deux axes d'analyse :

- Axe 1 : la présence des lettres majuscules et minuscules, des chiffres ou des caractères spéciaux ;
- Axe 2 : la longueur.

Ces deux axes sont relatifs aux bonnes pratiques recommandées par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) qui souligne que les mots de passe robustes : « [...] doivent être suffisamment longs, suffisamment

complexes (avec l'utilisation de minuscules, majuscules, chiffres et caractères spéciaux) » (ANSSI, 2021, p. 12).

4. Analyse et résultats

Nous avons recueilli et retranscrit 161 propositions (certains élèves en ayant fourni plusieurs), qui font l'objet de notre analyse ci-dessous.

Pour effectuer le premier traitement, nous comptons le nombre de fois où on trouve au moins un caractère majuscule, un caractère minuscule, un chiffre ou un caractère spécial dans la réponse obtenue.

La figure suivante (Figure 1) présente la répartition quantitative de ces propositions en fonction des différentes modalités de la catégorisation retenue.

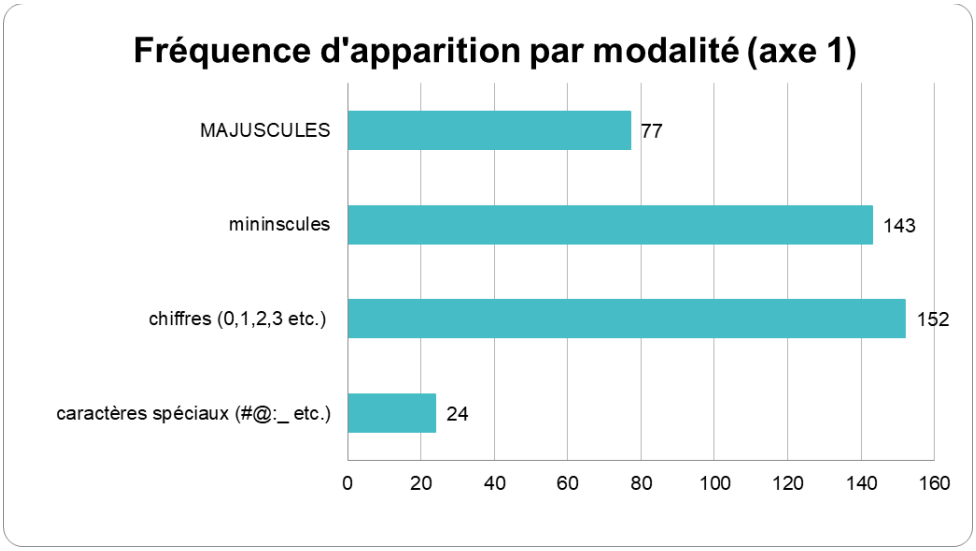

Figure 1 : Composition des mots de passe proposés (axe 1)

La majorité des propositions fournies inclut des minuscules (143 en total) et des chiffres (152 en total), comme dans les « informations personnelles » (prénom et date de naissance) qui ont été initialement fournies.

Presque la moitié des propositions (77 en total) inclut des majuscules. Toutefois, dans 55 sur 77 cas, la présence d'un caractère majuscule était un simple remplacement de la première lettre du prénom donné de la minuscule à majuscule (donc de « nathalie » à « Nathalie »).

En ce qui concerne les caractères spéciaux, nous avons reçu 24 propositions incluant des caractères comme : « = », « / », « . », « : », « , », « # », « @ » et « ! ». Dans certains cas, la barre oblique (« / ») ou la virgule (« , ») a été ajoutée pour que la date de naissance fournie puisse ressembler à une date « standard » (par exemple : « 16/08/1997 »).

Pour effectuer le deuxième traitement, nous comptons la longueur de propositions obtenues qui sont présentées dans la figure suivante (Figure 2).

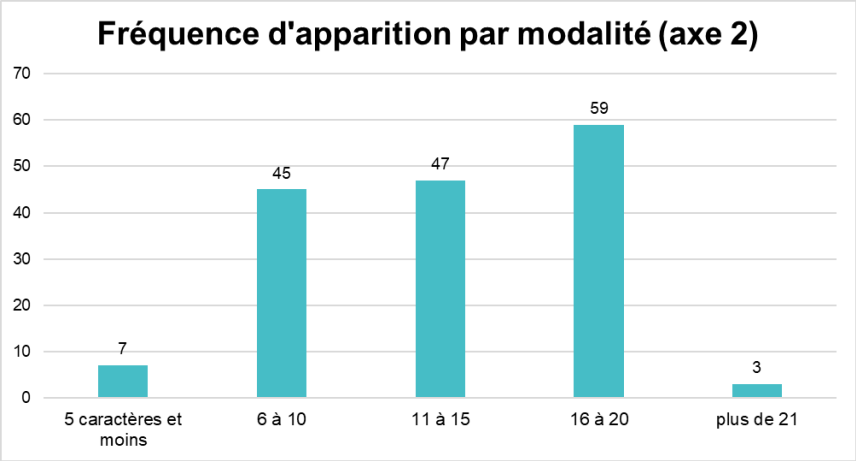

Figure 2 : Longueur des mots de passe proposés (axe 2)

La majorité des propositions est de 16 à 20 caractères. La plus courte proposition est de 4 caractères et la plus longue de 31 caractères (moyenne=12.78, écart type=4.30). Un quart des propositions (39) a une longueur de 16 caractères. Nous rappelons que les « informations personnelles » (prénom et date de naissance) fournies, possèdent un total de 16 caractères alphanumériques.

Nous nous interrogeons également sur les stratégies employées par les apprenants pour construire leurs propositions à partir des éléments fournis. Il faut rappeler que cette phase a été mise en place au début de l'expérimentation avant que les élèves bénéficient d'informations sur les recommandations de l'ANSSI dans le cadre du projet.

Le Tableau suivant (Tableau 1) récapitule, dans une entrée matricielle les deux stratégies principales identifiées dans les propositions fournies par les apprenants, ainsi que le nombre de réponses correspondant à ces deux stratégies.

Tableau 1 : Stratégies adoptées par les apprenants pour proposer un mot de passe « robuste »
à partir les éléments fournis

Éléments fournis *nathalie* *16081997*		**Stratégie 2 :** **Nouveaux apports**			
		2a. réorganisation des caractères	**2b. réorganisation des caractères et/ou autres modifications**		
Stratégie 1 :			**Majuscules**	**Caractères spéciaux**	**Autres**
	1a.	19	14	13	1

Usage des éléments fournis	**Dans leur totalité**				
	1b. Une partie	40	56	12	23

La première stratégie concerne l'usage des éléments fournis : 47 propositions incluent tous les caractères alphanumériques fournis (modalité 1a) tandis que 112 propositions incluent une partie de ces informations (soit une partie du prénom, soit une partie de la date de naissance, soit les deux etc.) (modalité 1b).

La deuxième stratégie porte sur les apports par rapport aux éléments fournis initialement. Ici, nous avons identifié deux modalités :

- Modalité 2a : La modification de l'ordre des éléments fournis (par exemple « n1a6t0h8a1l9i9e », « 1608nathalie1997 »)
- Modalité 2b : Le changement de l'ordre des éléments fournis et/ou d'autres modifications comme l'ajout, au moins, d'un caractère majuscule (par exemple « Nath1608alie1997 », « NaThAlIe »), l'ajout au moins d'un caractère spécial (par exemple « 1997nathalie/1608 », « halienat :1608 ») ou l'ajout d'autres éléments comme un mot aléatoire (par exemple « nathalie16081997zodique »), un ou plusieurs chiffres aléatoires (« Nathalie2198 ») ou dupliquer/répéter les caractères fournis (par exemple « nathalieN16081997 »).

Dans certaines propositions obtenues, plusieurs éléments de la modalité 2b ont été présents (par exemple « 15#Nathalie!1997@08 »).

5. Discussion

Ces résultats élargissent notre connaissance sur les conceptions des enfants du primaire sur la cybersécurité, et, plus précisément sur les pratiques qu'ils connaissent ou utilisent pour générer un mot de passe robuste.

Une grande partie des participants connaît déjà certaines règles à appliquer lors de la création d'un mot de passe ou les applique intuitivement. Il peut s'agir de l'usage d'informations personnelles mais pas dans leur intégralité ou encore de la réorganisation des différents alphanumériques caractères. Cependant, nous considérons qu'ils ne possèdent pas encore une grande expertise dans l'application de ces règles. C'est la raison pour laquelle ils proposent des mots de passe faciles à être devinés ou communs.

De plus, notre étude met aussi en évidence deux autres points :

a) L'usage de lettres majuscules est réduit aux seuls mots qui en comportent naturellement (comme la première lettre d'un nom ou prénom) ;
b) L'usage de caractères non-alphanumériques (caractères spéciaux) n'est pas une pratique très répandue chez les jeunes enfants.

Sur ce dernier point, il faut cependant souligner que certains caractères ne sont pas toujours éligibles dans la création d'un mot de passe, en fonction de la configuration des paramètres de stratégies de sécurité mises en place par un service donné.

Ces résultats doivent être interprétés avec prudence, en raison de l'échantillon restreint. La longueur des données initiales (prénom et date de naissance, 16 caractères au total) a également pu conduire les enfants à ne pas ajouter de caractères, voire à en enlever, les mots de passe utilisés « au quotidien » étant assez courts (recommandation de l'ANSSI : 12 caractères et plus). Toutefois, nous considérons que ces premières analyses fournissent un aperçu sur les points-clés sur lesquels il faut insister pour sensibiliser les jeunes enfants sur le sujet. Un traitement de données complémentaire serait nécessaire pour déterminer si et comment la participation de ses apprenants dans le projet *TiNum* a enrichi leurs connaissances sur le sujet.

Conclusion

Cet article présente un projet EMI, traitant une thématique complexe, celle du choix d'un mot de passe fort, destiné aux jeunes enfants. Si des traitements complémentaires des données recueillies lors du projet sont encore à effectuer pour en mesurer l'efficacité, il faut noter que l'activité est facilement reproductible à un coût faible, et que la première étude (Chartofylaka et Delcroix, 2018) a montré qu'elle permettait d'enrichir les connaissances des jeunes enfants face aux risques et à leur protection en ligne. L'adoption d'un comportement plus sain face aux enjeux numériques mais aussi l'utilisation des informations par les individus d'une façon responsable et intelligente, comme, par exemple, par le choix d'un mot de passe robuste, font partie également de la lutte contre la désinformation.

Bibliographie :

Agence nationale de la sécurité des systèmes d'information - ANSSI, *Recommandations relatives à l'authentification multifacteur et aux mots de passe - Version 2.0.*, Paris, France, Agence nationale de la sécurité des systèmes d'information - ANSSI, 2021, p.49

Artano S., Artigalas V. et Dindar N., *Urgence économique outre-mer à la suite de la crise du Covid-19*, Délégation sénatoriale aux outre-mer du Sénat, 2020, p.417

Capelle C., « "Risques numériques" : Qu'en pensent les jeunes et les enseignants ? », Que dit la recherche ?, 2020, s.p.

Chartofylaka L. et Delcroix A., « StoryPass – Password Rules Hidden in a Storytelling Game Activity. Steps towards Its Implementation », Proceedings of 8th International Toy Research Association World Conference, 2018, s.p.

Chartofylaka L., Troullinou P. et Delcroix, A., « Hard-to-guess but easy-to-remember: understanding children's password security issues », Methods in practice: Studying children and youth online (chapter 4), 2022, s.p.

Choong Y.-Y., Theofanos M. F., Renaud K. et Prior S., « "Passwords protect my stuff"—A study of children's password practices », Journal of Cybersecurity, 2019, 5, 1, 1-19

Commission Nationale de l'Informatique et des Libertés - CNIL, *Protéger les données personnelles, Accompagner l'innovation, Préserver les libertés individuelles*, Paris, France, Commission Nationale de l'Informatique et des Libertés - CNIL, 2021, p.120

Commission Nationale de l'Informatique et des Libertés - CNIL, CNIL.fr. [En ligne]. 2022, février 18 [2022, septembre 25]. URL : https://www.cnil.fr/fr/radio-france-et-la-cnil-sassocient-pour-sensibiliser-le-grand-public-la-protection-des-donnees

Joubaire C. « EMI : partir des pratiques des élèves », Dossier de veille de l'IFÉ - ENS de Lyon, 2017, 115

Kumar P., Naik S. M., Devkar U. R., Chetty M., Clegg T. L. et Vitak J., « "No Telling Passcodes Out Because They're Private": Understanding Children's Mental Models of Privacy and Security Online », Proceedings of the ACM on Human-Computer Interaction, 2017, 12, 1, 1-21

Lamond M., Renaud K., Wood L. et Prior S., « SOK: Young Children's Cybersecurity Knowledge, Skills & Practice: A Systematic Literature Review », European Symposium on Usable Security, 2022, 14-27

Maqsood S., Biddle R., Maqsood S. et Chiasson S., « An exploratory study of children's online password behaviours », Proceedings of the 17th ACM Conference on Interaction Design and Children, 2018, 539-544

Médiamétrie, Mediametrie.fr. [En ligne]. 2018, septembre 6 [2022, septembre 25]. URL : https://www.mediametrie.fr/fr/les-territoires-doutre-mer-une-passion-pour-linfo

Médiamétrie, Mediametrie.fr. [En ligne]. 2022, avril 29 [2022, septembre 25]. URL : https://www.mediametrie.fr/sites/default/files/2022-04/2022%2004%2019%20CP%20METRIDOM%20TV%20Janvier-Mars%202022.pdf

Ministère de l'Éducation Nationale, *Orientations pour l'éducation aux médias et à l'information (EMI) aux cycles 2 et 3*, Paris, France, 2022, p.5

Ministère de l'Éducation Nationale, *Programme d'enseignement français au cycle 3*, Paris, France, 2020, p.99