Comparing Teacher and Creator Perspectives on the Design of Cybersecurity and Privacy Educational Resources

Joy McLeod, *Carleton University;* Leah Zhang-Kennedy, *University of Waterloo;*
Elizabeth Stobert, *Carleton University*

https://www.usenix.org/conference/soups2024/presentation/mcleod

This paper is included in the Proceedings of the
Twentieth Symposium on Usable Privacy and Security.

August 12–13, 2024 • Philadelphia, PA, USA

978-1-939133-42-7

Open access to the Proceedings
of the Twentieth Symposium
on Usable Privacy and Security
is sponsored by USENIX.

Comparing Teacher and Creator Perspectives on the Design of Cybersecurity and Privacy Educational Resources

Joy McLeod
Carleton University

Leah Zhang-Kennedy
University of Waterloo

Elizabeth Stobert
Carleton University

Abstract

Various educational resources have been developed to teach children about cybersecurity and privacy. Our qualitative interview study with 15 middle school teachers and 8 creators of cybersecurity educational resources compares and analyzes the design considerations of cybersecurity resource creators with the resource selection strategies and classroom practices of teachers in their delivery of cybersecurity lessons to middle school students. Our thematic analysis showed that teachers predominately used free, low-tech, modular, and modifiable resources such as lesson plans, short educational videos, and segmented learning modules to fit their classroom teaching needs. The topics focus on helping students develop critical thinking skills rather than technical knowledge. Creators, on the other hand, focused their resource design considerations primarily on cybersecurity trends and students' media learning preferences, such as developing games and other types of interactive content to increase engagement. We highlight areas of misalignment between creators' design considerations compared to how teachers access and deliver cybersecurity and privacy lessons to students.

1 Introduction

Cybersecurity and privacy have emerged as a topic of concern for parents, educators, and policymakers [11] as people are using an ever-expanding number of services to live and work, and the importance of knowing how to stay safe online, protect personal information and verify the authenticity of information found online has never been greater [6, 16, 17, 23]. Due to the high potential for exposure to online risks, a focal point of intervention has been the development of initiatives that aim to educate young people about online risks. The goal is for young people to develop their knowledge about cybersecurity and privacy so they can critically examine their online experiences and protect themselves online. Teachers are increasingly asked to assume the responsibility of educating young people to thrive as digital citizens and future employees [16–18]. However, teachers may not be properly equipped with their own knowledge of security and privacy to teach these subjects to their students [4, 8, 16, 18, 21, 31, 33].

Various cybersecurity education resources for the K-12 classroom [1, 14, 26] have been created to help teachers carry out this important task. Previous research [39] found that about half of the tools and resources in the last decade are aimed at children and youth. However, there is limited understanding of how teachers utilize these resources in the classroom [23], making it difficult to assess how effectively these resources meet the needs of teachers and students.

This paper aims to compare the teaching practices of middle school teachers with the design considerations of creators of cybersecurity educational resources. Our goal is to determine if the process of creating and distributing resources by content creators aligns with how teachers discover and use these resources in the classroom. This intersection between creators and teachers in cybersecurity education has not been explored before. We define a resource creator (hereby referred to as "creators") as a stakeholder who has contributed to the design of cybersecurity educational materials. A creator could be a designer, developer, researcher, or project manager who has experience in industry or academia creating cybersecurity educational resources. Our research questions are:

RQ1 What do teachers consider when choosing cybersecurity and privacy educational resources to use in the classroom and how do they assess learning outcomes?

RQ2 What do creators consider when curating, designing, and evaluating cybersecurity and privacy resources for use in the classroom?

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

RQ3 How well do creators' design considerations and processes for the educational content and format of delivery align with the needs of teachers and students to teach and learn about cybersecurity and privacy?

To answer our research questions, we interviewed 15 middle school teachers who have taught tweens (aged 10–13 years) and 8 resource creators to understand their processes, challenges, experiences, and needs. We focus on middle school teachers because their tween students are a vulnerable demographic that needs significant support and guidance from teachers as they navigate digital media [10, 24].

We analyzed our data using thematic analysis and found that teachers were predominantly using freely available, low-tech, lesson-oriented resources in their teaching, such as lesson plans, short videos, and segmented learning modules, and generally found these resources effective. Their considerations in choosing resources focused on alignment with their classroom teaching needs and how well the resources supported inquiry and critical thinking skills. Most taught cybersecurity and privacy as an ad hoc reaction to classroom incidents, such as cyberbullying, which influenced their preferences for finding and choosing resources. Teachers reported a variety of assessment methods to measure learning outcomes, but showed a preference for critical reflection over formal assessment due to the sensitivity of the topics.

Creators showed a general awareness of the time constraints of teachers related to curricular expectations and the technical challenges teachers face in incorporating cybersecurity resources into the classroom. However, they prioritized the needs and learning preferences of the primary target audience of the educational resource, such as design considerations that make the resources engaging and fun for young people. Furthermore, our investigations into creators' design processes show that they lack centralized guidance on what baseline topics should be taught, causing them to develop resources based on current cybersecurity trends and funding opportunities.

2 Background and Related Work

Government, not-for-profit organizations, and academic researchers make available a variety of resources to assist teachers in teaching topics of privacy, cybersecurity and digital literacy to their students. Resources are generally provided online and organized by the curricular expectations, geography, topic, grade, and media type [12, 15, 26, 27, 35]. In more structured programs, the lessons are organized predominantly by topic and grade in discrete packages [3, 30, 34], such as Google's Applied Digital Skills curriculum on digital footprints, online scams, cyberbullying, and more [13].

Supporting resources for teachers are often included with the educational tools as lesson and facilitation guides to help them use the resources and deliver the lesson. Other related teacher resources include materials such as slides, tip sheets, videos, printable classroom activities, quizzes, and assessments [12, 15, 26, 27, 30, 34, 35].

2.1 Cybersecurity Educational Tools and Resources

A variety of multimedia tools such as games, videos, tabletop games, learning modules, and comics [37, 38, 40] have been developed to teach people of all ages about cybersecurity [39]. Games, in particular, are the most popular type of resource, as they are believed to be a particularly powerful experiential learning tool [23, 39].

In a systematic review of multimedia tools for cybersecurity awareness and education created between 2000 and 2019, Zhang-Kennedy and Chiasson [39] identified that approximately 43% of the tools are tailored to children and youth, but most tools lack evaluations to support the effectiveness of the learning outcomes. Another systematic review of the literature on children's cybersecurity awareness in 2021 [32] added to this by pointing out the lack of valid evaluation methods, theoretical frameworks, small sample sizes, and a bias toward early signs of positive results.

Although educational and training resources created to improve the general public's cybersecurity and digital literacy could be used by teachers(e.g., Cybersec101 [3]), public professional development training resources tailored to teachers are rare and focus primarily on students' privacy. For example, iKeepSafe [19] has an educator training course on data privacy in education. Common Sense Education [9] offers free teacher privacy compliance training to protect student privacy. The Student Privacy Compass [36] has a series of student privacy training for educators that touches on a variety of topics, including training on why students need to learn about privacy and the key topics to teach.

2.2 Challenges in Teaching Cybersecurity and Digital Literacy

Few studies have explored how teachers are currently using tools and resources to teach cybersecurity and digital literacy, the challenges they face, and their perceptions of students' skills and competencies.

Weinstein et al. [20] surveyed K–12 teachers in the U.S. and found that approximately 60% used some type of digital literacy curriculum or resource with students in the classroom. Furthermore, 70% of teachers reported teaching at least one type of digital literacy competency, with the most common being cyberbullying (46%) and privacy and safety (44%).

Maqsood and Chiasson [24] conducted a study with 21 Canadian elementary school teachers to understand the risks teachers were seeing their 10 to 13 year old students. They found that teachers regularly helped their students mitigate risks from minor policy violations to more serious forms of

cyberbullying. However, teacher reported a lack of knowledge, training, and support to address issues at their schools.

Corradini and Nardelli [10] conducted a study with 2,229 Italian primary and secondary school teachers' about their perceptions of their students' digital awareness. They found that teachers felt students should be better prepared to recognize risks when using digital technologies, pay more attention to protecting their personal data and privacy, and learn media literacy in terms of measuring the reliability of news on social media. Similar to the findings of Maqsood and Chiasson [24], the Italian teachers also reported that they needed additional training to improve their own digital awareness and administrative support in their activities.

Kumar et al. [22] conducted focus groups with 25 educators to better understand what privacy and security meant to them. They found that technology use is an integral part of the elementary school classroom and that educators consider digital privacy and security through the lens of their curricular and classroom management goals.

Nicholson et al. [28] conducted a study with 50 secondary school children aged 12-14 and found that teachers described the education process as a "*piecemeal approach*," with students reporting learning about related and non-technical aspects of privacy and security (e.g., cyberbullying) through sporadic lessons and not in a consistent, ongoing way.

Martin et al. [25] conducted a study with 107 K-12 educators to understand their perceptions of their students' digital citizenship knowledge and practices. They found that educators who taught digital citizenship had higher perceptions of their students' digital citizenship practices than other educators. Teachers reported the need for more training, resources, and activities relating real-world examples, and integrating digital citizenship into curriculum.

2.3 Research Gap

Significant work has been done to develop privacy and cybersecurity educational materials for children. However, there is a lack of studies that focus on teachers' perspectives when teaching these topics [22, 24]. While there are some studies that aim to evaluate specific resources, none of these studies explores how teachers approach these subjects with their students. Our goal is to compare teachers and creators' perspectives on teaching cybersecurity and privacy, to identify whether these materials are being designed well, accessed widely, and used effectively.

In our work, we interviewed 15 teachers and 8 creators to compare their perspectives on cybersecurity and privacy education, and identified overlaps and divergences between teachers' and creators' perspectives. Based on our findings, we highlight areas of misalignment between creators' design considerations compared to how teachers access and deliver cybersecurity and privacy lessons to students.

3 Methodology

We conducted semi-structured interviews with teachers and resource creators. We interviewed 15 pre-secondary school teachers and 8 creators. Both studies followed the same basic methodology and received clearance from our institution's Research Ethics Board.

3.1 Procedure

Study participants completed a brief screening questionnaire before being invited to participate in an online interview lasting 60 to 75 minutes. The interviews were audio-recorded and transcribed using Trint[1] and manually checked for accuracy. The participants were remunerated $45 CAD.

The teachers' pre-interview questionnaire (see Appendix 9) asked demographic questions, as well as questions about teachers' experience with cybersecurity and privacy topics and the resources they use. The teacher interview questions (see Appendix 11) explored the following areas:

- *Practices:* How do teachers teach cybersecurity and privacy to their students?
- *Selection:* How do teachers find and choose the resources they use to teach cybersecurity and privacy?
- *Effectiveness:* How effective do teachers find these resources?
- *Experience:* What do teachers like and dislike about these resources?

To ground teachers' responses in their classroom experiences, teachers participating in the interview were asked to bring examples of resources they had previously used to teach cybersecurity or privacy, and to explain how and why they were used.

The creators' pre-interview questionnaire (Appendix 10) asked demographic questions, and about creators' experiences designing educational materials for teaching cybersecurity and privacy, and what topics and issues they considered in the design of these materials. The creator interviews (Appendix 12) were structured around the following topics:

- *Processes:* How do creators go about developing educational resources for cybersecurity and privacy in their organizations?
- *Dissemination:* How do creators make schools and teachers aware of these resources?
- *Improvement:* How could creators' design processes or resources be improved?
- *Strategies:* What strategies do creators use when designing resources for different age groups?

[1] https://trint.com/

3.2 Participants

We recruited participants for both studies using a combination of snowball sampling, social media, and emails.

3.2.1 Teachers

To qualify for the study, teachers had to be Canadian and have had experience teaching cybersecurity and privacy to pre-secondary school students in the last two years. We limited recruitment to Canadian teachers so they could share experience in a similar educational system. Teacher recruitment notices were emailed to local contacts, teacher-oriented associations, and school mailing lists (with the approval of school boards). We also posted recruitment notices to relevant Facebook and Reddit groups.

In total, we interviewed 15 teachers from 11 schools in three of the largest Canadian provinces[2]. Table 1 summarizes the demographics of the teachers. The majority (67%) were female, and the remainder (33%) were male. Our participants had a wide range of teaching experience from 1 to 35 years ($Mdn = 15$). More than half (53%) were mid-career professionals over the age of 40. All had experience teaching middle grades, though many also had experience teaching a broader range of students ranging from kindergarten to grade nine. All but one participant (93%) taught in public schools. The majority of the teachers (87%) had an educational background in arts, languages, or education, with only one having a background in science.

3.2.2 Creators

We broadly defined a creator as a stakeholder who has professional experience in creating cybersecurity educational resources. As we did not limit their roles to the implementation of resources, these individuals could include designers, developers, researchers, project managers, and educational directors. As a starting point, the lead researcher emailed researchers and practitioners listed in the Canadian Cybersecurity Awareness Stakeholders Teleconference Report [2] and asked those contacts to pass the recruitment notice along to their contacts. We were able to recruit eight creators, summarized in Table 2. Of these eight, half were female. The majority (88%) were based in Canada, and one participant (C8) was based in the United States. Six participants (75%) were mid- to late-career professionals 40 years or older, with two over 60 years of age.

In total, our creator participants represented eight different organizations that represented the not-for-profit, public, and private sectors. We do not suggest that our sample is representative of creators in cybersecurity education. However, our sample includes creators with various educational work experiences. Three of the participants (38%) had been creating cybersecurity and privacy resources for 10+ years, and the remaining five participants (63%) had 5–9 years of experience. More than half (63%) of the participants reported being in senior leadership positions; the other three reported positions related to cybersecurity education research and consulting.

In terms of the educational levels of the participants, two (26%) had bachelor's degrees, three had master's degrees (37%), and three had doctoral degrees (37%). Six participants (75%) reported that their education was directly related to their work creating resources related to privacy and education, and the other two (25%) reported that although their education was not focused on these areas, they had learned the skills and knowledge they needed on the job.

3.3 Reflexive Thematic Analysis

We used reflexive thematic analysis [5, 7] for our qualitative analyses in both studies. This approach emphasizes the researcher's active and reflexive role in knowledge production, and acknowledges that codes are understood to represent the researcher's interpretation of meaning and patterns within the data set [7]. The lead researcher had some elementary school teaching experience and conducted all interviews. They were most closely involved with the research, giving them the most relevant contextual experience for the analysis. While codebooks were developed as part of the analysis process for both studies, coding reliability was not calculated due to the reflexive nature of data coding [7]. Instead, intermediate results were regularly reviewed and discussed with two other researchers to help refine the coding categories and extract meaning from the data.

The first stage of our thematic analysis was coding. The lead researcher familiarized themselves with the data by reading and re-reading the transcripts and adding annotations and comments line-by-line using Microsoft Word's commenting feature. This initial process focused on noting key terms and the underlying idea of each response to help get a sense of emergent patterns in the data. Once this was completed, the lead researcher began the process of assigning preliminary codes [5]. The process was repeated for each study.

For the teacher study, we coded 273 pages of transcriptions generated from over 21 hours of audio recordings of interviews. In total, we created 230 codes. For the creator study, we coded 124 pages of transcriptions generated from over 8.5 hours of audio recordings of interviews. In total, we created 280 open codes.

Following open coding, we transitioned to the process of identifying themes. Using Miro[3], we examined our open codes for the underlying patterns. We organized the uncategorized open codes into themes [5], which are presented below in Sections 4 and 5. We attribute direct quotes by appending the letter "T" (e.g., T4) or "C" (e.g., C8) to identify the participant as either a teacher or a creator.

[2] Canada's four largest and most populous provinces are Ontario, Quebec, British Columbia, and Alberta.

[3] Miro: https://miro.com

Table 1: Teacher demographics.

ID	Gender	Age	Educational Background	Exp. (years)*	Grades	School	Province
T1	Female	30–39	Drama, English (Minor)	8	7-12	Public	Ontario
T2	Female	30–39	Criminology	7	5-12	Public	Ontario
T3	Male	20–29	Arts, French, Education, History (Minor)	1	5-6	Public	Quebec
T4	Male	30–39	Drama, History	8	6	Public	Ontario
T5	Female	40–49	English Lit., Child Psychology (Minor)	15	5–8	Public	Ontario
T6	Male	50–59	History, Fine Art, Music	27	K–11	Private	Ontario
T7	Male	30–39	*Unspecified*	12	7–11	Public	Quebec
T8	Female	40–49	Kinesiology	20	6	Public	Ontario
T9	Female	20–29	Development Studies, English, Education	4	6	Public	Quebec
T10	Female	50–59	History, Classical Studies	31	3–6	Public	Ontario
T11	Female	60+	Education	35	1–12	Public	Alberta
T12	Female	50–59	History	31	7–8	Public	Ontario
T13	Female	50–59	History, English	27	7–8	Public	Ontario
T14	Female	30–39	Education	5	6	Public	Alberta
T15	Male	40–49	Arts, Education, Social Studies (Minor)	19	7	Public	Alberta

*Years of work experience related to general teaching

Table 2: Creator demographics.

ID	Gender	Age	Educational Background	Highest Degree	Exp. (years)*	Type of Organization	Organization Size	Job Title
C1	Male	40–49	Theatre, English, Education	Bachelor's	13	Not-for-profit	10–49	Director of Education
C2	Male	40–49	Info. Systems, Bus. Mgmt., Criminology	Doctoral	7	Public sector	0–9	Executive Director
C3	Female	40–49	*Unspecified*	Bachelor's	10	Public sector	1000–4999	Supervisor
C4	Male	60+	Engineering, Bus. Admin., Education	Doctoral	5	Both sectors	100–499	President
C5	Female	20–29	Public Policy	Masters	7	Public sector	10–49	Senior Manager
C6	Female	30–39	Computer Science, HCI, Usable security	Doctoral	7	Public sector	1000–4999	Post-doctoral Fellow
C7	Male	60+	Biochemistry, Education	Masters	5	Public sector	0–9	Educational Consultant
C8	Female	40–49	Linguistics	Masters	9	Not-for-profit	10–49	Research Scientist

*Years of work experience creating cybersecurity educational resources.

4 Teachers' Perspectives

Figure 1 shows commonly reported topics taught to students, including "*Cyberbullying*" (87%), "*Cybersecurity*" (80%), and "*Privacy*" (73%). The least commonly taught subjects were "*Authentication*" (20%), "*Gambling*" (20%), and *Pornography*" (20%).

The three most popular resource types used by teachers in our study were lesson plans (87%), learning modules (67%), and live videos (47%). The least-used resource types were comics and gamified activities (13%), and none of our participants reported ever using non-digital or mobile games. Resources that were frequently mentioned were from Media Smarts, Common Sense Media, and Teachers Pay Teachers.

4.1 Resource Discovery

The majority of teachers reported relying on Google searches using key terms and the grade level, highlighting the importance of search engine optimization to improve the chances of teachers finding relevant resources. More experienced teachers reuse the resources they have accumulated over time, and others go directly to trusted organizations' websites (e.g., MediaSmarts, Common Sense Media), or eliciting recommendations from trusted colleagues.

Our teacher participants reported that it is uncommon for their school boards or Ministries of Education to provide curriculum teaching resources on cybersecurity and digital literacy. While elements of these topics are taught as part of the health science and media literacy curriculum, most teachers reported that due to competing curricular priorities, they addressed these topics sporadically or only after a negative event occurred at school. For example, T15 commented, *"By and large, it's only brought up outside of health class when someone gets in trouble. Like, it's not something that is generally talked about in a regular, neutral fashion."* Only a few participants said they take a proactive approach, such as dedicating a week to an entire program, such as the suite of lessons developed by Common Sense Media. This suggests that there is considerable variability in how and when teachers address these topics. For the most part, teachers reported approaching cybersecurity and privacy topics reactively and ad hoc.

4.2 Resource Selection

Teachers had a myriad of considerations when choosing between resources. Their main concerns were how well the resource met their own needs while balancing that against

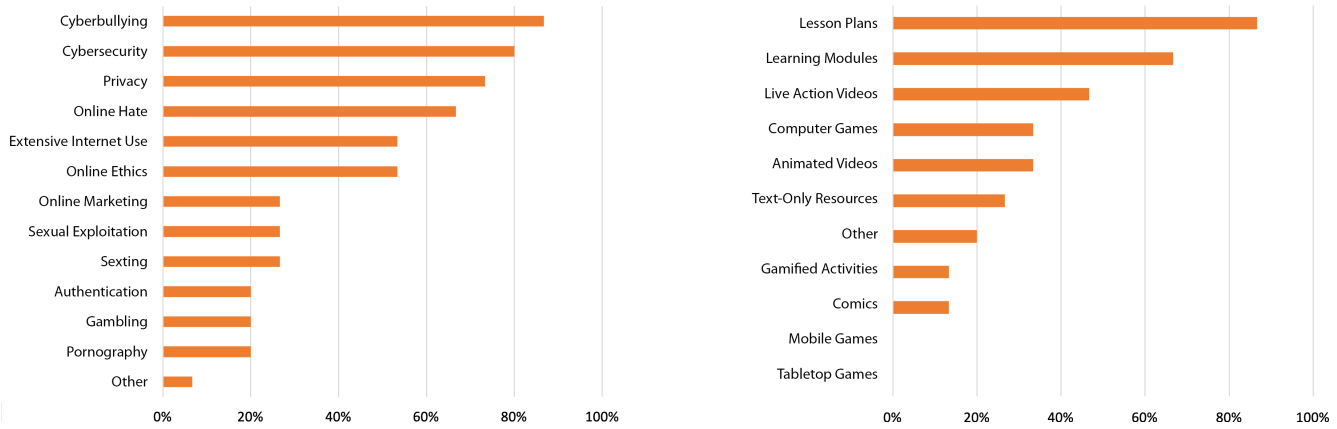

Figure 1: Percentage of teachers who had taught various cybersecurity topics (left) and used various types of resources (right).

how appealing and relatable the resource would be to their students. Although our participants reported using a variety of resources, we found that, in general, simple and accessible resources such as lesson plans, short videos and animations, computer games, quizzes, and classroom activities were the preferred resources used to teach cybersecurity and privacy compared to mobile games, board games, or comics.

4.2.1 Critical Thinking

Teachers preferred resources that promote inquiry and critical thinking skills. This was best done by providing "minds-on" (T12) questions, discussion prompts, or challenges where students were encouraged to investigate things within the resource. For example, T15 shared a resource by CIVIX, a Canadian not-for-profit that they felt did this well.

> *And the way that the CTRL-F program is designed, it starts with a question of some kind. And then they have to try and go into, well, how exactly does this work? And there's a lot of critical thinking for them to go back and rethink stuff that they've been assuming about their own practices and the Internet in general for a long time.*

Teachers frequently used discussions and reflection questions. T8 highlighted that they thought that discussion was the best methodology to engage students: *"It fuels the active exchange between the students. And I think it's actually a pretty good way to teach those subjects to get them engaged, to get them to share what they think... and feel kind of comfortable asking about these things."*

Interestingly, the sentiment was that discussion was somehow "*not about school... this isn't about learning*," (T9) or that these discussions would be something that students would respond to differently because they would not see it as a traditional part of their education. This highlights an interesting tension as it suggests that both teachers and their students may frame approaches focused on rote learning and grading as potentially undermining the goal of the lesson. Teachers reported using resources that incorporated stories, role-playing, and scenarios to help their students imagine potential scenarios and how they would respond to them as a means to help students learn about these topics.

4.2.2 "Safe" Topics

Teachers emphasized the importance of making students feel safe in the classroom. As such, they took great pains to create a sense of psychological safety when discussing sensitive topics around cybersecurity and privacy topics. Students may be uncomfortable because these topics are taboo in their households or because they have fears of being judged for their own behaviour. Due to the potentially difficult and in some cases taboo nature of some topics in cybersecurity and privacy, some teachers expressed concern that covering these topics put them at risk of overstepping their professional boundaries, which might result in professional reprisals. An example was the risk of being listed in the "blue pages," a disciplinary mechanic of the College of Teachers where teachers found to be incompetent or guilty of professional misconduct are publicly listed [29].

> *I feel that teachers are not given the full freedom to really provide their best because we are so damn scared of showing our name in the blue pages... with all good intentions I tried to teach all these things that I am teaching now which were not very well accepted eight or nine years ago... I don't feel comfortable talking about it. (T5)*

4.2.3 Relevant and Relatable

The perceived relevance of a resource was of paramount concern for teachers, as they noted their students are quick to reject resources that do not relate to their current interests and experiences. As a result, teachers highlighted the importance of keeping resources up-to-date both in terms of content and

physical design, including well-known stories and technologies relevant to their students' experiences. Further, it should include timely stories and situations relevant to their own experience or local community. T14 shared an experience that highlights this sensitivity:

> *The kids are always very quickly moving on to the next big thing that everybody's using. And I think staying on top of what that is and reflecting that in the resources is really important because we had some group come to do a talk on boundaries and stuff like that and they had Fortnite as one of their slides and all the kids just go up and, you know, Fortnite sucks and blah blah blah. So making sure that it stays relevant to what they're interested in it...*

Multiple teachers reported that they had modernized a resource themselves by changing a referenced technology or game to a more relevant example (e.g., changing a Facebook post to a TikTok post), or by finding widely known news stories, memes, and pop culture references currently popular on social media sites to help build interest and engagement with their students. Teachers also reported looking for resources that had a local focus where possible, whether to discuss a topic that was particularly relevant to their community, or something that they thought their students in particular needed to be aware of.

Teachers were concerned about how relatable the subject matter of the material was to their students. As such, they gravitated to resources that provided a clear rationale for why the lesson is important and how it relates to the experiences that their students have had. Teachers reported that they searched for stories from other young people who had experience with the topic to help communicate the importance of the topic and make it more relatable to their students. We also found instances where teachers gravitated towards resources that included information that their students would find shocking or interesting. As such, some teachers reported looking for resources that referenced highly publicized news stories or resources that incorporated real-life examples. For example, teachers using videos that had information shared by other children around their students' age, which they felt made it especially engaging for their students because it "*might also prompt the other students in the class to talk about their own*" (T4).

4.2.4 Simple, Polished, and Age-Appropriate

Teachers noted that their students are highly sensitive to design in a media-rich environment and are easily turned off by resources that do not align with their expectations. In general, teachers had found that their students preferred resources that looked polished, were not too mature or childish, and used neutral language. For example, T13 described their preferred resource *"as simplistic as possible and not super wordy... And it also needs to look polished... [Kids] are very dismissive... these are kids who are bombarded with media all the time. So, if it looks like it was done ten years ago, they're out."*

Teachers reported gravitating toward games or turning a static resource into an activity to increase engagement. For example, T12 said: "*I would copy, paste this into a little checklist, like go through and check off maybe one thing you learned. You know... it's just a handout. I would turn it into an activity."*

Teachers emphasized the importance of limiting the amount of written content in the resource and also how much writing the resource required students to do. In addition, teachers noted that it was also a deterrent to them. "*... if I'm reading a two-page document to find out what the lesson is"* said T14, *I'm not going to use it*." The tone of the resource should not come across as "*preachy*" (T15) or "*talking down to them*" (T13). Teachers are aware that students may feel judged by a resource that has an overly prescriptive tone and may become defensive and "*tune [it] out*" (T15) as a result.

4.2.5 Non-technical

Surprisingly, teachers had reservations about using resources that require the use of technology in the classroom because it creates many challenges and barriers for teachers. For example, not all schools have the ability to offer a one-to-one ratio of Chromebooks for students to use, which means that students have to share computers. This limited their ability to optimally engage with some type of resource, such as computer games.

Teachers also noted that resources designed with an overly technical focus can make them less usable to teachers. They reported rejecting or making modifications to the resources due to the lack of perceived appropriateness of the resource for their class, such as the correct literacy level whether they had the means to incorporate the resource into their classroom (e.g., number of available tablets to access the resource). Further, resources that required user account registration created significant barriers because having to remember multiple account details and logging in before each lesson is a hassle.

4.2.6 Modular and Adaptable

Teachers reported that they prefer to approach cybersecurity and privacy subjects in a flexible way. Therefore, they preferred resources that provided options to adapt the resource to accommodate their constraints and needs. These included modifying a resource, adjusting the length of the lesson, and making the lessons more accessible without technology.

Materials that included multiple smaller lessons packaged around a topic or educational outcome were preferred. Teachers noted that having multiple topics to choose from was helpful in offering them a "*starting point*" (T10). Further,

they appreciated being able to choose one or two pieces from a package of resources, rather than feeling constrained by a single resource or pressured to use a resource in its entirety.

4.2.7 Trusted and Free

In choosing resources, teachers considered the reputation of the organization making the resource. Their trust in the organization was mainly determined by the professional look of the resource and the website. They also perceived resources recommended by colleagues as more trustworthy. Most used free resources because they do not have a budget through their school to buy materials.

4.2.8 Fit Within Current Practices

Teachers reported seeking resources that they could easily incorporate into their teaching practices and responsibilities, such as how well the material met their curricular needs. Many felt that they did not have enough time to appropriately cover what they already have to teach in the curriculum. As a result, teachers are likely to dismiss resources that do not clearly outline how they connect to the existing curriculum.

Teachers gravitated to resources that clearly outlined the learning objectives and success criteria, noting that this helped them with their administrative responsibilities: "*learning goals is a big thing with our school board,* said T11, *"you have to state what your learning goal is, what your success criteria is...*"

4.3 Assessments

In general, teachers reported using a variety of measurement strategies with their students, although they had clear preferences for the type of assessment. Teachers reported overall positive outcomes from their lessons, but noted the lack of clarity around what effects of their lessons had on their students and the long-term learning outcomes. These concepts around measurement strategies and lesson results are explored further below.

4.3.1 Informal Assessments

The majority of the teachers preferred informal assessment strategies, such as relying on discussions and "*vibes*" (T8) to assess student understanding intead of using formal assessment tools such as quizzes and assignments. They opted for informal methods of assessment because they did not want to create anxiety or stress for their students due to the personal and potentially sensitive nature of cybersecurity and privacy. Assessments could also distract students from the central issue. T9 explained:

> *I don't want to grade a student on their response to something like this, because first of all, a lot of this is sort of opinion and experience-based. So, I can't really grade them on that because that's not part of the curriculum. And then if I grade them on something sort of adjacent like, for example, a written response, and I grade them on their grammar or something, then they're a lot more focused on that than the actual issue.*

Therefore, teachers felt that applying a grade did not represent the best pedagogy for teaching cybersecurity and privacy.

4.3.2 Critical Reflection

Teachers highlighted the importance of reflection in their assessment strategies. As such, they preferred assessments that facilitated critical reflection over those that measured correctness, such as multiple-choice questions. T13 explained:

> *... it's the sheer volume of media that they're consuming. It doesn't allow for reflection. It doesn't allow for you to think. It's just constant. So they don't slow down and think about it very often. And so any time that we can get them to slow down and think about what they're doing it's a win.*

Teachers also emphasized the importance of reflection for young people that extended beyond the classroom.

4.3.3 Short-Term vs. Long-Term Impact

Teachers reported mostly positive reactions to their lessons, but had mixed results when it came to seeing a lasting change in student attitudes and behaviour.

In most cases, teachers noted that their students responded positively to lessons with the immediate result being that students were eager to engage in discussions about these topics. Despite positive short-term engagement, teachers found it difficult to tell if their lessons had a lasting impact on student attitudes and behaviours. T2 noted that their presentations often ended with students self-reporting "*deleting their Facebook account*" or "*keep[ing] their eye out for activities or if their friends are acting strange*." However, T2 and other teachers noted that this was not something they could verify.

Complicating this issue further is that it is becoming increasingly difficult for both teachers and guardians to keep track of the ever-growing number of games and online services that their student have access.

> *It is almost impossible... And you just have to hope that you've laid enough of a foundation by the time they get to that point that they're going to talk to you about it. But in most cases, they don't. And so it's a really powerless feeling... (T13)*

This highlights a unique challenge for teachers: to know when to intervene or whether their lessons are having an impact. As such, this may be a significant contributor to why most teachers reported having a reactive approach to addressing cybersecurity and privacy risks with their students.

5 Creators' Perspectives

The resource creators in our study had experience creating resources covering a wide variety of topics: 88% indicated their resources taught authentication and privacy, and 63% addressed online ethics. Fewer had created materials covering more sensitive topics such as sexting (38%), sexploitation (25%), or pornography and gambling (13%). Most of the creators in our study said that they had experience developing lesson plans (88%), learning modules (88%,) and text-only resources (88%). Some had created animated videos (63%) and web-based games (38%) . Only 25% had experience creating mobile games, comics, and gamified activities.

5.1 Curation

Resource creators shared that their first step in creating a resource is research to help them better understand what contributes to the problem and where there are gaps that their materials need to fill. However, we found that most relied on ad hoc processes to determine the topics they covered and using a variety of sources to gather evidence to support their advice due to a lack of centralized knowledge and funding bodies to support cybersecurity education. C2 noted their process for curating resources:

> *So, the topics were picked based on what the biggest issues for those were. In terms of specific aspects of fraud and things like that, we go to the statistics and we talked to the Canadian Anti-Fraud Center... We try and get an idea of what the larger problems were and then build out units around that. It's very hard to get an idea of what basic cybersecurity is because a lot of the places that provide that kind of information aren't the kind of institutions that can also provide the evidence...*

These quotes highlight how the lack of clarity around the most pressing problems and how best to address them complicates creators' processes for determining appropriate topics and creating evidence-based materials. The fact that there is no centralized place for validated information coupled with a rapidly changing technology landscape makes it harder for creators to engage in efficient processes and risks their providing outdated or outright bad advice.

Organizations, particularly not-for-profits, generally focus on "hot" cybersecurity and privacy topics to attract funding, and funding for the project limited the resources they could create. As C1 explained:

> *It is either what we can attract funding for, or alternately when we consider something to be a priority, we find time to do it. Obviously, that's more practical with something like a tip sheet or a lesson plan than something like a video or something more, that has more hard costs or money out the door. So, what we kind of do is we try to match funding opportunities with things that we want to do, and we do that in a variety of different ways.*

5.2 Processes and Methodologies

Once a project plan or funding was secured, the creators reported a mix of activities, including engaging stakeholders, developing partnerships, bringing in subject matter experts, prototyping, reviewing, and then launching and promoting their products. In several cases, creators also hired translators to convert their materials into French.

While some creators used existing theories and academic practices (*e.g.*, participatory design, Agile, and user-centred design) to inform the development of their resources, others did not follow any established design methodology or framework. For example, C7 explained why they avoided using frameworks in the development of their resources:

> *I probably couldn't name a framework for you. How about that? I was a teacher for 38 years and a curriculum designer and I know there are frameworks for doing that. But you know what we've discovered over the years? Those frameworks get in the way of being productive. And as soon as you say framework, that means, okay, there are rules, this is the way we go. And that really limits these trips to the side that generate some serious fruit. And so what we did, we just went and just everything was on the table. And then we sift through it afterwards.*

In general, creators used broad terms to describe the effectiveness of the resource, such as "engaging", "usable", and "accessible". They spoke of concerns around the explainability and transmissibility of the material, with a focus on making the content understandable to audiences beyond its initial stakeholder group. They also mentioned concerns about knowledge transfer to apply the acquired knowledge to new situations and presenting authentic learning opportunities where students engage their problem-solving skills.

5.3 Design

We found that resource creators acknowledged many of the same high-level factors as teachers when discussing how resources were chosen. Creators discussed optimizing the design of their resources to suit the expectations of the students, such as incorporating modern design aesthetics to capture their interests and engagement during lessons. Further, creators highlighted the importance of age-appropriate design and communication in the design of their materials, many of which matched teachers sentiments. These included ensuring that the materials had "*fun and engaging branding*" (C5) to appeal to students' aesthetic tastes, have minimalist writing to make sure the resource isn't too "*text-heavy*" (C6), to ensure that the resource is at the right literacy level, and provide opportunities to develop skills for *"critical thinking [and] ethical decision-making"* (C1).

Like teachers, creators also acknowledged the importance of stories, analogies, and metaphors as educational tools. To

address this need, creators reported creating resources such as articles, comics, and games with a specific narrative focus. Creators also showed an awareness of the importance of tone in their resources, several highlighting that traditional advice had focused on "*only teaching the bad*" (C3) and understood that there is a growing need to balance negatives with the positives of technology use. Furthermore, one creator noted the importance of not being prescriptive in their advice and seeing their materials as "*a basis for a conversation*" (C2) so as not to shut down the communication channels between young people and educators. Creators were aware of the importance of keeping their materials up-to-date for teachers, despite this being a significant challenge for their organizations due to limited funding and resources.

Overall, the creators highlighted many of the same concerns and considerations as teachers, and generally showed an alignment of understanding with teachers' needs and constraints in the designs of the educational resources.

5.4 Evaluation

Resource creators overwhelmingly reported that teachers and students are difficult to reach or work with due to teachers being "*overwhelmed with the amount of work*" (C4), and students being a vulnerable stakeholder group that requires additional risk management and approval processes. This led to reliance on proxies, such as someone who worked closely with teachers rather than directly working with teachers, or involving teachers only near the end of the design process. C6 shared their struggle:

> *So doing something like, you know, a user-centered design process where the teachers were on the design team was just not in the cards. And we also had decided, you know, that was not something that was needed because we did have people on our team who work very, very closely with these teachers. And so they could kind of be their advocates. And again, they were former teachers... So yeah for the majority of the design process, they were our advocates for the teachers. We were not directly talking to the teachers... So we really started involving teachers at the end when the final product was ready. So when the high-fidelity prototype was completed, that's when I did a study with teachers.*

One risk of involving stakeholders at the end of the process is that it constrains what teachers can offer feedback on and missing important problems or opportunities that needed to be addressed near the beginning of the process.

Creators also wished to improve the measurement of the effectiveness of their resources by conducting more frequent and in-depth evaluations. However, due to limited funding and constraints on their time, the majority of creators do not evaluate their resources or used informal methods, such as soliciting opinions conversationally after presenting their resources to a small group of stakeholders. Furthermore, creators reported that they primarily focused on asking self-reports of behavior change in their evaluations, rather than on learning outcomes. Creators were concerned with their inability to measure whether there were long-term changes in behavior, the ecological validity of the materials they were creating.

6 Discussion

We conducted two qualitative interview studies examining how educational resources for teaching cybersecurity are being used and evaluated by teachers, and how they are being designed and distributed by creators. We interviewed 15 Canadian teachers about their experiences teaching cybersecurity and privacy in the classroom, and 8 creators about their experiences creating cybersecurity resources. We then conducted a thematic analysis of their responses.

From our analysis, we found that teachers were using predominantly lesson-oriented resources in their teaching which they generally found to be effective. Further, their considerations in deciding on resources focused on how well the resources aligned with their teaching needs and how engaging and effective they thought it would be for their students. The interviews further highlighted that teachers are predominantly approaching these topics in a reactive and ad hoc way which impacts their process for finding and choosing resources, and measurement strategies when teaching these topics to their students.

Creator interviews showed that creators had a generally good understanding of what teachers want and need from the resources they are creating. However, when investigating their processes for designing and disseminating their resources, we found inefficiencies as well as a mix of organizational and external constraints that limited their ability to engage in best practices.

6.1 Different Educational Approaches

It quickly became clear in our interviews that teachers were approaching topics in cybersecurity and privacy not from a technical perspective, but from a perspective framed around safety. This shaped what kind of resources they chose, how they approached teaching, and how they evaluated students.

Teachers often described taking a reflective approach to teaching security and privacy, and choosing teaching strategies that emphasized critical thinking and inquiry. Teachers sought to connect the material to students' lived experiences, often by approaching these topics reactively. Teachers frequently described teaching strategies such as class discussions, and emphasized the importance of candidness and students' emotional safety in these discussions. Teachers adapted existing materials to fit these reflective teaching modalities.

Rather than starting with technical strategies and integrating more personal impacts of the material from there, teachers

expressed a preference for using stories and role-play to encourage students to explore the ways in which their digital footprints might affect them. Teachers said that strategies such as scare tactics or presenting shocking information were often good ways to get students engaged in the material, and contrasted these "shock" techniques with maintaining an open and honest rapport with students that would enable honest and safe discussion. This emphasis also led to teachers adapting more technical material to work with their narrative-focused strategies.

Teachers expressed a clear preference for informal assessments for cybersecurity, privacy, and digital literacy topics. Much of this had to do with the style of teaching, and the method of approaching these topics, which did not lend themselves to formalized assignments or quizzes. The majority of teachers preferred informal evaluation strategies, and relied more on discussion, and engagement as metrics for the success. Teachers were clear that the subject matter itself was a source of stress for their students, and were reluctant to compromise or complicate the classroom tensions by adding formal assessment items.

In our interviews, creators rarely brought up these kinds of considerations about what kind of educational approach to take, or framed cybersecurity education as part of a conversation or situation outside of a dedicated lesson. While it is possible that they are aware of them, they did not seem to frame their approach to designing lessons with the same considerations. We suggest that if creators had a greater awareness of the constraints and considerations affecting teachers this could help them create resources that better served these approaches.

6.2 Conflicting Processes

Educators and resource creators approach the same problem from different perspectives: how can cybersecurity topics be best synthesized for delivery to students? However, in analyzing our interview data, we noticed that creators and teachers were approaching their task from different angles. Creators were using a top-down process, starting with trends in cybersecurity topics, funding considerations, and other high-level factors to consider the design of security resources. Teachers were more likely to be starting with bottom-up factors that reflected the realities of their teaching context, such as student safety and curriculum demands.

In our interviews, creators tended to start with more of a blank slate when considering the design and creation of resources. Creators brought up some constraints relating to factors such as funding, but in general, approached the design of resources from a perspective framed around the cybersecurity topics. Once a project plan or funding was formalized, creators reported a mix of activities, including engaging stakeholders, developing partnerships, bringing in subject matter experts, prototyping, reviewing, and then launching and promoting their products. Few of these activities involved direct feedback from teachers or students.

When teachers described how they chose resources, they mentioned a variety of factors. Many of these factors were directly related to emergent events in their classroom: instances of bullying or other conflict, interpersonal relations between students, students' digital lives and presence, events happening in the local community, etc. Teachers were also driven by contextual factors such as curriculum demands, the other material they were teaching, and the time available to them. As a result, teachers were likely to pick and choose pieces of resources, using a bottom-up technique to assemble material that suited these constraints. Their teaching tended to be reactive, rather than proactive, and their resource discovery strategies were broad. Instead of beginning with the resource packages made available through creators, they tended to begin with Google searching. Teachers also described addressing cybersecurity topics in non-technical classes (*e.g.,* health class), often because they afforded the time and discussion needed to approach topics in a way that was customized to teachers' students.

Although teachers expressed few complaints about the resources they were using, it seemed clear that these resources were not particularly created with their constraints in mind. One effect of the mismatch seemed to be that teachers were forced to de-prioritize cybersecurity topics in comparison to other curriculum topics. In our interviews, teachers suggested that having cybersecurity topics explicitly tied into other courses, particularly math and languages, would allow them more opportunities to engage with the material. Because of their reactive approach to teaching cybersecurity and privacy, teachers were in search of materials that they could easily fit into both their current class plan and their curricular mandates. To facilitate this, teachers generally reported using one-off lesson materials rather than resources that required a series of lessons that required building off on previous lessons and which would take multiple classes to cover.

We suggest that a better alignment between these two processes might help the development of resources that are more effective for teachers. Possibly, creators are aware of this mismatch – in our interviews, creators expressed frustration with the lack of communication with teachers and students. However, they also acknowledged the lack of a formal design process and methodology. Using a design process that prioritized direct involvement with teachers at early stages of the projects could help this mismatch, and better influence both the format and content of resources.

6.3 What is Available and What Gets Taught

Another way in which the differences in approach between teachers and creators became apparent was in the design and format of the resources themselves. The resources and materials created and disseminated by creators do not match

teachers' classroom constraints and needs.

Our research suggests that few available cybersecurity resources are taught to students in the classroom due to their incompatible formats or lack of flexibility in adapting the material to classroom teaching. We found that teachers relied mainly on lesson plans, short live-action and animated videos, and learning modules to teach cybersecurity and privacy. However, previous research [39] has found that most of the available cybersecurity educational tools are games and videos. Learning modules represent only around 8% of all available resources, and lesson plans are usually supplementary material to support other types of multimedia learning (but are not always available) [39]. We found that resources such as tabletop games, mobile games, comics, and gamified activities were rarely used by our teacher participants. While computer games were sometimes used for teaching purposes, creators may be overestimating their usefulness in classroom environments compared to other non-interactive material like text-only resources, which we found to be used almost as often as games.

Creators and teachers are key stakeholders in determining *what* and *how* cybersecurity and privacy topics should be taught. As curators of learning resources, resource creators communicated a lack of guidance on what cybersecurity problems should be prioritized, leading to confusion about what topics to cover. We also found that the topics creators support are sometimes constrained by lack of funding opportunities to support the development of the learning resource. Therefore, the disseminated resources may not always address security and privacy issues faced by children and youth on the ground or align with the topics that teachers need to cover in the classroom. Creators referenced blind spots in the development process, such as who they are designing for and the underlying need the material is trying to address. "*We'll just use the phishing example because most of the time we get requests around how do students be more aware of malicious attacks or phishing,*" C5 declared, "*But then we don't really understand who is this going to... what are the students really experiencing? How are they digesting that information? ...*" We found that creators' resource development efforts focus on design considerations to make resources more attractive and engaging for young people, which could lead creators to develop certain types of resources over others, such as games and videos [39]. Other stakeholder perspectives are also present in the design process, such as that of school boards and funding bodies, but our interviews suggest that creators were prioritizing the learning needs of their primary audience (i.e., children and young people), but the need to support teachers was usually not considered until the end of the design process (if at all).

Compared to creators, we found that teachers prioritized suitability to their teaching needs in conjunction with the learning needs of their students. For example, teachers sought resources that could easily fit into their current teaching plan and curricular mandates. To facilitate this, teachers generally reported using one-off lesson materials rather than scaffolding a series of lessons that could take multiple sessions to cover. Our results also suggest that teachers may deliberately avoid teaching certain topics that they consider sensitive and uncomfortable, such as sexting, or technical topics on which they lack expertise. This indicates that more careful curation of topics from creators is required to support teachers' needs. Our interviews suggest that simple, flexible, and modular resources like short videos, adaptable learning modules, and lesson plans for facilitating classroom discussions are easier to use by teachers than resources that require more complicated setups and time commitment. A closer relationship between teachers and creators in the design phase would likely help address many of these issues.

7 Conclusion

As online resources are entangled more and earlier into childrens' lives, the importance of effective education in cybersecurity and privacy continues to grow, bringing with it the need for well-designed and effective resources for teaching these topics. In this work, we explored how existing resources align with the needs of teachers using them. We conducted two qualitative interview studies with 15 teachers and 8 resource creators. We found that teachers approached cybersecurity and privacy from a safety-oriented rather than a technical perspective and often did so as an ad hoc reaction to external events in the classroom, school or community. As a result, they preferred informal assessment strategies like facilitated discussions over formal assessment methods like tests. Resource creators generally had a good understanding of the learning needs and interests of their students, but generally did not prioritize their design considerations of the resources for teachers' delivery of the material in the classroom. As a result, our findings suggest that teachers access and use only a small portion of the cybersecurity educational content available to instruct children due to their rigid and incompatible formats to adapt the material for classroom teaching. Specifically, computer and mobile games—the most widely available type of cybersecurity educational resource—are rarely used in classroom teaching contexts. In contrast, teachers are more likely to use modular lessons that can be easily adjusted to their teaching using resources such as lesson plans, short instructional videos, and segmented learning modules. We suggest that better integration of the factors affecting teachers into the resource creator processes could enable more flexible lessons that are more widely applied in the classroom, resulting in better knowledge of cybersecurity and privacy for students.

8 Acknowledgments

L. Zhang-Kennedy (RGPIN-2022-03353) and E. Stobert (RGPIN-2020-06574) acknowledge support from the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grants. The authors thank the teacher and creator participants for sharing their valuable insights and experiences.

References

[1] Media Education in Ontario. https://mediasmarts.ca/teacher-resources/digital-media-literacy-outcomes-province-territory/media-education-ontario, Jan 2012. 2022-04-15.

[2] Canadian Cybersecurity Awareness Stakeholders Teleconference Report. https://www.serene-risc.ca/public/media/files/prod/page_files/27/SETA-Conference-Report-FINAL.pdf, January 2020. 2022-03-12.

[3] Cybersec 101. Cybersec101. https://www.cybersec101.ca, 2016. 2022-06-22.

[4] Osman Sirajeldeen Ahmed, Saeed Ameen Nasef, Alaa Zuhir Al Rawashdeh, and Mohd. Elmagzoub Eltahir. Teacher's awareness to develop student cyber security: A Case Study. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(10):5148–5156, 2021.

[5] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[6] Kara Brisson-Boivin. The Digital Well-Being of Canadian Families. Media Smarts, 2018.

[7] David Byrne. A worked example of Braun and Clarke's approach to reflexive thematic analysis. *Quality & Quantity*, 56(3):1391–1412, 2022.

[8] Wen-Yen Chiu and Hsuan-Fu Ho. Time to Educate the Educators: An Evaluation of Cyber Security Knowledge Awareness and Implementation for School Teachers in Taiwan. In *Proceedings of International Conference on Technology and Social Science (ICTSS 2019)*. Atlantis Press, 2019.

[9] Common Sense Education. Compliance training: Protecting student privacy for teachers, 2023.

[10] Isabella Corradini and Enrico Nardelli. Developing Digital Awareness at School: a Fundamental Step for Cybersecurity Education. In *International Conference on Applied Human Factors and Ergonomics*, pages 102–110. Springer, 2020.

[11] Katie Davis and Carrie James. Tweens' conceptions of privacy online: Implications for educators. *Learning, Media and Technology*, 38(1):4–25, 2013.

[12] Facebook. Youth Portal. https://www.facebook.com/safety/youth. 2022-07-17.

[13] Google for Education. Teach and Learn Practical Digital Skills - Applied Digital Skills. https://applieddigitalskills.withgoogle.com, 2022. 2022-07-17.

[14] KnowledgeFlow Cybersafety Foundation. Curriculum Creation | KnowledgeFlow Cybersafety Foundation. https://knowledgeflow.org/solution/curriculum-creation. 2022-07-18.

[15] Google. Be Internet Awesome. https://beinternetawesome.withgoogle.com. 2022-07-17.

[16] Tea Hadziristic. *The State of Digital Literacy in Canada: A Literature Review*. Brookfield Institute for Innovation Entrepreneurship Toronto, Canada, 2017.

[17] Michael Hoechsmann and Helen DeWaard. USE, UNDERSTAND & CREATE: A Digital Literacy Framework for Canadian Schools. 2022-03-12, 2015.

[18] Annalise Huynh and Nisa Malli. *Levelling up: The quest for digital literacy*. Brookfield Institute for Innovation Entrepreneurship, June 2018.

[19] iKeepSafe. Data Privacy in Education: An iKeepSafe educator training course, 2016.

[20] Carrie James, Emily Weinstein, and Mendoza Kelly. Teaching Digital Citizens in Today's World: Research and insights behind the Common Sense K–12 Digital Citizenship Curriculum. 2022-07-14, 2021.

[21] Giti Javidi, Ehsan Sheybani, and Zacharias Pieri. A Holistic Approach to K12 Cybersecurity Education. In *Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS)*, pages 77–80. ProQuest, 2019.

[22] Priya C. Kumar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. Privacy and Security Considerations for Digital Technology Use in Elementary Schools. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13. ACM New York, NY, USA, May 2019.

[23] Sana Maqsood. *The Design, Development, and Evaluation of a Digital Literacy Game for Preteens*. PhD thesis, Carleton University, Ottawa, January 2020.

[24] Sana Maqsood and Sonia Chiasson. "They think it's totally fine to talk to somebody on the internet they don't know": Teachers' perceptions and mitigation strategies of tweens' online risks. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–17. ACM New York, NY, USA, 2021.

[25] Florence Martin, Tuba Gezer, and Chuang Wang. Educators Perceptions of Student Digital Citizenship Practices. *Computers in the Schools*, 36(4):238–254, 2019.

[26] Common Sense Media. Common Sense Media: Age-Based Media Reviews for Families | Common Sense Media. https://www.commonsensemedia.org. 2022-07-17.

[27] Microsoft. Digital literacy courses, programs and resources | Microsoft Digital Literacy. https://www.microsoft.com/en-us/digital-literacy. 2022-07-17.

[28] James Nicholson, Julia Terry, Helen Beckett, and Pardeep Kumar. Understanding Young People's Experiences of Cybersecurity. In *European Symposium on Usable Security 2021*, pages 200–210, 2021.

[29] Ontario College of Teachers. Discipline Decisions | Ontario College of Teachers. https://www.oct.ca/public/complaints-and-discipline/decisions. 2022-10-19.

[30] Teaching Privacy. Teaching Privacy. https://teachingprivacy.org. 2022-06-07.

[31] Portia Pusey and William A. Sadera. Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. *Journal of Digital Learning in Teacher Education*, 28(2):82–85, 2011.

[32] Farzana Quayyum, Daniela S. Cruzes, and Letizia Jaccheri. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30:100343, 2021.

[33] Nurul Amirah Abdul Rahman, Izzah Hanis Sairi, Nurul Akma M. Zizi, and Fariza Khalid. The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology*, 10(5):378–382, 2020.

[34] Teaching Security. Teaching Security. https://teachingsecurity.org. 2022-07-18.

[35] Media Smarts. Media Smarts | Teacher Resources. https://mediasmarts.ca/teacher-resources, November 2011. 2022-06-20.

[36] Student Privacy Compass. Student privacy training for educators, 2023.

[37] Leah Zhang-Kennedy, Khadija Baig, and Sonia Chiasson. Engaging Children about Online Privacy through Storytelling in an Interactive Comic. In *Electronic Visualisation and the Arts (EVA 2017*, pages 1–11, July 2017.

[38] Leah Zhang-Kennedy, Robert Biddle, and Sonia Chiasson. Secure Comics: An Interactive Comic Series for Improving Cyber Security and Privacy. In *Proceedings of the 31st British Computer Society Human Computer Interaction Conference*, Swindon, GBR, 2017. BCS Learning & Development Ltd.

[39] Leah Zhang-Kennedy and Sonia Chiasson. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys (CSUR)*, 54(1):1–39, 2021.

[40] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. The Role of Instructional Design in Persuasion: A Comics Approach for Improving Cybersecurity. *International Journal of Human-Computer Interaction*, 32(3):215–257, February 2016.

9 Appendix A: Teacher Pre-Interview Questionnaire

1. What is your gender? *[Multiple choice] (Male, Female, Self-identify [textbox])*
2. What is your age bracket? *[Multiple choice] 20–29, 30–39, 40–49, 50–59, 60+*
3. What did you study in university? *[Textbox]*
4. How long have you been teaching? (in years) *[Textbox]*
5. What subjects have you taught? *[Textbox]*
6. What grade(s) do you teach? *[Textbox]*
7. Where do you teach? (e.g., School name and district) *[Textbox]*
8. What technologies do you use in the classroom? *[Textbox]*
9. Have you ever helped a student deal with a digital literacy or cybersecurity issue? (e.g., cyberbullying, accidentally sharing personal information) *[Multiple choice] Yes, No*
   (a) If yes, please describe the incident (without identifying the student) *[Textbox]*

10. Have you used any educational resources designed to help you teach principles of cybersecurity and privacy in your classroom? *[Multiple choice] Yes, No*

    (a) If yes, please describe what resource you have used and who created it (e.g., MediaSmarts, Teachers-PayTeachers, a colleague, etc.) *[Textbox]*

11. How would you rate your comfort with teaching the following cybersecurity and privacy factors to your students? *[Likert scales: 5 = very knowledgeable, 1 = not at all knowledgeable] General cybersecurity (spoofing, malware, pharming, passwords), E-safety, E-privacy, Digital citizenship and literacy, Data security, Phishing, Network security, Software security*

12. Do you have any comments about the previous question you would like to share? *[Textbox]*

13. What are some of the types of educational resources you used in the past for teaching cybersecurity? *[Multiple answer-multiple choice] Games (web-based or computer games), Games (Apps on mobile devices), Games (Non-digital board or tabletop games), Videos-Films, Videos-Animations, Learning modules, Comics, Text-only resources, Gamified activities (e.g., role-playing), Lesson Plans, Other (Please specify)*

    (a) For each checked resource, please list the name of the sources and include links to the resources if possible. *[Textbox]*

14. What areas are you knowledgeable about in cybersecurity and privacy? *[Likert scales: 5 = very knowledgeable, 1 = not at all knowledgeable] Authentication, Cyberbullying, Cybersecurity (software threats, spam, scams, fraud, identity theft), Extensive Internet Use, Gambling, Online Hate, Online Ethics, Online Marketing, Privacy, Pornography, Sexual Exploitation, Sexting, Other*

15. What digital issues have you taught? *[Multiple answer multiple choice] Authentication, Cyberbullying, Cybersecurity (software threats, spam, scams, fraud, identity theft) Extensive Internet Use, Gambling, Online Hate, Online Ethics, Online Marketing, Privacy, Pornography, Sexual Exploitation, Sexting, Other*

10 Appendix B: Creator Pre-Interview Questionnaire

1. What is your gender? *[Multiple choice](Male, Female, Self-identify [textbox])*

2. What is your age bracket? *[Multiple choice] (20–29, 30–39, 40–49, 50–59, 60+)*

3. What organization do you work for?*[Textbox]*

4. Please indicate the type of organization you work for: *[Multiple choice] Private sector (e.g., business), Public sector (e.g., government, academic institutions), Not-for-profit, Other (please specify)*

5. How many employees are at your organization? *[Multiple choice] 1–9, 10–49, 50–99, 100–499, 500–999, 1,000–4,999, 5,000–9,999, 10,000+, Don't know*

6. What is your most recent job title? *[Textbox]*

7. What is your highest level of education? If you are currently in school, please choose the degree that you are enrolled in. *[Multiple choice] Less than a high school degree, High school degree or equivalent, College degree, Bachelor's degree, Master's degree, Doctoral degree, Other professional degree*

8. What did you study in university? *[Textbox]*

9. Does what you study in university relate to your work as a creator of these resources?

    (a) If yes, how so? *[Textbox]*

    (b) If no, where did you learn the skills related to your work? *[Textbox] (For example, cybersecurity, privacy, and instructional design)*

10. How long have you been creating these sorts of resources? (Professionally or otherwise) *[Textbox]*

11. What are some of the types of educational resources you helped to create in the past for teaching cybersecurity? *[Multiple choice multiple answer] Games (web-based or computer games), Games (Apps on mobile devices), Games (Non-digital board or tabletop games), Videos-Films, Videos-Animations, Learning modules, Comics, Text-only resources, Gamified activities (e.g., role-playing), Lesson Plans, Other (Please specify)*

12. For each checked resource, please list the name of the sources and include links to the resources if possible. *[Textbox]*

13. What digital issues do the educational resources you helped to create address? *[Multiple choice multiple answer] Authentication, Cyberbullying, Cybersecurity (software threats, spam, scams, fraud, identity theft), Extensive Internet Use, Gambling, Online Hate, Online Ethics, Online Marketing, Privacy, Pornography, Sexual Exploitation, Sexting, Other*

14. What areas are you knowledgeable about in cybersecurity and privacy? *[Likert scales: 5 = very knowledgeable, 1 = not at all knowledgeable] Authentication, Cyberbullying, Cybersecurity (software threats, spam, scams, fraud, identity theft), Extensive Internet Use, Gambling, Online Hate, Online Ethics, Online Marketing, Privacy, Pornography, Sexual Exploitation, Sexting, Other*

11 Appendix C: Teacher Interview Guide

Teaching Practices

1. How long have you been teaching cybersecurity and privacy topics to your students?
2. Have you done any professional development in cybersecurity or privacy through your school, and if so, can you describe what was involved?
3. Have you done any professional development in cybersecurity or privacy through your school, and if so, can you describe what was involved? If not, why not?
4. Please describe your most recent experience teaching cybersecurity or privacy to your students.
   (a) Why did you decide to teach this particular lesson? (What precipitated the need to cover this topic?)
   (b) What grade were these students when you taught this material?
   (c) How did they react to the lesson?
   (d) Did you see changes in the behaviour or attitudes of your students after the lesson?
5. What strategies do you use to engage your students with these topics in the classroom?
6. How else is privacy and security being addressed in your school?

Resource Selection, Effectiveness, and Experience

1. What I would like you to do now is walk me through how you would go about finding and choosing a lesson or resource for teaching cybersecurity and privacy to your students.
   (a) What are your considerations for choosing a resource?
   (b) Where do you start your search?
2. Now I would like you to show me the 1 or 2 resources you have been using in teaching cybersecurity and privacy to your students and then I'd like to ask you a few questions about them.
   (a) How did you first learn about "X" resource? (web page, lesson plan, etc.)
   (b) What concept(s) does this resource teach?
   (c) How long have you been using "X" resources to teach this concept?
   (d) Why did you choose this particular resource to teach this concept?
   (e) What is it about this resource that you like?
   (f) Do your students seem to be engaged when you use this resource?
      i. If yes, what do they seem to like about it?
      ii. If no, what seems to impede their engagement?
   (g) What part of the design do you think make the resource particularly effective for learning about cybersecurity or privacy?
   (h) Does this resource have a teacher's facilitation guide or any support material to help explain to you how to teach it? If yes: Do you use it?
   (i) How do you incorporate the resource in your teaching? For example, have you made any modifications to the resource to make it work better for you?
      i. If you made changes, what changes did you make?
   (j) Is there an assessment component to this resource?
      i. If yes, do you use the assessment?
      ii. If not, how do you measure the effectiveness of the resource?
   (k) Are there things about this resource that you dislike or feel could be improved? If yes, how so?
3. Do you have any other feedback you would like to share?

12 Appendix D: Creator Interview Guide

Background Questions

1. Can you describe the type of work you do relating to cybersecurity education?
2. Can you describe the types of resources you helped to create and the target audience?

Process for Resource Development and Dissemination

1. Can you describe for me what types of educational resources you create?
2. Do these include supporting materials like teaching guides and assessments?
3. How do you decide what topics to base your materials on (what topics should tweens need to know)?
4. Please walk me through your organization's design process for developing cybersecurity and privacy-related educational resources.

5. Can you describe the design methodologies and/or frameworks that your organization uses for developing educational resources? (e.g., user-centered design, agile, participatory design)
6. What are the types of stakeholders you engage within the design process (e.g., privacy experts, end-users, teachers, interaction designers, developers, content writers)?
7. When and how do you engage your stakeholders during the design process?
8. Do you measure the success of your resources? (e.g., the popularity of your resources via analytics, usability testing)?
    (a) If yes, what types of data do you collect?
    (b) If yes, is there anything from the data that surprised you?
9. Do you evaluate your educational resources with teachers and students?
    (a) If yes, please describe your process and methodology for doing the evaluation.
    (b) If yes, broadly speaking, what have your results been of your tests?
    (c) Where do you feel there are opportunities for improvement in your evaluation processes?
10. Have you gotten unsolicited feedback from educators after they've used one of your resources?
    (a) If yes, what sorts of things did educators highlight in their feedback?
11. What are things you wish you knew when designing these materials?
12. What is the process for disseminating or deploying these educational resources to teachers, administrators, and students when they are done?
13. Do you have a formal communications plan?
14. How do teachers, school administrators, and students find your educational resources (e.g., browsing, direct search, recommendations, curriculum)?
15. Are there specific support or resources for helping teachers adapt the educational resources for classroom use (e.g., teaching guide)?

Improvements and Recommendations

1. What do you like about your process for creating these resources?
2. Where do you feel there is room for improvement?
3. What is one thing you would like to find out from my interviews with teachers?
4. What are your design recommendations for designing security and privacy educational tools for tweens?
5. What are your design recommendations for creating support materials for teachers to facilitate the use of cybersecurity educational tools in the classroom (E.g., teacher's guide, activity guide)?