# The design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens*

SANA MAQSOOD, Carleton University, Canada
SONIA CHIASSON, Carleton University, Canada

Tweens are avid users of digital media, which exposes them to various online threats. Teachers are primarily expected to teach children safe online behaviours, despite not necessarily having the required training or classroom tools to support this education. Using the theory of procedural rhetoric and established game design principles, we designed a classroom-based cybersecurity, privacy, and digital literacy game for tweens, that has since been deployed to over 300 Canadian elementary schools. The game, *A Day in the Life of the JOs*, teaches children about 25 cybersecurity, privacy, and digital literacy topics, and allows them to practice what they have learned in a simulated environment. We employed a user-centered design process to create the game, iteratively testing its design and effectiveness with children and teachers through five user studies (with a total of 63 child participants and 21 teachers). Our summative evaluation with children showed that the game improved their cybersecurity, privacy, and digital literacy knowledge and behavioural intent, and was positively received by them. Our summative evaluation with teachers also showed positive results. Teachers liked that the game represented the authentic experiences of children on digital media and that it aligned with their curriculum requirements; they were interested in using it in their classrooms. In this paper, we discuss our process and experience of designing a production quality game for children, and provide evidence of its effectiveness with both children and teachers.

CCS Concepts: • **Security and privacy → Social aspects of security and privacy**.

Additional Key Words and Phrases: usable security, usable privacy, user education, educational game, tweens, teachers, classrooms

**ACM Reference Format:**
Sana Maqsood and Sonia Chiasson. 2021. The design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens. *ACM Trans. Priv. Sec.* 37, 4, Article 1 (June 2021), 36 pages. https://doi.org/10.1145/3469821

## 1 INTRODUCTION

Children use the internet to engage in activities central to their identity and cognitive development, such as expressing themselves online, fostering meaningful relationships, communicating with friends, and exploring their interests and hobbies [36, 60]. While beneficial to children's development and well-being, the internet also exposes them to various online risks such as phishing, cyberbullying, exposure to age-inappropriate content, misinformation, and privacy violations [36, 71]. Attackers are leveraging children's developing cognitive skills to design attacks specifically targeted at apps and platforms used by them [4, 5, 13, 17, 59]. For example, the *AdultSwine* malware displayed pornographic content on 60 child-friendly apps on Google Play [13].

*Portions of this paper appear in the *Proceedings of the ACM Conference in Interaction Design and Children (IDC, 2018)*, Maqsood et al. [41].

Authors' addresses: Sana Maqsood, sana.maqsood@carleton.ca, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario, Canada, K1S 5B6; Sonia Chiasson, chiasson@scs.carleton.ca, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario, Canada, K1S 5B6.


Manuscript submitted to ACM

Given these risks, various multimedia educational tools, such as games and interactive comics have been designed to improve children's mental models of security and privacy and develop their critical thinking skills [32, 75]. Most of these tools have been designed for the home. However, the inclusion of cybersecurity in K-12 curriculum [42, 47, 54–58] means that teachers often have the primary responsibility for educating children about these issues. Thus, there is a need to improve teachers' own awareness of cybersecurity and to provide them with the appropriate training tools for children [35, 61]. This has become even more important with the recent increase in cyberattacks on schools, such as Zoom bombing and ransomware, due to Bring-Your-Own-Devices (BYOD) policies and remote learning [3, 21, 23, 30, 53, 73, 74]. Thus, improving teachers' and children's awareness of cybersecurity not only keeps them safe, but also protects the school's infrastructure from cyberattacks involving end users (e.g., a user accidentally accessing a phishing URL).

Addressing this need, we developed a web-based cybersecurity, privacy, and digital literacy game for tweens -— children aged 11 to 13 years —- in collaboration with our educational partner, MediaSmarts, a national not-for-profit charitable organization which has promoted digital and media literacy in Canada for nearly 30 years [48]. Influenced by the theory of procedural rhetoric, we designed the game so that it nudges players towards the desired security and privacy behaviors and attitudes. *Procedural rhetoric* states that an argument or claim (rhetoric) should be embedded in the mechanics of a game so that players discover the rhetoric by playing the game [9]. We chose this as the underlying theoretical principle of our game because of its experiential nature. This is especially important for security and privacy, where the environment and risks are continually evolving. Tweens must be able to recognize threats or risky situations that they may never have encountered and reason about the best course of action. This skill requires significant vigilance and awareness that comes from experience. A game using procedural rhetoric can help with providing some of this experience.

Topics addressed in the game include cyberbullying, data privacy, online reputation, privacy and ethics, and verifying the veracity of information online. We used an iterative approach to design the game, frequently evaluating it with both children and teachers, through a total of five empirical user studies (with a total of 63 child participants and 21 teachers). Our last two studies showed that the game was positively received by children and teachers, and was effective at improving their cybersecurity, privacy, and digital literacy knowledge. Teachers were also interested in using the game in their classrooms, as it met their curriculum needs and they could easily incorporate it into their lessons using a strategy that matched their individual teaching style. The game, *A Day in the Life of the JOs* [8, 49], is available to schools in both English and French, and accessible on Desktop and iPads. Following the research presented in this paper, the game has since been adopted by 30 school districts, deployed in over 300 Canadian elementary schools, and an additional 35 school districts are currently previewing the game for use within their respective schools. Our educational partner has received positive feedback from schools currently using the game. For example, one school administer stated *"The scenarios are great and certainly reflect our students' realities online"*.

Our work makes the following main contributions:

(1) The design and development of a production-quality cybersecurity game with real world impact.
(2) Empirical evidence of the effectiveness of a cybersecurity game with both children and teachers, through a comprehensive set of user studies. Very few cybersecurity games are actually tested with end users, so there is little evidence on whether they are effective at improving users' cybersecurity and privacy mental models [75]. Those that are evaluated, usually only involve users at the end of the design process [75]. We involved users throughout the design process and also tested the effectiveness of the game, through five lab-based user studies.

(3) A demonstration of procedural rhetoric as a framework for designing cybersecurity, privacy, and digital literacy games. While procedural rhetoric has been used to design educational games, our work is the first to apply it to cybersecurity education. Not much work has critically examined the effectiveness of procedural rhetoric, so we also attempt to fill this gap in the literature.
(4) Insights into how teachers can use cybersecurity games in classrooms, and what they need from these resources.

## 2 RELATED WORK

### 2.1 Security and privacy educational games

From a pedagogical perspective, games are ideal for security and privacy education, because they naturally provide an environment for users to safely practice different behaviours, and to develop their critical thinking and reasoning skills in relation to technology use. Given this, in the past 15 years, academic, non-profit, and for-profit organizations have all designed games to educate adults, professionals, and children about a wide range of security and privacy issues, including online safety, phishing, digital citizenship, data security and network security [75]. Those designed for children are focused on digital citizenship, privacy, and online safety [75]. For example, in DataK, players help the mayor of the fictional town Dataville make decisions which have consequences on the privacy of the town's citizens [70].

While many games have been designed for security and privacy education, few have been evaluated with users to assess their usability and effectiveness [75]. Of the 54 games reviewed by Zhang-Kennedy and Chiasson, only 33% had been evaluated with users. Most of the evaluated games were developed by academic researchers and have not seen wide deployment [75]. The evaluation methodologies varied in rigour, and most assessed learning only with a post-test, without establishing baselines using a pre-test [75]. Thus, the empirical effectiveness of games at meeting their educational goals remains largely untested.

In Zhang-Kennedy and Chiasson's review, only three games were designed for classroom use [14, 29, 72]. While two of these provide accompanying teacher guides, there is no evidence that these games were evaluated with children or teachers. In addition, most have been archived or removed, possibly due to being outdated. This highlights an ongoing challenge of designing cybersecurity educational tools, which quickly become outdated due to the rapid evolution of technology, online risks, and cyberattacks. Addressing this issue, Zhang-Kennedy and Chiasson recommend designing cybersecurity educational tools with high adaptability, so they can be easily updated with new cybersecurity information, at a relatively low cost, with minimal disruptions to end users [75].

### 2.2 Game design principles and frameworks

*2.2.1 Meaningful play.* Motivated learners spend more time and effort on the learning activity, which leads to better outcomes [31, 38, 39, 63]. To motivate learners, Salen and Zimmerman [65] recommend creating games that allow players to engage in meaningful play, which emerges from their interaction with the game and their context of play. For example, players playing a chess game on their own (i.e., arbitrarily moving the game pieces) have a less meaningful play experience than those engaged in a match with another player. In both cases, players are interacting with the game, however, their interactions in a match have a purpose which leads to a more meaningful play experience [65]. The choices available in a game also contribute to players' experience, and all choices offered should affect the game state in some manner [65] in order to be meaningful. The outcome of each action should be clear to the player, so they can use it to create new meanings in the game. Finally, the relationships between actions and outcomes should be discernible and integrated into the larger context of the game [65].

*2.2.2 Gee's principles for learning games.* By analyzing the engaging aspects of popular entertainment games, Gee found that games provide experiential learning (i.e., learning by doing), which is more fun and effective compared to passive learning (i.e., learning facts) typically offered in schools [24, 25]. In the context of security and privacy, passive learning provides children advice on how to stay safe online. While knowing these facts is important, they are insufficient when children actually face dangerous situations online. In these cases, active learning, where students are allowed to practice being in these situations, is a more effective. Based on his work, Gee proposed 36 learning principles for designing engaging classroom learning environments, utilizing the effective learning techniques in games [25]. He also proposed 16 learning principles that he observed exhibited by good games [27].

*2.2.3 Procedural rhetoric.* Bogost [9] defined procedural rhetoric as the practice of using processes or mechanics to construct an argument in a game. It is useful in educational games which make a statement to the player [9]. Games employing procedural rhetoric make their argument by embedding it within the rules of the game. As players interact with the simulated game world, they progressively discover the argument presented by the game. The power of procedural rhetoric is that players are more likely to believe an argument if they experience it for themselves in a simulation, compared to being told about it. Procedural rhetoric has been used to design behaviour change games for homelessness [64], understanding Attention Deficit Hyperactivity Disorder (ADHD) [28], energy conservation [18], and healthy eating [22]. In Fitter Critters, a game to teach children healthy eating habits, players care for a virtual pet. They make choices affecting the health of the pet, and consequently learn about health and nutrition. Each choice has both positive and negative effects on the pet's well being, so players learn which choices are most beneficial [22]. A study showed that it was positively received by children and resulted in increased nutrition knowledge, positive attitudes toward healthy eating, and healthy eating self-efficacy [66]. Based on their experience of designing this game, Ferrara proposed the following guidelines for designing games using procedural rhetoric [22]:

- **P-G1: Defining a core message for the game.** The game must be designed around a clear and concise statement of what the players should do or believe.
- **P-G2: Offering meaningful choices.** Meaningful choices should be offered, and there should be benefits to making the least ideal choice, which will foster exploration and discovery.
- **P-G3: Enabling self-directed discovery.** The game should allow self-directed discovery of the message, which will give players a feeling of ownership and insight.
- **P-G4: Tying the message to strategy.** Games with the goal of winning should embed the message into the winning strategy, which will drive players efficiently towards the message.
- **P-G5: Keeping the simulation realistic.** The simulation should be realistic, giving it credibility and allowing players to apply the learned behaviour in the real-world.

We use these guidelines as the basis of our security and privacy game. While previous work shows that procedural rhetoric is effective for designing behaviours change games for different domains, it has not yet been used to design security and privacy educational games for classroom use.

## 3 *A DAY IN THE LIFE OF THE JOS* GAME

We designed a game to educate 11-13 year old children about cybersecurity, privacy, and digital literacy issues. Our educational game had the following learning objectives:

(1) Improve tweens' understanding and knowledge of cybersecurity, privacy, and digital literacy issues.


**Fig. 1.** Main screen of *The JOs* game

(2) Develop tween's critical thinking skills about novel situations that they may face online, especially on social media, as most will likely have social media accounts soon.

To meet our learning objectives, we used procedural rhetoric to create a game that provides an active learning environment for children. Our goal was to create a game that allows children to explore, practice different strategies, and learn from their experiences.

### 3.1 Overview

The main message of our game is that *life with digital media is complex, and the correct behaviour is not always clear. However, we have choices and the choices we make have consequences (good or bad) on our personal and digital lives* (P-G1). Given this, we used a-day-in-the-life approach to design our game, where players follow the main characters of Jo and Josie through a series of events in their daily life and help them make smart decisions online. The main characters are avid social media users, and reflect our target audience who are digital natives and use multiple electronic devices in their daily lives. By playing the game, children are able to see possible consequences of their choices in a simulation before they make them in the real world.

Since the game is meant to be used in classrooms, an additional constraint was to keep it short so that it can be completed as part of a lesson (typically lasting under 60-minutes) and foster discussion among students. It also needed to have measurable educational goals which can be used by teachers to evaluate students' performance. In collaboration with us, our educational partners specified the target audience, identified educational topics, and created scripts for the game.

Figure 1 shows the opening screen of our game, where the calendar represents a typical school month for the player. The game has five days which are active in the calendar and are highlighted in red. Days with a dark grey background have been completed by the player. As detailed in Table 1, each day addresses a different cybersecurity, privacy, and digital literacy topic, and includes five scenarios covering different aspects of the topic (for a total of 25 implemented scenarios – Appendix A). A short introduction and instructions on how to play the game are provided. To begin, players


**(a)** Introduction screen

**(b)** Middle screen

**(c)** Choices screen

**(d)** Newsfeed showing the consequences

**Fig. 2.** Scenes in a scenario of the game.

select a day from the calendar which directs them to the main screen for that day. The visual design is different for each day, reflecting the topic addressed by the day, and the page links to five related scenarios. Each scenario shows Jo or Josie in a situation where they require the player's help in deciding how to behave safely.

Figure 2 shows a scenario in the game. The first two screens present the scenario to the player. After viewing the scenario, the player is presented with three choices and has to decide what Jo/Josie should do. For example, in this scenario Josie takes a picture of a friend without her permission and wants to post it on social media. The player must help her decide what she should do in this situation. After making a choice, the player immediately see the consequences of their choice in the newsfeed component, which acts as an aggregator of the characters' digital media platforms. A score helps the player keep track of how well they are doing in terms of making privacy-conscious choices.

### 3.2 Detailed functionality of the game

In this section, we provide details of the different components in our game such as the scenarios, choices, newsfeed, scoring, feedback, and the characters. We briefly discuss these in terms of how they fit with procedural rhetoric theory. Details on the application of procedural rhetoric and other relevant game design principles is provided in Section 3.4.

*3.2.1 Scenarios.* Composed of text and graphics, scenarios are presented via a series of animations. The scenarios are quite diverse, for example Josie working with a friend in science class, or the siblings playing an online game with friends. Scenarios within a day must be completed in temporal order. Progress is automatically saved when a scenario is completed, so players can return to the game later. Players can replay completed days, which is useful if they want to see the outcomes of different choices. When replayed, the score and content of the newsfeed are adjusted accordingly.

| Day | Scenarios |
|---|---|
| Cyberbullying | Spreading rumors, dealing with online bullies, and dealing with embarrassing photos. |
| Data privacy | Providing data to apps, deleting online data, location tracking, phishing, and targeted advertising. |
| Online reputation | Controlling audiences for media, dealing with unwanted photos, dealing with the pressure to share personal content, preventing online impersonation, and managing online reputation. |
| Privacy and ethics | Sharing others' personal information or content (e.g., photos, videos) without their consent, and understanding copyright. |
| Fact checking | Verifying the authenticity of information on social media, wikis, and websites, recognizing bias and loaded language, and recognizing commercial content. |

**Table 1.** Cybersecurity, privacy, and digital literacy topics addressed by the game

We spent significant effort into devising realistic, relatable scenarios so that children are engaged and invested in the game outcomes (P-G5) [22, 44]. When children are able to see themselves in situations presented in the game, they are more likely to learn from them and apply the learned material to situations outside of the game [7, 44, 51]. Some scenarios had the main characters engaging in negative behaviours (e.g., sharing someone's photo without permission). To make these scenarios relatable, we framed them to represent situations where the characters accidentally engaged in the behaviour without malicious intent. Our intent was for children to develop empathy for the characters, and understand how children their age might engage in these behaviours. Thus, by playing the game, children not only saw how to avoid these behaviours but could also develop an understanding and empathy for individuals (e.g., friends) who might unintentionally engage in them.

*3.2.2 Choices.* The three choices in a scenario (Figure 2c) are the main mechanism of procedural rhetoric [10] in the game (P-G2). We provided three choices for every scenario in the game, to adequately capture the nuances of the choices available to children in real life, without creating a choice paradox[1]. Each choice may lead to positive and negative consequences, displayed in the newsfeed, so players have incentives to engage in each option in the game. For example, in the scenario shown in Figure 2c, if Josie chose to post the picture, then the newsfeed would show her friends' reactions. Her friend Sofia is mad at her for posting the photo, while others think the photo is funny, so she's getting both positive and negative reactions to her choice, which reflects something that may actually happen in real life. From a privacy perspective, Josie would get 0 points for posting the photo, but this is contrasted with the social capital that she gets from her friends' reactions in the newsfeed.

Through close collaboration with educators and formative user testing of the scenarios with children (Section 5), we iteratively designed the choices so that the most security- and privacy-preserving choice is not obvious, requiring players to critically think about the different options and the situation. This allows players to explore and discover the consequences of different choices, and come to realize the main message of the game (P-G3). Players can take a risky approach and pick all of the least security- and privacy-preserving choices, just to see their effects on Jo/Josie's digital lives, or they can try to pick the safest choices in each case.

*3.2.3 Newsfeed.* The newsfeed is the second component of procedural rhetoric in our game. After making a choice, players see the results and consequences of their choice in the newsfeed, which nudges them towards the main message of the scenario. For example, in the scenario shown in Figure 2c, if the player chooses the option of *Josie should limit who can see the photo*, the newsfeed will show that Josie's friend Sophia is mad at her for posting the photo without

[1]The choice paradox is a psychological principle, where having too many choices makes users anxious and leaves them unable to make a choice. That is because the more choices users have, the more effort they need to exert comparing all the different options before making a choice. This process is stressful, so when presented with too many options users are less likely to make a choice [67].

her permission. The consequences shown will help the player reconsider their use of privacy settings on social media. Seeing the consequences in the newsfeed will also promote reflection, where players can think of their choice and how it relates to their behaviour in the real world. After playing several scenarios, players should come to the conclusion that life with digital media is nuanced, and they need to think critically about the available choices before taking action.

We designed the newsfeed to be an aggregate social media feed, staying away from mirroring any specific social media platforms. Instead, the newsfeed shows a reverse chronological series of posts and actions from other people in Jo and Josie's lives with no mention of platform. Some are public and others are private messages. Actions might include "unfriending" or commenting on Jo or Josie's photos. Each posted item has a headshot image of the person and a textual description. For each choice in the game, 3-5 new items appear in the newsfeed one at a time, using a fade-in animation.

As a consistent element in the game, and accessible from any screen, the newsfeed allows players to review the consequences of their choices on demand, promoting further reflection on the learned material. Players can display/hide the feed and can switch between Jo and Josie's feeds (Figure 2d). When a scenario is played, the newsfeed is automatically hidden by the game and it is automatically displayed again at the end of the scenario to show the consequences of the player's choice. The visibility of the newsfeed is controlled by the game during a scenario, to guide players' attention to relevant components as they progress through the scenario. The newsfeed can also help players review their choices, which may encourage them to replay the scenarios and make different choices to explore different outcomes (P-G3).

*3.2.4 Scoring and Feedback.* Players choose one of three choices at the end of a scenario, and each choice is worth 0, 1, or 2 points. The total score for the game is always visible (Figure 1) and reflects children's overall privacy preserving or socially-conscious mindset. After completing a scenario, players are told whether they made the most appropriate choice. Detailed feedback is provided after a day is completed, and explains the player's performance for the whole day. It shows their choices per scenario and associated score, then offers commentary and advice of better alternatives if appropriate (P-G4). This review screen allows players to reflect on their choices and the learned material, which is intended to aid retention and application of the material to real world settings.

The feedback provided at different points in the game (immediately after viewing the consequences of a choice and after completing a whole day) provide children with several opportunities to reflect on the consequences of their choices. Reflection allows children to realize what they did and how they can improve in the subsequent parts of the game. To minimize disruptions, the short message at the end of a scenario only tells the player how their choice affected Jo or Josie. The complete summary provided at the end of a day shows them their choice, consequences, the most security- and privacy-preserving choice, and how they can improve in the future. This kind of reflection leads to a better understanding of the educational material than simply being told that a choice was least secure [11]. It also helps with the retention and knowledge transfer of the material learned from the game [31].

Feedback was also made available directly to teachers. In parallel development, our partner organization hired developers to build an educational portal, including a teacher evaluation module, to host The JOs and their other games. This portal was developed based on feedback from teachers about their needs and with extensive consultation with us. All outcomes of our game are available for tracking in the teacher evaluation module. Teachers can use this module to monitor student performance through game scores and detailed reports about each student's game choices and actions.

*3.2.5 Characters.* It is important for children to have positive associations with the game characters, otherwise they would be less inclined to learn from them [2, 37]. To facilitate positive associations, we chose two main characters (a girl and a boy), and designed them to be representative of 11-13 year olds. We made sure that both Jo and Josie were represented equally in game scenarios where they were the victims of negative behaviour and where they had an

opportunity to practice negative behaviour. We similarly tried to include diversity in ethnicity, abilities, and appearance among the secondary characters. Jo and Josie are siblings who attend middle school and take part in extracurricular activities such as basketball. They play video games, have cellphones, and use computers at school and at home for homework. They engage with their friends in person and through various digital channels.

*3.2.6 Navigation.* We used an explicit control (Figure 2a, yellow arrow on right edge) to transition between scenes within a scenario. This accommodates children's different reading levels and speed by allowing them to control the pace of transition. The game's logo, located at the top-left of the screen can be used to return to the Calendar page at any time during game play. Players can only move forward through scenes, to reinforce the relationship with real life. However, players can replay an entire day once completed in its entirety.

*3.2.7 Language.* The game could be played in English or French, and players select their preferred language from the login screen. Both the English and French versions had the same visual design and used the same underlying technical architecture, with a system parameter determining the language of the assets (e.g., text, graphics) to display. As their progress is automatically saved, players can switch the language anytime during the game by returning to the login screen and selecting a different language. While the game is currently available in two languages, we created a modular technical architecture, so more languages can be easily added in the future.

*3.2.8 Audio.* To reduce children's cognitive load, we minimized the amount of text used in the game and provided audio narration for all text. Players can control the audio using the persistent audio player located at the top of the screen. Narration was done by a hired voice actor in both English and French. Audio could be set to autoplay with each scene transition, allowing children to follow along with text as it appeared on the screen.

*3.2.9 Content.* Game content was designed at an appropriate reading level for our target audience in collaboration with K-12 Educators experienced in designing educational material for children. We minimized text where possible by including meaningful and visually appealing graphics. The scenarios were designed to be realistic and representative of the lives of 11-13 year old children to encourage transfer of lessons in the game to real world settings (P-G5). Scenarios were designed to be lighthearted and humorous to keep children engaged. We implemented twenty-five scenarios, and structured the visual design and technical architecture such that more scenarios (up to 150) can be added in the future by adding content for the other days in the calendar.

### 3.3 Cybersecurity, privacy, and digital literacy principles

The principles of cybersecurity, privacy, and digital literacy are nuanced, and in many cases the correct behaviour depends on the context of the situation and the user's personal beliefs and attitudes. For example, personal privacy does not necessarily mean that an individual should never share any information about themselves, but rather that it is an individualized choice and some people may choose to disclose more than others. In this case, our aim would be to help players consider the consequences (good and bad) and make an informed decision for themselves.

This makes it challenging to design learning tools to improve children's cybersecurity and privacy knowledge and behaviours. In The JOs game, the design team made a subjective determination about which choice was considered the *most security- and privacy-preserving* option in each scenario. Given the nuances of the situations represented in our game, it is possible that some players may disagree with our choices. However, when this happens, we believe that it will generate meaningful discussion among the players and the teacher about the different choices in the game. This type of discussion fosters critical thinking skills in children and creates a sense of agency, which is required when they

encounter these situations in real-life. Thus, the objective of our game is to create an environment that allows children to explore different aspects of nuanced cybersecurity, privacy, and digital literacy topics, and generate discussion, which ultimately fosters their critical thinking skills.

### 3.4 Demonstration of game design principles

The JOs game exhibits characteristics of procedural rhetoric and various educational design principles to create an environment that allows children to explore different online safety behaviours and practice them in a safe environment. The replayability feature makes failure a natural part of the learning process, as children can replay a scenario to explore different outcomes.

*3.4.1 Gee's learning principles.* Gee specified sixteen principles [27] for designing effective educational games and states that the number of principles applied to a game determines how effective it is as an educational tool. Thus, a game becomes a better learning tool as it respects more principles. The JOs applies ten out of the sixteen principles. According to Gee's *Agency* principle, an environment demonstrating these ten principles is an environment where players can feel a sense of ownership over what they are learning, because they are helping to create the learning environment by making choices in the game [27]. The following list shows the application of the remaining nine principles on The JOs game.

**Performance before competence.** The JOs is self-contained and can be played by tweens with varying levels of cybersecurity, privacy, and digital literacy skills. This aspect of our game respects the *Performance before competence* principle, where players can perform in the game before becoming competent in it, which is the reverse of traditional educational methods [27]. For players with low cybersecurity, privacy, and digital literacy skills, we believe that the additional support and classroom conversations surrounding the game can be especially beneficial.

**Just in time and On demand.** Information in The JOs is broken down into chunks, and players are only provided the relevant chunk when they need it in the game. For example, the content associated with each scenario is split into various scenes and the newsfeed, to avoid overwhelming players with the content, in accordance with the *Just in time and On demand* principle [27].

**Pleasantly frustrating.** By not making the most secure- and privacy-preserving choice obvious in a scenario, The JOs respects the *Pleasantly frustrating* principle [27], requiring players to critically think about the different options and the situation. However, we made sure that the most secure- and privacy-preserving choice is also not impossible to find, so players are not left frustrated.

**Risk taking.** The design of the choices in The JOs also respects the *Risk taking* principle, because it allows players to explore risky behaviours in a safe simulated environment, where the consequences are less severe than in the real-world [27]. This design might lead players to choose riskier choices compared to the real-world, because they are interested in exploring the consequences of these choices in a safe environment.

**Production.** The newsfeed respects the *Production* principle, because players are influencing their own ending to a scenario (i.e., story). This helps players feel empowered and in control of their learning, which should lead to better engagement and improved learning of the content [27].

**Interaction.** The choices and constant feedback provided by The JOs, especially through the newsfeed respects the *Interaction* principle, where players and the game world communicate through actions (by the player) and

feedback (by the game) [27]. Through their actions in The JOs, players are able to interact with other characters in the game, whose responses to their actions appear in the newsfeed.

**System thinking.** By applying the *System thinking* principle, The JOs encourages players to think about the relationships between different systems (i.e., digital media platforms), and how their actions affect others in the system [27]. For example, in scenarios involving social media, children learn how their actions affect others, and also how the actions of other people affect their own privacy. In the scenario shown in Figure 2, after choosing to post a photo without Sophia's permission, the player learns that Josie has accidentally compromised her friend's privacy. Thus, the game helps children understand the security, privacy, and ethical implications in complex socio-technical systems that represent the digital world.

**Challenge and consolidation.** This principle states that games should allow players to master a challenge before presenting them with a new set of challenges that require the use of the mastered skills [27]. While this aspect is not built into The JOs game, the replayability feature does allow teachers to implement this part of learning outside of the game. For example, teachers can assign children a day, and only allow them to move on to the second day once they have demonstrated sufficient mastery.

**Identity.** According to this principle, children learn from games when they can inhabit a character and manipulate the character by making choices for them [27]. The JOs game respects this principle, as children can take on the role of Jo or Josie and make choices that have consequences on their digital lives. Inhabiting these roles can also increase children's engagement and commitment to playing the game, which results in deeper learning [27].

*3.4.2 Meaningful play.* Salen and Zimmerman's principles of meaningful play [65] are apparent in our game. Our intention is that players will find the experience of playing the game meaningful, which will contribute to their engagement and improved learning of the cybersecurity, privacy, and digital literacy content. Players make choices in the game to create a story about the digital lives of Jo and Josie. Scenarios can be considered different scenes in the story. In each scenario, players make a choice on how they want that scene to end. Each choice is meaningful for the player because it creates a different ending for the scene. The choices affect the larger game context, by manipulating the player's total game score. A player's experience in the game depends on the choices that they have made, which means that players will have different experiences. This contributes to the fun and replayability of the game. Players may want to play the game again to make different choices and experience different outcomes. At any point, players can review the story they have created so far by reviewing Josie and Jo's newsfeeds to see the consequences of their choices on the characters' digital lives.

*3.4.3 Procedural rhetoric.* The theory of procedural rhetoric is evident in the design The JOs game. Specifically, our design fits with Ferrara et al's. design guidelines [22] for procedural rhetoric. We review parts of our design in light of these principles.

*(P-G1) Define a core message and (P-G5) Keep the simulation realistic:* Our game has a main message, which the players can piece together after playing multiple days in the game. To re-iterate, the main message of our game is that *life with digital media is complex, and the correct behaviour is not always clear. However, we have choices and the choices we make have consequences (good or bad) on our personal and digital lives.*

However, each scenario in the game also has its own message, which the player can discover by making choices in the scenario and viewing the consequences of their choice in the newsfeed. For example, the scenario shown in Figure 2, represents a situation that children actually encounter in the real-world.

*(P-G2) Offer meaningful choices:* After presenting the scenario, players are provided with three possible choices, and must pick an action that Josie should do (Figure 2c). We designed the choices to reflect the real world so that the most secure- and privacy-preserving choice was not always clear, requiring players to think critically of the choices and the situation. This type of design allows players to explore and discover the consequences of different choices, and also makes each choice meaningful.

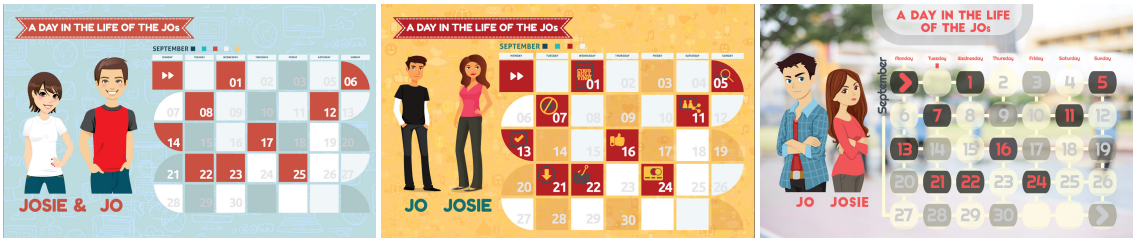
*(P-G3) Enable self-directed discovery and (P-G4) Tie the message to strategy:* After making a choice, players immediately see the consequences of their choice on Jo and Josie's digital lives in the newsfeed. At this point, players may have an "ah ha!" moment as they realize the unexpected effects of their choice on Jo and Josie. We used an animation to present the events in the newsfeed sequentially to the player. This was partly done for usability, but also to create suspense around the final outcome. For example, in the scenario shown in Figure 2c, if Josie chose to post Sophia's photo without her permission, then the newsfeed will sequentially show her friends' reactions. Sophia will be mad at her for posting the photo, while others think the photo is funny. The final event associated with this choice is that Sophia unfriends Josie on social media. After viewing the consequences and reflecting on their choice, the player may rethink their use of privacy settings, they may understand the importance of respecting other people's privacy, and they may realize that their expectations of privacy may not be the same as someone else's. Thus, the final message of a scenario depends on the player's choices and their own personal experiences. This exemplifies the rhetorical aspect of procedural rhetoric, where players experience the consequences of their choice, and then have to figure out what that means for them.

To summarize, the choices and the newsfeed form the core of the procedural rhetoric in The JOs game. The choices made by the player determine the consequences shown in the newsfeed. The newsfeed helps player reflect, realize the consequences of their actions, and come to the conclusion of what the scenario's main message is for them.

### 3.5 Design process

We used an iterative user-centered design process to create the game in collaboration with our partner organization. The conceptual design of our game was inspired by an existing MediaSmarts' resource, "Jo Cool or Jo Fool" [46]. Designed in 2000, the "Jo Cool or Jo Fool" quiz teaches 10-13 year-olds safe web browsing behaviours [46], and is still being used in schools despite being significantly outdated. The quiz also presents scenarios but is text-heavy and does not include feedback like our newsfeed. The design and development of our game was completed over a period of three years, using an interdisciplinary team of designers, developers, and K-12 Educators. We used a participatory design approach, where all stakeholders were actively involved in the design process to ensure that the final product met their requirements. Throughout this process, we conducted five user studies described in the following sections to evaluate aspects of the game with children and teachers.

We began by conducting a user study of the "Jo Cool or Jo Fool" quiz to discover areas of weaknesses and strengths (Study 1). The findings from the study were discussed with our educational partners to identify requirements for the game, educational topics, and the target audience. Next, we created three candidate visual designs for the game and evaluated them with children (Study 2). Feedback from this study was used to improve and create our final visual design, which was then prototyped in Adobe Illustrator and partially implemented in HTML5. We conducted a user study to evaluate this medium fidelity prototype with children (Study 3). Using feedback from the study, we refined our visual and game design and completely implemented them in HTML5 to create a production-quality game. We conducted a two-part summative study with children on the high-fidelity prototype to evaluate its usability and effectiveness at meeting the learning goals (Study 4). We improved the prototype based on feedback from the children, and then tested




**(a)** Design 1 **(b)** Design 2 **(c)** Design 3

**Fig. 3.** Three visual designs for The JOs game.

the prototype with teachers to explore how it can be used in classrooms (Study 5). In total, the game was evaluated with 55 children and 21 teachers at various stages of the design process.

### 3.6 Implementation

The web-based game was developed in HTML5, CSS, and JavaScript, and is hosted on our partner organization's educational portal for schools. The game is accessible to schools on all major web browsers, operating systems, and desktop and mobile devices. It collects data on the player's progress (e.g., score, scenarios played, etc.), and stores it on the portal through an API. In addition to saving game state, this portal also provides user authentication and a teacher module, which allows teachers to review students' progress in the game. As the portal was not evaluated in our user studies, we consider it out of scope for this paper. Further details on the portal and game architecture can be found in [40].

## 4 USER STUDY 1: FORMATIVE EVALUATION OF THE "JO COOL OR JO FOOL" QUIZ

We conducted a formative user study with 16 children (7 girls, 9 boys) between the ages of 11 and 14 to evaluate the existing "Jo Cool or Jo Fool" quiz [46]. Participants completed a pre-test questionnaire, completed parts of the quiz, and then completed a post-test questionnaire. The quiz consists of twelve mock websites which users assessed to determine whether the characters Jo and Josie made the correct decision. For example, a website might collect personal information, and the user is asked whether Jo was right to provide his information. Each participant attempted two or three websites in the quiz. The websites were assigned to ensure coverage of all scenarios.

Eye-tracking data revealed that children read the text line-by-line or in a zig-zag pattern. In the zig-zag pattern, they read some text, drifted their gaze to another object on the screen, and then returned to the text. This pattern was commonly observed in slow readers who frequently asked whether they really needed to read the text. Participants skipped reading chunks of text on websites that were text-heavy. However, the eye-tracking revealed that participants were drawn to Jo and Josie's faces, especially when the characters appeared to make eye-contact with them.

Participants felt they learned only a moderate amount from the game and this was confirmed through the pre-test and post-test knowledge questions. For 7 out of 12 scenarios, knowledge did not improve, because children already had the correct knowledge or because they retained their misconception. Overall, children liked the characters of Jo and Josie and the scenario-based approach. However, they did not like the visuals, found the content outdated, and ignored large blocks of text. For our new game, we kept the main characters of Jo and Josie, a brother sister duo, and the scenario-based approach since they were positively received by participants.

## 5 USER STUDY 2: FORMATIVE EVALUATION OF THE VISUAL DESIGN

We created three alternative visual designs for the game (Figure 3) and tested them with eight 10-12 year old children to evaluate the age appropriateness of the main characters, overall colour scheme, and design. For continuity, four returned from the previous study. Participants were shown the three designs in random order. We asked about character preference, layout, background, colour scheme, and also tested the text of some of the scenarios. Since the scenarios did not have a visual representation, we read a script and asked about the content and choices available for Jo and Josie.

Based on the feedback, we combined the facial expressions of the characters in Design 1 with the bodies of Design 3, and chose the colour scheme and layout of Design 3. Figure 1 shows our final design. Participants had a strong sense of "wrong" and "right" in the scenarios. For example, in the bullying scenario they wanted to confront the bully or ask them to stop. However, this is not always the best choice as confronting bullies can worsen the aggression. These comments encouraged us to include scenarios where "correct" choice is unclear, so children can learn about more nuanced situations. They also wanted more visuals to describe scenarios instead of text.

## 6 USER STUDY 3: FORMATIVE EVALUATION OF THE MEDIUM FIDELITY PROTOTYPE

This study assessed the usability of the *medium fidelity prototype*, the interaction flow, and the storyline before full implementation. We fully implemented the cyberbullying day in HTML5, JavaScript, CSS, and SVG, and the remaining four days were tested in PowerPoint using a wizard-of-oz approach. At this stage, we also implemented initial versions of the scoring, newsfeed, and review screen in the web-based prototype. We conducted a user study of the medium-fidelity prototype with fourteen 11-13 year old children. For continuity, four returned from previous testing sessions. Participants completed a pre-test questionnaire and interview, played the game, and then completed a post-test questionnaire and interview (see [50] for details).

Each participant played the functional day in the web-based prototype and a second pseudo-randomly assigned day in Microsoft PowerPoint. Participants were audio recorded and an eye-tracker recorded their gazes during game play. Participants found the length of the content to be acceptable, found the scenarios interesting, enjoyed playing the game, found the game fun, and liked the visual design. Returning participants liked the visual design better than the old quiz. Eye-tracking data revealed that participants were attracted to characters' faces and other game elements, such as the score and newsfeed. Qualitative feedback confirmed that participants liked the scoring and newsfeed features. They expressed excitement after receiving a high score or wanted to know how they could improve. Overall, participants liked the game; they particularly liked how the game showed current events using electronic devices and social media. They also liked the age appropriateness of the content, use of animations, and feedback.

## 7 USER STUDY 4: SUMMATIVE EVALUATION OF THE FUNCTIONAL GAME

We conducted a user study with twenty-five 11-13 year-old children to evaluate the functional prototype of our game. Children played three days in the game and completed questionnaires and interviews to provide us with feedback on the usability of the game. We also looked at whether their cybersecurity, privacy, and digital literacy knowledge and behavioural intent improved after playing the game.

### 7.1 Research questions

We had the following four research questions for our user study:

**RQ1-knowledge:** Does the game improve children's cybersecurity, privacy, and digital literacy knowledge?

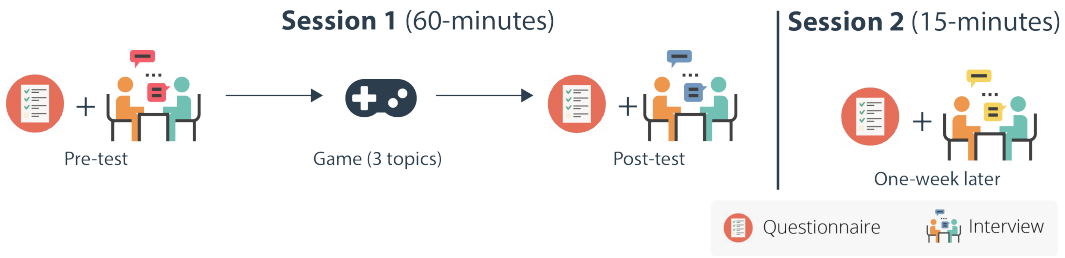



**Fig. 4.** Methodology of the Study 4 with children

**RQ2-intent:** Does the game improve children's cybersecurity, privacy, and digital literacy behavioural intent?
**RQ3-usability:** Do children find the *A Day in the Life of the JOs* game usable?
**RQ4-perception:** What do children think about the *A Day in the Life of the JOs* game?

### 7.2 Methodology

We conducted a two-part study to evaluate the usability and effectiveness of our fully functional game with children. The effectiveness of the game was determined by improvements in children's cybersecurity, privacy, and digital literacy knowledge and behavioural intent. For our purposes, we use Ajzen's definition of *Behavioural Intent* from the Theory of Planned Behaviour: Behavioural intent represents users' perceived likelihood of engaging in a particular behaviour in the future [1]. It is an antecedent of future behaviour and is determined by several factors, including users' attitude toward the behaviour, subjective norms, and their perceived behavioural control [1]. To evaluate the effects of online safety awareness training, it is common practice to measure users' behavioural intent, because we cannot put them in dangerous situations to evaluate their actual behaviour [52, 68, 69]. For these situations, behavioural intent is an appropriate measure, because it is a predictor of whether users will take part in certain behaviours in the future [1, 19].

Figure 4 shows the methodology of our study, which was approved by our University's Research Ethics Board (REB). The first session took an hour, and the second session about 15 minutes. In Session 1, participants completed a pre-test questionnaire and a short interview. Next, they played the English version of the game on a laptop and completed a post-test questionnaire and interview. To keep the session length manageable, children played three of the five days, selected using a Latin square. The game was instrumented and recorded players' choices, time to complete tasks, and the number of points earned. An eye-tracker tracked participants' gaze during game play. They were also encouraged to think-aloud while playing. The second session took place one week after the first, and assessed whether children retained the knowledge learned in the game. In the second session, children completed a questionnaire and an interview.

The pre-test questionnaire included demographic questions and a security, privacy, and digital literacy knowledge measure (SPDLK). Our *SPDLK* (Appendix B) had fifteen 5-point Likert scale knowledge questions (three questions per day of the game).

The post-test questionnaire collected opinions of the game and repeated the SPDLK. The SPDLK was also included in the one-week questionnaire to see if children improved and retained knowledge.

The interviews (Appendix C, Appendix D, Appendix E) evaluated whether children could apply their knowledge to new situations. They were provided with five situation-based questions (one per day of the game), regardless of which days they played, with reasoning that playing part of the game may raise their awareness and critical thinking skills in related topics not explicitly covered. We asked what they would do, and how it would affect their privacy and

| | | Score (/10) | Time (min:sec) |
|---|---|---|---|
| **Day** | **N** | ***M (SD)*** | ***M (SD)*** |
| Cyberbullying | 16 | 7.38 (1.15) | 4:31 (0:54) |
| Data privacy | 15 | 6.40 (2.20) | 4:47 (0:52) |
| Online reputation | 15 | 7.67 (1.95) | 5:10 (1:10) |
| Privacy and ethics | 13 | 9.54 (1.56) | 4:48 (0:57) |
| Fact checking | 16 | 4.69 (1.96) | 5:13 (1:06) |

**Table 2.** Children's mean game score and mean time per "day" (each day was played once per participant).

that of others. For example: *All your friends are playing a popular online game so you decide to sign-up for the game as well. When you sign-up, the game asks you to provide your full name (first and last name) and your home address, so that other players can contact you. What would you do in this situation? How might this affect your privacy? How might this affect others' privacy?* We created three sets of the questions and used a Latin square to decide which to use in the pre-test, post-test, and one-week interviews. The sets were similar in structure and evaluated the same topics, but had a different context to avoid children simply repeating their previous answers. Each interview took about 10 minutes and was audio recorded.

*7.2.1 Recruitment and Consent.* Participants were recruited through social media parenting groups, snowballing, and by distributing flyers in our local area. At the start of the session, a parent provided written consent for their child's participation and the child provided verbal consent. Each participant received a $20 gift certificate or cash. Parents were reimbursed for parking costs when applicable. Sessions took place in our research lab or other quiet, mutually convenient locations (e.g., public library). When sessions took place outside the lab, we chose locations with minimal distractions. We also ensured that other individuals were not nearby, to avoid accidentally audio recording them.

*7.2.2 Participants.* Ten girls and fifteen boys participated in the study. Fifteen were 11, nine were 12, and one was thirteen years old. They spent an average of 1 hour and 27 minutes online per day. Participants had access to computers (96%), tablets (80%), smartphones (44%), and music players (28%). Most used social media several times a day (40%), while some used it daily (16%) or monthly (8%). Most children (92%) reported some knowledge of how to protect their privacy online and how to behave on social media, saying they learned it from school (88%), parents (76%), and friends (16%).

### 7.3 Results

We analyzed the game logs, questionnaires, and interview data to evaluate the usability and effectiveness of the game.

*7.3.1 Time and scores.* Using the game logs, we tabulated some performance statistics. Table 2 shows players' mean scores and the time they took to complete each day in the game. The number of participants (*N*) varies because participants only played 3 game days each. On average, they took approximately 5 minutes to complete a day. The scores show that participants found the *ethics of privacy* day (i.e., ethics of sharing others' content) easiest. They found the days covering *data privacy*, and *fact checking* information most difficult, which suggests that participants were least familiar with these topics.

*7.3.2 Addressing RQ1-Knowledge.* To assess cybersecurity, privacy, and digital literacy knowledge, we analyzed data from the SPDLK (Appendix A). While children only played three days in the game, they answered SPDLK and behavioural intent questions corresponding to all five days in the game. When analyzing the data, we looked at the responses

| | Total | Pre-test | Post-test | One-week-test |
|---|---|---|---|---|
| **Measure** | **Score** | ***M (SD) %*** | ***M (SD) %*** | ***M (SD) %*** |
| SPDLK (3 days played) | 45 | 33 (3) 73% | 36 (4) 80% | 36 (4) 80% |
| Behavioural Intent (3 days played) | 27 | 17 (3) 63% | 20 (3) 74% | 21 (3) 77% |
| SPDLK (all days) | 75 | 55 (4) 73% | 60 (5) 80% | 60 (5) 80% |
| Behavioural Intent (all days) | 45 | 30 (4) 67% | 35 (4) 78% | 36 (5) 80% |

**Table 3.** Children's SPDLK and behaviour scores at three time points, for the three days played, and all five days in the game. The Total Score column indicates the total possible score for each measure.

corresponding to the days completed, and also for all the days, to see if learning from one topic improved their understanding of the others.

**Knowledge for Days Played:** We tabulated participants' scores for the nine 5-point Likert scale questions from the SPDLK corresponding to the days completed, and gave them a days-played knowledge score out of 45 (5 per question). Table 3 summarizes participants' pre-test, post-test, and one-week days-played knowledge scores. We conducted a one-way repeated measures ANOVA to determine whether children's days-played scores changed over time. Using a Greenhouse-Geisser correction, we found statistically significant differences in children's days-played scores over the three time points ($F(1.61, 38.69) = 41.61$, $p < .001$, $\eta_p^2 = .63$). Post-hoc analysis using the Bonferroni correction revealed that children's days-played knowledge scores improved significantly from pre-test to post-test ($p < .001$) and from pre-test to one-week test ($p < .001$). No significant differences were found between post-test and one-week scores ($p < .116$), suggesting that children retained the knowledge they learned in the game.

**Knowledge for All Days:** The scores for all fifteen 5-point Likert scale questions from the SPDLK were added to give participants' an all-days cybersecurity, privacy, and digital literacy knowledge score out of 75 (5 per question) (Table 3). We conducted a one-way repeated measures ANOVA to determine whether children's all-days scores changed over time. Using a Greenhouse-Geisser correction, we found statistically significant differences in children's all-days scores over the three time points ($F(1.56, 37.35) = 11.05$, $p < .001$, $\eta_p^2 = .32$). Post-hoc analysis using the Bonferroni correction revealed that children's all-days knowledge scores improved significantly from pre-test to post-test ($p < .004$) and from pre-test to one-week test ($p < .004$). No significant differences were found between post-test and one-week scores ($p = 1.00$). We thus see the same pattern as in the days-played scores.

*7.3.3 Addressing RQ2-Intent.* Children's behavioural intent scores were derived from the interview data. The interviews were transcribed from audio recordings and we organized the responses in Excel according to the 15 interview questions (3 questions × 5 scenarios). We coded each response on a 3-point scale (3 = very good, 2 = marginal, 1 = poor) for a total out of 45 points[2]. Appendix F provides an example of how an interview question was scored on the 3-point scale.

A second researcher independently coded the responses for the first 13 participants. A Cohen's Kappa (k) test showed moderate agreement between the two researchers' initial analysis of the pre-test (k = 0.65, 95% CI: .6 to .7, $p < .001$), post-test (k = 0.62, 95% CI: 0.5 to 0.7, $p < .001$), and one-week-test scores (k = 0.57, 95% CI: 0.5 to 0.7, $p < .001$). In cases of disagreement, both researchers discussed and consolidated the scores to be used in the final analysis. Since we had moderate agreement, and had calibrated scores for the first half of the responses before continuing, only the one researcher coded the responses for the remaining 12 participants.

[2]One question was poorly worded and could be interpreted in different ways. This resulted in too much variability in responses. We assigned it the middle score of 2 for each participant.

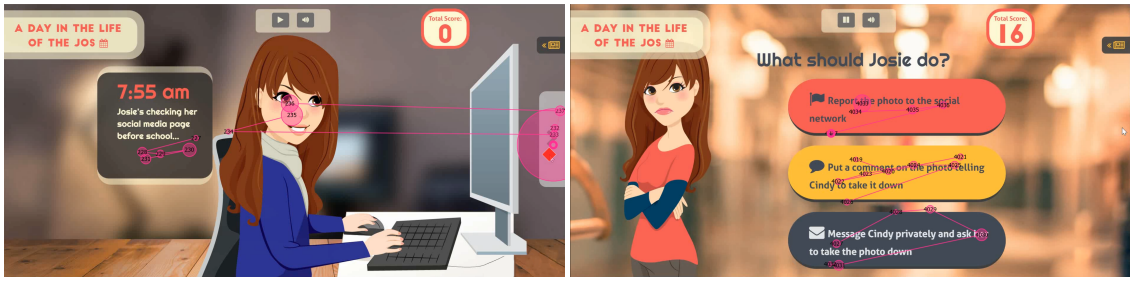
**Intent for Days Played:** The behavioural intent days-played scores were computed from responses to three scenarios relating to the Days children played in the game, giving participants a total score out of 27 (3 scenarios × 3 questions × 3-points per question). Table 3 shows a summary of children's days-played cybersecurity, privacy, and digital literacy behavioural intent scores. We conducted a one-way repeated measures ANOVA to see if these scores improved over time. Using a Greenhouse-Geisser correction, we found that the days-played intent scores significantly improved over the three time points ($F(1.61, 38.69) = 41.61$, $p < .001$, $\eta_p^2 = .63$). Post-hoc analysis using the Bonferroni correction revealed that children's days-played intent scores improved significantly from pre-test to post-test ($p < .001$), and pre-test to one-week test ($p < .001$). No significant differences were found between post-test and one-week scores ($p < .116$).

**Intent for All Days:** We also looked at the behavioural intent scores for all five days in the game, which gave a total score out of 45 (5 scenarios × 3 questions × 3-points per question) (Table 3). A one-way repeated measures ANOVA found that the all-days scores significantly improved over the three time points ($F(2, 48) = 50.13$, $p < 0.001$, $\eta_p^2 = .68$). Post-hoc analysis with Bonferroni correction revealed that children's all-days behavioural intent scores improved significantly from pre-test to post-test ($p < .001$), pre-test to one-week test ($p < .001$), and post-test to one-week test ($p < .019$); again showing that playing the game led to sustained improvements, this time in children's intent to take secure and privacy-preserving actions if faced with situations requiring such decisions.

*7.3.4 Addressing RQ3-Usability and RQ4-Perception.* The post-test questionnaire, included seven questions to evaluate the usability of the navigation, content, storyline, and fun of the game. One question measuring the challenge aspect of the game, was interpreted differently by children, making the results unreliable, so we excluded it from our analysis. All questions used a 5-point Smileyometer [62]. Participants were very positive in their responses. Most reported being able to find and use the navigation controls easily, and found the game content easy to understand.

We gathered further usability feedback in the interviews. Some did not understand certain words in the game or could not read the text because it was too small on a 13-inch laptop screen (1280 × 800 resolution). Most found the storyline interesting and enjoyable because they learned new concepts (e.g., using the rumor busting website Snopes), liked the overall design and artwork, liked the characters, and found the game realistic and relatable. One participant explained *I liked that the scenarios were realistic. They could mentally prepare you if you encounter them in the future, so you would know how to deal with them.* Most participants found the game fun, because it offered lots of interactions, engaged their critical thinking skills, included appealing graphics, and was relatable for their age group.

We asked children's opinion of the main characters, Jo and Josie, using open-ended questions. Most had positive perceptions of the characters. 52% thought that the characters were nice, interesting, and likeable. 24% thought that the characters were realistic and relatable. One participant stated *They were kind of relatable because they're around my age and if I used social media more often, I could also be having these problems, so it would be valuable to play this game and learn.* We asked children to rate the characters' likeability on a 5-point Smileyometer, with 1 being very dislikeable and 5 being very likeable. Most found the characters likeable ($M = 4$, $SD = 0.64$). Participants were clearly engaged with the characters and had formed opinions of them. Many said they would like to be friends with Jo (40%) and Josie (52%) if they were real people. Participants wanted to be friends with the characters because they had similar interests (e.g, skateboarding, video games), thought they were nice, and smart. One participant stated *Josie also seems like a nice person, and she has a lot of good friends that would be able to back her up in situations, and by extension back me up in a lot of sticky situations.* Those participants who were unsure about being friends with Jo (44%) and Josie (36%) explained that it was because they did not know enough about them or lacked shared interests.




**(a)** Gaze scanpath of a child viewing the first screen of a scenario. **(b)** Gaze scanpath of a child reading choices in a scenario.

**Fig. 5.** Eyetracking of scenes in a scenario.

*7.3.5 Eye-tracking.* We examined fixation patterns in the videos generated by the eye-tracker to see which elements of the game received attention from participants and how they interacted with the elements (Figure 5). In general, the different elements did not compete for children's attention because we used animation to sequentially present elements and guide their attention.

**Common Elements:** Common elements across screens include the audio player, score area, and "next button". Most participants noticed the audio player, but none used it to control the voice narration in the game, which was on by default. In fact, this area received the least attention, suggesting that the narration was at a good reading pace for children, and synced well with the game text. Participants were able to easily locate and use the "next" button to navigate between scenes in a scenario.

**Text and Graphics:** The game contains a considerable amount of text, however, we tried to facilitate reading by using humor, chunking text, and combining text with visuals. We used eye-tracking to determine children's reading behaviour, and found that they read most of the game text and newsfeed. In the feed, a new entry sometimes appeared before children were finished reading the previous entry. When this happened, children continued to read the previous entry and moved to the new one when they were finished. Some children read the text multiple times, especially when it was long, but most read it only once, suggesting that it was at an appropriate reading level. We observed that after playing two consecutive days (5 scenarios per day) in the game, children started to experience reading fatigue, leading some to skip text in the day review screen, possibly because it was too long or they were listening to the audio narration instead. Children paid close attention to the list of choices presented in each scenario (Figure 5b). Many read each option multiple times, considering the consequences of each option before making their choice. When game characters were present, children frequently focused on their faces, particularly the eyes.

## 8 USER STUDY 5: EVALUATING THE JOS WITH TEACHERS

Although K-12 Educators on our design team provided advice and feedback throughout the design process, we also conducted a user study of the fully functional game with a separate group of grade 4-8 teachers. Since games for classroom use have additional requirements that affect their adoption by teachers, we wanted to determine whether the game adequately addressed these requirements. These requirements include availability of empirical evidence on the effectiveness of the game, alignment with the curriculum, and ability to integrate seamlessly into lessons [20, 33, 34, 45].

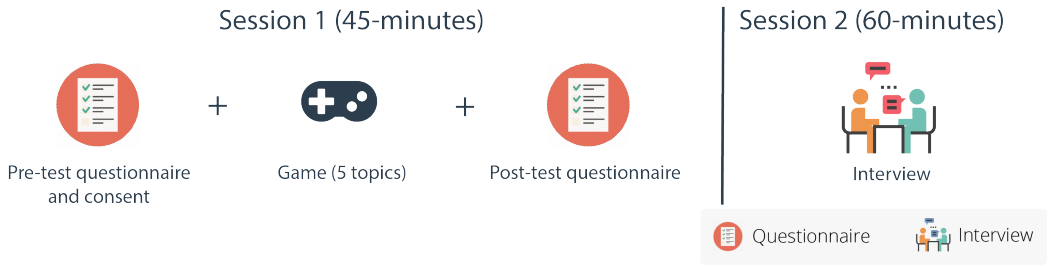



**Fig. 6.** Methodology of the user study with teachers

### 8.1 Research questions

We had the following four research questions for our user study with teachers:

**RQ1-knowledge:** Does the game improve teachers' own cybersecurity, privacy, and digital literacy knowledge?
**RQ2-usability:** Do teachers find the *A Day in the Life of the JOs* game usable?
**RQ3-perception:** What do teachers think about the *A Day in the Life of the JOs* game?
**RQ4-classroom:** How will teachers use the *A Day in the Life of the JOs* game in their classroom?

### 8.2 Methodology

Figure 6 shows the methodology of our study, which was cleared by our University's Research Ethics Board (REB). Data was collected using game logs, questionnaires, and a semi-structured interview. The study consisted of two sessions.

**Session 1:** The first session was completed online and took about 45-minutes. To begin, teachers completed a pre-test questionnaire online, which included the consent form. Next, they played all five days in the game on their own time and completed a post-test questionnaire.

**Session 2:** The second part took 60-minutes and was completed in person or via video-conferencing, whichever was more convenient for the participant. Participants completed a semi-structured interview with the researcher, discussing their experience with playing the game and teaching digital literacy in their school.

Participants were compensated with a $50 Chapters bookstore e-gift card or an email money transfer, depending on their preference. The questionnaires were created and distributed using the Qualtrics[3] survey tool. Upon completion of a questionnaire, templated emails in Qualtrics were used to send instructions to the participant on the next step of the study. Interviews were audio recorded, and the audio was transcribed using the automated transcription service Trint[4]. The transcripts were manually edited by a researcher to correct any inaccuracies.

*8.2.1 Recruitment and Participants.* Teachers were recruited from Facebook groups, teacher blogs, and other teacher-related websites such as the Canadian Teacher's Magazine[5]. Posters were also distributed at our university, and community centres in our area. Teachers were recruited from across Canada, and needed to have experience in teaching digital literacy, media literacy or digital citizenship. In addition, they needed to have experience teaching grades 4-8, which is the target audience of our game, but they could be currently teaching any grade. They had to be employed as a teacher in a Canadian school.

[3] https://www.qualtrics.com/
[4] https://trint.com
[5] https://canadianteachermagazine.com

21 teachers were recruited from eight different cities and four provinces across Canada, and taught at eighteen different schools. Twelve taught at schools in Ottawa. At the present, they were teaching grades 1-8. 48% of participants taught in private schools and 52% taught in public schools. 86% (n = 18) were female and 14% (n = 3) were male, which is representative of this user population.

*8.2.2 Pilot testing.* Before testing with teachers, we pilot tested our questionnaires with friends and members of our research lab, and made changes based on their feedback. We then conducted the study with two teachers, who helped test the study materials and the methodology. From this testing, we found that some of our interview questions were too specific, and were not providing sufficiently rich data. We also noticed that the interviews were skewed towards feedback about the game, so we were not collecting enough data to understand cybersecurity and privacy in classrooms. Our initial teachers completed the interview in about 30 minutes. Based on these results, we updated our interview script to make the questions more open-ended, and included new questions to understand cybersecurity and privacy in classrooms. The updated interview script was used with the remaining 19 participants. Although short, these two interviews did provide useful feedback so we include their data in our analysis.

*8.2.3 Research instruments.* The following are details of the questionnaires, game, and semi-structured interview used in the study.

(1) **Pre-test questionnaire:** Collected demographics information, details about teacher's classroom, their use of technology and social media, and resources used for cybersecurity and privacy education. The questionnaire also included the SPDLK from Section 7.2.
(2) **Post-test questionnaire:** Evaluated perceived usability of the game using same seven 5-point Likert scale questions from Section 7.2. It also repeated the SPDLK, to see whether teachers' cybersecurity, privacy, and digital literacy knowledge improved after playing the game. We slightly reworded the questions to ask teachers what they would do in the future, as opposed to asking what they currently do in the pre-test.
(3) **Game:** Instrumented game logs recorded teachers' actions in the game. Teachers could play the game in either English or French, could complete the task across multiple sessions, and could replay days if desired.
(4) **Semi-structured interview:** The interview was organized into three themes: issues observed around children's media use, experience teaching cybersecurity and privacy, and teachers' perception and potential usage of The JOs game. We focus on results from the third theme in this paper.

### 8.3 Results

We discuss the usability and learnability for teachers, and compare with our children study (Section 7.3) when applicable.

*8.3.1 Time and Scores.* Table 4 shows teachers' scores and the time they took to complete each day in the game. The results are similar to children's performance (Table 2). Like the children, teachers took on average 5 minutes per day. The speed of the text animations likely prevented teachers from progressing through the scenarios at a faster pace.

Assuming that most teachers tried to advance through the game by selecting the most secure- and privacy-preserving choices, their scores suggest that teachers found the *ethics of privacy* topic to be the easiest, and the topics of *data privacy* and *fact checking information* most difficult. Children also found these topics most difficult. Our results suggest that the game could be used as a learning tool for teachers, who can play it to improve their own knowledge before teaching certain topics to children. It is important to note that since the game is exploratory, teachers may have picked

| Day | N | Score (/10) | Time (min:sec) |
|---|---|---|---|
| | | *M (SD)* | *M (SD)* |
| Cyberbullying | 21 | 6.9 (1.45) | 5:20 (2:07) |
| Data privacy | 21 | 6.8 (1.65) | 4:54 (1:13) |
| Online reputation | 21 | 7.1 (1.58) | 5:40 (2:00) |
| Privacy and ethics | 21 | 8.9 (1.09) | 5:02 (1:17) |
| Fact checking | 21 | 5.8 (1.88) | 5:19 (2:32) |

**Table 4.** Teachers' mean game score and mean time per game day (each day was played once per participant).

the least security- and privacy-preserving choice on purpose to see its consequences in the game. As one teacher explained:

> "I clicked the ones I knew were the middle of the road answers, just to kind of see what happened. I was curious from the Choose Your Own Adventure approach to the game. I was like 'I want to know what happens if I press this one' " (t20).

Thus, the scores should not be used as the only indicator of learning in the game for adults nor children, unless players are explicitly instructed to pick the safest, most privacy-preserving choice.

*8.3.2 Addressing RQ1-knowledge.* Teachers' cybersecurity, privacy, and digital literacy knowledge was measured using the SPDLK completed at two time points: pre-test and post-test. The scores for all questions were summed to give a total knowledge score out of 75.

A paired t-test found that teachers' SPDLK scores improved significantly after playing the game (Pre-test: $M$ = 60.43, $SD$ = 5.84, Post-test: $M$ = 63, $SD$ = 4.77, $t(20)$ = -2.24, $p < .037$). Although significant, teachers had a fairly high initial SPDLK scores and their improvements after playing the game were small. Our participants were fairly experienced in teaching cybersecurity, privacy, and digital literacy, and were probably more knowledgeable about these issues than the average teacher. Thus, it is possible that the game would result in more improvements for teachers who are new to teaching the topic.

In the post-test interviews, teachers also reported improvements in their privacy attitudes and understanding of children's online risks after playing the game. For example, one teacher explained:

> "I really liked in the game how those kinds of concerns were addressed with private messages. And I thought, that was not something I would have necessarily thought about teaching kids. And I think that's really important. Like sending a private message to someone to say 'you know what you said to so-and-so was not kind and I think you should take that comment down' or 'I think it's hurtful' or whatever. And that way you're not starting this troll-y conversation but you're addressing it. I thought that was a really positive strategy that the kids could use to deal with those things" (t10).

*8.3.3 Addressing RQ2-usability.* Usability of the game was measured using semi-structured interviews and 5-point Likert-scale questions in the post-test questionnaire. Interview data was analyzed using thematic analysis [12], and is used to address this research question and RQ3-Perception and RQ4-classroom.

**Ease of use:** Most teachers found the game easy to use, visually appealing, and they liked the design of the user interface. One teacher explained her impression of the game's usability:

> "I found it really easy to play, [and] to navigate through. So when I first logged on, I'm pretty tech savvy, I'm not the highest, but I'm certainly not [on] the low end of the spectrum, so I found it easy to get to, easy to look at. I never got frustrated with where I was supposed to go next or what I was supposed to do next. The directions/instructions were pretty clear" (t14).

**Fun:** Teachers rated the game as moderately fun ($M$ = 3.52, $SD$ = 1.7) which is lower than the children ($M$ = 4.16, $SD$ = 0.60). This is understandable, as the game is designed for 11-13 year-old children, with a storyline aligning with their experiences. However, teachers still recognized several positive aspects, noting that the animations, humor, storyline, graphics, and the challenge presented by the choices contributed to their enjoyment of the game. As one teacher stated:

> "It was really fun! I really enjoyed it. Yeah I thought it was very colorful and attractive. It looked current. It was something that I think they would enjoy playing. I think the thing that immediately turns kids off is if it looks dated. So I think making it look sort of current and modern is really important. And I thought this game did a good job with that. I thought the game did a great job of balancing the information with the fun aspect" (t10).

*8.3.4 Addressing RQ3-Perception.* Overall, teachers had positive comments about the game, and expressed interest in using it in their classrooms. They found the game engaging, and liked that it had specific learning outcomes which aligned with their curriculum. One teacher expressed the difficulty of finding engaging security and privacy resources which meet their needs, and thought The JOs met their criteria.

> "Sometimes it's hard to find the right one, that is age-appropriate, targets learning outcomes that we need to reach as teachers, and a lot of times we're just spending hours and hours looking for these resources. There's been times when I really wanted to find an engaging activity for this specific type of thing that I want to talk about, whether it be game, a video, or whatever. And it just does not exist online for what I'm envisioning. So I think if the game becomes available to teachers I would really hope that there is a lot of advertisement where like a lot of teachers know about it. Because I'm sure teachers are looking, but we just don't know where to find it". (t17).

Many teachers appreciated the authenticity of the game in terms of the characters, storyline, and the situations represented by the scenarios. This confirms the effectiveness of the design guidelines we used to design The JOs, which emphasize the importance of creating authentic learning environments to improve user engagement and learning outcomes [9, 26, 65]. The comments from teachers further provide evidence that these guidelines are also effective for designing security and privacy games. We discuss three elements of the game which garnered the most feedback from teachers: characters, scenarios, and choices in the game.

**Characters:** Teachers appreciated the diversity of the characters, the gender-inclusive scenarios, and the presentation of situations from both the girl and boy characters' perspectives. As one teacher noted, typically in security and privacy education girls are portrayed as victims, especially in situations about online reputation and rumors, which does not reflect children's realities.

> "I like that [it] came from a boy and girl perspective, girls are usually seen as the only targets or more of the majority of the targets but I like that the boy could also be in a targeted role and that was really pushed to the forefront. So I thought it was very equal in that way" (t6).

**Scenarios:** Teachers liked the variety of scenarios in the game, which makes the game applicable and appealing to a wider range of students. They also liked that the scenarios reflected children's realities, and included scenarios

unfolding at home and school, because too often security and privacy education in schools only focuses on safe use of technology at school. As one teacher stated

> "I liked that there were different times of [the] day that you could click on. It wasn't always at school. It was also at home, before school, because we know [when] the kids wake up, first thing they do is go on their social media. You see them waking up at 7:30, and oh they are already on their phone. [There were] situations at school with friends, peers, classmates, in the evening, at home, and then you piece [it all together] at the end of every day. These are the choices you made today, and these are the ramifications or consequences or this is the learning that happens from your choices" (t16).

When designing the scenarios, we made the decision to avoid situations that may potentially scare or traumatize children. From our conversations with teachers, we learned that police and invited speakers often spoke to children about sexting and the dangers of communicating with strangers online. These talks often left children scared and with no opportunity for discussion.

While these topics are important, we excluded them from our role-playing game to prevent possible negative psychological consequences on children. We believe these topics should be introduced to children in a different format before they experience them in a game. They also require parents and teachers to be more involved, and available to offer support and answer students' questions. Affirming our decision, none of the teachers indicated a need for them to be included in the game. Their inclusion could be considered in future iterations, possibly as an optional/advanced topic that teachers could introduce with additional supports.

**Choices:** Teachers appreciated the gray or uncertain options in each scenario. They found it representative of the real-world where the correct choice is not always clear, and thought the uncertain choices could be used to generate post-game discussions among students. Teachers also believed the different choices would allow children to practice or build their critical thinking skills. One teacher stated

> "I liked the different options that the game gave them too, that had to actually make them think. 'oh, I could do this, or maybe I'll do that, or that option sounds better.' And then it gave them the feedback based on their choice. I thought that was really valuable too" (t16).

For a few scenarios, some teachers did not agree with a choice presented, felt their preferred action was not included, or wanted to pick multiple options. We also observed this in our user testing with children. After reviewing these scenarios, we found that the choices were nuanced and represented real life situations where adults also often have incorrect mental models. We consider these types of scenarios to be important in the game, as they can improve teachers' own mental models, and also lead to interesting discussions in class.

*8.3.5 Addressing RQ4-Classroom.* Teachers expressed several strategies for incorporating The JOs into their security and privacy lessons, reflecting personal teaching styles. During these discussions, they also described some of their requirements for security and privacy games, and how well The JOs meets them. We first explain teachers' approaches for integrating The JOs in their lessons, and then discuss some of their requirements for security and privacy games.

**Using The JOs in lessons:** Three common approaches described by teachers included using the game as a: (i) pre-assessment activity, (ii) post-assessment activity, or as (iii) the lesson itself. Outside a lesson, teachers stated possibly using the game to establish rapport with students, or as a training tool before granting students technology privileges. As a pre-assessment tool, the game can be used to evaluate students' current security and privacy knowledge, prior to a main learning activity designed by teachers. Teachers explained potentially using results from the pre-assessment

activity to develop their actual lessons. For example, one teacher explained that if all students have sufficient knowledge of a fundamental topic, then her lesson would focus on more advanced topics. Thus, the game can be used to develop targeted security and privacy lessons, optimized to the unique learning needs of the students in a class.

As a post-assessment activity, teachers expressed that students would play The JOs after the lesson to practice their critical thinking skills in different security and privacy situations, presented in a safe simulated environment. When used for pre/post assessment, teachers described using The JOs with a security and privacy lesson they had already designed or envisioned during the interview. However, many teachers wanted to use The JOs as their main lesson, briefly introducing a topic and then having students play a day in the game to learn details. We believe that this preamble by teachers is important because children have different levels of security and privacy, and need to be introduced to certain concepts before encountering them in the game. For example, some children may be very familiar with social media, while others might have little to no direct experience with it. The teacher guide accompanying the production version of The JOs would help teachers in preparing their lessons, as it provides additional relevant material.

For all the approaches described, teachers expressed that instead of using the score to evaluate students' performance, they would use it as a guide to further explore certain security and privacy topics with children. For example, if most students picked the least privacy preserving choice in a scenario, teachers would mediate post-game conversations on why they chose this option. For students who were exploring and curious about the consequences, teachers would ask them to share their understanding of the topic with their peers as part of a peer-assisted learning approach. For students who believed the least privacy preserving choice was best, teachers would have conversations with them to improve their understanding of the topic. Thus, teachers expressed using the score to foster discussions, and using external assessment mechanisms to evaluate children's understanding of a topic. As one teacher explained:

> "So, I wouldn't necessarily use it as a marking or an assessment tool but as a tool for me to target who is my priority gonna to be when we work on digital literacy things. Like who seems to get it from a safety perspective. And I think this would be like a great activity to do early in the school year" (t28).

This approach was consistent with teachers' general attitude towards educational games, which they viewed as augmenting traditional learning mechanisms and approaches instead of replacing them. Teachers compared their intended use of The JOs to other educational games, such as *Prodigy Math*, which also use a scoring feature. Essentially, they expressed that since students' performance in a game can be influenced by other factors (e.g., distractions on the computing device), they preferred to use traditional evaluation mechanisms.

**Design considerations for security and privacy games:** Our conversations with teachers revealed three properties, which they considered to be important for security and privacy games for classrooms. Specifically, they expressed that these games should target learning goals from their curriculum, facilitate diverse types of play (individual and collaborative), and facilitate review and discussion. We discuss each of these requirements, providing evidence from teacher interviews on how well The JOs meets them.

***Integrate with the curriculum:*** Our interviews confirmed that The JOs met the curriculum needs of a diverse group of educators, both from public and private schools in different geographic areas. Specifically, teachers stated that the game addressed core components of their grade 6-8 Health, Language Arts, and Technology curriculum, making it easier for them to incorporate it into their lessons. One teacher stated:

> "It definitely covers some of the stuff as far as the media literacy part, where the kids have to use critical thinking skills when it comes to determining how they're using media. It covers some of the expectations. Well, I think the critical thinking section of media literacy is kind of the most important piece there, because

that's what I thought the game did the most, it got them thinking critically about the choices that they were making. And that's such a key piece for [grades 7 and 8]. So that's the section I'd focus on the most" (t14).

These comments indicate that security and privacy games designed for classrooms, must address core competencies in the curriculum for teachers to use them in their lessons.

***Facilitate diverse play:*** Teachers appreciated that The JOs supported both individual and collaborative play, and described strategies for incorporating both in their lessons, depending on the availability of classroom technology and the needs of the class. For example, they explained that collaborative play might be beneficial for ESL or students with learning disabilities who may benefit from working with their peers.

"A couple of the kids I could see pairing up just based on their learning difficulties. I have a little boy that's new to Canada, so his English is pretty limited. I would probably pair him up with somebody else because the language would be difficult for him to understand. There's another girl that's reading at the grade 2 level. I might have her just paired with a friend, but most students could do it on their own"(t1).

In other cases, given enough devices, teachers would ask students to play The JOs individually. With regards to individual play, some teachers noted that since The JOs is web-based and records players' progress, they may assign it as homework, and use class time for discussion and feedback about the students' choices and experiences with the game.

Our conversations with teachers showed that their use of games in classrooms depends on multiple factors unique to their students, their teaching style, and their school. However, the variety of strategies they described for using The JOs show that it could successfully accommodate a diversity of teacher and classroom needs.

***Facilitate review and debriefing:*** Regardless of how The JOs was used in lessons, teachers agreed that providing students feedback and discussing their choices was important, noting that scenarios in The JOs naturally lend themselves to these types of discussions. They specified several strategies for engaging in a discussion with students, such as using fishbowl, sharing circle, and think-pair-share strategies. Through these discussions, teachers hoped to create safe spaces for students to discuss their personal security and privacy experiences without judgement and repercussions. One teacher stated:

"Like, what are they really seeing online that they didn't think was big enough to tell me? But, then they see this example in the game, we talk about it and what variables would make it different. Then they go 'ding ding ding ding ding: We had a situation like this, and this is how it was different"' (t28).

These debriefs would also provide teachers an opportunity to holistically explore game scenarios. The JOs primarily explores scenarios from the victim's perspective, but teachers emphasized the importance of exploring different perspectives, especially for situations where children are both victims as well as the perpetrators. For example, in cyberbullying scenarios, The JOs teaches children what to do if they are a victim or bystander of cyberbullying. However, it does not explore why a child may engage in cyberbullying. As explained by one teacher, this perspective is also important to help perpetrators reflect on their behaviours and understand how it affects others, making the lesson more authentic for them.

"Why would Ben [perpetrator] want to do that? Why would Ben want to abuse this? Why would somebody want to have people miss their class because of a snow day [scenario in The JOs]? Because you're gonna have different kids in each class and some are going to be naturally the kids that want that and don't know a way to get out of it. And this might not reach them because they might be on the other side, [but] it doesn't need to be a lost lesson" (t6).

To facilitate these discussions, teachers expressed that The JOs must provide them the ability to review student responses. For example, they wanted to see which topics most students found challenging, such as potentially those with the lowest privacy/security score or with a high variability. While not included in our user testing, the production version of The JOs does include a teacher evaluation module that allows teachers to review student responses and complete other class management activities, such as creating and managing student accounts on the platform. Although this component was out of scope of our user testing, teacher feedback indicates that it is an expected component of security and privacy educational tools designed for classrooms.

## 9 DISCUSSION

Our main research goal was to design and develop an effective and empirically validated cybersecurity game for tweens, meant for use in the classroom. Our secondary goal was to explore whether procedural rhetoric is an effective strategy for designing cybersecurity games. We first designed and developed The JOs game and reflected on its design through the lens of procedural rhetoric. We then evaluated the game with children and teachers.

### 9.1 Acceptance by children

Our user testing showed that children found the game fun, and liked the realistic situations portrayed in the game. Their cybersecurity, privacy, and digital literacy knowledge and behavioural intent improved significantly immediately after playing the game, and the learning was sustained one week later. Children appreciated aspects of the game that can be attributed to procedural rhetoric. For example, they liked the anticipation of waiting to see the consequences of their actions. They also liked the exploratory nature of the game, and trying out different things to see different outcomes. This aspect of games is what makes them truly effective as a learning tool. It was important for our game to be accepted and enjoyable by children, because it contributes to improved learning as children invest more time in the learning activity[26]. We believe that children's engagement with The JOs contributed to their improved cybersecurity, privacy, and digital literacy scores after playing the game, and that these scores would further improve if The JOs was integrated as part of a classroom lesson.

### 9.2 Acceptance by teachers

Our teacher evaluation of The JOs revealed similar results. Specifically, teachers found that the situations portrayed reflected children's actual experiences with digital media. They also found the game engaging, and thought their students would enjoy the game. Teachers appreciated specific aspects of procedural rhetoric in the game, such as feedback and the experiential learning environment. They liked that the game offers feedback allowing children to reflect on their choices. Many teachers considered debriefing an important part of their lessons, and planned on using game feedback to have further discussions with students. Recent research with US teachers showed that to be accepted, cybersecurity educational tools for classroom use should highlight teachable privacy and security moments, and incorporate privacy and security features that meet educators' needs [35]. Our teacher feedback suggests that we have created such a tool.

We note that children and teachers have different acceptance criteria for educational games. For children, the most important factor is whether the game is fun. Regardless of the educational content, children are unmotivated to play games that are not fun. Teachers recognize this but they also value the game content, which must meet their curriculum and learning goals. They need to use the game within the constraints of a typical classroom lesson. Teachers found that The JOs met their learning goals for cybersecurity, privacy, and digital literacy. Teachers often frame lessons around issues that they observe from their students' use of digital media. Teachers reported that recent areas of concern include

cyberbullying, respecting the privacy of others, and copyright and ownership. These topics are among those addressed by The JOs. Our game also provides a modular design so that new topics can easily be added with no programming effort.

The JOs supports the digital literacy curriculum requirements of all thirteen provinces and territories in Canada. Teachers specifically appreciated this aspect of the game, and indicated that they often struggle to find relevant and engaging digital resources that also meet their curriculum needs. Teachers described various strategies of incorporating the game in their lessons, indicating that the game can accommodate different teaching styles and meet diverse classroom needs. Overall, the teachers in our study positively perceived The JOs game and wanted to use it in their classroom. However, we acknowledge a potential selection bias may have skewed the results in favour of the game. Specifically, we recruited teachers with interest in digital literacy and their participation in the study may indicate that they are in favour of using educational games. For other teachers, we hope that the alignment with the curriculum and the teacher guides (including lesson plans) would make The JOs an appealing educational tool.

### 9.3 Procedural rhetoric approach

Aligning with procedural rhetoric, we tried to create an environment where children can explore meaningful cybersecurity and privacy scenarios and gain an understanding of the consequences of their actions. Our game shows that simple game mechanics and narrative as advocated by procedural rhetoric can effectively teach children about a complex issue such as cybersecurity and privacy. In most cases, security and privacy cannot be adequately defined by a set of rules; situations are nuanced and we need children to develop empathy, awareness, vigilance, and an ability to weigh the potential consequences of their actions.

The game helped children become more conscious of their decisions, even for topics that they had not covered during their session's game play. We believe that our procedural rhetoric approach was at least in part responsible for this shift in mindfulness. The children were overall more conscious of their actions after game play, and several families later reported that the game led to further conversations about online security and privacy issues. Given these positive outcomes, we believe that procedural rhetoric is an effective approach for children's educational games addressing such nuanced subjects, at least for this age group.

Our game used simple game mechanics and an engaging narrative, and was effective at improving children's cybersecurity, privacy, and digital literacy knowledge and behaviour after being played for a short time. The simplicity of our game allows children to focus on the persuasive message of the game instead of being distracted by complex narrative or game mechanics. This also means that the game can easily be played by children with different gaming experience, which is particularly important for educational games. In our summative user study, many children who did not regularly play games were able to play The JOs without difficulty.

### 9.4 Designing cybersecurity games

Based on our experience with The JOs, we next discuss several design considerations.

*9.4.1 Foster critical thinking skills:* Security and privacy are key digital literacy topics, however, designing educational material for them presents some unique challenges. For example, security advice keeps changing due to the evolution of attacks and introduction of new threats. Thus, we cannot simply educate users once, but instead need to constantly re-educate them. This requires users to unlearn certain behaviours and learn new behaviours, which is difficult for adults, let alone children. Thus, in addition to teaching security- and privacy-preserving behaviours, cybersecurity games must

help children develop critical thinking skills which they can use to deal with new types of attacks. Our conversations with teachers confirmed the importance of developing these skills in children, as they are a core competency in their digital literacy curriculum. Teachers expressed difficulty in finding good cybersecurity resources for developing children's critical thinking skills, indicating a need for The JOs. Based on our experience, we have identified several factors which enable critical thinking in cybersecurity games.

**Allow exploration:** Games should allow users to explore choices for different security and privacy situations, instead of focusing on teaching them only the *correct* behaviour. That is because some digital literacy topics, such as privacy are nuanced and do not always have a *correct* answer. Others have multiple reasonable paths, where each choice provides different benefits and risks. In all these cases, the best approach is to educate users about possible choices and consequences, and allow them to choose the best path given their personal preferences. Thus, the objective of cybersecurity and privacy tools is not only behaviour change, but also to create informed digital citizens equipped with critical-thinking skills in an evolving digital world. Our game allows children to explore the consequences of different choices, in situations representing children's real-life digital experiences. While the game does identify the *most security- and privacy-preserving* choice for each scenario, its main objective is to allow children to explore different options, and consider the benefits and consequences of their choices.

The choices presented in The JOs allowed children to gain a more thorough understanding and be more mindful of cybersecurity and privacy issues, including privacy and security. We used established game design principles [10, 26, 65] to design choices such that both the least and most security- and privacy-preserving choices were meaningful for children, reflecting real-life situations where the lines between these types of choices is unclear. While the game nudges children towards more security- and privacy-conscious behaviours by offering more positive outcomes for these choices, the least security- and privacy-preserving choices also help children understand the main message of the game by demonstrating possible negative consequences and encouraging reflection. Similarly, the aggregate score displayed at the top of the screen acts as an indicator of children's overall security and privacy preserving behaviours in the game, but has no impact on the game outcomes. While its presence may gently nudge children towards making more security- and privacy-conscious choices, the objective of the game is not to achieve the highest score, and the design does not actively promote this strategy. We used careful messaging in the game, and instead of encouraging children to pick the "highest scoring" option, the game actually encourages them to make choices which they feel are best for Jo and Josie in a given situation. In fact, children could progress through the game by intentionally making the least security- and privacy-preserving choices simply to see their outcomes. In our user studies with both children and teachers, we observed that the consequences displayed in the newsfeed influenced their subsequent choices more than the score they received, and some made choices specifically to explore consequences.

**Promote reflection:** To help children think critically of their choices, cybersecurity games should offer sufficient opportunities for reflection, which is a key component of critical thinking [16]. Reflecting on their choices allows children to figure out what they did, and how they can improve in the subsequent parts of the game. A common mechanism for reflection is feedback, and The JOs used it to provide two opportunities for reflection: immediately after viewing the consequences of a choice and after completing a whole day (5 scenarios). To minimize disruptions, the short message at the end of a scenario only told the player how their choice affected Jo or Josie. The complete summary provided at the end of a day shows them their choice, consequences, the most security- and privacy-preserving choices choice, and how they can improve in the future. Another mechanism for reflection in The JOs was the newsfeed, which allowed players to review the consequences of their choices. Thus, different game mechanics can be used to enable reflection, with the goal of allowing the player to pause, think about their choices, and plan their next move.

Reflection not only leads to a better understanding of the educational material [11], but it also helps with the retention and knowledge transfer of the material learned from the game [31], as shown in the post-test interviews and questionnaires. We also observed children engaging in reflection while playing The JOs. They would look forward to the feedback, and then verbalize their thought process, such as why they made a specific choice or what they would have done differently. Thus, our work demonstrates that enabling reflection in games supports critical thinking. While games should provide opportunities for reflection, too many of these opportunities can be disruptive and annoying for children because it takes their attention away from the primary task, which is to play the game. Thus, designers should provide a balance between offering opportunities to reflect and not disrupting the player's flow in the game.

We also note that assessing 'critical thinking' is challenging since it is difficult to quantify. In our work, we relied on observational and interview data, as well as indirect measures. Children would verbalize their thought-process as they considered the choices, demonstrating reflection, and teachers repeatedly remarked that the game would help their students with critical thinking. Indirectly, children spent the most time on the Choices screens, and we have eye-tracking data showing them pausing on the different options.

**Promote discussion:** Games can provide reflection opportunities to children by triggering discussions with peers, teachers, and parents. These discussions can take place within the game or outside as a separate component. Having discussions about the game content with peers allows children to hear from others' experiences, which helps them reflect on their own choices and broaden their understanding of the content beyond what is provided by the game. Adults, such as parents and teachers can have discussions with children to provide additional scaffolding, especially for sensitive topics. To this extent, cybersecurity games must facilitate these types of discussions. We found scenarios having multiple reasonable paths led to the most discussion with the researcher for both children and teachers. Teachers also found these type of scenarios valuable, and envisioned using them to generate classroom discussion with students. Several families in our user study with children also reported that the game led to subsequent family conversations about online security and privacy issues. We further observed this during the study when some parents were seated next to the child. To prevent parents from influencing children's measured performance in our user study, we tried to minimize these discussions by seating the parent/child in different locations of the study space, but in a real-life situation, these conversations would be beneficial.

Potential discussion questions should also accompany cybersecurity games, especially those designed for classroom use, to make it easier for teachers to incorporate discussion into their lessons. The production version of The JOs game comes packaged with teacher guides that include lesson plans and discussion questions, and teachers expressed that these will make it easier for them to use the game in classrooms.

*9.4.2 Authenticity.* Our user testing with both children and teachers showed that participants appreciated the authenticity of The JOs. They liked that the scenarios represented realistic situations, and teachers remarked that children are not interested in learning from security and privacy situations that do not reflect their reality. Authenticity in games allows children to learn more effectively, as they can use prior knowledge and experiences to process new information and concepts [44]. As shown in the post-test interviews, authentic scenarios also help children apply what they have learned to situations outside of the game. Thus, cybersecurity games should create authentic experiences for children, by making all aspects of the game relateable, including the educational content, characters, and choices.

**Educational content:** Security and privacy advice presented in games should reflect children's reality and not an adult's perspective on how children should behave. For instance, some experts believe that children under the minimum age for social media platforms (13-years) [6] should not use social media. However, in reality many younger children

regularly use these platforms. Instead of simply telling them to not use these platforms, we should advise them on safe practices and provide strategies for avoiding common pitfalls. Sensitive topics or situations, while relevant, should be presented with sufficient scaffolding from adults (parents or teachers), who can answer questions children may have.

The rapid evolution of technology introduces new security and privacy concerns relevant to children; cybersecurity educational tools should address these new concerns and update old advice. For example, many tweens are now concerned about privacy violations from family, especially parents who access their data or share information about them without their consent [15, 43]. Many parents are unaware that they are violating children's privacy when sharing information about them (i.e., photos) on social media, as pointed out by a teacher who was a parent herself. She expressed that playing The JOs helped her understand these issues better, and will influence her future sharing behaviours. Thus, cybersecurity educational tools should address emerging security and privacy concerns, and engage all parties involved.

**Characters:** Positive associations and perceptions of game characters facilitate children's learning in educational games. This also includes the trustworthiness of characters, as children are more likely to believe security and privacy advice from characters they consider to be trustworthy. One way to increase positive associations is to make characters relatable to children. In The JOs, we chose two main characters so both boys and girls could relate, and designed them to be representative of 11-13 year-old children. Children in our testing liked the characters and thought they were good people who tried to do the right thing — a message we wanted to convey in our game. In game scenarios, we made sure that both Jo and Josie were represented equally in situations where they were the victims of negative behaviour and situations where they had an opportunity to practice negative behaviour. We similarly tried to include diversity in ethnicity, abilities, and appearance among the secondary characters. Teachers appreciated the diversity of the game characters, and especially liked the gender inclusivity of the scenarios, which equally portrayed Jo and Josie as victims. They stated that cybersecurity tools often portray only girls as victims, especially in situations involving rumors and online reputation, which is not representative of what happens in real life. We believe the authenticity of the characters contributed to children's improved learning in the game. While children had an overall positive perception of the characters, some showed a same-gender preference for either Jo or Josie. Some boys expressed that they would be friends with Jo and not Josie and the girls expressed a similar preference for Josie.

**Improving authenticity:** Authenticity should be a key design consideration for cybersecurity games, and should be incorporated into the design from the beginning. This can be achieved by involving representative users early in the design process to understand their requirements, and evaluate potential designs. For The JOs, we evaluated the design with children at different stages of the design process, through four user studies, iteratively improving the designs based on user feedback. For example, early testing of the visual designs showed that children preferred slightly older characters (closer to 13-year olds), because they considered them to be aspirational. We used this feedback to improve our character designs, which children liked and found relatable in our summative user study. User involvement can vary, ranging from being part of the design team to only evaluating the designs and providing feedback. We used both approaches in the design of The JOs. Although children were not part of the design team, we frequently conducted user studies to involve them at key stages of the design process, such as requirements gathering. A group of K-12 Educators was part of the design team, so they were very involved, provided requirements for the game, and helped design the educational content. We also tested the final prototype of the game with a new group of teachers.

*9.4.3 Technological considerations:* A challenge with developing cybersecurity resources, especially games, is that they can become outdated fairly quickly with the evolution of technology and the introduction of new threats. Thus, their designs need to be future-proofed so they can be updated with little development effort. The use of outdated resources

negatively affects learning, because children may not be engaged, or may learn outdated lessons. In addition to this, users may be unable to actually access old resources because their underlying technology is no longer supported, as is the case now with many Flash games. Teachers in our user study echoed some of these concerns. They liked that The JOs was current, both in terms of its design and educational content, and could be easily accessed without needing to install any special software, which can be an issue for classroom resources. They expressed that available cybersecurity resources are often outdated, which makes students not take their educational content seriously.

During our initial discussions with our partner organization, we learned that they also found it challenging to keep their cybersecurity resources updated, mostly due to the development work required. Their "Jo Cool or Jo Fool" resource, which inspired the design of The JOs, was developed in 2000 and has never been updated. Given this, we created a modular design so individual components (e.g., images, text) can be updated with little development effort. New scenarios can be added to address topics that become important due to the culture or political climate (e.g., spotting misinformation in the era of "fake news"). As the game gets used in classrooms, we envision ideas for these new scenarios to come from teachers, who have first-hand knowledge of the security and privacy issues children experience when using digital media. Although the game is designed for 11-13 year-olds, the modular design makes it easy to extend for younger children. Players might benefit from such a game where they can see Jo/Josie's digital lives evolve as they grow older. Currently, the game is available in English and French, but more languages can be easily added. This might benefit schools with a significant number of ESL students.

For the development of new cybersecurity games, we recommend a modular design using development technology or frameworks that allow easy updates. We developed The JOs using popular web-based technology and frameworks, as these technologies are less likely to become obsolete in the near future. When designing for classroom use, developers should be mindful of the technology available in schools. Many schools do not have access to the latest digital devices or software, and teachers often have to go through their IT support to install applications. Thus, cybersecurity games may need to be compatible with older technology, and teachers should be able to access them easily. We designed The JOs for high compatibility across platforms. It is accessible on both desktops and tablets, using all major web browsers and has backwards compatibility with older versions of the web browsers. Although this added significant development time to the game, it was necessary for the game to be accessible to a wide range of schools across the country.

### 9.5 Limitations

We note the limitations of our work, specifically relating to the user studies:

**Recruitment:** Results may have been influenced by a sampling bias in terms of participants. Specifically, we found that test scores were quite high and improvements in tweens' cybersecurity, privacy, and digital literacy were fairly small between test points. This could be because we unintentionally recruited participants who already had above average digital literacy. Anecdotally, our teachers asserted that many of the tweens they teach would significantly benefit from the game. For teachers, while we made an effort to recruit from different locations across Canada, more than half were from Ottawa, and generally employed in schools located in areas of medium to high socioeconomic status.

**Evaluating improvements in cybersecurity, privacy, and digital literacy:** We tested children after one week to assess improvements in children's cybersecurity, privacy, and digital literacy; although promising, we cannot be certain whether these improvements will be sustained and whether these result in lasting real-life behaviour changes. Furthermore, we used self-reports and hypothetical scenarios, so participants' actual behaviour may differ.

**Lack of a control group:** We did not compare our results against existing educational mechanisms used by participants. Determining an equivalent and reliable control condition poses significant challenges.

**Social-desirability effect:** We note that due to the social-desirability effect, participants in our lab-based user studies may have responded differently to the game than they would in a more realistic setting. In future work, we hope to test the game in classrooms, where children would play it around their peers and in the presence of teachers.

### 9.6 Future work

We intend to evaluate the game with parents to understand their perceptions, and explore whether it can be used within families to promote security and privacy-conscious conversations. We will also evaluate the game with children from different socioeconomic backgrounds to explore any potential effects. With a more representative sample, we hope to see more improvements in digital literacy than was observed in our study. In classrooms, we will evaluate the usability and effectiveness of the game against experiential learning mechanisms commonly used by teachers.

## 10 CONCLUSION

With the growth of tweens' technology use, it is important to improve their cybersecurity, privacy, and digital literacy skills to protect them from online threats. As teachers are often expected to teach tweens about these issues, there is also a need to improve their own awareness of cybersecurity and to provide them with the appropriate educational tools for tweens. This paper explores how a game exhibiting properties of procedural rhetoric can be used in classrooms to improve tweens' cybersecurity and privacy skills. We worked with MediaSmarts to design and develop *The JOs*, which has already demonstrated real-world impact through deployment in over 300 Canadian elementary schools since this research was concluded. An additional 35 school districts are currently previewing The JOs for use within their respective schools.

Using a systematic approach to the design and development, we evaluated the usability and effectiveness of The JOs through five user studies. The first three studies provided iterative feedback on the conceptual design and content during development of the JOs. The fourth user study of the fully-functional game with tweens showed that The JOs improved tweens' cybersecurity, privacy, and digital literacy, and was positively received overall. Importantly, tweens reported that the game reflected their real-life encounters. In our fifth user study, elementary school teachers confirmed that the game aligned with their curriculum, and that they wanted to integrate it into their classroom.

Overall, we contribute a modular, easily extensible, and widely-deployed educational game that is grounded in the persuasive theory of procedural rhetoric and that is demonstrated to increase tweens' critical thinking skills related to cybersecurity, privacy, and digital literacy. Furthermore, we offer evidence that the game promotes larger discussions around these topics between tweens and the adults in their lives. We also provide reflections and insights on the overall design and development process, which can be helpful for future designers of cybersecurity and privacy educational tools.

## ACKNOWLEDGMENTS

**Other Contributors:** We gratefully acknowledge the contributions of Christine Mekhail, who did most of the graphic design work and early formative testing with users. We are also grateful for our educational partners at MediaSmarts and their involvement in the design, development, and deployment of The JOs game.

**Funding:** This work was funded by the MITACS, Canada Research Chairs, and NSERC Discovery Grant programs.

## REFERENCES


[1] Icek Ajzen. 1991. The Theory of Planned Behaviour. *Organizational Behaviour and Human Decision Processes* 50, 2 (1991), 179–211.

[2] Leonard Annetta and Stephen Bronack (Eds.). 2011. *Serious Educational Game Assessment: Practical Methods and Models for Educational Games, Simulations and Virtual Worlds.* Springer, New York, NY, USA.

[3] Sabra Ayres. 2020. Zoom Bombing and Data Breaches: As Classrooms Go Back Online, Will Hackers Find Opportunities? Retrieved June 25, 2021 from https://spectrumlocalnews.com/tx/san-antonio/news/2020/07/23/cybersecurity-schools-online-learning.

[4] Bradley Barth. 2020. Roblox Hacker Enabled by Insider Threats; Expert Offers Tips to Curb Rogue Employees. Retrieved June 25, 2021 from https://www.scmagazine.com/home/security-news/roblox-hacker-enabled-by-insider-threats-expert-offers-tips-to-curb-rogue-employees.

[5] Kanad Basu, Suha Sabi Hussain, Ujjwal Gupta, and Ramesh Karri. 2020. COPPTCHA: COPPA Tracking by Checking Hardware-Level Activity. *IEEE Transactions on Information Forensics and Security* 15 (2020), 3213–3226. https://doi.org/10.1109/TIFS.2020.2983287

[6] Shea Bennett. 2014. Minimum Age Requirements: Twitter, Facebook, Instagram, Snapchat, WhatsApp, Secret. Retrieved June 25, 2021 from http://www.adweek.com/digital/social-media-minimum-age.

[7] Jim Bizzocchi. 2010. The Role of Narrative in Educational Games and Simulations. In *Educational Gameplay and Simulation Environments: Case Studies and Lessons Learned.* IGI Global, Hershey, PA, USA, 68–83. https://doi.org/10.4018/978-1-61520-731-2.ch004

[8] Yukon Digital Literacy & Citizenship Blog. 2019. A Day in the Life of the JOs. Retrieved June 25, 2021 from https://yukondigitalcitizen.ca/2019/07/18/a-day-in-the-life-of-the-jos.

[9] Ian Bogost. 2007. *Persuasive Games: The Expressive Power of Videogames.* MIT Press, Cambridge, MA, USA.

[10] Ian Bogost. 2008. The Rhetoric of Video Games. In *The Ecology of Games: Connecting Youth, Games, and Learning*, Katie Salen (Ed.). MIT Press, Cambridge, MA, USA, 117–140.

[11] John Bransford and Rodney Cocking (Eds.). 2000. *How People Learn: Brain, Mind, Experience, and School: Expanded edition.* National Academies Press, Washington, DC, USA. https://doi.org/10.17226/9853

[12] Virginia Braun and Victoria Clarke. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. https://doi.org/10.1191/1478088706qp063oa

[13] Deccan Chronicle. 2018. New Malware Attacks Children's App With Pornographic Content. Retrieved June 25, 2021 from https://www.deccanchronicle.com/technology/in-other-news/170118/new-malware-attacks-childrens-app-with-pornographic-malware.html.

[14] Australian Communications and Media Authority. 2012. Zippep's Astro Circus. Retrieved June 25, 2021 from https://fuse.education.vic.gov.au/Resource/LandingPage?ObjectId=e6a6a20d-6dc6-4602-a739-2ad7d6616465.

[15] Katie Davis and Carrie James. 2013. Tweens' Conceptions of Privacy Online: Implications for Educators. *Learning, Media and Technology* 38, 1 (2013), 4–25. https://doi.org/10.1080/17439884.2012.658404

[16] John Dewey. 1933. *How We Think: A Restatement of the Relation of Reflective Thinking to the Educative Process.* D.C. Heath & Company, Lexington, MA, USA.

[17] Frances Dewing. 2019. The Emerging Gray-App Threat: Mobile Kids' Apps. Retrieved June 25, 2021 from https://www.rsaconference.com/library/presentation/the-emerging-grey-app-threat-mobile-kids-apps-are-gateway-to-parents.

[18] Lars Doucet and Vinod Srinivasan. 2010. Designing Entertaining Educational Games Using Procedural Rhetoric: A Case Study. In *Proceedings of the Symposium on Video Games (Sandbox '10).* ACM, New York, NY, USA, 5–10. https://doi.org/10.1145/1836135.1836136

[19] Serge Egelman, Marian Harbach, and Eyal Peer. 2016. Behavior Ever Follows Intention?: A Validation of the Security Behavior Intentions Scale (SeBIS). In *Proceedings of the Conference on Human Factors in Computing Systems (CHI '16).* ACM, New York, NY, USA, 5257–5261. https://doi.org/10.1145/2858036.2858265

[20] Simon Egenfeldt-Nielsen. 2007. Third Generation Educational Use of Computer Games. *Educational Multimedia and Hypermedia* 16, 3 (2007), 263–281.

[21] Europol. 2020. Catching the Virus: Cybercrime, Disinformation and the COVID-19 Pandemic. Retrieved June 25, 2021 from https://www.europol.europa.eu/track/click/8391/11931.

[22] John Ferrara. 2013. Games for Persuasion: Argumentation, Procedurality, and the Lie of Gamification. *Games and Culture* 8, 4 (2013), 289–304. https://doi.org/10.1177/1555412013496891

[23] Consortium for School Networking. 2020. State of EdTech Leadership Report. Retrieved June 25, 2021 from https://www.cosn.org/focus-areas/leadership-vision/state-edtech-leadership.

[24] Howard Gardner. 2011. *The Unschooled Mind: How Children Think and How Schools Should Teach.* Basic Books, New York, NY, USA.

[25] James Paul Gee. 2003. *What Video Games Have to Teach Us about Learning and Literacy.* Palgrave Macmillan, New York, NY, USA.

[26] James Paul Gee. 2005. Learning by Design: Good Video Games as Learning Machines. *Digital Education Review* 2, 1 (2005), 5–16. https://doi.org/10.2304/elea.2005.2.1.5

[27] James Paul Gee. 2007. *Good Video Games and Good Learning: Collected Essays on Video Games, Learning and Literacy.* Peter Lang Publishing, Bern, Switzerland.

[28] Thomas A. Goldman, Frank J. Lee, and Jichen Zhu. 2014. Using Video Games to Facilitate Understanding of Attention Deficit Hyperactivity Disorder: A Feasibility Study. In *Proceedings of the Symposium on Computer-Human Interaction in Play (CHI PLAY '14).* ACM, New York, NY, USA, 115–120. https://doi.org/10.1145/2658537.2658707

[29] Google. 2017. Interland - Be Internet Awesome. Retrieved June 25, 2021 from https://beinternetawesome.withgoogle.com/en_us/interland.

[30] Boston Herald. 2020. 'Zoom-bombing' on the Rise: Hijackers Invade Videoconferences for Work, School, FBI Says. Retrieved June 25, 2021 from https://www.mercurynews.com/coronavirus-zoom-bombing-hijackers-videoconferences.

[31] Talib S Hussain and Susan L Coleman (Eds.). 2014. *Design and Development of Training Games: Practical Guidelines from a Multidisciplinary Perspective.* Cambridge University Press, Cambridge, United Kingdom.

[32] Gokul Chettoor Jayakrishnan, Gangadhara Reddy Sirigireddy, Sukanya Vaddepalli, Vijayanand Banahatti, Sachin Premsukh Lodha, and Sankalp Suneel Pandit. 2020. Passworld: A Serious Game to Promote Password Awareness and Diversity in an Enterprise. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '20).* USENIX, Berkeley, CA, USA, 1–18.

[33] Mansureh Kebritchi. 2010. Factors Affecting Teachers' Adoption of Educational Computer Games: A Case Study. *British Journal of Educational Technology* 41, 2 (2010), 256–270. https://doi.org/10.1111/j.1467-8535.2008.00921.x

[34] Robert Kenny and Glenda Gunter. 2011. Factors Affecting Adoption of Video Games in the Classroom. *Interactive Learning Research* 22, 2 (2011), 259–276.

[35] Priya C Kumar, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 2019. Privacy and Security Considerations for Digital Technology Use in Elementary Schools. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI '19).* ACM, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300537

[36] Sonia Livingstone, Leslie Haddon, Anke Görzig, and Kjartan Ólafsson. 2011. Risks and Safety on the Internet: The Perspective of European children: Full Findings and Policy Implications from the EU Kids Online Survey of 9-16 year olds and their Parents in 25 Countries. In *EU Kids Online, Deliverable D4.* EU Kids Online Network, London, United Kingdom, 9–16.

[37] Minhua Ma and Andreas Oikonomou (Eds.). 2011. *Serious Games and Edutainment Applications.* Springer, New York, NY, USA. https://doi.org/10.1007/978-1-4471-2161-9

[38] Thomas W Malone. 1981. Toward a Theory of Intrinsically Motivating Instruction. *Cognitive Science* 5, 4 (1981), 333–369.

[39] Thomas W Malone and Mark R Lepper. 1987. Making Learning Fun: A Taxonomy of Intrinsic Motivations for Learning. In *Aptitude, Learning, and Instruction, Vol. 3: Conative and Affective Process Analyses*, Richard E Snow and Marshall J Farr (Eds.). Lawrence Erlbaum Associate, Hillsdale, NJ, USA, 223–253.

[40] Sana Maqsood. 2020. *The Design, Development and Evaluation of a Digital Literacy Game for Preteens.* Ph.D. Dissertation. Carleton University, Ottawa, Canada. https://doi.org/10.22215/etd/2020-13968

[41] Sana Maqsood, Christine Mekhail, and Sonia Chiasson. 2018. A Day in the Life of JOs: A Web-Based Game to Increase Children's Digital Literacy. In *Proceedings of the Conference on Interaction Design and Children (IDC '18).* ACM, New York, NY, USA, 241–252. https://doi.org/10.1145/3202185.3202753

[42] Allan Martin. 2005. DigEuLit - A European Framework for Digital Literacy: A Progress Report. *Journal of eLiteracy* 2, 2 (2005), 130–136.

[43] Florence Martin, Chuang Wang, Teresa Petty, Weichao Wang, and Patti Wilkins. 2018. Middle School Students' Social Media Use. *Educational Technology & Society* 21, 1 (2018), 213–224.

[44] Caroline Masse, Kelly Pounds, Eric Church, Robert E Waters, and Vance Souders. 2014. Story for Learning and Gaming. In *Design and Development of Training Games: Practical Guidelines from a Multidisciplinary Perspective*, Talib S Hussain and Susan L Coleman (Eds.). Cambridge University Press, Cambridge, United Kingdom, 93–120. https://doi.org/10.1017/CBO9781107280137.005

[45] Angela McFarlane, Anne Sparrowhawk, and Ysanne Heald. 2002. Report on the Educational Use of Games. Retrieved June 25, 2021 from http://consilr.info.uaic.ro/uploads_lt4el/resources/pdfengReportontheeducationaluseofgames.pdf.

[46] MediaSmarts. 2000. Jo Cool or Jo Fool Game. Retrieved June 25, 2021 from http://mediasmarts.ca/game/jo-cool-or-jo-fool-grades-6-8.

[47] MediaSmarts. 2012. Digital and Media Literacy Outcomes by Province and Territory. Retrieved June 25, 2021 from http://mediasmarts.ca/teacher-resources/digital-and-media-literacy-outcomes-province-territory.

[48] MediaSmarts. 2012. MediaSmarts' Games. Retrieved June 25, 2021 from http://mediasmarts.ca/digital-media-literacy/educational-games.

[49] MediaSmarts. 2018. A Day in the Life of the JOs (Grades 6-8). Retrieved June 25, 2021 from http://mediasmarts.ca/teacher-resources/licensed-resources/day-life-jos-grades-6-8.

[50] Christine Mekhail. 2016. *A Day in the Life of the JOs: The Design of an Educational Game on Privacy.* Master's thesis. Carleton University, Canada.

[51] David Michael and Sandra Chen. 2005. *Serious Games: Games That Educate, Train, and Inform.* Course Technology, Boston, MA, USA.

[52] Bukelwa Ngoqo and Stephen V Flowerday. 2015. Exploring the Relationship Between Student Mobile Information Security Awareness and Behavioural Intent. *Information & Computer Security* 23, 4 (2015), 406–420. https://doi.org/10.1108/ICS-10-2014-0072

[53] Lindsey O'Donnell. 2020. Ransomware and Zoom-Bombing: Cyberattacks Disrupt Back-to-School Plans. Retrieved June 25, 2021 from https://threatpost.com/ransomware-zoom-cyberattacks-school/159093.

[54] Government of Alberta. 2017. Information and Communication Technology Curriculum (Grades 1-12). Retrieved June 25, 2021 from https://education.alberta.ca/media/3114953/ictpos.pdf.

[55] Government of British Columbia. 2017. Applied Design, Skills, and Technologies Curriculum (Grades 1-12). Retrieved June 25, 2021 from https://curriculum.gov.bc.ca/curriculum/adst/6/core.

[56] Ontario Ministry of Education. 2012. K-12 Ontario Curriculum. Retrieved June 25, 2021 from http://www.edu.gov.on.ca/eng/teachers/curriculum.html.

[57] Government of Manitoba. 2012. Literacy with Information and Communication Technology Curriculum (Grades 1-12). Retrieved June 25, 2021 from http://www.edu.gov.mb.ca/k12/tech/lict/index.html.

[58] Government of Saskatchewan. 2012. Digital Citizenship Education in Saskatchewan Schools. Retrieved June 25, 2021 from https://publications.saskatchewan.ca/#/products/74447.

[59] Sarah Perez. 2018. Roblox Responds to the Hack That Allowed a Child's Avatar to Be Raped in Its Game. Retrieved June 25, 2021 from https://techcrunch.com/2018/07/18/roblox-responds-to-the-hack-that-allowed-a-childs-avatar-to-be-raped-in-its-game.

[60] Pooja Pradeep and Sujata Sriram. 2016. The Virtual World of Social Networking Sites: Adolescent's Use and Experiences. *Psychology and Developing Societies* 28, 1 (2016), 139–159. https://doi.org/10.1177/0971333615622911

[61] Portia Pusey and William A Sadera. 2011. Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. *Digital Learning in Teacher Education* 28, 2 (2011), 82–85. https://doi.org/10.1080/21532974.2011.10784684

[62] Janet C Read. 2008. Validating the Fun Toolkit: An Instrument for Measuring Children's Opinions of Technology. *Cognition, Technology & Work* 10, 2 (2008), 119–128. https://doi.org/10.1007/s10111-007-0069-9

[63] Ute Ritterfeld, Michael Cody, and Peter Vorderer (Eds.). 2009. *Serious Games: Mechanisms and Effects.* Routledge, Oxfordshire, United Kingdom.

[64] Dana Ruggiero. 2014. Spent: Changing Students' Affective Learning Toward Homelessness Through Persuasive Video Game Play. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI '14).* ACM, New York, NY, USA, 3423–3432. https://doi.org/10.1145/2556288.2557390

[65] Katie Salen and Eric Zimmerman. 2004. *Rules of Play: Game Design Fundamentals.* MIT Press, Cambridge, MA, USA.

[66] Kristin L Schneider, John Ferrara, Bri Lance, Andrew Karetas, Susan Druker, Emily Panza, Barbara Olendzki, Victoria Andersen, and Lori Pbert. 2012. Acceptability of an Online Health Videogame to Improve Diet and Physical Activity in Elementary School Students: "Fitter Critters". *Games for Health: Research, Development, and Clinical Applications* 1, 4 (2012), 262–268. https://doi.org/10.1089/g4h.2012.0009

[67] Barry Schwartz. 2004. *The Paradox of Choice – Why More Is Less.* Ecco, New York, NY, USA.

[68] Mikko Siponen, Seppo Pahnila, and Adam Mahmood. 2007. Employees' Adherence to Information Security Policies: An Empirical Study. In *Proceedings of the International Information Security Conference (SEC '07).* Springer, New York, NY, USA, 133–144. https://doi.org/10.1007/978-0-387-72367-9_12

[69] Tony Stephanou and Rabelani Dagada. 2008. The Impact of Information Security Awareness Training on Information Security Behaviour: The Case for Further Research. In *Proceedings of the Information Security South Africa Conference (ISSA '08).* Springer, New York, NY, USA, 1–21.

[70] Radio Télévision Suisse. 2017. DataK Game. Retrieved June 25, 2021 from https://seriousgamessociety.org/2017/03/13/datek-a-game-on-the-use-of-personal-data.

[71] Sreenivas Sremath Tirumala, Abdolhossein Sarrafzadeh, and Paul Pang. 2016. A Survey on Internet Usage and Cybersecurity Awareness in Students. In *Proceedings of the Conference on Privacy, Security and Trust (PST '16).* IEEE, New York, NY, USA, 223–228. https://doi.org/10.1109/PST.2016.7906931

[72] Carnegie Mellon University. 2007. Carnegie Cyber Academy. Retrieved June 25, 2021 from http://www.carnegiecyberacademy.com.

[73] Arielle Waldman. 2020. Cyber Attacks on Schools Increasing Amid Remote Learning Shift. Retrieved June 25, 2021 from https://searchsecurity.techtarget.com/news/252489363/Cyber-attacks-on-schools-increasing-amid-remote-learning-shift.

[74] Lance Whitney. 2020. School-based Cyberattacks Are on the Rise. Retrieved June 25, 2021 from https://www.techrepublic.com/article/cyberattacks-against-schools-are-on-the-rise.

[75] Leah Zhang-Kennedy and Sonia Chiasson. 2021. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *Computing Surveys* 54, 1 (2021), 1–39. https://doi.org/10.1145/3427920