Engagement, Usability, and Learning in Narrative-Driven Cybersecurity Awareness Games

Claire Jennings
Computing & Software Systems
University of Washington
Bothell, USA
clairejennings343@gmail.com

Seth Pham
Computing & Software Systems
University of Washington
Bothell, USA
seth.pham@gmail.com

Marc J. Dupuis
Computing & Software Systems
University of Washington
Bothell, USA
marcjd@uw.edu

***Abstract*—Cybersecurity awareness remains a persistent challenge despite significant investment in technical defenses. Attackers exploit the human element, requiring new approaches that sustain attention and promote actionable decision-making. This paper evaluates a narrative-driven, choose-your-own-adventure (CYOA) serious game designed to teach core cyber-hygiene practices. Narrative drafts were generated with the assistance of AI-based text generation tools and subsequently refined by the research team, illustrating the potential of AI to support scalable development of cybersecurity training content. Two design variables were systematically compared: narrative depth (long-form versus short-form storytelling) and interaction modality (link-based versus swipe-based navigation). A total of 422 participants were recruited via Amazon Mechanical Turk, representing a diverse adult population. Outcomes were measured through custom Likert-style items assessing engagement, usability, and perceived learning, supported by qualitative reflections. Results show that long-form narratives increased immersion and contextual understanding, while short-form narratives emphasized efficiency and decision reinforcement. Usability ratings were high across all conditions, with swipe-based navigation slightly preferred on mobile devices. Participants consistently reported increased awareness of phishing, oversharing, identity theft, and ransomware. These findings demonstrate the viability of narrative-driven games as scalable, user-centered cybersecurity training tools. We discuss design implications for organizations deploying awareness programs across heterogeneous desktop and mobile platforms and highlight opportunities for hybrid narrative strategies that balance immersion and efficiency. (*Abstract*)**

***Keywords*— cybersecurity awareness, serious games, narrative learning, human factors in security, AI-based narrative development, game-based learning** *(key words)*

I. Introduction

Cybersecurity incidents increasingly exploit human factors, from hurried clicks on suspicious links to habitual oversharing of personal information. Despite continuing investment in technical defenses, individuals remain a critical line of defense against common threats such as phishing, identity theft, and ransomware [1]. Traditional awareness training—policy briefings, slide decks, and periodic emails—often struggle to hold attention or translate abstract rules into everyday judgments. Research on serious games suggests an alternative: interactive experiences that situate decisions in meaningful contexts, provide immediate feedback, and leverage intrinsic motivation to sustain engagement. At the same time, not all games are equally effective; the design of narrative and interface can strongly influence learner experience and outcomes.

This paper examines a narrative-driven, choose-your-own-adventure (CYOA) game created to teach core cyber-hygiene concepts through branching scenarios. The game covers four threats that are both prevalent and personally consequential: phishing, oversharing on social platforms, identity theft, and ransomware. Each scenario places the learner in a concrete situation with choices at critical junctures and immediate, in-story consequences. Narratives were drafted with the assistance of AI-based text generation tools, which provided branching variations and alternative phrasings. Human researchers iteratively refined these drafts to ensure accuracy, coherence, and alignment with pedagogical objectives. Two design dimensions are varied systematically. First, narrative depth alternates between long-form passages that layer character background and contextual cues, and short-form passages that compress the storyline to emphasize decision points. Second, interaction modality alternates between traditional link-based navigation and swipe-based navigation optimized for touch devices. These dimensions reflect common design choices faced by practitioners who must balance immersion against efficiency and desktop-first layouts against mobile-first access.

The study focuses on three outcomes that are both practical and measurable in awareness contexts: engagement, usability, and perceived learning. Engagement captures the degree of attention, immersion, enjoyment, and perceived realism experienced during play. Usability assesses whether the interface gets out of the way—supporting clear instructions, intuitive navigation, and low friction on common devices. Perceived learning captures changes in self-reported awareness and confidence to apply best practices, complemented by qualitative reflections that can surface what ‘stuck’ and why. These outcomes align with the immediate goals of many organizational programs: sustain attention long enough to practice decisions, ensure the tool is easy to use for a broad audience, and reinforce actionable strategies that transfer to daily behavior.

Two design tensions motivate our comparisons. The first is the depth-efficiency trade-off in narrative. Long-form stories can model social pressure, ambiguity, and cascading consequences—the psychological texture of real incidents—but they demand more reading time and risk fatigue among learners seeking concise guidance [2], [3]. Short-form narratives address efficiency by streamlining exposition and concentrating on decisions, yet they may fail to produce the sense of realism needed for deep reflection [4], [5]. The second tension concerns interaction modality. Touch-centric environments are increasingly common in both consumer and workplace settings. Swipe-based navigation promises fluid progression on mobile devices, but link-based options remain familiar and precise on desktops. Understanding whether modality meaningfully alters engagement and perceived learning is important for teams that must deploy training across heterogeneous device fleets.

Against this backdrop, the present study addresses the following questions: (RQ1) How does narrative depth (long-form vs. short-form) relate to self-reported engagement? (RQ2) How does interaction modality (link vs. swipe) relate to perceived usability? (RQ3) To what extent do participants report learning gains across conditions, and do qualitative reflections clarify how narrative or modality contribute to those gains? We explore these questions through the use of a large-scale survey.

Our findings preview three themes. First, narrative depth emerges as the primary driver of engagement: long-form passages increase immersion and emotional connection, whereas short-form passages support quick, decision-focused practice. Second, usability is consistently high across conditions; differences between link and swipe interactions are modest, with a slight preference for swiping on mobile devices. Third, perceived learning improves overall: participants report greater awareness of phishing and social engineering tactics, the risks of oversharing, and the consequences of weak account hygiene, alongside greater confidence in applying safeguards.

This work contributes to the design literature on security awareness by disentangling the roles of story richness and interface mechanics, offering actionable guidance for different deployment priorities. Programs emphasizing culture change and reflective dialogue may favor long-form arcs, whereas programs emphasizing rapid reinforcement may favor short-form sequences. We also argue for a hybrid path: modular narratives that interleave brief decision points with occasional deeper scenes, paired with interfaces that make progress visible and text legible across devices. The remainder of the paper is organized as follows. Section II reviews related work on serious games, gamification, cybersecurity learning, and narrative immersion. Section III describes the game design, measures, participants, procedures, and analytic approach. Section IV reports results on engagement, usability, perceived learning, and qualitative themes. Section V concludes with implications, limitations, and directions for future research.

II. Background

A. Serious Games

The field of serious games traces back to Abt's foundational work, "Serious Games" [6], which first articulated the notion that games could serve purposes beyond entertainment. Serious games are defined as interactive systems designed to both educate and engage, blending play with instruction in a manner that motivates users to learn complex concepts through experience. Over the decades, serious games have become widely used in domains such as military, environmental sustainability, and education. Their enduring appeal lies in their ability to combine intrinsic motivation, goal-oriented interaction, and active experimentation in safe but meaningful contexts [7].

Educational settings provide another fertile ground for serious game adoption. Teachers have used games to teach subjects as varied as mathematics, history, and foreign languages, capitalizing on the immersive nature of play to reinforce concepts that might otherwise seem abstract or inaccessible [8]. Research indicates that serious games can increase student motivation, sustain attention longer than traditional lectures, and improve knowledge retention. Importantly, serious games also support differentiated instruction, as players progress at their own pace, revisiting material until mastery is achieved.

The impact of serious games has also extended to civic engagement and social issues [9], [10]. Games have been designed to raise awareness of climate change, highlight issues of poverty, and even simulate the challenges of policymaking. These experiences encourage empathy by allowing players to inhabit perspectives different from their own. By framing abstract or global problems through concrete, interactive stories, serious games make complex social dynamics understandable and emotionally resonant. This use of narrative immersion has become increasingly important as researchers examine how to create long-term attitudinal and behavioral change through gameplay.

Taken together, the literature on serious games demonstrates their utility across multiple fields. Key themes include experiential learning, safe environments for decision-making, increased motivation through play, and long-term knowledge retention. While serious games have traditionally thrived in healthcare, education, and the military, the principles underpinning their effectiveness—immersion, feedback, and contextual relevance—are directly transferable to cybersecurity awareness and training initiatives.

Recent scholarship has also explored the role of AI in game and educational content generation [11]. Studies highlight how generative models can accelerate scenario development, adapt narratives to learner profiles, and expand branching pathways [12], [13]. While much of this research is still emergent, our study contributes to this discussion by demonstrating the feasibility of AI-assisted narrative design in cybersecurity awareness games, where content accuracy and realism are critical.

B. Gamification

Gamification, distinct from serious games, refers to the integration of game design elements into non-game contexts to enhance engagement, motivation, and learning outcomes [14]. Core elements often include points, badges, leaderboards, levels, and progress bars—mechanics that are inherently rewarding and encourage continued interaction. The theoretical basis of gamification is rooted in self-determination theory, which emphasizes the importance of intrinsic motivation. Game mechanics can fulfill psychological needs for competence, autonomy, and relatedness, thereby increasing user engagement and satisfaction [7], [15].

The adoption of gamification has grown rapidly in education, workplace training, and marketing [16]. In educational settings, gamified platforms encourage learners to complete assignments, collaborate with peers, and progress through challenging material. In corporate environments, gamification has been leveraged to drive employee participation in training modules, boost productivity, and even foster innovation by rewarding creative contributions. These diverse applications demonstrate the flexibility of gamification as a strategy to influence behavior and reinforce desired practices.

However, research also highlights important limitations and challenges of gamification. One risk is the phenomenon of 'pointsification,' where the focus on extrinsic rewards undermines intrinsic motivation [17]. Learners or employees may engage with a task simply to earn points or badges, rather than to internalize knowledge or improve performance. Over time, this can reduce long-term effectiveness and lead to disengagement once novelty wears off. Studies have also noted that leaderboards may foster unhealthy competition or discourage those who consistently rank lower. Similarly, poorly designed gamified systems risk trivializing serious content, especially in sensitive areas like health or cybersecurity training.

Despite these challenges, well-designed gamification can significantly enhance learning outcomes. Key design principles include aligning rewards with meaningful goals, maintaining balance between competition and collaboration, and providing timely feedback. Adaptive gamification, which personalizes challenges and rewards to user abilities and preferences, is emerging as a promising solution to some of the limitations observed in earlier studies. By leveraging data-driven personalization, designers can ensure that gamification supports intrinsic motivation rather than undermining it.

C. *Cybersecurity Applications*

Cybersecurity has become an increasingly active and important domain for the application of serious games and gamification. The unique challenges of cybersecurity—abstract risks, invisible threats, and often low personal salience—make traditional awareness campaigns less effective. Games and gamified approaches provide opportunities to render these threats tangible, simulate real-world attack scenarios, and allow users to practice defensive strategies in safe but realistic contexts. By situating learning in interactive environments, these approaches foster both conceptual understanding and practical skills.

Jaffray et al. [18] developed "SherLOCKED", a detective-style game where players solve puzzles linked to cybersecurity challenges. Their findings highlighted the value of narrative immersion in sustaining engagement and enhancing knowledge retention. Similarly, Dillon et al. [19] introduced "PeriHack", a phishing awareness game that underscored tensions between authenticity and accessibility. While highly realistic simulations increase fidelity, they may overwhelm novice users; simplified versions, by contrast, risk losing educational value.

Blackburn et al. [20] extended this body of work by creating a password hygiene game designed to improve both knowledge and behavioral intentions. Their evaluation demonstrated measurable improvements in players' ability to create and remember strong passwords. Additionally, several reviews further indicated that cybersecurity games tend to be engaging and promising, but also pointed out consistent methodological limitations [21], [22], [23]. Many studies lack rigorous control conditions, sufficiently large sample sizes, or longitudinal follow-ups, leaving open questions about the durability of observed effects.

Gamification has also been widely applied in cybersecurity training. Organizations frequently use simulated phishing campaigns that reward employees for identifying suspicious emails or penalize them for falling victim to tests. Other initiatives incorporate leaderboards to recognize top performers or progress bars to encourage steady improvement. These methods have been shown to increase short-term vigilance, but evidence for long-term resilience against phishing attacks is mixed. In some cases, repeated simulations lead to training fatigue or desensitization, highlighting the need for carefully balanced design.

Overall, the literature suggests that cybersecurity applications of games and gamification offer substantial promise but require more rigorous empirical validation. Future research should address issues of scalability, cross-cultural relevance, and integration with organizational policies. Despite limitations, the body of work illustrates that games can transform cybersecurity training from a passive compliance exercise into an active, engaging learning process, making them a vital tool in the ongoing fight against cyber threats.

D. *Narrative Immersion*

Narrative immersion has emerged as a powerful mechanism in both education and behavioral interventions, offering a way to transform abstract information into relatable, emotionally engaging experiences. Research across psychology and learning sciences suggests that stories are uniquely effective in enhancing comprehension, empathy, and long-term recall [15]. Narrative structures allow learners to contextualize abstract risks and connect them to lived experiences. This process of identification with characters and scenarios creates a sense of transportation, where players become absorbed in the unfolding events and are more likely to internalize the embedded lessons.

Snyder's "Save the Cat" framework [24] has been influential in guiding narrative design, emphasizing the importance of relatable protagonists, clear stakes, and emotionally resonant story beats. In educational contexts, narratives designed around these principles have been shown to increase motivation and engagement while supporting knowledge retention. Within digital learning, immersion is further strengthened by interactivity, as players are not merely observers of a story but active participants whose choices shape outcomes. This creates deeper investment in the learning process and helps bridge the gap between abstract concepts and practical decision-making.

In the domain of cybersecurity, narrative immersion has been applied to simulate realistic threats such as phishing or identity theft, allowing players to experience the consequences of poor decisions in a safe environment. Roepke et al. [25] emphasize that narrative effectiveness is tied to usability: strong storytelling cannot compensate for confusing or frustrating interfaces. This highlights the need for thoughtful integration of narrative with intuitive design. Moreover, research shows a trade-off between narrative length and user experience. Long-form narratives offer greater context and immersion, deepening reflection, but risk user fatigue. Short-form narratives streamline the experience, increasing efficiency, but may reduce depth of engagement [21], [22], [23].

Recent systematic reviews echo this tension and call for hybrid approaches that integrate narrative with multimodal elements such as visuals, branching paths, and adaptive pacing. Moumouh et al. [26] argue for greater personalization and cultural sensitivity in narrative design, noting that users from different cultural backgrounds may interpret stories differently and require tailored scenarios. Taken together, the literature highlights both the promise and the complexity of narrative immersion. While it offers clear advantages in engagement and retention, achieving consistent impact requires balancing story depth, interactivity, usability, and cultural relevance. This ongoing challenge makes the study of narrative depth in cybersecurity games especially timely and important.

III. Methods

This section outlines the methodology adopted to evaluate a narrative-driven, choose-your-own-adventure (CYOA) serious game designed to enhance cybersecurity awareness. It provides detailed accounts of the game design, evaluation framework, participant recruitment and demographics, experimental procedures, and analytic strategy.

A. Game Design

The design of the CYOA cybersecurity game was grounded in principles of serious game development, with an emphasis on interactivity, narrative immersion, and decision-based learning. Four scenarios were developed, each representing a distinct but common cybersecurity risk: phishing, oversharing of personal information, identity theft, and ransomware. These were chosen because they represent both the most frequent and most personally consequential forms of cybercrime encountered by the public. Each scenario was structured with branching paths, requiring players to make choices at critical junctures (*see* Fig. 1). These decision points mirrored real-world dilemmas, such as whether to click on a suspicious email link or how to respond to a ransomware demand.

Narrative development combined human authorship with AI-assisted drafting. Large language model–based tools were employed to generate initial scenario descriptions, dialogue variations, and alternative branch structures. The research team reviewed these AI-generated drafts, editing or discarding content that lacked accuracy or thematic relevance. This hybrid process accelerated the creation of multiple story paths while ensuring that the final narratives retained high fidelity to cybersecurity risks and training objectives. In this way, AI served as an augmentative design tool rather than a replacement for human judgment.

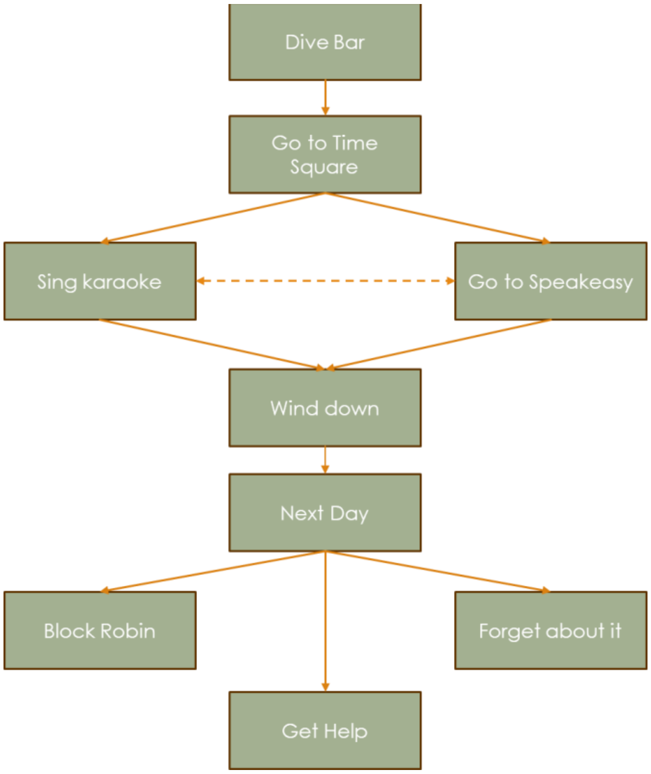
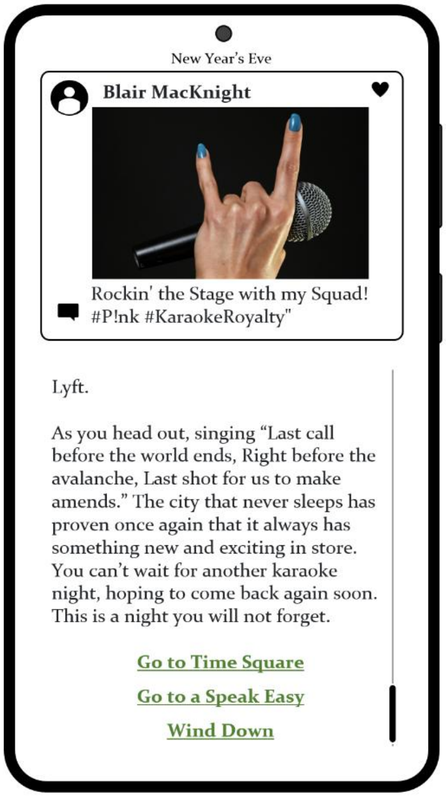


Fig. 1. Story Flow

Two narrative depths were developed for each scenario. The long-form versions contained detailed descriptions, character development, and emotionally resonant storylines (*see* Fig. 2). These aimed to create immersion and simulate realistic social pressures or cues, thereby encouraging reflective engagement. Conversely, the short-form versions condensed narrative elements to focus more directly on decision points, streamlining the experience. This approach allowed the study to systematically examine whether narrative richness or efficiency was more impactful for engagement, usability, and perceived learning.

Accessibility and usability were also prioritized in the game's technical design. The game was deployed as a browser-based platform to ensure compatibility across operating systems and devices. Two interaction modes were implemented: link-based navigation and swipe-based gestures (*see* Fig. 3). This choice allowed examination of how interface design influences usability and engagement. Visual design remained intentionally minimalistic, avoiding heavy graphics in favor of clear text presentation and intuitive choice architecture. This ensured that the focus remained on the narrative and decisions rather than aesthetic complexity, aligning the design with cognitive load considerations.



New Year's Eve

Blair MacKnight

Rockin' the Stage with my Squad! #P!nk #KaraokeRoyalty"

Lyft.

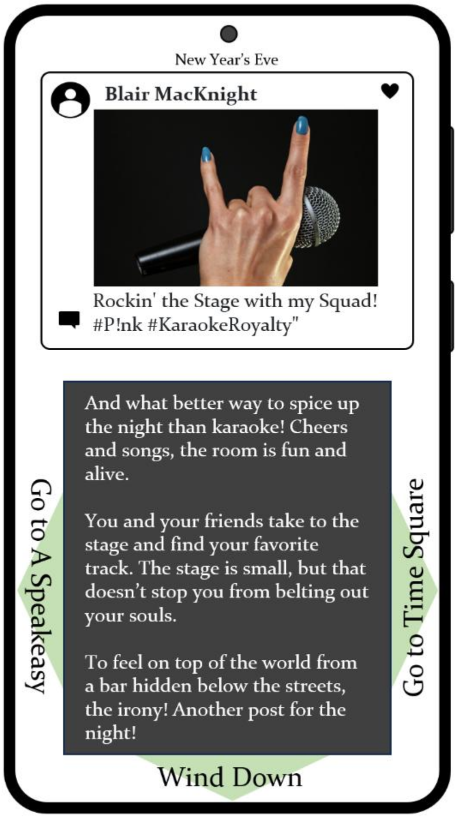
As you head out, singing "Last call before the world ends, Right before the avalanche, Last shot for us to make amends." The city that never sleeps has proven once again that it always has something new and exciting in store. You can't wait for another karaoke night, hoping to come back again soon. This is a night you will not forget.

Go to Time Square

Go to a Speak Easy

Wind Down

Fig. 2. Long-Form Narrative UI with Links



New Year's Eve

Blair MacKnight

Rockin' the Stage with my Squad! #P!nk #KaraokeRoyalty"

And what better way to spice up the night than karaoke! Cheers and songs, the room is fun and alive.

You and your friends take to the stage and find your favorite track. The stage is small, but that doesn't stop you from belting out your souls.

To feel on top of the world from a bar hidden below the streets, the irony! Another post for the night!

Go to A Speakeasy

Go to Time Square

Wind Down

Fig. 3. Short-Form Narrative UI with Arrows

B. Evaluation Framework

The evaluation framework was adapted from prior studies of serious games in education and cybersecurity training [25]. Three key outcome categories were prioritized: engagement, usability, and perceived learning: 1) Engagement was defined as the degree of psychological involvement in the game, encompassing attention, emotional investment, and perceived realism. Engagement was measured through custom Likert-scale items focusing on immersion, attention, and enjoyment, informed conceptually by existing instruments such as the Immersive Experience Questionnaire (IEQ) but not directly adapted [27], supplemented with custom items specific to cybersecurity contexts. 2) Usability was measured using custom items addressing navigation clarity and intuitiveness, conceptually aligned with scales such as System Usability Scale (SUS) but not directly employed [28], which captured participants' perceptions of navigational ease, clarity of instructions, and intuitiveness of interaction. 3) Perceived learning was measured through Likert-style questions asking participants to rate their awareness of cybersecurity risks before and after the intervention, their confidence in applying best practices, and their sense of preparedness to avoid threats. Open-ended questions encouraged reflection on what participants learned and offered feedback on the game design.

Additionally, the evaluation framework was adapted from earlier research that delineated five dimensions for assessing the effectiveness of the game: gaming experience, learning experience, adaptivity, usability, and fidelity (*see* Fig. 4) [29].

- **Gaming experience** captured attention, immersion, and enjoyment, reflecting the extent to which the CYOA format engaged participants.
- **Learning experience** measured self-reported gains in cybersecurity awareness, confidence, and decision-making skills.
- **Adaptivity** assessed how well the game's branching narrative responded to player choices and whether participants felt that outcomes reflected their decisions.
- **Usability** evaluated clarity of instructions, ease of navigation, and interface intuitiveness.
- **Fidelity** examined the authenticity of scenarios, including whether they realistically represented situations participants might face in daily life.

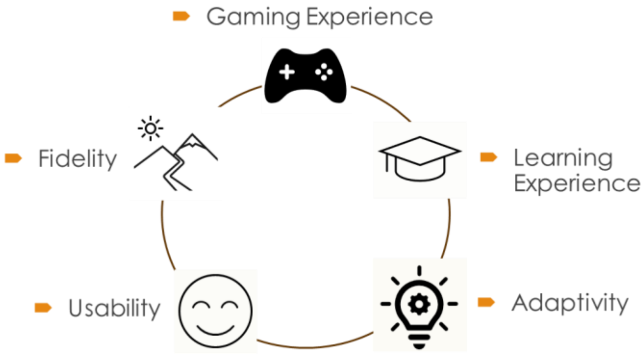


Fig. 4. Five Dimensions of Evaluating the User Experience in Games

Together, these dimensions provided a comprehensive basis for interpreting both quantitative ratings and qualitative reflections, ensuring the analysis addressed not only usability and learning outcomes but also narrative adaptivity and experiential realism.

The integration of validated scales with tailored items ensured both reliability and contextual relevance. By triangulating quantitative and qualitative measures, the framework provided a robust structure for interpreting outcomes, while acknowledging the multi-dimensional nature of engagement and learning in serious games.

C. Participants

Participants were recruited via Amazon Mechanical Turk (MTurk), a platform widely used for online behavioral studies. Inclusion criteria required participants to be at least 18 years old, located in the United States, and to have a task approval rating of at least 95%. These criteria balanced the need for participant diversity with data quality safeguards. A total of N = 422 participants were enrolled in the study with 492 initially recruited (70 failed quality control checks), which consisted of 99 in a control group and 323 in the four treatment groups. Quality control checks consisted of providing instructions to participants that were simple if they were paying attention and taking the time to read the questions (e.g., "Select "agree" in order to get paid for your participation in this study."). Random assignment distributed participants evenly across the four conditions: (1) long-form narratives with link navigation, (2) long-form narratives with swipe navigation, (3) short-form narratives with link navigation, and (4) short-form narratives with swipe navigation. Each condition included approximately one-quarter of the total sample from the treatment group subsample.

Demographic information was collected at the outset, including age, gender, education, employment status, and prior exposure to cybersecurity training. The sample included participants ranging from 18 to over 65 years old, with an average age in the mid-30s. Gender distribution was balanced, and educational attainment ranged from high school completion to postgraduate degrees. Roughly one-third of participants reported some prior exposure to cybersecurity training, while the remainder had minimal or no formal background. This distribution allowed for examination of how cybersecurity knowledge might moderate the effects of narrative depth and usability.

Ethical approval for the study was granted by an Institutional Review Board (IRB). Informed consent was sought and obtained prior to participation. Compensation of $3 was provided, which most participants considered comparable or better than similar projects.

D. Procedures

The study followed a randomized between-subjects design. Participants were randomly assigned to one of the four conditions. They were then instructed to play through all four cybersecurity scenarios in randomized order to reduce sequence effects. Depending on assignment, participants encountered either long-form or short-form narratives and interacted using either link- or swipe-based navigation. Instructions were standardized and delivered via the platform to ensure consistent communication across participants.

Each scenario required participants to make choices at multiple decision points. Consequences of these choices were immediately displayed within the narrative, reinforcing the relationship between decision-making and outcomes. Some branches incorporated cues such as urgency or authority to mimic real-world phishing or social engineering tactics, though the focus of the study remained on engagement and learning rather than stress induction. After completing the scenarios, participants filled out a post-test survey with both Likert-scale items and open-ended prompts.

Attention checks were embedded in the survey to ensure data integrity. Participants who failed these checks were excluded from final analysis, although all participants were compensated. This approach ensured rigor in data quality while upholding ethical responsibilities to participants.

E. Data Analysis

The analytic strategy was based on a combination of quantitative descriptive statistics and qualitative thematic analysis. For quantitative analysis, frequencies, percentages, and mean scores were calculated for engagement, usability, and perceived learning items. These descriptive summaries allowed for straightforward comparisons across conditions, while avoiding overstatement of significance. Data were presented in tables and figures to illustrate differences between narrative length and navigation modality conditions.

Qualitative analysis focused on responses to open-ended questions included in the post-test survey. These responses were analyzed using inductive thematic coding. Two independent coders reviewed the dataset, developed preliminary codes, and refined categories through iterative discussion. This collaborative process ensured that the final themes accurately reflected participant perspectives. Areas of disagreement were discussed until consensus was achieved. Themes were then grouped under broader categories related to engagement, usability, and perceived learning. This approach allowed the qualitative analysis to enrich the quantitative findings, offering insight into why participants responded the way they did and how narrative structure and usability influenced their experiences.

By combining descriptive quantitative analysis with qualitative thematic coding, the study was able to capture both patterns of response and nuanced individual perspectives. This mixed-methods strategy strengthened the validity of the findings while remaining aligned with the scope of the project and the data that were actually collected.

IV. Results and Discussion

A. Participant Demographics

A total of 492 participants were initially recruited through Amazon Mechanical Turk (MTurk). After excluding individuals who failed attention checks or provided incomplete responses, the final sample included N = 422 participants. Participants were evenly distributed across the four experimental conditions: long-form narratives with link navigation, long-form narratives with swipe navigation, short-form narratives with link navigation, and short-form narratives with swipe navigation. This balanced design ensured that comparisons across conditions were not confounded by unequal group sizes.

Demographic information was collected at the start of the study to capture the diversity of the participant pool. Participants ranged in age from 18 to over 65 years, with a mean age of approximately 34. The sample included 55% male, 44% female, and about 1% identifying as non-binary or another gender. Educational attainment was diverse: approximately 30% reported holding a bachelor's degree, 25% indicated some college or an associate degree, 20% had completed high school, 15% held a graduate-level degree, and the remainder reported other forms of educational background.

Exposure to cybersecurity training prior to the study was mixed. Approximately 35% of participants reported having completed some form of cybersecurity awareness training, while the majority (65%) indicated limited or no formal experience. This variation was valuable, as it provided a basis for examining how prior knowledge may have influenced engagement, usability, and learning outcomes.

Overall, the demographic profile of the 422 participants reflected broad diversity in age, gender, education, and prior experience with cybersecurity. This heterogeneity enhanced the ecological validity of the study, increasing the relevance of findings to a wide range of potential end users of cybersecurity awareness training.

B. *Narrative Depth and Engagement*

One of the central research questions concerned how narrative depth influenced participant engagement with the game. Engagement was operationalized through measures of immersion, attention, enjoyment, and perceived realism, supplemented by open-ended reflections. The results demonstrated clear differences between participants who experienced long-form narratives and those who completed the short-form versions.

Overall, participants in the long-form conditions reported higher levels of engagement compared to those in the short-form conditions. Long-form narratives provided more detailed context, character development, and emotional framing, which appeared to draw participants deeper into the scenarios. Several participants noted in qualitative feedback that the longer stories felt more realistic and relatable. One participant wrote, *"I absolutely would be interested in participating. If nothing else, I want to find out how that 'Choose Your Own Adventure' game goes."* This reflection highlights how narrative richness contributed to immersion and participant investment in the story.

At the same time, some participants did perceive drawbacks to the long-form narratives. A subset described them as overly detailed or slow-paced, noting that they preferred faster progression through decision points. In contrast, participants in the short-form conditions valued efficiency and clarity. The concise passages allowed them to focus more directly on the cybersecurity decisions without being distracted by extended storytelling. However, some felt that this brevity came at the cost of depth or clarity. One participant commented, *"I really like the game play. It reminded me of books when I was young [...] I also did like the 3 arrow to pick which action the character does next but I choose links for that question. If the character has less than 3 choices I don't think the arrows will look correct. I would always be looking for 3 arrows and it would be visually unpleasing if there were less."* Another added, *"I suppose posting too much personal information online could put some at risk, but that's not really the main thing I got when reading the text."*

Navigation modality—link-based versus swipe-based interaction—was less influential on engagement than narrative depth. Across both narrative formats, participants reported similar levels of attention and enjoyment regardless of whether they clicked links or swiped between passages. While some participants found swipe navigation to be slightly more intuitive on mobile devices, these differences did not appear to significantly affect engagement overall.

Taken together, the results suggest that narrative depth was a stronger determinant of engagement than interface style. Long-form narratives fostered greater immersion and emotional connection, while short-form narratives supported efficiency and focus. These findings align with prior research emphasizing the importance of narrative detail for promoting immersion in serious games. They also highlight a trade-off: while long-form narratives enhance realism and investment, they may also risk overwhelming participants who prefer streamlined experiences. The balance between narrative richness and efficiency therefore remains a critical consideration for designing cybersecurity awareness tools.

C. *Usability Findings*

In addition to engagement, the study examined how interface modality and narrative depth influenced perceptions of usability. Usability was assessed through items adapted from the System Usability Scale (SUS), as well as participant feedback on the intuitiveness and clarity of the game's design.

Overall, participants rated the game as moderately to highly usable across all conditions. Most reported that the instructions were clear, the interface was easy to navigate, and the branching structure of the game was intuitive. Minimal technical issues were encountered, and the browser-based format functioned reliably on both desktop and mobile devices. The minimalist visual design also contributed positively to usability by keeping attention focused on text and decisions rather than on distracting graphics.

When comparing interaction modalities, participants expressed slightly higher satisfaction with the swipe-based interface, particularly when accessing the game on mobile devices. Swiping was described as more natural and fluid for sequential narrative progression. However, participants using the link-based navigation also reported positive experiences, noting that the clickable options provided a sense of clarity in decision-making. Importantly, the differences between the two modalities were relatively modest, suggesting that both approaches were broadly effective.

Narrative depth appeared to play a lesser role in perceptions of usability than it did for engagement. Both long- and short-form narratives were generally seen as easy to follow, though some participants in the long-form condition commented that the extended passages occasionally made navigation feel slower. Conversely, the concise structure of short-form narratives was praised for its efficiency and straightforwardness. Still, usability ratings remained high across conditions, indicating that narrative length did not fundamentally hinder user interaction.

Qualitative feedback reinforced these findings. Participants frequently emphasized that the interface “got out of the way” of the narrative, allowing them to focus on choices and consequences. Suggestions for improvement included minor interface enhancements, such as larger font size options and clearer progress indicators. Overall, the results suggest that while interface modality and narrative length influenced usability perceptions to some extent, the game’s design was broadly successful in supporting intuitive interaction

D. Learning Outcomes

A central aim of the study was to evaluate the extent to which the game enhanced participants’ understanding of cybersecurity risks and their confidence in applying safe practices. Perceived learning was measured through self-report items asking participants to assess changes in their awareness and preparedness, complemented by qualitative reflections on what they had learned.

Across all conditions, participants reported increased awareness of key cybersecurity threats after completing the game. The majority indicated greater confidence in recognizing phishing attempts, understanding the risks of oversharing personal information, and appreciating the consequences of identity theft and ransomware. One participant reflected, *“Seeing what could happen if I clicked made it stick with me more than just being told not to click.”* These self-reported gains suggest that the game succeeded in delivering core educational objectives regardless of narrative depth or navigation modality.

Some differences emerged between conditions. Participants in the long-form narrative groups tended to describe a deeper understanding of the context surrounding cybersecurity risks. For example, they often highlighted how detailed storylines helped them connect abstract risks to real-life situations, such as workplace email practices or online account management. In contrast, participants in the short-form conditions emphasized the efficiency of the experience and its value in reinforcing specific decision-making strategies. Another commented, *“The text-based game was kind of fun! I know it was supposed to deal with cybersecurity, but the short version didn’t really make that clear. I suppose posting too much personal information online could put some at risk, but that's not really the main thing I got when reading the text.”* These individuals often described the scenarios as “practical” and “straight to the point,” which supported their sense of preparedness without requiring extensive reading.

Qualitative responses offered further insight into learning outcomes. Many participants recalled specific lessons, such as the importance of verifying sender addresses in emails, using strong and unique passwords, and being cautious about sharing personal details on social media.

Overall, the results suggest that the game effectively improved cybersecurity awareness and confidence across all participants, with narrative depth influencing the type of learning experienced. Long-form narratives promoted deeper contextual understanding, while short-form narratives supported efficient reinforcement of practical strategies. Both approaches appear valuable depending on training objectives, underscoring the flexibility of narrative-driven serious games as educational tools.

E. Qualitative Insights

Beyond quantitative ratings of engagement, usability, and learning, participants provided open-ended feedback that offered valuable qualitative insights into their experiences with the game. These reflections highlighted both strengths and limitations of the design, as well as broader considerations for the role of narrative in cybersecurity awareness training.

Many participants appreciated the overall format and the branching choices, connecting the game to familiar interactive experiences. For instance, one participant remarked, *“I really like the game play. It reminded me of books when I was young.”*

At the same time, qualitative feedback revealed a split between preferences for shorter and longer narratives. Some participants in the long-form narrative conditions expressed fatigue, noting that the passages occasionally felt too lengthy or slowed the pace of decision-making. Others, however, described the longer stories as more engaging and worthwhile. One wrote, *“I absolutely would be interested in participating. If nothing else, I want to find out how that ‘Choose Your Own Adventure’ game goes.”* Another emphasized the broader educational potential: *“I like the idea of a fun way to teach safer practices online and actually for learning most topics, so I wish you guys the best of luck with this project.”*

Participants also reflected on usability and interface elements. While most agreed that the design was intuitive, some requested additional features, such as clearer indicators of progress through scenarios or options for adjusting text size. These suggestions highlight the importance of small interface refinements in supporting user comfort and accessibility, particularly when delivering training to broad and diverse audiences.

Another theme concerned the realism of the scenarios. Several participants reported that the situations felt authentic and aligned with challenges they had faced in daily life, such as suspicious emails at work or managing online accounts. Others suggested expanding the scope of scenarios to include emerging risks, such as multifactor authentication fatigue attacks or scams targeting mobile payment apps. These comments underscore the dynamic nature of cybersecurity threats and the need for training tools to evolve alongside them.

Although narratives were initially drafted with AI assistance, participants described the scenarios as authentic and realistic. This suggests that the refinement process preserved fidelity, addressing potential concerns that AI-generated content might appear artificial

Overall, the qualitative insights provided nuance to the quantitative findings. While long-form narratives promoted immersion and short-form narratives supported efficiency, participants’ feedback emphasized the value of flexibility, authenticity, and user-centered design. Incorporating these lessons into future versions of the game can strengthen its impact as a cybersecurity awareness tool and ensure it remains relevant in a rapidly changing threat landscape.

V. Conclusion

This study evaluated the effectiveness of a narrative-driven, choose-your-own-adventure (CYOA) game as a tool for cybersecurity awareness and training. By comparing long-form and short-form narrative structures and testing two interface modalities—link-based and swipe-based navigation—the research provided insight into how narrative depth and usability influence engagement, learning, and user experience in the context of serious games.

A. Summary of Key Findings

The results revealed several important findings. First, narrative depth significantly shaped participant engagement. Long-form narratives fostered greater immersion, emotional investment, and perceived realism, allowing participants to connect cybersecurity threats to everyday experiences. Short-form narratives, while less immersive, offered efficiency and directness, which some participants preferred. These differences highlight the trade-off between narrative richness and efficiency, suggesting that both formats may be valuable depending on the training context and objectives.

Second, usability was consistently rated as high across all conditions. While swipe-based navigation was slightly more intuitive for participants on mobile devices, link-based navigation was also effective, with participants appreciating the clarity of clickable options. Importantly, neither modality created substantial usability barriers, indicating that interface design should prioritize accessibility and clarity rather than relying on elaborate technical features. Qualitative feedback underscored that the minimalist, text-focused design allowed participants to concentrate on decision-making rather than interface mechanics.

Third, perceived learning outcomes were strong across conditions. Participants reported increased awareness of phishing, oversharing, identity theft, and ransomware risks. They also expressed greater confidence in applying safe practices, such as verifying email senders, creating strong passwords, and limiting personal disclosures on social media. Long-form narratives promoted contextual understanding, while short-form narratives reinforced practical strategies. Both approaches proved valuable, underscoring the adaptability of narrative-driven serious games for different learning goals.

B. Practical Implications

The findings hold important implications for the design and implementation of cybersecurity awareness initiatives. Organizations seeking to cultivate deeper awareness and reflection may benefit from incorporating long-form narratives into training programs. These narratives provide realism and emotional resonance, which can enhance retention. Conversely, organizations prioritizing efficiency and quick reinforcement of best practices may prefer short-form narratives, which deliver concise decision-making practice without extended reading. A hybrid approach that blends immersive storytelling with concise decision points may provide the most balanced and effective strategy.

The study also demonstrates that usability should not be overlooked in cybersecurity training tools. Even the most engaging narratives will lose impact if users struggle with the interface. Ensuring compatibility across devices, providing intuitive navigation, and maintaining clear progress indicators are critical to creating accessible and sustainable learning tools. Feedback about text size and progress indicators further suggests that small refinements can meaningfully improve the learning experience.

C. Limitations

While the study produced promising results, several limitations must be acknowledged. First, the participant pool was drawn from Amazon Mechanical Turk (MTurk), which, while diverse, does not fully represent the broader population. Additionally, quality control issues can be significant if proper quality control procedures are not implemented, which was done in the current study [30]. Common method bias and social desirability bias are also issues that may influence the results [31], [32]. The level of anonymity provided to participants and the incorporation of scenarios within the survey do help to address these concerns to come extent.

Generalizability to other contexts—such as corporate employees or non-U.S. populations—may therefore be limited. Second, outcomes relied heavily on self-reported measures of engagement and learning. While useful for gauging perceptions, self-reports may be subject to biases such as social desirability or limited self-awareness. Third, the scope of the game was restricted to four scenarios: phishing, oversharing, identity theft, and ransomware. Although these represent important threats, the cybersecurity landscape is broader and continually evolving. Training modules that expand to cover emerging risks, such as multifactor authentication fatigue attacks or mobile payment scams, may provide more comprehensive protection.

D. Future Research Directions

Future research should build upon this foundation in several ways. First, studies should explore hybrid narrative approaches that combine immersive detail with concise decision points to address the trade-off between depth and efficiency. Adaptive storytelling techniques, in which narrative complexity adjusts dynamically to the learner's preferences and pace, may offer personalized and more effective learning experiences. Second, integrating behavioral assessments alongside self-report measures would provide stronger evidence of actual learning gains. For example, participants could be tested on their ability to detect phishing emails in simulated inboxes following gameplay.

Third, future work should examine the effectiveness of such games across different populations and contexts, including corporate training environments, educational settings, and international audiences. Customizing scenarios to reflect cultural and organizational contexts could increase both relevance and impact. Fourth, future work could expand the role of AI beyond draft generation toward real-time adaptivity. Generative models could dynamically tailor storylines to a learner's prior choices, demographic profile, or emerging threat landscapes. Such integration could enhance both adaptivity and personalization, aligning cybersecurity awareness training with the broader shift toward AI-driven educational technologies.

Finally, iterative development informed by user feedback should continue to refine interface design and scenario selection, ensuring that tools remain responsive to evolving threats and user needs.

E. Conclusion

This study demonstrates the potential of narrative-driven serious games as engaging, usable, and effective tools for cybersecurity awareness. By highlighting the influence of narrative depth on engagement, usability, and learning, it contributes to a growing body of evidence supporting the role of interactive storytelling in security education. Although limitations exist, the findings emphasize that serious games can complement traditional training approaches by providing experiential, memorable learning opportunities. With thoughtful design, attention to usability, and ongoing adaptation to emerging threats, narrative-driven games represent a promising avenue for strengthening cybersecurity awareness in diverse user populations.

VI. References

[1] A. Sangwan, “Human factors in cybersecurity awareness,” in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, IEEE, 2024, pp. 1–7.

[2] A. Alshhre, “The Ascendancy of Video Games: Can They Eclipse Literary Works?,” *Taduction Et Langues*, 2024, doi: 10.52919/translang.v23i1.979.

[3] H. Wei, J. Bizzocchi, and T. Calvert, “Time and Space in Digital Game Storytelling,” *International Journal of Computer Games Technology*, 2010, doi: 10.1155/2010/897217.

[4] D. T. Kline, “Bringing Interactive Storytelling to Industry: Designing a Reactive Narrative Encounter System,” *Proceedings of the Aaai Conference on Artificial Intelligence and Interactive Digital Entertainment*, 2009, doi: 10.1609/aiide.v5i1.12367.

[5] J. George-Palilonis and B. King, “A Framework for Authoring Interactive, Tablet-Based Books,” *The International Journal of the Book*, 2013, doi: 10.18848/1447-9516/cgp/v10i01/36966.

[6] C. C. Abt, *Serious Games*. New York City, New York, USA: Viking Press, 1970.

[7] J. Hamari, J. Koivisto, and H. Sarsa, “Does Gamification Work? A Literature Review of Empirical Studies on Gamification,” *Proceedings of the 47th Hawaii International Conference on System Sciences*, pp. 3025–3034, 2014.

[8] S. Pescarin and D. S. Martinez Pandiani, “The Impact of Story Structure, Meaningfulness, and Concentration in Serious Games,” *Information*, vol. 13, no. 12, p. 567, Dec. 2022, doi: 10.3390/info13120567.

[9] W. Peng, M. Lee, and C. Heeter, “The Effects of a Serious Game on Role-Taking and Willingness to Help,” *Journal of Communication*, vol. 60, no. 4, pp. 723–742, Dec. 2010, doi: 10.1111/j.1460-2466.2010.01511.x.

[10] S. M. H. Sadati and C. Mitchell, “Participatory Arts-based Game Design: Mela, a Serious Game to Address SGBV in Ethiopia,” *Loading*, vol. 16, no. 26, pp. 16–39, May 2024, doi: 10.7202/1111258ar.

[11] J. S. Park, J. O’Brien, C. J. Cai, M. R. Morris, P. Liang, and M. S. Bernstein, “Generative Agents: Interactive Simulacra of Human Behavior,” in *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology*, San Francisco CA USA: ACM, Oct. 2023, pp. 1–22. doi: 10.1145/3586183.3606763.

[12] A. Filipović, “The role of artificial intelligence in video game development,” *Kultura polisa*, vol. 20, no. 3, pp. 50–67, 2023.

[13] S. Gill and S. Bibi, “The Role of AI in Game Storytelling and Narrative Development,” *Journal of Linguistic and Literary insights*, vol. 1, no. 2, pp. 1–9, 2025.

[14] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, “From Game Design Elements to Gamefulness: Defining ‘Gamification,’” in *Proceedings of the 15th International Academic MindTrek Conference*, ACM, 2011, pp. 9–15.

[15] M. Sailer, J. U. Hense, S. K. Mayr, and H. Mandl, “How gamification motivates: An experimental study of the effects of specific game design elements on psychological need satisfaction,” *Computers in human behavior*, vol. 69, pp. 371–380, 2017.

[16] F. F.-H. Nah, Q. Zeng, V. R. Telaprolu, A. P. Ayyappa, and B. Eschenbrenner, “Gamification of Education: A Review of Literature,” in *HCI in Business*, vol. 8527, F. F.-H. Nah, Ed., in Lecture Notes in Computer Science, vol. 8527. , Cham: Springer International Publishing, 2014, pp. 401–409. doi: 10.1007/978-3-319-07293-7_39.

[17] J. Swacha and A. Kulpa, “Gamitest: A Game-like Online Student Assessment System,” *Future Internet*, vol. 17, no. 3, p. 103, Feb. 2025, doi: 10.3390/fi17030103.

[18] A. Jaffray, C. Finn, and J. R. Nurse, “Sherlocked: A detective-themed serious game for cyber security education,” in *International Symposium on Human Aspects of Information Security and Assurance*, Springer, 2021, pp. 35–45.

[19] R. Dillon, “‘PeriHack’: Designing a serious game for cybersecurity awareness,” in *2022 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE)*, IEEE, 2022, pp. 630–634.

[20] N. N. Blackburn, “Promoting End-User Security and Privacy Through Serious Games,” in *Companion Proceedings of the 2024 Annual Symposium on Computer-Human Interaction in Play*, Tampere, Finland: ACM, 2024, pp. 409–412.

[21] A. K. Gwenhure and F. S. Rahayu, “Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review,” *International Journal of Serious Games*, vol. 11, no. 1, pp. 83–99, 2024.

[22] O. Pahlavanpour and S. Gao, “A Systematic Mapping Study on Gamification within Cybersecurity Awareness,” *Heliyon*, vol. 10, no. 19, 2024.

[23] C. Y. Ng and M. K. B. Hasan, “Cybersecurity serious games development: A systematic review,” *Computers & Security*, vol. 150, p. 104307, 2025.

[24] B. Snyder, *Save the Cat! The Last Book on Screenwriting You’ll Ever Need*. Michael Wiese Productions, 2005.

[25] R. Roepke, V. Drury, U. Meyer, and U. Schroeder, “Exploring and evaluating different game mechanics for anti-phishing learning games,” *International Journal of Serious Games*, vol. 9, no. 3, pp. 23–41, 2022

[26] C. Moumouh, J. A. García-Berná, M. Y. Chkouri, and J. L. Fernández-Alemán, “Serious Games to Improve Privacy and Security Knowledge for Professionals: a Systematic Literature Review,” *International Journal of Serious Games*, vol. 12, no. 1, pp. 3–24, 2025.

[27] C. Jennett *et al.*, “Measuring and defining the experience of immersion in games,” *International Journal of Human-Computer Studies*, vol. 66, no. 9, pp. 641–661, Sep. 2008, doi: 10.1016/j.ijhcs.2008.04.004.

[28] J. Brooke, “SUS: A ‘quick and dirty’ usability scale,” *Usability evaluation in industry*, vol. 189, pp. 4–7, 1996.

[29] J. Moizer *et al.*, “An approach to evaluating the user experience of serious games,” *Computers & Education*, vol. 136, pp. 141–151, Jul. 2019, doi: 10.1016/j.compedu.2019.04.006.

[30] M. Dupuis, K. Renaud, and R. Searle, “Crowdsourcing Quality Concerns: An Examination of Amazon’s Mechanical Turk,” in *The 23rd Annual Conference on Information Technology Education*, Chicago IL USA: ACM, Sep. 2022, pp. 127–129. doi: 10.1145/3537674.3555783.

[31] A. J. Nederhof, “Methods of coping with social desirability bias: A review,” *European Journal of Social Psychology*, vol. 15, no. 3, pp. 263–280, 1985, doi: 10.1002/ejsp.2420150303.

[32] S. B. MacKenzie and P. M. Podsakoff, “Common method bias in marketing: Causes, mechanisms, and procedural remedies,” *Journal of retailing*, vol. 88, no. 4, pp. 542–555, 2012.