Université de Montréal

Enhancing Cybersecurity Awareness through Educational Games: Design of an Adaptive Visual Novel Game

Par

Firdaous Bouzegza

Département d'informatique et de recherche opérationnelle

Faculté des arts et des sciences

Mémoire présenté en vue de l'obtention du grade

de Maître ès sciences (M.Sc.)

en Informatique

30 Avril 2023

Université de Montréal

Faculté des arts et des sciences

Ce mémoire intitulé

Enhancing Cybersecurity Awareness through Educational Games: Design of an Adaptive Visual Novel Game

Présenté par

Firdaous Bouzegza

A été évalué(e) par un jury composé des personnes suivantes

Michalis Famelis
Président-rapporteur

Esma Aïmeur
Directeur de recherche

Margarida Carvalho
Membre du jury

Résumé

Dans un monde qui est en numérisation constante, la dépendance aux outils technologiques est devenue inévitable. La pandémie de COVID-19 a encore accéléré la tendance vers le travail et l'éducation à distance, entraînant une augmentation de l'activité en ligne et de l'échange de données. Cependant, malgré cette augmentation de l'activité en ligne, le niveau de sensibilisation à la cybersécurité chez un nombre important d'utilisateurs reste insuffisant. De nombreux utilisateurs manquent d'une éducation appropriée en matière de cybersécurité et de confidentialité en ligne et démontrent une compréhension insuffisante de la sensibilité de leurs données. Nous avons mené une enquête auprès de plus de 300 utilisateurs qui a confirmé que le besoin de contenu de meilleure qualité était évident. Les jeux éducatifs ont démontré leur efficacité en tant qu'outils d'enseignement et d'apprentissage, en particulier pour vulgariser des sujets qui nécessitent généralement une connaissance approfondie pour être maîtrisés. Cependant, des défis sont associés quant à la qualité et à l'évaluation des jeux sérieux, car plusieurs aspects de l’amusement sont subjectifs et intangibles.

Motivée par le besoin de jeux éducatifs "de haute qualité" améliorés, cette thèse construit une échelle pour affiner les critères mentionnés par l'évaluation des jeux sérieux de Caserman et l'applique à 45 jeux de cybersécurité. L'évaluation a révélé une insuffisance dans les critères de l’amusement, en particulier le manque d'adaptation dynamique. En conséquence, cette étude propose le cadre de jeu de cybersécurité EVNAG (Educational Visual Novel Adaptive Game), qui s'articule autour de l'adaptation dynamique de la difficulté comme solution à ce problème. Inspiré par cette architecture, le roman visuel de cybersécurité "Grown-Up Blues" a été implémenté.

La thèse contribue au corpus croissant de recherches sur les jeux éducatifs en cybersécurité et fournit des idées pour concevoir des jeux éducatifs efficaces qui améliorent l'éducation en matière de cybersécurité.

Mots-clés : Jeux éducatifs, Jeux Sérieux, Sensibilisation à la Cybersécurité, Nudge, Design de Jeux, Cadre Théorique

Abstract

In a world that continues to be increasingly digitalized, the dependency on technological tools has become unavoidable. The COVID-19 pandemic has further accelerated the trend towards remote work and education, leading to an increase in online activity and data exchange. However, despite this surge in online activity, the level of cybersecurity awareness among a significant number of users remains inadequate. Many users lack proper education on cybersecurity and online privacy and demonstrate a lack of understanding of the sensitivity of their data. A survey we conducted on more than 300 users confirmed that the need for more quality content was blatant. Educational games have demonstrated their effectiveness as teaching and learning tools, particularly in vulgarizing topics generally requiring in-depth knowledge to master. However, challenges are associated with the quality and assessment of serious games, as multiple aspects of game enjoyment are subjective and intangible.

Motivated by the need for improved "high quality" educational games, this thesis builds a scale to refine the criteria mentioned by Caserman's assessment of serious games and applies that to 45 cybersecurity games. The assessment indicated a deficiency in the enjoyment criteria, specifically the lack of dynamic adaptation.

As a result, this study proposes the EVNAG (Educational Visual Novel Adaptive Game) cybersecurity game framework, which centers on Dynamic Difficulty Adaptation as a solution to this issue. Inspired by this architecture, the cybersecurity visual novel "Grown-Up Blues" was implemented.

The thesis contributes to the growing body of research on educational games in cybersecurity and provides insights for designing effective educational games that enhance cybersecurity education.

Keywords: Educational Games, Serious Games, Cybersecurity Awareness, Caserman's quality criteria, Nudges, Game Design, Visual Novel, Theoretical Framework

Table of Contents

List of Tables

List of Figures

List of abbreviations

EVNAG: Educational Visual Novel Adaptive Game

GBL: Game-Based Learning

NPC: Non-Player Character

RPG: Role-Playing Game

SBL: Scenario-Based Learning

SG: Serious Games

UI: User Interface

VN: Visual Novel

A ma maman

Acknowledgments

First and foremost, I would like to thank God for providing me with the strength and guidance I needed to complete this research project.

I want to express my heartfelt appreciation to Pr. Esma, my supervisor, for her constant encouragement and support throughout my research. With her extensive knowledge and experience, she challenged me to push beyond my limits and strive for excellence in my work. Her patience and understanding were deeply appreciated and have helped me to grow both personally and professionally. I owe my thesis success to her and am grateful for her unwavering support and guidance at every stage of my research. Her mentorship has been a transformative experience that has prepared me well for the challenges that lie ahead. I will always remember her lessons and strive to apply them in my future endeavors.

Moreover, I want to extend my thanks to Rim, my fellow researcher and lab comrade for her constructive feedback and suggestions, as well as her encouragement in helping me stay focused and engaged. Her friendship made the lab more enjoyable and productive. In that regard, I would like to express my appreciation to my lab mates Dorsaf, Alexis, Muxue, Yasmine, Rafael, Khalida, Lissethy, Kasra and Victor for all the diverse cultural and scientific discussions we had.

Additionally, I would like to express my gratitude to the members of the jury, Professor Margarida Carvalho, and Dr. Michalis Famelis, for their invaluable time and effort in carefully reading, correcting, and enhancing my thesis.

Last, but never least, I would like to thank my dearest family for their continuous support throughout this journey. I am grateful for my parents who made me the person I am today and to my sisters without whom I wouldn't have been able to accomplish this project. I would like to extend my thanks to my aunt Kenza and her family for all their kindness and generosity while I was under their care. You have made a lasting impact on my life, and I will always be grateful for everything that you have done for me.

Chapter 1 – Introduction

In this chapter, we provide an overview of our research work by introducing the context of our study. We also highlight the issues that we aim to tackle in this thesis, identify the research questions that will guide our investigation, and discuss the objectives of our research.

1.1. Problem Definition and Motivation

The past decades have witnessed an increase in the use of technology in different fields. Along with the good comes the bad, as the adage goes, since technological innovations brought forth their fair share of cybersecurity issues. The digitalisation of information and the exponential growth of the virtual universe makes it difficult nowadays for users to be exempt from having a cyber presence. The integration of internet-based services into our daily lives means that being offline is no longer an option, making it crucial to address the cybersecurity challenges that come with this new reality. Although this greatly facilitates many activities and tasks previously thought of as time-consuming, this new reality is not without its challenges. The private details of individuals have emerged as a highly prized asset (Aïmeur & Schőnfeld, 2011). Cybersecurity is more at risk than ever before with the rise of adverse technology like malicious phishing bots. Meanwhile, there is a common belief among users that privacy is necessary only if they "had something to hide"(Marwick & Hargittai, 2019).

While a lot of effort has been dedicated to fortifying systems, risk management, and deploying counter-hacking strategies, the human link remains the weakest in the cybersecurity chain (S. Mittal, 2016). As Kevin Mitnick, the infamous hacker said: "A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and encryption and other security technologies, but if an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent in technology is essentially wasted" (Mitnick & Simon, 2003). This highlights the need for more comprehensive approaches to cybersecurity that address not only technical issues but also human behaviors and attitudes towards security.

Fixed systematic approaches may not be enough to address the ever-changing nature of cyber threats, making cybersecurity education a potentially more effective solution. While traditionally, cybersecurity education was confined to upper-level undergraduate and graduate computer science courses (Švábenský et al., 2020), more efforts are dedicated to educating users of all ages and backgrounds on the dangers of cyberspace. In fact, cybersecurity is and "needs to be everyone's business" (Rothrock et al., 2018). As such, reaching a broad audience and teaching them which habits and reflexes to adapt is crucial to the success of these approaches.

Serious games are a valuable tool in achieving this goal, as they have the ability to raise public awareness and maintain user engagement. Furthermore, serious games have the potential to level the playing field in terms of knowledge acquisition, as they are not restricted by the formal rules of official curriculums. They were found to be effective in learning and retention (Wouters et al., 2013), and their use in training has been shown to increase student motivation (J. Cain & Piascik, 2015) in various fields.

While many serious games are designed for this purpose, the question of their effectiveness remains to be assessed. Similar to other educational methods, it is possible to evaluate the quality of games based on specific criteria. Caserman proposed in his work (Caserman et al., 2020) a quality criteria guide for analyzing games given both the serious part and the enjoyment part of the educational game. For the sake of this research, the terms "games", "serious games", and "educational games" are used interchangeably.

1.2. Research Objectives

This chapter presents the goals and objectives of this research.

- RQ1: How can we assess the gaps in users' understanding of cybersecurity best practices, including behaviors, tools, and concepts, and determine the need for more effective educational cybersecurity games?

- RQ2: How well do current cybersecurity games satisfy Caserman's quality criteria of serious games? What criteria can be improved to make players more engaged with cybersecurity games?

- RQ3: What are the key requirements and features needed to design an adaptable framework for a high-quality educational cybersecurity game?

These research questions lead to the contributions specified in the following subsection.

1.3. Main Contributions

Given that the potential of cybersecurity educational games remains largely untapped, this presents a compelling opportunity for researchers and game developers. By integrating educational content into interactive and immersive game experiences, educational games can offer a unique and engaging learning environment for individuals that need cybersecurity training. However, to fully exploit this potential, it is crucial to ensure the development of high-quality educational games that effectively deliver the intended learning outcome. To achieve that, the first step of this research is to explore the gaps in cybersecurity, by taking into consideration both the limitations in human knowledge and the quality aspects of educational games. Firstly, we run a survey to ascertain knowledge gaps that users may have regarding primary cybersecurity concepts. Then, among the different assessment methods used for evaluating educational games, we create a scale that refines the games' quality criteria described by Caserman's in his approach. The scale is built upon refining the aforementioned criteria, and specifically tailored to evaluate the quality of cybersecurity educational games, making it a useful tool for future game developers. Using this scale, the assessment of 45 cybersecurity educational games is carried out, which permits the identification of areas that require improvement by analyzing which criteria should be prioritized for enhancing the quality of these games. Seeing as adaptability is one of the criteria requiring improvement, we develop a cybersecurity educational games framework that prioritizes adaptability as a core component. Lastly, this work will involve the design and partial implementation of an educational cybersecurity visual novel. This interactive narrative-based game format holds potential in engaging learners and presenting complex cybersecurity concepts in a captivating manner. The visual novel will serve as a practical demonstration of the proposed framework.

This work presents the following contributions:

- Development of a scale that refines the criteria used in Caserman’s assessment of serious games to assist future game developers into developing high-quality educational games.
- Assessment of 45 cybersecurity educational games using the developed scale, identification of areas that require improvement by analyzing which criteria should be prioritized for enhancing the quality of these games.
- Development of a cybersecurity educational games framework that prioritizes adaptability as a core component.
- Design and partial implementation of an educational cybersecurity visual novel.

The contributions were structured as specified in the next subsection.

1.4. Thesis Structure

In Chapter 2, we present a review of the literature on cybersecurity education and educational games, highlighting their potential benefits and limitations. Specifically, the chapter examines the role of educational games in improving students' cybersecurity skills and knowledge, as well as their impact on student engagement and motivation. Chapter 3 presents the results of a survey on online privacy and security habits among students. Chapter 4 presents a comprehensive assessment of existing educational games in cybersecurity, using a rating process based on Caserman’s predefined criteria. In Chapter 5, we propose a new educational visual novel adaptive game (EVNAG) designed to enhance students' cybersecurity knowledge and skills. The chapter outlines the theoretical game framework and theory, the game's requirements, the learning objectives, and the adaptive algorithm that we propose. It also details the design of “Grown-Up Blues”, a visual novel game based on the EVNAG. Chapter 6 explains the software tools used in the implementation of the game and describes the game's technical implementation and the evaluation methodology used to assess the game's effectiveness. Finally, Chapter 7 concludes the thesis by summarizing its main findings and discusses their implications for cybersecurity education.

Chapter 2 – Background and Literature Review

This section starts by presenting the evolution of cybersecurity education and the variety of means utilized by different authorities to raise the level of awareness of Internet users. Then among the education methods, a discussion regarding educational games ensues based on the empirical evidence. We then explore multiple assessment methods for serious games. Finally, we take a look at the role adaptivity plays in education.

2.1. Overview of cybersecurity education

In 2022 and for the first time, the cybersecurity workforce gap had decreased from 4 million to 3.4 million[1]. However, despite the narrowed gap, 56% of participants say cybersecurity staff shortages are putting their organizations at risk. Raising awareness about the importance of cyber-literacy in users' everyday life is an effective way of reducing the gap and mitigating the dangers presented by the ever-changing nature of cyberattacks. In fact, the human factor poses a growing menace to information security (Hadlington, 2021) and is thus the link to strengthening the cyber defense chain.

Cybersecurity is a field that encompasses multiple subtopics, namely network security, application security, physical security, phishing attacks, social engineering, data breaches, malware, and privacy. The educational methods used to teach the field are very diverse, as can be said about the array of concepts that are included in it. Starting from traditional educational methods like teaching official curriculums in schools and universities to more modern techniques like cybersecurity games and simulations, educators are constantly researching new ways of improving the teaching experience for teachers and learners alike to maximize knowledge retention.

[1] The (ISC)^2 Cybersecurity Workforce Study is conducted annually to assess the size of the current cybersecurity workforce as well as the existing talent shortage: https://www.isc2.org/Research/Workforce-Study#. Accessed 10/05/2023

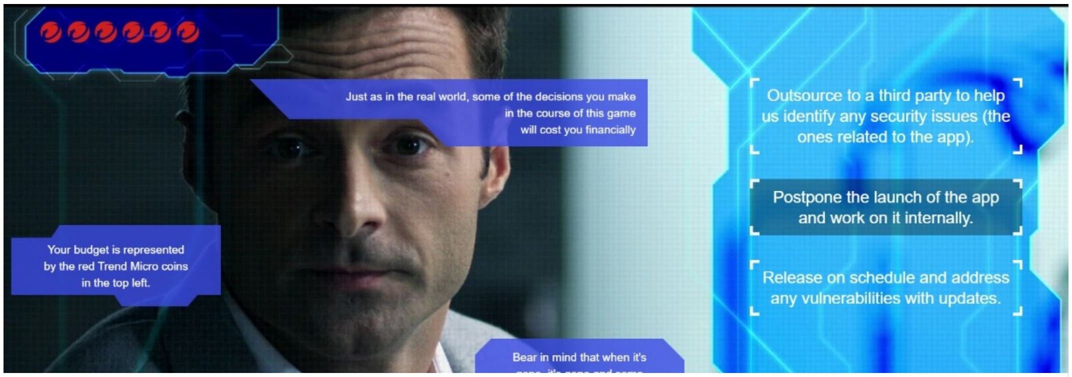
In terms of traditional education, Chen *et al.* compared between American and Chinese universities and identified 64 Chinese universities offering the information security curricula versus 190 universities in the US (Chen et al., 2013). Most programs in both countries relied on formal textbooks and shared the same three teaching approaches: lecture-based teaching, workshops, and design projects. To stay up to date with the market needs, universities constantly update their master's programs by either updating the contents of the courses or changing the structure of the programs to incorporate more specific or elective courses (Cabaj et al., 2018). Moreover, traditional techniques are usually taught using a bottom-up approach, starting with principles and topics of security that are taught separately. Still, there are efforts to restructure cybersecurity education using a top-down and case-driven (TCDC) teaching model (Cai, 2018).

Even though a great demand exists for well-qualified graduates in cybersecurity, it is unfeasible to expect that level of proficiency from everyday users, who are the most at risk of being exploited. That is one of the major incentives behind increasing non-traditional means and methods to raise cyberdefense awareness. Another way of raising awareness about cybersecurity would be embedding cybersecurity concepts in general education classes to provide an opportunity for non-CS majors to discover the field and how it applies to their majors. For example, Harris *et al.* described ways to include cybersecurity topics within the information technology program without adding extra credits (Mark A. Harris & Karen P. Patten, 2015). Traditional methods can be summarized into three sections: 1) Majoring in Computer Science or Information Security, 2) Undergraduate research, and 3) General Education.

Different ways of teaching cybersecurity through gaming and active learning are steering away from traditional methods. Through a review of 71 cybersecurity education papers from 2010 to 2019, Švábenský *et al.* (Švábenský et al., 2020) indicated that within 64 papers describing teaching interventions, the most common teaching method mentioned in 51 articles involves a form of hands-on learning. They list labs, exercises, practical assignments, educational games, and other activities. Based on the academic literature, multimedia can increase a learner's motivation, engagement, and comprehension of educational content (R. C. Clark & Mayer, 2016).

Serious or educational games have several characteristics that make a compelling argument for their adoption in cybersecurity teaching. First, gaming is an active process that gives the player the power to make decisions during a game session. A meta-study prepared by Clark *et al.* (D. B. Clark et al., 2016) observed that games are effective in teaching because of the active nature of playing. Indeed, active learning and active engagement are two facilitators of the learning-teaching experience. Games have the advantage of being interactive as well, which is expected to increase the attention span of learners (Geri et al., 2017) and keep them entertained while they are learning. As any educator would agree, motivation is a crucial component of successful learning. Unfortunately, traditional methods gravitate towards coming across as "dull" or "repetitive." Prensky considers that the more recent generations are used to using electronic devices in their daily life, what he calls "digital natives". The disparity between this modern technological familiarity and the conventional methods of instruction in schools could potentially contribute to a decline in motivation (Prensky, 2009). However, games serve as a means to bridge this gap.

Moreover, the use of multiple media, namely, audio, video, text, and images, as well as sound and graphics, makes for a highly immersive game. For example, Murray (Murray, 2017) subscribes to the belief that more sensory information leads to more immersion. However, when discussing computer text games like Infocom's Planetfall, she observes that multisensory interaction is not necessary to create a successful entrancing experience, implying that immersion might depend on factors other than the number of media and sensory stimuli applied.



Just as in the real world, some of the decisions you make in the course of this game will cost you financially

Your budget is represented by the red Trend Micro coins in the top left.

Outsource to a third party to help us identify any security issues (the ones related to the app).

Postpone the launch of the app and work on it internally.

Release on schedule and address any vulnerabilities with updates.

Bear in mind that when it's

Figure 1: Targeted Attack - The game

For example, Figure 1 illustrates a game with multimodal scenarios and situations. The player chooses from a few possible security solutions with a limited budget, and the chain of decisions determines the game's outcome. Building a good educational game requires the game designer to find the balance between an immersive experience and a learning opportunity to keep the players' attention while instilling concepts that will outlive their playing sessions.

2.2. Educational games in cybersecurity

Despite initial skepticism, games and gamification have increasingly been used to grow knowledge and enhance or set off positive behavior (Sanchez et al., 2020). Blunt gathered evidence from three studies that unmistakably corroborate that the students who had serious games incorporated in their classes had significantly better results than the control group (Blunt, 2009). Furthermore, Furuichi *et al.* (Furuichi & Aibara, 2019) organized a Game Jam, tested the effectiveness of some games on students, and compared it with other learning methods. Written material improved the students' knowledge by 37.5%, while serious games raised the bar to 50%. They also identified a weakness in their games: a minimal effect on players who felt that the games were "not fun."

The analysis of four serious games by Roepke *et al.* (Roepke & Schroeder, 2019) finds that to teach more sustainable knowledge or skills in CS, and there needs to be a mixture of factual, conceptual, and procedural knowledge. Game-based approaches need to create relevance for the content and answer imminent questions regarding why to learn about a topic of cyber security and what the risks are. Due to constant changes in cyber security (i.e., adversaries trying new techniques, using hidden backdoors, or relying on unaware users), teaching cyber security needs to be sustainable. It needs to guide users to use the gained knowledge or skills and adapt them to new challenges in cyber security. They still need to continue learning about unknown risks, but with foundational skills and knowledge from previous learning opportunities, this should be less challenging than before.

Jin *et al.* delivered summer camp activities using game-based learning to teach concepts of cybersecurity principles to a total of 181 high-schoolers (Jin et al., 2018). The post-camp survey indicated that the game-based learning approach had enhanced students' knowledge of cybersecurity and educated them on the digital citizenry and security awareness. It also motivated the students to pursue careers in the field of cybersecurity.

Švábenský et al. went a step further in their research and showed that even the process of designing serious cybersecurity games strongly benefits cybersecurity education (Švábenský et al., 2018).

2.3. Evaluation of educational games

To ensure the continuous creation of good quality games, it is important to find accurate ways of assessing them and gathering criteria upon which the judgment of the games will fall.

Calderon and Ruiz (Calderón & Ruiz, 2015) reviewed 102 articles on educational games' evaluation methods. They found that questionnaires were the main assessment method in 90% of the studies. A common approach used in games assessment is pre-testing and post-testing. This method tests the participants pre- and post-experiment, attributing any significant difference in the test scores to the experiment. However, this method fails to address whether the act of pre-testing influenced the results (Walsh, 2020). Afterward, Suryapranata *et al.* proposed an assessment method that relies on grouping the software quality factors into two sections: a player-related category and a software-related category (Suryapranata et al., 2017). The player-related category concerns aspects of the game that can be seen and felt by the players, whereas the software-related category concerns the aspects of the game that can neither be seen nor felt**.**

Caserman *et al.* use another approach to assess serious games (Caserman et al., 2020). Considering the double mission of serious games, the researchers grouped their criteria into a "serious" part, described in Table 1 and a "game" part, described in Table 2. This innovative approach considers both sides of educational games, allowing for a more encompassing method of analyzing games. The serious part describes the essential elements for the serious part of the game, whereas the game part describes core elements for appropriate game design and suitable interaction technology. For this reason, this assessment approach is chosen as the assessment method for this research.

Table 1: Caserman's quality criteria for the **serious** component of the game assessment

Quality Criteria	Quality Aspects	Explanation
Characterizing Goal	Focus on the characterizing goal	Learning/Training Goal must remain in focus
		Support players to achieve the characterizing goal
		Game elements should not interfere with the learning process
	Clear goals	Appropriate methods are for the specific application area
		Goals are clear and appropriate
	Indispensability of the goal	Serious part must be mandatory
		Characterizing goal must not be avoidable
		Training and learning tasks should not be a hurdle
Methods	Correctness of the domain expert content	Avoid errors and ensure that the content is technically correct
		Ensure correct technical language
		Remain neutral, especially on political and social issues
	Appropriate feedback on progress	Players should receive feedback on their performance and progress
		Visible and recognizable effects
		Provide simultaneous feedback (visual, audio, haptic, multimodal feedback)
	Appropriate rewards	Provide positive reinforcement and in-game awards
Quality	Proof of effectiveness & sustainable effects	Prove that the characterizing goal is achieved
		Learning/Training effects need to be sustainable
	Awards and ratings	Game awards, professional and user ratings, recommendations by domain experts, game reviews, and number of players/downloads state the quality of the game

As we can see in Table 1, the serious components can be divided into three parts: Characterizing Goal, Method, and Quality.

For the first part, one of the primary objectives of serious games is to ensure that players successfully attain the characterizing goal. The core goal of a serious game is closely tied to its specific application. For educational games, these defining goals often revolve around providing learning or training effects. For that to happen, the learning content needs to remain visible throughout the gameplay. The goal also needs to be clear, so that the player can work towards it, and either a tutorial must be provided, or the game should ensure that the player knows how to complete the tasks. Furthermore, to avoid the player jumping directly into the gameplay while ignoring the learning content, the two must be closely intertwined. In other words, it is essential that the learning goal be indispensable to the game progression.

The second concern of the serious games criteria are the methods. The methods ensure first that the content is factually, historically, and politically correct, and should be expressed in an appropriate technical language. Then, the player needs to quantify his/her progress, and that is achieved by providing different types of feedback, which was found in the literature to increase player motivation. Another important method in managing player motivation is the implementation of appropriate rewards to improve player immersion.

Finally, the quality of educational games is generally validated in research with a study or an empirical evaluation to find proofs of effectiveness and sustainable effects. In addition to controlled trials, game awards also constitute an important way of assessing the quality of educational games.

Secondly, Table 2 presents the criteria for the enjoyment part of serious games. The quality criteria are divided into the player enjoyment aspects and the media presentation aspects. The enjoyment criteria can be divided into the following: the player engagement and experience, the flow of the game, the establishment of an emotional connection between the game and the player, giving the player a sense of control, supporting social interactions, and ensuring that the gameplay is an immersive experience.

Table 2: Caserman’s quality criteria for the **enjoyment** component of the game assessment

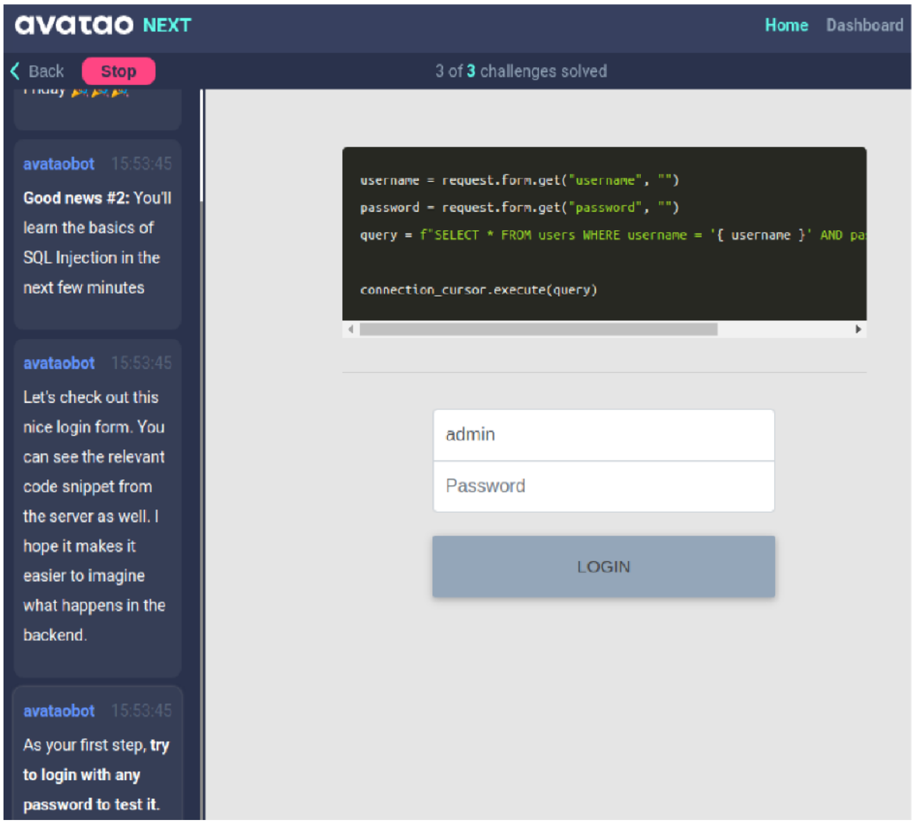
Quality Criteria	Quality Aspects	Explanation
Enjoyment	Player engagement and experience	Provide an engaging experience for different player types
	Ensure flow	Balance between a player's skills and challenge
		Dynamically adapt the difficulty level
		Increase complexity as the player gets better
		Provide varied gameplay
	Establish an emotional connexion	Allow emotions and arouse instinct
	Sense of control	Players should have control over their actions
	Support social interactions	Provide different game modes
	Ensure immersive experience	Multimodal sensory stimulations
Media Presentation	Attractive graphics	Appropriate graphics
		Clear interface
	Appropriate sounds	Appropriate background music and sound effects

The other factor we consider in assessing educational games is the media presentation. To explain it further, media presentation is the way the game is presented, graphic and audio-wise. The graphics are important to a high-quality game, and the interface should be intuitive and easy to use. The background music and sound effects are essential to immerse the player in the process.

The evaluation framework used in this work is based on Caserman's assessment of serious games. The "Proof of Effectiveness and Sustainable Effects" and the "Awards and Ratings" criteria were not assessed or discussed in this research, as the former requires to validate effectiveness with a long-term scientific, clinical, or empirical evaluation, while the latter does not concern most of the online games that were collected (they have not received awards).

2.4. Adaptive Educational Games in Cybersecurity

To the best of our knowledge, and until recently, there was a limited amount of research available on adaptive learning in the field of cybersecurity, as it has remained unexplored for a long time. Gaurav et al. design two cybersecurity games and create two versions of each, one with adaptive features and one without (Gaurav et al., 2023). To make the game adaptive, they classify the users into beginners vs experts, and propose to the user to skip a level when the current level proves too easy. The adaptive version shows improvement of learning outcomes and subjective feedback. Mittal et al. also propose a blockchain-based serious game, where they enhance the NPC interactivity based on players' responses (A. Mittal et al., 2021). They plan to evaluate the game using a subjective questionnaire.



3 of 3 challenges solved

avataobot 15:53:45

Good news #2: You'll learn the basics of SQL Injection in the next few minutes

avataobot 15:53:45

Let's check out this nice login form. You can see the relevant code snippet from the server as well. I hope it makes it easier to imagine what happens in the backend.

avataobot 15:53:45

As your first step, **try to login with any password to test it.**

```
username = request.form.get("username", "")
password = request.form.get("password", "")
query = f"SELECT * FROM users WHERE username = '{ username }' AND pa

connection_cursor.execute(query)
```

admin

Password

Figure 2: Avatao Chat Interface

Also, a few companies use small adaptive learning techniques in the cybersecurity training and education they offer on their platforms. Avatao for example is a cost-free platform that provides a collection of cybersecurity CTF (Capture the Flag) games in its library[2]. As shown in Figure 2, the Avatao[3] interface offers step-by-step explanations to help players understand solutions. Additionally, when a player attempts an incorrect solution, the interface provides them with additional hints.

2.5. Adaptive Nudges in Education

Adaptive nudges can be used to guide the player towards specific choices or behaviors based on their individual preferences or past decisions. Adaptive nudges can take different forms, such as:

- Default nudges (Van Gestel et al., 2021): The concept of a default refers to a preselected option that remains active unless a decision is actively made to change it. The choice of default can have a significant impact on which option is chosen most often. When an opt-out system is used, where a default option is provided, the resulting frequencies are typically higher than in an opt-in system, which lacks a default option.
- Tutorial nudges (Mitrovic et al., 2019): These nudges are designed to guide players through the initial stages of the game and teach them the basic mechanics and controls.
- Feedback nudges (Cappa et al., 2020): These nudges used in games may provide players with real-time feedback on their performance and progress in the game, such as scores, rankings, and achievements.
- Social Norm nudges: These nudges use social comparison and peer pressure to encourage players in adopting certain behaviors or achieve specific goals (Mills, 2022).

Overall, the research aims to fill the gap of information about educational games in cybersecurity. To do that, we followed a three-step approach. Firstly, we survey Internet users to evaluate their knowledge level about cybersecurity. Secondly, we evaluate the quality of existing serious games using Caserman's quality criteria. Lastly, we use the gathered information to propose a framework

[2] https://avatao.com/

[3] (Pavelů, 2021)

to create cybersecurity serious games. Moreover, based on that framework, we implement a visual novel game that incorporates adaptivity in its design. The next chapter will tackle the intricacies of the cybersecurity awareness survey.

Chapter 3 – Survey on Online Privacy and Security Habits

This chapter outlines a survey conducted on the Amazon Mechanical Turk platform to assess the need for educational games in cybersecurity. The aim of the survey was to gauge users' attitudes towards cybersecurity and evaluate their level of awareness and understanding of the subject matter. As the human factor is a critical element in breaking the cybersecurity chain, investigating end-users' cyber knowledge and practices is of utmost importance (Hadlington, 2021). The online study was conducted in May 2021 on the Amazon platform Mechanical Turk (MTurk) with the participation of 400 subjects (reduced to 368 after filtering the answers). MTurk is a crowdsourcing marketplace that allows requesters to gather data by outsourcing tasks to remote workers. We selected this platform since it provides an efficient way of hiring a large, on-demand, global workforce. This approach has also been used in similar studies, such as Cain *et al.*'s investigation of "cyber hygiene," which involved 268 computer users answering questions about their cyber knowledge and behavior (A. A. Cain et al., 2018).

This survey has a total of 45 questions. Its main purpose is to gauge users' attitudes towards cybersecurity and evaluate their level of awareness and understanding of the subject matter. In particular, this survey delves into the area of cybersecurity education, covering aspects such as the tools, the means, and the overall level of concern regarding privacy, as well as the perceived effectiveness of serious games.

The study was directed toward countries with national cybersecurity authorities to perceive the degree of awareness of the populations. Moreover, we surveyed two batches to discern potential differences between American and European countries.

The first batch consisted of 200 people from the US and Canada. The second batch included 200 people as well but from 21 European countries, namely, Austria, Belgium, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Ireland, Italy, the Netherlands, Norway, Portugal, Serbia and Montenegro, Slovakia, Spain, Sweden, Switzerland, Ukraine, and the United Kingdom.

The following section discusses the study design, data analysis procedures, results, and limitations.

3.1. Study Design

The study was designed as a three-step survey. The first part of the survey aims to collect demographic information about the participants. During the second part of the survey, the participants are presented with statements about their awareness of various cybersecurity education tools and their online behavior. The third part of the survey submits a series of scenarios relating to phishing scams that the participants must identify as "suspicious" or "legitimate."

The participants must choose an answer from a 5-point Likert scale, ranging from "Strongly Disagree" to "Strongly Agree." On average, it took European participants 15 minutes to complete the survey, while American participants took 22 minutes to fill it out.

3.1.1. Demographics

The survey starts by providing the participants with a consent form they agree to sign as a first step. Adding control questions in the middle of the study was vital in ascertaining whether bots were used or demonstrating that the responder was meaningfully answering. The control questions request that a specific word be typed, like "CONTROL," for example, to avoid participants mass filling the questionnaire. The survey then asks general demographic questions to establish the participants' age, gender, highest degree earned, technical background, and proficiency in cybersecurity. In the first part of the survey, all questions are in a multiple-choice format.

3.1.2. Cybersecurity

In the second part of the survey, participants were asked questions about their knowledge of cybersecurity education to gauge their preference regarding tools and media (on a scale from "strongly disagree" to "strongly agree"). First, their awareness of multiple media types of cybersecurity education, including games, films, and comics, was tested. Then, the next step was to compare traditional educational tools and non-traditional educational options and ask for the participants' preferences regarding these two different paths. Next, we recorded their opinions regarding the relationship between the type of media used to convey information and the amount of knowledge retained. Here are a few statements presented to the participants in this section:

- I don't feel concerned about cybersecurity because I have "nothing to hide."
- There is a relationship between the type of media used to teach cybersecurity concepts and the amount of knowledge learned.
- Educational games are efficient in getting players to learn new concepts

3.1.3. Case Study: Phishing

The second objective of the survey is related explicitly to phishing and attempts to measure the users' level of proficiency in detecting phishing scams as a case study. The participants were presented with ten scenarios depicting real-life situations, some of which were situations of phishing. The scenarios followed a similar outline in each case. They provided additional information to help the participants choose whether the scenario they were witnessing showed evidence of phishing or if it was a legitimate situation. If they identified the scenario as "suspicious," they were then asked a follow-up question to pinpoint what evidence led them to choose that option.

The scenarios presented seemingly trusted authorities asking for private information from the user in different circumstances. Classifying the scenarios relied on choosing the circumstances that justified trusting the authority.

Each phishing scenario included mention of an authority, which may be trusted or not. That authority is then charged with a message:

You receive a [message] from an [authority]. That message makes a [claim] regarding a specific situation. You need to take [action] to solve that situation.

When the scenario is suspicious, the flaw lies in at least one of the four attributes stated above (message, authority, claim, action). These are the scenarios:

Scenario 1: You are a full-time student and just received a link from the university informing you that you won a tuition-free semester after your name was picked in a raffle draw. You just need to click a link and log in with your student account to collect your prize. (FINANCIAL GAIN)

Scenario 2: You receive an email from your bank, where they address you by your full name. The objective of the email is to present a new type of credit card that the bank is launching. As a long-time customer, you are invited to use it for free for a trial period.

Scenario 3: You register in a community of practice related to your field of research. After a few days, you receive multiple emails from members of that community asking you to click a link and install a program on your laptop or mobile. The link will facilitate sharing of documents and research papers among community members for free.

Scenario 4: You work as an employee in a company, and you receive an email from Human Resources concerning an urgent matter. They ask you to open a PDF attachment and sign it. You notice that HR used a different font and format from their regular communications.

Scenario 5: You receive an email from an unknown sender asking you to fill out a survey regarding your shopping supplies and habits. They claim that once the survey is filled out, you will receive a coupon for $25, meaning that you will need to provide your bank account details to redeem it.

Scenario 6: You are browsing the Internet on Google Chrome while signed into your Google account. You suddenly receive an email from Google claiming that your account was suspended. They ask you to click on a link and enter your Google credentials to activate your account.

Scenario 7: You order an iPhone from Walmart. The following day, you receive an email informing you that your specified address was not found. The email asks you to fill out a form with your address information. You notice that the email is riddled with grammatical and syntax errors.

Scenario 8: It is the end of the month. You received a text message from your boss informing you that you received a big bonus on your salary as a reward for your hard work this month. He asks you to send your social insurance number so he can transfer the bonus directly to you.

Scenario 9: You receive an email from Netflix informing you that someone just logged into your account from a different country. The message does not provide a link and instead tells you to go to Netflix.com, log into your account, and change your password to keep your account secure.

Scenario 10: You are scrolling through your Instagram feed. A post grabs your attention. It asks you to enter information about yourself, namely your name, age, gender, location, and Instagram handle. In exchange for giving away this information, your name gets added to a draw for a $25 Amazon coupon.

The authority is either trusted or untrusted, depending on whether it is known, and its credentials are accurate in the described scenario. The claim may raise red flags if it seems unusual or extreme. The message itself is an indication of the credibility of the scenario. Uncommon fonts or grammatical and syntax errors are generally proof of the unreliability of the message.

The action requested from the user is a key factor in deciding if the scenario is legitimate. For example, suppose the situation requires the user to divulge personal information that would never be otherwise requested. In that case, this suggests to the user that the case's reliability is to be challenged.

3.2. Study Statistical Results

This section presents a detailed examination of the participants' demographic makeup, as well as their responses to the security questions featured in the survey. It also presents the findings and conclusions drawn from the data collected using the MTurk platform.

3.2.1. Participants and Demographic Conditions

Four hundred participants (400) were initially recruited. Incomplete responses were then rejected, as well as responses where the control question was not answered correctly. This resulted in 32 people being excluded from the analysis, leaving a total number of 368 participants. The demographic details of the study sample are presented in Table 3.

Table 3: Demographic characteristics of the study sample

Demographic Variable	Category	Frequency %
Gender	Female	31%
	Male	69%
	Non-binary	<1%
Age	18-25	20%
	26-34	42%
	35-44	20%
	45+	18%
Education	No high-school diploma	1%
	High-school diploma	19%
	University or College Degree (Undergraduate Studies)	59%
	Professional Degree (Masters/Ph.D./Medical/Law)	21%
Location	Europe	48%
	North America	52%

The study further reveals that the gender repartition is similar in both locations, with the number of male participants being twice as great as the number of female participants. 80% of overall participants had at least a university or college degree. Their age follows approximately a normal distribution, with 63% of the participants between the ages of 26 and 44. It is also important to estimate the level of cybersecurity awareness, and whether the participants had any technical background to place the responses accordingly. A third of the participants reported being beginners, while almost half of the participants, i.e., 46%, reported having an intermediate level of proficiency in cybersecurity. The last 20% described themselves as experts in cybersecurity. There was no noticeable difference between the participants from Europe and North America regarding their respective technical backgrounds. Figure 3 indicates no discernable difference between the participants from Europe and North America regarding their cybersecurity expertise.

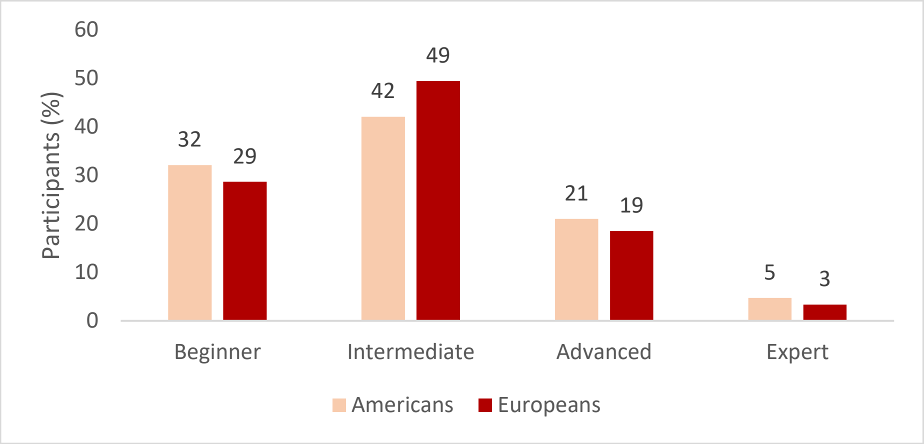


Figure 3: Level of proficiency in Cybersecurity by Location

After having gone over the demographics of the survey, we tackle the summary statistics of the participants' responses.

3.2.2. Participants' Answers

This section describes the answers of the participants to the survey, which was divided into three subjects. The first topic touched on the level of awareness of users about cybersecurity educational tools. The second discussed the users' level of confidence in their online behavior, while the third subsection took phishing as a case study to gain more clarity.

3.2.2.1. Initial cybersecurity educational tools awareness

The study revealed that a high percentage of participants (52%) lacked awareness about the existence of different media and tools that teach cybersecurity. In fact, the statement "I am aware that cybersecurity concepts are being taught through games, comics, films, tabletop games" received mixed responses, as 48% confirmed they agreed with the statement. In comparison, 52% either said they did not know or disagreed. Most participants agreed on a relationship between the type of educational tool used and knowledge retention (71%), and they believe that teaching cybersecurity through games will lead to increased knowledge retention.

3.2.2.2. Level of confidence in online behavior

This question led us to examine the behavior of the users online, or at least their perception of it. The recurrent idea is that some people are confident in their online behavior and consider themselves careful enough to protect their confidential information. The study pointed out a slight difference between American and European responses. Figure 3 shows that 47% of Americans agreed with the following survey statement: "I think I am careful enough with my data not to need cybersecurity training." In comparison, only 33% of Europeans did the same.

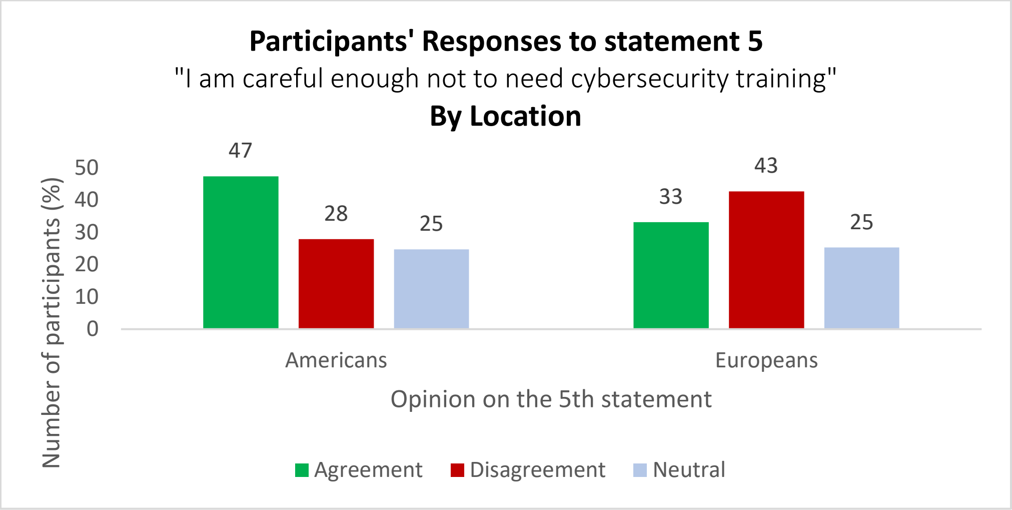


Figure 4: Participants' answers to the 5th statement of the survey by Location

While 13% of European participants did not feel concerned about cybersecurity as they felt they had "nothing to hide," more than a third of American participants, i.e., 37%, agreed with that statement.

Solove answers the nothing-to-hide argument: instead of viewing privacy as secrecy that only wrongdoers should fear, all users should be concerned with their data, as government information-gathering is problematic, and the users' opinions get overlooked (Solove, 2007).

By associating the level of cybersecurity knowledge with the participants' response to the statement: "I don't feel concerned about cybersecurity because I have nothing to hide", we notice that 43% of self-described experts either agreed with the statement or were neutral about it, as well as 48% of participants who described themselves as having an advanced level of

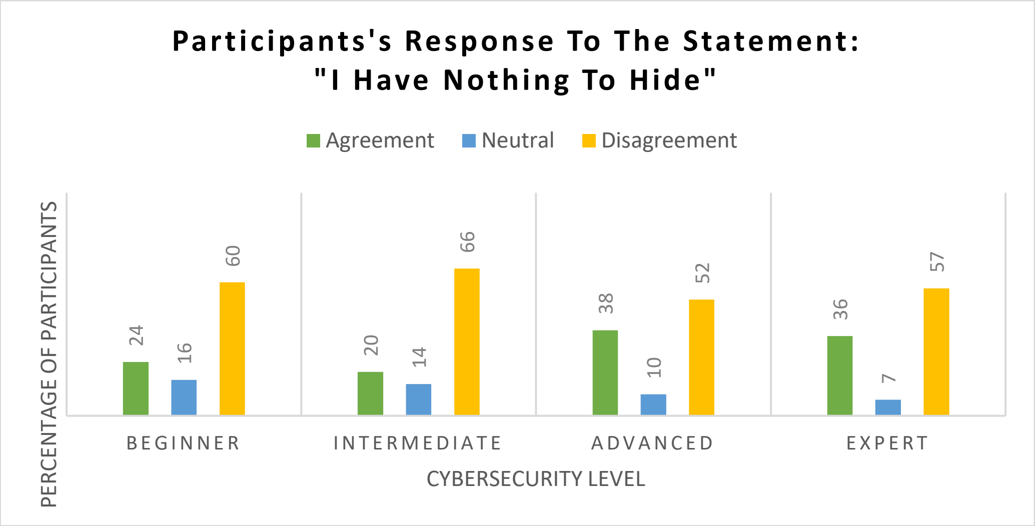


Figure 5: Participants' Reponses to the 6th statement by Cybersecurity Level

cybersecurity. This goes to show a possible discrepancy between the users' knowledge and behavior.

To give tangible form to these statements and test the participants' level of knowledge, they were tested on one of the most common types of cyberattacks: phishing, which is tackled in the next section.

3.2.2.3. Phishing

Phishing is an attack wherein the attacker exploits social engineering techniques to perform identity theft. Phishing traditionally functions by sending forged emails mimicking an authority, like an online bank, an auction, or a payment site, guiding users to a bogus web page that is carefully designed to look like the login page to the genuine site or links [66]. There are other multiple phishing methods, including fake inheritance letters, phony donations, and credit card scams.

In our case, more than 80% of the participants were familiar with phishing, and 69% reported being cautious when receiving any email or link. The survey presented the participants with suspicious and legitimate situations. For example, as seen in Table 4, we classify the first scenario as suspicious. Indeed, as a rule in cybersecurity practices, if it seems too good to be true, it probably is. In this case, universities rarely have a raffle draw to offer free tuition and the need for students to offer their credentials seems suspicious. 67% of participants classified it correctly as suspicious. We classify the second scenario as suspicious as well, because the sense of urgency created by the email is a typical strategy used by phishing actors. Also, the threat of the account being suspended acts as a perfect trap to push users into taking the wrong decisions. 49% of participants wrongly classified it as suspicious. The third scenario is legitimate as the bank addresses the user by their full name, invite them to visit the bank and do not provide any other suspicious items such as links or attachments. 81% of people classified it correctly as “legitimate”. Moving on to the fourth scenario, the reception of multiple emails from different senders with the same link makes the situation suspicious. Furthermore, installing unknown software can be problematic. Only 53% of participants classified the scenario as suspicious.

Table 4: Scenarios Classification Correctness

Scenario	Correct Classification	Correctness of Survey Answers
1	Suspicious	67.9%
2	Suspicious	51.4%
3	Legitimate	81%
4	Suspicious	53.8%
5	Suspicious	62.7%
6	Legitimate	92.1%
7	Suspicious	72.8%
8	Suspicious	61.1%
9	Suspicious	68.7%
10	Suspicious	57.8%
11	Legitimate	96.1%
12	Suspicious	53.2%

Even though the participants declared being familiar with phishing, when presented with phishing situations, almost half of them misclassified 6 out of 12 scenarios.

3.3. Survey Limitations and Discussion

In this subsection, we discuss the limitations or threats to validity of the survey in the first instance, then we proceed to discuss the survey's findings.

3.3.1. Limitations and Threats to Validity

The study was conducted on Mechanical Turk, which carries its own set of biases. Every year, 100,000 workers in Mechanical Turk participate in academic studies, and in any month, there can be up to 25,000 participants that work on more than 600,000 tasks. The same participants repeatedly working on multiple problems exposes them to various experiments and manipulations, creating a situation of "non-naivete"(Meyers et al., 2020). Another drawback is that the population of MTurk lacks diversity and is more highly educated compared to the US population (Chandler et al., 2019). This can complicate how data can be interpreted to be reliable on a population level. Regarding the questions on the survey, they were formulated to consider essential topics in cybersecurity, but they are not exhaustive. Considering the broadness of the topic, it can be impractical to try to cover every aspect of users' cyber knowledge and behavior.

Another factor to consider as well is the level of familiarity users have with certain situations mentioned in the phishing scenarios. If the users have not encountered specific situations, it can be hard to understand the security risks and issues associated with the topic. There are contextual clues that some users might not pick on for example in the scenarios, and it can be relative whether a situation is considered "suspicious" or not.

In addition to that, there may be different responses based on the region of the participant. Indeed, the sensitivity of the data may differ, i.e., some information might be less critical to share (i.e. social insurance number).

Finally, the participants' awareness of being part of a research study can also affect their results and decisions due to the Hawthorne Effect (Ross & Bibler Zaidi, 2019). In our study's case, participants may be affected by the knowledge of being in a cybersecurity research study and become more aware and cautious about their choices. That might misrepresent the reality of users' choices and decisions when confronted with similar situations in everyday life.

3.3.2. Discussion

The study did yield interesting results regarding people's online behaviors, thoughts, and practices. Seeing that our work revolves around cybersecurity and educational games, it was important that the questionnaire treat these topics. In fact, the three parts of the questionnaire were created in response to the following research questions:

1. What educational media and tools are users familiar with in the context of cybersecurity?
2. How aware are the general users of the importance of their security habits and knowledge?
3. In real-life situations, do users know how to spot suspicious situations?

As seen from section 3.2.2.1, more than half of the study participants lacked awareness about the existence of different media and tools that teach cybersecurity. That indicates that the existence of educational games and other media like comics and interactive videos must be promoted in order to shine the light on them and maximize their learning and teaching potential. Furthermore, the discrepancy between the level of confidence and actual level of awareness is problematic. 48% of participants who described themselves as having an advanced level of cybersecurity didn’t care about privacy because they had nothing to hide for example. In fact, even though 84 % reported being familiar with the concept of phishing, more than 56% of participants either thought that antiviruses were the cure to phishing attacks or just did not know. This aligns with the 2020 user risk report from ProofPoint (“2020 User Risk Report: Exploring Vulnerability and Behavior in a People-Centric Threat Landscape,” 2020), which found that "many working adults mistakenly rely on technical safeguards on home and work devices to be failsafe solutions". Going back to our study, we noted a clear difference between the opinions of Europeans and Americans regarding this topic. Indeed, 48% of North Americans thought that antiviruses were very effective against phishing attacks whereas 62% of Europeans disagreed with that statement. A possible explanation is that European companies or companies that collect data on citizens in the European Union need to comply with strict rules regarding the protection of customer data. The General Data Protection Regulation (GDPR), which the European Parliament adopted in 2016, sets a standard for consumer rights regarding their personal data and privacy, indicating that the interest of Europeans regarding their cybersecurity may be higher. Another difference is the approach to cybersecurity. Indeed, the United States favor a bottom-up approach with no specific regulating federal agency, whereas the European Union prefers a top-down approach with a comprehensive legislation and has made data protection a high priority (*Differences Between EU and US Data Protection*, n.d.).

It is also interesting to note that more than a third of Americans felt that they had "nothing to hide", and thus felt that they did not need any cybersecurity training.

In conclusion, the survey showed a lack of understanding of some users of the importance of privacy, as well as a discrepancy between the users' knowledge and behavior. More than half of the participants were not aware of the diversity of tools used to teach correct cybersecurity practices. This confirms that the need for cybersecurity awareness is present. This consolidates the idea that games are an effective means of teaching and transferring knowledge, as most learning happens in an environment free from judgment and where a user is allowed to fail. It is also far from a long and traditional course that may be unpractical to follow for multiple users.

In the next chapter, we will use Caserman's method of educational games assessment, and review current serious games on the market to determine what they are lacking.

Chapter 4 – Assessment of Educational Cybersecurity Games

In this chapter, we survey and analyze educational cybersecurity games using Caserman's assessment method to gain an in-depth understanding of the cybersecurity education landscape. This analysis will enable us to pinpoint any shortcomings in existing cybersecurity games, which will assist us in developing our own cybersecurity educational game framework. Assessing educational cybersecurity games is crucial in determining whether they are effective in teaching cybersecurity to learners. These games are becoming more popular as they provide hands-on experience in identifying and mitigating cyber threats. The assessment process involves evaluating the game's usability, engagement, and effectiveness in achieving learning objectives. It is essential to determine whether the game meets the needs of the learners and promotes knowledge retention and transfer. Several methods are used to assess educational cybersecurity games, such as surveys, pre- and post-game knowledge assessments, gameplay analytics, and expert evaluations. We use Caserman's assessment method as it is not based on specific users' performance and builds its foundation on both the educational and enjoyment criteria that make a game high quality. Considering that some of the criteria need refining, we propose a scale that defines each criterion.

4.1. Games Assessment

This subsection starts by presenting the game search process, the game selection criteria, and the chosen criteria for the evaluation framework. Afterward, each criterion's scale is outlined and used to establish the assessment of cybersecurity educational games.

4.1.1. Search Protocol

The game search was conducted from January 2021 to April 2022. It covered web, desktop, and mobile applications and contained games covering multiple topics of cybersecurity, including phishing, malware, and identity theft. To ensure comprehensive coverage of available games, the study used Google's search engine and the Android Play Store for the search. These two sources are among the primary platforms used by players to download games, making them representative of a significant portion of the market. This approach ensured that the review encompassed a wide range of games available to players. The keywords used mentioned the topic covered, the type of the game, as well as the age group of the targeted users. The keywords that uncovered the highest number of games are: "Cybersecurity Interactive Game," "Cybersecurity Simulation Game," "Cybersecurity Awareness Game," "Security Game," "Privacy Game," and "Cybersecurity Game for Children." These keywords yielded a harvest of more than 60 games, a few of which were discarded for not adhering to the selection checklist in section 4.1.2. below.

4.1.2. Game Selection

According to Khan (KS Khan et al., 2001), systematic reviews must have clear-cut inclusion or exclusion criteria. Keeping up with the latest trends in cybersecurity gaming, the games selected were developed during the last decade (between 2012 and 2022) to create a more detailed and comprehensive image of what the cybersecurity games market presents.

Table 5: Inclusion/Exclusion Criteria

Selection question	Inclusion	Exclusion
Is the game in English or French?	The game is in English or French.	The game is in a different language.
Does the game treat subtopics of cybersecurity (phishing, malware, e-safety, etc.)?	The game does treat one of the cybersecurity subtopics.	The game does not treat cybersecurity topics.
Is the game free?	Yes, the game is free.	No, the game is not free (license, membership, one-time fee, demo…)
Was the game developed after the year 2012?	The game was developed between 2012 and 2022.	The game was developed earlier than the year 2012.

As Table 5 displays, games were eligible for inclusion if they used English or French and if they discussed and treated cybersecurity topics like privacy and internet security.

To ensure the relevance of the selected games to the current market, only the games released after 2012 were considered. Also, we made sure that the selected games were free and accessible to all internet users. These games include a variety of genres such as quiz, adventure, and strategy games, and were designed to balance educational content with enjoyable gameplay. Consequently, they are categorized as serious games. Table 6 shows the games that passed the selection criteria.

Table 6: Reviewed Cybersecurity Games

Game Number	Game Name	Privacy Issues Tackled	Age-Group	Year
1	The Missing Link	Phishing and smishing	All	2020
2	Cybersecurity Circus	Identity theft, passwords, general cybersecurity, e-safety	All	2019
3	AggieLife	Online scams, passwords, e-safety, spyware	All	2018
4	Keep tradition secured	Spoofing, privacy, internet security, phishing	All	2017
5	What's your status	Privacy, Passwords, general cybersecurity	Young adults and older	2013
6	Fight Back	Identity Theft, Online Shopping, Malware	Young adults and older	2014
7	Targeted Attack	Company Security	Young adults and older	2015
8	CyberAwareness Challenge	General cybersecurity, Insider Threats, Social Networking	Young adults and older	2022
9	Tomorrow's Internet	Phishing, Passwords, Malware	All	2015*
10	Who is the risk	Insider Threats	All	2015*
11	Whodunit Mystery Game	Insider Threats and Phishing, Hacking, Malware	All	2015*
12	CyberJulie	Privacy, Cybersecurity practices	Children	2017

Game Number	Game Name	Privacy Issues Tackled	Age-Group	Year
13	Cybersecurity Lab	General Cybersecurity, Data breaches, Phishing, malware, general cybersecurity, Password Security	All	2021
14	Microsoft Security Adventure	Phishing, Malware, Identity Theft, Hackers	Young adults and older	2020
15	Interland	Privacy	Children	2017
16	Hotspot (Living Security)	Phishing, Good security practices	Young adults and older	2021
17	Cybersecurity Ops	General Cybersecurity	Young adults and older	2020
18	Trend Micro (Data Center Attacks)	Privacy, Data Leakage	Young adults and older	2017
19	Cyberhunters – Ghost in the net	Identity theft	Young adults and older	2019
20	Officeware Inc.	Phishing, Malware, Updates	All	2021
21	CyberJeopardy	RMF, Cyberattacks, Network Security, Roles, Cryptography	Young adults and older	2015*
22	CyberLand	Routers, Security Laws, Passwords, Firewall	All	2020
23	CDSE Insider Threat Concentration	Insider Threats	Young adults and older	2016
24	Hacker Bot	Passwords	Young adults and older	2021
25	Education Arcade: Brute Force	Passwords	All	2020
26	Cryptris	Asymmetric Cryptography	Young adults and older	2018
27	Privacy Pirates	Privacy	Children (7 to 9)	2021
28	Blue Team: A firewall Setup game	Firewall Setup	Cybersecurity specialists	2017
29	Conectado	Cyberbullying	Teenagers	2018
30	The weakest link	Password, general cybersecurity, User security	Employees	2015

Game Number	Game Name	Privacy Issues Tackled	Age-Group	Year
31	HackTale3D	Hacking, Security Key, Database Encryption, SQL, Cyberdefense	Cybersecurity Students or people familiar with security	2018
32	SOS FBI - Safe Online Surfing	Online Safety and Privacy	Children	2018
33	Datak	Protection of data, privacy, and cost-benefit analysis	All	2016
34	J'accepte (UFC)	Privacy and online safety	All	2019
35	Cybersecurity Game Spoofy	Online safety, Privacy	Children	2021
36	Centigrade Black Belt Cybersecurity Training	Privacy, Cybersecurity, Spam Defense, Phishing, Social Engineering	Employees	2019
37	Data Defenders	Privacy	Children	2016
38	Infosec Deep Space Danger	Social Engineering and malware	Young adults and older	2021
39	Cyber Challenge	Cybersecurity	Young adults and older	2020
40	Reality Check: The Game	Authentication, Fake News	All	2016
41	Click if you agree	Privacy terms and conditions	Pre-teens	2016
42	CyberSprinters	General Cybersecurity	Children	2021
43	Hacking Hero – Cyber Adventure Clicker	Hacking	Young adults	2019
44	Band Runner	Online safety	Children (8 to 10)	2020
45	Enter	IT security, Phishing, Cybersecurity	All	2018

(Continuation: Reviewed Cybersecurity Games)

*The release year of the game was conjectured as best as possible given the surrounding elements of the game.

We identified 45 educational games for educating users about cybersecurity created this last decade. Table 7 presents a heatmap of the number of games that tackle each educational subject between 2012 and 2022.

Table 7: Number of Games by the Educational Subject between 2012 and 2022

Date	General Cybersecurity	E-safety	E-privacy	Data Security	Phishing	Network Security	Total
2013	1	0	0	0	0	0	1
2014	0	1	0	0	0	0	1
2015	2	0	0	2	1	1	6
2016	1	1	2	1	0	0	5
2017	0	0	3	1	0	1	5
2018	0	3	0	2	1	0	6
2019	2	1	1	1	0	0	5
2020	3	1	0	0	2	1	7
2021	3	2	1	0	2	0	8
2022	0	0	0	0	0	1	1
Total	**12**	**9**	**7**	**7**	**6**	**4**	**45**

The educational subject was defined based on the previous assessment of the games' educational content as well as the work done in a similar study (Zhang-Kennedy & Chiasson, 2021). Games that teach a wide range of cybersecurity concepts are placed under the subject of "general cybersecurity". The sub-topics related to privacy, like terms and conditions for example, are gathered under "e-privacy". Sub-topics relating to passwords and authentication, as well as identity theft and social engineering are under the category "e-safety". Under "network security" are the sub-topics of security of networks, firewalls, routers, and databases. Then, the sub-topics assembled under "data security" are social networking, online shopping, and user security. Table

7 shows that the number of games being designed appears to be steadily increasing over the past few years. The review was conducted until the month of April 2022, which explains the discrepancy of the number of games for the year 2022.

After selecting the games following the requirements above, the next step is to determine the evaluation framework and choose the criteria on which the assessment will be based.

4.1.3. Criteria Rating Scale

The evaluation framework used in this paper is based on Caserman's assessment of serious games. As this paper is a first approach to this topic, the criteria selection was based on short-term impact. The "Proof of Effectiveness and Sustainable Effects" and the "Awards and Ratings" criteria were not assessed or discussed in this paper. The former requires validating effectiveness with a long-term scientific, clinical, or empirical evaluation; while the latter does not concern most of the online games that were collected (they have not received awards). These games will be used as a reference to build a blueprint for future educational games.

These criteria need to be gauged and evaluated using a rating scale that would cater to the different characteristics of every feature. The specificities of the scale of each criterion are detailed in the following subsection. Every game was assessed for each criterion in both tables (for the serious and enjoyment components) following a general 3-point rating scale.

Table 8: General Rating Scale

Scale	Explanation
3 points	Better than average set of practices, that addressed the criterion well and created a good level of performance for the game.
2 points	Multiple elements of the feature implemented, and the criterion present.
1 point	Insufficient implementation of the features relative to the mentioned criterion.
0 point	Criterion not met.

This rating scale in Table 8 represents how features are assessed from a general point of view. To evaluate objectively the criteria, we create a scale specific to each criterion based on the characteristics and rules presented below.

a. Focus on goal

By definition, serious games aim to convey educational content or training to the users (Almeida, 2017). As such, the games should focus on supporting the player to achieve that goal by emphasizing the learning material during gameplay and preventing the game elements from interfering with the teaching/learning process (Caserman et al., 2020). Table 9 presents the characteristics used to rate this criterion.

Table 9: "Focus on Goal" Characteristics

Characteristics **(Caserman et al., 2020)**	**Low focus (1pt)**	**Medium focus (2pts)**	**High focus (3pts)**
Goal described at the start	Yes	Yes	Yes
Learning and training remain in focus during gameplay		Yes	Yes
Game elements don't interfere with the learning process			Yes

b. Clear goal

Serious games need to ensure that the goal is clear, as in entertainment games so that players know how to work towards it and achieve it. In this case, either the goal should be transparent, or a tutorial should be presented to ensure that the players acquire the skills needed to play the game, as shown in Table 10. The intermediate goals should also be clear and introduced appropriately during gameplay [(Sweetser & Wyeth, 2005), (Desurvire & Wiberg, 2009)].

Table 10: Clear Goal" Characteristics

Characteristics *(Sweetser & Wyeth, 2005), (Desurvire & Wiberg, 2009)*	**Low clarity (1pt)**	**Medium clarity (2pts)**	**High clarity (3pts)**
General goal described	Yes	Yes	Yes
Game ensures players know how to play (rules, tutorial)		Yes	Yes
Skills needed are taught early enough to use to play			Yes
Intermediate goals are clear and presented at appropriate times			Yes

c. Indispensable goal

It should be mandatory for the player to engage in the serious part of the game. Otherwise, the enjoyment part might prevent the player from learning or training. As Giessen (Giessen, 2015) explains, "many learners try to avoid learning modes to return as fast as possible to a gaming mode." Therefore, the characterizing goal should be "embedded in the gameplay" (Caserman et al., 2020). The rating features for this criterion are detailed in Table 11**.**

Table 11: "Indispensable Goal" Characteristics

Characteristics *(Giessen, 2015)**,** (Caserman et al., 2020)*	**Low level (1pt)**	**Medium level (2pts)**	**High level (3pts)**
The goal is present but can be skipped to go to the fun part.	Yes	Yes	Yes
The goal is not avoidable (it is not possible to skip the serious part to get to the fun part).		Yes	Yes
The training and learning tasks are not a hurdle.			Yes

d. Correctness of the domain expert content

An evident requirement for serious games is the correctness of the domain expert content. The language, factual knowledge, and technical content must be adequate and correct, as shown in Table 12.

Table 12: "Correctness" Characteristics

Characteristics *(Caserman et al., 2020)*	**Low correctness (1pt)**	**Medium correctness (2pts)**	**High correctness (3pts)**
Language Correctness	Yes	Yes	Yes
Correct Factual Knowledge		Yes	Yes
Correct Technical Content		Yes	Yes
Social/Political Neutrality			Yes

“The games must not contain any errors concerning their subject matter, such as erroneous mathematical equations, incorrect information on historical events, or inadequate information" (Caserman et al., 2020). Furthermore, the games should remain neutral regarding social and political issues.

e. Appropriate feedback

Feedback is delivering information to the players about the "correctness of their responses" to improve the players' performance, motivation, or learning outcomes (Graesser, 2017). First, feedback is essential to serious games as a way for the users to evaluate their progress in achieving the characterizing goal (Caserman et al., 2020). Then, the timing of the feedback matters as well, and immediate feedback has shown some preliminary evidence of achieving more significant results than delayed feedback (Landers & Callan, 2011). Finally, multimodal feedback (visual, audio, or haptic) can also be valuable (Desurvire & Wiberg, 2009) and contribute to a highly immersive experience. This criterion is rated following the heuristics gathered in Table 13.

Table 13: "Appropriate Feedback" Characteristics

Characteristics *(Desurvire & Wiberg, 2009),* *(C. I. Johnson et al., 2017), (Landers & Callan, 2011)*	**Low feedback** **(1pt)**	**Medium feedback** **(2pts)**	**High feedback** **(3pts)**
Light Feedback	Yes	Yes	Yes
Continuous Immediate Feedback		Yes	Yes
Comprehensive Feedback		Yes	Yes
Multimodal Feedback			Yes
Progress Assessment (bar…)			Yes

f. Appropriate Rewards

Following Johnson et al. (D. Johnson et al., 2018), we classify rewards into three categories: "low reward," "medium reward," and "high reward" conditions in Table 14. The players' immersion in the game was shown to be positively impacted by the presence and multitude of rewards (Caserman et al., 2020).

Table 14: The "Appropriate Rewards" Characteristics

Characteristics *(D. Johnson et al., 2018), (Malouf, 1988), (Semet et al., 2019)*	**Low rewards** **(1 pt)**	**Medium rewards** **(2 pts)**	**High rewards** **(3 pts)**
The reward of access (Access to a new level)	Yes	Yes	Yes
Rewards of facility and sustenance		Yes	Yes
Rewards of glory and praise			Yes
Rewards of sensory feedback			Yes

Research suggests that even though designers lean towards giving higher value to intrinsic motivation, the latter can be fueled by extrinsic motivation, i.e., rewards (Malouf, 1988). The learning process can also be more efficient when accompanied by "mechanical motivation mechanisms" like rewards (Semet et al., 2019). Points, virtual badges, power-ups, achievements, and updating avatar functionalities are all examples of in-game rewards.

g. Ensure Player Engagement and Experience

Engagement and enjoyment are crucial to the gameplay experience (Koster, 2013). Sweetser and Wyath built the GameFlow model, consisting of 8 elements that include a set of criteria to achieve enjoyment (Sweetser & Wyeth, 2005). For example, to help the players concentrate and increase their engagement, the games should provide a lot of stimuli from different sources, as shown in Table 15. Also, players should not be distracted from tasks that are not important to the gameplay.

Table 15: "Player engagement and experience" characteristics

Characteristics *(Bartle, 1996), (Sweetser & Wyeth, 2005), (Koster, 2013),*	**Low Engagement & Experience (1pt)**	**Medium Engagement & Experience (2pts)**	**High engagement & Experience (3pts)**
No distraction from essential tasks - players should not be distracted from tasks that they want or need to concentrate on (not burdened with seemingly unimportant tasks)	Yes	Yes	Yes
Game provides stimuli from different sources.		Yes	Yes
Provide an engaging experience for at least 2 of Bartle's player types (narrative, different fun components to provide an engaging experience for different player types).			Yes

However, the presence of different types of players makes it mandatory for the game designer to include various enjoyment components and cater to all the types of players (Bartle, 1996). Bartle's player types are Achievers, Explorers, Socialisers, and Killers (depending on whether the player is acting on or interacting with the game world and the other players).

h. Ensure Flow

Csikszentmihalyi highlights in his research that people worldwide describe flow, or "optimal experience," similarly when enjoying different activities (Csikszentmihalyi & Csikzentmihaly, 1990). Regardless of social class, age, or gender, the researcher found that enjoyment was expressed in the same manner.

Table 16: "Ensure Flow" Characteristics

Characteristics *(Brom et al., 2014),(Van Oostendorp et al., 2014),(Kiili, 2005)*	**Low flow (1pt)**	**Medium flow (2pts)**	**High flow (3pts)**
Balance between challenges and skills (easy to learn, difficult to master)	Yes	Yes	Yes
Varied Gameplay (Strategy, Narration, Choices, Arcade, Exploring...)		Yes	Yes
Statically adapt difficulty level (Offline adaptivity)		Yes	Yes
Increase complexity as the player gets better			Yes
Dynamically adapt difficulty level depending on current player's performance (Online adaptivity)			Yes

The optimal experience improves when "a participant's skills required to accomplish a given task match the task's demands" (Brom et al., 2014), i.e., when a balance between challenges and skills exists. Therefore, the game should adapt the difficulty level depending on the players' level, performance, and experience. Lopes and Bidarra mention multiple adaptation components, like "the layout of the game world can be made simpler for underachieving players" (Lopes & Bidarra, 2011). Table 13 highlights the rating details for the "ensure flow" criterion.

i. Establish Emotional Connection (Allow emotion and arouse instinct)

Creating an immersive experience involves creating great experiences built on players' emotions (Desurvire & Wiberg, 2009).

Table 17: "Establish Emotional Connection" Characteristics

Characteristics *(Sweetser & Wyeth, 2005), (Desurvire & Wiberg, 2009), (Dillon, 2011)*	**Low emotional connection (1pt)**	**Medium emotional connection (2pts)**	**High emotional connection (3pts)**
The game engages at least one of the 11 core instincts	Yes	Yes	Yes
There is an emotional connection between the player and the game world and their "avatar."		Yes	Yes
The game transports the player into a level of personal involvement emotionally (e.g., scare, threat, thrill, reward, punishment) and viscerally (e.g., environment sounds).			Yes

To analyze gameplay, Dillon proposes a theoretical framework based on six basic emotions and eleven instincts, like survival and self-identification (Dillon, 2010). Emotional involvement allows the players to connect with the game world (Sweetser & Wyeth, 2005). In fact, emotions influence both the player's immersion sensation and motivation. This feature was described in more detail in Table 17**.**

j. Sense of Control

The sense of control attained through the ability of the players to influence the course of events, and the outcome of the game is one of the primary motivators in video games (McCallum, 2012). Indeed, "players should feel in control over their actions in the game world" (Sweetser & Wyeth, 2005).

Table 18: "Sense of Control" Characteristics

Characteristics *(Sweetser & Wyeth, 2005),(McCallum, 2012)*	**Low control** **(1 pt)**	**Medium control** **(2 pts)**	**High control** **(3 pts)**
Control over the game interface and input devices.	Yes	Yes	Yes
Control over the characters or units and their movements and interactions in the game world.		Yes	Yes
Impact on the game world (Different actions lead to different outcomes)		Yes	Yes
Control over actions and strategies (not simply discovering actions and strategies planned by the game developers)			Yes

The bigger the impact of their choices, the more the games become replayable, as the players enjoy trying different paths to discover the available endings of the game (Sweetser & Wyeth, 2005). We elaborate on that in Table 18 above.

k. Support Social Interactions

Squire believes that social interactions are critical aspects of learning through games (Squire & Steinkuehler, 2014) and reiterates that good educational games must provide group networks and social interactions. Bond and Beale agree with that concept and Ryan theorizes that interactions between players validate players' psychological need for relatedness, in a self-deterministic approach to investigating motivation for gameplay [(Bond & Beale, 2009) (Ryan et al., 2006)].

Table 19: "Support Social Interactions" Characteristics

Characteristics *(Bartle, 1996), (Sweetser & Wyeth, 2005), (Ryan et al., 2006), (Squire & Steinkuehler, 2014)*	**Low social interactions (1pt)**	**Medium social interactions (2pts)**	**High social interactions (3pts)**
Small social interactions (invite a friend, share the result with a friend, leaderboard…)	Yes	Yes	Yes
Competitive or cooperative elements		Yes	Yes
Competitive-based or cooperative-based play (Support social interactions between players like chats…)			Yes
Include multiplayer game mode			Yes (Optional)

Moreover, considering the existence of different types of players, i.e. players who prefer to interact with other players (Bartle's player types), social interactions in games are essential (Bartle, 1996), as presented in Table 19. Social interactions may even encourage players who dislike games to play, regardless of the tasks proposed (Sweetser & Wyeth, 2005).

I. Ensure immersive experience

Witmer and Singer define immersion as "a psychological state characterized by perceiving oneself to be enveloped by, included in, and interacting with an environment that provides a continuous stream of stimuli and experiences"(Witmer & Singer, 1998). Immersion increases with the use of visceral, audio, and visual content in the game, as shown by Desurvire *et al.* in their Game Usability Heuristics for evaluating and designing better games (Desurvire & Wiberg, 2009).

Table 20: Ensure Immersive Experience" Characteristics

Characteristics [*(Witmer & Singer, 1998), (Desurvire & Wiberg, 2009), (Sweetser & Johnson, 2004), (Naul & Liu, 2020)]*	**Low immersion (1pt)**	**Medium immersion (2pts)**	**High immersion (3pts)**
Visual elements	Yes	Yes	Yes
Audio (sound effects, background soundtracks)		Yes	Yes
Narrative (e.g., introduction, storyline…)			Yes
Haptic			Yes (Optional)

Audio, specifically, is essential for involving and engaging players (Sweetser & Johnson, 2004). Also, Naul et al. (Naul & Liu, 2020) present evidence of a strong relationship between serious games narratives and immersion, with the narratives making the player feel a part of the game. We summarize the information necessary to make the experience immersive in Table 20.

m. Attractive Graphics:

Ravyse et al. describe the success factors of serious games to enhance learning (Ravyse et al., 2017). The recurring terms regarding graphics are "simple interface," "uncomplicated interface," "easily learned interface," and "intuitive interface”, which are organized in Table 21. They also recommend interfaces high in realism with high-end graphics. This, however, does not disqualify reduced graphics, as they can be appropriate for some game types (Minecraft).

Table 21: "Attractive Graphics" Characteristics

Characteristics *(Ravyse et al., 2017)*	**Low-level graphics (1 pt)**	**Medium level graphics (2 pts)**	**High-level graphics (3 pts)**
Basic interface	Yes	Yes	Yes
Straightforward interface with no unnecessary information		Yes	Yes
High in realism			Yes

n. Appropriate Sound:

Engaging the player with quality auditory content (e.g., sound effects, soundtracks) is essential to draw players into the game and keep them immersed (Cummings & Bailenson, 2016).

Table 22: "Appropriate Sound" Characteristics

Characteristics *(Sanders & Cairns, 2010), (Cummings & Bailenson, 2016), (Caserman et al., 2020)*	**Low-level sound (1pt)**	**Medium level sound (2pts)**	**High-level sound (3pts)**
Background music	Yes	Yes	Yes
Sound effects		Yes	Yes
Customize sounds			Yes

Sanders et al. found that the players disliking the music decreased the overall sense of immersion (Sanders & Cairns, 2010). It is important that the player be able to customize the game sounds and music. The criterion is better described in Table 19.

4.1.4. Games Rating Process

The selected games were assessed based on the objective criteria defined in the previous sections, with each criterion rated and analyzed individually. The appendix displays our assessment of enjoyment characteristics in the selected games, with scores given by the author of this research. This should not mean that the characteristics are subject to the person evaluating them. To ensure that, the developed set of features for each criterion allows for the creation of accurate and reproducible scales that can be used by other researchers. These criteria were refined into characteristics or heuristics that can be applied to evaluate serious games. The subsequent section provides an interpretation of the tables and results.

4.2. Games Assessment Results

This section details the findings of our review of 45 cybersecurity-related games. To assess the games, we employed Caserman's classification, which involves identifying key elements of serious games and adapting principles and requirements from existing game-related literature. This approach allowed us to identify which factors were most prominent in the games and which factors were lacking.

Since our data is ordinal, we use the mode and median measurements to ascertain what criteria are mostly satisfied, and what criteria are lacking. Starting with the criteria for the serious part of the games, we can see from that the criterion that obtained that out of 8 criteria, 3 obtained a median and mode of 5 out of 5. These highest rating criteria are "*Content Correctness", "Indispensable Goal", and "Focus on Goal".* The first criterion evaluated factual, technical, and language correctness and social and political neutrality. This result is not unexpected as the correctness of content is paramount to the design of any educational game. The cybersecurity games we reviewed fulfilled that objective well. Then, the second and third criteria have obtained 5 out of 5 in every game. Indeed, the key characteristic differentiating serious games from digital games is the purpose-driven or goal-driven design (Emmerich & Bockholt, 2016). Engaging in the serious part of the game should be unavoidable when playing a serious game, as we can see was the case with most of the games assessed.

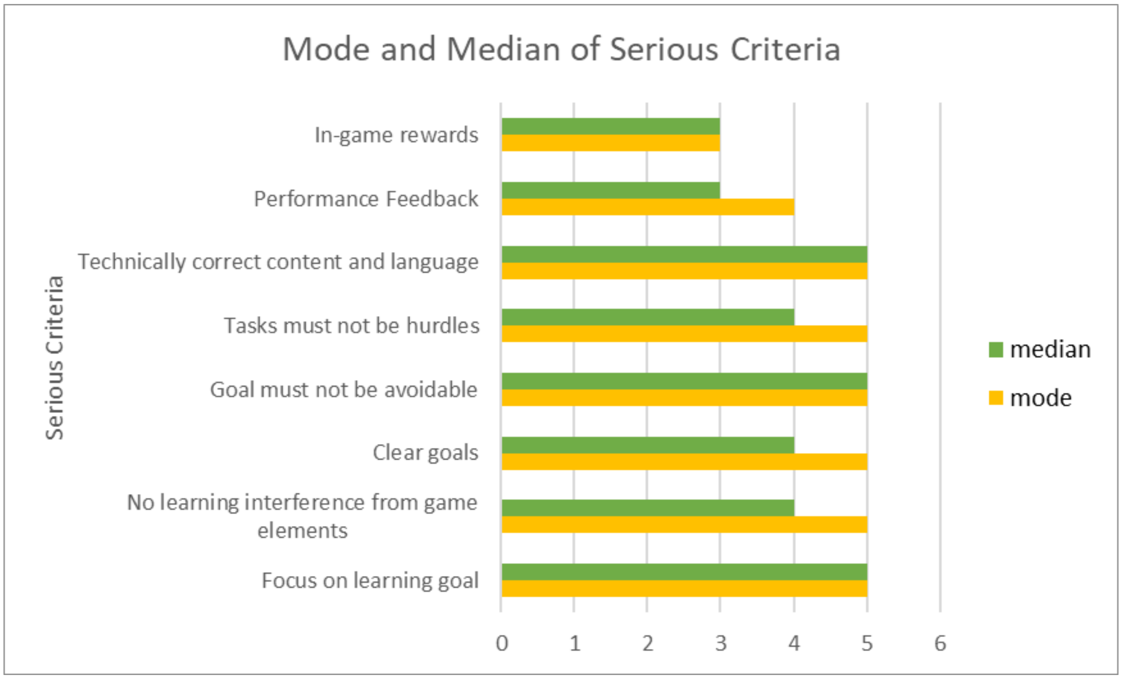


Figure 6: Mode and Median Rating of Serious Criteria

The criterion least fulfilled in the serious part was evaluated to be the "*Appropriate rewards,*" with a mode and median of 3 on the rating scale. Appropriate rewards include positive reinforcement and in-game awards to immerse players more profoundly in the game. The low score of this criterion can be problematic in case of the absence of intrinsic motivation in the games, as reward-based systems can be valuable to motivate players (Nicholson, 2015). In some cases, however, rewards did not affect the learning process. The second least fulfilled factor was the "*performance feedback*" with a mode of 3 and a median of 7. This criterion is important, and an educational game needs to have a way for the players to assess their progress. Continuous (Nkhoma et al., 2014) and postgame (Ravyse et al., 2017) feedbacks are essential in improving the learning process.

Then, we analyze the criteria for the enjoyment part of the game. As apparent in Error! Reference s ource not found., the factors most fulfilled were the *"Sense of Control"* and *"Varied Gameplay"* criteria, rating at a mode and median of 3 on the scale. Indeed, when the player senses that his/her actions control the game, the learning process becomes fun, exciting, and challenging (Tsopra et al., 2020). The varied gameplay ensures that the game is enjoyable to a variety of players.

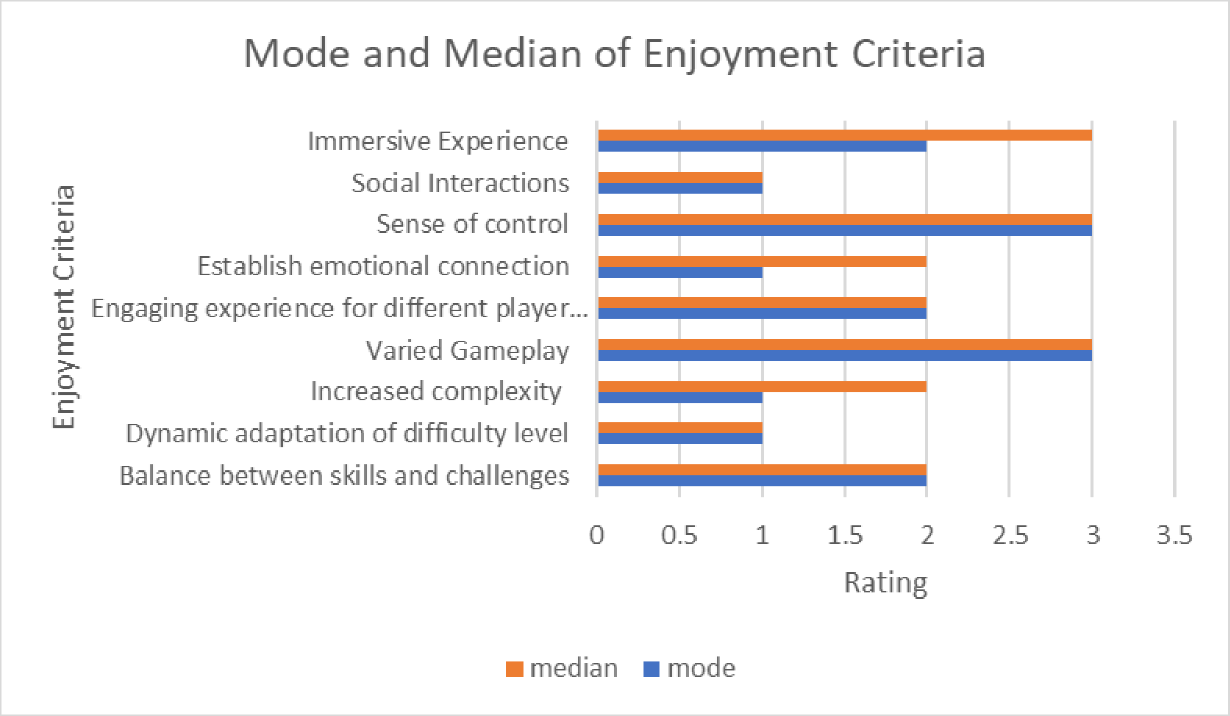


Figure 7: Mode and Median Rating of Enjoyment Criteria

Then, the "*Immersive Experience"* was the third most satisfied criterion with a mode of 2 and a median of 3, which indicates that a considerable proportion of the reviewed games included multimodal sensory simulations like visual, audio, and video to ensure an immersive experience for the players.

We notice that "*Social Interactions*" comes at the bottom of the list with a median and mode of 1. Overall, the reviewed games lacked social interactions, neither having competitive nor collaborative elements or other multiplayer options. The low score indicates that the cybersecurity games reviewed may be perceived as too serious and lack motivation or enjoyment. A study conducted by Vorderer et al. suggests that the competitive elements in games are a "key element of the explanation of players' entertainment experience" (Chan & Vorderer, 2006), while others indicate that cooperation leads to better results than competition among players (Marker & Staiano, 2015). In any case, depending on the player type, the presence of social interactions can increase motivation. The "Ensure flow" criterion also ties at the bottom of the list with a rating of a median and mode of 1, which is low. This criterion refers to the importance of adapting the game's difficulty level to match the player's performance, a crucial element of game design. If a game does not adapt to the player's performance, it can become frustratingly difficult, causing the player to lose interest or abandon the game altogether. On the other hand, if the game is too easy, the player may lose interest due to a lack of challenge. Therefore, it is essential to ensure flow in games to maintain the player's interest and engagement.

Table 23: Measures of the central tendency and variability of the assessment criteria

Measures	Serious Criteria	Enjoyment Criteria
Mode	5	1
Median	4	2
Range	4	4

As indicated in Table 23, there is a substantial discrepancy between the enjoyment criteria and serious criteria modes. The enjoyment criteria received lower ratings compared to the serious criteria, suggesting that many existing serious games prioritize knowledge transfer based on behavioralist principles.

In the context of a cybersecurity educational game, a lack of flow could diminish the effectiveness of the game in delivering its educational content. Serious game developers must address this imbalance and prioritize the enjoyment component of educational games in future cybersecurity games. This concludes the evaluation of the research goal, which aimed to assess the extent to which current games meet Caserman's quality criteria. Based on these findings, we propose in the next chapter the framework of an educational visual novel game with adaptive elements to tackle the flow criterion.

Chapter 5 – Analysis and Design of the Proposed Educational Visual Novel Adaptive Game (EVNAG)

In the first part of this chapter, we propose a theoretical framework for cybersecurity adaptive educational games that we break down into five modules. We describe each module separately and provide an algorithm to apply the framework. The framework was developed based on the games assessment done previously in Chapter 4. Then, in the second part of the chapter, we present "Grown-Up Blues", a visual novel adaptive game based on the EVNAG framework. We detail the game's learning objectives, the design process, the use case, the game's flowchart, as well as the game's functional and non-functional requirements.

5.1. Theoretical Game and Framework

In this section, we introduce the theoretical framework that underpins the design of our proposed cybersecurity adaptive game (Figure 8). It consists of five essential units: a domain model module, a user model module, a user interface module, a learning style module, and a game engine module. The user interface module contains two different views: an interface only visible to the administrator, and a separate interface for the user. The domain model consists of the gameplay story, divided by scenarios, topics, and units. The user model builds a profile of the players by saving their information such as: age, gender, expertise, and background. To preserve the privacy of the users, the user profile information they provide will be associated with a pseudonym and avatar of their choice. Moreover, the user model also considers the player's responses to a pre-defined pre-test to define the difficulty level of the gameplay. This profile allows the game experience to be customizable and adaptable to each different player, which will be carried on by the game engine module.

The game engine module controls the following processes: first, it controls the process of assigning the next scenario of the correct difficulty level to the player. That encompasses Dynamic Difficulty Adaptation (DDA), which adapts the scenario and gameplay to the type and level of the player and introduces nudges to the gameplay to level out the playing field and keep the player's motivation high. Then, the game engine also provides individualized feedback and rewards to each player. The adaptivity feature of the game creates the need for a continuously updated user

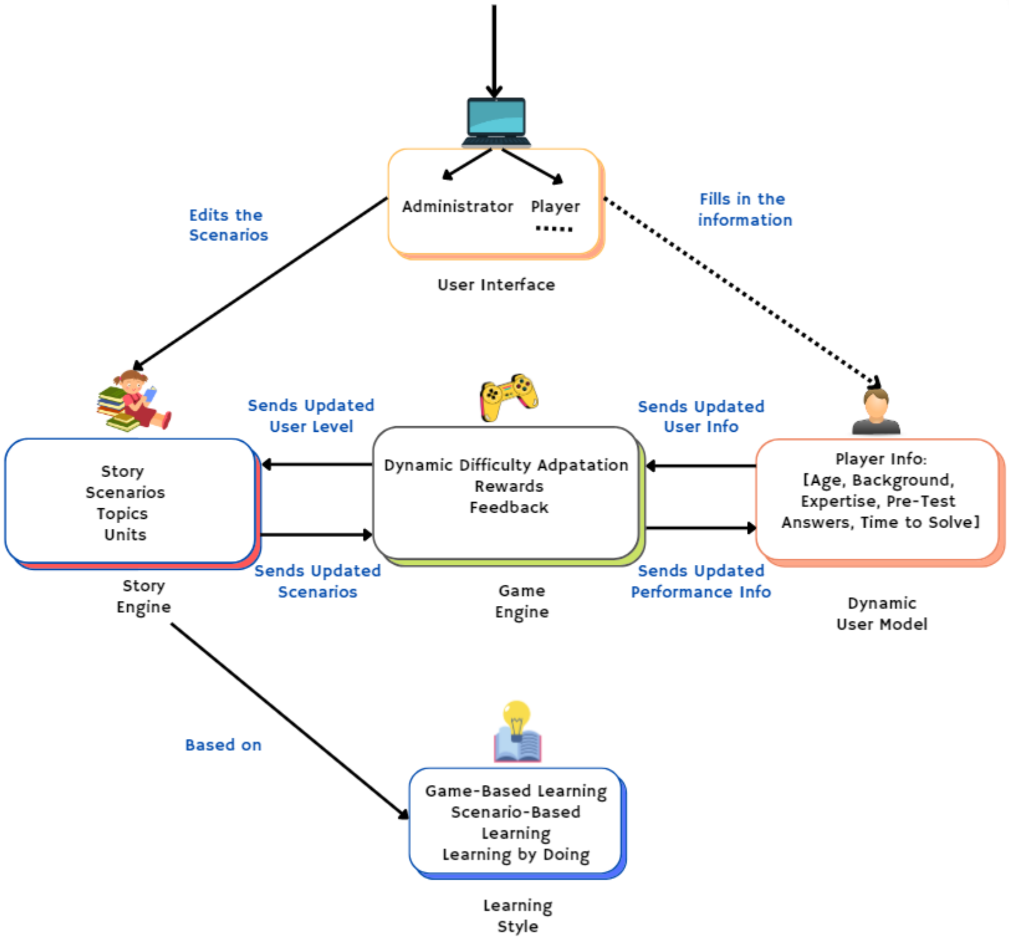


Figure 8: The proposed game architecture Framework (EVNAG)

profile, and continuous communication between the game engine component, the user model component, and the domain model component. Finally, the learning style module represents the techniques and methods used in the creation of the educational content of the game. The concepts used here are game-based learning, case-based learning (or scenario-based learning) and learning by doing.

5.1.1 The Dynamic User Model Module

The user model represents the profile of the player, and it contains all the information that would be useful to determine the level of the player and how to personalize the game according to his/her abilities, characteristics, and preferences. In the proposed serious game, the user model contains the player's login information, age, gender, background, and expertise. This information is stored in the user model the first time the player signs up. The player then proceeds to take a pre-test to allow the system to evaluate his/her initial level of knowledge (in our case in the topics of privacy, security, general cyber-hygiene, and phishing). Once the pre-test is completed, the personal information, as well as the answers to the pre-test questions, are sent to the user-modeling module, which classifies the user into one of five categories of the game difficulty (Beginner, Novice, Intermediate, Advanced, and Expert). The user starts playing at that pre-defined level. However, the user module is dynamically updated with the user's performance, i.e., new information is added to the user profile.

In fact, the user's performance is monitored in two ways. First, the system keeps track of the time taken by the player to complete the level. Then, it monitors whether the user's answers are correct. In whichever case, the gameplay will be changed adaptively depending on his/her performance. The user module finally sends the updated information to the game engine.

5.1.2 The Game Engine

The game engine acts as an intermediary between the dynamic user model and the story engine. At the start of the game, the game engine receives information about the user from the user model. To decide which story unit should be loaded next, the model can consider different features, depending on the specific application: age, gender, background, expertise, pre-test score and assigns weights to each feature, depending on the patterns observed in the user data. There are pre-defined levels of difficulty, and at each checkpoint, the model updates what level the next story unit is going to be. The following NLC Algorithm shows the process of making the game engine choose the level for the next scenario.

NLC Algorithm

(The Next Level Choice Algorithm)

```
Input:
$v_d = (x_1, x_2, \dots, x_n)$, the user vector of dynamic features.
$v_s = (y_1, y_2, \dots, y_m)$, the user vector of static features.
$L = (l_1, l_2, \dots, l_p)$, the set of the different levels of difficulty.
$S = (s_1, s_2, \dots, s_q)$, the set of the different possible stages
(checkpoints).


$\forall s \in S$ and $\forall l \in L$
function levelPredict ($v_d$, $v_s$, $l$, $s$ )
{
  //l being the current level
  Update $v_d$ //update dynamic information like solving time

  $l = \mathrm{DDA}(v_d, v_s, l)$ //get the next level

   return $l$
}
Output:
The next stage's level of difficulty.
```

This algorithm matches a difficulty level to a checkpoint to determine the next scene that the player views and plays. The algorithm takes as input both the user vector of dynamic and static features, the current level and stage. The involved features could be age, gender, self-defined expertise level, the pre-test score etc. It also needs the current level, as well as the current checkpoints. The output computed by the NLC algorithm is the level of the next scenario. The next level is decided by applying the DDA function. Since this is an architecture, we only indicate where the DDA function should be used. The content of the function itself will depend on the game and cybersecurity application.

Let's apply this in an example to understand the algorithm better:

The user "SRAH80", a 34-year-old female, plays a game based on the EVNAG framework. The game starts with the pre-test. She described herself as being of "intermediate" level in cybersecurity, and she scored 75% on the pre-test. Given this data, the model classifies her initially as a Level 3 at the first checkpoint.

The game she is playing, *"Troubles at the university"*, is built on ten different checkpoints, meaning that she will need to make ten different decisions to reach the game ending.

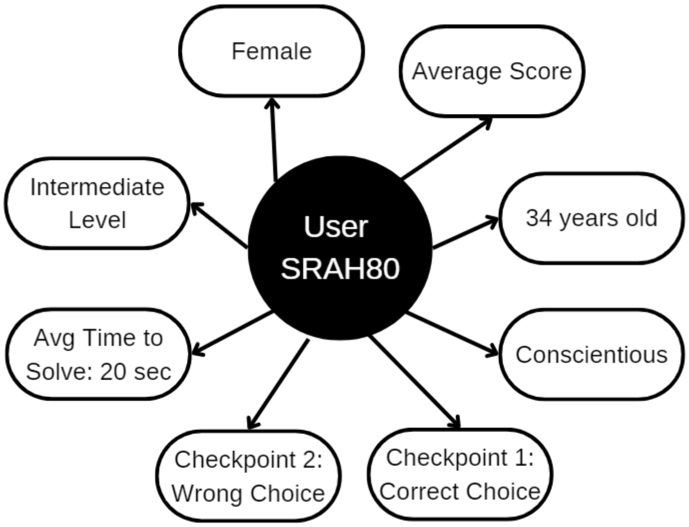

Female
Average Score
Intermediate Level
User SRAH80
34 years old
Avg Time to Solve: 20 sec
Conscientious
Checkpoint 2: Wrong Choice
Checkpoint 1: Correct Choice

Figure 9: An illustration of a User Case

At the second checkpoint, new information appears: the Answer Correctness that was calculated to be 83%, and the Time to Solve estimated at 45 seconds. The current checkpoint user values are calculated by taking the average value of these features from all checkpoints. This data is then fed to the NLC algorithm, which outputs the corresponding level of the next story. **Error! Reference source not found.** below shows an example of a user model for one specific user called "SRAH80":

In this case, the NLC algorithm determined that the next scenario to be loaded at Checkpoint 2 should be of Level 4. The average time to solve and the average correctness of the player's choices are the specific features that take part in deciding how the algorithm makes the next-level choice. We're more concerned with providing a broad understanding of how the NLC algorithm operates, rather than getting into its technical specifics.

5.1.3 The Story Engine

The story engine contains the narrative of the gameplay, divided into topics, levels, scenarios, and units. The topics covered are related to the previously done survey in Chapter 3 to probe into the cybersecurity misconceptions that Internet users may have. Depending on the correctness of their choices during the gameplay, the users will either follow an “ethical” or “non-ethical” path, and the ending of the game will pan out accordingly, by granting a successful ending to the ethical path whereas the users will face a grim finale when following the non-ethical path. However, nuance can be introduced by implementing redemption arcs so that the player can have a bigger sense of control, and improve despite “bad” or incorrect decisions.

It is no secret that malevolent actors create software and use malicious programs to steal user information. However, an insidious way of manipulating users to give their information willingly is perpetrated by the use of nudges. Everyday users lack awareness of the maliciousness and manipulation of ill-wishing Internet programs motivated by criminal reasons or financially exploitable business strategies (van Bavel et al., 2019). The addition of nudges to the game is a way of conveying the dangers of such techniques to Internet users.

Making users experience first-hand the maliciousness of malevolent nudges is part of the “learning by doing” paradigm and aims to teach them how to prevent falling prey to this manipulation.

5.1.4 The User Interface Module

The framework proposes two aspects for the game interface, one for the player and one for the developer or administrator. The players have access to the following functionalities: they can build their profile by adding in their basic information. They can choose a pseudonym, fill in their age, gender, and their expertise level between one and five (1: Novice, 2: Advanced Beginner, 3: Competent, 4: Proficient, 5: Expert). They then have access to the pre-test and answer ten questions in the specified field (privacy and cyber-hygiene questions in our case) that are used by the game engine to determine the player level. Users can also check their profile information including their avatar, their answers to the pre-test, their rewards, and their current quests. The developer has access to the players’ profile information, their answers to the pre-test, their level at each checkpoint, as well as the time taken to solve each scenario. The developer needs access to the game engine as well to update the scenarios if needs be.

5.1.5 The Learning Style Module

The learning style is the method that learners should adopt for treating and interacting with information (Jafari & Abdollahzade, 2019). Game-based learning or educational games have several characteristics that make a compelling argument for their adoption in cybersecurity teaching. First, gaming is an active process that gives the player the power to make decisions during a game session. A meta-study prepared by Clark et al. observed that games are effective in teaching because of the active nature of playing (D. B. Clark et al., 2016). Indeed, active learning and active engagement are two facilitators of the learning-teaching experience. Games have the advantage of being interactive as well, which is expected to increase the attention span of learners (Geri et al., 2017) and keep them entertained while they are learning. A critical review on the effectiveness of narrative-driven digital educational games (Jackson et al., 2018) registers knowledge acquisition in 69.9% of the studies, accomplishment of engagement in 88.4%, motivation in 88.2%, skills acquisition in 90.9%, enjoyment effectiveness in 68.4%, attitude change in 86.7%, and behavior change in 50%. The proposed game uses the following learning styles: game-based learning, scenario-based learning, and learning-by-doing.

The characteristics of the game that work on increasing the motivation of learners are the story narration and the dynamic adaptivity, as well as the rewards, the feedback, and the customizability of the game elements.

5.2. “Grown-Up Blues” Design Process

In this subsection, we present a proof-of-concept experimental visual novel game’s design process. The main goal of our experimental educational game is to showcase how to design a high-quality cybersecurity educational game by integrating all the different parts of this research. The game is based on the EVNAG architecture, which will let us implement the proposed architecture and show its feasibility. First, we discuss the educational content and identify the learning objectives of our educational visual novel “Grown-Up Blues”. Then, we explain the design of the scenarios and provide a visual representation of the game flowchart to illustrate the sequence of events and choices. Next, we outline the requirements of the game. Finally, we explain a few adaptive elements that were incorporated into the game.

5.2.1. Process

The design process of the serious game "Grown-Up Blues" encompasses a series of sequential steps as shown in Figure 10. Firstly, the educational nature of the game necessitates the identification of learning objectives and the determination of educational content. Once this initial phase is completed, the choice of the educational game is made, taking into consideration the targeted age group and player type.

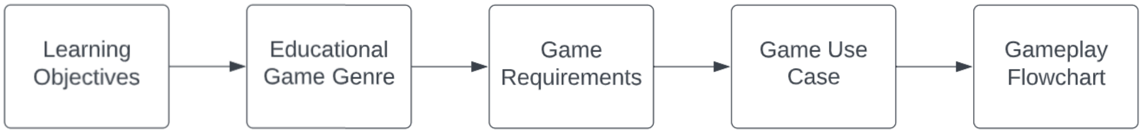


Figure 10: "Grown-Up Blues" Design Process

Then, the game's functional and non-functional requirements are decided to clarify what functions the game will accomplish. The use case is then drawn-up to differentiate between the player roles and system actions. Finally, we build the gameplay flowchart to give an idea of the dynamic execution of the game. The next subsections will address each phase separately.

5.2.2 Learning Objectives:

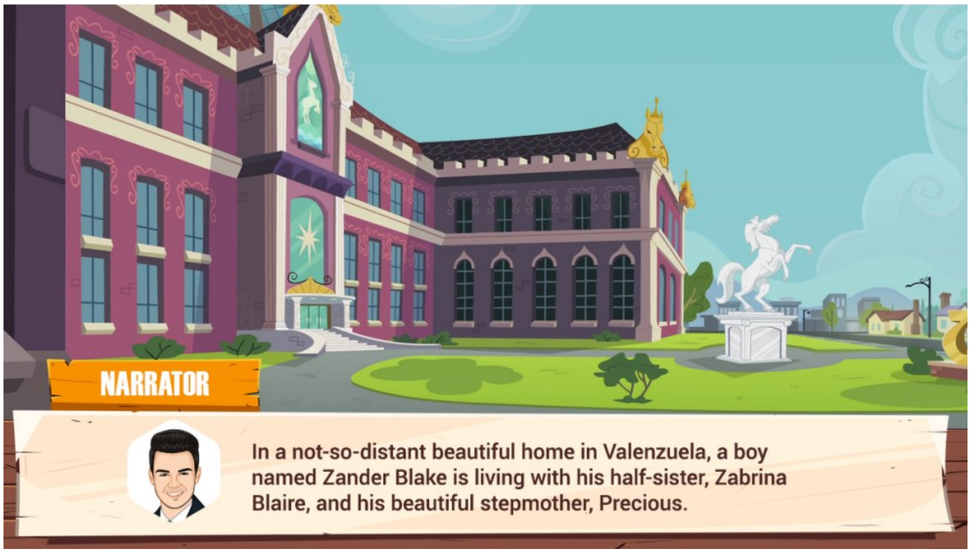
The first phase of the design process is determining the learning objectives of the game. The game stages different situations that have skills for the user to learn. “Grown-Up Blues” tackle the following topics:

- Understanding online privacy and security: “Grown-Up Blues” teaches the player how to identify potential threats to their online privacy and security. This includes recognizing the risks of connecting to unsecured Wi-Fi networks, sharing personal information on social media, and using weak passwords.

- Recognizing phishing scams and social engineering tactics: The game teaches the player how to identify common phishing scams and social engineering tactics used by cybercriminals to steal personal information. This includes understanding the warning signs of fraudulent emails and phone calls and knowing how to verify the authenticity of requests for personal information.
- Protecting sensitive information: The game teaches the player how to protect their sensitive information, such as bank account details and login credentials. This includes understanding the importance of using strong passwords, enabling two-factor authentication, and avoiding the use of public Wi-Fi networks for sensitive transactions.

5.2.3. Educational Game Genre

The second design phase is the choice of the educational game genre. There are various types of educational games, including strategy games, first-person shooters, mini-games, and narrative-based games such as visual novels as seen in Figure 11 (Garcia, 2020). Figure 11 gives us an idea of the allure of narrative-based games. Research has demonstrated that narratives play a significant role in influencing learning outcomes (Plass et al., 2020).



In a not-so-distant beautiful home in Valenzuela, a boy named Zander Blake is living with his half-sister, Zabrina Blaire, and his beautiful stepmother, Precious.

Figure 11: Kinder Learns - An educational visual novel game

Moreover, games incorporating narratives can enhance immersion, engagement, motivation, and learning experiences (Naul & Liu, 2020). Also, when students are familiar with or find the narrative and aesthetics of a game to be surprising, it tends to increase their level of engagement and commitment to the gamification process (Manzano-León et al., 2021).

Considering the rising interest in narrative-based games, we choose to implement a visual novel game, as well as being a fit for our goal to have the player go through seemingly innocuous cybersecurity situations. We will go into that in depth in the next section.

5.2.4 The Game Requirements

After deciding on the game genre, game requirements are a critical aspect of game development as they outline what the game should accomplish, how it should function, and what features and capabilities it should possess. Game requirements can be categorized as either functional or non-functional, with functional requirements describing the specific tasks or actions the game must perform, and non-functional requirements addressing the qualities or characteristics the game must have.

In this section, we outline the functional and non-functional requirements for the development of the EVNAG-based educational game. The game's functional requirements will be based on its learning objectives, while its non-functional requirements will address aspects such as usability, performance, and adaptability.

5.2.4.1 Functional Requirements:

- The game shall present content through visual novel-style storytelling.
- The game shall provide interactive gameplay mechanics to reinforce learning.
- The game shall adapt difficulty based on the player’s performance.
- The game shall provide feedback to the player on their performance.
- The game shall include quizzes or assessments to evaluate the player's knowledge retention.
- The game shall allow players to save their progress and return to the game later.

5.2.4.2 Non-functional Requirements:

- The game shall have a user-friendly and intuitive interface.
- The game shall have a fast-loading time and minimal lag during gameplay.

- The game shall be compatible with a range of devices and operating systems.
- The game shall have a visually appealing design that is appropriate for the intended audience.

Following this, we specify the roles and actions of the two actors of our game: the player and the system.

5.2.5. The Use Case

The following figure illustrates the use case diagram that has been developed to model the behavior of the Educational Visual Novel Adaptive Game (Figure 12).

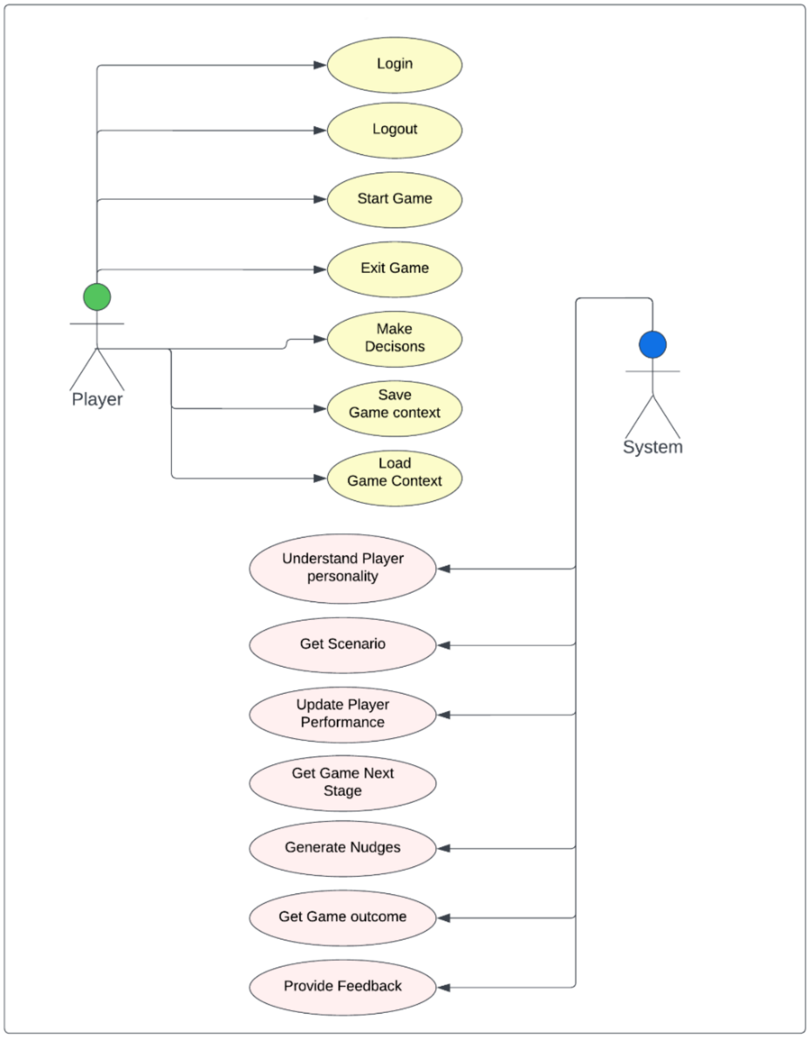


Figure 12: The proposed Cybersecurity Game Use Case Framework

5.2.6. Game Flowchart

The flowchart (Figure 13) is a visual representation of the game's process. The table (Table 24) explains in detail the functionality of each method, as well as its inputs and outputs.

Method	Role	Input	Output
Understand User Personality	Fills in the personality traits of player based on the results of the pre-test	Player Answers to pre-test questions	Personality Trait Scores
Get Scenario	Chooses a scenario from the available pool		
Update Player Performance	Based on the correctness of the choices of the user throughout the game, update his performance score	Previous Performance Score	New Performance Score
Generate Adaptive Nudge or Element	Chooses an appropriate nudge based on the player's personality type and performance	Personality Type & Performance Score	Adaptive Nudge or Element

Table 24: Game Flowchart Methods

The so-called stages are the checkpoints previously mentioned in the EVNAG theoretical framework, which are also the decision points of the players. Here, the flowchart showcases that the game has 5 checkpoints. We give the players a score of 10 at first, and we ask them a personality question whose answer we use to determine the type of nudge we generate. Then, while the player is going through the game, his performance is continuously updated. If the performance stays high, we increase the difficulty of the game by generating a confusing nudge, increasing the number of choices, or introducing timed responses.

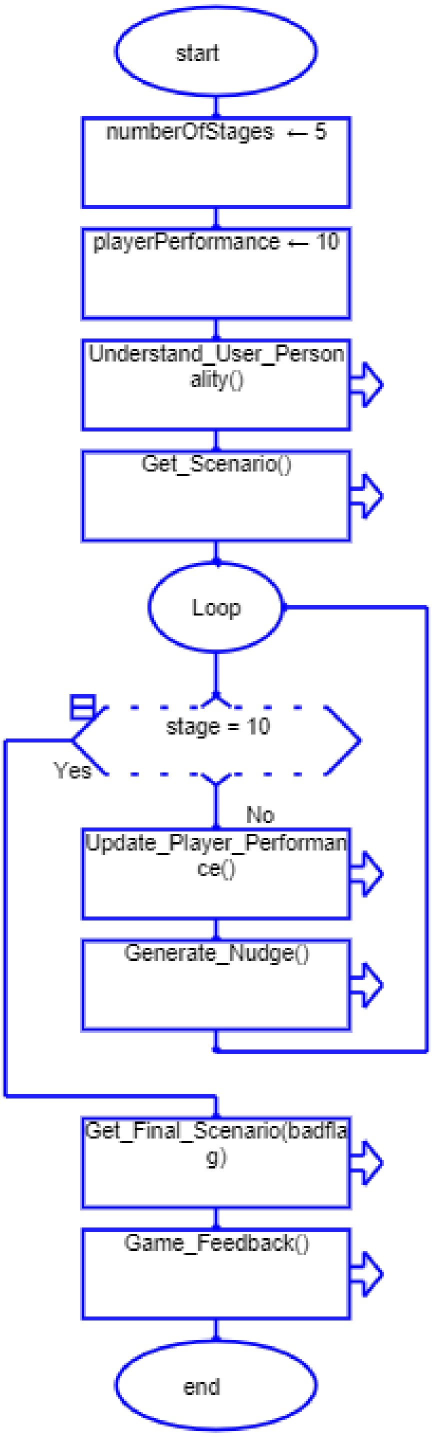


Figure 13: Game Flowchart

Then depending on their choices, the players get either the “happy”/satisfactory ending or the “sad”/unsatisfactory ending. The game then gives them feedback to teach them what they did wrong.

In this section, we covered the analysis and design of our proposed cybersecurity educational game framework. We proposed the NLC algorithm for adaptive serious games. Then, we presented the design of “Grown-Up Blues”, our visual novel game, including the justification of the game genre choice, the design process, the educational content and scenarios, the use case, and requirements. The next section will display the implementation of “Grown-Up Blues” by showing the way we implemented the choices, scenarios, and graphics, as well as the different software used. Then, we conduct an experimental evaluation where we compare the performance of our game with two other cybersecurity games previously assessed in this research.

Chapter 6 – Development and Experimental Evaluation

This section covers the practical application and experimental evaluation of the proposed educational visual novel adaptive game (EVNAG). In the first part of this chapter, we show how we implemented “Grown-Up Blues” by going through the game setting, the scenarios, the dynamic adaptation of level, and the game feedback. We then go through the software and tools used in the implementation of this project. Finally, in the second part, we evaluate three games, including our own, to evaluate their performance.

6.1. Implementation of Design Elements

In the design process, we mentioned multiple design elements in the game requirements, namely: interactive storytelling through scenarios, difficulty adaptation of levels, and game feedback. In this section, we provide a representation of the implementation of these elements.

6.1.1. Game Setting

The game is set in the imaginary city of “Avalora” to which the character “Firdaws” has just moved. “Firdaws” is a university student on a scholarship that needs help to adapt to the

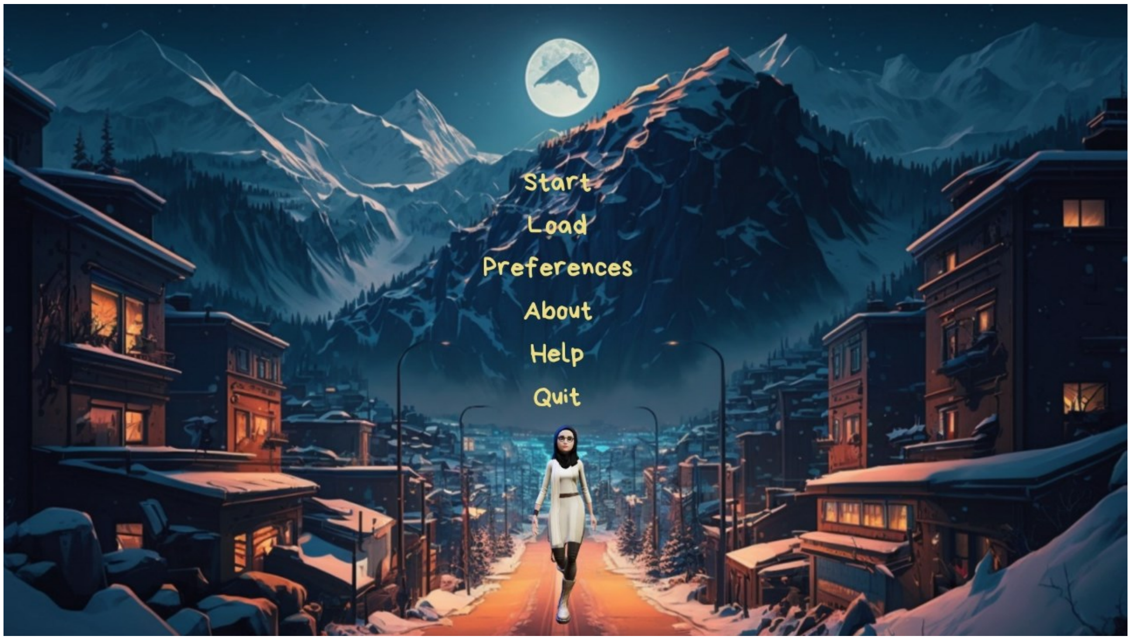


Figure 14: "Grown-Up Blues" Start Menu

challenges of a new home and a new university. The apparent goal is to help the character navigate through social interactions to successfully adapt to the new place. However, during each step, the player is actually taking security decisions that will determine the final outcome of the game.

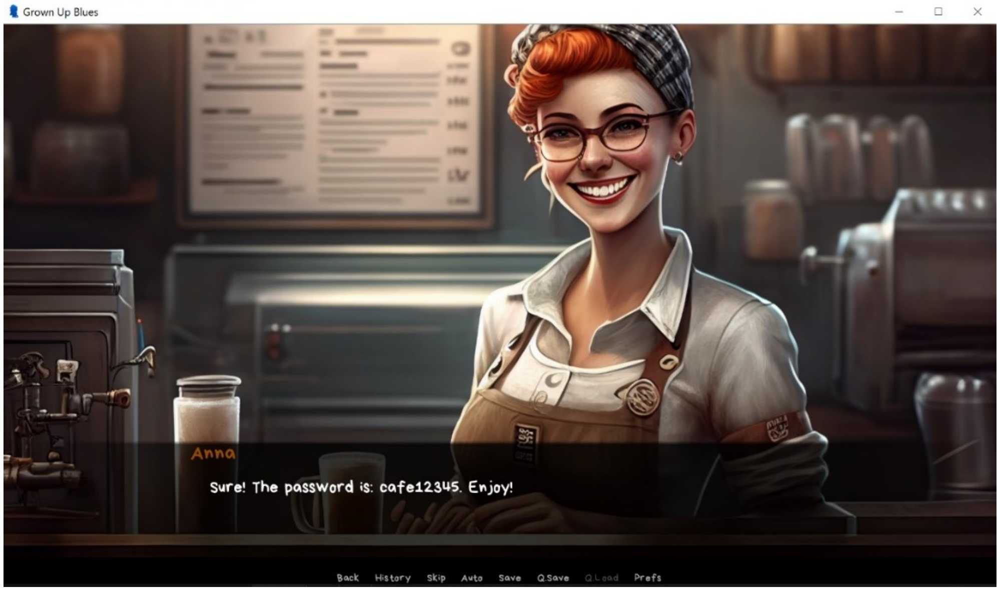
6.1.2. “Fake-out” Strategy

The game we propose doesn’t initially reveal its purpose. Similarly to an increasing long line of “fake-out” visual novel games, the real objective of the game becomes clear after the player is already deep in the game, or after the player has lost. This approach is similar to one of the most popular visual novels of the genre, Doki Doki Literature Club! (Barnabé, 2018). According to the reviewers, the game's ability to have a surprising impact on players is due to its resemblance to typical visual novel games (Barkman, 2021). We apply this “fake-out” to place players in a real-life environment, similar to when actual security incidents occur unexpectedly in our everyday lives. Our game, "Grown-Up Blues," does not give away its cybersecurity educational purpose upon first glance, allowing players to uncover its secrets as they play. This contributes to producing a shock factor, help leave a long-lasting effect on the player, and thus possibly increase the chances of knowledge retention.

6.1.3. Scenarios

These are some of scenarios that we propose in the game, and these are customizable by the developer.

- Unsecure Public Hotspot: The player unsuspectingly needs to connect to the WiFi in a café where they are studying, as shown in Figure 15. However, an intruder is listening on the network and steals sensitive information, i.e. the player’s bank account credentials.
- Fake Social Media Profile: The player receives a message from a fake social media profile that appears to be from a classmate or friend but is actually an imposter who wants to gain access to their personal information as shown in Figure 16.

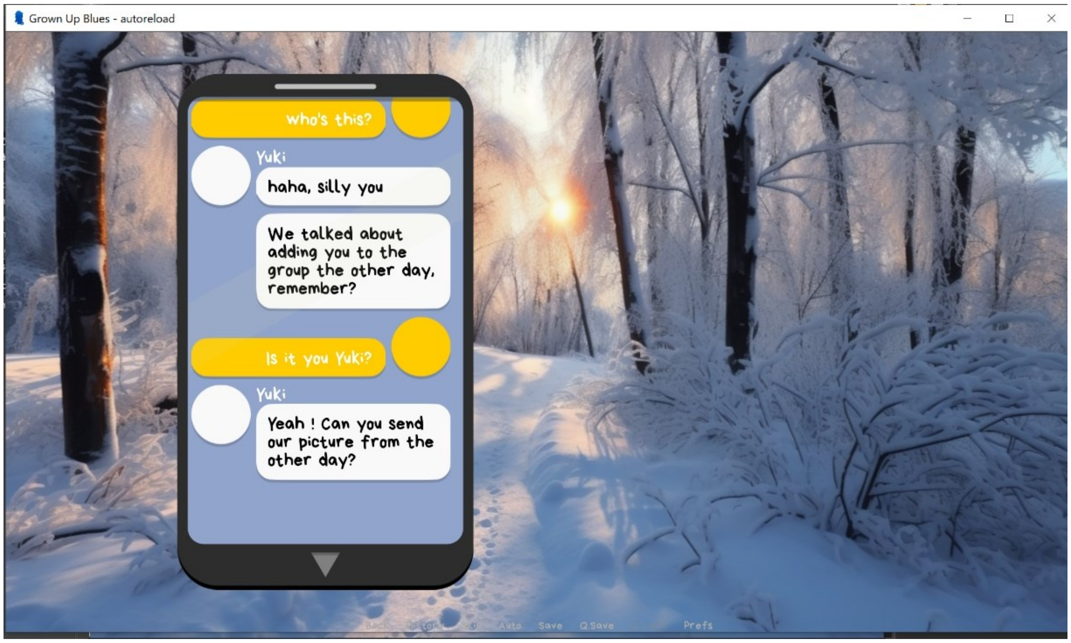


Anna

Sure! The password is: cafe12345. Enjoy!

Figure 15: Public Hotspot Scene Screenshot

- Online Dating Scam: The player meets someone on a dating app or website who claims to be interested in a relationship but is actually a scammer who wants to steal their identity.
- Clickbait Link: The player clicks on a sensational or misleading headline or image on a website or social media platform that leads to a phishing site.



who's this?

Yuki

haha, silly you

We talked about adding you to the group the other day, remember?

Is it you Yuki?

Yuki

Yeah ! Can you send our picture from the other day?

Figure 16: Yuki Message Scam

These cybersecurity hidden challenges reinforce the need for the player to understand that they need to protect themselves by increasing their knowledge of how other people might target them.

6.1.4. Dynamic Adaptation of Level:

The level of difficulty of a scene is increased in three different ways. In the case that the player is finding the game too easy – we know that by measuring the time that the player takes to make his/her choices - we increase the number of options that the user must choose from.

The second way of increasing the difficulty is by implementing timed choices. We give the players a limited time to make decisions, which will force them to make quick and decisive choices without the luxury of taking too much time to consider the consequences. Figure 17 shows the timer button implemented in the game. When the time runs out, the game makes a choice on its own, and the player is not aware of it.

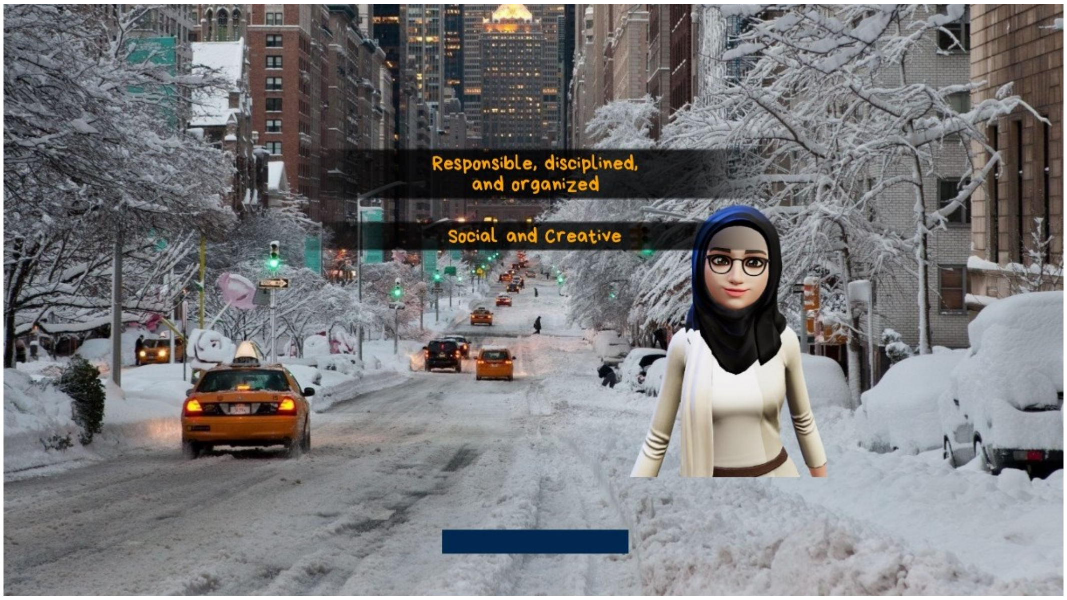
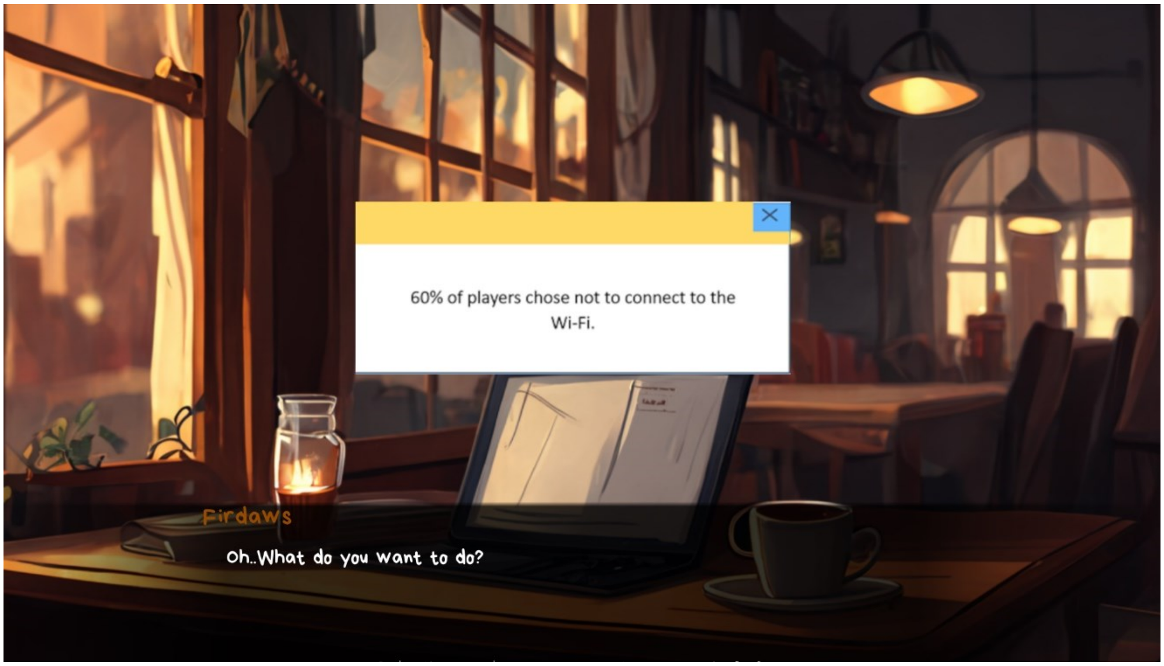


Figure 17: Timed Choice in "Grown-Up Blues"

The third way of increasing the difficulty is by implementing adaptive nudges. Adaptive nudges can be used to guide the player towards specific choices or behaviors based on their individual preferences or past decisions. In “Grown-Up Blues”, we use two different types of nudges: default nudges and social nudges. Will ask players to take a short test to determine if they have a social personality type.



60% of players chose not to connect to the Wi-Fi.

Firdaws

Oh..What do you want to do?

Figure 18: Social Nudge Implementation

Based on the results of this test and their performance in the game, we will use social nudges to influence their decisions and actions. If the players show signs of having a social personality and do not respond to peer pressure, the default nudge will be shown.

For players who are more likely to respond to social influence, we will guide them to use social nudges as shown in Figure 18. This personalized approach to nudging will help us provide a more tailored and effective gaming experience, while still allowing players to make their own choices and maintain control over their gameplay.

The fourth way of increasing the difficulty is by applying peer pressure through the implemented character. We can see in Figure 19 that this is implemented by letting the other character "Yuki", pressure the user into making incorrect security decisions. Peer pressure can often lead to incorrect security decisions, especially among young people who are more susceptible to the influence of their peers. In some cases, peers may encourage each other to take risks, such as

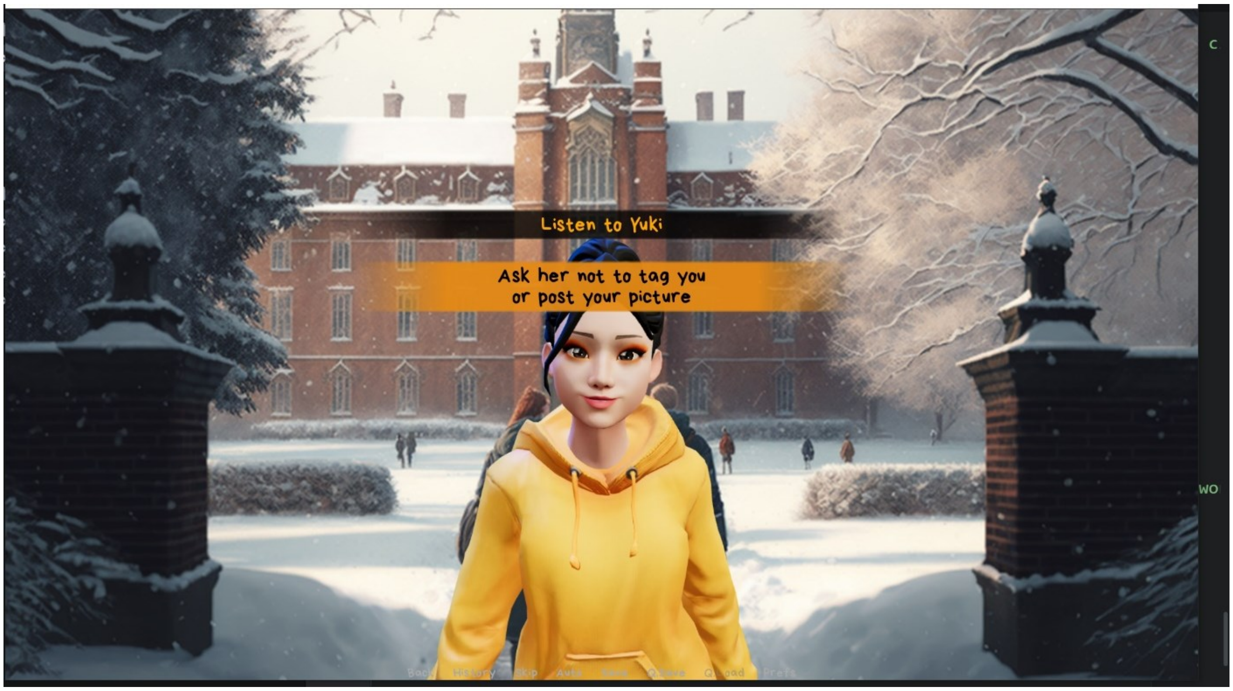

Listen to Yuki
Ask her not to tag you or post your picture
Back History Skip Auto Save Q.Save Q.Load Prefs

Figure 19: Yuki's Peer Pressure Nudge

sharing passwords, accessing unsecured Wi-Fi networks, or downloading unverified software, in the belief that such actions are harmless or cool.

These are some types of nudges that affect the game’s flow, by making it harder or easier while monitoring the user’s performance.

6.1.5 Feedback

During the gameplay, we also provide the player with feedback regarding his/her performance by updating the character characteristics.

For example, as we can see in Figure 20, once the player makes the choice to accept to help the character “Firdaws”, she becomes happy and her “happiness” feature is increased by 1. A small image accompanies the notification to incorporate different types of feedbacks (written and graphic).

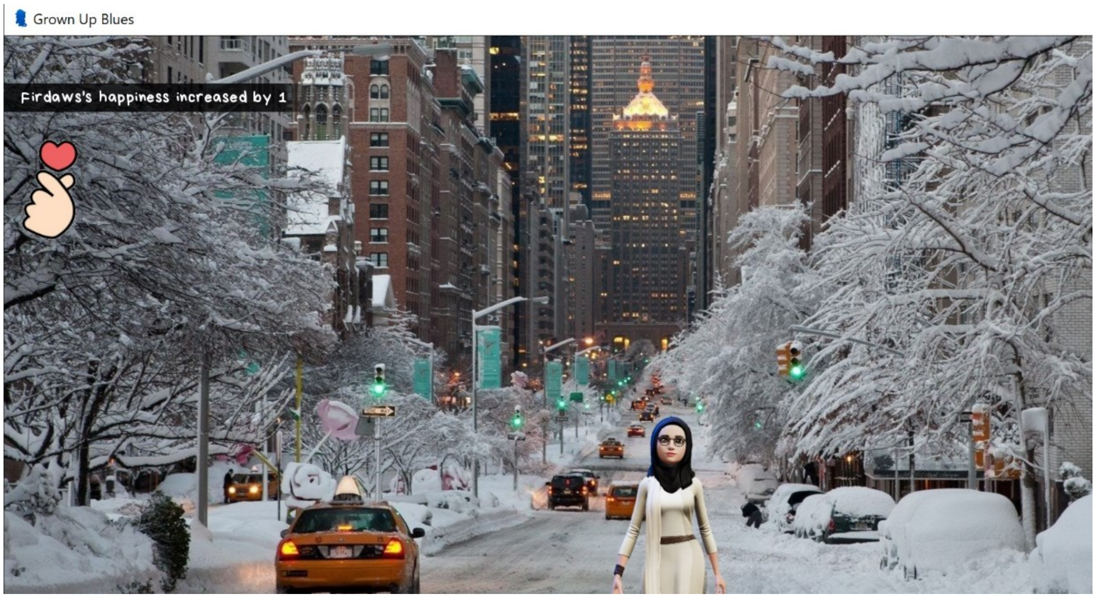


Figure 20: Happiness Feedback

The next section presents the software tools needed to implement parts of the game, as well as the interface. Since "Grown-Up Blues" is a dynamic web-based game, we used the following technologies:

6.2. Software Tools and Implementation

- Twine is an open-source tool for telling interactive, nonlinear stories. We used it to create the initial draft of the story and organize the elements of the story. This program enables us to organize the scenarios and endings in a tree format. It publishes directly to HTML and supports JavaScript and CSS. The software is depicted in Figure 21.

- We used Raptor, which is a graphical authoring tool to generate a flowchart-based programming environment, and it is designed specifically to help visualize algorithms and avoid syntactic baggage.

- Ren'Py is a software tool based on Python that is designed to develop interactive stories for desktop and mobile devices. Ren'Py's cross-platform compatibility ensures that interactive stories can run seamlessly on both desktop and mobile devices.

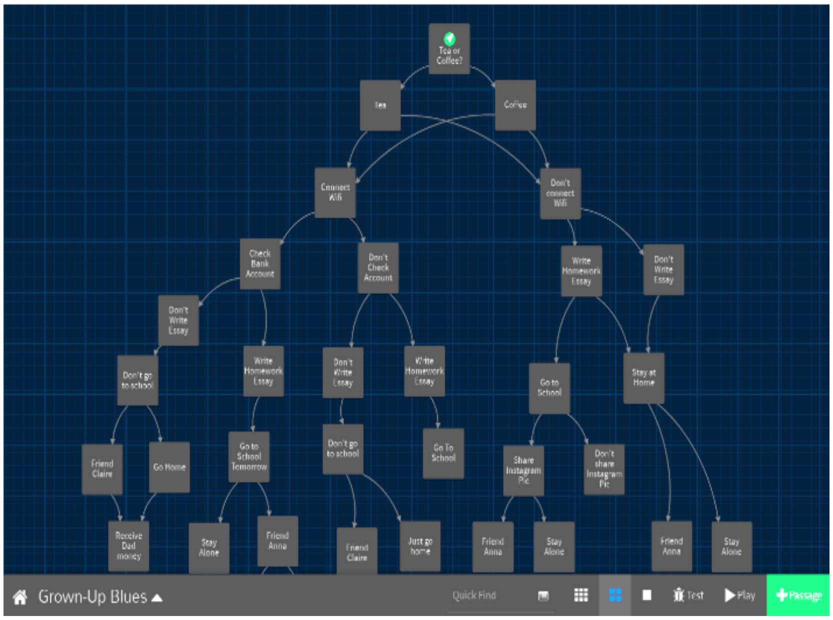


Figure 21: Scenario Tree

- Gimp is a free and open-source image editor that was used for designing graphics and images for the game scenes. It provides the tools needed for high quality image manipulation.

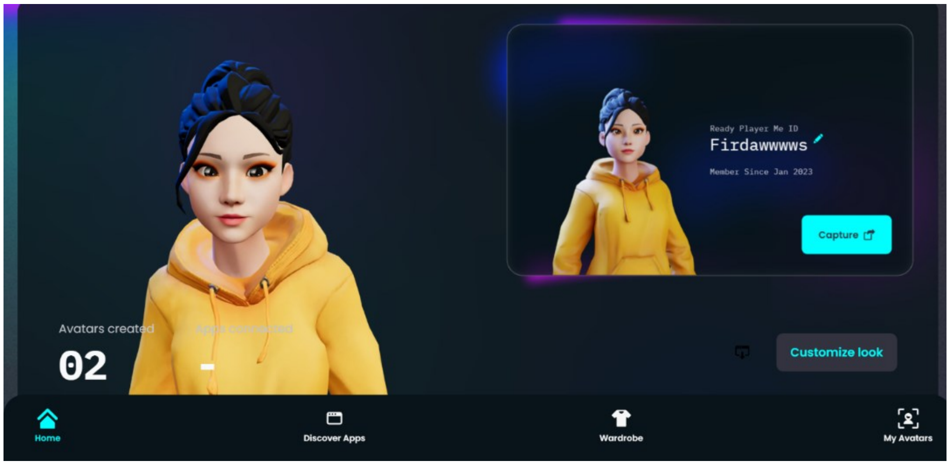
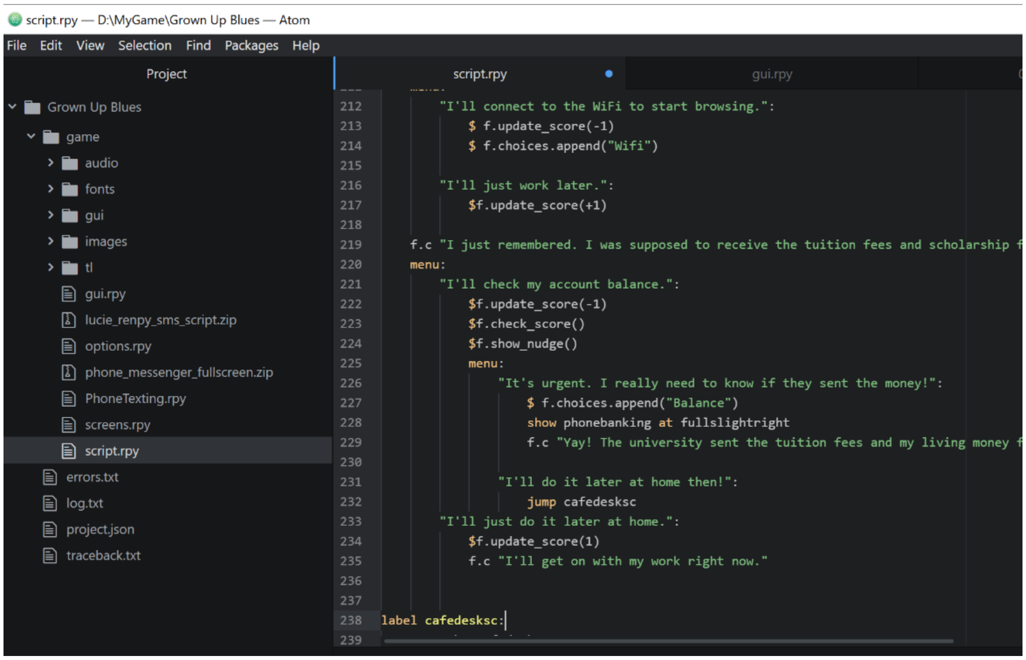


Figure 22: Ready Player Me Avatar Creation Platform

- To generate the characters, we used Ready Player Me, which is a cross-game avatar platform for Unity, Unreal Engine, and all web-based stacks, as shown in Figure 22.



```
        "I'll connect to the WiFi to start browsing.":
            $ f.update_score(-1)
            $ f.choices.append("Wifi")

        "I'll just work later.":
            $f.update_score(+1)

    f.c "I just remembered. I was supposed to receive the tuition fees and scholarship f
    menu:
        "I'll check my account balance.":
            $f.update_score(-1)
            $f.check_score()
            $f.show_nudge()
            menu:
                "It's urgent. I really need to know if they sent the money!":
                    $ f.choices.append("Balance")
                    show phonebanking at fullslightright
                    f.c "Yay! The university sent the tuition fees and my living money f

                "I'll do it later at home then!":
                    jump cafedesksc
        "I'll just do it later at home.":
            $f.update_score(1)
            f.c "I'll get on with my work right now."


label cafedesksc:
```

Figure 23: Python Code Screenshot

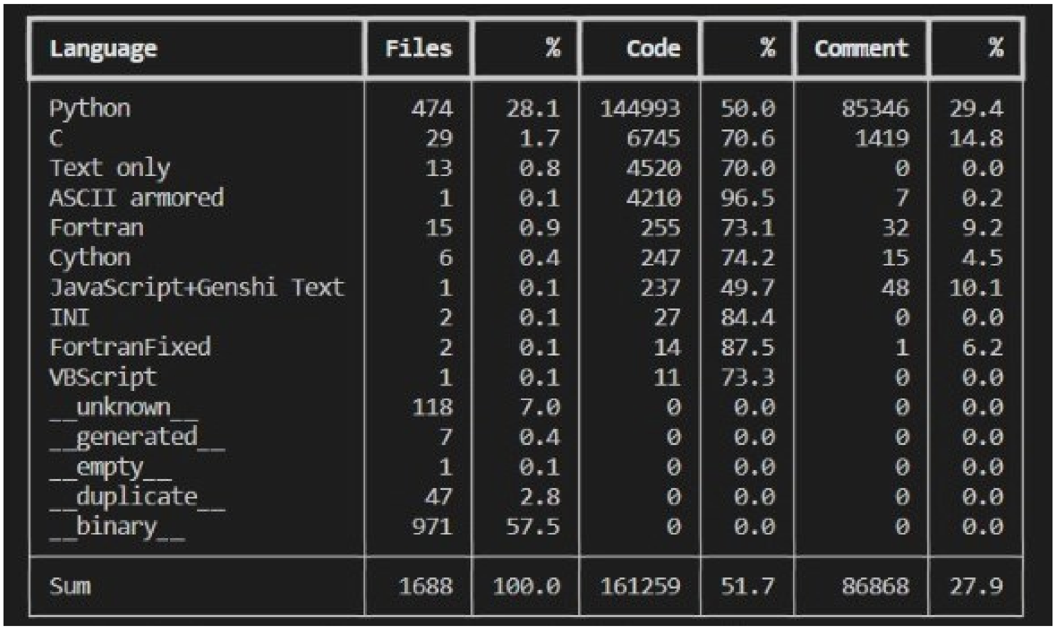
- Python was employed in the development of the player, scene, and game classes, as well as in the coding of the game itself (Figure 23).

- We created the graphics using a blended approach that mixes the following parts:
    - Artificial Intelligence generated basic backgrounds using the Photoleap AI Image Generator Midjourney (Figure 25)
    - Manually edited images using GIMP, Word, and PowerPoint.
    - Manually edited characters using Ready Player Me, which is a cross-game avatar platform for Unity, Unreal Engine, and all web-based stacks.

The way these three components are put together depends on the scene. However, we used tools like GIMP to embed the manually generated parts into the AI-generated ones.

Figure 25: Midjourney Image Generation Tool

The core of the game is implemented. We mean by this that we have written the code needed to implement one scenario. The number of scenarios being theoretically infinite, the same classes and methods used in the first scenarios can be used to extend the game. The game is available on Github[4]. We used the Python pygount utility[5] to determine the software code count, and the results are summarized in the following table:



Language	Files	%	Code	%	Comment	%
Python	474	28.1	144993	50.0	85346	29.4
C	29	1.7	6745	70.6	1419	14.8
Text only	13	0.8	4520	70.0	0	0.0
ASCII armored	1	0.1	4210	96.5	7	0.2
Fortran	15	0.9	255	73.1	32	9.2
Cython	6	0.4	247	74.2	15	4.5
JavaScript+Genshi Text	1	0.1	237	49.7	48	10.1
INI	2	0.1	27	84.4	0	0.0
FortranFixed	2	0.1	14	87.5	1	6.2
VBScript	1	0.1	11	73.3	0	0.0
__unknown__	118	7.0	0	0.0	0	0.0
__generated__	7	0.4	0	0.0	0	0.0
__empty__	1	0.1	0	0.0	0	0.0
__duplicate__	47	2.8	0	0.0	0	0.0
__binary__	971	57.5	0	0.0	0	0.0
Sum	1688	100.0	161259	51.7	86868	27.9

Figure 24: Lines of Code of the Game

[4] https://github.com/PotatoHijabi/GrownUpBlues

[5] https://pypi.org/project/pygount/

As for the installation, it is easy as the Ren'py platform provides different ways of installing the game on different operating systems, Windows, Linux, Mac, Android, and iOS. In the next subsection, we present an experimental evaluation of our educational game by comparing it with two other games previously assessed.

6.3. Experimental Evaluation

In this study, we compared our educational game with two other games that are currently used to achieve the same objectives. HotSpot and AggieLife are games we evaluated earlier in the research, and we use them as baseline to test the performance of our game. We evaluated the three games based on eleven criteria, including enjoyment, learning, engagement, easiness, feedback, motivation, adaptivity, and usability. From the criteria mentioned in Chapter 4, we measured enjoyment criteria, like the engagement of the users, the flow and difficulty of the game, as well as serious criteria, like whether the game was understandable and if the users learnt from it.

Table 25: Games Evaluation Quiz

	Games Assessment	Grown-Up Blues	HotSpot	Aggie Life
1	How much did you enjoy playing the game?	7.52	6.16	7.48
2	How much did you learn while playing the game?	6.72	6.56	7.16
3	Was the game engaging?	7.36	6.60	7.32
4	Was the game easy to understand and use?	7.64	6.12	7.16
5	Did the game provide you with feedback on your performance?	7.44	6.80	6.16
6	Was the game challenging enough to keep you motivated?	7.72	7.40	7.16
7	Did the game meet your expectations?	6.92	6.36	6.32
8	Did the game help you achieve the best outcome?	7.36	5.68	5.76
9	How much would you recommend this game to others?	6.96	6.48	7.16
10	Do you think you would play this game again in the future?	6.72	6.20	6.88
11	How much did you expect this game to be cybersecurity-oriented?	5.16	6.28	5.96
	Total Average	**7.05**	**6.42**	**6.77**

The following table (Table 25) and chart (Figure 26) show the results obtained after surveying 25 people of different ages and backgrounds who tried the three games. We contacted a total of 40 people between the ages of 20 to 28 utilizing video conferencing platforms such as Zoom. We received a response of 25 people who played the 3 games and sent us their assessments of the three games which they rated out of 10 based on the criteria in Table 25. We compiled the average score of their results.

The results showed that our game outperformed the two others in many of the criteria and users agree that our game helps the player achieve the best outcome. In our analysis, we can say that the use of nudges may have played a role in achieving that outcome. Otherwise, the game scored comparably in a few other criteria like engagement and challenge.

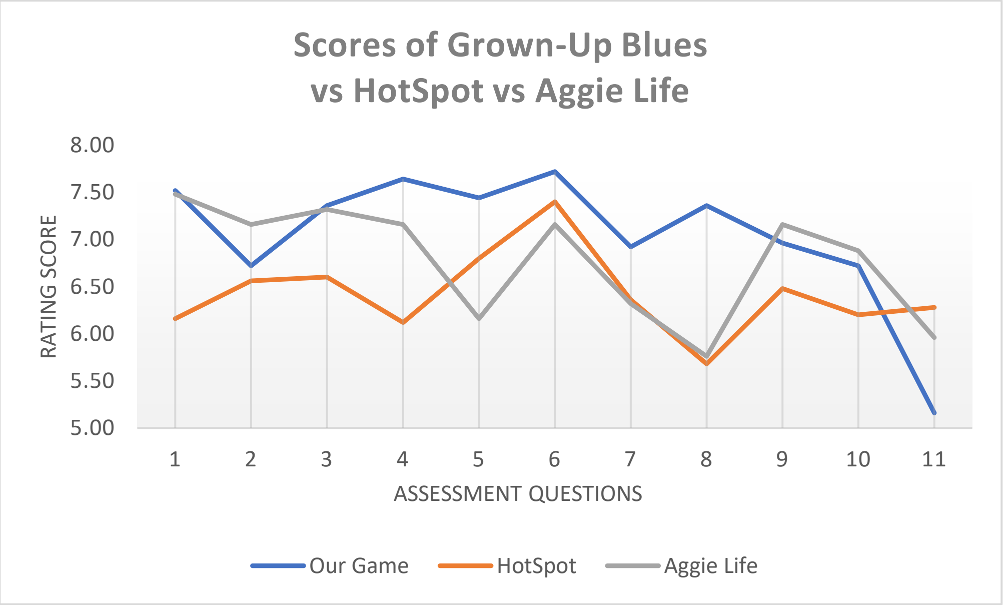


Figure 26: Comparative Scores of our Game (Grown-Up Blues)

These findings highlight the potential of our EVNAG-based game to enhance the learning experience through gaming and support the development of future educational games with similar design principles. In the next section, we will synthesize our contributions and findings.

Chapter 7 – Conclusion and Future Work

In conclusion, the main objective of this work was to investigate and provide a perspective through which future research can contribute to educational games' development in general, and cybersecurity educational games specifically.

We answered the first research question by surveying more than 350 Internet users and concluded the following: the need for better cybersecurity educational content is present and the diversity of tools used to teach cybersecurity is an important factor to consider. Indeed, the survey completed through Mechanical Turk gauged the level of awareness of internet users by asking them questions about their online behavior and challenging them with different phishing scenarios which they had to classify as suspicious or legitimate. Among relatively educated participants, knowledge of multiple key concepts of cybersecurity and privacy was lacking. Moreover, a noticeable difference exists between the correctness of the answers given by Europeans versus Americans. This gives an insight into the way that security and privacy are perceived in both locations. Given the fact that security regulations (i.e. GDPR) are different from place to place, this further highlights the need for serious cybersecurity games as a knowledge equalizer.

Backed up by extensive research on the matter, this has led us to consider educational games as an effective medium of raising awareness. Educational games have demonstrated their effectiveness as teaching and learning tools, particularly in vulgarizing topics requiring in-depth knowledge to master. However, challenges are associated with assessing the quality of serious games, as multiple aspects of game enjoyment are subjective and intangible.

To improve the design of cybersecurity serious games, the second goal of this work is to assess the essential characteristics of current cybersecurity serious games. This objective is fulfilled by analyzing 45 serious games based on Caserman's evaluation guide, which has the particularity of considering both the serious and enjoyment components of educational games. Given that the criteria needed refining to be reusable as an assessment method, we built a scale that allowed us to break down every criterion into its characteristics. The assessment revealed that the two criteria least satisfied in the serious part were the *in-game rewards feature* and the *performance feedback* feature. Then, the two criteria least satisfied by the game part were found to be the *social interaction* criterion and the *flow criterion (dynamic adaptation of the game level)* criterion. By identifying the gaps in educational games' design, what emerges from this analysis is that new cybersecurity games should capitalize on the current absence of these criteria from the current games and create games that take the user on a path where the information encountered becomes knowledge acquired. Between the serious part and the enjoyment part, we found the enjoyment part more lacking, which indicates as well that cybersecurity educational games should focus on how to make the game enjoyable, as well as instructional.

The lacking criteria gave us the key requirements and features needed to design an adaptable framework for a high-quality educational cybersecurity game: EVNAG. We proposed an architecture for an adaptive serious game, that was divided into different modules: the user interface, the dynamic user model, the story engine, the game engine, and the learning style module. We also proposed an algorithm that tackles DDA by breaking up a visual novel into stages or scenes, and then nudging the players towards a certain outcome. To ensure the presence of flow in the game, the nudges can either be beneficial to the players by giving them hints when their performance drops, or malicious by using peer pressure or/and timed choices to make it harder to achieve a satisfactory game ending. Inspired by this architecture, we partially implemented the cybersecurity visual novel “Grown-Up Blues”. The VN was tested against two other previously assessed cybersecurity games and got higher scores in the enjoyment of the game, while the other criteria scored similarly.

For future work, there are several potential areas for improvement in this thesis. First, we considered all Caserman’s quality criteria to be of equal weight. While that made the assessment easier, some of the criteria are not independent and future work should focus on determining the correlations and interactions between the different criteria. Also, assuring a comprehensive evaluation would be improved by the incorporation of human-based assessments. Although human-based assessments can be time-consuming, subjective, and may have limitations in terms of consistency and scalability, they can provide valuable insights into the learner's engagement and identify specific areas for improvement.

Moreover, the proposed framework could be tested by building a higher scale game that incorporates more complexity. That encompasses allowing for more endings, adding avatar personalization, and increasing the number of choices the players can make to enhance their experience. It would be productive as well to include other types of gameplays to incorporate and interest other types of players that could be less interested in narrative-based gameplay. Another interesting future work possibility is the assembling of a database of players that would record the player types, ages, genders, gameplay preferences, and computer literacy. That could prove a very interesting resource for game developers.

Finally, this thesis contributes to the growing body of research on educational games in cybersecurity and provides insights for designing effective educational games that enhance cybersecurity education.

Annexes

Table 26: Games Assessment - Serious Part

Game Number	Focus on Goal	Clear Goal	Indispensable Goal	Content Correctness	Appropriate Feedback	Appropriate Rewards
1	3	2	3	3	2	2
2	2	2	2	3	2	1
3	2	2	3	3	2	2
4	1	2	2	3	2	2
5	3	1	3	3	1	1
6	3	2	2	3	1	1
7	2	2	3	3	3	2
8	3	3	2	3	3	1
9	3	3	2	3	2	2
10	3	3	3	3	2	1
11	2	2	1	3	1	1
12	2	1	2	3	2	2
13	2	1	2	3	2	2
14	3	2	3	3	2	1
15	2	2	1	3	3	2
16	3	3	2	3	2	2
17	2	2	3	3	2	3
18	2	2	3	3	3	2
19	3	2	2	3	1	1
20	2	3	3	3	3	2
21	3	2	3	3	1	0
22	3	3	3	3	3	2
23	2	3	1	3	2	1
24	1	2	3	3	3	1
25	2	2	2	3	0	1
26	1	2	1	3	2	1
27	3	3	2	3	2	2
28	3	2	3	2	1	1
29	1	3	3	3	1	1
30	3	3	3	3	3	1
31	3	2	3	2	2	2
32	2	2	3	3	2	2

Game Number	Focus on Goal	Clear Goal	Indispensable Goal	Content Correctness	Appropriate Feedback	Appropriate Rewards
33	3	2	3	3	2	2
34	3	3	3	3	3	1
35	2	1	2	3	3	2
36	3	3	3	3	2	2
37	1	0	1	3	1	3
38	3	3	3	3	2	1
39	3	3	3	3	3	2
40	3	3	3	3	3	2
41	3	2	2	3	2	2
42	1	3	2	3	2	3
43	1	1	0	3	2	3
44	1	2	1	3	2	2
45	1	2	0	3	3	2

Games Assessment - Serious Part (Continuation)

The following table (**Table 27**) unveils the way that the enjoyment characteristics were rated and analyzed.

Table 27: Games Assessment - Enjoyment Part

Game Number	Ensure Player Engagement Experience	Ensure Flow	Establish Emotional Connection	Sense of Control	Support Social Interactions	Ensure Immersive Experience	Attractive Graphics	Appropriate Sound
1	2	2	1	2	0	1	2	0
2	1	1	1	1	0	1	1	0
3	1	1	1	1	1	1	2	0
4	1	1	1	1	0	2	3	0
5	1	0	1	0	1	0	2	0
6	1	1	1	1	0	1	2	0
7	2	1	3	2	0	3	3	2
8	2	1	2	2	0	3	3	2
9	1	0	0	1	0	1	1	2
10	2	1	1	2	0	3	2	2
11	3	1	1	1	0	2	3	2
12	2	1	1	2	0	2	3	2
13	3	1	2	2	0	1	2	1
14	2	1	1	2	0	2	2	2
15	3	1	1	2	1	3	3	3
16	1	1	1	1	0	1	3	0
17	3	2	3	1	1	3	3	2
18	2	1	3	2	0	3	3	2
19	2	1	2	2	0	2	3	2
20	3	2	3	2	0	3	3	2
21	1	1	1	1	3	1	1	0
22	2	2	2	2	0	2	3	0
23	1	0	1	1	0	1	1	1
24	3	2	3	1	2	2	3	2
25	1	0	1	1	0	2	1	1
26	1	1	3	1	1	3	3	0
27	1	0	1	1	0	2	2	2
28	1	2	1	1	0	1	1	0
29	2	1	3	2	1	3	3	0
30	1	1	2	1	1	1	2	0

Game Number	Ensure Player Engagement Experience	Ensure Flow	Establish Emotional Connection	Sense of Control	Support Social Interactions	Ensure Immersive Experience	Attractive Graphics	Appropriate Sound
31	1	1	2	1	0	2	3	1
32	2	2	1	1	0	1	2	0
33	2	3	2	2	1	2	3	1
34	2	1	2	2	1	2	2	2
35	2	1	3	2	0	3	3	3
36	3	2	2	2	0	1	1	0
37	1	1	1	2	0	2	2	1
38	2	1	2	2	0	3	3	2
39	2	2	1	1	1	2	3	2
40	1	1	1	2	1	2	3	0
41	1	1	1	2	0	1	1	2
42	3	1	2	2	0	2	3	2
43	2	1	2	2	2	2	2	2
44	2	2	2	2	0	2	3	2
45	3	2	3	2	1	3	3	2

Games Assessment - Enjoyment Part (Continuation)

References

2020 User Risk Report: Exploring Vulnerability and Behavior in a People-Centric Threat Landscape. (2020). *ANNUAL REPORT*, 14.

Aïmeur, E., & Schőnfeld, D. (2011). The ultimate invasion of privacy: Identity theft. *2011 Ninth Annual International Conference on Privacy, Security and Trust*, 24–31. https://doi.org/10.1109/PST.2011.5971959

Almeida, F. (2017). *Learning Entrepreneurship with Serious Games—A Classroom Approach* (arXiv:1710.04118). arXiv. https://doi.org/10.48550/arXiv.1710.04118

Barkman, C. (2021). 'There's no point in saving anymore': Diegesis and Interactional Metalepsis in Pony Island and Doki Doki Literature Club. *Journal of Games Criticism*, *5*(1), 1–22.

Barnabé, F. (2018). The Playful Function of Paratext in Visual Novels: The Case of Doki Doki Literature Club! *Mechademia Kyoto Conference 2018:" Manga Nexus: Movement, Stillness, Media*".

Bartle, R. (1996). Hearts, clubs, diamonds, spades: Players who suit MUDs. *Journal of MUD Research*, *1*(1), 19.

Blunt, R. (2009). Do Serious Games Work? Results from Three Studies. *ELearn*, *2009*(12), 1. https://doi.org/10.1145/1661377.1661378

Bond, M., & Beale, R. (2009, September 1). *What makes a good game? Using reviews to inform design*. People and Computers XXIII Celebrating People and Technology. https://doi.org/10.14236/ewic/HCI2009.52

Brom, C., Buchtová, M., Šisler, V., Děchtěrenko, F., Palme, R., & Glenk, L. M. (2014). Flow, social interaction anxiety and salivary cortisol responses in serious games: A quasi-experimental study. *Computers & Education*, *79*, 69–100. https://doi.org/10.1016/j.compedu.2014.07.001

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, *75*, 24–35. https://doi.org/10.1016/j.cose.2018.01.015

Cai, Y. (2018). Using Case Studies To Teach Cybersecurity Courses. *Journal of Cybersecurity Education, Research and Practice*, *2018*(2). https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss2/3

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Cain, J., & Piascik, P. (2015). Are Serious Games a Good Strategy for Pharmacy Education? *American Journal of Pharmaceutical Education*, *79*(4). https://doi.org/10.5688/ajpe79447

Calderón, A., & Ruiz, M. (2015). A systematic literature review on serious games evaluation: An application to software project management. *Computers & Education*, *87*, 396–422. https://doi.org/10.1016/j.compedu.2015.07.011

Cappa, F., Rosso, F., Giustiniano, L., & Porfiri, M. (2020). Nudging and citizen science: The effectiveness of feedback in energy-demand management. *Journal of Environmental Management*, *269*, 110759. https://doi.org/10.1016/j.jenvman.2020.110759

Caserman, P., Hoffmann, K., Müller, P., Schaub, M., Straßburg, K., Wiemeyer, J., Bruder, R., & Göbel, S. (2020). Quality Criteria for Serious Games: Serious Part, Game Part, and Balance. *JMIR Serious Games*, *8*(3), e19037. https://doi.org/10.2196/19037

Chan, E., & Vorderer, P. (2006). Massively multiplayer online games. *Playing Video Games: Motives, Responses, and Consequences*, 77–88.

Chandler, J., Rosenzweig, C., Moss, A. J., Robinson, J., & Litman, L. (2019). Online panels in social science research: Expanding sampling methods beyond Mechanical Turk. *Behavior Research Methods*, *51*(5), 2022–2038. https://doi.org/10.3758/s13428-019-01273-7

Chen, H., Maynard, S. B., & Ahmad, A. (2013). A Comparison of Information Security Curricula in China and the USA. *Australian Information Security Management Conference*, 15.

Clark, D. B., Tanner-Smith, E. E., & Killingsworth, S. S. (2016). Digital Games, Design, and Learning: A Systematic Review and Meta-Analysis. *Review of Educational Research*, *86*(1), 79–122. https://doi.org/10.3102/0034654315582065

Clark, R. C., & Mayer, R. E. (2016). *e-Learning and the Science of Instruction: Proven Guidelines for Consumers and Designers of Multimedia Learning*. John Wiley & Sons.

Csikszentmihalyi, M., & Csikzentmihaly, M. (1990). *Flow: The psychology of optimal experience* (Vol. 1990). Harper & Row New York.

Cummings, J. J., & Bailenson, J. N. (2016). How immersive is enough? A meta-analysis of the effect of immersive technology on user presence. *Media Psychology*, *19*(2), 272–309.

Desurvire, H., & Wiberg, C. (2009). Game Usability Heuristics (PLAY) for Evaluating and Designing Better Games: The Next Iteration. In A. A. Ozok & P. Zaphiris (Eds.), *Online Communities and Social Computing* (pp. 557–566). Springer. https://doi.org/10.1007/978-3-642-02774-1_60

Differences Between EU and US Data Protection. (n.d.). Arkansas State University Online. Retrieved June 20, 2022, from https://degree.astate.edu/articles/media-management/eu-and-us-data-protection.aspx

Dillon, R. (2010). *On the Way to Fun: An Emotion-Based Approach to Successful Game Design*. CRC Press.

Emmerich, K., & Bockholt, M. (2016). Serious Games Evaluation: Processes, Models, and Concepts. In R. Dörner, S. Göbel, M. Kickmeier-Rust, M. Masuch, & K. Zweig (Eds.), *Entertainment Computing and Serious Games: International GI-Dagstuhl Seminar 15283, Dagstuhl Castle, Germany, July 5-10, 2015, Revised Selected Papers* (pp. 265–283). Springer International Publishing. https://doi.org/10.1007/978-3-319-46152-6_11

Furuichi, M., & Aibara, M. (2019). A Challenge of Developing Serious Games to Raise the Awareness of Cybersecurity Issues. *Digital Games Research Association Conference*. Digital Games Research Association Conference.

Garcia, M. B. (2020). Kinder learns: An educational visual novel game as knowledge enhancement tool for early childhood education. *The International Journal of Technologies in Learning*.

Gaurav, D., Kaushik, Y., Supraja, S., Yadav, M., Gupta, M. P., & Chaturvedi, M. (2023). Adaptive Serious Games to Teach Cybersecurity Concepts Using a Machine Learning Approach. In A. Kumar, G. Ghinea, S. Merugu, & T. Hashimoto (Eds.), *Proceedings of the International Conference on Cognitive and Intelligent Computing* (pp. 373–384). Springer Nature. https://doi.org/10.1007/978-981-19-2358-6_35

Geri, N., Winer, A., & Zaks, B. (2017). A Learning Analytics Approach for Evaluating the Impact of Interactivity in Online Video Lectures on the Attention Span of Students. *Interdisciplinary Journal of E-Learning and Learning Objects*, *13*(1), 215–228.

Giessen, H. W. (2015). Serious Games Effects: An Overview. *Procedia - Social and Behavioral Sciences*, *174*, 2240–2244. https://doi.org/10.1016/j.sbspro.2015.01.881

Graesser, A. C. (2017). Reflections on Serious Games. In P. Wouters & H. van Oostendorp (Eds.), *Instructional Techniques to Facilitate Learning and Motivation of Serious Games* (pp. 199–212). Springer International Publishing. https://doi.org/10.1007/978-3-319-39298-1_11

Hadlington, L. (2021). *The "Human Factor" in Cybersecurity: Exploring the Accidental Insider* [Chapter]. Research Anthology on Artificial Intelligence Applications in Security; IGI Global. https://doi.org/10.4018/978-1-7998-7705-9.ch087

Jackson, L. C., O'Mara, J., Moss, J., & Jackson, A. C. (2018). A Critical Review of the Effectiveness of Narrative-Driven Digital Educational Games. *International Journal of Game-Based Learning (IJGBL)*, *8*(4), 32–49.

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Game based Cybersecurity Training for High School Students. *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 68–73. https://doi.org/10.1145/3159450.3159591

Johnson, C. I., Bailey, S. K. T., & Van Buskirk, W. L. (2017). Designing Effective Feedback Messages in Serious Games and Simulations: A Research Review. In P. Wouters & H. van Oostendorp (Eds.), *Instructional Techniques to Facilitate Learning and Motivation of Serious Games* (pp. 119–140). Springer International Publishing. https://doi.org/10.1007/978-3-319-39298-1_7

Johnson, D., Klarkowski, M., Vella, K., Phillips, C., McEwan, M., & Watling, C. N. (2018). Greater rewards in videogames lead to more presence, enjoyment and effort. *Computers in Human Behavior*, *87*, 66–74. https://doi.org/10.1016/j.chb.2018.05.025

Kiili, K. (2005). Digital game-based learning: Towards an experiential gaming model. *The Internet and Higher Education*, *8*(1), 13–24. https://doi.org/10.1016/j.iheduc.2004.12.001

Koster, R. (2013). *Theory of fun for game design*. O'Reilly Media, Inc.

KS Khan, Gerben ter Riet, Julie Glanville, AJ sowden, & Jos Kleijnen. (2001). *Undertaking systematic reviews of research on effectiveness: CRD's guidance for carrying out or commissioning reviews* (4 (2n; Issue 4 (2n). NHS Centre for Reviews and Dissemination. http://www.york.ac.uk/inst/crd/crdreports.htm

Landers, R. N., & Callan, R. C. (2011). Casual Social Games as Serious Games: The Psychology of Gamification in Undergraduate Education and Employee Training. In M. Ma, A. Oikonomou, & L. C. Jain (Eds.), *Serious Games and Edutainment Applications* (pp. 399–423). Springer. https://doi.org/10.1007/978-1-4471-2161-9_20

Lopes, R., & Bidarra, R. (2011). Adaptivity Challenges in Games and Simulations: A Survey. *IEEE Transactions on Computational Intelligence and AI in Games*, *3*(2), 85–99. https://doi.org/10.1109/TCIAIG.2011.2152841

Malouf, D. B. (1988). THE EFFECT OF INSTRUCTIONAL COMPUTER GAMES ON CONTINUING STUDENT MOTIVATION. *The Journal of Special Education*, *21*(4), 27–38. https://doi.org/10.1177/002246698802100406

Manzano-León, A., Camacho-Lazarraga, P., Guerrero, M. A., Guerrero-Puerta, L., Aguilar-Parra, J. M., Trigueros, R., & Alias, A. (2021). Between Level Up and Game Over: A Systematic Literature Review of Gamification in Education. *Sustainability*, *13*(4), Article 4. https://doi.org/10.3390/su13042247

Mark A. Harris & Karen P. Patten. (2015). Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity. *Journal of Information Systems Education*, *26*(3), 219–234.

Marker, A. M., & Staiano, A. E. (2015). Better Together: Outcomes of Cooperation Versus Competition in Social Exergaming. *Games for Health Journal*, *4*(1), 25–30. https://doi.org/10.1089/g4h.2014.0066

Marwick, A., & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*, *22*(12), 1697–1713. https://doi.org/10.1080/1369118X.2018.1450432

McCallum, S. (2012). Gamification and serious games for personalized health. *PHealth*, 85–96.

Meyers, E. A., Walker, A. C., Fugelsang, J. A., & Koehler, D. J. (2020). Reducing the number of non-naïve participants in Mechanical Turk samples. *Methods in Psychology*, *3*, 100032. https://doi.org/10.1016/j.metip.2020.100032

Mills, S. (2022). Personalized nudging. *Behavioural Public Policy*, *6*(1), 150–159. https://doi.org/10.1017/bpp.2020.7

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Mitrovic, A., Gordon, M., Piotrkowicz, A., & Dimitrova, V. (2019). Investigating the Effect of Adding Nudges to Increase Engagement in Active Video Watching. In S. Isotani, E. Millán, A. Ogan, P. Hastings, B. McLaren, & R. Luckin (Eds.), *Artificial Intelligence in Education* (pp. 320–332). Springer International Publishing. https://doi.org/10.1007/978-3-030-23204-7_27

Mittal, A., Gupta, M. P., Chaturvedi, M., Chansarkar, S. R., & Gupta, S. (2021). Cybersecurity Enhancement through Blockchain Training (CEBT) – A serious game approach. *International Journal of Information Management Data Insights*, *1*(1), 100001. https://doi.org/10.1016/j.jjimei.2020.100001

Mittal, S. (2016). *Understanding the Human Dimension of Cyber Security* (SSRN Scholarly Paper No. 2975924). Social Science Research Network. https://papers.ssrn.com/abstract=2975924

Murray, J. H. (2017). *Hamlet on the Holodeck: The Future of Narrative in Cyberspace*. MIT Press.

Naul, E., & Liu, M. (2020). Why story matters: A review of narrative in serious games. *Journal of Educational Computing Research*, *58*(3), 687–707.

Nicholson, S. (2015). A recipe for meaningful gamification. In *Gamification in education and business* (pp. 1–20). Springer.

Nkhoma, M., Calbeto, J., Sriratanaviriyakul, N., Muang, T., Ha Tran, Q., & Kim Cao, T. (2014). Towards an understanding of real-time continuous feedback from simulation games. *Interactive Technology and Smart Education*, *11*(1), 45–62. https://doi.org/10.1108/ITSE-03-2013-0005

Pavelů, L. (2021). *Adaptive cybersecurity games* [Masarykova univerzita, Fakulta informatiky]. https://theses.cz/id/f7u3y9/

Plass, J. L., Mayer, R. E., & Homer, B. D. (2020). *Handbook of Game-Based Learning*. MIT Press.

Prensky, M. (2009). H. Sapiens Digital: From Digital Immigrants and Digital Natives to Digital Wisdom. *Innovate: Journal of Online Education*, *5*(3). https://www.learntechlib.org/p/104264/

Ravyse, W. S., Seugnet Blignaut, A., Leendertz, V., & Woolner, A. (2017). Success factors for serious games to enhance learning: A systematic review. *Virtual Reality*, *21*(1), 31–58. https://doi.org/10.1007/s10055-016-0298-4

Roepke, R., & Schroeder, U. (2019). The Problem with Teaching Defence against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education. *Conference on Computer Supported Education*, 58–66.

Ross, P. T., & Bibler Zaidi, N. L. (2019). Limited by our limitations. *Perspectives on Medical Education*, *8*(4), 261–264. https://doi.org/10.1007/s40037-019-00530-x

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *59*(2), 12–15.

Ryan, R. M., Rigby, C. S., & Przybylski, A. (2006). The motivational pull of video games: A self-determination theory approach. *Motivation and Emotion*, *30*(4), 344–360.

Sanchez, E., van Oostendorp, H., Fijnheer, J. D., & Lavoué, E. (2020). Gamification. In *Encyclopedia of Education and Information Technologies* (pp. 816–827). Springer.

Sanders, T. A., & Cairns, P. (2010). *Time perception, immersion and music in videogames*.

Semet, Y., Marcon, B., Demestichas, K., Koutsouris, N., & Ascolese, A. (2019). *Artificial Ant Colonies for Adaptive Rewards in Serious Games*. 533–540. https://doi.org/10.1162/isal_a_00217

Solove, D. J. (2007). I've Got Nothing to Hide and Other Misunderstandings of Privacy 2007 Editor's Symposium. *San Diego Law Review*, *44*(4), Article 4.

Squire, K., & Steinkuehler, C. (2014). Video games and learning. *Cambridge Handbook of the Learning Sciences*, 377–396.

Suryapranata, L. K. P., Soewito, B., Kusuma, G. P., Gaol, F. L., & Warnars, H. L. H. S. (2017). Quality measurement for serious games. *2017 International Conference on Applied Computer and Communication Technologies (ComCom)*, 1–4. https://doi.org/10.1109/COMCOM.2017.8167098

Švábenský, V., Vykopal, J., & Čeleda, P. (2020). What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, 2–8. https://doi.org/10.1145/3328778.3366816

Švábenský, V., Vykopal, J., Cermak, M., & Laštovička, M. (2018). Enhancing cybersecurity skills by creating serious games. *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, 194–199. https://doi.org/10.1145/3197091.3197123

Sweetser, P., & Johnson, D. (2004). Player-Centered Game Environments: Assessing Player Opinions, Experiences, and Issues. In M. Rauterberg (Ed.), *Entertainment Computing – ICEC 2004* (pp. 321–332). Springer. https://doi.org/10.1007/978-3-540-28643-1_40

Sweetser, P., & Wyeth, P. (2005). GameFlow: A model for evaluating player enjoyment in games. *Computers in Entertainment*, *3*(3), 3. https://doi.org/10.1145/1077246.1077253

Tsopra, R., Courtine, M., Sedki, K., Eap, D., Cabal, M., Cohen, S., Bouchaud, O., Mechaï, F., & Lamy, J.-B. (2020). AntibioGame®: A serious game for teaching medical students about antibiotic use. *International Journal of Medical Informatics*, *136*, 104074. https://doi.org/10.1016/j.ijmedinf.2020.104074

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Van Gestel, L. C., Adriaanse, M. A., & De Ridder, D. T. D. (2021). Do nudges make use of automatic processing? Unraveling the effects of a default nudge under type 1 and type 2 processing. *Comprehensive Results in Social Psychology*, *5*(1–3), 4–24. https://doi.org/10.1080/23743603.2020.1808456

Van Oostendorp, H., Van der Spek, E. D., & Linssen, J. (2014). Adapting the Complexity Level of a Serious Game to the Proficiency of Players. *EAI Endorsed Trans. Serious Games*, *1*(2), e5.

Walsh, C. E. (2020). *Scoring games fairly: Biases and interference in games based assessment* [Phd, University of Southampton]. https://eprints.soton.ac.uk/448273/

Witmer, B. G., & Singer, M. J. (1998). Measuring presence in virtual environments: A presence questionnaire. *Presence*, *7*(3), 225–240.

Wouters, P., van Nimwegen, C., van Oostendorp, H., & van der Spek, E. D. (2013). A meta-analysis of the cognitive and motivational effects of serious games. *Journal of Educational Psychology*, *105*(2), 249–265. https://doi.org/10.1037/a0031311

Zhang-Kennedy, L., & Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys*, *54*(1), 12:1-12:39. https://doi.org/10.1145/3427920