PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
Higher Normal School of Technological Education. SKIKDA
Department of Mathematics and Computer Science

DISSERTATION

Presented to obtain a degree in Computer Science as a teacher of
middle school

Gamification of cybersecurity: developing practical skills through play

Field of study: **Computer Science**

Presented by
Soumaia FARES
Nesrine BENRAZEK

Board of examiners

President	Dr. Safia Bekhouche MCB Enset-Skikda
Supervisor	Dr. Rida Mezghache MCB Enset-Skikda
Examiners	Ms. Rafika Bouteghane MAA Enset- Skikda
	Dr. Riad Bouaita MCB Enset- Skikda

Academic year: 2024/2025

Acknowledgements

الحمد لله الذي بنعمته تتم الصالحات ,و بتوفيقه تنال الغايات له الحمد حمدا كثيرا ,بفضله و تيسيره مضت خطاي حتى هذا
الإنجاز

الى امي الحبيبة شكرا لك بعدد ما نبض قلبي كنت السند الذي لم يخذل ,يا من كانت دعواتك زادي و اهتمامك ضياء طريقي ,جزاك الله عني خير الجزاء
والى روح والدي الغالي , رحمك الله و غفر لك و جعل مثواك الجنة , هذا العمل ثمرة من غرسك اهديه لك مع كل دعائي
الى اختي الحبيبتين نريمان و ريتاج , رفيقتا دربي شكرا لكما على كل ما قدمتماه لي من من دعم لا يقدر بثمن كنتما الراحة في أوقات تعبي وجودكما بجانبي جعل الطريق اسهل فلكما مني كل الامتنان
اخي انيس و اخي هاني كنتما ظهرا قويا في كل المواقف ,دعمكما المادي و المعنوي كان له الأثر العميق في مواصلة هذا المشوار

الى رفيقاتي العزيزات رفيقات الدرب من شاركنني التعب و الفرح و الحزن ,لكل من كانت الى جانبي بكلمة بموقف شكرا لكن من القلب ,كنتن يد العون حين اثقلني التحدي سمية ,لينة ,ندى ,نسرين ,جيهان ,أسماء و من لم اذكرها عفوا .
و شكرا لكل من ساندني و لو بكلمة طيبة او دعوة صادقة , لكم جميعا اهدي هذا النجاح .

Nesrine

Praise be to Allah, who granted me a thoughtful mind and an eloquent tongue, who illuminated my path and eased my way to complete this work.

Peace and blessings be upon the best of all creation, our Prophet Muhammad, peace be upon him.

If a dedication can express even in part a sense of loyalty and gratitude, Then I dedicate this work to the one who raised me, who watched over me with eyes weary from sleepless nights and a heart full of love, To the one whose prayers were the secret behind my success: my beloved mother.

To the one whom Allah has blessed with dignity and wisdom, To the one whose presence is a source of pride, and whose life is a model I aspire to follow: my dear father, may Allah preserve him.

To those with whom I share the most sacred bond of existence, My beloved siblings, my unwavering support and companions through every step of this journey.

To my supervising professor, For his invaluable guidance, steadfast support, and insightful direction extend my deepest gratitude and sincere appreciation.

To my colleague and partner in this academic endeavor, whose support was essential throughout

To everyone who stood by me through words, advice, or heartfelt prayers.

And to all who may benefit from this humble work and remember me with a sincere prayer,

I dedicate this effort… as a symbol of love, a gesture of gratitude, and the first step on a lifelong path of contribution and growth.

Soumaia

Abstract

Serious game are digital applications that aren't just built for entertainment. they're designed to achieve educational, training, or awareness goals through engaging and interactive experiences. over the past few years, these games have really caught people's attention as powerful tools across various field, including healthcare, education, and cybersecurity.
Our project focuses on using serious games to improve cybersecurity awareness and help learners develop practical skills. The game we've designed simulates real-word cybersecurity scenarios, giving users the chance to recognize digital threats, make critical decisions, and apply the right countermeasures all within a safe and interactive environment.
What we're doing is combining the core principles of cybersecurity with game-based learning strategies. this creates an engaging alternative to traditional training methods, helping users build both confidence and competence when it comes to navigating digital risks. Instead of just learning theory, people get to practice and experience what it's really like to deal with cybersecurity challenge without any real-world consequences.

Keywords :
Serious games, cybersecurity, digital threats, game-based learning, learning theory.

ملخص

الألعاب الجادة هي تطبيقات رقمية ليست مصممة فقط للترفيه،تم تصميمها لتحقيق اهداف تعليمية او تدريبية او توعوية من خلال تجارب تفاعلية جذابة.

على مدى السنوات القليلة الماضية لفتت هذه الألعاب انتباه الناس حقا كادوات قوية في مجالات مختلفة ,بما في ذلك الامن السيبيراني، التعليم والرعاية الصحية.

يركز مشروعنا على استخدام الألعاب الجادة لتحسين الوعي بالامن السيبيراني و مساعدة المتعلمين على تطوير المهارات العملية ,مما يمنح المستخدمين الفرصة للتعرف على التهديدات الرقمية ,و اتخاذ القرارات الحاسمة و تطبيق التدابير المضادةالصحيحة كلها ضمن بيئة تفاعلية .ما نقوم به هو دمج المبادئ الأساسية للامن السيبيراني مع استراتيجيات التعلم القائم على الألعاب .وهذا يخلق بديلا جذابا لاساليب التدريب التقليدية ,مما يساعد المستخدمين على بناء الثقة و الكفاءة عند التعامل مع المخاطر الرقمية .بدلا من مجرد التعلم النظري ,يحصل المستخدمين على فرصة للتدرب و تجربة مايشبه حقا التعامل مع تحديات الامن السيبيراني دون أي عواقب في العالم الحقيقي.

الكلمات المفتاحية :

الألعاب الجادة, الامن السيبيراني , التعلم القائم على الألعاب , التهديدات الرقمية, التعلم النظري.

Table of Contents

1 Table des matière

List of Figures

List of Tables

Introduction

Cyber Security is the ongoing effort to protect individuals, Organizations and Governments from digital attacks by protecting networked systems and data from unauthorized use or harm. [1]

Cyber-attacks are increasing in number and sophistication, causing organizations to continuously adapt management strategies for cyber security risks [2]. As a key risk Mitigation Policy, organizations are investing in professional training courses for their employees to raise awareness on cyber-attacks and related defenses. Serious games have emerged as a new approach that can complement instruction-led or computer based security training by providing a fun environment where players learn and practice cyber security concepts [3]. This results in participants' faster learning and mastery of cyber security concepts. A number of serious games have been proposed with the aim of educating on different topics in cyber security. These games create realistic simulations of cyber threats and attacks without risking actual systems or data, allowing participants to gain hands-on experience in identifying, preventing, and responding to Security incidents, and help security professionals and employees better understand and respond to cyber threats.

Our project is structured to address this need by dividing the work into two main sections Theoretical Section Consisting of three chapters aimed at building the theoretical foundation for the research.

In the first chapter we introduced the concept of serious games, its history and classifications, as well as varied fields of application and differences from other entertainment games.

Chapter 2 is about The Coupling of Serious Games with Learning Covers the

integration between the learning process and serious games, specifying how the entire gaming operation affects improving learning outcomes, as well as enhancing motivation among learners.

Chapter 3: General Introduction to Cybersecurity Covers a complete portion of what cybersecurity can mean as a concept, there are different types of electronic threats out there; protection methods used under them, forming a theoretical foundation for the practical side.

Practical Section Consisting of one chapter divided into two parts: Game Design establishes the design process of the cybersecurity serious game, including educational objectives, character creation, scenario design, and gameplay mechanics as part one, part Two Game Implementation covers the technical aspects of game development, including technologies, development phases, and performance testing applied.

Chapter I. Introduction to serious games

I.1) Introduction

in this chapter We present a review of the definition of serious games and their history and classifications, after that we mentioned the most important areas of their use and examples of serious games.

I.2) Definitions

I.2.1) Serious game

A serious game is typically a computer application that combines a serious objective (in terms of learning, communication, information, etc.) with a fun means of achieving it (inspired by video games and the gaming world, etc.). Many definitions of serious games exist, but all imply a serious purpose that transcends mere entertainment.
The idea of using games for purposes other than fun was first formulated in the book Serious Games by Clark C. Abt (1975) [4]. When he introduces the subject of his book, he states: “We are concerned with serious games in the sense that these games have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement.” [4]. The educational purpose of Abt’s serious games does not necessarily have to be in the game’s design, but can be assigned to the game by the context it is used or embedded in. What this means is that for example a board game originally designed for fun can be used in a military training context to teach strategic thinking and the principles of tactical warfare. While the learning process takes place via the game, the effect intended by it may well be an exogenous one. The term ‘serious game’ as it applies to digital games was coined by Ben Sawyer in his 2003 paper on the potential of using digital games for policy making (Sawyer 2003). [5]
If we look at current definitions of serious games that imply that we are dealing with

digital games, we can see that Abt's definition is still mostly valid. Game designers Michael and Chen (2006) e.g. define serious games as follows: "A serious game is a game in which education (in its various forms) is the primary goal, rather than entertainment" [6]. This definition, however, can only be considered valid with a very broad understanding of education. As mentioned before, there are serious games that do not have a direct educational focus, but can still be considered serious. A more open definition is offered by Michael Zyda (2005) who states: "Serious games have more than just story, art, and software, however. (…) They involve pedagogy: activities that educate or instruct, thereby imparting knowledge or skill. This addition makes games serious" [7]. Again, for this definition to match the heterogeneous field of serious games, pedagogy would have to be defined flexibly as any form of change in a person brought about by external measures such as (educational) games. [5]
The definitions quoted here are just a snapshot from a great number of definitions which differ in some respects, but the great majority share the core statement that serious games are games which are used for more than just mere entertainment [8]
Finally, a serious games are a combination of serious dimension and playful dimension.

I.2.2) Gamification

is the use of game design elements in non-game contexts. [9]
It is not necessarily about learning at all and can be used in any context. Examples include companies that offer points, reward systems, badges, and other incentive based techniques, usually with the intent of increasing brand association and loyalty. In education it often involves attempts to wrap a game narrative around a course, topic, or project. It could also include multiple paths to the end, choices in what work is submitted for grading, criterion based rather than time- based assessment, and a decidedly learner-centered approach.

I.2.3) Game based learning

refers to the borrowing of certain gaming principles and applying them to real-life settings to engage users [10]. The motivational psychology involved in game-based learning allows students to engage with educational materials in a playful and dynamic way. Game-based learning is not just creating games for students to play, it is designing learning activities that can incrementally introduce concepts, and guide

users towards an end goal. Traditional games can incorporate competition, points, incentives, and feedback loops.

These concepts have become increasingly popular in higher education and in libraries as a way to engage students in learning.

I.2.4) Summary and Distinction Between Key Concepts

So serious games are purpose built educational tools that prioritize learning outcomes over entertainment, focusing on delivering essential concept through realistic scenarios. Games for learning integrate content into engaging game mechanics to systematically build competencies in different areas, commonly used in academic and professional development settings. Gamification applies game elements such as points, badges, and leaderboards to traditional training programs, enhancing learner engagement and motivation without creating a full game experience.

I.3) History of serious game

Before the more modern notion of Serious Games took hold, the US military made many attempts at using video games for training. The earliest being in 1980 when the US Army commissioned Atari to build the Atari Bradley Trainer This game was a modified version of the popular vector graphics-based game Battle zone, also published in 1980 [11]. Only 2 Atari Bradley Trainers were ever built and shown at a trade show. It is unknown why the US Army never deployed the game, but it was never actually used by soldiers. Another military project was started by 1984, this time by the US Navy, to use a video game to teach Morse Code. This project also only made it through the prototyping phase. The US military's view of games at the time was that they were not serious enough for military training, though the problem seemed to be one of vocabulary only. In other words, the military may have dismissed games because they associated them with casual play rather than recognizing their potential as « simulators » or « interactive training tools ». The problem wasn't that games were inherently unsuitable for training, but rather that the military lacked the right *vocabulary* (or mindset) to see them as valuable beyond entertainment.

in the 2000s, and even more so in the 2010s, the use of serious games for various applications in numerous sectors exploded. In 2002, America's Army was launched. This delivered virtual experiences simulating working in the United States army. This

was a US government-funded

Serious game for recruitment. In 2006, serious games were even used in journalism, with the release of Darfur is Dying. This Flash-built “news game” had over 800,000 players and brought awareness to the war in Darfur, and the subsequent humanitarian disaster. [12]

Over this period, various large multinationals started incorporating serious games into recruitment to identify talent and whittle down applicant lists. They also created bespoke serious games as parts of e-learning programs to simulate business scenarios for employees to train through and learn from. These programs of serious game training immersed employees in a low stakes environment where mistakes were learning experiences rather than costs to business.

I.4) Classifying of serious game

Since 2002, several methods and tools have been introduced to classify Serious Games.

Each of these methods endeavors to address the issues of its predecessors. However, no classification system has yet achieved a level of general acceptance. In this section, we will present some of these systems, and attempt to highlight their respective limitations. [13]

From a chronological point of view, the first classification systems were based on a single criterion. As pointed out by Sawyer & Smith (2008), these models can be divided into two categories: market-based classifications and purpose-based classifications.

I.4.1) A single criteria classification

I.4.1.1) Market base classification

These classification systems are designed to index games according to the “markets” which use them (i.e. the kind of people who play them). Here are some examples of market-based classifications:

•In a 2005 article, Zyda (2005) divided Serious Games into five domains: Healthcare, Public policy, Strategic Communication, Defense, Training & Education. [14]

•In a 2008 study, Alvarez & Michaud (2008) identified seven Serious Games markets, quite similar to those mentioned above: Defense, Training & Education Games, Advertising, Information, Communication, Health, Culture, Activism [14].

Albeit very useful, these market-based classifications suffer from two limitations. First, due to the discovery of new markets for Serious Games, their boundaries continue to expand. Secondly, these classifications are based solely on the applications of Serious Games rather than on the games themselves.

In other words, market-based classifications are able only to inform about the uses of Serious Games, not about their content. [13]

I.4.1.2) Purpose based classification

Alongside the classifications based on the uses of Serious Games, there are systems based on the intention that each Serious Game was designed to satisfy: the "purpose" [13].

Some examples of such classifications include:

- In his 2006 book, Bergeron (2006) presented seven "purpose" categories: Activism games, Advergames, Business Games, Exergaming, Health and Medicine Games, News Games, Political Games.
- In a 2008 article, Despond (2008) proposed a typology of four Serious Games "purposes": Advert Games, Institutional Serious Games, Business Games, Learning Games. [14]

This typology is based on another typology by the same author, which identified six "Serious intentions": to increase awareness, to simulate, to train, to inform, to teach and to influence. [14]

While they are still based on a single criterion, purpose-based classifications are harder to use than market-based ones. In each of the above models, categories seem heterogeneous. For example, "Health and Medicine Games", "Institutional Serious Games" and "Business Games" are tied to the "targeted market" of the game, while categories such as "Edu games", "Learning Games" and "Exergaming" are clearly based on the "purpose besides entertainment" and are features of the game. Overall, these systems are an interesting step towards understanding the purpose of Serious Games. They encourage separating "purposes" from "markets", which at first is not an obvious distinction. Unfortunately, they suffer from heterogeneous categories that prevent them from being a reliable source for general classification.[13]

I.4.2) A multiple criteria classification

The complementary nature of the criteria used in the market-based and purpose-based

classifications inspired a system based on multiple criteria: the “Serious Game Taxonomy”. Introduced by Sawyer & Smith (2008) [13], this global taxonomy indexes Serious Games according to two criteria:

•Market: Government & NGO, Defense, Healthcare, Marketing & Communication, Education, Corporate, Industry.

•Purpose: Games for Health, Advergames, Games for Training, Games for Education, Games for Science and Research, Production, Games as Work.

Each “purpose” category also comes with a “sub-taxonomy” whose complexity varies greatly from one “purpose” to another. At first glance, this global taxonomy uses 49 categories, plus many additional sub-categories. This taxonomy cleverly analyzed and merged previously available classification systems.

It is more complex to use than single-criterion systems, but it provides a better understanding of Serious Games through a more precise categorization. Shaped as a table, this “Serious Game Taxonomy” is also useful to detect “empty fields”, i.e. a combination of “market + purpose” that lacks any Serious Game reference.

Nevertheless, this system also suffers from certain issues. For example, the “purpose” criterion appears not to be sufficiently accurate, as a game such as September 12th falls outside of its scope. Furthermore, some “market” and “purpose” categories overlap. These issues appear to be inherited from previous single criterion classifications, especially the “purpose-based” ones which suffer from similar limitations. [13]

But Games are defined by both a “serious” and a “game” dimension, and all the systems we have presented so far focus on one single dimension at a time. In order to build an overall classification system for Serious Games, we should try surely to try to define a classification system that uses both dimensions at the same time. [13]

From an overall perspective, to classify Serious Games with more precision, they propose a new classification model that combines the analysis of both “serious” and “game” dimensions: the (G/P/S) model.

I.4.3) The (G/P/S) model

Referring back to observations concerning definition, a Serious Game is composed of both a “serious” and a “game” dimension [13]. To combine both dimensions, the G/P/S model extends the “Purpose & Market” paradigm by the addition of a “Gameplay”

related criterion. More specifically, the G/P/S model relies on three aspects:

•**Gameplay**, which refers to the type of game-play used. This aspect is intended to Provide information about the game structure of the Serious Game: how it is played.

•**Purpose**, which refers to the designed purpose. This aspect accounts for the eventual purpose(s) apart from entertainment intended by the designer of the Serious Game.

•**Scope**, which refers to the targeted application(s) of the title. This aspect suggests the actual use(s) related to the Serious Game: the kind of market, the audience… who uses it.

These three aspects, defined in the G/P/S model, can be used to build criteria suitable for the classification of any video game. The model places serious and entertainment games on the same footing (i.e.) any video game can be defined by a gameplay structure, a targeted scope of use, and an optional "purpose" apart from entertainment. [13]

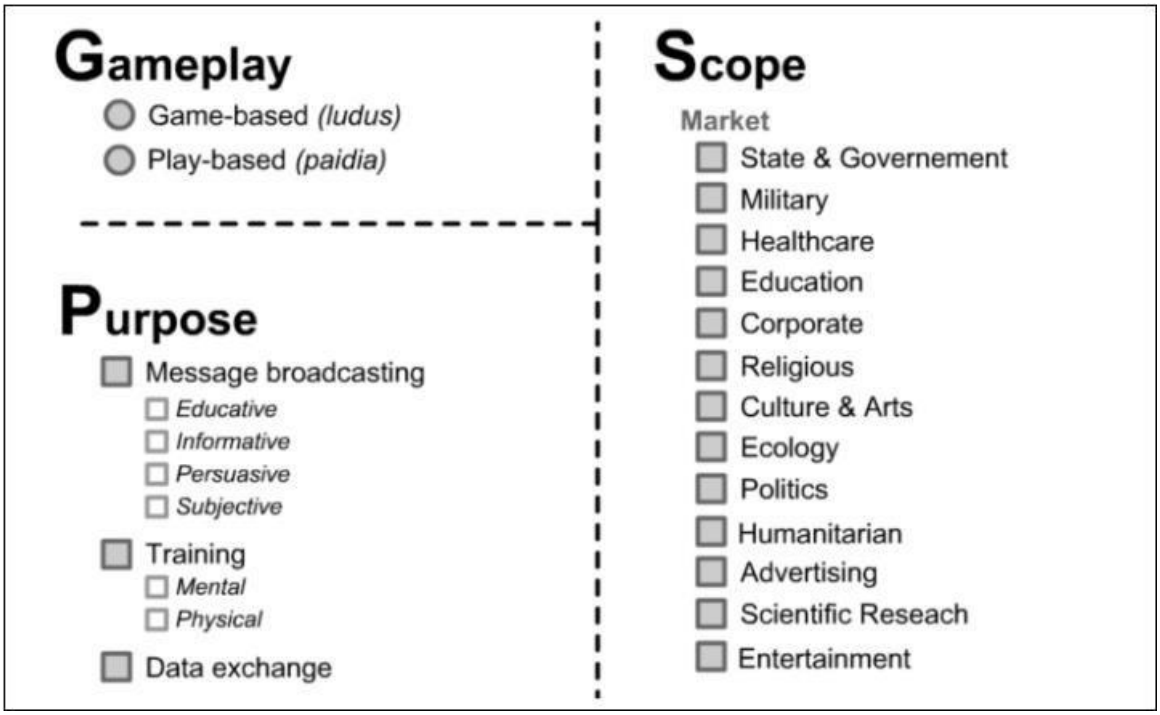

Figure 1: representation of GPS model

I.5) Serious gaming areas of application

Today, serious games are employed in a wide variety of sectors, including education, training, defense, health, simulation, communications and career management.

Drawn up by research laboratories, institutions and businesses, this list is also far from exhaustive. As serious games are designed to offer more than pure entertainment, they can be employed in a vast number of areas. Below is a selection of sectors that employ serious games to a significant degree.[15]

I.5.1) Defense

This is one of the biggest sectors for serious gaming. The American army actively supports the industry by commissioning military games such as America's Army. Military applications have also been developed in Europe, though their use is not as widespread: one example is IPCA by Script 'Games studio.

I.5.2) Teaching and training

Edu-games, when genuinely incorporating a videogame base, represent a sub category of serious games. The industry is investing considerably in the education, training and e- learning markets, as can be seen by programs such as the Education Arcade at MIT (Massachusetts Institute of Technology), which specializes in serious game projects [16] and has seen the development of Labyrinth, Revolution, Supercharged and more.

I.5.3) Advertising

Serious games designed for advertising purposes allow advertisers to continually promote a particular brand or product to users while they play the game. The approach is usually used to complement other e-commerce tools, in the same way as the Playmobil [17] website.

I.5.4) Information and communication

Serious games can be used to transmit messages and information in a wide variety of areas, such as to promote industrial careers in Technicity, Environmental Awareness: Fate of the World (2011), This sector is often combined with that of advertising in the form of viral marketing or Edu market games.

I.5.5) Health

Serious games dedicated to the health sector aim to improve users' mental and physical abilities.

One of the leading titles in the field is Dr Kawashima's Brain Training: How Old Is Your Brain, which evaluates the age of users' brains by having them carry out a range of exercises (including multiple choice questionnaires, sudoku, and observation games),

and allows them to maintain or improve their cognitive performance.

Many experts in serious games, including Ben Sawyer, expect significant growth in the health sector over the next few years.

I.6) Examples of serious game

[18]

I.6.1) Minecraft: education edition

Is developed by Mojang Studios and published by Microsoft. It aims to harness the creativity of students and educators to learn in a variety of subjects.

Gameplay:

- **Type:** Ludus (goal-oriented learning).
- **Objectives:** Explore, Create, Solve.
- **Mechanics:** Build, Code, Collaborate, Assess.

Functions:

- Deliver immersive STEM/humanities lessons.
- Provide collaborative problem-solving training.

Sector:

- **Markets:** Education, Government (schools/libraries).
- **Target Audience:** Ages 6+, Students & Educators.

Figure 2 : MINECRAFT education edition

I.6.2) Re-Mission

Remise is a serious game designed to educate and motivate young cancer patients. Developed by Hope lab and supported by the non-profit organization, it aims to improve treatment adherence and empower patients in their fight against cancer.

Gameplay:

- **Type:** Ludus (goal-oriented mission).
- **Objectives:** Destroy cancer cells, Manage treatment.
- **Mechanics:** Control Roxxi (nanobot), Combat infections, Take virtual meds.

Functions:

- Educate young patients about cancer biology.
- Motivate treatment adherence through empowerment.

Sector:

- **Markets:** Healthcare, Pediatrics.
- **Target Audience:** Ages 8–12, Cancer patients & clinics.

Figure 3 Remission game

I.6.3) Super Better

takes a unique approach by focusing on improving the players mental and emotional well-being. Originally designed as a tool for personal resilience, the game has gained popularity thanks to its positive impact on mental health.

Gameplay:

- **Type:** Paidia (open-ended, player-driven).
- **Objectives:** Build resilience, Overcome challenges.
- **Mechanics:** Complete quests, Track habits, Battle "bad guys" (negative thoughts).

Functions:

- Improve mental/emotional well-being.
- Turn real-life struggles into motivating adventures.

Sector:

- **Markets:** Healthcare, Self-Improvement.
- **Target Audience:** Teens & Adults (12+).

Figure 4 : SUPER BATTLE game

I.7) Conclusion

this chapter established the foundational concepts of serious games, distinguishing them from entertainment games through their explicit educational, training, or informational purposes. We explored definitions, historical evolution from military simulators to diverse sectors, and classification frameworks (market-based, purpose based, and the multidimensional G/P/S model). Key application areas—defense, education, health, and advertising—highlight the versatility of serious games. Examples like Minecraft: Education Edition and Re-Mission illustrate their real-world impact. The chapter underscores that serious games merge serious intent with engaging gameplay to achieve non-entertainment goals.

Chapter II. Serious games &learning

II.1) Introduction

Building on the foundational concepts of serious games established in Chapter I, this chapter explores their transformative role in modern pedagogy and skill development. As digital technologies reshape educational paradigms, serious games emerge as powerful tools that merge engagement with efficacy. We delve into the theoretical frameworks including gamification, game-based learning, and pedagogical psychology that underpin how serious games enhance knowledge retention, motivation, and practical skill acquisition. Through case studies (e.g., Duolingo, Class craft) and structural analysis, we dissect the core educational attributes *rules, goals, challenges, collaboration, and feedback* that define successful learning-oriented games. Crucially, we introduce the "pedagogical scenario" model, emphasizing the seamless integration of gameplay with educational objectives. This chapter bridges theory and practice, setting the stage for understanding how serious games can revolutionize cybersecurity training and beyond.

II.2) Learning theory games

E-learning is a very important tool in business today, and there is a trend towards these technologies to enhance learning and gain multiple skills. E-learning has many benefits, including providing high-quality material and reaching diverse audiences from diverse countries and ages. E-learning has improved immensely and now includes the web and applications, not just CDs. E-learning fosters communication and interaction between its users and is a must in companies and organizations. [19]

II.2.1) Gamified learning

Gamification is an educational approach that incorporates academic content into game design.

The goal is to make learning enjoyable and maintain the enthusiasm of learners.

Edutainment is the combination of education and play, transferring knowledge and educational skills in relaxed and creative ways. [20]

Gamification is the use of game elements such as assessment, challenge, human interaction, and rules to make the learning process purposeful and engaging. It is not limited to learning and participation only, but also appears in the workplace and during training. [21]

II.2.2) Gamification in education examples

- Duolingo

is a free application that uses gamification for language learning.[22]

- Class craft

is a digital platform that provides curriculum-aligned learning experiences with real time student monitoring. [23]

- Leaderboards

display participant rankings to motivate engagement and track group progress. [24]

- Coursera

is a massive open online course (MOOC) provider established by Stanford University professors Andrew Ng and Daphne Koller in Mountain View, California. The platform distinguishes itself by partnering exclusively with prestigious universities and organizations to deliver high-quality educational content online [25]

II.2.3) theory based applications for enhanced learning

We classify game elements based on learning theories and how these elements affect the player's experience. The following table illustrates the relationship between control, challenges, and human interaction with learning theories, highlighting the importance of these elements in enhancing interaction within the serious game environment, thereby supporting the learning experience in serious games. [26]

attribute	Theory	Definition
Action language	Presence theory	The method and interface by which communication occurs between a player and the game itself
Assessment	The testing effect	The method by which

		accomplishment and game progress are tracked
Conflict/ challenge	Goal-setting theory	The problems faced by players, including both the nature and difficulty of those problems
control	Self-determination theory	The degree to which players are able to alter the game and the degree to which the game alters itself in response
Environment	Presence theory	The representation of the physical surroundings of the player
Game fiction	The narrative hypothesis	The fictional game world and Story
Human interaction	Social constructivism	The degree to which players interact with other players in both space and time
Immersion	Presence theory	The affective and perceptual experience of a game
Rules/goals	Goal-setting theory	Clearly defined rules, goals, and information On progress toward those goals, provided to the player

Table 1: *Game element categories from the theory of gamified learning and theories*

II.3) Educational attribute of serious game

- **Rules:** The rules explain the components of the game and what players can do, as well as prohibiting certain principles. Without these elements, the game will not work. [27]

  For example, in a cybersecurity game, players may have a limited time to solve security challenges before a breach occurs.

- **Goals and Choices**: A specific goal without which the experience loses its structure. The extent of our work to achieve the goal represents the measure of

participation in the game. Players are also guided through storytelling and various challenges, thus providing a more immersive experience in the story. [27]
For example, players can choose between different security measures to protect their virtual assets.

- **Challenges:** The challenge creates a conflict that players are forced to solve, resulting in tension and varying levels of achievement, which is an essential element for maintaining player engagement. [27]
  For example, a player analyzes a phishing attack to determine the best response.
- **Collaboration and Competition**: “Inter-group competition in a gamified learning environment encourages students to maximize their individual performance for the sake of the team (Hung et
  al., 2015).”; [28]
  The evaluation features and virtual currencies enhance competitive and cooperative gameplay.[29]
  For example, in a cybersecurity training game, teams might compete to secure a network against simulated attacks.
- **Feedback and Assessment**: Providing continuous feedback keeps the player engaged, and rewards are also a fundamental element in designing attractive and motivating games. [27]
  For instance, a game might reward players with points for correctly identifying security threats.

II.4) Serious game underlies “pedagogy scenario “

A video game has a story, art along with software. A serious game also uses a story, art as well as software. But it adds pedagogy, which means educational activities that spread knowledge or skills.

Zyda's method for putting these parts together is to build the game first. People develop the entertainment part of the game at the start. Pedagogy comes after, and it reports to the story. The education fits into the game's overall structure.

Tricot's method for putting parts together is to build education first. Design the educational scenario first. People create a usage or game scenario. Both scenarios must work well with each other. Educational goals move the design process.

Both Zyda in addition to Tricot share a critical requirement - Educational and game parts must work together from the beginning. One cannot simply add education to a

game that already exists. This comes as an afterthought. Production and design teams need to work closely together.

A serious game needs a pedagogical scenario. Designers plan this scenario Specifically to reach educational goals - it does not just use standard video game mechanics with educational content that people attach later. The game's educational purpose must be plain. [30]

II.4.1) Pedagogical scenario

the serious game is integrated into an overall usage scenario. The educational scenario defines the learning sequences and the associated means. The educational scenario must enable students to acquire the skills defined in the educational objectives. [31]

What happens around the game is as (or more) important as the game itself. A good definition and organization of the educational scenario should allow:

● to ensure coherence in the order of activities

● for the teacher to feel comfortable and know where they are going

● for the students to find themselves in a structured framework

Start by defining the general structure of the course and the alternation of the different sequences: game, theoretical inputs, personal work, feedback, etc.

Next, define the specific scenario for the sequences dedicated to the game. A typical usage scenario for a serious game includes three phases:

-before: introduction and briefing

- during: orchestration, use of the simulation, the game

- after: debriefing These three phases can be iterated.

II.5) The fundamental qualities of good serious game

According to Bertrand Marne & al [32] The quality of serious games primarily relies on the reuse of principles that ensure the success of video games in general.

By analyzing different software, they identified five fundamental principles behind simulations and games in education:

- A sense of challenge fueled by the various problems the user must solve.
- An immersive and responsive game engine that responds to the player's manipulations and initiatives.

- Significant actions with which learners will overcome the obstacles of the game.
- A playful interface that will stimulate both the enjoyment and the motivation to continue the experience.
- A gradual difficulty in maintaining interest throughout the game.

But what makes a serious game different from a simple game? The educational dimension, of course.

Six facets to work on, with an educational objective:

- First of all, the educational objectives of the game, which must be clear both for the designers and the users. What do we want the learner to retain from their gaming session and their entire gaming practice?
- Next comes the domain simulation. The goal here is to find solutions so that learners acquire knowledge through an attractive and meaningful interface, and that they can perform operations utilizing the knowledge acquired or in the process of being acquired.

For these first two points, trainers and professionals in the educational field will be valuable advisors to the game designers, suggesting ideas and indicating the information to be integrated into the software.

- It is then appropriate to consider the interaction mechanisms in the simulation.
- The fourth facet concerns problems and progression: what obstacles will stand in the Learner's way? A progressive difficulty and the customization of the player's avatar are important elements of any good video game, and serious game developers must do at least as well, so that learners are motivated to stay in front of their screens.
- The fifth facet is what the authors of the document call the decorum, that is, all the multimedia or narrative elements that promote the player's immersion. For this facet and the two previous ones, game designers must draw on their knowledge and professional experiences to create a tool that is as entertaining and exciting as a video game, with a solid foundation of knowledge and educational objectives that will remain etched in the player's memory.

- The sixth facet directly concerns teachers and trainers. It involves identifying the conditions for using the game and its ability to fit into various and simple educational scenarios. For example, do we want a game that can be used in the classroom? If so, for how long? What feedback will be provided on the knowledge acquired in the game? It is up to teachers and trainers to answer these questions and a few others.

II.6) Evaluation of serious game

Evaluating serious games is important to determine their effectiveness beyond entertainment. It provides clear evidence of whether the games achieve their intended goals. Careful evaluation helps demonstrate the value of serious games to stakeholders and users, while also supporting their commercial success and the growth of the serious games industry. Four main stakeholder groups benefit from evaluation: developers, researchers, intermediaries, and users. [33]

II.6.1) Challenges in serious game evaluation

[33]

- Recruiting suitable participants, especially from vulnerable populations
- Operationalizing abstract concepts into measurable outcomes
- Choosing appropriate measurement methods and instruments
- Designing proper control group conditions for valid comparisons
- Assessing both short-term and long-term effects
- Measuring transfer of skills/knowledge to real-life contexts
- Processing results meaningfully to improve the game

II.6.2) Evaluation frame work and model

The evaluation process of serious games can be challenging due to the wide variety of games and their diverse contexts. Nevertheless, general guidelines and models can be developed to support the evaluation of a broad and abstract range of serious games.

Within this landscape, three prominent approaches offer complementary strategies for balancing substantive goals (e.g., learning, behavioral change) and design coherence: Kirkpatrick's Model (hierarchical outcome-focused evaluation), Mitgutsch & Alvarado'

Framework (purpose-driven design assessment), Evaluation-Integrated Models (e.g., ADDIE, embedding evaluation in development). [34] [35]

The following table contrasts these frameworks across key dimensions enabling researchers and developers to select context-appropriate evaluation strategies:

Aspect	Kirkpatrick's Model	Mitgutsch & Alvarado Framework	Evaluation-Integrated Models
Primary focus	Learning outcomes evaluation	Design and purpose assessment	Evaluation integration in design
Structure	4 hierarchical levels: reaction, learning, behavior and results.	6interconnected components: content, game mechanics, fiction, aesthetics, framing and overall coherence between these elements	Continuous process
Output	Effectiveness measurement	Coherence analysis	Design improvement
Application	Post development/during use	During design and development	Throughout project lifecycle
Evaluation timing	After implementation	During design phase	Continuous throughout process
Main strength	Comprehensive outcome assessment	Purpose-driven design evaluation	Iterative improvement approach
Primary challenge	Time-dependent effects	Does not measure direct effectiveness	Process complexity
usage	Essential when you need to prove return on investment, Critical for measuring long-term organizational impact.	Optimal for rapid design quality checks, Perfect for teams new to serious game evaluation	Best for projects where design flexibility is crucial, Ideal when you have development expertise and time

Table 2 :difference between frameworks across key dimensions

II.6.3) Usability testing for serious game

II.6.3.1) Introduction

product designers are increasingly focusing on usability testing during the prototype phase to identify design or implementation issues that might prevent users from successfully interacting with a final product. [36]

Usability testing is critical for ensuring that users can interact effectively with new technologies, especially for diverse populations.

Serious games pose unique usability challenges because they differ from traditional productivity software. They require balancing engagement, learning, and usability. Traditional usability metrics (e.g., efficiency, error rates) may not apply to games, as games intentionally include challenges, exploration, and trial-and-error loops. [36]

II.6.3.2) Usability testing and serious game

1. Usability testing methods

Macleod in addition to Renger state that usability assessments fall into three general kinds. Expert methods mean that experienced evaluators find possible problems with usability because they know the field. Theoretical methods compare ideas about tools and how people act to foresee usability trouble. The third kind is user methods, which give software samples to people who use them, so they can try them out and offer comments.

With user methods, two main ways of working apply. One is observational analysis – users try the system, and developers watch what they do, either live or by watching recordings. The other way is survey-based methods - users fill out forms about their experience after they use the system - these forms, for example, SUS, SUMI along with QUIS, also find use in expert methods. A form usually follows heuristic rules, which help spot possible usability problems. [37]

2. Common usability metrics

- System Usability Scale (SUS): Quick Likert-scale survey.
- Software Usability Measurement Inventory (SUMI): provides detailed

evaluations by measuring usability across five different dimensions (efficiency, affect, helpfulness, control, and learnability).

- Questionnaire for User Interaction Satisfaction (QUIS): Focuses on technical

aspects (screen design, learning factors).

- ISO/IEC 9126: Comprehensive standard for software quality.

Frankly, traditional usability evaluation methods come with some pretty glaring drawbacks. Their reliability is questionable—you can apply the same method to the same system and end up with totally different results. That's a red flag for consistency. On top of that, these approaches tend to focus on generating usability scores, rather than highlighting concrete issues or suggesting practical improvements. Most critically, they're just not designed for games. They end up penalizing exploration and trial-and-error, which are actually crucial elements of gameplay and player learning. In short, the standard usability playbook doesn't quite fit the unique demands of game evaluation. [36]

3. Development of the serious game usability evaluator (SeGUE)

Designed specifically for serious games, unlike generic usability tools, focuses on both identifying problems and recognizing engaging elements.

SeGUE Works for Serious Games because: Doesn't penalize exploration or failure (key to gameplay), Values positive engagement (e.g., learning, excitement), Reveals what works well (to preserve in design). [36]

Two Key Dimensions of Analysis:

- System -relate events (game design & interface)

Category	Description
Game flow	Core gameplay design issues (may require major change
Functionality	Problems with specific game mechanics
Layout/UI	Visual /interface problems (e.g.: confusing menus)
Content	Issues with text, instructions, or educational material
Technical Errors	Bugs or glitches
Nonapplicable	Events not tied to the system but still relevant

Table 3: system-relate events

- User-relate events (emotional & cognitive responses)

Category	Description
Negative	Frustrated, confusing, annoyed, unable to continue

positive	Learning, reflecting, satisfied/excited, pleasantly frustrated
neutral	Suggestions/comments, nonapplicable
other	Unclassifiable events (may indicate need for new categories)

Table 4 :user-relate events

SO, SeGUE bridges the gap between usability testing and game design principles, its two-dimensional framework ensures comprehensive evaluation and designed to adapt to different serious games' needs.

II.6.4) General methodology

gathering data to evaluate the usability of a serious game is an open-ended task with different possible approaches and several potential pitfalls. Therefore, there is a need for straightforward and reliable methods that help developers identify usability issues for their serious games before releasing them. In specific case, it focuses on facilitating an iterative analysis process based on observational methods, in which users play with early prototypes and researchers gather data with the objective of identifying and resolving design and UI issues that affect the usability of the games. [36]

II.6.4.1) key requirement for testing

it is possible to identify some initial requirements to perform usability testing of serious games:

- Test Users: Should represent the target audience (age, gender, education, etc.), In terms of number of test users, according to Virzi [38], five users should be enough to detect 80% of the usability problems, Nielsen and Landauer [39] countered that using up to 16 test participants would be worthwhile for a "medium" sized project.
- Prototype Session Evaluators: Multiple reviewers improve reliability (Kessner et al.).[40]
- Instrument for Serious Game Usability Evaluation: Needed to categorize usability events systematically, and tailored for serious games (unlike generic usability tools).
- Data Recording Setup: Screen + audio/video capture of play sessions to Avoids real-time note-taking, which can distract users or miss subtle cues.

- "Ready-to-Play" Prototype: should be as close to the final product as possible for test users to evaluate, allowing them to experience the interface and intended functionalities. Incomplete prototypes may not reflect the final product's usability once polished. A "vertical slice quality" approach was used in usability studies.
- Goal-Oriented Play-Session Script: Script should be brief and focused, Cover key gameplay mechanics and learning objectives, but may require multiple sessions to test all features.

This Methodology Balances thoroughness with practicality, adapts to games' unique needs (Recognizes that fun, challenge, and learning are as important as task completion and Structured yet flexible.

II.7) The future of serious game

The goal of serious games is to maintain user engagement and continuity. In recent years, these games have gained attention for their ability to deliver complex knowledge through engaging, interactive environments. With the rise of technologies like artificial intelligence, virtual reality, and augmented reality, serious games are becoming more immersive and adaptive to individual learners 'needs. Companies like "Cross Knowledge" are playing a key role in this evolution. Their "Serious Series" combines storytelling with workplace simulations to develop soft skills and promote behavioral change. They added the principle of "TV series for remote training". Including short episodes depicting the daily life of a team. Where all the situations are presented to the learner so they can understand the roles. Then the user chooses one of the proposed scenarios. The company broadcasts around 17,000 training courses in various languages. This kind of experience-driven learning exemplifies how serious games can effectively bridge the gap between theory and real-world application, and this is what serious games will witness as a real transformation in the coming years. [19]

II.8) Conclusion

This chapter examined the pedagogical integration of serious games within learning frameworks. We discussed how gamification (e.g., Duolingo, Class craft) and game based learning leverage motivation, competition, and feedback loops to enhance

engagement. Core educational attributes rules, goals, challenges, collaboration, and assessment was linked to learning theories like presence theory and self determination. The "pedagogical scenario" (pre-game briefing, gameplay, post-game debriefing) emerged as critical for aligning educational objectives with game design. Future trends point toward AI-driven personalization and immersive technologies (VR/AR) for adaptive, real-world skill transfer.

Chapter III.Introduction to cybersecurity

III.1) Introduction

The rapid advancement of internet technologies has revolutionized global communication, commerce, and information exchange. While these developments have facilitated unprecedented interconnectivity, they have also introduced a wide range of vulnerabilities and threats. The digital infrastructure that underpins modern society has become a prime target for malicious actors, whose methods evolve at a pace that often outstrips defensive countermeasures. As a result, cybersecurity has emerged as a critical domain in both public and private sectors. [41]

Cyber Security is being protected by internet-connected systems, including hardware, software and data, from cyber-attacks. In a computing context, security comprises cyber security and physical security both are used by enterprises to safe against unauthorized access to data center and other computerized systems. The security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber security.

The range of operations of cyber security involves protecting information and systems from major cyber threats. These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks were, in their most innovative form, cyber threats often take aim at secret, political and military assets of a nation, or its people. Some of the common threats are:

Cyber terrorism: Terrorist groups using IT attacks on networks and infrastructure for

political purposes.

Cyber warfare: Nation-states attacking other countries' digital systems to cause damage and disruption.

Cyber espionage: Illegally stealing secret information using technology for strategic advantage.

III.2) Definitions

III.2.1) Cybersecurity

The word ‘security’ is defined in the online version of the Oxford English Dictionary (Oxford University Press, 2015) as “The state of being free from danger or threat”. However, that simple definition belies the complexity of the actual use of the word, and particularly when it comes to cyber- security. The latter term is used continuously by politicians, computer specialists, IT managers, tech entrepreneurs, health industry professionals and national security operators, a spectrum so wide it would seem almost impossible that so many people would agree on a definition. As it turns out, there are differing views on what cybersecurity is. The term is used to cover the measures government institutions take to protect the public and the institutions themselves from threats in the ‘cyber’- domain, also known as ‘cyberspace’. Yet it is also used on a level that is somewhat closer to the individual, when it refers to protection against viruses and other malware on a computer, whether this is personally owned or used in the work situation. [42]

III.2.2) Information security

The international standard, ISO/IEC 27002 (2005), defines in- formation security as the preservation of the confidentiality, integrity and availability of information

In the context of ISO/IEC 27002 (2005), information can take on

many forms. It can be printed or written on paper, stored electronically, transmitted by post or electronic means, shown on films, conveyed in conversation, and so forth [43]

III.3) Cybersecurity objectives

The goals that institutions and individuals strive to achieve in order to protect their digital assets and data from various cyber threats. These goals are summarized in three concepts known as the CIA Triad:

III.3.1) Confidentiality

Confidentiality means maintaining the privacy of our information so that it is only accessible to authorized individuals. There are various means to achieve this, such as encrypting data to make it unreadable except to those who possess the decryption key, or defining access permissions to the data. It is also essential to ensure that the data cannot be altered or used in an unauthorized manner.

Data confidentiality in cybersecurity ensures data protection by restricting access to authorized personnel only. This, in turn, reduces the risk of breaches and unauthorized changes, thereby maintaining the integrity and reliability of the data. [44]

III.3.2) Integrity or safety

Safety means preserving data by ensuring it is not tampered with. Data deduplication is one of the processes used to reduce storage space and bandwidth consumption. We use dynamic encryption and private keyword search to achieve data integrity. Data integrity is very important in cybersecurity. For example, let's assume we have a working system. The security team ensures that it is not possible to change the way this system operates or the information stored in it. Because if someone manages to do that, it will lead to the entire system being compromised or important information being stolen. This summarizes the importance of maintaining data integrity. [44]

III.3.3) Availability

Availability is making information and systems accessible to authorized individuals. To ensure data integrity, we use identity to maintain privacy. There is also another method called symmetric token that allows secure operations on data stored online, thus protecting it from any attempts to tamper with or access it without permission. Additionally, the integrity of data stored in the cloud is verified by an independent party, providing extra protection against unauthorized access to user information.

Despite maintaining the confidentiality and integrity of the data and not tampering with it, it may be useless unless it is available to the employees within the organization and the customers they serve. [44]

This means that systems and networks must function as required and on time.

For example, we have important information, but it can only be accessed by authorized personnel, ensuring that this information is accurate. However, if the system displaying this information is down and not functioning, then this information becomes worthless

at that time. Therefore, it is essential to ensure that the systems are functioning well so that people can access and use the data when needed.

III.4) The domains of cybersecurity

there are too many domains of cyber security including: [45]

domains	Description
Framework& standards	Establish guidelines and best practices for managing and securing information systems. They provide a structured approach to implementing and maintaining security measures.
Application Security	Focuses on keeping software and applications safe from threats. It involves securing applications throughout their lifecycle, from design to deployment and maintenance.
Risk Assessment	Involves identifying and evaluating risks to an organization's information assets. It's crucial to develop strategies to mitigate identified risks effectively.
Enterprise Risk Management	A comprehensive approach to managing an organization's risk exposure. It integrates risk management practices across all aspects of the organization.
Governance	Refers to the policies and procedures that ensure an organization's security strategies align with its goals. It's key for maintaining operational integrity and regulatory compliance.
Threat Intelligence	Involves analyzing and understanding potential threats to anticipate and prevent attacks. It's essential for proactive security planning and response.
End-user Education	Focuses on training users to recognize and avoid security threats. Effective user education can significantly reduce the risk of security breaches.
Security Operations	Encompasses the day-to-day processes and technologies used to detect and respond to threats. It's vital for maintaining

	continuous security monitoring and incident response.
Physical Security	Ensures the protection of physical assets like servers and data centers. It's an essential complement to digital security measures.
Career Development	Involves building skills and knowledge in cyber security. Continuous learning is essential in this rapidly evolving field.
Security Architecture	The structural design of IT systems for maximum security. It's fundamental in ensuring all components of the IT infrastructure are secure.

Table 5 :cyber security domains.

III.5) Cyber threats

III.5.1) Software attack

Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. This attack can consist of specially crafted software that attackers trick users into installing on their systems. This software can be used to overwhelm the processing capabilities of online systems or to gain access to protected systems by hidden means. [46]

III.5.1.1) Malware

Computer software specifically designed to perform malicious or unwanted actions. Is known as malicious code or malicious software. These software components or programs are designed to damage, destroy or deny service to targeted systems. Malicious code attacks include the execution of viruses, worms, Trojan horses and active web scripts with the intent to destroy or steal information. [47]

- spyware Any technology that aids in gathering information about people or organizations without their knowledge.
- Trojan horse: A malware program that hides its true nature and reveals its designed behavior only when activated.
- Virus: A type of malware that is attached to other executable programs. When activated, it replicates and propagates itself to multiple systems, spreading by multiple communications vectors. For example, a virus might send copies of itself to all users in the infected system's e-mail program.

- virus hoax: A message that reports the presence of a nonexistent virus or worm and wastes valuable time as employees share the message.
- worm: A type of malware that is capable of activation and replication without being attached to an existing program.
- zero-day attack: An attack that makes use of malware that is not yet known by the anti-malware software companies.

III.5.1.2) Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

An attack that attempts to overwhelm a computer target's ability to handle incoming communications, prohibiting legitimate users from accessing those systems. [47]
in a Denial of Service (DoS) attack: the attacker sends a large number of connection or information requests to a target. So many requests are made that the target system becomes overloaded and cannot respond to legitimate requests for service. The system may crash or simply become unable to perform ordinary functions.
In a distributed denial of service (DDoS) attack: a coordinated stream of requests is launched against a target from many locations simultaneously. Most DDoS attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised. The compromised machines are turned into bots or zombies, machines that are remotely controlled by the attacker (usually via a transmitted command) to participate in the attack. DDoS attacks are more difficult to defend against and there are currently no controls that an individual organization can apply.

III.5.1.3) E-mail attack

- Spam: is unsolicited commercial email. While many consider spam to be a trivial nuisance rather than an attack, it has been used as a means of enhancing malicious code attacks. In March 2002, there were reports of malicious code embedded in MP3 files attached to spam messages.49 The most significant consequence of spam, however, is the waste of computer and human resources. Many organizations try to deal with the flood of spam by using email filtering technology. Other organizations simply instruct users of the mail system to delete unwanted messages. [47]

- a mail bomb: A form of email attack that is also a DoS attack. It can be carried out using traditional email techniques or by exploiting various technical flaws in

the Simple Mail Transport Protocol (SMTP). The target of the attack receives an unmanageable amount of unsolicited email. By sending large emails with forged headers, attackers can take advantage of poorly configured email systems on the Internet and trick them into sending many emails to an address of the attacker's choice. If many such systems are tricked into participating, the target email address will be buried under thousands or even millions of unwanted emails.

Although phishing attacks occur via email, they are much more commonly associated with a method of social engineering designed to trick users into performing an action, rather than simply making the user the target of a DoS email attack.

III.5.1.4) Communications Interception Attacks

Common software-based communications attacks include several subcategories designed to intercept and collect information in transit. The emergence of the Internet of Things (IoT) - the addition of communication and interactivity to everyday objects – increases the possibility of these types of attacks. Our cars, appliances and entertainment devices have joined our smartphones in being connected and remotely controlled. The security of these devices has not always been a primary concern. [47]

- Spoofing: In IP spoofing, hackers use a variety of techniques to obtain trusted IP addresses and then modify packet headers to insert these spoofed addresses.50 Newer routers and firewall configurations can provide protection against IP spoofing.
- Pharming: Pharming attacks often use Trojans, worms, or other virus technologies to attack the address bar of an Internet browser so that the valid URL that the user types is changed to that of an illegitimate Web site. A form of pharming called Domain Name System (DNS) cache poisoning targets the Internet's DNS system, corrupting legitimate data tables.
- Man-in-the-Middle: A group of attacks in which a person intercepts a communication stream and inserts himself into the conversation to convince each of the legitimate parties that he is the other communication partner. Some man-in- the-middle attacks use encryption functions.

III.5.2) Cyber threats techniques

There are many cyber security techniques to combat the cyber security attacks:

III.5.2.1) Antivirus

There are lots of malicious programs such as viruses, worms, trojans, etc. that are spread over the Internet to compromise the security of a computer, either to destroy data stored in the computer or to gain financial benefits by sniffing out passwords, etc. To prevent these malicious codes from entering your system, a special program called an antivirus is used to protect the system from viruses. It not only prevents malicious code from entering the system, but also detects and destroys malicious code that is already installed on the system. There are many new viruses every day. The antivirus programmer regularly updates its database and provides the system with immunity against these new viruses, worms, etc. [46]

III.5.2.2) Encryption

It is a technique that converts the data into an unreadable form before transmitting it over the Internet. Only the person who has access to the key and converts it into readable form can read it. Formally, encryption can be defined as a technique for locking data by converting it into complex codes using mathematical algorithms. The code is so complex that even the most powerful computer will take several years to crack it. This secure code can be securely transmitted over the Internet to the recipient. After receiving the data, the recipient can decrypt it using the key. Decoding the complex code back to the original text using the key is known as decryption. If the same key is used to encrypt and decrypt the data, it is called symmetric key encryption. [48]

III.5.2.3) Authentication

refers to the process of verifying a user's identity. When a router challenges you for a login username and password, this is an example of authentication.

Authentication is divided into two major types: normal and AAA (Authentication, Authorization, and Auditing). [49]

- Basic (Non-AAA) Authentication: Non-AAA authentication is the basic authentication capability built into a router or other network device's operating system. Non-AAA authentication does not require access to an external server. It is very simple to set up and maintain, but lacks flexibility and scalability.
- AAA Authentication: AAA stands for Authentication, Authorization, and Accounting.

it is a security framework that controls access to computer resources, enforces policies, and audits usage using protocols like: RADIUS, TACACS+. AAA and its combined processes play a major role in network management and cybersecurity by screening users and keeping track of their activity while they are connected.
Authentication is the process of verifying a user's identity to determine whether the user should be allowed access to a device.
Authorization is the act of limiting or permitting access to certain features within the device once a user has been authenticated.
Accounting is the recording of actions taken by the user once she has been authenticated and authorized.

III.5.2.4) Firewall

It is a hardware/software which acts as a shield between an organization's network and the internet and protects it from the threats like virus, malware, hackers, etc. It can be used to limit the persons who can have access to your network and send information to you.
There are two types of traffic in an organization viz. inbound traffic and outbound traffic. Using firewall, it is possible to configure and monitor the traffic of the ports. Only the packets from trusted source address can enter the organization's network and the sources which are blacklisted and unauthorized address are denied access to the network. It is important to have firewalls to prevent the network from unauthorized access, but firewall does not guarantee this until and unless it is configured correctly. A firewall can be implemented using hardware as well as software or the combination of both. [48]

- Hardware Firewalls: example of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet.
- Software Firewalls: These firewalls are installed and installed on the server and client machines and it acts as a gateway to the organizations' network.

Firewalls often have what is commonly called a DMZ
DMZ: stands for demilitarized zone, this is a military/political term referring to a zone created between opposing forces in which no military activity is allowed.
In the network security realm, a DMZ is a network that is neither inside nor outside

the firewall. The idea is that this third network can be accessed from inside (and probably outside) the firewall, but security rules will prohibit devices in the DMZ from connecting to devices on the inside. A DMZ is less secure than the inside network, but more secure than the outside network.

The DMZ can initiate connections to the outside network, but not to the inside network. [49]

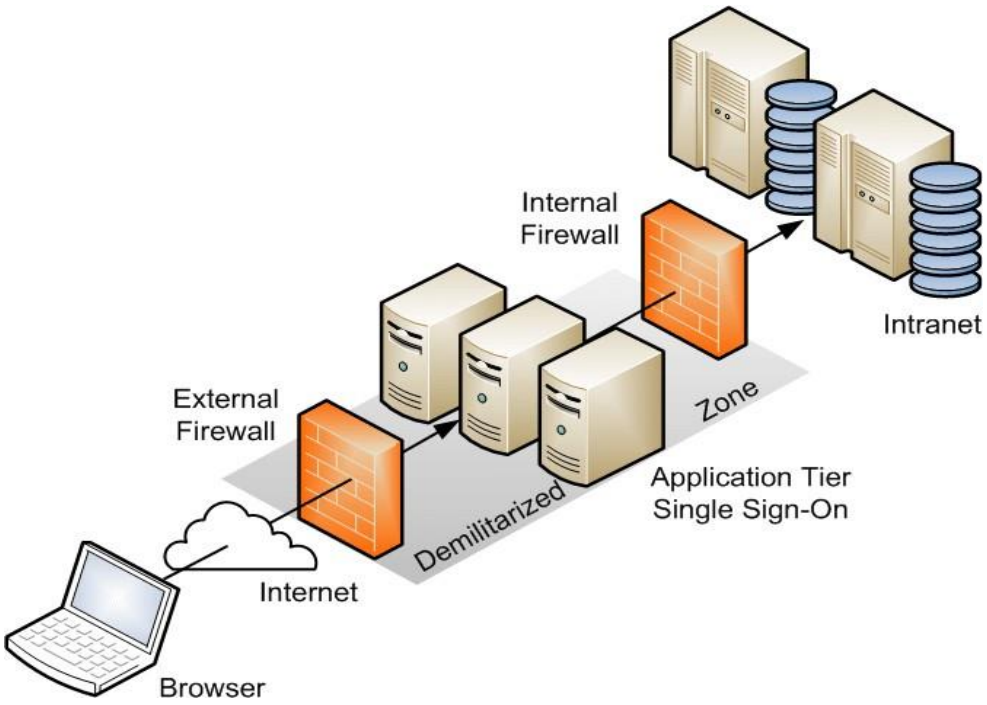

Figure 5 : DMZ

III.6) Conclusion

This chapter introduced key cybersecurity concepts, highlighting the shift from traditional information security to comprehensive digital protection. It emphasized the CIA Triad(Confidentiality, Integrity, and Availability) as the core framework for guiding cybersecurity strategies. we identified major cyber threats such as malware, DoS attacks, and communication interception, stressing the need for effective defense and risk management. Key security techniques like antivirus software, encryption, authentication, and firewalls were explored as pillars of layered protection. Finally, the chapter underscored the importance of integrating technical, organizational, and human elements across the eleven cybersecurity domains, laying a theoretical

foundation for the following chapter.

Chapter IV. Design & implementation

IV.1) Introduction

This project aims to develop a serious game with GDevelop. it teaches users about cybersecurity principles through interactive material. The game contains 3 levels. We shaped these levels to hold learners by adding quizzes and action problems.
A main goal is to show students plus new learner's common cyber threats. The basic rules of cybersecurity develop useful skills. This lets people manage cybersecurity events. Training shows learners how to spot threats and react. That helps them think well also act fast in digital areas. The goal is to build trust in safe online choices through platforms, because the instruction provides basic knowledge and hands on experience.

IV.2) Design

IV.2.1) Project overview and objectives

Our serious game project intends to transform cybersecurity education specifically for high school and college students aged between 15 and 25 but would also interest adult learners who want scholarship about cybersecurity. This beginner-friendly but intermediate-level design requires no prior technical background, and for use by individual learners and classrooms. The games aim to introduce students and novices to common cyber threats and teach them the fundamental principles of cybersecurity. By engaging in games, they develop practical skills that teach them how to assess, manage, and mobilize resources in the real-world, conditioned to recognize threats and respond effectively to them, developing critical thinking and quick decision making in the digital space. Ultimately, this platform builds students' exuding confidence in making safe online choices, delivering a complete learning experience in how theoretical cybersecurity knowledge converts into practical practice through engaging game-based learning methodologies.

IV.2.2) Scenario and storyline

The game progresses through a series of increasingly complex levels, each presenting a distinct scenario designed to demonstrate key cybersecurity concepts. Rather than repeating the same format, every stage introduces a new context or challenge. This structure facilitates a comprehensive understanding of cybersecurity principles while maintaining engagement and variety throughout the learning process.

- Level 01: knowledge foundation quiz: The initial stage introduces participants to a series of multiple-choice questions addressing essential cybersecurity principles, such as password management, recognition of social engineering tactics, basic malware identification, and secure browsing behaviors. This structured assessment not only establishes a foundational understanding but also highlights specific areas where further study may be beneficial
- Level 02: is divided into 3 stages, displays a group of threats (3 threats) where the player must choose the appropriate action to avoid being compromised/hacked.
- At Level 3: The gamers navigate through a large virtual space where they are pursued by different viruses. The player must collect the correct antivirus to deactivate every virus.

IV.2.3) Cybersecurity concepts

Each level in the game is associated with specific concepts and objectives, as shown in the following table:

Level	Environment/task	Key concept	Learning objectives	Validation criteria
1	Quiz Room (Multiple-choice quiz)	Cyber Threats, Safe Practices	Identify cyber threats and safe behaviors, recall core cybersecurity knowledge	Correctly answer all questions, nail the high score
2	Mission Area (Like, story mode with choices)	Phishing, Malware, Privacy,	Recognize phishing attempts, avoid malicious	Complete all tasks without falling for threats.

		Decision-Making	downloads, protect privacy; make safe cybersecurity decisions	
3	Open Space (Virus Chase)	Fighting virus, antivirus	React to threats in real time; match threats with correct defenses; understand active protection	get why active protection matters Wipe out all the viruses by grabbing the right antivirus each time

Table 6: Game 's cyber security concept

IV.2.4) System Architecture

purpose of the system is to train the learners into understanding cybersecurity's fundamental principles through a participatory learning format and simplified educational methods. Thus, they would first be able to recognize cyber threats in order to follow through with theoretical concepts (question test) and eventually, application in practice (simulation game: a scene simulating a digital environment with security challenges) thereby increasing security awareness among all learners.

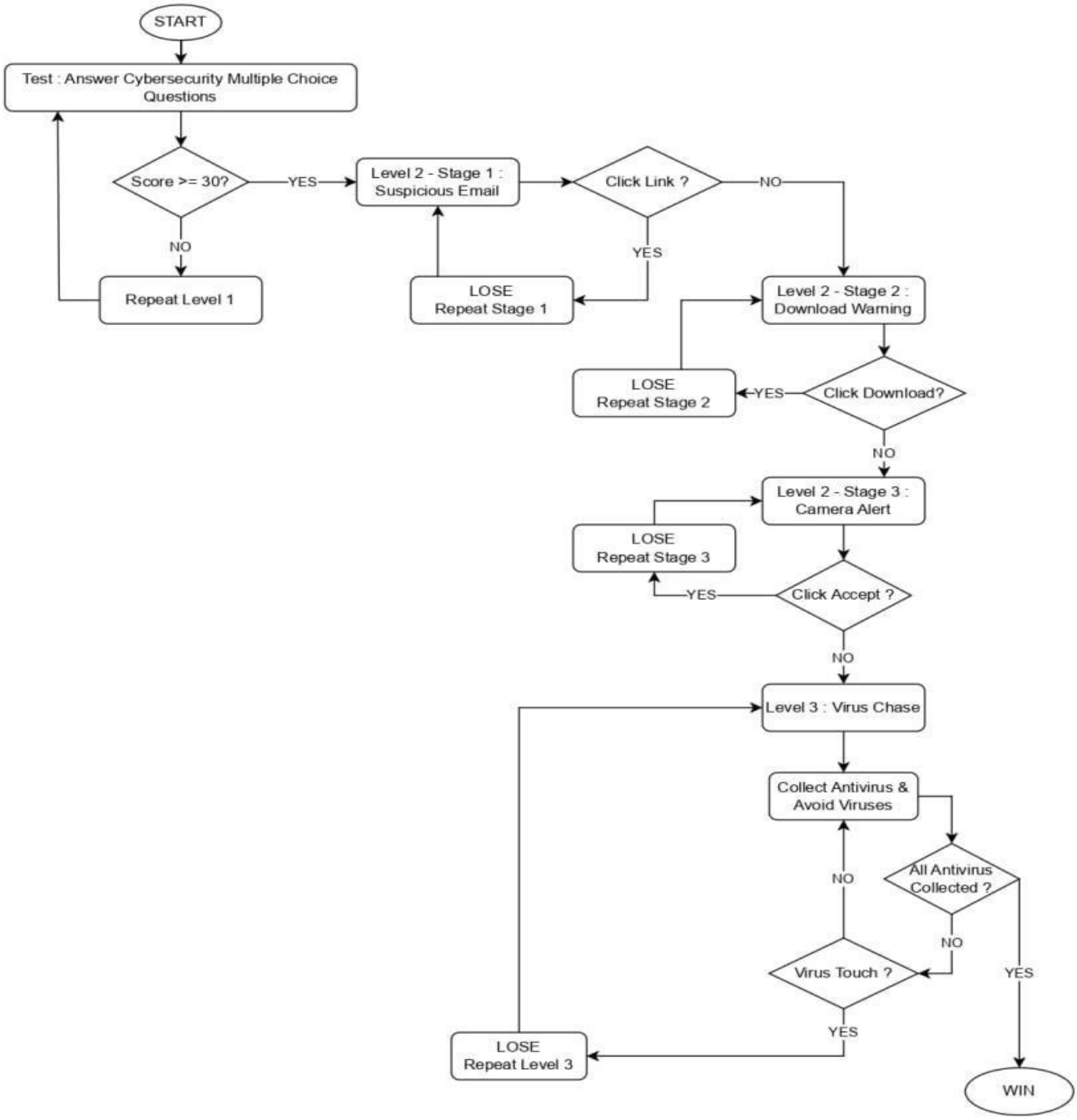

Figure 6: system architecture of the game

User interface

IV.2.4.1) Visual and Accessibility Considerations

The platform presents a distinctly cyber-digital aesthetic, characterized by the consistent use of circuit-inspired motifs, neon highlights, and stylized digital typography. This cohesive visual language not only reinforces the thematic underpinnings of the interface but also facilitates intuitive user navigation. Interactive elements are thoughtfully sized and labeled, promoting both usability and accessibility across diverse user groups and reflecting a genuine commitment to best practices in inclusive design.

Moreover, the environment leverages layered thematic backgrounds and well constructed navigation systems to foster a sense of immersion. Immediate feedback upon user interaction ensures clarity and engagement, supporting a seamless user experience. Collectively, these design choices enable participants to become deeply engaged with the cybersecurity narrative, while simultaneously advancing the educational objectives of the platform.

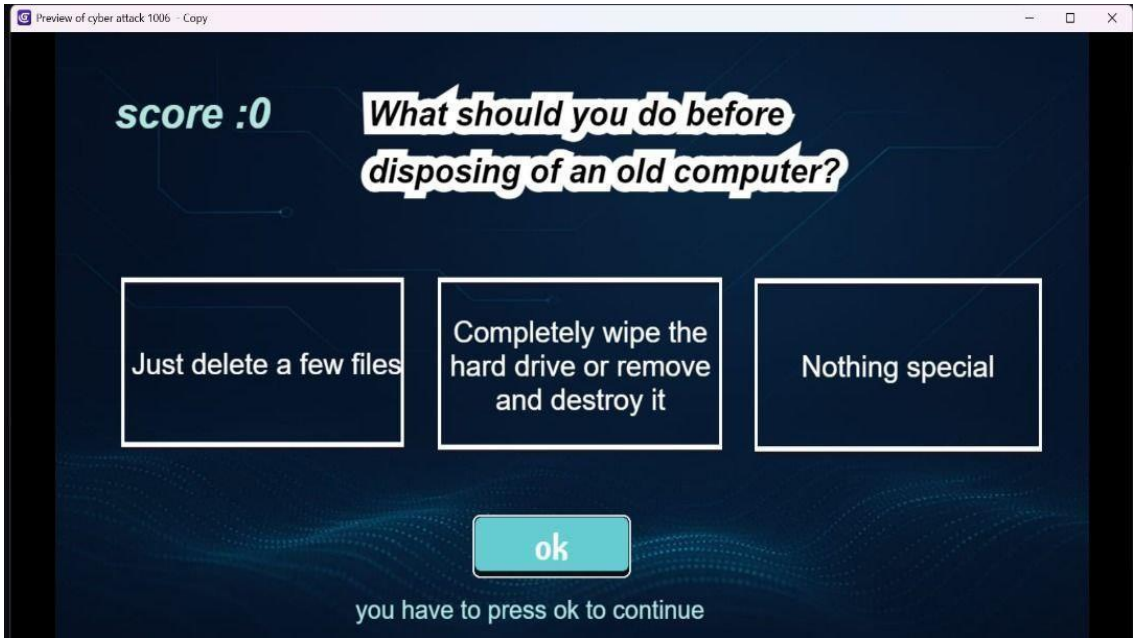

Figure 7 : level 01

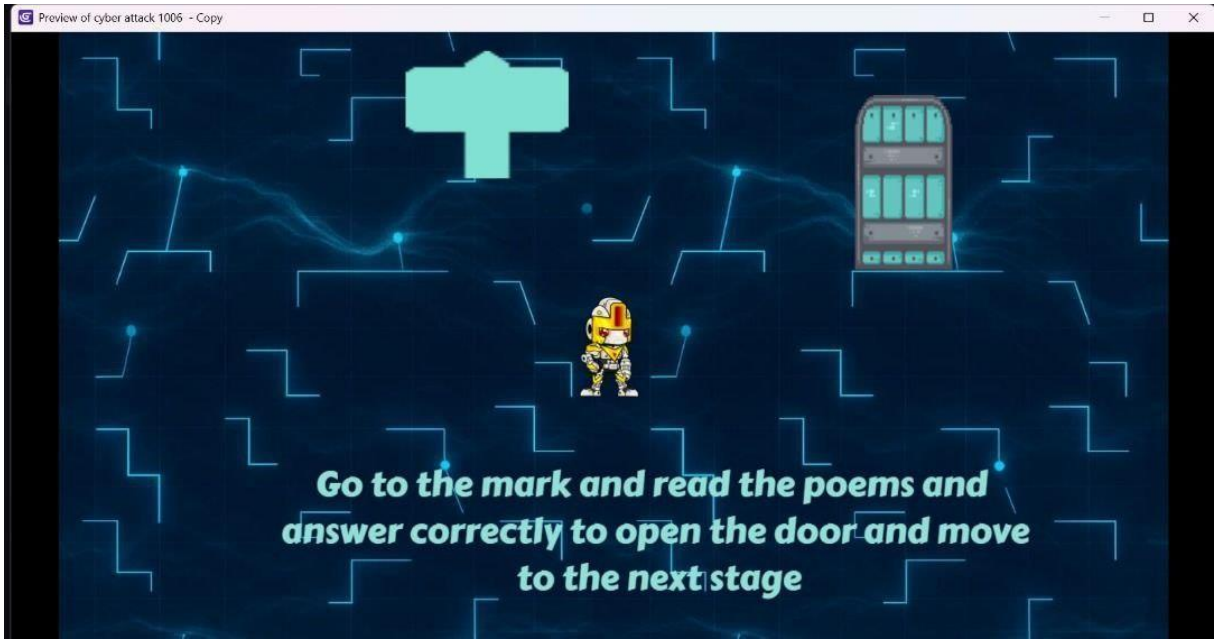

Figure 8 :level 02

IV.3) Implementation

We present our implementation of the system. We talk about our tools and technologies choices and development tools, such as programming languages, then, we will present the interfaces and functionalities of the system in detail.

IV.3.1) Tools and Technologies

[50]

GDevelop 5.5.231 is an open-source game development platform that allows users to create games without writing code. with its event-based visual programming, it empowers to focus on designing gameplay rather than worrying about complex coding. Its simplicity and versatility make it ideal for both beginners and experiences developers looking for a quick and efficient way to build games.

IV.3.2) Key Features

- Visual programing: GDevelop uses an intuitive event system to define game logic, making it easy to create mechanics without programming knowledge.
- Multi-platform export: build once and export your games to Windows, macOS, Android, iOS, or as HTML5 web games to reach players everywhere.
- Ready-to-use Templates: kickstart your project with templates for popular game genres like platforms, puzzles, and shooters.
- Built-in-Asset Store: access free sprites, sound, and animations directly within the platform to save time during development.

- Extensibility: while it's no code by default, GDevelop support JavaScript for users who want to enhance their games with custom functionality.
- Open Source: As an open-source tool, GDevelop lets developers contribute to its features or customize it for their unique needs.

IV.3.3) Scenario execution

Each level's cybersecurity scenario is represented as an independent "GDevelop" scene that is structured in a specific way:

- Scene Structure

is explicitly designed to bring an integrated experience of cybersecurity education and threat simulation regarding interactive gameplay across three levels. Cyber-themed background layers with circuit board patterns and digital network aesthetics establish the visual context. An interactive quiz interface button at Level 1, threat simulation panels at Level 2, and dynamic virus/antivirus objects at Level 3 were provided within each level, responding to players through input devices-the keyboard and mouse. On screen text prompts guide educational material through directing the players toward cybersecurity challenges, making them meaningful learning contexts. The game goes on under a scoring mechanism coupled with completion criteria that ensure educational objectives get satisfactorily attained before the player's progress to subsequent challenges.

- Initialization

load level variables (question strings, answer options, score counter = 0, threat objects, virus/antivirus entities).

Thus, each level in "Preview of Cyber Attack 1006" becomes a step classification that is structured as an educational progression with clearly defined mechanics for cybersecurity learning and skills testing:

It has three levels that progressively build on the basic knowledge learned in each level. In Level 1, the player's understanding of the theories is tested through a quiz containing 10 questions. To move to Level 2, players must score above 30 points: 10 points for each correct answer and minus 2 points for an incorrect one. Level 2 brings the action close to hands-on practice in threat recognition, where players will maneuver through three cybersecurity threats via keyboard commands and interaction with the 'E' key, making Accept or Reject decisions to counter the threats wholly. Level 3 will

put players into real-time cyber defense simulation as they guide a character to avoid virus entities and collect all antivirus objects scattered in the environment. This kind of structured learning path ensures the complete education of a player in cybersecurity by theoretical assessment, practical threat identification, and active defense gameplay.

- Asset Pipeline

The asset pipeline features an integrated sprite system in GDevelop that implements a cybersecurity theme with visual question interface panels, threat simulation objects, character sprites, virus entities, and antivirus representations. All assets are optimized for GDevelop's rendering engine with resolutions appropriate for good visibility on varied screen configurations.

- Scripts & Events

The GDevelop venting system controls the game's logic based on conditional statements that evaluate quiz validation, score processing, threat recognition assessment, and character movement mechanics. Variable management stores the questions, maintains score, and keeps track of level completion criteria. Keyboard input events in Level 3 are responsible for character movement, whereas in Levels 1 and 2, mouse/touch events operate all UI interactions. A progression system instituted conditional logic that evaluates how the performance is measured before allowing the levels to be transitioned, thus ensuring educational goals are adhered to throughout the cybersecurity training.

IV.3.4) User interaction

- Button based decision making

the UI interaction mechanism uses buttons for click-based inputs so that players can get into engagement scenarios concerning cybersecurity through this method of input. The case of consideration is computer disposal: the subject sees three options (file deletion, complete wiping, no action) and clicks on one to evaluate the protocol. The last step is pressing the "Ok" button as confirmation of the decision made. The game engine processes these clicks through an event handler recording what decisions players made and later invoking feedback responses for correct or incorrect practices and/or informing the user about dangers implied by wrong decisions. In the end, the improvement was in threat recognition and procedural security knowledge.

- Top-down character movement

under the top-down movement behavior system, the users move within the game environment. It provides an intuitive control by character across the two geographically-based levels built around the 2D cyber security-themed levels. Therefore, the movement system needs some pretty easy game logic that makes smooth and playful character motion: interactive items like terminals, question marks, and secured access may be interacted with by exploring terre. This could also manage an integrated input system responding to keyboard and controller inputs and perfectly fluid navigation alongside that feeling of using that environment to contribute to enhanced immersion and learning. The input system would manage these possible methods.

- Ai pathfinding navigation

this movement system includes artificial intelligence through pathfinding behavior using A* (A-star algorithm) to find optimal routes connecting two points in the computer games cape. By interacting with distant objectives or by-passing barriers, the pathfinding system can autonomously determine the shortest and, most importantly, path for character movement through space. It's how this AI maximizes the flow of gameplay while the player faces challenges posed by cybersecurity problems and learns security concepts: effortless interactions provide an intuitive model that pedagogy servomechanisms without mechanical navigation barriers.

IV.3.5) Screenshots

This are a groups screenshots of the game:

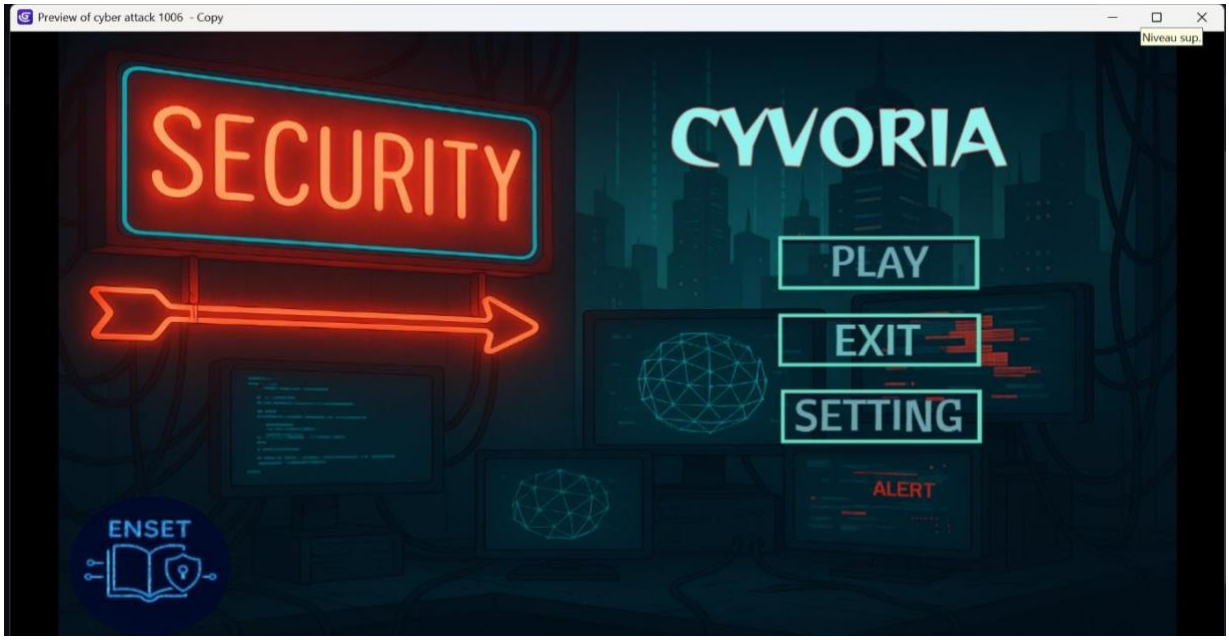

Figure 9: Main Menu Interface of the Game

The interface provides access to the three main sections: Play, Exit, and Settings. The background features a neon “SECURITY” sign and several computer screens displaying cybersecurity-related graphics and alerts, creating a thematic atmosphere. The ENSET logo is visible in the lower left corner, indicating the institutional affiliation of the project.

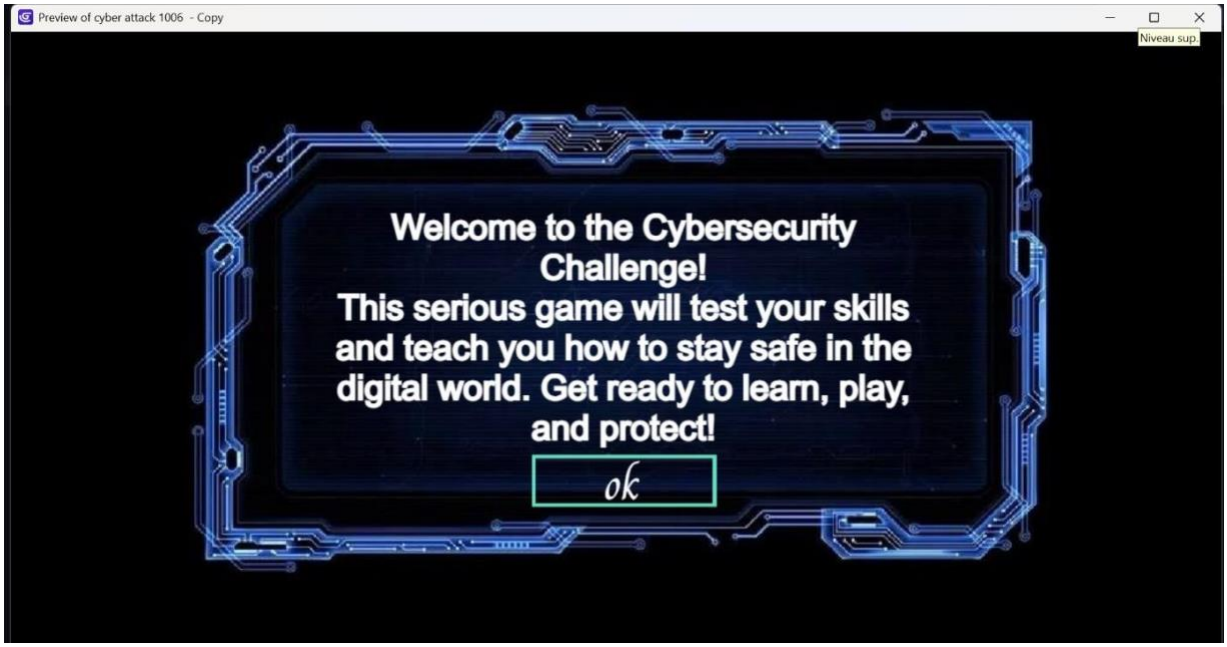

Figure 10 : Welcome Scene of the Game

This scene introduces the player to the game environment and prepares them to face cybersecurity-related challenges.

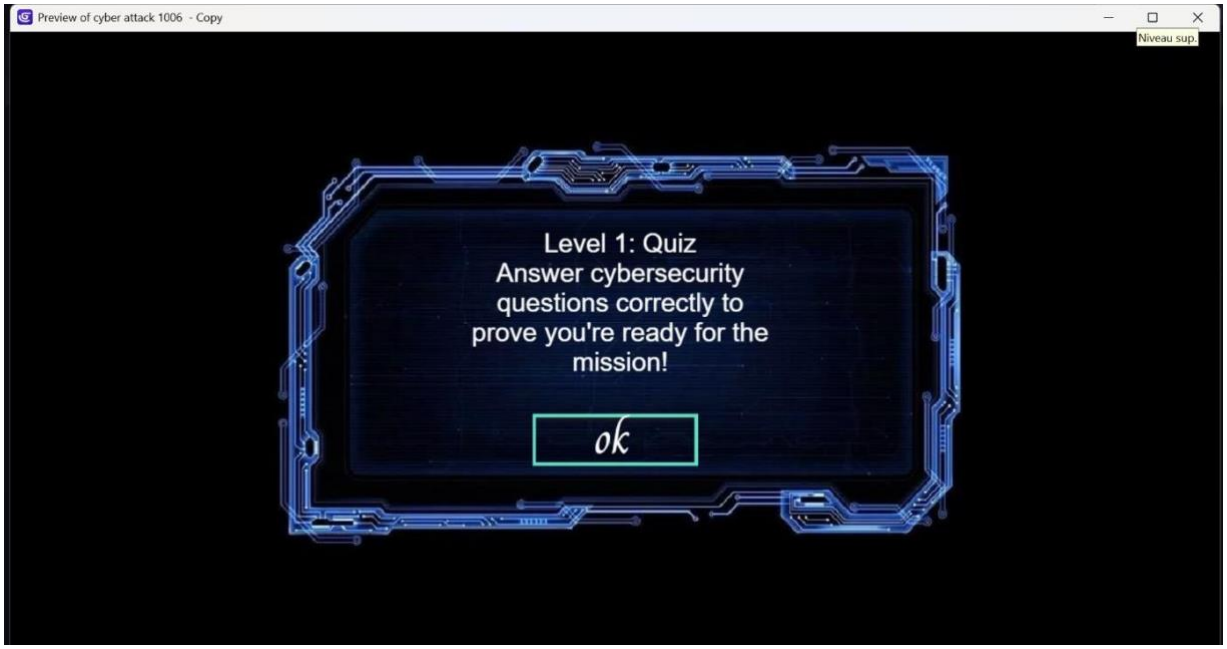

Figure 11 :Level Information Window in the Game

This window illustrates the interface design that displays the level one instruction within the game. The design reflects a cyber aesthetic and provides clear guidance to the player.

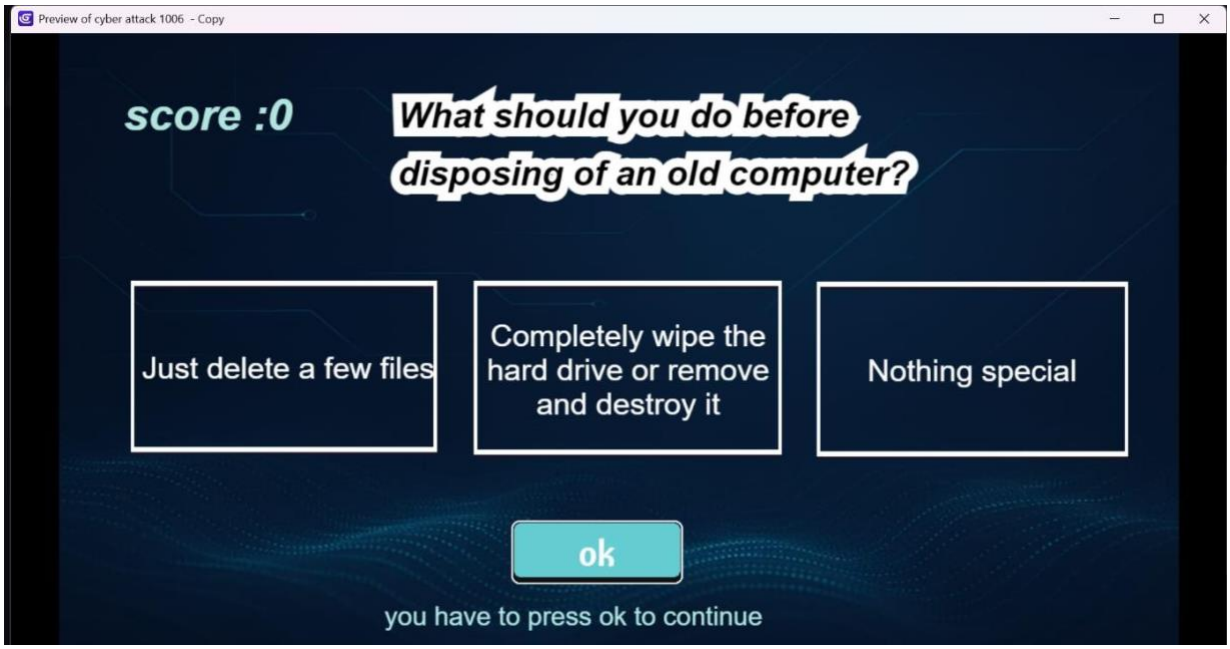

Figure 12: Level 1 - Multiple Choice Question Interface

The figure displays the quiz. It features the question along with three multiple-choice answer options presented in white boxes. The score is visible in the top left, and an "ok" button at the bottom indicates progression. The interface is set against a dark

background with subtle blue digital elements, typical of cybersecurity game aesthetics.

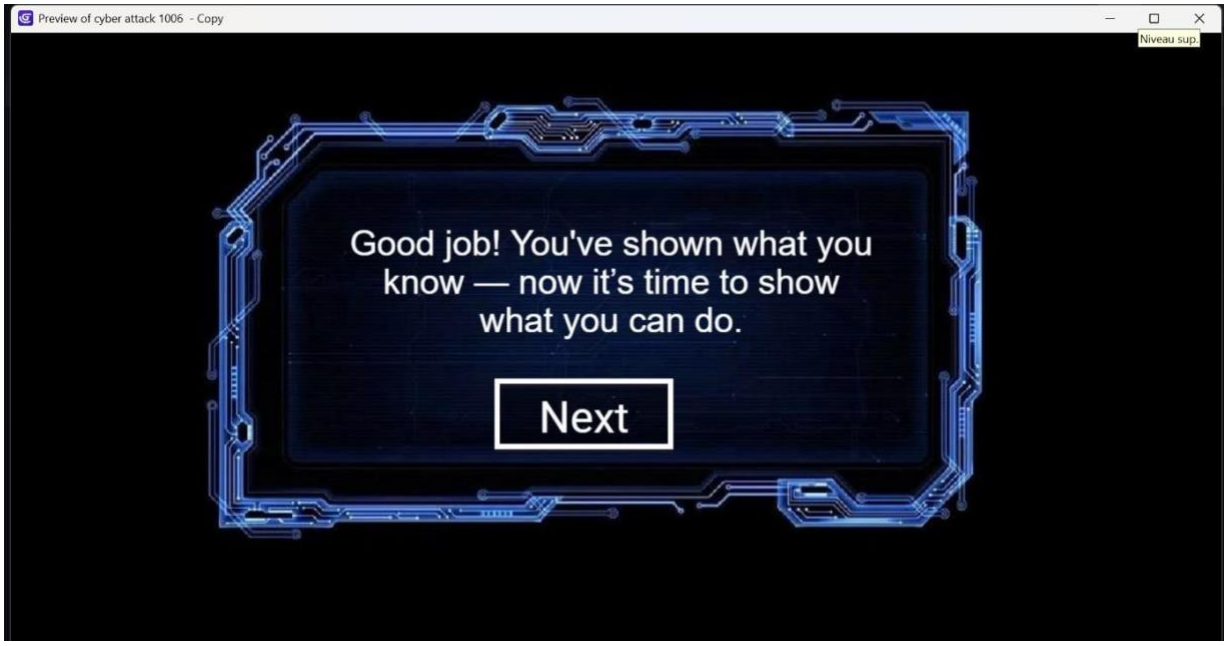

Figure 13 : Transition message from Level 1 to Level 2 in the Game

This figure shows the motivational message displayed after the player completes the first level, which consists of a cybersecurity knowledge quiz. The message congratulates the player and sets the tone for the upcoming level, where practical cybersecurity scenarios are introduced. It serves as a narrative bridge between theoretical learning and applied gameplay, enhancing player engagement and immersion.

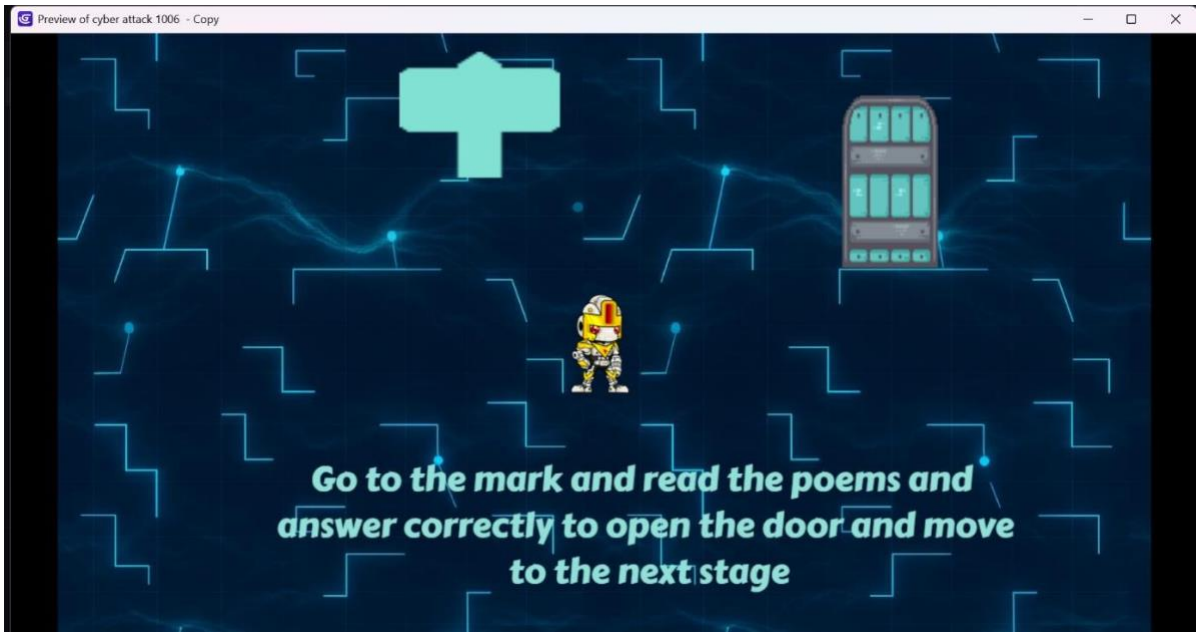

Figure 14 : Level 2 - Cybersecurity Awareness Interface in the Game

This figure shows the game screen, which contains a central character (a robotic character) and on-screen instructions for a mission.

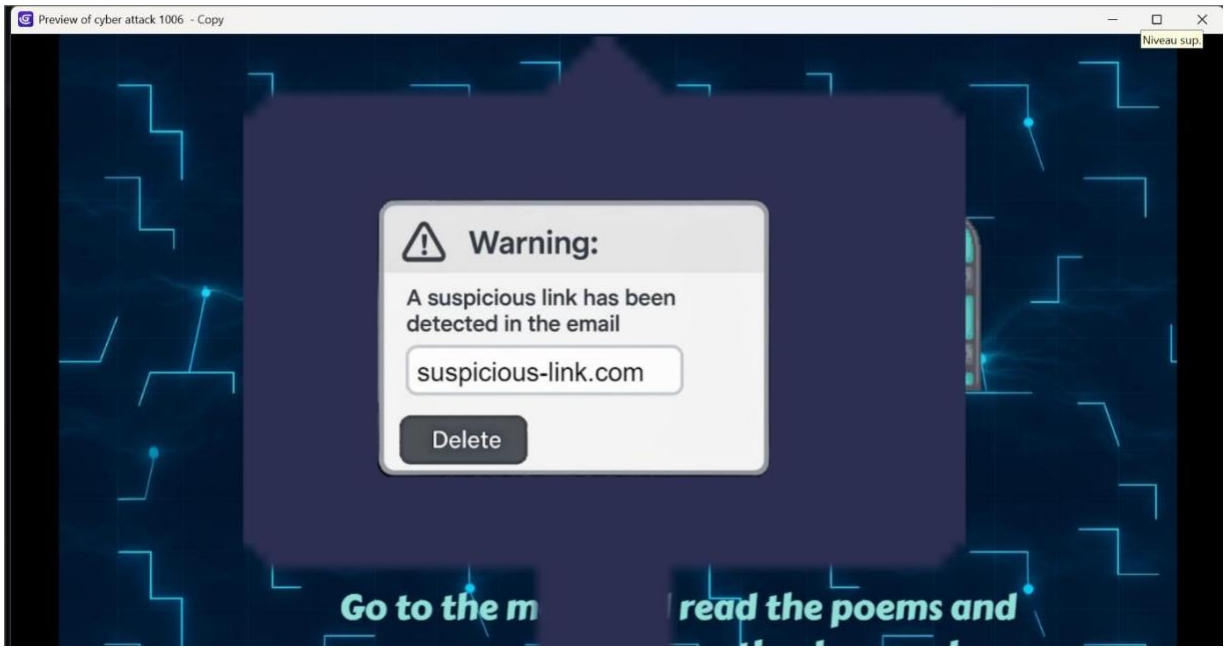

Figure 15 : Example of a Suspicious Email Scene in Level 2 Stage 3

In this scene from the second level of the game, the player is presented with a realistic looking email containing a suspicious link. The goal is to carefully evaluate the content and decide whether to click on it or delete it. The presence of a "Delete" button encourages safe behavior by allowing the player to reject a phishing attempt.

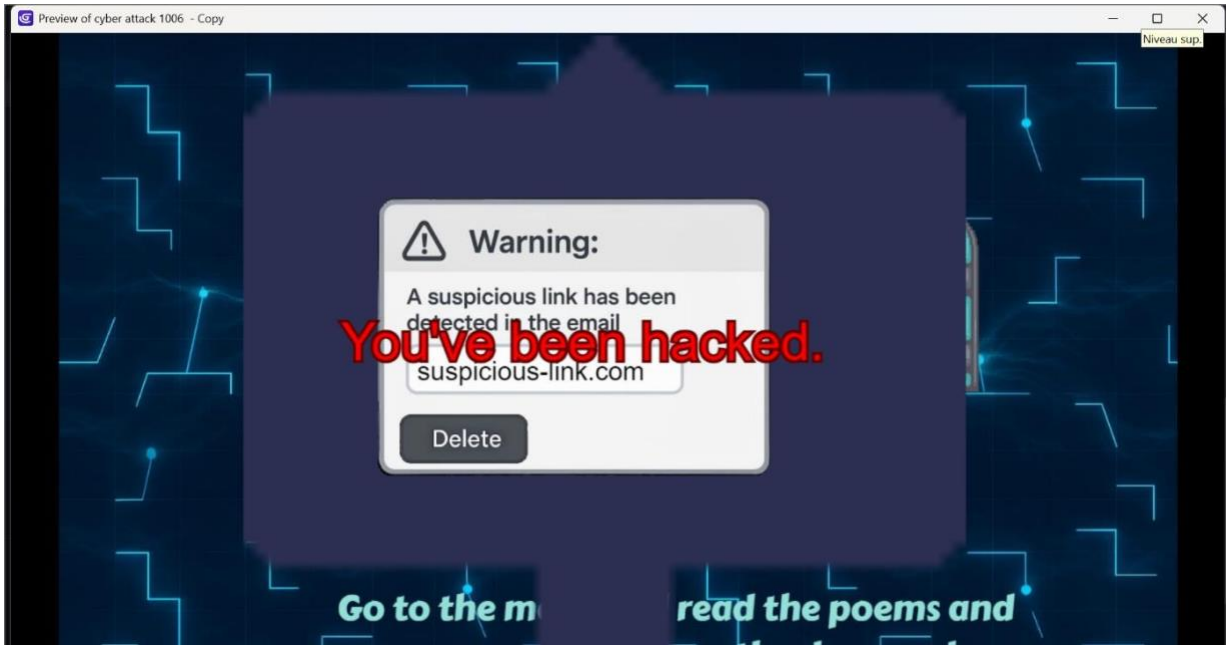

Figure 16 : Consequence of Clicking a Phishing Link in the Game

If the player clicks on the link, a message saying "You have been hacked!" appears, and the level restarts. This mechanism reinforces the importance of caution when using the internet.

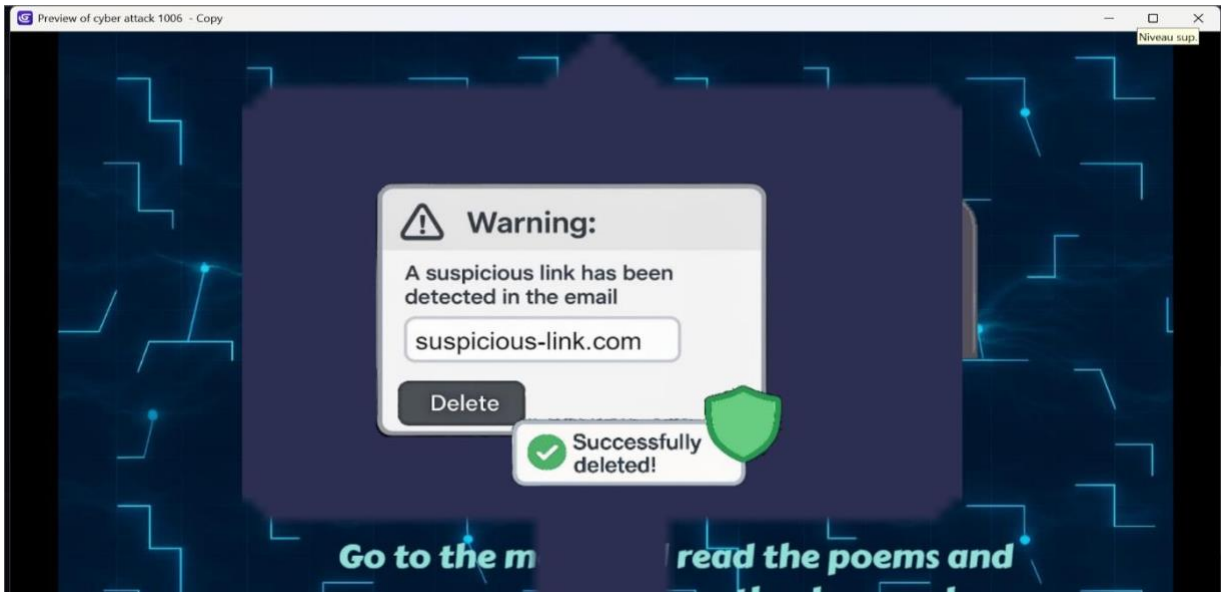

Figure 17 : Positive Feedback After Deleting a Suspicious Email

This figure shows the positive feedback displayed when the player correctly deletes a suspicious email. A "Successfully deleted!" message appears along with a green security shield, reinforcing safe online behavior.

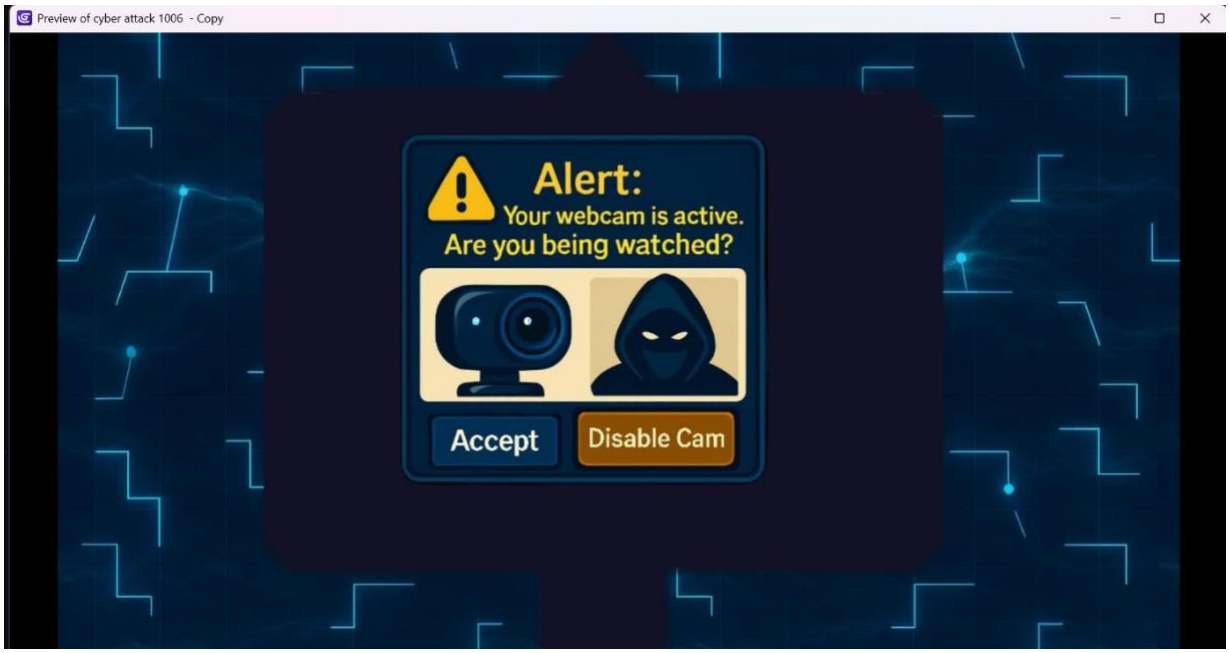

Figure 18 : Level 2 - Stage 3: Webcam Access Alert Interface

This figure simulating a cybersecurity threat. The central features a prominent "Alert!" warning icon and text stating: "Your webcam is active. Are you being watched?" Visual icons of a webcam and a hooded figure reinforce the message. Below the warning, "Accept" and "Disable Cam" buttons offer player choices.

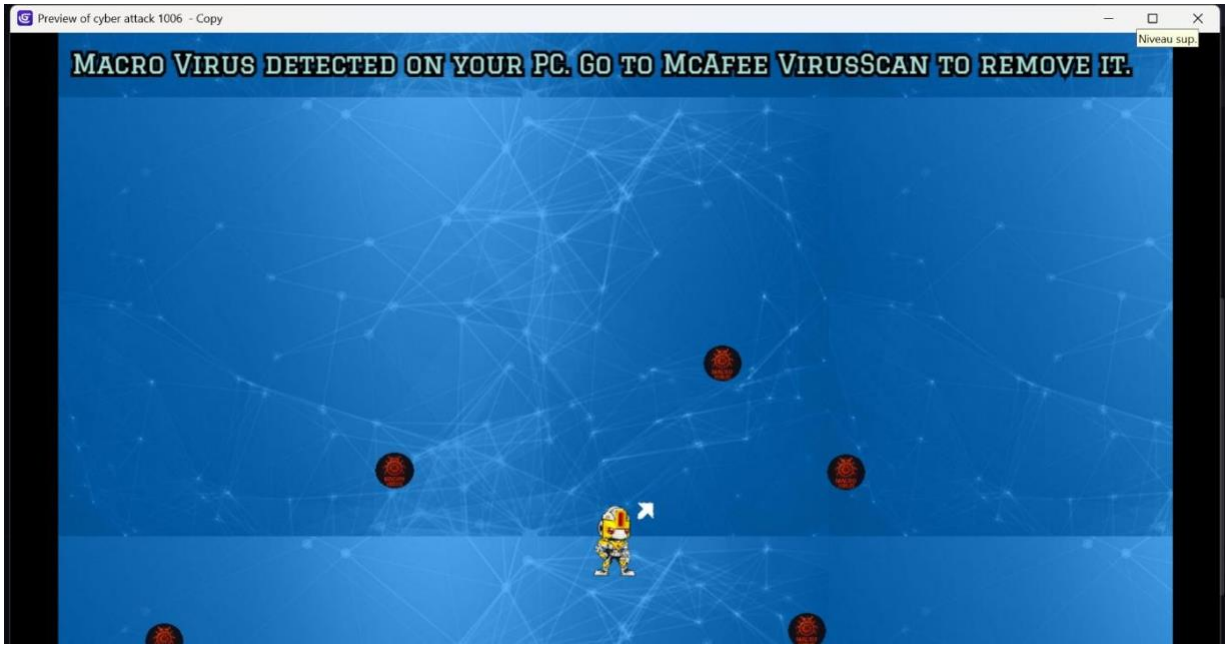

Figure 19 : Level 3 - Virus Chase

This image shows the game screen at level three depicting a virus attack scenario. The central robot character is surrounded by several viruses. A warning message at the top directs the player to find an antivirus until the viruses disappear.

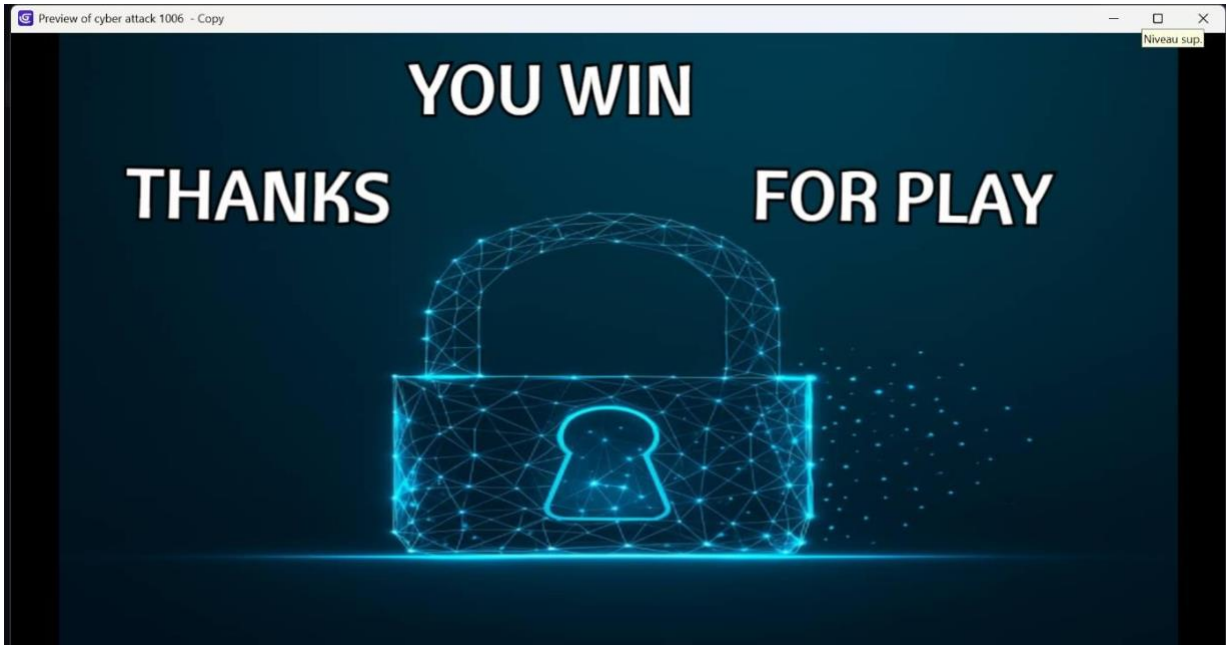

Figure 20 : Victory Screen of the Game

Game completion screen, indicating a successful outcome. The phrase "You won" is prominently displayed along with the phrase "Thank you for playing." A large, glowing lock icon, designed with connected lines and dots, symbolizes cybersecurity and successful protection.

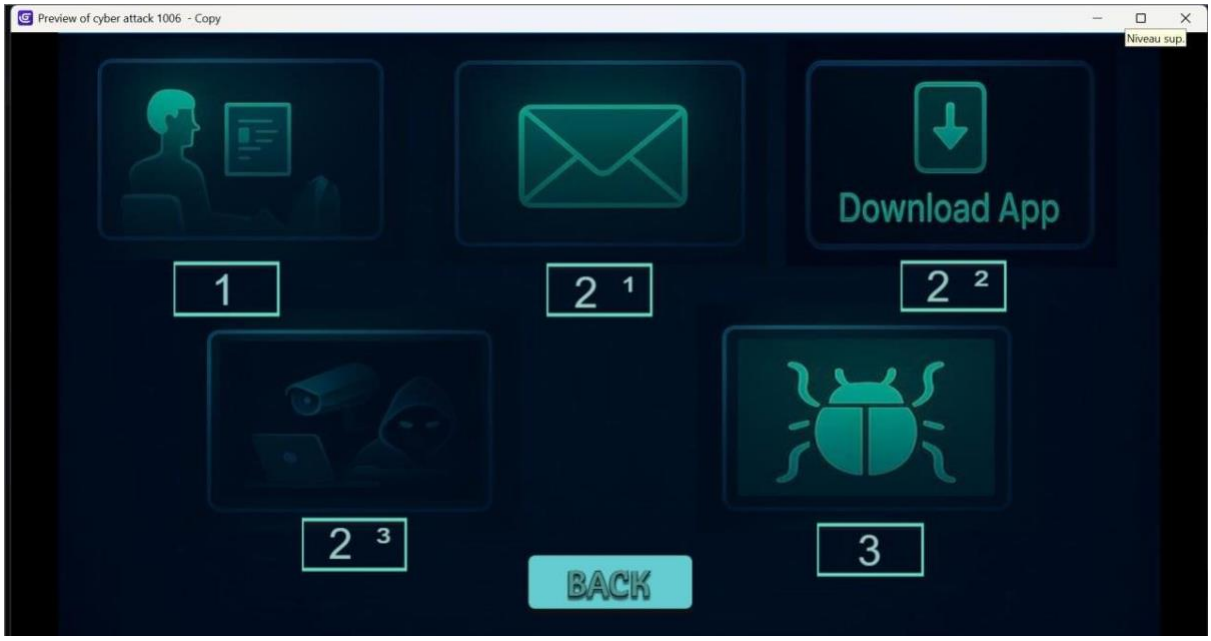

Figure 21: Levels Overview

Display a game level selection menu that features five unique icons, each representing a specific unit or level, accompanied by numerical labels. A 'Back' button is positioned at the bottom for easy navigation.

IV.4) Conclusion

This chapter presented the technical and practical aspects of designing and developing the educational serious game. It explained the tools and methods used in its development, along with the key features that make it an effective interactive platform for cybersecurity education. The chapter also demonstrated user interaction scenarios, showing how learners engage with the game through screenshots that illustrate the different stages of the gaming experience.

This implementation phase represents a critical step in achieving the project's educational objectives, marking the transition from theoretical design to a functional educational tool that can be evaluated and improved in future research based on user needs and feedback.

The successful development of this prototype demonstrates the practical application of serious gaming approaches in cybersecurity education, contributing to innovative teaching methods in technical fields.

Conclusion

The rapid evolution of cybersecurity threats in this digital age necessitates an educational approach that transcends traditional training models. This study addressed this challenge by developing a serious game specifically designed for cybersecurity education, demonstrating the transformative potential of game-based learning in technical education.

Through theoretical analysis and practical application, this study has demonstrated that serious games represent a qualitative shift in cybersecurity pedagogy, particularly for beginners. These advanced educational environments effectively integrate interaction and educational rigor, addressing the limitations of traditional methodologies. The research framework confirmed three key hypotheses: enhancing learner interaction leading to deeper understanding of concepts, providing risk-free educational environments that allow experimentation without compromising systems, and enabling the effective transfer of skills from virtual scenarios to real-world cybersecurity applications.

The results extend beyond cybersecurity education to contribute to the discussion of digital pedagogy. The developed methodology provides a replicable framework for creating serious games across technical disciplines, while the defined success metrics offer criteria for evaluating the effectiveness of educational games.

The main objectives achieved through this research include creating a comprehensive theoretical framework for serious games in cybersecurity, developing a functional prototype for beginners, and establishing metrics for evaluating educational effectiveness. While these achievements demonstrate a promising theoretical foundation, our future goals focus on conducting extensive testing with diverse groups of beginner learners to verify the educational effectiveness of the game, measuring actual learning outcomes, and refining the game mechanics based on user feedback.

As cyber threats continue to evolve, this study demonstrates that serious games offer effective and adaptable solutions while maintaining educational effectiveness for novice learners. The established foundations indicate that the future of cybersecurity education lies in integrating game-based approaches with traditional methods to create comprehensive educational experiences specifically designed for beginners.

In conclusion, this study successfully demonstrates that serious games transcend being mere modern educational tools to become essential means of preparing the future workforce in cybersecurity, providing a sustainable solution to the ongoing gap in specialized skills.

References

[1] Cisco Networking Academy. (2025, February 13). *Introduction to cybersecurity*. https://netacad.com/courses/introduction-to-cybersecurity

[2] AAG-IT. (n.d.). *The latest cyber crime statistics*. https://aag-it.com/the-latest-cyber-crime-statistics

[3] Bada, A., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *Computers & Security, 87*, 101568. https://doi.org/10.1016/j.cose.2019.101568

[4] Abt, C. C. (1975). *Serious games*. Viking Compass.

[5] Breuer, J. S., & Bente, G. (2010, April). Why so serious? On the relation of serious games and learning. *EJCGC, 4*(1), 7-24.

[6] Michael, D., & Chen, S. (2006). *Serious games: Games that educate, train and inform*. Thomson Course Technology.

[7] Zyda, M. (2005). From visual simulation to virtual reality to games. *Computer, 38*(9), 25-32. https://doi.org/10.1109/MC.2005.297

[8] *(Missing reference—please provide full citation or remove [8].)*

[9] Becker, K. (2021, February). What's the difference between gamification, serious games, educational games, and game-based learning? *Academia Letters*. https://doi.org/10.20935/AL209

[10] Tips and Trends. (2015, Spring). *Spring 2015*. *(Incomplete – please specify document title or source)*

[11] Alvarez, J. (n.d.). *Histoire du serious game*. *(Add URL if available)*

[12] Drimify. (n.d.). *The history of serious games*. https://drimify.com/en/resources/serious-games-history/

[13] Djaouti, D., Alvarez, J., & Jessel, J.-P. (2008). Classifying serious games: The G/P/S model. [Conference presentation]. *(Add event and location if known)*

[14] Marfisi-Schottman, I., Labat, J.-M., & Carron, T. (2016). A comprehensive taxonomy for serious games. *International Journal of Computer Games Technology, 2016*, Article 6891345. https://doi.org/10.1155/2016/6891345

[15] Michaud, L., & Alvarez, J. (2008). Serious games: Advergaming, edugaming, training. In *Understanding the digital world*. IDATE.

[16] MIT Scheller Teacher Education Program. (2025, February 13). https://education.mit.edu/

[17] Playmobil®. (2025, February 13). https://www.playmobil.com/de-de/

[18] *(Missing reference – please provide source for [18].)*

[19] Les Échos. (n.d.). *Business Les Échos*. http://business.lesechos.fr/

[20] Neoloji. (n.d.). *Edutainment*. https://www.neoloji.fr/edutainment

[21] Sea Monster. (n.d.). *Gamification in education: The most useful educational innovation in ages*. https://www.seamonster.digital/articles/gamification-in-education-the-most-useful-educational-innovation-in-ages
[22] Duolingo. (n.d.). https://fr.duolingo.com/
[23] HMH & Class craft. (n.d.). https://www.hmhco.com/programs/classcraft
[24] Redis. (n.d.). *Leaderboards solutions*. https://redis.io/solutions/leaderboards/
[25] My Mooc. (n.d.). *Cours sur Coursera*. https://www.mymooc.com/fr/conceptor/coursera/
[26] Landers, R. N., Armstrong, M. B., & Collmus, A. B. (2017). How to use game elements to enhance learning: Applications of the theory of gamified learning. In M. Ma, A. Oikonomou, & L. C. Jain (Eds.), *Serious games and edutainment applications* (Vol. 2, pp. 457–483). Springer. https://doi.org/10.1007/978-3-319-51645-5_21
[27] Fullerton, T. (n.d.). Chapter 2: The structure of games. In *Game design workshop: A playcentric approach to creating innovative games*. *(Add publisher and year)*
[28] Qiao, S., Yeung, S. S.-S., Shen, X., Leung, J. K. L., Ng, D. T. K., & Chu, S. K. W. (2024). How competitive, cooperative, and collaborative gamification impacts student learning and engagement. *Language Learning & Technology, 28*(1), 1–19.
[29] Lameras, P., Arnab, S., Dunwell, I., Stewart, C., Clarke, S., & Petridis, P. (2017). Essential features of serious games design in higher education: Linking learning attributes to game mechanics. *British Journal of Educational Technology.*
[30] Alvarez, J. (2007). *Du jeu vidéo au serious game: Approches culturelle, pragmatique et formelle*. Unpublished. https://doi.org/10.13140/RG.2.1.2527.1767
[31] Serious Game Design Guidelines. (n.d.). *(Missing publisher or source – please complete)*
[32] Thot Cursus. (2025, February 21). *Les qualités fondamentales d'un bon jeu sérieux*. https://cursus.edu/fr/8252/les-qualites-fondamentales-dun-bon-jeu-serieux
[33] 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* (Vol. 9970, pp. 265–283). Springer. https://doi.org/10.1007/978-3-319-46152-6_11
[34] Kirkpatrick, D. L., & Kirkpatrick, J. D. (2006). *Evaluating training programs: The four levels* (3rd ed.). Berrett-Koehler.
[35] Mitgutsch, K., & Alvarado, N. (2012). Purposeful by design?: A serious game design assessment framework. In *Proceedings of the International Conference on the Foundations of Digital Games (FDG 2012)* (pp. 121–128). ACM.
[36] Advances in Human-Computer Interaction. (2012). *Hindawi Publishing Corporation*, 2012, Article ID 369637. https://doi.org/10.1155/2012/369637
[37] Macleod, M., & Rengger, R. (1993). The development of DRUM: A software tool for video-assisted usability evaluation. In *Proceedings of the 5th International Conference on Human-Computer Interaction (HCI '93)* (pp. 293–309).

[38] Virzi, R. A. (1992). Refining the test phase of usability evaluation: How many subjects is enough? *Human Factors, 34*(4), 457-468. https://doi.org/10.1177/001872089203400407

[39] Nielsen, J., & Landauer, T. K. (1993). A mathematical model of the finding of usability problems. In *Proceedings of the INTERACT'93 and CHI'93 Conference on Human Factors in Computing Systems* (pp. 206-213). ACM. https://doi.org/10.1145/169059.169166

[40] Kessner, M., Wood, J., Dillon, R. F., & West, R. L. (2001). On the reliability of usability testing. In *Proceedings of the Extended Abstracts on Human Factors in Computing Systems (CHI '01)* (p. 97). ACM.

[41] Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering, 7*(11). https://doi.org/10.17148/IJARCCE.2018.71150

[42] Bay, M. (2016). What is cybersecurity? In search of an encompassing definition for the post-Snowden era. *French Journal for Media Research, 6*, 1-8. https://frenchjournalformediaresearch.com/lodel/index.php?id=692

[43] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-115. https://doi.org/10.1016/j.cose.2013.04.004

[44] Yee, C. K., & Zolkapli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education, 8*(2), 34-42. https://doi.org/10.37134/jictie.vol8.2.4.2021

[45] Universal Training. (n.d.). *What are the domains of cyber security?* Retrieved April 17, 2025, from https://universaltraining.ca/what-are-the-domains-of-cyber-security/

[46] Pande, D. J. (n.d.). *Introduction to cyber security*. *(Add publisher if available)*

[47] Whitman, M. E., & Mattord, H. J. (2018). *Principles of information security* (6th ed.). Cengage Learning.

[48] Cisco Networking Academy. (n.d.). *Introduction to cybersecurity*. Retrieved February 13, 2025, from https://netacad.com/courses/introduction-to-cybersecurity

[49] Fortinet. (n.d.). *What is AAA security?* Retrieved April 17, 2025, from https://www.fortinet.com/resources/cyberglossary/aaa-security

[50] https://codeparrot.ai/blogs/what-is-gdevelop-a-beginner-friendly-open-source-game-engine