electronics

MDPI

Article

CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness

Rania Hodhod [1,*], Harlie Hardage [1], Safia Abbas [2] and Eman Abdullah Aldakheel [3]

[1] TSYS School of Computer Science, Turner College of Business, Columbus State University, Columbus, GA 31907, USA; hardage_harlie@columbusstate.edu
[2] Department of Computer Science, Faculty of Computer and Information Sciences, Ain Shams University, Cairo 11566, Egypt; safia_abbas@cis.asu.edu.eg
[3] Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh 11671, Saudi Arabia; eaaldakheel@pnu.edu.sa
* Correspondence: hodhod_rania@columbusstate.edu

Abstract: The lack of cybersecurity awareness among everyday users is a significant issue that can have detrimental effects on individuals and organizations alike. Traditional training methods such as slideshows and presentations have proven to be ineffective and can cause trainees to feel overwhelmed, overloaded, confused, or bored. To address this issue, the development of an adaptive serious game that teaches cybersecurity in an effective, engaging, and personalized manner is proposed. Serious games provide an immersive and simulated experience that can help users determine how they might act in real-life scenarios. However, existing cybersecurity serious games often measure effectiveness outside of the game using surveys, tests, and interviews, which can lessen immersion and the simulated experience. Therefore, measuring improvement within the game itself can provide more meaningful data and derive truer conclusions about the usefulness of serious games in teaching cybersecurity. The goal of this research study is to develop such a game and measure its effectiveness in a way that can inform future cybersecurity training programs. By providing an engaging and personalized experience, serious games can improve cybersecurity awareness and reduce the risk of cyber threats. The results show that 79% of the participants admitted that they learned new things by playing the game, 84% said that they were engaged by the background story, 68% agreed that they had fun while playing the game, and 84% would recommend the game to others.

Keywords: serious games; cybersecurity education; user modeling; certainty factor

check for updates

Citation: Hodhod, R.; Hardage, H.; Abbas, S.; Aldakheel, E.A. CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness. *Electronics* **2023**, *12*, 3544. https://doi.org/10.3390/electronics12173544

Academic Editor: George A. Tsihrintzis

Received: 29 May 2023
Revised: 12 August 2023
Accepted: 18 August 2023
Published: 22 August 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Cybersecurity is crucial in today's digital age, and end users play a significant role in ensuring the security of their computer systems and the Internet. Studies have shown that humans are the weakest link of any security infrastructure [1,2]; according to the data breach investigation report, the human element is implicated in 74% of all breaches, where individuals are involved through errors, misuse of privileges, use of stolen credentials, or social engineering tactics [3]. External actors are responsible for 83% of breaches, and the primary motive behind these attacks remains predominantly financial, accounting for 95% of breaches. Attackers typically gain access to organizations through three primary methods: stolen credentials, phishing, and exploiting vulnerabilities, which raises the need for effective training methods that can address this weakness.

Conventional training methods like slideshows and presentations often fall short in effectively achieving their learning objectives as they may fail to engage users effectively and can lead to negative predispositions towards cybersecurity, thus achieving limited success in instigating lasting changes in behavior [4]. Moreover, traditional training methods are often insufficient in effectively mitigating cyber-related human errors and losses. This is partially due to the fact that the issue is not adequately defined and reinforced through these methods [5]. In recent decades, various innovative security methodologies and tools have emerged, such as web-based adaptive learning, video interaction, and serious games, in various fields. Serious games are games that are designed for a primary purpose other than pure entertainment, offering an exciting and interactive alternative to traditional training methods. They introduce gamification to promote behavioral changes and situational awareness in many fields, such as computer programming [6], conflict resolution [7], and health exercise [8], but are relatively new to the cybersecurity field.

In the context of cybersecurity, serious games can be used to simulate real-world scenarios and provide learners with hands-on experience in identifying and responding to cyber threats. However, current serious games' effectiveness in measuring behavioral changes and knowledge retention is a concern [9]. Many games rely on pre- and post-surveys or tests to determine users' knowledge levels, which can diminish the game's effectiveness since surveys may not elicit accurate and honest responses from participants, as they might feel disinclined to provide answers that paint them unfavorably or may lack full awareness of their reasons for each response due to memory limitations or even boredom. Adaptive serious games have offered a solution to this issue by personalizing the game to the user's knowledge level and measuring their progress and refinement of their skill set within the game itself [10], allowing for a non-disruptive learning experience with the user's knowledge being evaluated while they actively interact with the game.

Given the significant role of human factors in cybersecurity incidents, it is crucial to prioritize cybersecurity education and training for individuals. Serious games that utilize learning theories can simulate learning-related behavior and can provide a means to enhance the effectiveness of cybersecurity education, making it more engaging, personalized, and interactive for learners. This paper presents CyberHero, an adaptive serious game that considers learning theories and gamification aspects to effectively improve cybersecurity awareness and accurately measure users' knowledge and behavioral changes in a non-disruptive manner while the user is interacting with the game. The paper is organized as follows: The next section summarizes the popular learning theories in cybersecurity education. Section 3 describes the methodology followed in this study. Section 4 presents the architecture of the cybersecurity game. Section 5 discusses the results achieved. Finally, Section 6 presents the conclusion of this work.

2. Learning Theories in Cybersecurity Education

In "Advancing Cybersecurity Education", Dark [11] explains that learning theories "attempt to describe how information is absorbed, processed, retained, and recalled during and after learning". Five commonly applied learning theories (behaviorism, cognitivism, humanism, connectivism, and constructivism) were assessed to understand these theories to teach subject matters. In this section, we will discuss how these learning theories are applied specifically to cybersecurity education and how effective these methods can be at building a strong understanding of security practices and behaviors.

Behaviorism is a learning theory that focuses on the concept that behaviors are learned from environmental interactions and experiences [12]. It defines successful learning as demonstrating the correct response when presented with an environmental stimulus [13]. There is an emphasis on repetition, motivation, and reinforcement to create an automatic behavioral response [12]. The behaviorist learning theory may not be suitable for cybersecurity education, particularly in the context of phishing awareness training. The emphasis on repetition, motivation, and reinforcement to create an automatic behavioral response may lead to individuals feeling overconfident in their abilities and neglecting to continue their training. Furthermore, the rule-based approach of behaviorism may not account for the fluidity and variability of potential threats in the rapidly changing cybersecurity landscape. Lastly, behaviorism does not acknowledge the cognitive thought process involved in responding to a threat, which may result in individuals failing to allocate attention to critical tasks and falling victim to an attack.

Cognitivism is a learning theory similar to behaviorism as it highlights the significance of environmental conditions in facilitating the learning process. The primary focus of the cognitive approach is centered around transforming the learner's approach by motivating them to adopt suitable learning strategies [14]; this involves instructional explanations, demonstrations, illustrative instances, and matched non-examples, all of which are deemed essential for guiding students' learning. Likewise, there's an emphasis on the importance of practicing with corrective feedback. Until this juncture, there appears to be a minimal disparity between these two theories. However, the distinction arises in how the learner's "active" involvement is perceived. Cognitive theories propose that learning outcomes within an instructional context cannot be fully attributed to environmental cues and instructional elements alone.

Humanism is a learning theory that emphasizes the individual and their personal growth and development. It is centered around the belief that individuals have the capacity for self-actualization and that education should focus on fulfilling that potential [15]. Humanistic learning is learner-centered, meaning that the learner's needs and interests are the focus of the educational experience. The teacher's role is to facilitate the learning process rather than dictate it, and to provide support and guidance to the learner. In the context of cybersecurity education, humanism can be applied by creating personalized learning experiences for each learner. This can include allowing learners to choose their own topics of study or allowing them to learn at their own pace. By creating a learner-centered environment, individuals may feel more invested in their education and more motivated to learn. This approach can also promote critical thinking skills and encourage learners to take responsibility for their own learning. However, humanism may not be the most effective approach for cybersecurity education on its own. While personalized learning experiences can be beneficial, they may not provide the necessary structure and guidance needed for complex topics and require a certain level of expertise. Therefore, humanism may be best used with other learning theories, such as cognitivism, which focuses on internal mental processes that occur to create meaningful knowledge, and constructivism, which focuses on the learner's active construction of their knowledge and understanding of reality through their experiences and interactions. to ensure that students develop a well-rounded understanding of cybersecurity practices and behaviors.

Connectivism learning theory emphasizes the importance of technology and networking in learning. According to [16], the abundance of information available in today's digital age requires learners to develop skills in filtering, synthesizing, and making connections between various sources of information. Connectivism places a strong emphasis on the importance of networking, collaboration, and technology in the learning process, recognizing that the acquisition and application of knowledge in today's world requires a different approach than traditional learning theories. The concept of "currency" in connectivism emphasizes the importance of staying up to date with current information and recognizing the changing nature of knowledge in today's rapidly evolving world. Decision making is also viewed as a learning process, with learners continually evaluating and reevaluating information to make informed decisions. In the context of cybersecurity education, connectivism can be particularly useful. As cybersecurity education is often conducted online or via e-learning, individuals unintentionally utilize the principles of connectivism in acquiring knowledge about security-related topics. However, it is important to note that connectivism does not eliminate the need for cybersecurity training and education. While individuals can retrieve cybersecurity information on demand, they must still be able to recognize potential threats in a situation and respond appropriately, which requires situational awareness and critical thinking skills. Therefore, cybersecurity training and education remain essential for developing these skills and ensuring individuals are prepared to handle security incidents effectively.

Constructivism emphasizes that individuals create their own understanding of knowledge and reality and that learning is a personal and contextual process [17]. The theory suggests that individuals are constantly learning how to learn and that social interactions play a vital role in shaping their learning experiences. In the context of cybersecurity education, constructivism provides a promising approach to teaching and learning. Cybersecurity is an ever-evolving field that requires individuals to have a deep understanding of the subject matter to effectively utilize their knowledge in a meaningful way. The constructivist approach allows individuals to connect their prior knowledge and experiences to new information, which can lead to a more thorough and dynamic understanding of the subject matter.

In summary, the above learning theories can be applied to cybersecurity education in many ways. For example, behaviorism can be used to teach specific security procedures and behaviors, while cognitivism can be used to help learners understand the underlying concepts and principles behind security practices. Humanism can be used to encourage learners to explore their personal motivations and values related to security, and connectivism can be used to help learners connect with other security professionals and resources online. Finally, constructivism can be used to encourage learners to actively engage with security concepts and practices and to construct their own understanding of the subject matter.

Since constructivism suggests that learners construct their knowledge and understanding through interaction with the environment rather than passively receiving information, constructivism seems to be the most suitable learning theory to be considered while designing and developing a serious game for cybersecurity training; it can help learners to develop critical thinking and problem-solving skills, as they navigate through simulated scenarios and learn to make decisions based on their understanding of cybersecurity concepts in a safe and controlled environment, gaining practical experience that is transferable to real-world situations.

3. Related Works

Story-based serious games were developed to immerse the players and allow for an engaging learning experience. Cyber Attack [18] is a story-driven educational hacking game that utilizes various elements, including progression, rewards, rules, and competition, to improve players' involvement. The game has time constraints to complete the tasks and utilizes scoring mechanisms such as ethics levels, points progression, and leaderboards. Passworld [19] is a scenario-based serious game for promoting password awareness and diversity in an enterprise. The game uses both Bloom's Taxonomy and the Six "I" Framework of Serious Game Design. Through these scenarios, users were taught best practices for creating strong passwords and how to identify and avoid common password pitfalls. Along the same line, Cyber Air-Strike [20] is a web-based 2D game created using the Buildbox game engine and utilized Bloom's Taxonomy to teach cybersecurity awareness. The game covers various cybersecurity topics such as malware, phishing, password hacking, viruses, and unauthorized data. The game has not been tested with actual players. Make My Phone Secure! [21] is a gamified approach that uses scenarios to educate users about cell phone permission security. The findings concluded that the approach was fun and informative.

Unity 3D game engine was utilized by many researchers to develop immersing and engaging environments to teach cybersecurity. For example, two decision-making games were found; one is What.Hack [22], which aims to teach students anti-phishing methods. The game was able to enhance players' precision in identifying upcoming threats by 36.7%. And the second is Cyber Detective [23], a mobile game that aims to teach cybersecurity awareness using mini-games. After each mini-game, the player's decisions are explained and corrected if necessary, promoting cybersecurity literacy. Security Game (DdSG) [24] is another single-player game that was also created using the Unity 3D game engine to teach novice developers how to select conventional mitigation strategies and patterns to defend against different security attack scenarios. Lastly, the DDoS Attack game [25] was created to teach students about DDoS attacks. The game has the flexibility to be deployed on different platforms. Other game engines like the Blender Game Engine were used to create the Cryptography 3D escape game [26] to teach students about computer security and cryptography. The results showed that the game successfully increased their understanding of cryptographic concepts, and the students enjoyed the game.

Other game engines were also used to create serious games for cybersecurity; the Cryptography 3D escape game [26] was created using Blender Game Engine to teach students about computer security and cryptography. The results showed that the game successfully increased their understanding of cryptographic concepts, and the students enjoyed the game. Quasim [27] is a gamified intelligent tutoring system built using the Unreal 4 Engine to teach quantum cryptography. The results showed that the scores of the students increased after gameplay, indicating that the game was effective in teaching quantum cryptography.

The game stores user data on an online database server and displays progress on a leaderboard. Evaluation results indicate that users improved their post-test scores and were generally satisfied with the game, while Bird's Life [28] was designed for college-level students and general individuals to gain knowledge about phishing attacks. The results showed a significant improvement in their understanding of phishing attacks after playing the game.

Be Aware! [29] is an augmented reality game for Android that aims to teach about compromised ATMs by requiring users to identify the uncompromised ATM among the three displayed on the screen using AR technology. (Smart) Watch Out! [30] is an online simulation that aims to teach security and privacy on smartwatch devices. Researchers investigated if protective behavior could be inspired by a smartwatch simulation or PC application. The results showed that the treatment group's protective behavior became significantly more frequent, while SSETGami [31] is a gamification approach developed using HTML5 to teach students how to create secure web applications.

What Can Go Wrong? [32] is a decision-making game designed for desktops that uses humor to increase awareness of privacy and security concerns on mobile devices. The game covers topics such as screen locks, phishing attacks, malicious Android Packages (APKs), and app permissions.

The Security Requirement Education Game (SREG) [33] is a multiplayer card game designed to improve cybersecurity awareness using a game-based technique combined with security requirement engineering concepts. The game was evaluated and found to be helpful for players to understand security attacks and vulnerabilities. Google's Interland [34] is a 3D game that teaches online safety to second- to sixth-grade children. The game covers topics like anti-bullying, strong passwords, being careful what you post online, and phishing detection. The Internet Hero [35] is a game designed to teach children aged nine to twelve the technical and social basis of using the Internet, including emails, malicious programs, social networks, and connection types.

The Anti-Phishing Educational Game [36] aims to enhance an individual's phishing threat avoidance behavior. The game is designed to educate users on how to distinguish between legitimate and fraudulent URLs (Uniform Resource Locators). CyberAware is a mobile serious game based on the ARCS model and designed for K6 educators for cybersecurity education and awareness [37]. CyberAware is made up of a series of minigames that cover topics such as firewalls, antivirus, software updates, and spam filtering emails. On the other hand, the Attacker-Centric Gamified Approach [36] aims to teach workers and leaders cybersecurity skills using eight attacker types and six entrepreneurial views to create avatars for the game. The effectiveness of this approach has not yet been evaluated through testing.

CounterMeasures [38] is a single-player game that teaches about computer security methods related to buffer overflows, scanning systems, and string format vulnerabilities. It is worth noting that the game was found to be able to teach security concepts in half the time compared to reading. The Internet security game by Next Generation Security (NGSEC) systems [39] is an online game designed to teach network security principles. After evaluation, researchers concluded that online labs increased students' understanding of network security. The Security Protocol Game [40] is a group activity that uses pen and paper, envelopes, and printed game pieces to help students understand the design and operation of protocols for secure data communications. The game allows students to reproduce a range of computer network security protocols and explores possible attacks against them, such as SSL and Pretty Good Privacy.

Some of the drawbacks encountered in existing games include small testing groups and poor metrics and testing mechanisms, which can question the validity of the game, such as the use of extrinsic evaluation. Results from the games are often unclear or unrelated to the users' improvements or awareness of cybersecurity topics [9]. Additionally, information overload and the repetition of information can cause users to lose interest in the game. Web-based applications can also be problematic for users without Internet access. Finally, the lack of instructional components may result in users not learning the topic, and the excessive focus on scoring may also hinder the learning process [41]. On the other hand, personalization and adaptivity in serious games have proven to motivate the players [8], which is currently missing from the existing games. Moreover, by incorporating feedback and instructional strategies into game design, serious games have the potential to engage learners and facilitate long-term learning outcomes, in addition to creating a better learning environment by providing instant feedback to motivate users.

4. CyberHero: A Serious Game for Cybersecurity Training

The creation process for the serious game, CyberHero, is built upon the Stenmap framework developed by Sten Mäses and his team in 2018. Stenmap is a framework designed for computer simulations in the field of cybersecurity to assess individuals' skill sets [42]. Unlike other approaches that prioritize winning or completion, the Stenmap model places emphasis on understanding the individual's competencies. It was specifically tailored to measure specific skills within the cybersecurity domain. The Stenmap approach follows a 10-step process, as illustrated in Figure 1.

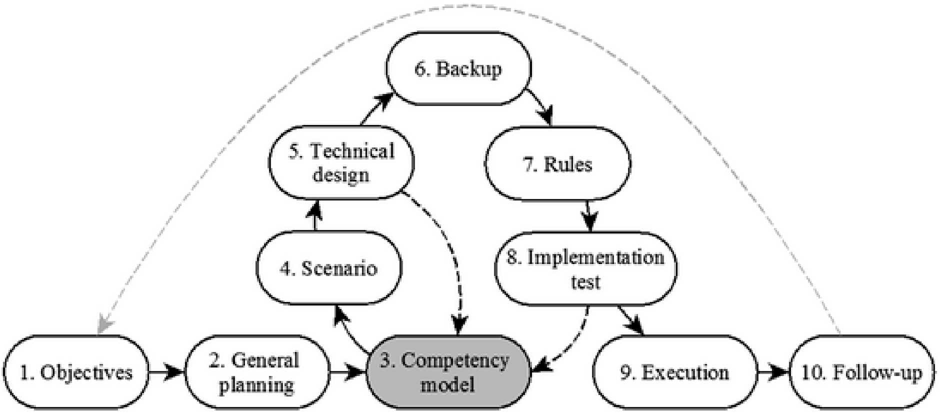


Figure 1. Stenmap 10-step process for designing and implementing a cybersecurity exercise (from Stenmap Framework for Evaluating Cybersecurity Related Skills Based on Computer Simulations.

The architecture of CyberHero comprised two main components: an intelligent tutoring system and a narrative manager. At the core of CyberHero's architecture, the intelligent tutoring system has four models (domain model, user/player model, pedagogical model, and interface model) that interact together, as shown in Figure 2, to provide a seamless storyline with personalized teaching moments. The following subsections describe these models in detail.

The other main component of CyberHero is a narrative manager that drives the development of the overall story using an interactive branching storyline (see Figure 3) to educate users about cybersecurity by allowing the users to experience the consequences of their actions in the digital world. The framework followed to create the game narrative is inspired by [10] to ensure the scenarios are interesting, influential, and hold relevant but intriguing meanings to the players.

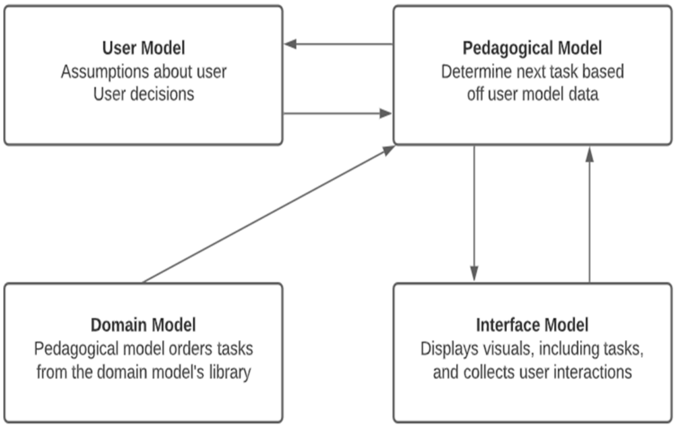
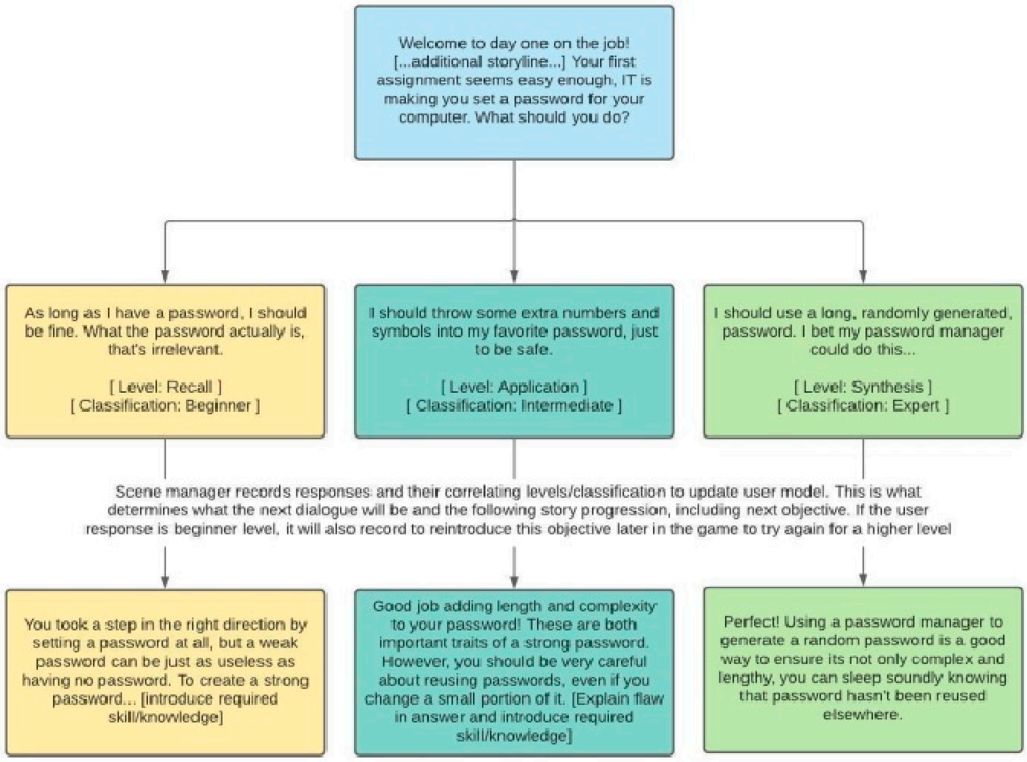

User Model
Assumptions about user
User decisions
Pedagogical Model
Determine next task based off user model data
Domain Model
Pedagogical model orders tasks from the domain model's library
Interface Model
Displays visuals, including tasks, and collects user interactions

Figure 2. Intelligent tutoring system in CyberHero.



Welcome to day one on the job! [...additional storyline...] Your first assignment seems easy enough, IT is making you set a password for your computer. What should you do?

As long as I have a password, I should be fine. What the password actually is, that's irrelevant.

[Level: Recall]
[Classification: Beginner]

I should throw some extra numbers and symbols into my favorite password, just to be safe.

[Level: Application]
[Classification: Intermediate]

I should use a long, randomly generated, password. I bet my password manager could do this...

[Level: Synthesis]
[Classification: Expert]

Scene manager records responses and their correlating levels/classification to update user model. This is what determines what the next dialogue will be and the following story progression, including next objective. If the user response is beginner level, it will also record to reintroduce this objective later in the game to try again for a higher level

You took a step in the right direction by setting a password at all, but a weak password can be just as useless as having no password. To create a strong password... [introduce required skill/knowledge]

Good job adding length and complexity to your password! These are both important traits of a strong password. However, you should be very careful about reusing passwords, even if you change a small portion of it. [Explain flaw in answer and introduce required skill/knowledge]

Perfect! Using a password manager to generate a random password is a good way to ensure its not only complex and lengthy, you can sleep soundly knowing that password hasn't been reused elsewhere.

Figure 3. Branched interactive narrative in CyberHero.

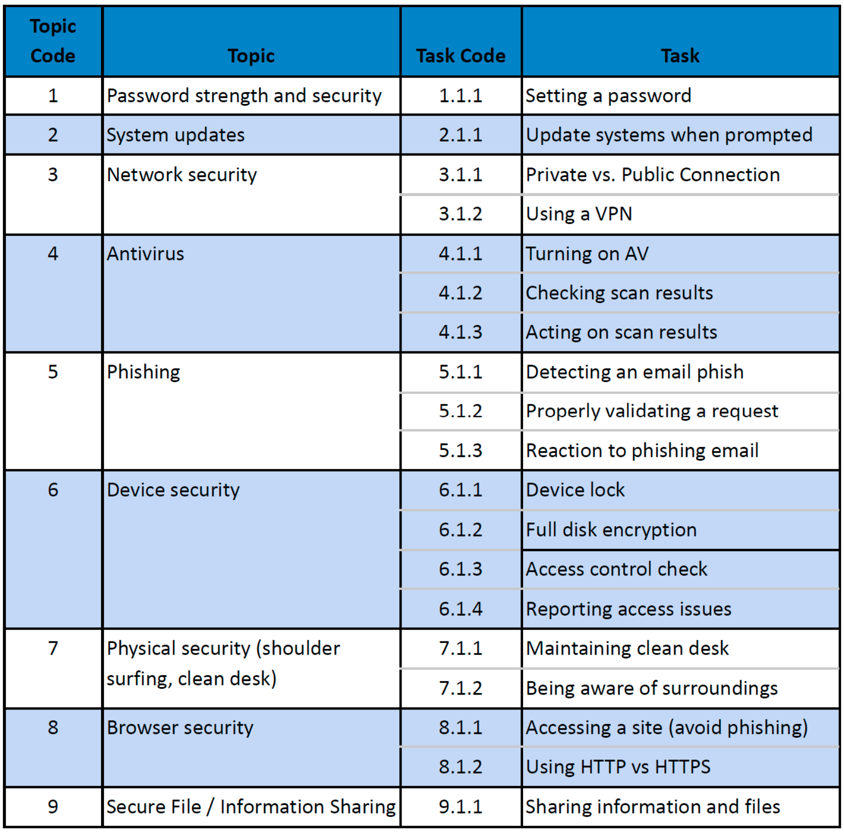
By showing players how their choices can have a long-term impact on the storyline and the consequences that can arise from poor cybersecurity practices, CyberHero helps players develop a deeper understanding of the importance of cybersecurity in their daily lives.

The Super Mario Effect is a concept proposed by Mark Rober [43] based on his experiment with a coding game. The experiment showed that participants who were not penalized for making mistakes had higher success rates and tried more times before succeeding than those who were penalized. The concept is based on the idea that when playing Super Mario games, players are motivated to keep trying and learning from their mistakes because they focus on the goal of rescuing Princess Peach instead of the obstacles and challenges they face along the way. In general, the Super Mario Effect highlights the importance of creating a positive learning environment where failure is not seen as a negative outcome but rather as an opportunity to learn and improve, which was considered in the design of CyberHero; by focusing on the goal and staying motivated, learners are more likely to persevere and learn more effectively.

4.1. Domain Model in CyberHero

The domain model in CyberHero contains all the data related to the game's concepts, topics, and tasks. The game tasks were influenced by various methodologies. Initially, the learning outcomes for each task were defined based on the National Initiative for Cybersecurity Education (NICE) framework provided by the National Institute of Standards and Technology (NIST) [44], which is a comprehensive resource for identifying and standardizing cybersecurity education and training. In addition to these frameworks, CyberHero covers topics that are relevant and accessible to the average end user/player. This consideration included both the complexity of the topics and their practical relevance in everyday life. To further refine the scope, a learning plan developed by Project Lead the Way was followed, which aligns with the NICE guidelines. The objective was to cover essential cybersecurity topics while considering the expectations and capabilities of an average end user, considering both complexity and relevance.

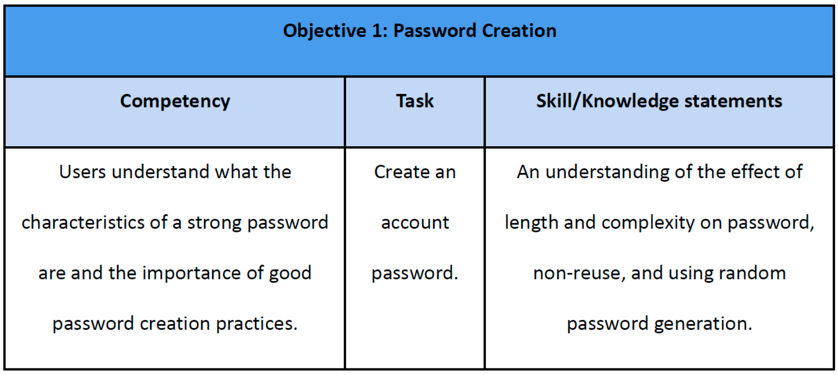
As a result, nine competencies were identified: password security, system updates, network security, antivirus protection, phishing awareness, device security, physical security, browser security, and secure file and information sharing. Each of these competencies requires the inclusion of specific tasks that users must complete. This necessitated the creation of at least nine tasks, with two variants available for each task—one for the initial trial and another for retesting if the user needed it. The second task was not an exact repetition but rather a similar task addressing the same competency. An outline of the tasks is summarized in Figure 4.



Topic Code	Topic	Task Code	Task
1	Password strength and security	1.1.1	Setting a password
2	System updates	2.1.1	Update systems when prompted
3	Network security	3.1.1	Private vs. Public Connection
		3.1.2	Using a VPN
4	Antivirus	4.1.1	Turning on AV
		4.1.2	Checking scan results
		4.1.3	Acting on scan results
5	Phishing	5.1.1	Detecting an email phish
		5.1.2	Properly validating a request
		5.1.3	Reaction to phishing email
6	Device security	6.1.1	Device lock
		6.1.2	Full disk encryption
		6.1.3	Access control check
		6.1.4	Reporting access issues
7	Physical security (shoulder surfing, clean desk)	7.1.1	Maintaining clean desk
		7.1.2	Being aware of surroundings
8	Browser security	8.1.1	Accessing a site (avoid phishing)
		8.1.2	Using HTTP vs HTTPS
9	Secure File / Information Sharing	9.1.1	Sharing information and files

Figure 4. Task outline. Task code is {topic}. {version}. {task}, with each task having two versions.

Each competency and corresponding tasks are mapped to the corresponding skill/knowledge in NICE. An example of how the password creation competency and one of the tasks are mapped to the corresponding skill/knowledge is shown in Figure 5.



Objective 1: Password Creation		
Competency	**Task**	**Skill/Knowledge statements**
Users understand what the characteristics of a strong password are and the importance of good password creation practices.	Create an account password.	An understanding of the effect of length and complexity on password, non-reuse, and using random password generation.

Figure 5. Example mapping of a competency to a NICE skill/knowledge.

The domain model has a pre-defined set of tasks (see Figure 6) that players can complete to demonstrate their understanding of each competency based on their progress in the game. The game tasks were influenced by a few different methodologies. First, the task's learning outcomes were defined using NIST's NICE framework, as discussed in a previous section. The scope was narrowed down a bit by following a learning plan created by Project Lead the Way, which maps back to the NICE guidelines. The goal was to cover topics that are vital to cybersecurity but also to focus on topics that fall into what is expected of your average end user, considering both complexity and relevance. The tasks with a dashed edge are the retest tasks, which will not show up if the player scores expert on the first version of that task. One example of the alignment shown in Figure 3 is Tasks 3.1.1 and 3.1.2. These two tasks, when completed at an expert level, will satisfy the network security competency. Another example is Task 4.1.1, which is related to antivirus competency, and Task 5.1.2, which covers phishing competency. If the user did not complete Task 3.1.1 at an expert level, that competency would reappear after Task 7.1.2. They must then complete Task 3.2.1 to satisfy the network security competency.

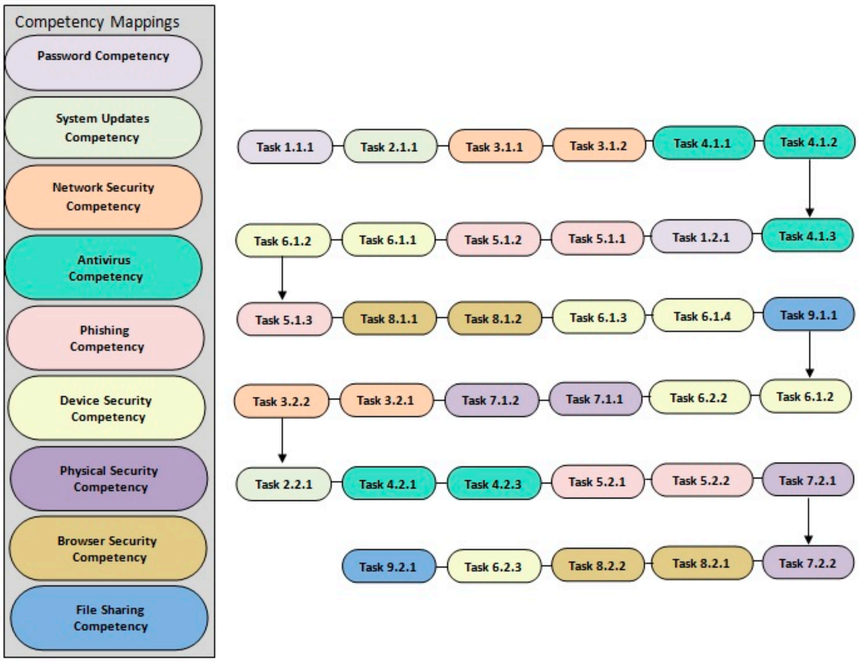


Figure 6. Information related to the different competencies in CyberHero.

A pre-defined hierarchy of the tasks is also available in the domain; see Figure 7. This pool of data is available in the form of an internal database for the pedagogical model to draw upon as it determines the next task to present to the player.

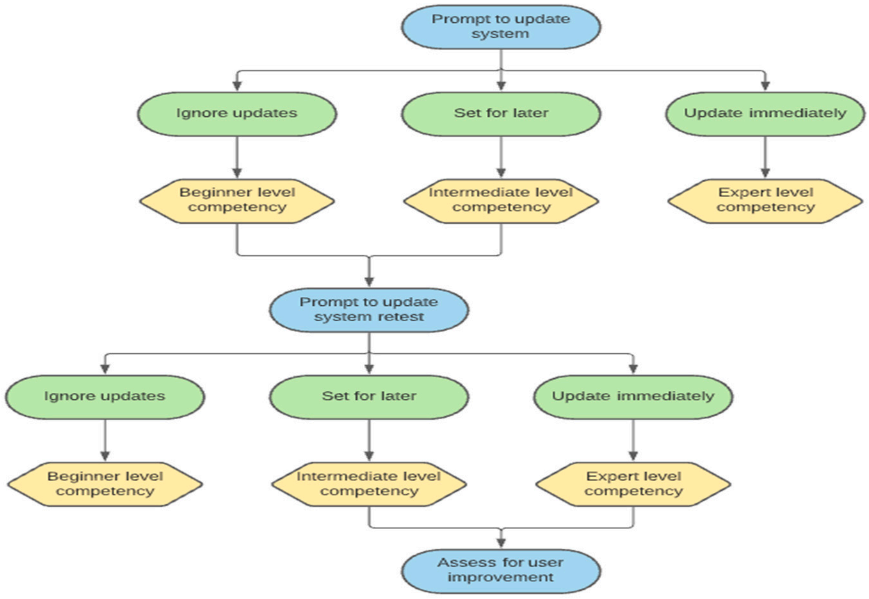

Prompt to update system
Ignore updates
Set for later
Update immediately
Beginner level competency
Intermediate level competency
Expert level competency
Prompt to update system retest
Ignore updates
Set for later
Update immediately
Beginner level competency
Intermediate level competency
Expert level competency
Assess for user improvement

Figure 7. Hierarchical representation of tasks in CyberHero.

4.2. User Model in CyberHero

One of the unique features of CyberHero is its adaptive approach to the player's responses throughout the game. In CyberHero, an individual user model is developed for each player, which allows the game to adapt to the player's unique needs and abilities. The player model is created based on assumptions about the user's knowledge and skills, which are refined and updated as the player progresses through the game and makes decisions.

The game has four levels, each with at least four tasks. If the player demonstrates expert-level knowledge and skills in all tasks within a level, they will not be presented with a retake of those tasks. However, if the player demonstrates beginner- or intermediate-level knowledge in any task, a modified version of that task will be added to a future level. Example rules are provided below:

Sample rule 1 (task mastery):

IF on Task 2 user updated system when prompted THEN update task mastery to expert (cf = 1.0)
ELSE IF on Task 2 user chose to be reminded later THEN update task mastery to intermediate (cf = 0.6)
ELSE IF on Task 2 user chose to skip updates altogether THEN update task mastery to beginner (cf = 0.9)

Sample rule 2 (competency mastery):

IF task mastery for task 3.1.1 = expert AND task master for task 3.1.2 is expert THEN update competency mastery to expert (cf = min(TM3.1.1, TM3.1.2))

The use of certainty factors in CyberHero's user model is an interesting approach in order to understand the user's thought process and knowledge level. The certainty factor model assigns a certainty value for each response that a player can give for the password security task. The values range from -1 to 1, where -1 indicates a high degree of certainty that the player is a beginner, 0 indicates uncertainty, and 1 indicates a high degree of certainty that the player is an expert.

By considering several factors that could contribute to a user's response to a task, such as their awareness of password managers or their understanding of password complexity, the certainty factors provide a more nuanced assessment of the user's skill level. This can be particularly helpful in determining which tasks to present to the user next and how to modify tasks based on their responses. For example, if a player chooses to use a password manager for the password security task, they are assigned a certainty factor of 1, indicating a high degree of certainty that they are an expert. If they choose to use a weak or easily guessable password, they are assigned a certainty factor of -1, indicating a high degree of certainty that they are a beginner. It is worth noting that the certainty factor model for the password security learning outcome considers varied factors such as the complexity of the password, the use of password managers, and the player's understanding of the requirements for a strong password. This information is used later by the pedagogical model to determine the appropriate level of difficulty for future tasks and to adapt to the player's level of knowledge and skill.

By skipping tasks that they have already mastered, players are able to progress more quickly through the game and focus on areas where they still need to improve. At the same time, by presenting new or challenging tasks, the game keeps the players engaged and motivated to continue learning. Lastly, the pedagogical model would make decisions based on the current information in the user model by retrieving the best matching task to the player from the repository of tasks in the domain model.

4.3. Pedagogical Model in CyberHero

The pedagogical model in CyberHero uses data from both the user model and the domain model to make decisions about what tasks and content to present to the player. The model considers the player's skill level and uses Bloom's Taxonomy mastery levels to guide the pedagogies used. The goal is to provide a personalized learning experience that is challenging enough to promote growth but not so difficult that it discourages the player.

By tracking the player's decisions and progress throughout the game, the pedagogical model can adapt and provide appropriate instruction to address any knowledge gaps or areas for improvement. This approach can lead to more engaging and effective cybersecurity education for individuals, helping strengthen the security defenses of organizations. The player's responses to the presented challenges guide the branching effect of the storyline. For example, if the player makes poor security choices, it can lead to a breach of customer data. This breach would trigger the pedagogical model to then introduce a reporter character who aims to get to the source of the breach. On the other hand, if the player makes proper security choices, there is no breach, and the reporter character will not be introduced. Another example of branching consequences in CyberHero is failing to properly secure a device, which can lead to it getting stolen. If the device is not properly secured with password protection and disk encryption, this can have further consequences. As players progress further into the game and make more decisions, the storyline changes accordingly. A demonstration of this approach is shown in Figure 8.

In general, if a player struggles with a particular concept, the pedagogical model may present the information in a different way or provide additional resources to help the player understand. Similarly, if a player is progressing quickly, the model may present more challenging tasks to keep them engaged. In general, if a player is classified as a beginner in a particular learning outcome, the pedagogical model will present them with a series of tasks that progressively become more difficult until they reach an intermediate level. The pedagogical model will then retest the user to determine if they have improved and are ready to move on to more complex tasks. If the user demonstrates an understanding of the more complex tasks, they will be classified as an expert in that learning outcome and will not be retested in that area. However, if the user does not demonstrate an understanding of the more complex tasks, the pedagogical model will continue to present them with tasks until they achieve the desired level of mastery. An example of a generic pedagogical rule is as follows:

IF task mastery on Task X.1.1 is Beginner or Intermediate
OR
IF task mastery on Task X.1.1 is Expert and CF < 0.6
THEN present Task X.2.1 (alternate version of Task X.1.1)

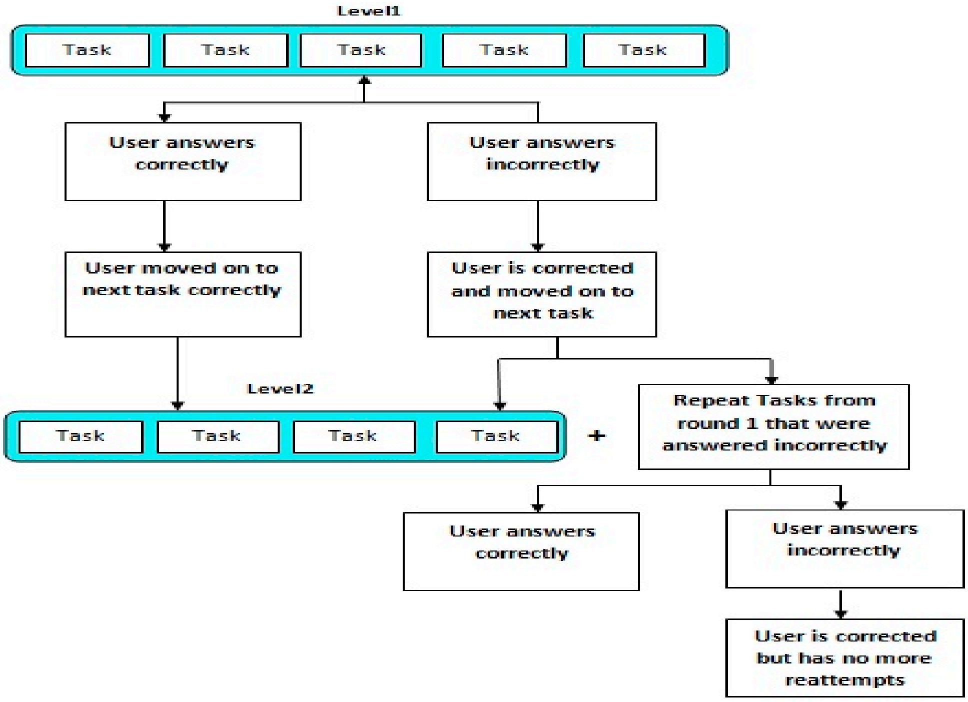

Level1
Task
Task
Task
Task
Task
User answers correctly
User answers incorrectly
User moved on to next task correctly
User is corrected and moved on to next task
Level2
Task
Task
Task
Task
+
Repeat Tasks from round 1 that were answered incorrectly
User answers correctly
User answers incorrectly
User is corrected but has no more reattempts

Figure 8. Simplified visual of game progression based on correctly or incorrectly responding to tasks.

4.4. Interface Model in CyberHero

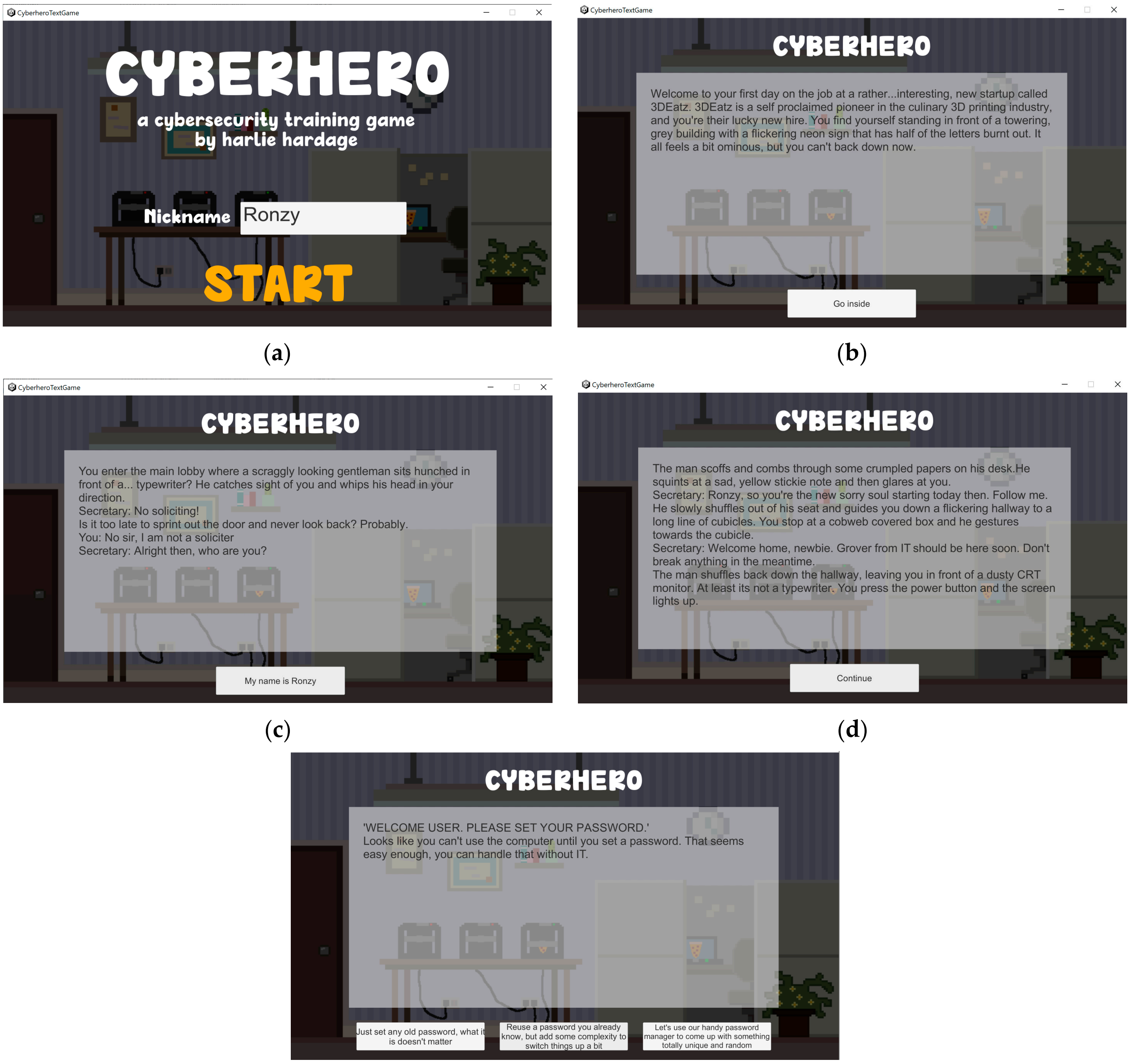
In CyberHero, the interface model is designed to be engaging and immersive. It is responsible for presenting information in a clear and engaging manner, making it easy for players to understand and interact with the game. A well-designed interface can help keep players engaged and motivated to continue playing, while a poorly designed interface can lead to frustration and disinterest. The interface model must consider factors such as user experience design, visual design, and usability testing to ensure it is effective and enjoyable for players.

The game utilizes a 2D side-scrolling interface with a cartoon-like visual style. The interface includes elements such as health bars, inventory menus, and task lists to help players keep track of their progress and objectives. The interface model also includes features for player feedback, such as notifications and pop-ups to inform players of their progress and achievements. This feedback is important to keep players motivated and engaged with the game.

4.5. Example Run

CyberHero is a desktop game that requires the players to download the game from a shared drive and run it on their local computers. CyberHero was developed using the Unity game engine and implemented in C#. Within CyberHero, a unique player model is constructed for every individual participant. This process commences by establishing initial suppositions about the user and subsequently expanding upon those suppositions to monitor the user's advancement as additional input is garnered. CyberHero employs an interactive branching storyline structure. Although the sequence of tasks follows a linear progression, the reactions to these tasks take on a branching nature. To illustrate, making inadequate security decisions can result in a compromise of customer data. In the event of a security breach, the narrative introduces a reporter who endeavors to uncover the origin of the breach. Conversely, opting for sound security choices eliminates the possibility of a breach occurring.

The game starts with a window that asks the user to enter their nickname (Figure 9a), and then the story unfolds (Figure 9b–d) until reaching the first task (Task 1.1.1) that the user needs to complete in order to satisfy password competency (Figure 9e). The story would continue to unfold based on how the user performs in this task. The next task will be chosen by the pedagogical model based on the user's current skill level and the hierarchal structure provided by the domain model.



(**a**)

Welcome to your first day on the job at a rather...interesting, new startup called 3DEatz. 3DEatz is a self proclaimed pioneer in the culinary 3D printing industry, and you're their lucky new hire. You find yourself standing in front of a towering, grey building with a flickering neon sign that has half of the letters burnt out. It all feels a bit ominous, but you can't back down now.

(**b**)

You enter the main lobby where a scraggly looking gentleman sits hunched in front of a... typewriter? He catches sight of you and whips his head in your direction.
Secretary: No soliciting!
Is it too late to sprint out the door and never look back? Probably.
You: No sir, I am not a soliciter
Secretary: Alright then, who are you?

(**c**)

The man scoffs and combs through some crumpled papers on his desk.He squints at a sad, yellow stickie note and then glares at you.
Secretary: Ronzy, so you're the new sorry soul starting today then. Follow me.
He slowly shuffles out of his seat and guides you down a flickering hallway to a long line of cubicles. You stop at a cobweb covered box and he gestures towards the cubicle.
Secretary: Welcome home, newbie. Grover from IT should be here soon. Don't break anything in the meantime.
The man shuffles back down the hallway, leaving you in front of a dusty CRT monitor. At least its not a typewriter. You press the power button and the screen lights up.

(**d**)

'WELCOME USER. PLEASE SET YOUR PASSWORD.'
Looks like you can't use the computer until you set a password. That seems easy enough, you can handle that without IT.

Just set any old password, what it is doesn't matter
Reuse a password you already know, but add some complexity to switch things up a bit
Let's use our handy password manager to come up with something totally unique and random

(**e**)

Figure 9. Sample run. (**a**) Start window, (**b**–**d**) Scenario progression (**e**) resentation of Task 1.1.1.

5. Methodology and Discussion of Results

The study's representative validity is restricted. To assess potential learning effects, we utilized a questionnaire that we created ourselves since there are no established questionnaires available for this specific task. The designed questionnaire allows the participants to reflect on their learning and examines the participants' awareness of any learning that may have occurred as a result of the game's adaptation to their current skills and the subsequent customization of the story and the tasks presented to them. In addition to the questionnaire, CyberHero creates log files on the users' computers that store information related to the user's progress in the game. The users were asked to send the log files to the authors after they completed the game.

The study was performed with 42 participants from computer science and 40 participants from other classes, including business, marketing, fine arts, and engineering, at the sophomore and junior levels (82 participants total participated in testing and evaluating CyberHero). Among those participants, there were 37 male and 28 female students, while 17 students decided not to reveal their gender. The participants were asked to download the game from Google Drive and play it locally on their machines. After they were done playing the game, they were asked to fill out a questionnaire using Google Forms to solicit their feedback. Only participants who completed the game were included in the results. The participants were asked to use the same nickname when playing the game and filling out the questionnaires.

5.1. Quantitative Analysis

Analyzing the results from the questionnaire shows that 79% of the participants strongly agreed/agreed that they learned something new from the game. When the participants were asked if they had fun playing the game, 68% strongly agreed/agreed with this statement. A total of 84% of the participants said that they would recommend this game to others to learn about different cybersecurity issues and the best ways to handle them. A total of 84% of the participants agreed that the story was engaging. Finally, when asked about their overall experience with the game, 79% said that it was enjoyable. Figure 10 shows a chart that represents these results.

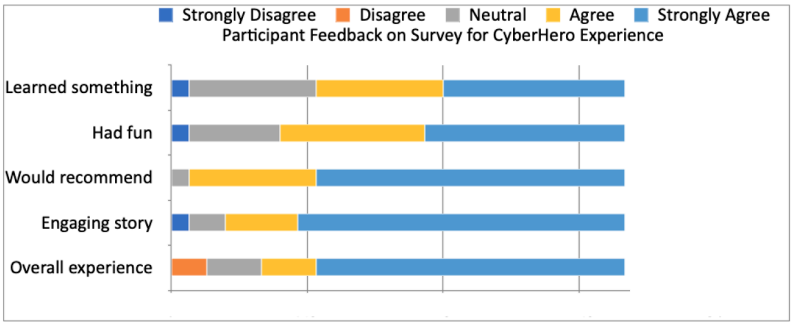


Figure 10. Results from the questionnaire.

Through an examination of the log files pertaining to 55 users who had to complete both the first and second tasks for a particular competency, the findings indicate that the majority of students demonstrated enhancement during their second endeavor (only about 16% completed the second task with no improvement or at a lower scale). Figure 11 shows a graphical representation of these results.

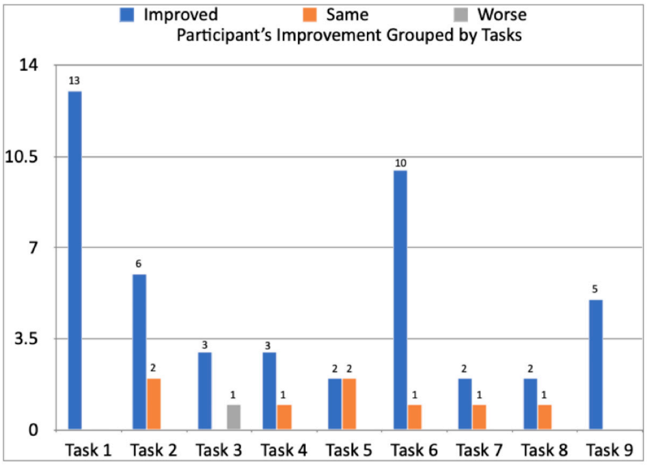


Figure 11. Users' improvement grouped by tasks.

5.2. Qualitative Analysis

The qualitative questions in the questionnaire reflect a big interest in CyberHero as a way to educate people about different cybersecurity issues. One of the questions this work tried to answer is, "Does using in-game techniques provide a truer measurement of the user's competencies?" Though substantial work remains before confidently arriving at an answer, the fact that only about 16% of the users did not exhibit improvement can serve as substantiation for the efficacy of in-game testing.

Consider an experiment where subjects undergo testing, engage in a serious game, and subsequently face retesting. Even without explicit awareness of the post-test phase, numerous participants are likely to infer its inclusion in the experiment. In the context of this study, participants did not encounter any pre-test exposure and were unaware of the possibility of retesting within the game. As a result, the responses provided during the second test are more apt to reflect learning from the game and genuine advancement, rather than attempts to memorize answers in anticipation of testing. This approach also implies that certain participants who did not closely attend to the game and overlooked opportunities for improving their responses might repeat their previous errors.

Example feedback that shows the effectiveness of CyberHero based on the users' self-reflections on their experience includes "I was rated intermediate on the first two tasks and I faced similar tasks toward the end of the game, and I believe this concept of testing reinforced the information of how to solve the specific task I did not solve efficiently.", "I think the story was engaging as it related to the work-environment theme. It was interesting to learn about VPN, HTTP, and HTTPS, as I was not too familiar with them. I think it gave me a good grasp and knowledge of what to do and what not to do. Also, I think it gave a good understanding of what needs to be done to keep everything secure and away from viruses as well.", "It helped correct my mistake. Lately, I tend to use similar passwords, so it was a bit of a wake-up call to get the part wrong and to try again.", "It helped me to reinforce the concept. At first, when I was doing it, I answered as if how I would answer, but later when it asked similar tasks again in the game, I thought of it again and corrected my prior mistakes.", "I would prefer if it was containing more info about other security concerns.", "I do not feel the task was redundant, being given a similar task helps myself grasp a certain subject with a better understanding.", "I had fun while playing the game", "I would recommend this game to someone wanting to learn more about cybersecurity", and "The story was engaging and easy to follow".

An interesting finding was the focus of the computer science students' feedback on the game elements like background story, graphics, and non-player characters, while the non-computer science students focused on the scenarios, cybersecurity topics, and their learning experience. They requested adding more scenarios and addressing more cybersecurity issues that may occur in the workplace or in normal daily activities. These results make sense because of the background and expertise level of the different groups.

6. Conclusions and Future Work

CyberHero addressed most of the drawbacks that existing games might be suffering from, such as a lack of learning theories in the game design, non-adaptivity, non-disruptive within the game assessment, compliance with the NICE framework, and real-world scenarios that can facilitate the transfer of these skills to real life.

Some of the drawbacks encountered in existing games include small testing groups and poor metrics and testing mechanisms which can question the validity of the game, such as the use of extrinsic evaluation; results from the games are often unclear or unrelated to the users' improvements or awareness of cybersecurity topics [8]. Additionally, information overload and the repetition of information can cause users to lose interest in the game. Web-based applications can also be problematic for users without Internet access. Finally, the lack of instructional components may result in users not learning the topic, and the excessive focus on scoring may also hinder the learning process [41]. On the other hand, personalization and adaptivity in serious games have proven to motivate the players [7], which is currently missing from the existing games. Moreover, by incorporating feedback and instructional strategies into game design, serious games have the potential to engage learners and facilitate long-term learning outcomes, in addition to creating a better learning environment by providing instant feedback to motivate users.

CyberHero provides self-assessment through similar scenarios (teaching moments) at different points in the story. The users can evaluate their performance and can tell if they gained any learning. The survey has questions that aim to measure the players' learning by allowing them to reflect on their learning and examining their awareness of any learning that may have occurred because of the game's adaptation to their current skills and the subsequent customization of the story. The fact that 80% of the participants moved from beginner and intermediate status during the game to expert at the end of the game provides some evidence of the effectiveness of CyberHero as a training/teaching tool.

Future work may include enhancing the adaptation aspect of CyberHero by incorporating more advanced machine learning algorithms to personalize the game experience for each individual player, involving the creation of a 3D world with non-player characters in order to engage the users and increase believability and immersion in the game world, deploying CyberHero on the web, and making use of the data analytics tool in Unity to track the user's performance and their progression in the game. This could involve analyzing player behavior and learning patterns to provide tailored feedback and challenges and conducting interviews with focus groups to better understand their experience and their knowledge gain.

While the game currently covers important cybersecurity concepts, such as phishing attacks and password security, there are many other topics that could be included, such as malware, network security, and social engineering. Expanding the game to cover a wider range of topics would provide a more comprehensive education for users and help them better understand the complexities and current challenges of cybersecurity. This could help the users to better understand how cybersecurity concepts apply in real-life situations and give them practical experience in dealing with cybersecurity threats.

Author Contributions: Conceptualization, H.H., R.H. and S.A.; methodology, H.H., R.H. and S.A.; software, H.H. and R.H.; validation, S.A. and E.A.A.; formal analysis, R.H. and E.A.A.; investigation, E.A.A., S.A. and R.H.; resources, R.H. and H.H.; data curation, R.H. and H.H.; writing—original draft preparation, R.H., E.A.A. and S.A.; writing—review and editing, E.A.A., S.A. and R.H.; visualization, R.H. and H.H.; supervision, R.H. and S.A.; project administration, E.A.A. and R.H.; funding acquisition, E.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2023R409), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Data Availability Statement: Not applicable.

Acknowledgments: The authors acknowledge Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R409), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Li, L.; He, W.; Xu, L.; Ivan, A.; Anwar, M.; Yuan, X. Does Explicit Information Security Policy Affect Employees' Cyber Security Behavior? A Pilot Study. In Proceedings of the 2014 Enterprise Systems Conference, Shanghai, China, 2–3 August 2014.
2. Shropshire, J.; Warkentin, M.; Sharma, S. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Comput. Secur.* **2015**, *49*, 177–191. [CrossRef]
3. Enterprise, V. Verizon Data Breach Investigations Report. 2020. Available online: https://www.verizon.com/business/en-gb/resources/reports/2020-data-breach-investigations-report.pdf (accessed on 29 May 2023).
4. Nurse, J.R. *Cybersecurity Awareness*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 1–4.
5. Ceesay, E.N.; Myers, K.; Watters, P.A. Human-centered strategies for cyber-physical systems security. *EAI Endorsed Trans. Secur. Saf.* **2018**, *4*, e5. [CrossRef]

6. Miljanovic, M.A.; Bradbury, J.S. Making Serious Programming Games Adaptive. In Proceedings of the 4th Joint Conference on Serious Games (JCSG), Darmstadt, Germany, 7–8 November 2018.
7. Yannakakis, G.N.; Togelius, J.; Khaled, R.; Jhala, A.; Karpouzis, K.; Paiva, A.; Vasalou, A. Siren: Towards adaptive serious games for teaching conflict resolution. In Proceedings of the 4th European Conference on Games-Based Learning: ECGBL, Copenhagen, Denmark, 21–22 October 2010.
8. Streicher, A.; Smeddinck, J.D. Personalized and adaptive serious games. In Proceedings of the Entertainment Computing and Serious Games: International GI-Dagstuhl Seminar 15283, Dagstuhl Castle, Germany, 5–10 July 2015.
9. Hendrix, M.; Al-Sherbaz, A.; Victoria, B. Game based cyber security training: Are serious games suitable for cyber security training? *Int. J. Serious Games* **2016**, *3*, 53–61. [CrossRef]
10. Mäses, S.; Hallaq, B.; Maennel, O. Obtaining Better Metrics for Complex Serious Games Within Virtualised Simulation Environments. In Proceedings of the 11th European Conference on Game-Based Learning (ECGBL), Graz, Austria, 5–6 October 2017.
11. Dark, M. Advancing cybersecurity education. *IEEE Secur. Priv.* **2014**, *12*, 79–83. [CrossRef]
12. Nagowah, L.; Nagowah, S. A Reflection on the Dominant Learning Theories: Behaviourism, Cognitivism and Constructivism. *Int. J. Learn.* **2009**, *16*, 3–9.
13. Ertmer, P.A.; Newby, T.J. Learning theory and technology: A reciprocal relationship. In *Wiley Handbook of Learning Technology*; Wiley: Hoboken, NJ, USA, 2016; pp. 58–76.
14. Ertmer, P.A.; Newby, T.J. Behaviorism, cognitivism, constructivism: Comparing critical features from an instructional design perspective. *Perform. Improv. Q.* **2013**, *26*, 43–71. [CrossRef]
15. Huitt, W. *Humanism and Open Education: Educational Psychology Interactive*; Valdosta State University: Valdosta, GA, USA; Available online: http://www.edpsycinteractive.org/topics/affect/humed.html (accessed on 29 June 2023).
16. Siemens, G. Connectivism: Creating a learning ecology in distributed environments. In *Didactics of Microlearning*; In Concepts, Discourses and Examples; Waxmann Verlag: Münster, Germany, 2007; pp. 53–68.
17. Murphy, E. Constructivism: From Philosophy to Practice, Reports—Descriptive (141). 1997. Available online: https://files.eric.ed.gov/fulltext/ED444966.pdf (accessed on 29 June 2023).
18. Dincelli, E.; Yayla, A.; Kusyk, Ł. Cyber Attack! A Story-driven Educational Hacking Game. In Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS), Boston, MA, USA, 7–11 August 2020.
19. Jayakrishnan, G.C.; Sirigireddy, G.R.; Vaddepalli, S.; Banahatti, V.; Lodha, S.P.; Pandit, S.S. Passworld: A serious game to promote password awareness and diversity in an enterprise. In Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security, Boston, MA, USA, 7–11 August 2020.
20. Bhardwaj, J. Design of a Game for Cybersecurity Awareness. Master's Thesis, North Dakota State University, Fargo, ND, USA, 2019.
21. Bahrini, M.; Volkmar, G.; Schmutte, J.; Wenig, N.; Sohr, K.; Malaka, R. Make my Phone Secure!: Using gamification for mobile security settings. In Proceedings of the Mensch und Computer, Hamburg, Germany, 8–11 September 2019.
22. Wen, Z.A.; Lin, Z.; Chen, R.; Andersen, E. What.Hack: Engaging anti-phishing training through a role-playing phishing simulation game. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow Scotland, UK, 4–9 May 2019.
23. Lopes, I.; Morenets, Y.; Inácio, P.R.; Silva, F.G.M. Cyber-detective—A game for cyber crime prevention. In Proceedings of the Play2Learn, Loja MEO Lisboa—Fórum Picoas, Lisbon, Portugal, 19 April 2018; pp. 175–191.
24. Løvgren, D.E.H.; Li, J.; Oyetoyan, T.D. A data-driven security game to facilitate information security education. In Proceedings of the 41st International Conference on Software Engineering: Companion Proceedings, Montreal, QC, Canada, 25–31 May 2019.
25. Johnson, J.; Weanquoi, P.; Zhang, J.; Xu, J. Learn DDoS attacks with a game. In Proceedings of the World Congress on Engineering and Computer Science, San Francisco, CA, USA, 23–25 October 2018.
26. Deeb, F.A.; Hickey, T.J. Teaching introductory cryptography using a 3D escape-theroom game. In Proceedings of the IEEE Frontiers in Education Conference (FIE) Covington, Covington, KY, USA, 16–19 October 2019.
27. Vadla, S.; Parakh, A.; Chundi, P.; Surbamaniam, M. Quasim: A multi-dimensional quantum cryptography game for cyber security. In Proceedings of the 22nd Colloquium for Information System Security Education, New Orleans, LA, USA, 11–14 June 2018.
28. Weanquoi, P.; Johnson, J.; Zhang, J. Using a game to improve phishing awareness. *J. Cybersecur. Educ. Res. Pract.* **2018**, *2018*, 2.
29. Sharma, A.; Palrecha, D.; Parekh, M. Security awareness game (Augmented Reality). In Proceedings of the International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur, India, 26–28 February 2019.
30. Williams, M.; Nurse, J.R.; Creese, S. (Smart) Watch Out! Encouraging privacyprotective behavior through interactive games. *Int. J. Hum.-Comput. Stud.* **2019**, *132*, 121–137. [CrossRef]
31. Suarez, H.; Kincannon, H. SSETGami: Secure software education through gamification. *Proc. Cybersecur. Educ. Res. Pract.* **2017**. Available online: https://digitalcommons.kennesaw.edu/ccerp/2017/education/1 (accessed on 29 May 2023).
32. Zargham, N.; Bahrini, M.; Volkmar, G.; Wenig, D.; Sohr, K.; Malaka, R. What could go wrong?: Raising mobile privacy and security awareness through a decision-making game. In Proceedings of the Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts, Barcelona, Spain, 22–25 October 2019.
33. Yasin, A.; Liu, L.; Li, T.; Wang, J.; Zowghi, D. Design and preliminary evaluation of a cyber security requirements education game (SREG). *Inf. Softw. Technol.* **2018**, *95*, 179–200. [CrossRef]
34. Seale, J.; Schoenberger, N. Be Internet Awesome. *Emerg. Libr. Inf. Perspect.* **2018**, *1*, 34–58. [CrossRef]

35. Kayali, F.; Wallner, G.; Kriglstein, S.; Bauer, G.; Martinek, D.; Hlavacs, H.; Purgathofer, P.; Wölfle, R. A case study of a learning game about the Internet. In Proceedings of the International Conference on Serious Games, Darmstadt, Germany, 1–5 April 2014.
36. Arachchilage, N.A.G.; Hameed, M.A. Integrating self-efficacy into a gamified approach to thwart phishing attacks. *arXiv* **2017**, arXiv:1706.07748.
37. Giannakas, F.; Kambourakis, G.; Gritzalis, S. CyberAware: A mobile game-based app for cybersecurity education and awareness. In Proceedings of the 2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL), Thessaloniki, Greece, 19–20 November 2015.
38. Jordan, C.; Knapp, M.; Mitchell, D.; Claypool, M.; Fisler, K. CounterMeasures: A game for teaching computer security. In Proceedings of the 2011 10th Annual Workshop on Network and Systems Support for Games, Ottawa, ON, Canada, 6–7 October 2011.
39. Ariyapperuma, S.; Minhas, A. Internet security games as a pedagogic tool for teaching network security. In Proceedings of the Frontiers in Education 35th Annual Conference, Indianapolis, IN, USA, 19–22 October 2005.
40. Hamey, L.G. Using the security protocol game to teach computer network security. In Proceedings of the Australian Conference on Science and Mathematics Education (Formerly UniServe Science Conference), The University of Sydney, Camperdown, NSW, Australia, 26–28 September 2012.
41. Kolb, A.Y.; Kolb, D.A. The learning way: Meta-cognitive aspects of experiential learning. *Simul. Gaming* **2009**, *40*, 297–327. [CrossRef]
42. Mäses, S.; Randmann, L.; Maennel, O.; Lorenz, B. Stenmap: Framework for evaluating cybersecurity-related skills based on computer simulations. In *Learning and Collaboration Technologies, Proceedings of the Learning and Teaching: 5th International Conference, LCT 2018, Held as Part of HCI International, Las Vegas, NV, USA, 15–20 July 2018*; Springer: Berlin/Heidelberg, Germany, 2018.
43. Rober, M. The Super Mario Effect: Tricking Your Brain into Learning More; TEDxPenn. Available online: https://www.youtube.com/watch?v=9vJRopau0g0 (accessed on 29 June 2023).
44. Wetzel, K. *NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.