information

Perspective

Improving the Cybersecurity Awareness of Young Adults through a Game-Based Informal Learning Strategy

Giorgia Tempestini, Sara Merà, Marco Pietro Palange, Alexandra Bucciarelli and Francesco Di Nocera *

Department of Planning, Design and Technology of Architecture, Sapienza University of Rome, 00196 Rome, Italy
* Correspondence: francesco.dinocera@uniroma1.it

Abstract: Knowing about a danger is not enough to avoid it. Our daily lives offer countless examples of occasions in which we act imprudently for various reasons, even though we know we are taking risks. Nevertheless, circumstances in which we lack the necessary knowledge can lead us to run into unpleasant or harmful situations without being aware of it. In cybersecurity, knowledge of the dangers (as well as the mechanics of a possible attack) makes a huge difference. This is why specific training is provided in organizations, along with awareness campaigns. However, security training is often generic, boring, and a mere fulfillment of obligations rather than a tool for behavioral change. Today, we can deliver content through various devices and platforms that people access for both work and leisure, so that learning can happen incidentally and with almost no effort. Distributing knowledge in small, dedicated units creates the conditions for lasting, effective learning and is more effective than teaching through traditional courses (whether delivered in-person or online). In this article, we present an ongoing project on cybersecurity informal learning, including the design of a small video game. The intervention is aimed at helping young adults (18–25 years) to understand the mechanics of cookies and their role in the dynamics of cyberattacks. Consistent with the idea that a comprehensive course may be unsuitable for delivering cybersecurity training, the game covers and deliberately limits itself to that topic only. We also provide detailed considerations related to the evaluation of its effectiveness, although this is outside the scope of the present paper.

Keywords: cybersecurity; behavior; knowledge; learning; games; gamification; cookies

Citation: Tempestini, G.; Merà, S.; Palange, M.P.; Bucciarelli, A.; Di Nocera, F. Improving the Cybersecurity Awareness of Young Adults through a Game-Based Informal Learning Strategy. *Information* **2024**, *15*, 607. https://doi.org/10.3390/info15100607

Academic Editors: Heming Jia, Jose de Vasconcelos, Hugo Barbosa and Carla Cordeiro

Received: 26 July 2024
Revised: 10 September 2024
Accepted: 2 October 2024
Published: 3 October 2024

1. Introduction

The human element is a critical weak point in the Information Technology (IT) security chain [1,2]. People are vulnerable to cybersecurity threats, either because they have limited knowledge or because, despite their awareness, they apply "only minimal protective measures, usually relatively common and simple ones" ([3], p.82), if any. Here, we are not concerned with the distinction between knowledge and awareness, which some authors consider to be separate constructs. For the purposes of this paper, we will consider knowledge to be indicative of awareness, whether or not it leads to appropriate behavior. Knowledge alone is not sufficient to explain behavior. For example, Lorenz and colleagues [4] observed that when information was provided on how to create passwords, only 2% followed the instructions at follow-up. Nevertheless, a lack of knowledge is usually associated with less attention being paid to cybersecurity threats. For example, Tempestini and colleagues [5] observed how those who have poorer knowledge of procedures, the consequences of their actions, policies, and their responsibilities are less careful about the actions they take, and do not protect their devices from different types of threats. Moreover, Di Nocera and colleagues [6] demonstrated that poor cybersecurity knowledge is associated with ignoring good practices, like using two-factor authentication.

While attitudes toward risk are not easy to change, knowledge can be easily improved. Indeed, in response to the exponential growth of security threats, a great deal of cybersecurity training is currently being offered. These courses target two different types of audience:

some courses are aimed at students or professionals in the field, while others are intended for non-technical employees to minimize the risk of insecure IT behavior. Both types have been addressed in the literature with the final objective of providing recommendations and guidelines to help design better cybersecurity courses. For example, González-Manzano and De Fuentes [7] analyzed 35 free courses, offered on various platforms (i.e., Coursera, Cybrary.it, edX, and Udacity) and aimed at individuals with various levels of knowledge (beginner, intermediate, and advanced). The authors provided indications relating to the contents, the delivery methods, the teachers' attitude towards the topics covered, the personalization of the courses, and the duration of the modules. In another work, Payne et al. [8] presented a detailed description of a cybersecurity course on which they based their recommendations for the design of future courses. Their contribution highlights, above all, the importance of the interdisciplinarity of the courses. This is an aspect that is certainly important, but which needs to be tested empirically.

Although it is interesting to analyze the literature devoted to professional training, our focus is on organizational cybersecurity training delivered along with (or as part of) awareness programs. In this area, the literature points to several limitations, particularly with respect to employees' perceptions of the courses themselves. In fact, employees often believe that the courses are boring and not very personalized to the needs of their organization, and there is a lack of incentive from the organization to the employees to participate in the course [9].

2. Background

Among the papers suggesting guidelines and best practices, few studies have empirically examined the effectiveness of cybersecurity training. He and colleagues [10] investigated the effect of different cybersecurity training methods on employees' cybersecurity risk perception and self-reported behavior. Employees were divided into four groups: a group who watched short educational videos, a group who read four reports, a group who watched videos and read reports, and a control group who received no intervention. All participants were required to complete a pre- and post-intervention test, specifically devised by the authors to assess perceived vulnerability, perceived severity, perceived benefits, perceived barriers, response efficacy, response cost, security self-efficacy, and behavioral intention. The study found positive effects for all methods with respect to vulnerability, barriers, response costs, self-efficacy, and behavioral intentions. Moreover, they found that evidence-based malware reporting is a relatively better training method than the other two training methods: people remember information more easily when it is presented in a way that makes it personally relevant.

Recently, Prummer and colleagues [11] investigated various learning modes in a review in which 142 articles (empirical articles, speculative articles, and intervention proposals) were analyzed. The authors identified the following types of training: game-based, presentation-based, simulation-based, information-based, video-based, text-based, and discussion-based. The authors compared all the courses by analyzing specific aspects, including the following:

- Properties: online or in person, group or individual;
- The theories on which the courses were based: Protection Motivation Theory, Theory of Planned Behavior, Theory of Reasoned Action, Signal Detection Theory, and General Deterrence Theory;
- The targets at which the courses were aimed: employees, students, young adults, or the general population;
- The effects of the training: fun, usefulness, or effectiveness.

The latter criterion is crucial because it is helpful for clarifying the actual utility of the different methods. Several studies among those analyzed in the review reported positive feedback, especially when techniques such as game-based or simulation-based training were used. Regarding effectiveness, the results showed an increase in almost all cases (except for in five articles), albeit with some differences depending on the type of training

used. Abawajy [12], for example, analyzed and compared the effects of game-, video-, and text-based training and found that awareness rates increased significantly across all conditions. It was also found that participants showed improvements in different areas depending on the training method they were assigned to. For example, game-based intervention led to an increase in the ability to identify scam sites, whereas video-based intervention increased knowledge about phishing.

2.1. Informal Learning

It appears clear that knowledge gained through formal training is not always sufficient to make users adopt secure behaviors. Formal training programs cannot always adequately prepare people to generalize their knowledge to all possible scenarios and are typically not designed to equip individuals for continuous learning.

Therefore, it becomes essential to explore alternative methods of delivering cybersecurity education that can be adapted to real-world scenarios and foster continuous and autonomous, self-paced learning. Currently, we can deliver content across various devices and platforms that people access for both work and leisure, so that learning about a great variety of topics can happen casually and almost effortlessly. Research suggests that a significant amount of learning happens through informal activities [13]. These activities can create an environment that fosters deeper and more effective learning compared to traditional courses. While traditional courses offer valuable information, they may not always be engaging for everyone. By incorporating informal learning methods, it would be possible to create a more well-rounded educational experience that promotes lasting behavioral change. Marsick and Watkins [14] actually make a distinction between "informal learning" and "incidental learning", distinguishing them on the basis of intentionality. People may learn informally, while intentionally choosing to seek out and learn new ideas, albeit in a less structured way than in formal settings. In contrast, incidental or implicit learning occurs during everyday activities, without a conscious attempt to learn or an awareness of what has been learned. However, this distinction is not made by everyone, and the two terms are often used interchangeably.

Here, with the expression "informal learning", we are referring to all those methods that take place in an unstructured way, often through daily experiences, social interactions, and environmental resources. It is characterized by the speed with which new knowledge can be acquired in response to emerging needs, and often does not entail significant costs. The importance of informal training has been documented in various contexts, both at the workplace [15] and in schools [16]. Many advantages have been found, including flexibility, the practical application of acquired skills, self-direction [14], and a greater level of involvement, especially with adolescents [17]. While there are numerous articles that deal with informal learning, its advantages, and its peculiarities, there are not many contributions specifically addressing the topic of informal learning in the field of information computer security. Rader and Wash [18] compared three different forms of informal learning related to computer security (news articles, web pages containing computer security advice, and stories about the experiences of friends and family). They observed that information provided by peers focuses mainly on the subjects who conduct the attacks, the information provided by web pages focuses instead on how the attacks are conducted, and the information coming from the news focuses on the consequences. Rader et al. [19] dealt with "stories" as informal lessons about security. Stories about others reveal useful information and it is easier to make our way through our complex world if we can learn from the experiences of others. Users reported that learning about other people's stories changed the way people think about security and act in similar occasions. The study was replicated 10 years later by Pfeffer et al. [20], who updated the contents to reflect contemporary technological advancements. While confirming the importance of storytelling as a means of informal learning, the authors also observed how storytelling worked when delivered via social media. They also observed how younger and more

educated participants perceive threats as less serious, probably because they have been more exposed to security news and therefore perceive security threats as less impactful.

Informal learning in a context such as cybersecurity is critical for several reasons: First, cybersecurity evolves constantly, with threats and vulnerabilities emerging rapidly and becoming more sophisticated, especially with the advancement of AI. Second, informal learning involves the application of knowledge to real life. For example, in competitions such as Capture the Flag (CTF), participants must—individually or as part of a team—test their knowledge by solving some security problems, which can range from exploiting websites to breaching unsecured networks [21]. The use of CTFs has been shown to be an effective way of improving cybersecurity education through gamification [22].

From our perspective, an informal learning approach is based on the idea that, rather than trying to categorize topics and merge many specific issues into formal training modules, cybersecurity education is more effective if information on each specific threat (e.g., phishing emails) or countermeasure (e.g., multiple factor authentication) is delivered in single "learning pills". Each "pill" may repeat different things to settle knowledge and may have a convenient outlet and modality to assist delivery. The proposal is very straightforward. If we need to inform people that do not know about phishing emails, we are obviously targeting people who do not know about this from other sources and have not looked it up themselves. We should expect them not to have even basic knowledge about cybersecurity. Formal training might be out of their comfort zone, being considered too complicated or too tedious. A communication campaign within the organization, in which examples of phishing emails are publicly dissected, may be much more informative than a formal training explaining the details of phishing (Figure 1a–c). The best outlet for such a campaign mostly depends on the type of target being addressed. Posters in the corridors of a school or a company as well as carousel posts on social media are examples of interventions that need less than a minute to be "consumed" by the user and that can be recalled more easily than a learning module on the concept of phishing. Humor could also be used to convey meaning and make the content highly shareable on social media. Other forms of content may have other more appropriate outlets. For example, some content may be easily shared using simple games when targeting people who normally spend time playing them. Here, the idea is to let people stumble upon content so that their knowledge changes from zero ("I didn't know that!") to where they have the ability to recognize the threat. What we are devising here is "molecular training", which is delivered informally, repeatedly, and through various media, contexts, and situations chosen from among those more appropriate for the type of user being targeted.

2.2. Serious Games

The literature on using game strategies for learning is highly diverse, with multiple research communities exploring this topic. A significant portion of this research falls under the umbrella of "serious gaming". To better understand the distinction between informal learning (described earlier) and serious gaming, it is useful to outline some key concepts that define this area. It is worth noting that many times "serious games" and "gamification" are used interchangeably. However, we prefer to use the term gamification to describe a process whose roots are in the functional analysis of behavior (see Section 2.3).

Serious gaming refers to games that are specifically designed with the primary goal of educating, training, or solving problems, rather than simply providing entertainment. These games employ game mechanics to engage users while imparting specific knowledge or skills [23]. While serious games have long been recognized as effective tools in fields such as education, healthcare, business, and military training, their potential in cybersecurity has only recently begun to be explored. Early research in this area mainly focused on testing the effectiveness of serious games in cybersecurity education. For example, Hendrix et al. [24] conducted a literature review of serious games available at the time, classifying them by their creators (academia or industry) and by type (e.g., 2D point-and-click turn-based scenarios, 3D virtual worlds, and corporate contingency planning). However, Hendrix

found that these games were primarily used for short-term education, which is generally less effective at driving long-term behavioral change.

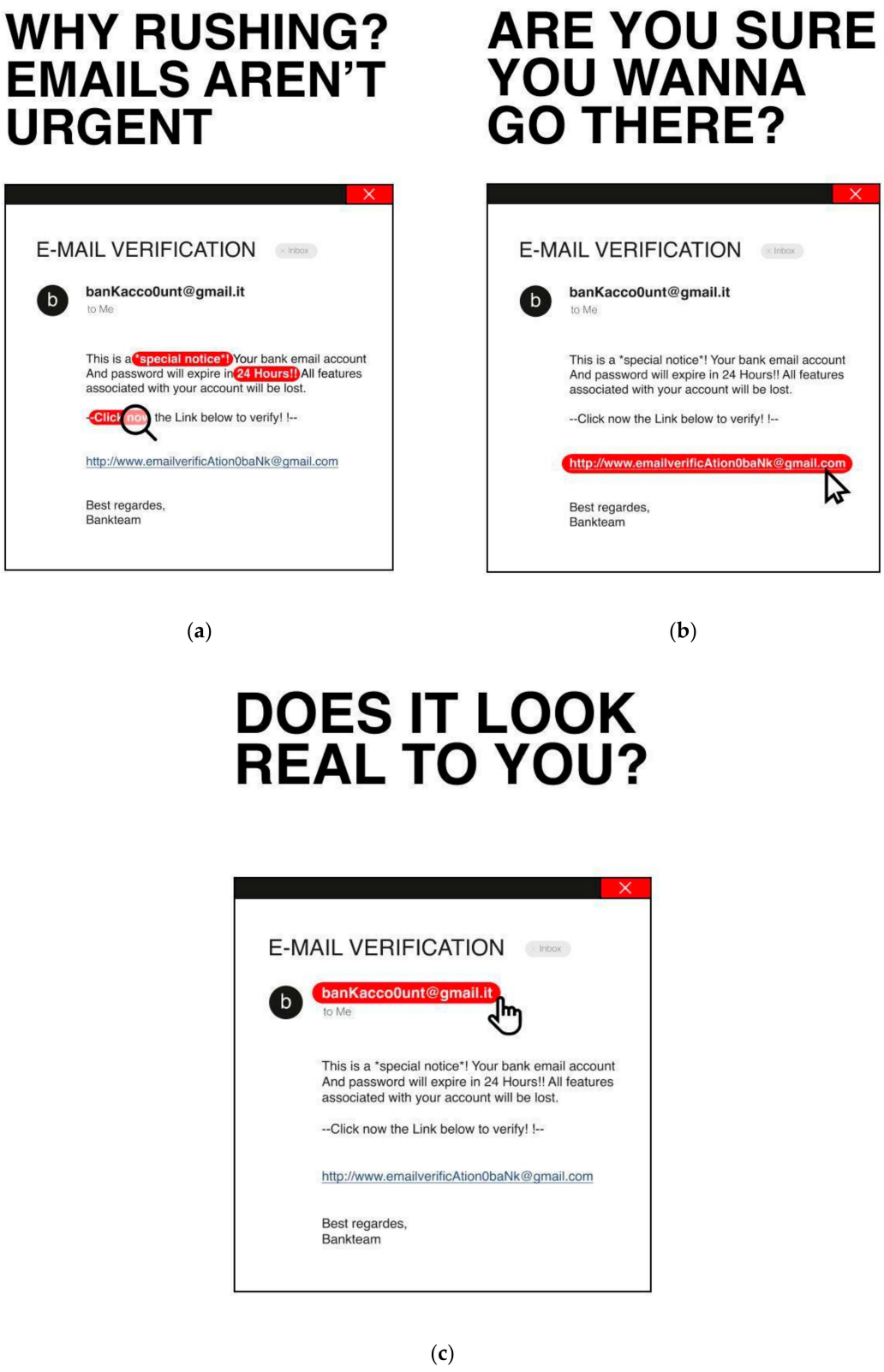

Figure 1. An example of a fictional communication campaign on the subject of phishing. There is emphasis on (**a**) a text that signals urgency, (**b**) a suspicious link within an email, and (**c**) a suspicious sender's email address.

Similarly, Alotaibi et al. [25] reviewed serious games in the field of cybersecurity and noted positive outcomes in terms of education and awareness. However, they also highlighted limitations, such as small sample sizes and content that was often too broad, making the games less effective for training in specific contexts. Hill et al. [26] echoed these concerns in their study, which aimed to provide an overview of existing cybersecurity games, particularly those focused on threats and protection, anti-phishing, and device security and privacy. They found that many of these games suffered from information overload and repetitive content, causing players to lose interest as they progressed through the game.

An analysis of recent studies on serious games reveals various interpretations of the concept. For example, Kulshrestha et al. [27] conducted a preliminary analysis of a serious game aimed at teaching network firewall concepts, using both objective and subjective methods. The objective analysis involved tracking player interactions, while the subjective analysis was based on user experience surveys. They also employed the learning mechanics–game mechanics framework to examine the relationship between game elements and learning outcomes. However, their study focused more on evaluating the quality of data using their hybrid approach than on assessing the game's overall effectiveness.

Much of the existing literature focuses on developing serious games for individuals with technical backgrounds in computer security. Coenraad et al. (2020) [28] noted that there are few games designed for users who do not consider themselves professionals in the field. One such study that addressed this gap is by Hart and colleagues [29], who introduced a board game called Risko designed to educate employees without technical training about the risks of cyberattacks and strategies for self-defense. The authors chose a card-based format, grounded in constructivist theory, and referenced existing games whose effectiveness had already been evaluated. In Risko, one player assumes the role of the attacker each turn, while the others propose countermeasures. Both attacks and defenses are inspired by industry and government standards, allowing the game to be adapted to various contexts and scenarios. A game master facilitates learning by encouraging players to reflect on their strategies, fostering discussion, and providing immediate feedback on the effectiveness of their decisions. The authors conducted a thorough analysis of existing board games, identifying potential flaws they should avoid in their own designs. Subsequent experiments confirmed the effectiveness of the game [29].

In contrast, Jaffray and colleagues [30] introduced SherLOCKED, a 2D, multi-level, top-down detective-themed game. Players control a detective, exploring rooms to find objects and answer related questions. The authors argue that role-playing games are often valuable and preferred by their target audience—students.

Other researchers have compared different types of serious games to determine which approaches are most effective. For example, Gaurav et al. [31] compared two games: one focused on teaching firewall protection against unauthorized access and another illustrating how SQL injection attacks compromise online databases. Both games were developed in two versions: a non-adaptive version that did not adjust to the player's abilities and a machine learning-based adaptive version. In the adaptive version, a machine learning agent classified players as beginners or experts based on their gaming behavior and adjusted the game's difficulty accordingly. The goal was to keep players consistently challenged without making the game too easy or too difficult. The results indicated that well-designed adaptive games can lead to better learning outcomes and a more satisfying user experience by catering to the specific needs of each player.

This brief overview reveals that the field of "serious gaming" is still evolving and lacks unified design frameworks and standardized methodologies for evaluating the effectiveness of interventions.

2.3. A Behavioral Account

So far, we have described two approaches to informal learning, one based on communication and the other on gaming. Both these approaches can be addressed in behavioral

terms. Indeed, the use of verbal descriptions of behaviors and their consequences (positive or negative), as in the examples reported in Figure 1, represents an instance of learning based on rule-governed behaviors. In contrast, gaming represents a situation in which users are both rewarded for appropriate behavior (positive reinforcement) and encouraged to avoid conditions leading to a loss (negative reinforcement). This latter situation represents a form of learning based on contingencies. The distinction between rule-governed behavior and contingency-shaped behavior was first made by Skinner in the late 1960s [32,33]. He pointed out that, in the first form of learning, there is an instructional episode, the presentation of an instruction, a response provoked by the instruction, and a consequence provided by an instructional agent as a function of its fulfillment. Rules are stimuli that specify, either directly or indirectly, consequences for behavior. In contrast, contingency-shaped behavior is behavior directly controlled by the relations between responses and their consequences. Nevertheless, behavior may also come under the control of antecedent stimuli. These are stimuli whose presence causes responses to produce their consequences.

A comprehensive discussion of the principles underlying behavior analysis is out of the scope of this article. However, it is worth noting that the behavior analysis approach provides one of the most comprehensive accounts of learning. Behavioral principles provide a scientific understanding of how people and animals learn to deal with complex situations, without referring to theories or models based on aspects that are not fully observable [34]. Essentially, this perspective emphasizes the importance of there being consequences for behavior. In practice, a behavior is more likely to be repeated if it is "reinforced", that is, when it is followed by beneficial consequences for the individual. Beneficial consequences can involve either the acquisition of beneficial stimulation (positive reinforcement) or the removal of aversive stimulation for the individual (negative reinforcement).

Although the technicalities of behavior analysis are often not adhered to, these principles are actually already integrated into many software applications under the name of gamification. The term gamification began to grow in popularity as late as 2010, when Deterding and colleagues [35] defined it as a strategy of incorporating game-like elements into non-game contexts, highlighting its relevance as a tool with which to advance learning objectives and motivate behavior change. The basic concept of gamification, however, has been around for much longer. In the literature, this is also referred to by other terms (e.g., serious games, persuasive games, and alternate reality games). Gamification involves the redesign of everyday activities based on the methods employed in game design. This redesign often involves socially relevant behavioral changes and, for that reason, has not gone unnoticed by behavior analysts. Skinner [36] had already noted how video games constituted an excellent example of contingency programming, in that players interact with a system of contingencies in which their behavior is guaranteed to be reinforced. By contacting salient and immediate consequences, players are almost guaranteed to succeed. In a nutshell, game playing is about organizing contingencies. As reported by Di Nocera and Tempestini [37], this is usually implemented using the so-called token economy, "a rather complex reinforcement system based on the accumulation of objects, namely tokens, that can be eventually exchanged for goods, services, or privileges" (p. 251).

2.4. Cookies Anyone?

In this article, we discuss an attempt to promote informal learning regarding computer cookies, a topic that is often overlooked by security training. This is an ongoing project still in its early phases of development. However, it is an appropriate example of what we are advocating here: the informal and short delivery of information on a specific topic, allowing people to gather new knowledge they would not seek independently (due to a lack of interest or any other reason). It should be clear that the choice of the topic is incidental here, and the same rationale applies to any other topic.

Computer "cookies" are text files used by websites to store information on user behavior while browsing. Cookies are usually harmless, and people do not pay much attention to dialog boxes that require them to accept cookies. Users typically click the

default option without much thought [38]. Cookie banners are designed to inform users about the data being collected and to enhance the user experience. However, they are often perceived negatively due to their invasiveness and potential privacy violations. Their design frequently encourages users to accept cookies [39], as their omnipresence tends to annoy users [40]. This issue extends beyond just cookies. Due to habituation—the diminishing response to a frequently repeated stimulus—users often overlook crucial messages when repeatedly encountering security-related dialog boxes. Their response becomes automatic, leading them to click buttons merely to acknowledge the message without fully engaging with its content [41,42].

Cookies are also highly valuable pieces of information for malicious users. To illustrate their importance, a study by NordVPN [43] revealed that hackers have stolen 54 billion cookies, later distributing them on the Dark Web. Cookies involved in authentication procedures are particularly valuable, as these are used by browsers to identify users and verify their login status.

Recently, a critical exploit was discovered that allows the generation of persistent Google cookies through token manipulation. This exploit enables continuous access to Google services, even after a password reset. Another well-documented (https://github.com/mrd0x/WebView2-Cookie-Stealer, accessed on 1 July 2024) example comes from Mr.D0x, an anonymous penetration tester and security researcher who demonstrated how Microsoft Edge WebView2 can be exploited to steal authentication cookies, potentially bypassing multi-factor authentication when accessing stolen accounts.

These examples clearly show that cookies, typically considered harmless, can pose significant security threats. Increasing user awareness about the potential risks associated with cookies could encourage more cautious behavior regarding their use and management.

2.5. Target Population

In an increasingly fast-paced and digitally driven society, online security has become a key concern for all age groups. However, not all people are equally aware of or protected against cyber risks. In particular, young adults are a particularly vulnerable group due to a number of specific factors that make them more susceptible to cyberattacks than other segments of the population.

Young adulthood or late adolescence is a developmental phase spanning the ages of 18 to 25 [44]. During this transitional period, young people move from childhood and adolescent systems into adult-centered systems. The number of young adults spending their free time on gaming consoles, computers, and smartphones is increasing rapidly. As a result, they are the most likely group to encounter various cyber threats and other risks associated with Internet use. A study by Zhao et al. [45] showed that young adults have a good awareness of the risks associated with sharing inappropriate content and approaching people unknown to them, but demonstrated that they lack awareness of the risks associated with sharing personal information online. As reported by Alanazi et al. [46], young adults should be made aware of the risks posed by cyber threats that arise from neglecting online security practices. They need to understand how adopting proper cybersecurity behaviors can lead to positive outcomes, such as staying safe online. Cybersecurity education should include practical demonstrations of the essential security measures that should be practiced in everyday Internet use. Therefore, integrating cybersecurity education with activities that promote incidental learning is especially advantageous for this age group.

3. Game Design

As mentioned earlier, game-based training is gaining popularity as a method for raising awareness about cyber risks [11]. Several notable examples of educational games exist. For instance, Space Shelter (https://spaceshelter.withgoogle.com/intl/it_it/, accessed on 1 July 2024) is a web-based video game developed by Google to raise awareness about online privacy and security. The game educates users about safe web browsing and personal data protection through a fun and interactive experience. Players navigate

a spaceship, choosing an astronaut avatar and advancing by correctly answering quizzes and completing mini-games on online security. Key game mechanics include quizzes, guided completion, and drag-and-drop activities. The game has achieved a high level of engagement with 450,000 unique users, 40% of whom completed the game in an average of 10 min, and is available in seven languages.

Another game aimed at young people is Datak (https://www.datak.ch/#/start, accessed on 1 July 2024). In this single-player game, the player is hired as an intern by the mayor of a city and tasked with managing the social media network, facing various daily dilemmas and time constraints, with advice from YouTube videos. The game addresses topics such as the role of the Internet in everyday life, social networks, user actions, state surveillance, and commerce.

A more ambitious game is Interland (https://beinternetawesome.withgoogle.com/es_es/interland, accessed on 1 July 2024), which is designed to help children (ages 6 to 13) learn key lessons about web safety through four different experiences: the River of Reality (distinguishing truth from falsehood), the Treasure Tower (guarding personal information), the Courteous Kingdom (spreading kindness), and the Responsible Mountain (using technology wisely). The game teaches users to recognize scams, understand phishing and how to report it, safeguard personal information, and create secure and memorable passwords.

All the games mentioned above share a variety of content aimed at providing comprehensive training. This contrasts with the approach we are emphasizing here, the "molecular" and effective transfer of knowledge on a very circumscribed topic.

The game described below targets young adults who frequently use the Internet and are likely to encounter various cyber threats and other risks associated with Internet use [46]. This audience comprises digital natives with a direct and personal relationship with technology and a preference for gamified, active, and competitive learning methods. Involving them in initiatives to raise awareness can promote responsible online behavior and provide them with essential knowledge to help manage their digital privacy effectively. The game is designed to be played on smartphones, which are chosen for their accessibility, familiarity, interactivity, portability, and connectivity.

Razali and colleagues [47] recently tested alongside experts a guideline for designing educational games (in their case, in the field of climate change). The guideline is based on 13 game elements, and it is general enough to be applied to other topics. Below, we will employ their game elements to describe the characteristics of Cookie Aware.

3.1. Goal

The game must have a clear objective so that players can easily understand how to win the game. These goals can be ascribed to what Starks [48] refers to as "in-game" goals and are distinct from the "real-life outcomes", which fall under what Razali and colleagues refer to as "Scope" (see Section 3.4). Therefore, the goal is to obtain citizenship in CookieLand by demonstrating knowledge about cookies. The achievement of this goal is signaled by earning badges, which visibly represent the completion of levels or objectives [49].

3.2. Narrative Content

Storytelling in games enables players to identify with the main character, fostering a stronger connection and increased engagement. Isbister and Schaffer [50] have noted that games with a rich narrative component can significantly enhance the user experience by promoting deeper immersion and involvement. In Cookie Aware, village exploration is the key element of storytelling. To gain citizenship in CookieLand, the main character (Bibi) must earn badges that certify their knowledge of cookies. This knowledge is acquired through interactions with non-playable characters (NPCs), the inhabitants of CookieLand, who share stories about their cookie-related experiences. The believability of these stories can greatly influence player engagement, highlighting the crucial role of a well-crafted narrative in game design [51].

The story takes place in CookieLand (Figure 2), a peaceful village inhabited by various types of cookies. CookieLand exists within everyone's computers, where each cookie has its own unique personality and interests. The game's narrative follows Bibi, an explorer who wishes to move to CookieLand. However, Bibi's transfer is initially halted by the village mayor. According to the village rules, in order to gain citizenship, Bibi must first demonstrate knowledge about the inhabitants and the community's hierarchical relationships.

Figure 2. Graphic visualization of the game setting, CookieLand village.

Bibi begins the journey by speaking with the villagers, who share information and interesting facts about the four quiz challenges that must be completed. After successfully completing each challenge, Bibi earns a badge (Figures 3–5), an official document certifying knowledge advancement. Once Bibi has earned all four badges, the player can finally move to CookieLand.

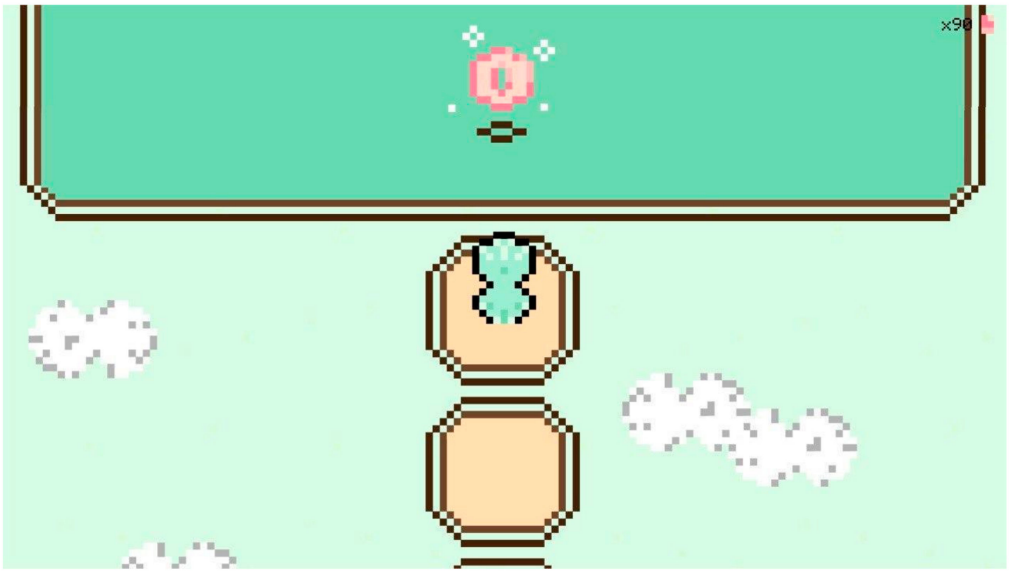

Figure 3. The moment at which the badge is obtained.

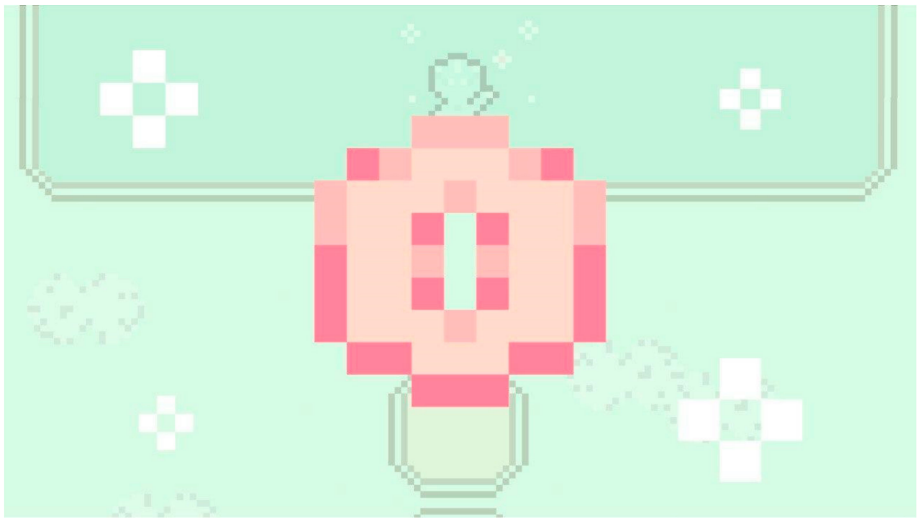

Figure 4. Badge graphics.

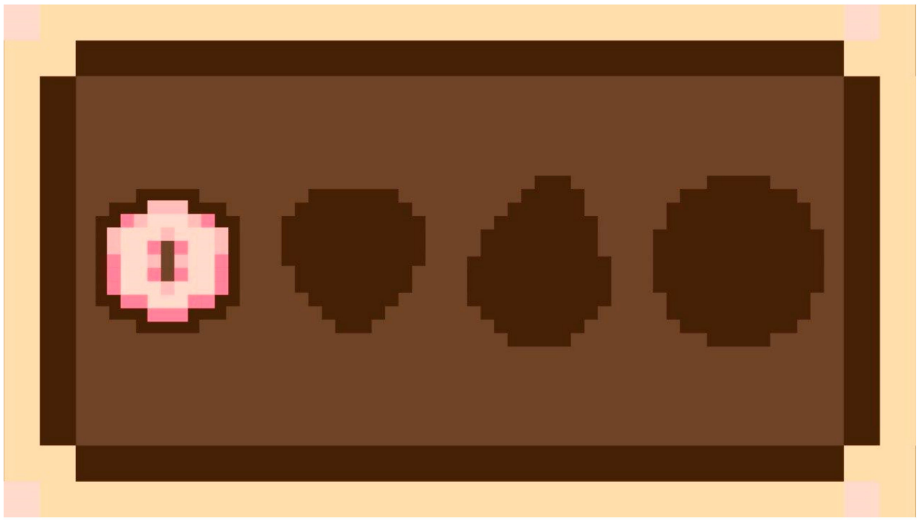

Figure 5. Badge insertion in the medallion box.

3.3. Rules

The game is structured into four levels, each requiring approximately 10 min to complete. To progress to the next level, the player must correctly answer questions related to the current level. Upon successfully completing a level, the player earns a badge. Collecting all the badges demonstrates the player's mastery and grants access to rewards, such as free selected products from vending machines.

3.4. Scope

The scope of the game is to enhance individuals' awareness and knowledge of cybersecurity. Specifically, the game aims to educate players on the importance of cookie management, explaining how cookies impact online privacy and security, and promoting responsible practices to protect personal data.

3.5. Genre

Cookie Aware blends two game genres to create an engaging experience. The first genre is the quiz, where players answer questions correctly to progress. Quizzes are known for their benefits in terms of learning and memory retention. Research by Butler and Roediger [52] highlighted how tests and quizzes can enhance information retention over time, demonstrating that testing is a powerful educational tool. In 2011, Butler and

Roediger further emphasized that the act of retrieving information during quizzes can improve long-term knowledge storage. Similarly, Blunt [53] explored how educational games, including quizzes, positively impact learning by boosting both engagement and memorization. There is a strong consensus that quizzes are effective learning tools.

The second genre featured in Cookie Aware is the role-playing game (RPG). RPGs enhance user immersion by encouraging players to identify with the game's protagonist, allowing for a deeper, more engaging experience. Role-playing games can enhance problem-solving skills by teaching players to first gather information and devise a strategy before attempting to solve a problem. In a longitudinal study, Adachi and Willoughby [54] showed that adolescents who played strategic video games across many years of high school reported steeper increases in self-reported problem-solving skills over time compared to participants who reported less sustained play.

3.6. Esthetic

The visual elements of the game are crucial in creating an engaging and memorable experience. Cookie Aware achieves this through a combination of pixel art graphics, pastel colors, and playful electronic sounds. The game's design draws inspiration from some of the most beloved classics in gaming, including *Pokémon Sapphire*, *The Legend of Zelda*, *Dragon Quest III*, and *Space Invaders*. Key visual elements from these games have been adapted and integrated to enhance the overall gaming experience.

Pixel art graphics were chosen for their simplicity and clarity, making the information easy to comprehend. Each character, icon, and scene is meticulously crafted with detailed pixel art, blending both playful and informative aspects. The typography features the Minecraft font, which is widely recognized due to its popularity.

Saturated, high-contrast colors were selected to ensure that there was a clear distinction between game elements, improving usability. The pastel palette creates a relaxing atmosphere, with blue and pink hues often used in confectionery advertising to offer a pleasant visual experience (Figure 6). Animations and transitions add dynamism to the gameplay. The initial vertical scrolling transition provides a panoramic view of the village, followed by a zoom-in on the protagonist entering the settlement. The game's instructions and objectives are then presented. Subsequent transitions track the protagonist's movements, zooming in on character interactions and changes in setting.

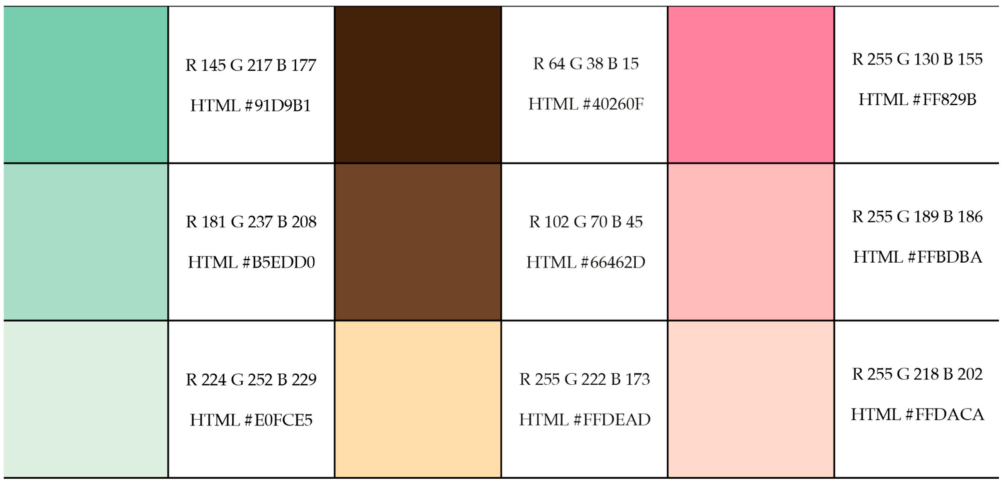

Figure 6. Color palette.

Playful electronic sounds further enhance the game's immersion. The soundtrack deepens the context of on-screen actions, while sound effects make the virtual world feel more realistic and responsive, providing immediate feedback to the player's actions and changes within the game environment.

3.7. Character Design

The game character represents the player within the game and often determines its success. In any game, the character plays a unique and crucial role, serving as the player's avatar as they navigate a virtual world filled with adventures and challenges [55]. However, a character holds little significance if it is not designed with a clear goal in mind. A game's storyline, conflicts, challenges, and atmosphere come together meaningfully when the main character has a specific objective for players to achieve at each level [56].

For the development of character design, Burgerman's [57] "20 Top Character Design Tips" served as a reference. The protagonist of Cookie Aware is Bibi, who resides within our electronic device but dreams of living in the beautiful town of CookieLand. Bibi is gender-neutral and designed without any specific characteristics that might hinder players' ability to empathize with them. Bibi's signature color is a light blue/teal, while the non-playable characters (NPCs) in CookieLand feature colors reminiscent of real cookies, making them easily recognizable and allowing Bibi to stand out within the setting.

3.8. Game Mode

Cookie Aware is designed as a single-player offline game where players earn badges by demonstrating their knowledge about cookies, enabling Bibi to eventually move into the village. The game features a scoring system, which ranks players and introduces an (online) element of competition. This can be especially beneficial at the class or school level, as it encourages greater participation in the game.

3.9. Game Level Design

The game's allocentric representation is based on a map constructed over a geometric grid. Only a portion of the world is displayed on the screen at any given time, encouraging players to explore further. This type of design is common in video game sagas such as Pokémon, Zelda, and Dragon Quest. The game features five distinct areas, each designed to introduce different concepts and information to the player.

3.10. Quiz

The game's narrative structure guides players through a series of quiz levels, where they receive immediate feedback and can earn badges. Forty questions were initially developed and divided across four levels to help users gain a solid understanding of cookies. Players start at the first level and advance to the next after successfully answering all questions in the current level. This progressive structure keeps players motivated and engaged, continuously challenging them to improve their performance.

The questions are varied, ranging from informative to ironic and friendly, making the experience both educational and entertaining. The initial questions are relatively simple, helping participants ease into the topic and build confidence. As the game progresses, the questions become more complex, requiring a deeper understanding, critical analysis, and practical application of the information. Each question offers four options, with only one correct answer (see the question example in Figure 7). Regardless of whether the player answers correctly, a detailed explanation is provided to deepen their understanding and prevent misconceptions (see Figure 8).

Each level focuses on a specific aspect of cookies, providing a comprehensive overview:

- Knowledge (Introduction to Cookies): The first level introduces players to the basics of cookies, covering key concepts such as what cookies are, where they come from, their primary purpose, and the types of information they store. This level also explains relevant cookie regulations, including the GDPR 2018 regulation. It serves as an essential foundation for players, helping them understand cookies before moving on to more complex topics in later levels.
- Types (Types of Cookies): In the second level, players learn to identify different types of cookies and understand the kinds of information they store. This level distinguishes between technical, profiling, and third-party cookies, as well as between session and

persistent cookies. It also explains the differences between hybrid and zombie cookies, highlighting how they differ from traditional cookies and the common issues caused by zombie cookies during browsing.

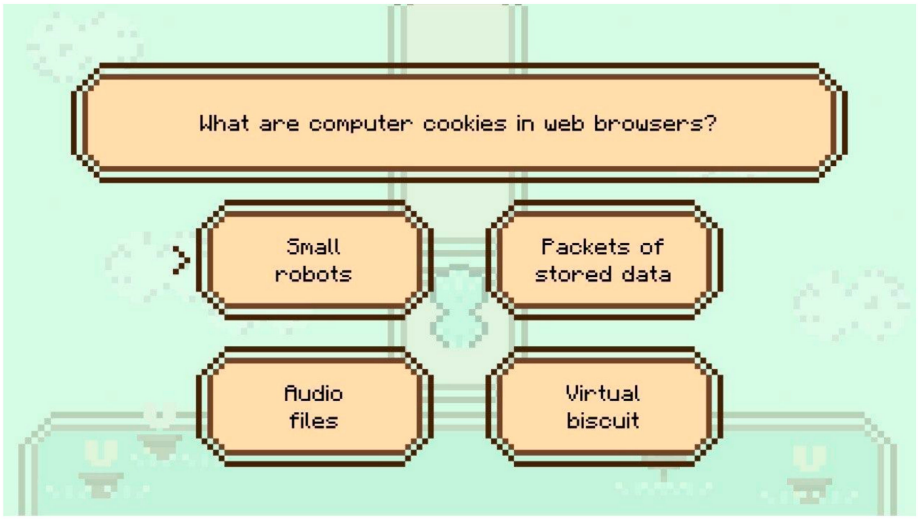

Figure 7. Example question with answer alternatives.

Figure 8. A more detailed explanation of the correct answer. Feedback is given both in the case of an incorrect answer and a correct answer by the player.

- Risks (Risks and Threats): The third level focuses on the potential risks associated with cookies, such as user tracking. It emphasizes the importance of being aware of these risks, particularly since cookies can handle sensitive information, including personal and financial data. This level also covers cyberattacks that exploit cookies, such as cookie poisoning and cross-site scripting (XSS), as well as the consequences of session cookie breaches and the best practices for safely managing cookies.
- Solutions (Solutions and Best Practices): The final level provides practical tips and strategies for safely managing cookies. It covers the importance of deleting cookies and offers guidance on how to control and manage them in browsers. This level also explains the functions of common cookie management tools, the effects of browsing in private or incognito mode, and explores safer alternatives to cookies. Additionally, it highlights the benefits of using the "I Don't Care About Cookies" extension and discusses how to identify GDPR-compliant sites, stressing the importance of reading privacy policies and cookie-related documents.

After correctly answering all 10 questions in a level, the level is considered complete (see Figure 9).

Figure 9. Screen upon the completion of the level.

3.11. Reward

Cookie Aware involves a token economy, an exchange system that provides immediate feedback on the appropriateness of individuals' behavior [58]. Tokens, or "exchangeables," are earned by achieving specific behavioral goals over a set period and can be traded for tangible rewards or privileges. Although tokens have no intrinsic value, they function as reinforcers—stimuli or events that increase the likelihood of a behavior when given in response to that behavior. If a stimulus does not result in a higher frequency of the target behavior, it is not considered a reinforcer. A key component of the token economy is the exchange of tokens for backup rewards.

The game will also feature a response cost system, taking away tokens when inappropriate behavior occurs. That will also add dynamism to the game.

3.12. Challenge

The game's challenge is driven by two mechanisms: (1) the progressively increasing difficulty of the questions within each level and during transitions between levels; (2) occasional pop-ups prompting choices to give consent to a great variety of permissions. Player responses will determine the dynamics of the game by allowing either a smooth exploration or disadvantages (e.g., obstacles, opponents).

3.13. Rank

Rank is an integral part of the game dynamics. The character's status changes from level to level, also changing some features of the character's appearance (e.g., color) and an update of the progress bar. As mentioned in Section 3.8, introducing a ranking system can encourage participation, with competition serving as a significant motivator [59]. The score obtained can also provide valuable feedback, helping players decide whether to replay a level to improve their ranking.

4. Discussion and Conclusions

The goal of this article was twofold. On the one hand, we wanted to argue for the preference of information/education "pills" over the more comprehensive courses usually offered in organizations to improve the awareness of non-expert users. On the other hand, we wanted to provide an example of a forthcoming intervention on a circumscribed topic that would take advantage of an informal/incidental learning mode.

From the literature review, two aspects seem to be salient in the use of informal learning strategies. The first is the need to define the audience for training. For example, adult employees of an organization and college students represent two different populations with different habits and approaches to information consumption. Second, it is necessary reduce the complexity of information/training units to ensure the learning and generalization of key concepts. Although any type of content can be delivered using informal learning approaches, the temptation to explain a phenomenon (e.g., phishing) in exhaustive detail must be resisted in favor of exposing the user to instances of a phenomenon (e.g., using mouseover to verify the nature of a link before clicking) that can then be more easily generalized to other situations. Traditional courses, by their nature, tend to consist of instructional modules that represent a more or less homogeneous organization of content. However, any categorization is reductive to the myriad of issues within the broad context of cybersecurity, some of which are often overlooked, even though they can have devastating consequences for the victims.

The concept is not new, and we can find similar approaches under the name of "microlearning" [60,61], in which complex information is broken down into smaller modules that are easy for the learner to use. However, microlearning still involves short lessons that can be accessed via mobile phone apps or via computers, whereas what we are advocating here is to create situations in which the users stumble upon content and increase their knowledge while they are doing something else. Social media offer an ideal venue for providing short, circumstantial content that is easy to consume, and that can be propagated through the mechanism of sharing. It is definitely an approach that should be considered in order to create awareness in a population and instill proper behavior. Indeed, this approach also qualifies as a strategy for creating verbal antecedents for rule-governed behavior. As an alternative to rule-governed behaviors, learning often occurs as a function of reinforcement contingencies. People enact behaviors that are followed by consequences, and these consequences reinforce that behavior.

Game environments are highly effective for establishing contingencies. The feedback received during gameplay, along with badges and accumulated points, provides positive reinforcement that helps to solidify learning. The use of a token economy is well documented in the literature as a strategy to keep the individual engaged in the learning process. Here, we have designed a simple game that can appeal to students and let them learn about a very specific topic usually overlooked by traditional cybersecurity training. Points and badges gained throughout the game experience could be used to gain status in classroom or school rankings, stimulating students to improve their performance (i.e., learning) while they are performing a leisure activity.

Future Directions

In this article, we presented a minimalist game to informally educate about cookies. Here, we explained its background, purpose, target audience, structure, content, game dynamics, and style. This is the first step in a project with many more phases. The next phases will focus on implementing the game and evaluating its effectiveness. The evaluation of strategies to improve cybersecurity awareness—and their potential impact on the adoption of appropriate behavior—should be a focus of research in this area. Cookie Aware will serve as a test bed for this, comparing the knowledge gained through this gaming platform with traditional teaching methods on the same topic.

A forthcoming study will assign participants to one of three experimental conditions: watching a video lesson, interacting directly with the game, and watching a video of a third person playing the game. The third condition is designed to assess the actual impact of the game experience beyond the content delivery method. All participants will complete the Cybersecurity Awareness Inventory [5], which will be used as a covariate to check prior cybersecurity knowledge. This study should provide valuable data on students' cybersecurity knowledge and establish a benchmark for future applications.

In addition, partnerships could be established with companies that operate vending machines in schools and colleges, as these machines often integrate smartphone applications that facilitate purchases. Cookie Aware could be seamlessly integrated into these applications, creating an innovative incentive for students to participate in the game by converting virtual rewards (points, badges) into tangible benefits such as free or discounted snacks and drinks from vending machines.

This partnership model could be customized for different institutions, allowing schools and universities to tailor rewards to their students' preferences, which could further increase engagement.

For educational institutions, this approach offers an innovative way to integrate gamified learning into daily routines, making cybersecurity education more relevant, interactive, and accessible. This collaboration could eventually serve as a model for other educational games that seek to combine learning with real-world incentives.

Cookie Aware could also be incorporated into high school projects focused on cybersecurity education. Such projects, aimed at teenagers, aim to develop the skills required for the safe and conscious use of the Internet and provide students with the resources to manage digital risks. These educational programs typically cover topics such as protecting personal information, managing strong passwords, recognizing online threats (such as phishing), and using social media responsibly. Cookie Aware, with its focus on educating users about cookies and privacy, aligns perfectly with these goals by providing tools that demonstrate how everyday online behavior can affect personal security.

In addition, Cookie Aware could facilitate discussions about digital ethics and privacy by encouraging students to think critically about the information they share online and the consequences of their actions. By incorporating Cookie Aware into cybersecurity education, schools can provide students with better tools to make informed decisions about their online presence, fostering a generation that is not only tech-savvy, but also aware of the importance of maintaining privacy and security in an increasingly connected world.

Author Contributions: The activity reported in this paper originates from a project work carried out by S.M., M.P.P. and A.B., under the supervision of F.D.N. and G.T., as part of their participation in class activities at the Master Program in Design, Multimedia, and Visual Communication, Sapienza University of Rome, Italy. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study.

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

References

1. Rahman, T.; Rohan, R.; Pal, D.; Kanthamanon, P. Human factors in cybersecurity: A scoping review. In Proceedings of the 12th International Conference on Advances in Information Technology, Bangkok, Thailand, 29 June–1 July 2021; pp. 1–11.
2. Alsharif, M.; Mishra, S.; AlShehri, M. Impact of Human Vulnerabilities on Cybersecurity. *Comput. Syst. Sci. Eng.* **2022**, *40*. [CrossRef]
3. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A comparative study. *J. Comput. Inf. Syst.* **2022**, *62*, 82–97. [CrossRef]
4. Lorenz, B.; Kikkas, K.; Klooster, A. The four most-used passwords are love, sex, secret, and god: Password security and training in different user groups. In Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust, Las Vegas, NV, USA, 21–26 July 2013; pp. 276–283.
5. Tempestini, G.; Rovira, E.; Pyke, A.; Di Nocera, F. The Cybersecurity Awareness INventory (CAIN): Early Phases of Development of a Tool for Assessing Cybersecurity Knowledge Based on the ISO/IEC 27032. *J. Cybersecur. Priv.* **2023**, *3*, 61–75. [CrossRef]
6. Di Nocera, F.; Tempestini, G.; Presaghi, F. Reliability and validity of the Cybersecurity Awareness INventory (CAIN). *Behav. Inf. Technol.* **2024**, 1–12. [CrossRef]

7. González-Manzano, L.; de Fuentes, J.M. Design recommendations for online cybersecurity courses. *Comput. Secur.* **2019**, *80*, 238–256. [CrossRef]
8. Payne, B.K.; He, W.; Wang, C.; Wittkower, D.E.; Wu, H. Cybersecurity, technology, and society: Developing an interdisciplinary, open, general education cybersecurity course. *J. Inf. Syst. Educ.* **2021**, *32*, 1334. [CrossRef]
9. He, W.; Zhang, Z. Enterprise cybersecurity training and awareness programs: Recommendations for success. *J. Organ. Comput. Electron. Commer.* **2019**, *29*, 249–257. [CrossRef]
10. He, W.; Ash, I.; Anwar, M.; Li, L.; Yuan, X.; Xu, L.; Tian, X. Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *J. Intellect. Cap.* **2020**, *21*, 203–213. [CrossRef]
11. Pruemmer, J.; van Steen, T.; van den Berg, B. A systematic review of current cybersecurity training methods. *Comput. Secur.* **2023**, *136*, 103585. [CrossRef]
12. Abawajy, J. User preference of cyber security awareness delivery methods. *Behav. Inf. Technol.* **2014**, *33*, 237–248. [CrossRef]
13. Cerasoli, C.P.; Alliger, G.M.; Donsbach, J.S.; Mathieu, J.E.; Tannenbaum, S.I.; Orvis, K.A. Antecedents and outcomes of informal learning behaviors: A meta-analysis. *J. Bus. Psychol.* **2018**, *33*, 203–230. [CrossRef]
14. Marsick, V.J.; Watkins, K. *Informal and Incidental Learning in the Workplace*; Routledge: New York, NY, USA, 2015.
15. Blume, B.D.; Ford, J.K.; Baldwin, T.T.; Huang, J.L. Transfer of training: A meta-analytic review. *J. Manag.* **2010**, *36*, 1065–1105. [CrossRef]
16. Lecat, A.; Raemdonck, I.; Beausaert, S.; März, V. The what and why of primary and secondary school teachers' informal learning activities. *Int. J. Educ. Res.* **2019**, *96*, 100–110. [CrossRef]
17. Mahoney, J.L.; Larson, R.W.; Eccles, J.S. (Eds.) *Organ. Act. as Context. Dev. Extracurricular Act. after-School Community Programs*; Lawrence Erlbaum Associates Publishers: Mahwah, NJ, USA, 2005; pp. 3–22.
18. Rader, E.; Wash, R. Identifying patterns in informal sources of security information. *J. Cybersecur.* **2015**, *1*, 121–144. [CrossRef]
19. Rader, E.; Wash, R.; Brooks, B. Stories as informal lessons about security. In Proceedings of the Eighth Symposium on Usable Privacy and Security, Washington, DC, USA, 11–13 July 2012; pp. 1–17.
20. Pfeffer, K.; Mai, A.; Weippl, E.; Rader, E.; Krombholz, K. Replication: Stories as informal lessons about security. In Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022), Boston, MA, USA, 7–9 August 2022; pp. 1–18.
21. Švábenský, V.; Čeleda, P.; Vykopal, J.; Brišáková, S. Cybersecurity knowledge and skills taught in capture the flag challenges. *Comput. Secur.* **2021**, *102*, 102154. [CrossRef]
22. Balon, T.; Baggili, I. Cyber Competitions: A survey of competitions, tools, and systems to support cybersecurity education. *Educ. Inf. Technol.* **2023**, *28*, 11759–11791. [CrossRef]
23. Breuer, J.; Bente, G. Why so serious? On the relation of serious games and learning. *J. Comput. Game Cult.* **2010**, *4*, 7–24. [CrossRef]
24. 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]
25. Alotaibi, F.; Furnell, S.; Stengel, I.; Papadaki, M. A review of using gaming technology for cyber-security awareness. *Int. J. Inf. Secur. Res. (IJISR)* **2016**, *6*, 660–666. [CrossRef]
26. Hill, W.A., Jr.; Fanuel, M.; Yuan, X.; Zhang, J.; Sajad, S. A survey of serious games for cybersecurity education and training. *KSU Proc. Cybersecur. Educ. Res. Pract.* **2020**, *7*, 1–17.
27. Kulshrestha, S.; Agrawal, S.; Gaurav, D.; Chaturvedi, M.; Sharma, S.; Bose, R. Development and validation of serious games for teaching cybersecurity. In Proceedings of the Serious Games: Joint International Conference, JCSG 2021, Virtual Event, 12–13 January 2022; Proceedings 7. Springer International Publishing: Berlin/Heidelberg, Germany, 2022; pp. 247–262.
28. Coenraad, M.; Pellicone, A.; Ketelhut, D.J.; Cukier, M.; Plane, J.; Weintrop, D. Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games. *Simul. Gaming* **2020**, *51*, 586–611. [CrossRef]
29. Hart, S.; Margheri, A.; Paci, F.; Sassone, V. Riskio: A serious game for cyber security awareness and education. *Comput. Secur.* **2020**, *95*, 101827. [CrossRef]
30. Jaffray, A.; Finn, C.; Nurse, J.R. Sherlocked: A detective-themed serious game for cyber security education. In Proceedings of the Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, 7–9 July 2021; Proceedings 15. Springer International Publishing: Berlin/Heidelberg, Germany, 2021; pp. 35–45.
31. Gaurav, D.; Kaushik, Y.; Supraja, S.; Yadav, M.; Gupta, M.P.; Chaturvedi, M. Empirical study of adaptive serious games in enhancing learning outcome. *Int. J. Serious Games* **2022**, *9*, 27–42. [CrossRef]
32. Skinner, B.F. An operant analysis of problem solving. In *Problem Solving: Research, Method, and Theory*; Kleinmuntz, B., Ed.; Wiley: New York, NY, USA, 1966; pp. 225–257.
33. Skinner, B.F. An operant analysis of problem solving, Note 6.1–6.4. In *Contingencies of Reinforcement: A Theoretical Analysis*; Skinner, B.F., Ed.; Appleton-Century-Crofts: New York, NY, USA, 1969; pp. 157–171.
34. Pierce, W.D.; Cheney, C.D. *Behavior Analysis and Learning: A Biobehavioral Approach*; Routledge: London, UK, 2017.
35. Deterding, S.; Sicart, M.; Nacke, L.; O'Hara, K.; Dixon, D. Gamification. Using game-design elements in non-gaming contexts. In Proceedings of the CHI'11 Extended Abstracts on Human Factors in Computing Systems, Vancouver, BC, Canada, 7–12 May 2011; pp. 2425–2428.
36. Skinner, B.F. The shame of American education. *Am. Psychol.* **1984**, *39*, 947. [CrossRef]
37. Di Nocera, F.; Tempestini, G. Getting rid of the usability/security trade-off: A behavioral approach. *J. Cybersecur. Priv.* **2022**, *2*, 245–256. [CrossRef]

38. Utz, C.; Degeling, M.; Fahl, S.; Schaub, F.; Holz, T. (Un) informed consent: Studying GDPR consent notices in the field. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 973–990.
39. Giese, J.; Stabauer, M. Factors that Influence Cookie Acceptance. In *HCI in Business*; Fui-Hoon Nah, F., Siau, K., Eds.; Government and Organizations; HCII 2022; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2022; Volume 13327.
40. Kulyk, O.; Hilt, A.; Gerber, N.; Volkamer, M. "This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer. In Proceedings of the European Workshop on Usable Security (EuroUSEC), London, UK, 23 April 2018.
41. Bravo-Lillo, C.; Cranor, L.; Komanduri, S.; Schechter, S.; Sleeper, M. Harder to ignore? Revisiting {Pop-Up} fatigue and approaches to prevent it. In Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS 2014), Menlo Park, CA, USA, 9–11 July 2014; pp. 105–111.
42. Bravo-Lillo, C.; Komanduri, S.; Cranor, L.F.; Reeder, R.W.; Sleeper, M.; Downs, J.; Schechter, S. Your attention please: Designing security-decision UIs to make genuine risks harder to ignore. In Proceedings of the Ninth Symposium on Usable Privacy and Security, Newcastle, UK, 24–26 July 2013; pp. 1–12.
43. NordVPN Misfortune Cookie? Billions of Stolen Cookies Expose Your Data. Available online: https://nordvpn.com/research-lab/stolen-cookies-study/ (accessed on 1 July 2024).
44. Higley, E. Defining Young Adulthood. *DNP Qualif. Manuscr.* **2019**, *17*, 1–28. Available online: https://repository.usfca.edu/dnp_qualifying/17 (accessed on 1 July 2024).
45. Zhao, J.; Wang, G.; Dally, C.; Slovak, P.; Edbrooke-Childs, J.; Van Kleek, M.; Shadbolt, N. I make up a silly name' Understanding Children's Perception of Privacy Risks Online. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, Scotland, UK, 4–9 May 2019; pp. 1–13.
46. Alanazi, M.; Freeman, M.; Tootell, H. Exploring the factors that influence the cybersecurity behaviors of young adults. *Comput. Hum. Behav.* **2022**, *136*, 107376. [CrossRef]
47. Razali, N.E.M.; Ramli, R.Z.; Mohamed, H.; Zin NA, M.; Rosdi, F.; Diah, N.M. Identifying and validating game design elements in serious game guidelines for climate change. *Heliyon* **2022**, *8*, e08773. [CrossRef]
48. Starks, K. Cognitive behavioral game design: A unified model for designing serious games. *Front. Psychol.* **2014**, *5*, 28. [CrossRef]
49. Antin, J.; Churchill, E.F. Badges in Social Media: A Social Psychological Perspective. In Proceedings of the CHI 2011 Gamification Workshop Proceedings, Vancouver, BC, Canada, 7–12 May 2011; ACM Press: New York, NY, USA, 2011.
50. Isbister, K.; Schaffer, N. *Game Usability: Advancing the Player Experience*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2008.
51. Lankoski, P.; Björk, S. Gameplay design patterns for believable non-player characters. In Proceedings of the DiGRA 2007 Conference: Situated Play, Tokyo, Japan, 24–28 September 2007.
52. Butler, A.C.; Roediger, H.L., III. Testing improves long-term retention in a simulated classroom setting. *Eur. J. Cogn. Psychol.* **2007**, *19*, 514–527. [CrossRef]
53. Blunt, R. Do serious games work? Results from three studies. *ELearn* **2009**, *2009*, 1. [CrossRef]
54. Adachi, P.J.; Willoughby, T. More than just fun and games: The longitudinal relationships between strategic video games, self-reported problem solving skills, and academic grades. *J. Youth Adolesc.* **2013**, *42*, 1041–1052. [CrossRef] [PubMed]
55. Rogers, S. *Level Up! The Guide to Great Video Game Design*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
56. Kuntjara, H.; Almanfaluthi, B. Character design in games analysis of character design theory. *J. Games Game Art Gamification* **2017**, *2*, 42–47. [CrossRef]
57. Burgerman, J. 20 Top Character Design Tips. Available online: http://www.creativebloq.com/character-design/tips-51326432015 (accessed on 7 August 2024).
58. Ivy, J.W.; Meindl, J.N.; Overley, E.; Robson, K.M. Token economy: A systematic review of procedural descriptions. *Behav. Modif.* **2017**, *41*, 708–737. [CrossRef] [PubMed]
59. Vorderer, P.; Klimmt, C.; Ritterfeld, U. Enjoyment: At the heart of media entertainment. *Commun. Theory* **2004**, *14*, 388–408. [CrossRef]
60. Busse, J.; Lange, A.; Hobert, S.; Schumann, M. How to Design Learning Applications That Support Learners in Their Moment of Need–Didactic Requirements of Micro Learning. In Proceedings of the Americas Conference on Information Systems (AMCIS 2020), Salt Lake City, UT, USA, 12–16 August 2020; pp. 1–10.
61. Leong, K.; Sung, A.; Au, R.; Lee, C. A study of preferred learning time of online learners in multimedia microlearning in higher education contexts. *Online J. TVET Pract.* **2022**, *7*, 11–23. [CrossRef]