

## A comprehensive cybersecurity learning platform for elementary education

Filippos Giannakas, Andreas Papasalouros, Georgios Kambourakis & Stefanos Gritzalis

To cite this article: Filippos Giannakas, Andreas Papasalouros, Georgios Kambourakis & Stefanos Gritzalis (2019) A comprehensive cybersecurity learning platform for elementary education, Information Security Journal: A Global Perspective, 28:3, 81-106, DOI: [10.1080/19393555.2019.1657527](https://doi.org/10.1080/19393555.2019.1657527)

To link to this article: <https://doi.org/10.1080/19393555.2019.1657527>



Published online: 30 Aug 2019.



Submit your article to this journal [↗](#)



Article views: 29



View related articles [↗](#)



View Crossmark data [↗](#)



# A comprehensive cybersecurity learning platform for elementary education

Filippos Giannakas <sup>a</sup>, Andreas Papasalouros<sup>b</sup>, Georgios Kambourakis<sup>a</sup>, and Stefanos Gritzalis<sup>a</sup>

<sup>a</sup>Department of Information and Communication Systems Engineerings, University of the Aegean, Samos, Greece; <sup>b</sup>Department of Mathematics, University of the Aegean, Samos, Greece

## ABSTRACT

For elementary students, security and privacy education is anticipated to be more joyful when the knowledge is delivered in the form of a digital game-based learning activity. This paper details on the development of a novel learning platform that comprises a web-based Learning Content Management Systems (LCMS) and a mobile client application (app) for educating and raising young learners' awareness on basic cybersecurity and privacy issues. The app, which comprises a suite of quick games, can be played either in standalone or in client/server mode and it is especially destined to elementary students. Further, due to the anytime and anywhere characteristics of the app, it can be experienced as a classroom or an outdoor learning activity. Contrary to analogous studies found in the literature so far, during the design phase of the app, our focus was not solely on its technological aspects, but we uniformly paid special attention to the educational factor by applying the Attention, Relevance, Confidence, and Satisfaction (ARCS) model of motivation. A preliminary evaluation of the app, including learning effectiveness, usability, and user's satisfaction was conducted with 52 elementary-aged students. Among others, the results show that the interaction with the app significantly increases the mean performance of the participants by almost 20%.

## KEYWORDS

Security and privacy education; m-Learning; mobile-DGBL; motivation; ARCS; learning theory



## 1. Introduction

Over the last decades, the concept of integrating learning and entertainment appeared in the Information Technology (IT) field and shaped new terms including “learning by playing”, “Educational entertainment (Edutainment)” and “Digital Game Based Learning (DGBL)”. Today, the latter term typically refers to the use of digital games to support teaching and learning. Such games can be played over the Internet, on personal computers, smartphones, or on specific mobile or traditional game consoles. From the time of legacy edutainment software designed to serve educational purposes back in the 1990s to modern educational game software, many researchers agreed on the value of DGBL to the learning process (Burguillo, 2010; Lepper & Malone, 1987; Malone, 1981; Woo, 2014; Yang, 2012).

Nowadays, smart mobile devices have established themselves as one of the most developing markets worldwide transforming e-Learning to a new type of independent and ubiquitous type of learning, which is known as “mobile-Learning

(m-Learning)” (Kambourakis, Kontoni, Rouskas, & Gritzalis, 2007; Kambourakis, Kontoni, & Sapounas, 2004). In m-Learning, various forms of activities are enabled, such as discussions, collaboration, access to learning content and course materials available anywhere, anytime, and from arbitrary device types (Gikas & Grant, 2013; Korucu & Alkan, 2011). On the other hand, blending m-Learning with games, becomes gradually a disciplinary challenge, since this type of learning combines mobile characteristics and the human activity of play for motivating learners (Rau, Gao, & Wu, 2008).

Moreover, the proliferation of Internet-connected devices along with the rise of social networking has revolutionized the way people communicate with their peers, do business, and manage their online daily activities. However, this ubiquitous connectivity is associated with various delinquent behaviors pertaining to a great variety of cyber crimes and frauds. For instance, semantic attacks (also known as social engineering) such as phishing, aim to deceive or lure people into, say, visiting a seemingly

**CONTACT** Filippos Giannakas  [fgiannakas@aegean.gr](mailto:fgiannakas@aegean.gr)  Department of Information and Communication Systems Engineerings, University of the Aegean, Greece

Color versions of one or more of the figures in the article can be found online at [www.tandfonline.com/uiss](http://www.tandfonline.com/uiss).

legitimate hyperlink in hopes to disclose their personal information. Similar attacks intend to violate computing devices and usurp users' personal information via the use of malware. Ordinary users are also prone to identity theft and fraud when they choose weak passwords to access their accounts over the Web. Mostly, the aforementioned attacks aim to exploit humans' weaknesses and the lack of knowledge about security and privacy, rather than taking advantage of vulnerabilities found in operating systems, communication protocols, and so forth. This is quite expected since threats of this kind are typically unknown to the non-security-savvy individual, while for some others, the knowledge on security protection measures and privacy awareness is mostly regarded as a secondary task (Kambourakis, 2014).

In this context, mitigating the human-related vulnerabilities is a dominant factor for improving security either at a personal or organizational level. This can be done by raising user awareness on cybersecurity and privacy issues (Giannakas, Kambourakis, Papasalouros, & Gritzalis, 2016), already since the early school-age. This learning goal becomes more important especially among primary (K-6) and secondary school-age students (K-12) due to their increasing engagement in various online activities, often via a range of mobile devices. According to the literature (Giannakas, Kambourakis, & Gritzalis, 2015), the particular learning task has greater chances to succeed if it is delivered through the use of DGBL. If so, the learning experience turns out to be more attractive and personalized, especially for the young learners (Komalawardhana & Panjaburee, 2018). Also, given that the great majority of children and teenagers experience the Internet via mobile devices, the positive outcomes of DGBL can be further enhanced if the learning content is delivered via the use of a mobile app. In fact, this form of learning has been applied to diverse scientific fields and curricula, and more lately to cybersecurity education (Giannakas, Kambourakis, Papasalouros, & Gritzalis, 2017).

Given the above, we consider that in science education in general, and in cybersecurity and privacy in particular, the design and implementation of an effective DGBL platform is a multidisciplinary challenge. This stands true for a number of reasons. First, human learning particularities must be taken into account

along with the inherent technological characteristics and the advances of mobile technology. Second, special attention should be paid on how a learning theory and an appropriate instructional design model are embedded in the development of the (serious) game in order to maximize its learning outcomes. Third, due to the plethora of Internet connected devices and the efforts in coding new apps, there is a need of deploying the DGBL app in arbitrary mobile devices. In this respect, DGBL platform independence becomes an important issue not only because it overcomes the different mobile peculiarities, but also because it is expected to augment the anywhere, anytime learning experience. The latter point can be also examined in conjunction with the Bring Your Own Device (BYOD) policy, since it is anticipated to increase learners' satisfaction when they use their own devices, and to extend the app's dissemination prospects (Vieira & Coutinho, 2017).

*Our contribution:* Motivated by the aforementioned issues, the paper at hand details on the design and development of a novel educational platform called "CyberAware". Specifically:

- A cross-platform app was developed destined to cybersecurity and privacy education with a special focus on elementary students.
- Learning content administration and management functionalities (e.g., managing educators, learners, and virtual classes) were applied, by developing a Learning Content Management System (LCMS) as the back-end.
- Contrary to other works in the literature, our contribution does not only concentrate on the technical aspects of the platform, but also on pedagogical factors with the aim of keeping learners on track. That is, as detailed in Section 4, the app is based on the Attention, Relevance, Confidence, and Satisfaction (ARCS) model of motivation (Keller, 1987a).
- Both a descriptive and differential parametric analysis were applied for the evaluation of the app under different prisms, namely learning effectiveness, usability, system resource consumption, and students' satisfaction and expectations.

The rest of the paper is structured as follows. The next section briefly addresses the related

work. Section 3 details on the LCMS and the gaming app. The motivational learning model along with the conceptual framework that drive the design of the app are discussed in Section 4. Implementation issues are addressed in Section 5. Section 6 is devoted to the evaluation of the app, while the last section concludes the paper and gives pointers to future work.

## 2. Related work

In information security and privacy domains, DGBL is probably the sole method to be used toward educating young learners (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010). This section succinctly reviews the corresponding literature and identifies its shortcomings. For a more detailed coverage of DGBL, the interested reader can refer to Giannakas et al. (2017).

“PhishGuru” (Kumaraguru et al., 2010) is a story-based anti-phishing educational standalone software that aims at alerting learners about email phishing attacks. Also, “Anti-Phishing Phil” (Sheng et al., 2007) complements Kumaraguru et al. (2010) for the purpose of teaching users how to properly use cues in Uniform Resource Locators (URLs) in order to protect themselves against phishing attacks. That is, the authors’ main goal is to familiarize users with ways of identifying if a cue that appears in the web browser’s address bar corresponds to a malicious site. In this respect, Anti-Phishing Phil provides an entertaining platform for teaching more difficult anti-phishing tactics which are not addressed by PhishGuru. Both the aforementioned games are based on certain learning theories, namely Conceptual knowledge (Star & Stylianides, 2013) and Reflection (Boud, Keogh, & Walker, 2015) respectively. From the results in (Kumaraguru et al., 2010), it seems that the individuals who played the aforementioned games were more skillful in identifying fraudulent websites and phishing-account emails. “SecurityCartoons” (Srikwan & Jakobsson, 2008) is another online web-based game that simply embeds the graphical concept of cartoons as its main media type. This game is designed to increase users’ security awareness against security threats as well as to advise them on how to protect themselves against major Internet attacks, including identity theft, phishing, and others. The work by

Dasgupta, Ferebee, and Michalewicz (2013) is a puzzle-based interactive learning environment for teaching basic cybersecurity issues. The authors elaborate on the possible ways a network protocol and inbound/outbound communications in general can affect system security. The authors focus on sensitive data breaches and their implications to the individuals involved. “Be Internet Awesome” (Google, 2017) is an online web-based game that introduces topics related to phishing attacks, Internet harassment, password security, and other networking safety issues. The game comprises four learning sections in regards to the sharing of personal information online, avoiding phishing attacks or falling for scams, guidelines for choosing strong passwords, and rules for avoiding negative online behavior. Each section comprises one web-based game and a number of offline activities.

“GAP” (Tupsamudre et al., 2018) is another online web-based game for educating users about various features that have negative impact on password security. Specifically, during the game play the participants are asked to identify insecure password practices. In the game design, the authors have incorporated two principles from the learning theory; reflection and contextual-procedural. The participants who played GAP improved their awareness of the insecure password practices.

The only works so far that implemented a mobile app to teach cybersecurity are those given below in Arachchilage and Cole (2011), Visoottiviset, Phungphat, Puttawong, Chantaraumporn, and Haga (2018) and Giannakas et al. (2016). The first app introduced a standalone mobile app that consists of one mini-game for increasing the awareness of home computer users against phishing attacks.

“Lord of Secure” (Visoottiviset et al., 2018) is a virtual reality (VR) learning game for Android users. In this game, the learners intend to gain knowledge about network security. The game is composed of main topics of network security such as Firewall, DMZ (Demilitarized Zone), Honey Pot, Intrusion Prevention System (IPS) and Intrusion Detection System (IDS).

The work by Giannakas et al. (2016) is a germinal version of the CyberAware platform without the LCMS back-end, supporting a limited number of mini-games dedicated only to information security topics. So, the current work can be seen as a major

improvement of Giannakas et al. (2016) in terms of both platform architecture and educational content.

An observation stemming from the related work is that so far the majority of contributions concentrate on the technological aspect (i.e., the usability and look and feel of the mobile app) rather than on the learning theories the app should embrace. Only the works in Sheng et al. (2007), Kumaraguru et al. (2010) and (Tupsamudre et al., 2018) have been built with a learning theory in mind. However, these works do not pay any attention on learners' motivation. Even more, the majority of the works included in this section either do not offer any kind of evaluation for their proposal or the evaluation results are only concerned with usability. As detailed in Sections 4 and 6, CyberAware tries to tackle the aforementioned shortcomings by dealing with both the technical and educational aspects of the platform in a more holistic manner and from the outset.

Conclusively, it is to be noted that all the research works included in this section do not take any care for altering the learning content, and some of them have been implemented solely with desktop computing platforms in mind. Further, most of these

educational apps introduce only one learning topic, and none of them apply any motivational learning theory to the game flow. Finally, none of the apps is destined to primary education. The goal of this paper is to fill this literature gap by dealing with the particular shortcomings in a more holistic manner.

### 3. The CyberAware platform

A high-level view of CyberAware is depicted in Figure 1. As observed from the figure, the platform consists of a web-based custom LCMS and an app as the front-end. The app comprises a suite of seven serious learning mini-games, destined to cybersecurity and privacy education. Assuming a mobile device, the app connects to the LCMS so as to retrieve the appropriate learning and informational material. Additionally, as further discussed in Section 5, the front-end is designed to be platform independent, which means that the app can run virtually in any computing platform, including Android and desktop ones.

The platform is available either from the following URL address <http://icsdweb.aegean.gr/cybera>

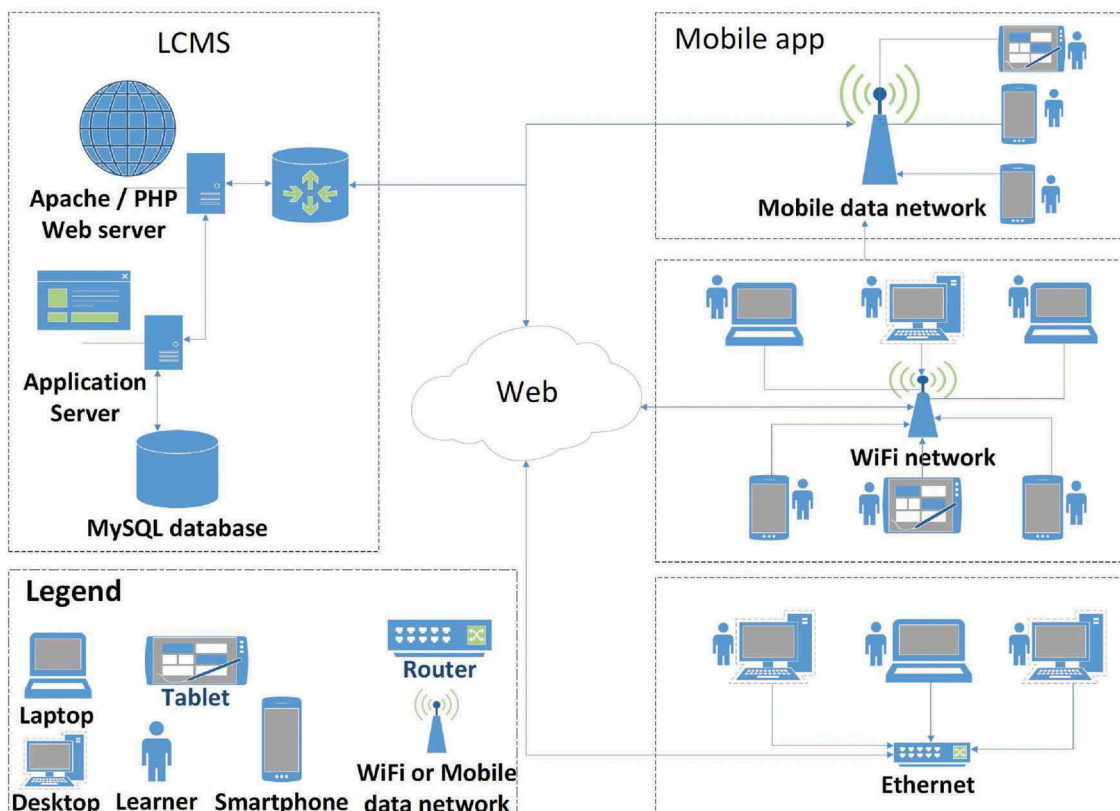


Figure 1. A high-level view of the CyberAware architecture.



ware/, or through the web page of Laboratory of Information & Communication Systems Security (Info-Sec-Lab) at the University of the Aegean (<http://www.icsd.aegean.gr/info-sec-lab>).

### 3.1. Gaming app

The CyberAware gaming app is a learning environment where the students actively engage for the purpose of accomplishing a number of quick challenges. The game supports two learning goals. First, to familiarize learners with fundamental cybersecurity technologies that are required to keep their Internet-connected devices protected against legacy threats, as well as to keep their passwords safe. Second, it aims at raising learners' awareness on privacy issues mostly related to their identity and the protection of their personal information published on the web. In several countries so far there is a significant shortage of efforts toward creating full-fledged computer security curricula for preteens, early teens, and generally for people who have only basic computer skills. Therefore, the educational content and security/privacy scenarios created for the purposes of the CyberAware app are based on the related literature (Chai, Bagchi-Sen, Morrell, Rao, & Upadhyaya, 2009; Kambourakis, 2013; Le Compte, Elizondo, & Watson, 2015) and on notable cybersecurity curricula or campaigns for children aged 6 to 12 years old. Specifically, we relied on the content and guidelines found in the "CERIAS K-5 Information Security Curriculum" (CERIAS, 2018), the Australian Government "eSafety" website classroom resources (eSafety, 2018), the UK government "GetSafeOnline" campaign for children aged 6 to 9 old (GetSafeOnline, 2018), the National Cyber

Security Alliance (NCSA), "StaySafeOnline" Grades 3–5 teaching resources (StaySafeOnline, 2018), and the National Integrated Cyber Education Research Center (NICERC) "Cyber Literacy 2" curriculum (CyberLiteracy, 2018).

The learner may choose to play the app either in a client/server or standalone mode. In the former mode, using their credentials (username/password), the player must first login to the app. Next, the app interacts with the LCMS and downloads the learning content along with the informational material. In standalone mode, the app does not interact with the LCMS, and the games run using the default settings.

As shown in Figure 2, in the game scenario, the player selects a learning topic either from the security or the privacy domain, and accordingly plays a series of short (quick session) mini-games. For spurring learners' intrinsic and extrinsic motivation, upon the successful completion of each mini-game a virtual shield unlocks, allowing the learner to play the next game in the row. If all the mini-games pertaining to the cybersecurity or data privacy topic are successfully completed, then a final virtual shield is removed and the corresponding "Arena" mini-game starts. As explained later in this subsection, the "Arena" game aims at interlinking the knowledge already acquired by the player with real-life situations (case studies).

Before starting a mini-game, the learner is able to read brief guidelines about the rules of playing it and information related to the current learning goal. We chose to include the least but most meaningful learning and informational material we could, in order to overcome long-term reading,

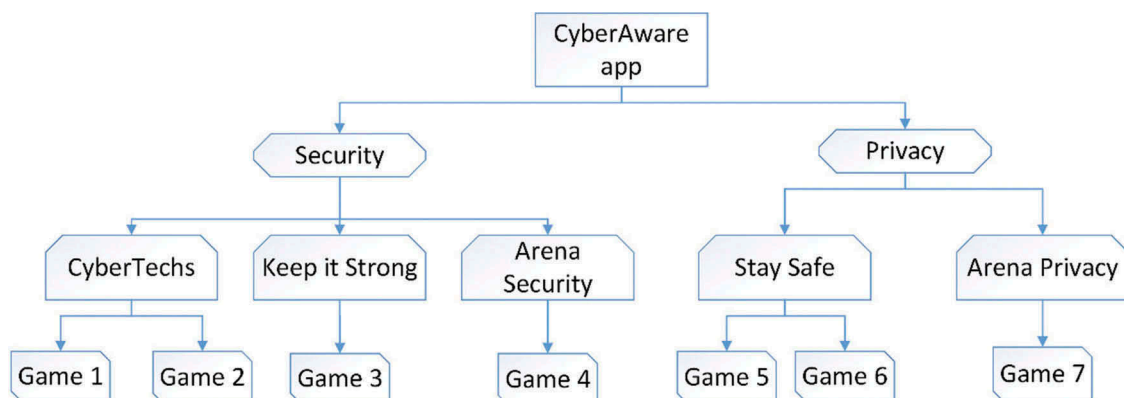


Figure 2. A map of the games contained in CyberAware.



Figure 3. Game 1: identify the cybersecurity technologies.

and thus to avoid boredom and inattention. The aforementioned minimalistic approach is not only driven by the inherent constraints of mobile devices (e.g., limited screen size), but it is also selected as a learning strategy for increasing learners' engagement, and consequently producing better learning outcomes.

The app is designed to aid autonomous and self-directed learning. Specifically, its main purpose is to steer the learners to discover new knowledge entirely by themselves following problem-based learning activities. That is, while playing a mini-game, the learners are actively supported by receiving advising tips and hints, when, say, the player's answer is incorrect, toward finding the right answer. Also, as detailed in sub-section 3.1, the activities which are delivered to the learners by the gaming app intend to promote their critical thinking. This is achieved by motivating learners to extend the knowledge gained from the various concepts being taught in different real-life situations by playing the "Arena" mini-games. In the following subsections, we detail on the architecture, the conceptual framework, and the ARCS model of motivation on which the front-end app is built.

### 3.1.1. Security section

As shown in Figure 2, this part of the app comprises three subcategories, namely "CyberTechs", "Keep it Strong", and "Security Arena". The first subcategory comprises two mini-games where the student learns about the use of basic cybersecurity technologies; Antivirus, Firewall, Security updates, and email spam filters. As depicted in Figure 3, mini-game 1 presents to the learner four relevant and an equal number of irrelevant technologies pertaining to basic cybersecurity technologies. The challenge for the pupil is first to recognize the correct ones and place them in the corresponding "NEEDED for protection" horizontal compartments.

After the successful completion of mini-game 1, a second one for the same subcategory starts. A snapshot of mini-game 2 of the same subcategory is shown in Figure 4. The goal here is for the player to identify and then associate each already identified cybersecurity technology from mini-game 1 with their correct use in keeping their Internet-connected device safe.

The next subcategory of the security section is named "Keep it Strong". The goal of this mini-game is to familiarize the student with basic rules

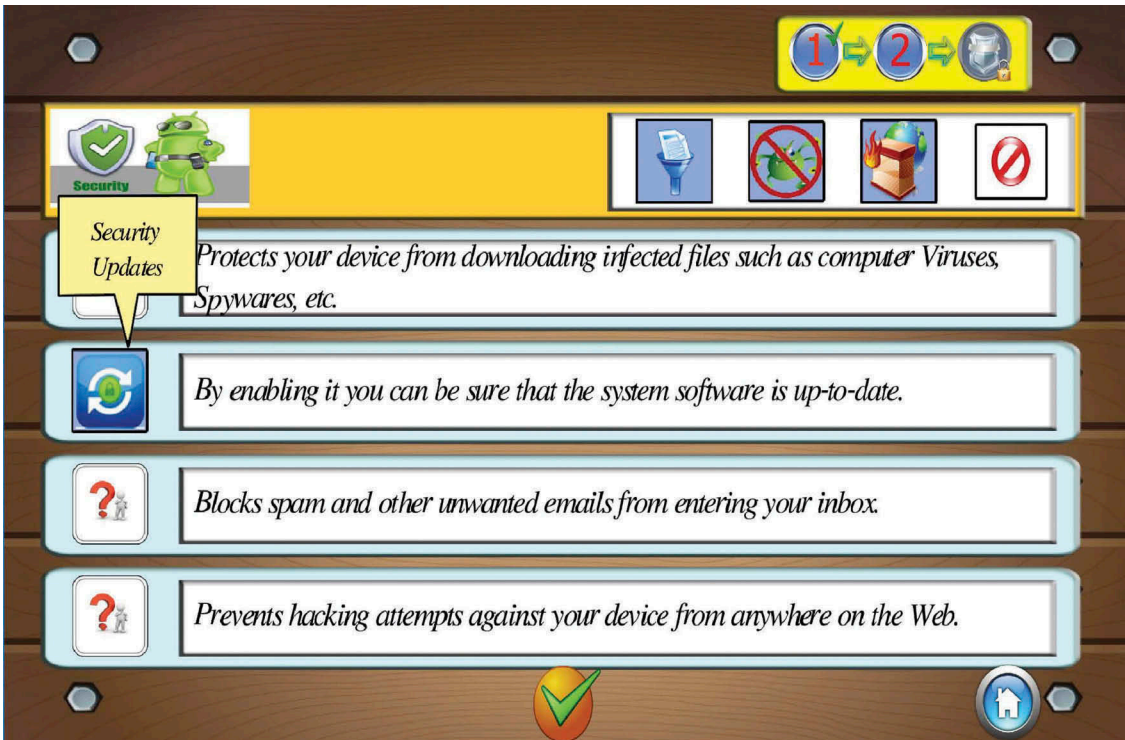


Figure 4. Game 2: associate each cybersecurity technology with its specific usage.

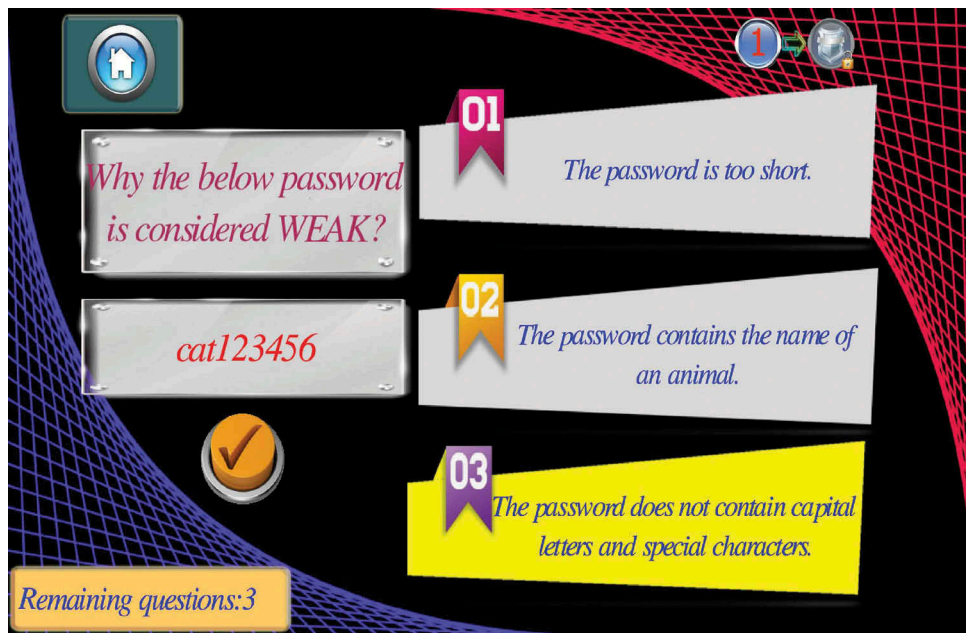
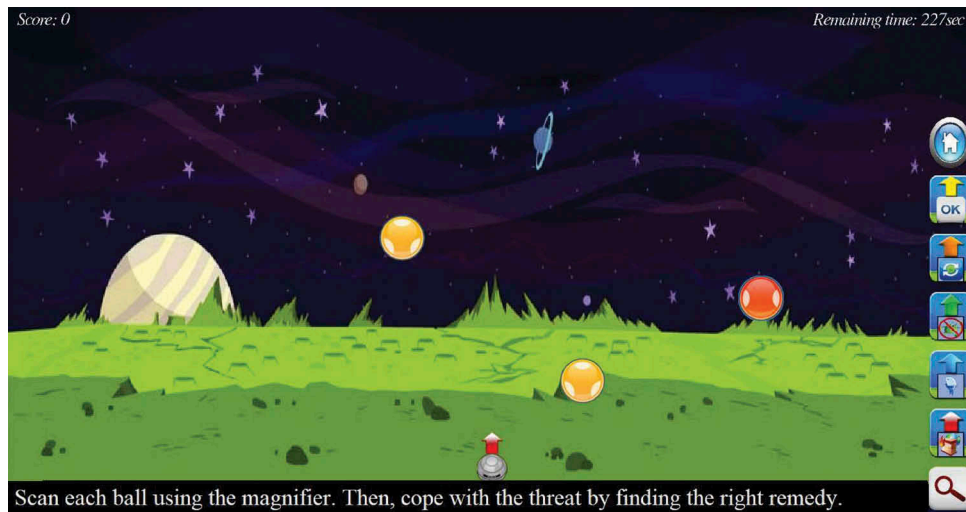


Figure 5. Game 3: identify if a password is considered strong or weak.

regarding password construction. A snapshot of this mini-game is depicted in Figure 5. Here, the student is asked to recognize if a series of given

passwords are considered weak or strong. If the answer is wrong, the player receives targeted advices, say, “Nowadays, a strong password should





**Figure 6.** Game 4: identify the cyber-threat and face it.

be at least 8 characters long, combining letters, numbers, and special symbols”.

After successfully finishing the first three mini-games, the “Security Arena” mini-game unlocks. Its goal is to engage students in a meaningful learning process by enabling authentic security scenarios. That is, challenging real-life scenarios typically foster student’s attention, which in turn amplifies knowledge retention. As such, the purpose of the mini-game 4 is twofold. First, the student needs to understand the threat that a specific online real-life web scenario presents, and then find out the appropriate security technologies for coping with it. The above mentioned learning flow is anticipated to steer students to associate the new knowledge they gained, after they have played the three first games, with real-life scenarios.

More precisely, as shown in [Figure 6](#), the learning scenario of “Security Arena” comprises colorful balls that fly horizontally from the right to the left side of the game screen. Each ball is randomly assigned to a specific real-life scenario, e.g., “You have just received an email that instructs you to review a product by clicking on a web-link”, “You chose to download a file, but before you proceed, you have to consent to a browser alert”, etc. A toolbox is placed at the right side of the game screen. By using the magnifier tool, the student is able to scan any ball in order to reveal the corresponding scenario. When doing so, the learning scenario corresponding to the selected ball appears at the bottom of the screen.

Then, the player needs to recall the knowledge that they have already gained so far from the previous mini-games in order to correctly identify the threat. Finally, they have to choose the correct data security technology that eliminates or mitigates the identified threat. This is accomplished by first selecting from the toolbox the colorful arrow that is associated with the correct cybersecurity technology (i.e., Antivirus, Firewall, Email spam filter, Security updates), and then shooting against the ball of interest. For each successful strike, the player collects a number of points. The learner has 4 min to shoot against as many colorful balls they can with the aim of collecting as many points as possible. Note that the game is pre-configured so as the player does not receive any negative points on an unsuccessful attempt. Nevertheless, if needed, negative scoring can be enabled by the educator via the LCMS.

### 3.1.2. Privacy section

As observed from [Figure 2](#), this module consists of the “Stay Safe” subcategory and the “Privacy Arena” mini-games. “Stay Safe” comprises two mini-games. Their goal is to enable students’ critical thinking on identifying the information that is considered personal and therefore sensitive. Precisely, mini-game 5 presents to the learner pieces of private or public information in order for the player to decide whether each of them is considered sensitive or not. A snapshot of this mini-game is shown in [Figure 7](#).



**Figure 7.** Game 5: identify if information is considered public or private.

After the successful completion of mini-game 5, another one starts. This time, as illustrated in [Figure 8](#), mini-game 6 challenges the learner to identify if a given short message can be published as is on the web without disclosing any personal information. The “Privacy Arena” mini-game unlocks only after the player successfully finishes the previous two mini-games. The main objective of this game is similar to the “Security Arena” described in [Subsection 3.1.1](#). That is, first, the student must identify if the information given in response to a question is considered public or private, and second to decide if it can be published on the web. Note that these questions pertain to typical real-life situations. As already pointed out, this challenge helps students to associate the new knowledge they gained after their interaction with mini-games 5 and 6 with real-life scenarios.

As shown in [Figure 9](#), the learning scenario of the “Privacy Arena” shows a spaceship that travels in the outer space. There, a number of planets fly horizontally from the right to the left side of the game screen. Each planet is randomly associated with a specific scenario, e.g., “Hi guys! I will wait for you at my home located at 4325 W. Palm Beach Rd.”, “The food I ordered last night was fresh and very tasty”, etc. On the lower middle of the screen there exists a scanning tool. The student needs to use it for

revealing the planet’s corresponding scenario, which, then, is displayed in a panel located at the middle of the game screen. Based on the acquired knowledge, the pupil must decide if the corresponding information can be safely published as is on the web. This is achieved by selecting the correct button located in the spaceship console. If it is correct, the player collects a number of points. The learners have a handful of minutes to successfully identify as many planet scenarios as they can in order to increase their score. Similar to the “Security Arena”, the default configuration is for the player to not receive negative points. This setting however can be changed via the LCMS by the educator at any time.

### 3.2. LCMS

Typically, an LCMS is used for centrally administrating the learning content and the associated activities. That is, via the LCMS, the learning content is delivered and can be accessed anytime, anywhere. This facilitates the upgrading or amendment of both the learning and informational content of the courses, and simplifies the learning process by administering learners’ enrollment and managing the virtual classrooms. For the time being, and for achieving maximum compatibility with the app, we implemented a custom LCMS, which from top to bottom



Figure 8. Game 6: identify if the information can be published or not on the web.

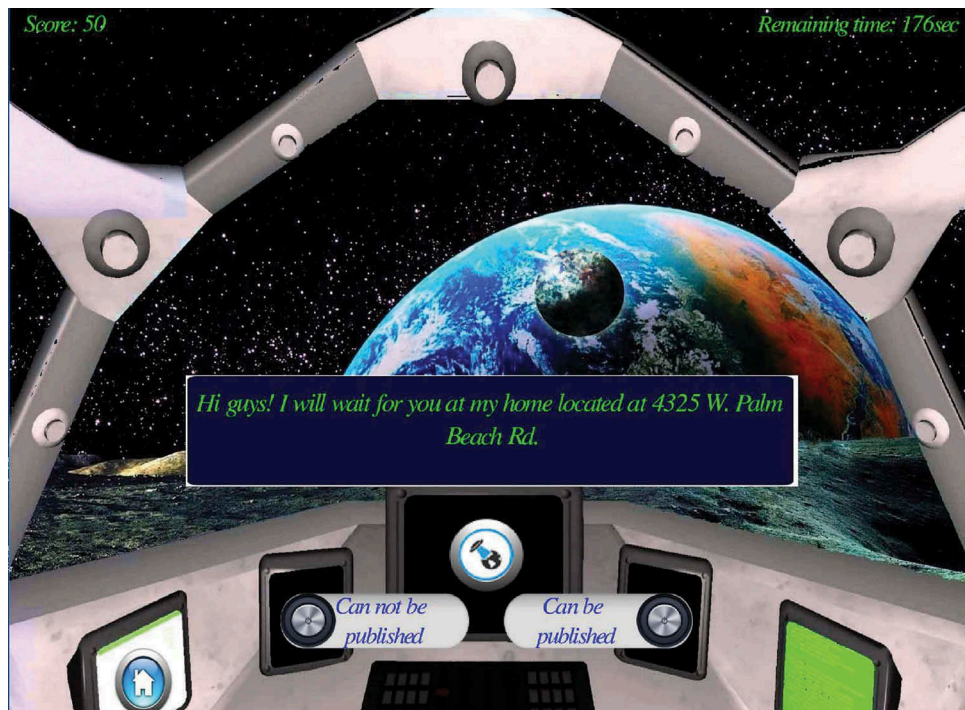


Figure 9. Game 7: identify if a real-life scenario contains sensitive personal information.

comprises five layers, namely Administrator, Educator, Class, Learner, and Learning/Informational material.

An educator can access and register with the LCMS by inserting their personal information. Upon successful registration, they are able to manage their own

virtual classrooms, and enroll pupils into it. Recall that the main objective of the LCMS is to feed the associated app with the appropriate content consisting of learning and informational material. The former comprises the information that is relevant to each mini-game, that is, the questions, the possible



answers, the correct answer, and so on. The informational material on the other hand contains the guidelines, hints, and tips which are displayed to the players. Also, the LCMS stores any information related to the configuration of the game app and to the user's interface, e.g., the remaining time before a mini-game finishes, the number of scenarios or questions, the text shown in the various Graphical User Interfaces (GUIs), and so on.

All the aforementioned functionalities are enabled only after the learner successfully logs in the LCMS by using their personal credentials given by the educator. After that, the app retrieves the course material and stores it locally in JavaScript Object Notation (JSON) formatted files, so as to be available for further analysis to anyone at any time. At the same time, learner's engagement with the app is constantly tracked and stored locally in JSON formatted files. These files contain information regarding the time each learner spent playing a mini-game, their scores per mini-game, whether they answered correctly a given question, and so on. The files are available to the educator for retrieving useful information regarding the learning curve of each learner. It is to be noted that the current version of the LCMS does not support an automatic analysis of these logs. This means that the educator must download the JSON log files and manually analyze them locally.

Finally, if the app runs for the first time and the learner does not log in, then it starts using a standard profile corresponding to the default learning material and configuration. Otherwise, the app is launched using the last successfully retrieved material.

#### 4. Model of motivation and conceptual framework

In educational settings, motivation, whether it is intrinsic or extrinsic, is considered a fundamental element for improving the learning process and associated outcomes (Hodges, 2004). However, the proper consideration of motivational characteristics in any serious DGBL app requires among others careful course design. For achieving such a goal, the DGBL environment needs to at least fulfill the following conditions: be content-rich, be learning effective and efficient, and embrace attractive game characteristics, including

interesting plot, and well-designed and easy-to-navigate GUI (Anaraki, 2004; Yee, 2006). In this respect, this section implicitly provides an answer on what are the benefits of incorporating a learning theory into a DGBL app.

Given the previous requirements, CyberAware has been designed with the following principles in mind: (a) the learning goals should be clear and easy to comprehend, (b) the challenges for the player should be short, attractive, and easy to understand, (c) the learning content should be possible to alter or extend at any time, focused to specific learning topics, concise, and easy to comprehend, and d) the app should be able to navigate and run on a variety of modern computing platforms, including mobile ones. To reach the aforementioned four goals, we concluded that the app should be guided by an instructional strategy for ensuring the quality of the learning experience and guaranteeing the learning outcomes. Such a strategy should be properly driven by an Instructional Design Model (IDM) (Gibbons, Boling, & Smith, 2014) that details on how the learning experience can be synthesized so that the acquired knowledge and skills become more attractive to the learners. Broadly speaking, an IDM contains general principles that guide the creation of engaging pedagogical scenarios that contain realistic and unambiguous learning goals.

In the literature there exist a variety of IDMs, including Dick and Carey (Dick, Carey, & Carey, 2014), ADDIE (Branch, 2009; Peterson, 2003), ASSURE (Heinich, Molenda, Russell, & Smaldino, 2005), ARCS, and others. In our case, the ARCS model of motivation is chosen for the design of the learning strategy of the CyberAware app. The next subsections detail on the ARCS model and how this is considered in each stage of the mobile app. Also, Figure 10 illustrates the conceptual framework of our platform outlining the logical interconnections among four entities; the game app, the learner's motivation, the IDM, and the LCMS.

##### 4.1. Conceptual framework

A learning process owes to find ways to sustain learners' motivation. If properly done, this situation is anticipated to increase learners engagement and satisfaction which in turn stimulate them to



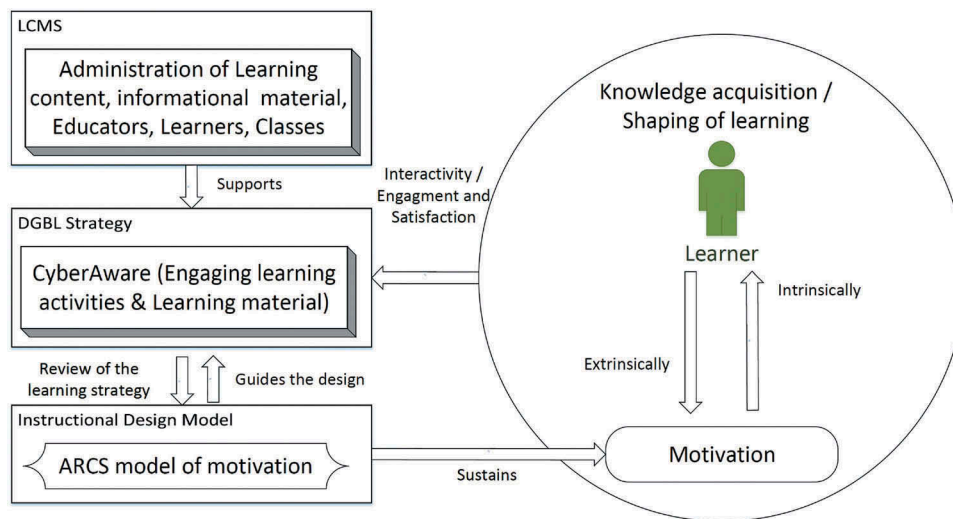


Figure 10. Abstract view of CyberAware conceptual framework.

keep learning in track and meet the expected learning goals (Burguillo, 2010; Keller, 1987b). As already pointed out, the design of CyberAware app is based on the ARCS model of motivation. As further detailed in this section, ARCS comprises four distinct components, each describing specific strategies, guidelines, and learning processes. All these components enable the design of a suitable instructional learning experience that sustains motivation and actively engages the learner during the learning process. Also, the ease of altering the educational material and the associated parameters is also tightly connected to the app's lifespan. Therefore, the easier the amendments, the greater the anticipated lifetime of the app.

Figure 10 illustrates CyberAware's conceptual framework that details on how the learning app, the learner's motivation, the IDM, as well as the LCMS are interconnected. As observed from the figure, the learner is placed in the center of knowledge acquisition, while they engage and interact with the app and the learning material. The conceptual framework is neither unidirectional nor static. Rather, it should be seen as a circular and continuously adjusting process between learner's motivation and the DGBL app. If necessary, the instructor is able to alter the learning content and informational material delivered to the app so as to embed new challenges toward improving the learning experience and outcomes.

#### 4.2. ARCS and app interconnection

The main purpose of ARCS (Keller, 1987a) is to spur motivation by systematically guiding the design of engaging learning activities that produce specific learning outcomes according to the learners' behavior. In general, ARCS comprises different motivational theories, including skills and knowledge, cognitive accounting of individual abilities, behavioral contingency design and management, and expectancy-value theory, that all meet in the context of social learning. In our case, this can be achieved while learners participate in learning activities which are intrinsically interesting to them.

The rationale behind the selection of the ARCS model was based on the existence of four distinct components, namely Attention, Relevance, Confidence, and Satisfaction, for enhancing and retaining learners' motivation during the learning process. These components are further divided into several other subcomponents that outline specific learning strategies for instructing self-directed learning and spurring motivation. Figure 11 illustrates the interconnection of the structural elements of CyberAware with each ARCS component. For instance, starting from the inner part of the figure, we can observe that the "Attention" component is connected to the "Maintain attention" subcomponent, which in turn is related to "Time countdown" and "Score" features of the app. The following subsections discuss the abovementioned components and detail

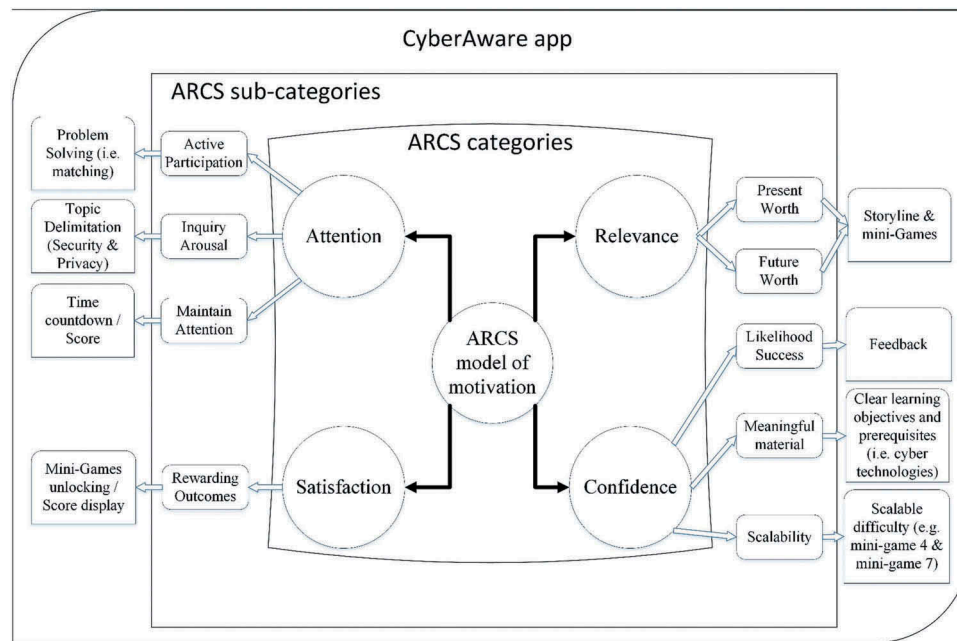


Figure 11. CyberAware and ARCS interplay.

on the way they are incorporated during the design phase of the app.

#### 4.2.1. Attention

As already pointed out, the first goal of the ARCS model of motivation is to maintain learners' attention. This quality is proved to be vital, since the challenge is to retain learners' attention at a high level for keeping them engaged during the learning process. As observed from Figure 11, our app fulfills the component of attention by enabling the following ARCS sub-components: "Active Participation", "Inquiry Arousal", and "Maintain Attention".

The active participation of the students during the learning process is an important incentive element that intensively retains their attention. In our case, this is achieved when they mandatorily play a number of mini-games in a row. That is, in the security section, the student plays four mini-games in a row, as depicted in Figures 3–6. Similarly, in the privacy section, they play three mini-games in a row, as illustrated in Figures 7–9.

Additionally, as shown in Figures 5 and 9, the app engages various features for triggering and retaining learner's attention, such as score and remaining time count-down. Finally, as shown in Figure 12, learner's attention is also retained via

the use of inquiry arousal screens which are displayed before starting a topic or a mini-game. These screens inform the player about the current learning goal.

#### 4.2.2. Relevance

Another important component of the ARCS model is that of relevance. As shown in Figure 11, this component consists of the "Present Worth" and "Future Worth" subcomponents. Primarily, relevance has to do with the retention of learner's interest. This can be achieved via a number of ways, including a clear explanation of (a) the merit of the course and its goals, and (b) its relevance to real-life problems and situations. In our case, both the aforementioned requirements are fulfilled by enabling specially crafted storyline inquiries to the learners. Specifically, for each mini-game, a main inquiry is displayed on the game screen that explains to the player the merit (goals) of the current challenge.

As observed from Figure 13, before the Stay-Safe subcategory starts, relevant inquiries are displayed on the screen that inform the pupil for the learning goals associated with the current topic. Similarly, after the selection of each learning module (i.e., security, privacy), similar inquiries are displayed for that specific topic.

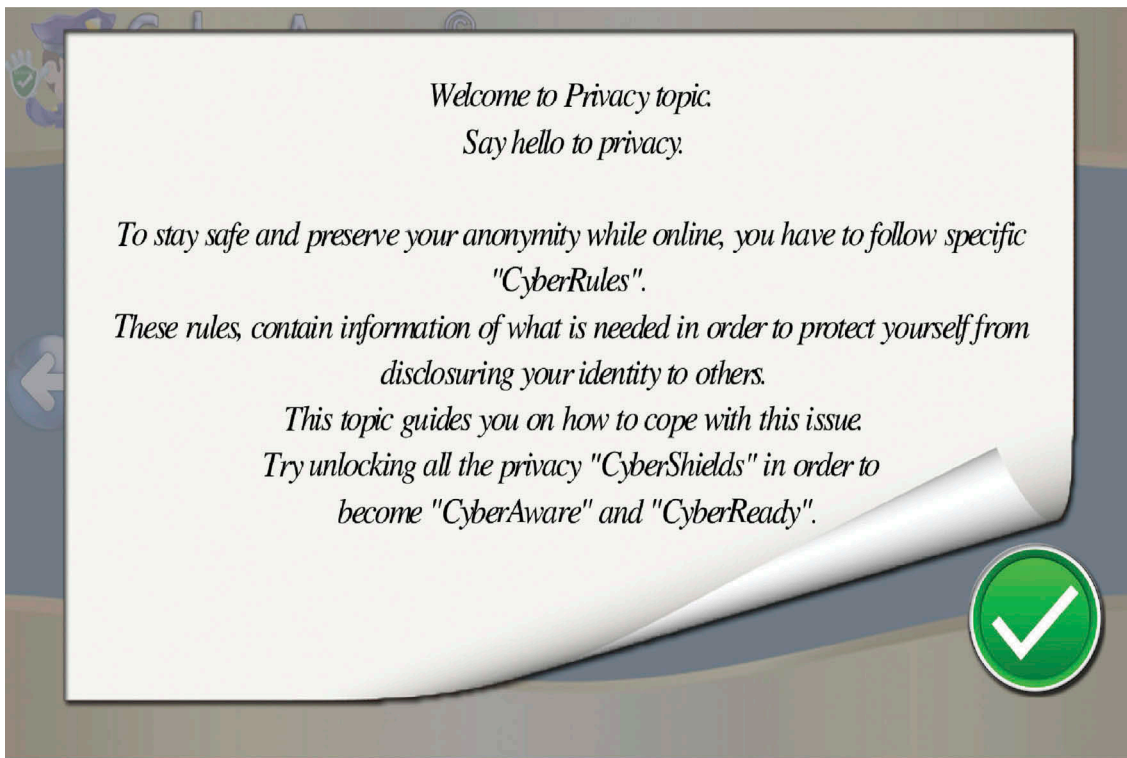


Figure 12. The main information screen of the privacy topic.



Figure 13. The initial information screen for games 5 and 6.

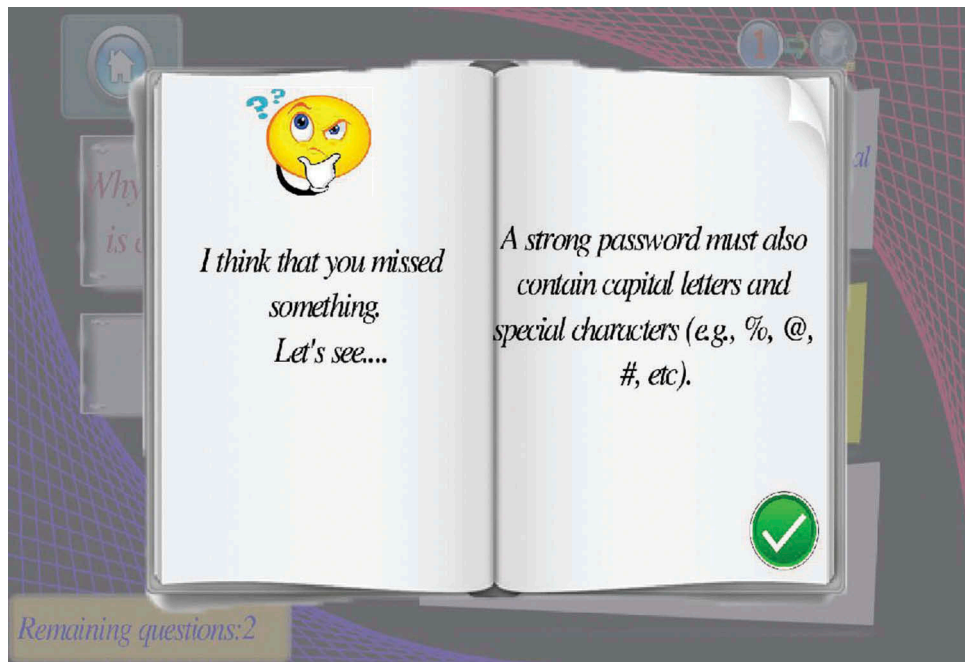


Figure 14. Advising tips and hints.

#### 4.2.3. Confidence

Confidence is another key component of the ARCS model. As shown in Figure 11, this component is divided into “Likelihood success” and “Meaningful material” subcomponents. Based on the model’s layout, each learning challenge should rely on the learner’s capabilities. It is also important for the learners to feel that they can successfully accomplish a given task in order not to drop out of the learning process. For the CyberAware app, this goal is achieved via hints and tips provided during each challenge or after the player chooses a wrong answer. This situation is depicted in Figure 14.

Confidence between the learner and the app is also accomplished by designing the learning material in such a way that its objectives are meaningful to the player. This result is amplified when the learning material incorporates clear and realistic expectations, and if possible, scalable levels of difficulty. Under this prism, the user app is designed to elaborate straightforward learning objectives for both the security and privacy topics.

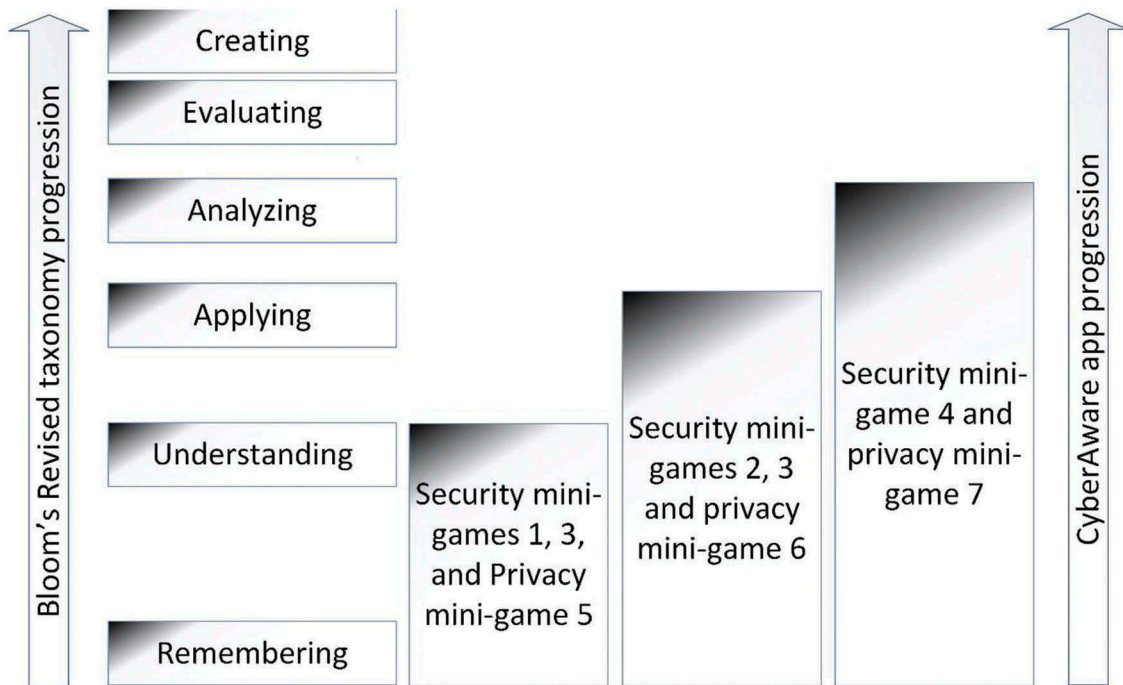
Specifically, the objectives associated with the security topic are as follows:

- (1) The player must be able to correctly identify the right cybersecurity technology for securing their device in the cyberspace.
- (2) The player must be able to identify the merit of each cybersecurity technology and the level of protection it offers.
- (3) The player needs to tell between a weak and strong password.
- (4) The player must be able to cope with basic real-life situations regarding cyber- threats. That is, they must be able to identify the threat and select the correct remedy as the case may be.

The learning objectives associated with the privacy topic can be summarized as follows:

- (1) The learner must be able to identify if a piece of information contains personal data.
- (2) The learner must be able to tell if a piece of information can be safely posted on the web without disclosing their identity.
- (3) Given a real-life Internet usage scenario, the learner must be capable of identifying if it is privacy-invading or not.





**Figure 15.** CyberAware’s games series progression and its correspondence to Bloom’s revised taxonomy.

The aforementioned educational objectives adhere to the first four levels of the Bloom’s revised taxonomy (Anderson et al., 2001). As observed from [Figure 15](#), Bloom taxonomy is interlinked from the “Remembering” up to the “Analyzing” level. Specifically, for the learner to better understand the objectives of each mini-game, they have to recall previously acquired information after participating to a traditional teaching process in their curriculum. After that, the learner may proceed to play the Security Arena and the Privacy Arena mini-games. There, the player needs to recall the newly acquired knowledge for applying it to new situations. It is to be noted that this work follows the basic instructional design principle of clearly specifying the learning objectives of the learning environment under consideration. Therefore, as explained above, the revised Bloom taxonomy, widely used in the literature, was a useful framework for specifying these objectives. Nevertheless, the reader must remember that this taxonomy has received a lot of criticism regarding its validity and usefulness for instructional design (Sugrue, 2002; Case, 2013).

Confidence is also cultivated by designing scalable learning activities in terms of difficulty. So, in the CyberAware app, the difficulty of the learning scenarios of each mini-game augments as the

player advances to the next mini-game. More precisely, the “Arena” mini-games are considered more difficult than the previous ones in the same learning topic, since the learner must first understand the given scenario and then recall the knowledge they acquired in order to successfully tackle it.

#### 4.2.4. Satisfaction

The fourth component of the ARCS model is also considered an important criterion for preserving learners’ motivation. This is because the student is most likely to play the game again if they feel contented about the knowledge they acquired. As observed from [Figure 11](#), the app fulfills the aforementioned criterion by implementing specific outcomes for rewarding extrinsically the learners. This component is achieved by enabling new learning challenges, such as those presented in the Security Arena and Privacy Arena mini-games, unlocking virtual shields, and constantly displaying the player’s score on the screen during the two “Arena” mini-games.

## 5. Implementation aspects

The development and implementation phases of every serious learning game need to consider

several aspects, including ways to extend its life-span. Nowadays, due to the plethora of computing devices of all kinds, this is becoming more evident since the porting of the app to run on different computing platforms is considered a critical factor for its success. In fact, app porting is something that developers often neglect since it requires a significant and continuous effort in coding and testing. Consequently, most of the time, the aforementioned implementation practice is proved to be ineffective. Platform independence is also closely related to BYOD scenarios where learners are not using dedicated devices to play the game, but they are at liberty to use their own. From a learner's viewpoint, this is supposed to increase their confidence and satisfaction because the player feels more familiar and comfortable when experiencing the corresponding app via their own personal device. Additionally, considering BYOD from an educational organization viewpoint, it can drastically reduce the development time and the maintenance and upgrading costs of the different versions of the learning app.

Bearing the above into mind, the CyberAware app is developed to run on different platforms, ranging from mobile to desktop ones. That is, for the development of the app, we used standard software tools, including Android studio, Android Development Kit and the open-source libGDX game engine (Zechner, 2012). This game engine was not only selected because it is open source, but also because it enables cross-platform development. More precisely, libGDX framework supports four layers, namely Desktop, Android, iOS, and HTML5. This modularisation enables the CyberAware app to run on both desktop and Android platforms. It also makes possible the extension of the app to run on iOS and support HTML5 contents, without additional coding efforts.

On the other hand, for the design of the LCMS, we relied on the Model View Controller (MVC) software architectural pattern. This model separates the way the information is stored on a server and how it is fetched and presented to the clients. For the LCMS and app interoperability, we relied on the Representational State Transfer (REST), i.e., the RESTful web services architecture. Currently, the LCMS is deployed on an Apache server along with a MySQL database.

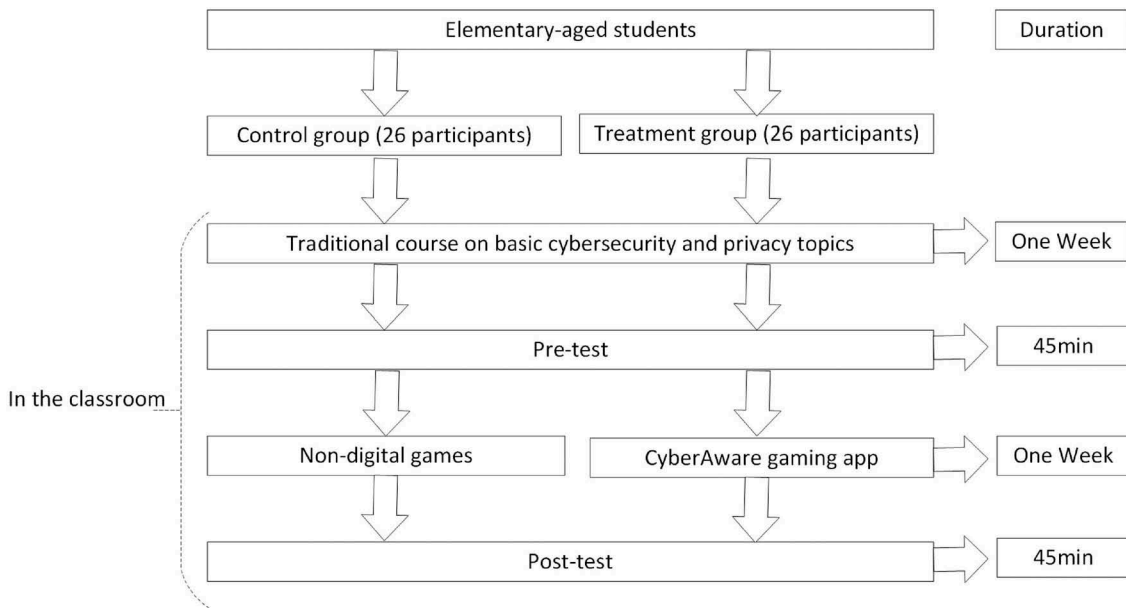
## 6. Evaluation

The purpose of the current section is to assess the overall quality of game app from a learner's viewpoint. This has been done in three axes. First, we evaluated the app's learning outcomes (effectiveness), by means of both pre- and post-tests taken before and after the pupils have experienced the app. Secondly, we assessed the functional characteristics of the app (usability), we well as students' attitude (satisfaction and expectations). Fifty-two elementary-aged students participated in the evaluation process, 25 boys and 27 girls, ranged in age from 9 to 12 years. All the pupils had a written consent from their parents or guardians to participate in the evaluation phase of the app.

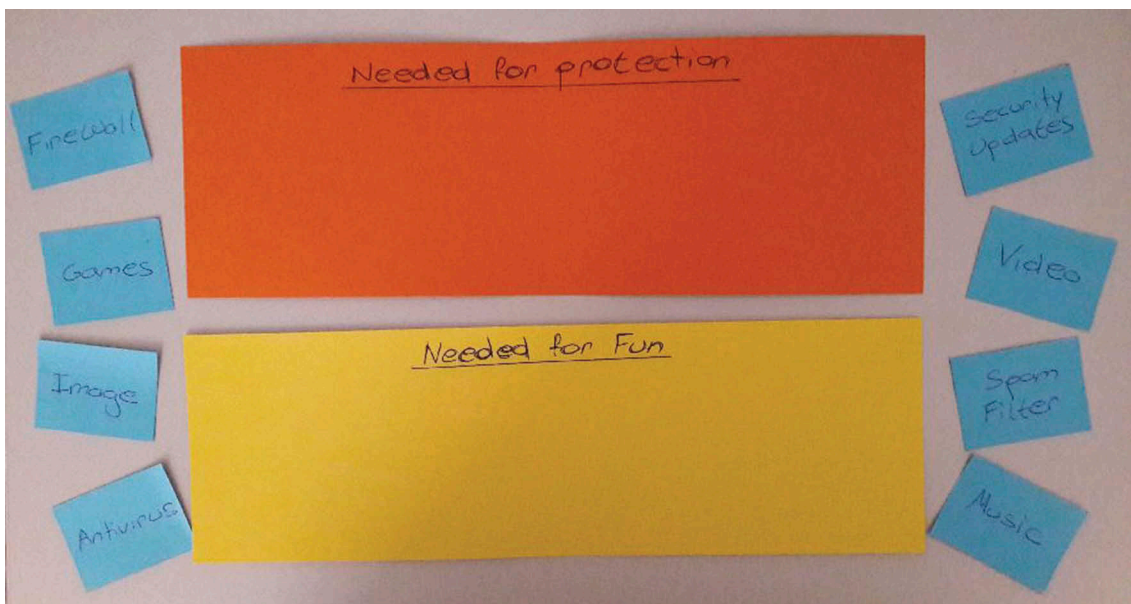
### 6.1. Learning/knowledge acquisition effectiveness

#### 6.1.1. Method

Knowledge delivery from external resources, such as e-Learning systems in general or m-Learning in particular, is of great importance in learning environments. In this context, knowledge acquisition effectiveness was examined via pre- and post-tests that learners answered during the experimental phase. Specifically, as shown in Figure 16, the pupils were divided into two groups, the control (26 pupils) and the treatment (26 pupils). Both groups answered the pre-test after attending a traditional course on basic cybersecurity and privacy topics according to their curricula. After that, the control group played some non-digital activities similar to the gaming app and they answered the post-test. For instance, as shown in Figure 17, the learners had to put the blue labels in the correct place (i.e., needed for protection, or needed for fun). On the other hand, the learners of the treatment group interacted with the app before answering the same post-test. The content of the tests for both the security and privacy sections is given in Tables 1 and 2 in the Appendix. The two groups of pupils were assembled randomly without any criteria, and the tests were completed in the classroom under the supervision of a teacher. The teaching duration of the subject using classical instruction was two teaching hours delivered in two different days of the same week (~90 min). Further, each of the non-digital and the gaming app activities lasted two teaching hours in two different days.



**Figure 16.** Experimental procedure for the knowledge acquisition effectiveness.



**Figure 17.** A non-digital learning activity used for the evaluation.

### 6.1.2. Results

We conducted a comparison of the increase of performance for the two conditions, namely, control and treatment. A total of 10 questions were answered in the pre- and post-tests. The total score ranges from 0 to 11. The difference between the performance of each student between pre- and post-test was used as the dependent variable.

**Table 1** summarizes the results of the performance difference for the two groups.

The Shapiro–Wilks test showed that the results for the control group did not follow the normal distribution ( $W = 0.88, p < .05$ ). A non-parametric analysis based on the Kruskal–Wallis test ( $H(2) = 4.7344, p = .02957$ ) showed statistically significant difference among the two groups ( $\alpha = 0.05$ ).

**Table 1.** Summary of knowledge acquisition results.

Groups	N	Mean performance difference	SD	Mean performance difference %
Control	26	0.77	1.66	6.99%
Treatment	26	2.19	2.06	19.93%

### 6.1.3. Discussion

According to the findings of the above experiment, the experimental (treatment) group outperformed the control group in their increase of knowledge after interacting with the CyberAware game. The activities of both groups, experimental and control, involved the same learning content, that is, the same information and self-assessment material, as illustrated in Figure 17. The factor that differentiated the two activities is the gaming factor that was involved in the CyberAware app. This factor is likely to have promoted cognitive engagement and motivation to students, thus resulting to the improvement of their learning of the topic. Their engagement to the activities of the game is supported by the findings of the following Subsection 6.2.

The current subsection offers a more detailed descriptive analysis based on the data provided by the participants. Specifically, in the test given in Table 1, and for question Q1 the learners were asked to select from a provided list of answers about which technologies are needed for protecting an Internet-connected device. As observed, the list contains several relevant and irrelevant cybersecurity technologies aiming to better detect the quality of knowledge acquired by the student. Further, for questions Q2 to Q5, the learners were asked to identify the merit of each cybersecurity technology contained in the corresponding list of answers. Regarding question Q6,

learners were invited to identify real-life web activities for which at least one cybersecurity technology is required. This kind of assessment is deemed necessary since the interconnection of knowledge obtained with real-world challenges shuttles learning from the classroom settings to the actual realm of practice (J. R. Anderson, Reder, & Simon, 1996; Lebow & Wager, 1994; Lee, Huang, Wu, Huang, & Chen, 2012). Finally, Q7 and Q8 investigate the learner's view about the creation of a strong password. For the privacy section, in question Q1 the learners were requested to identify if a piece information is private or not. In Q2, the learners were asked to identify if a certain statement can be safely posted in an online social network.

We analyzed the results of our findings, before and after the learners interacted with the security topic of the game. The results of our analysis are summarized in Table 2.

Before the learners interacted with the privacy topic, only 30.8% of them were able to recognize all the sensitive information provided, including those that can be safely published on online social networking sites. This was improved and reached at 80.8% after playing the app. Also, while the 46.2% of the learners recognized the 2 out of 3 sensitive information before playing the CyberAware app, this factor was improved by almost 34.6% after playing it.

### 6.2. Usability, and user satisfaction and expectations

To collect students' opinions about the usage of the app, we created a questionnaire that consists of nine questions. Two of them are Likert-type, while the others were open type, and dropdown or

**Table 2.** Summary of the results of knowledge acquisition for the security section.

Description	Before playing the game	After playing the game
Learners recognized all 4 technologies that are required to keep their Internet-connected devices protected	34.6%	53.8%
Learners recognized more than 3 learning scenarios out of 6 that an Internet-connected device needs to be protected	34.6%	65.4%
Learners recognized all the learning scenarios that an Internet-connected device needs to be protected	7.7%	38.5%
Learners recognized all the desirable qualities of a strong password	26.9%	42.3%
Learners identified the wrong formatted password	19.2%	65.4%



**Table 3.** Descriptive statistics per each answer contained in Table 3.

Q/A (n = 26)	Mean	SD
Q6(a) – It was easy to use.	4.48	.50
Q6(b) – The instructions on how to play were easy to understand.	4.35	.49
Q6(c) – The game’s information (game play and learning goals) were comprehensible.	4.29	.78
Q6(d) – The messages displayed on the screen after a given answer were comprehensible.	4.32	.79
Q6(e) – When a given answer was wrong, the displayed message helped me to find the correct answer.	4.48	.54
Q6(f) – Every mini-game was easy to navigate.	4.39	.57
Q6(g) – After an action, it was easy to understand what to do next.	4.41	.60
Q8(a) – It was very funny to learn while playing the game.	4.39	.49
Q8(b) – I liked that the game has a short amount of reading material and more action.	4.58	.45
Q8(c) – I would like to play the game again in my classroom.	4.35	.60
Q8(d) – I would like to play the game again outside the classroom in my free time.	4.50	.58
Q8(e) – I became familiar with what is required for a personal device to be protected against basic online attacks from the Web.	4.44	.57
Q8(f) – I realized the importance of privacy in the Internet age.	4.40	.57
Q8(g) – I will recommend it to my friends.	4.81	.40

checkbox value lists. Each Likert-type question had five alternatives to choose from: strongly disagree, disagree, neither agree nor disagree, agree, and strongly agree. The participants had to answer the questions shortly after playing the CyberAware Android app.

As shown in Table 3, the questionnaire is split into three parts. The first part contains general and demographical questions (Q1 to Q5). The second part aims at investigating the usability issues of the app. It contains Likert-type question Q6, and non-mandatory open type question Q7, in which the users are encouraged to flag any problem they faced during the game play, including those related to the mobile device (e.g., small screen, difficulties interacting with the touch screen, etc). The last part of the questionnaire aims at investigating the overall degree of user satisfaction and expectations. It contains the Likert-type question Q8 and the open type question Q9. In Q8 the players need to express their satisfaction during the game play, while in Q9, they can optionally mark down their expectations about the game. The reader may discern that several questions existing in our questionnaire are more or less similar to System Usability Scale (SUS) tool for measuring the usability. Actually, we did not employ this out-of-the-box industry standard because we preferred to amend the questions for better adjusting it to the young age of the participants.

The internal reliability of the questionnaire was assessed using the Cronbach’s alpha parameter and it was found to be sound ( $\alpha = 0.8$ ). Table 3 presents the mean and the standard deviation (SD) of the given answers for each question contained in Table 3.

The highlights of the findings are summarized below.

- 69.2% of the learners had interacted with at least one mobile digital game some- time in the past.
- 88.5% of them had played a digital game using a desktop computer.
- 76.9% of the pupils have not interacted with educational digital games in the past.
- 92.3% of them love to play digital games.
- 65.4% agreed that the app was easy to navigate, while another 34.6% had a neutral opinion on this.
- 100% of the learners agreed that was easy to familiarize themselves with the app.
- 69.3% agreed that information regarding the game play and the learning goals were comprehensible, while another 30.7% had a neutral opinion on this.
- 80.8% agreed that every message displayed on the screen was comprehensible, while another 19.2% had a neutral opinion on this.

- All of the learners agreed that after a wrong answer, the displayed message was comprehensible.
- Everyone agreed that they had understood clearly what to do in each mini-game. All of them agreed that after an action, it was easy to understand what to do next.
- All of them agreed that it was really funny to learn while playing. Also, they liked the plot of the game, which is focused on action rather on informational material.
- 80.8% agreed that they would like to play again the app in the classroom, while another 19.2% had a neutral opinion on this.
- Everyone agreed that they would like to play the game again outside the classroom in their free time and they would recommend the app to their friends.
- All the players agreed that they have learnt a lot about how to protect their devices against basic online attacks and how to safeguard their personal information.

To summarize, it is encouraging to see that all the participants would like to play the game again outside the classroom in their free time. This was one of our goals since the app was designed mainly for anytime and anywhere use. From the results, it is also obvious that the learning material and the instructions provided by the app were found to be comprehensible to the majority of the learners. Also, all the participants expressed a common opinion that the learning objectives across the various learning activities were clear and easy to navigate. Unfortunately, Q7, Q9 of Table 3 were left unanswered by all the pupils. This may indicate that the learners did not encounter any major problem and/or they were satisfied with the overall functionality of the app.

### 6.3. System resources

For evaluating the mobile version of the app, we used the Android Studio Profiler for conducting a benchmarking analysis of the CPU, memory, and network traffic. The results indicate that the current version of the app is lightweight in terms of system resources usage. Specifically, it consumes an average of 6.5% of the CPU, while memory

utilization fluctuates between 30 and 93 MB of RAM depending on which mini-game is currently active. Also, network utilization during app's login and learning content download fluctuates between 2.83 and 81.54 Mbit/s.

## 7. Conclusion

In this paper, we presented a novel DGBL platform for elementary students with the purpose of addressing certain topics in cybersecurity and privacy education. The platform comprises a web-based LCMS and a DGBL app, and intends to complement traditional teaching rather than replace it. This is fulfilled by enabling short session serious mini-games for the purpose of applying burst-session learning experience in terms of short time period tasks. This type of mini-games is a strategic design choice for maximizing learner attention and knowledge retention, and subsequently, minimize their boredom and distraction. Contrary to similar works in the literature, apart from dealing with the technical issues of the app and the LCMS, we pay special attention to the learning/pedagogical aspects, and evaluate the app under different prisms.

Regarding the technical and architectural aspects, we concentrate on the administration of the learning resources and device platform independence. For the first goal, we developed a LCMS for managing educators, learners, and virtual classes, as well as customizing and delivering the appropriate learning content and information material to the app. For the second, we implemented the app to run in a platform-independent manner. Both of the aforementioned characteristics are major parameters that not only extend the lifespan of the DGBL app but also make it ideal for BYOD scenarios. Interacting with the mini-games was found to positively influence learning of cybersecurity and privacy in primary school children, corroborating the pedagogical value of our approach. Specifically, for the educational/learning needs, we focused on ways to keep learners on track and maximize the learning outcomes. This has been primarily achieved with the incorporation of the ARCS model of motivation. The assessment of the app via a pre- and post-test, provided non-conclusive indications that, for the particular learning domain, DGBL has greater

chances to succeed, and young learners are more likely to learn and retain the acquired knowledge. A preliminary evaluation of the app, including learning effectiveness, usability, and user's satisfaction was conducted with 52 elementary-aged students. The results show that the interaction with the app significantly increases the mean performance of the participants (19.93%) compared to the control group (6.99%) (Kruskal–Wallis test,  $p < .05$ ). Also, all the participants would like to play the game again outside the classroom in their free time, and they also expressed that the learning objectives were clear and easy to navigate. However, additional evaluation efforts with diverse pupil samples are needed to better assess and estimate the positive impacts of this kind of learning for this particular domain. The CyberAware platform can be extended in different ways. We are already working on a software module that will let the educators to automatically analyze the log files produced by the gaming app. This will enable the generation of visual representations of the student's learning curve and enable (semi)automatic content adaptation depending on the learner's age and journey/progress within the app. Moreover, our intention is to examine the potential integration of the app with well-known open source LCMS platforms like Moodle and others. This would not only bring along a greater variety of synchronous and asynchronous learning tools to both the learner and the educator but also help to boost its impact and lifetime.

Finally, while our initial findings are positive, more work has to be done, involving a greater number of participants and a calibrated evaluation instrument in order to further study the pedagogical value of our approach.

## ORCID

Filippos Giannakas  <http://orcid.org/0000-0002-9172-8966>

## References

- Anaraki, F. (2004). Developing an effective and efficient e-learning platform. *International Journal of the Computer, the Internet and Management*, 12(2), 57–63.
- Anderson, J. R., Reder, L. M., & Simon, H. A. (1996). Situated learning and education. *Educational Researcher*, 25(4), 5–11. doi:10.3102/0013189X025004005
- Anderson, L. W., Krathwohl, D. R., Airasian, P. W., Cruikshank, K. A., Mayer, R. E., Pintrich, P. R., ... Wittrock, M. C. (2001). *A taxonomy for learning, teaching, and assessing: A revision of bloom's taxonomy of educational objectives, abridged edition*. White Plains, NY: Longman.
- Arachchilage, N. A. G., & Cole, M. (2011). Design a mobile game for home computer users to prevent from "phishing attacks". In *International conference on, information society (i-society)* (pp. 485–489), London, UK.
- Boud, D., Keogh, R., & Walker, D. (2015 November 26). *Reflection: Turning experience into learning*. Routledge. <https://www.taylorfrancis.com/books/9781315059051>
- Branch, R. M. (2009). *Instructional design: The addie approach* (Vol. 722). Springer Science & Business Media. <https://link.springer.com/book/10.1007/978-0-387-09506-6>
- Burguillo, J. C. (2010). Using game theory and competition-based learning to stimulate student motivation and performance. *Computers & Education*, 55(2), 566–575. doi:10.1016/j.compedu.2010.02.018
- Case, R. (2013). The unfortunate consequences of bloom's taxonomy. *Social Education*, 77(4), 196–200.
- CERIAS. (2018, August). *K-5 information security curriculum*. Retrieved from <https://www.cerias.purdue.edu/site/education/k-12/infosec/activities/k5>
- Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication*, 52(2), 167–182.
- CyberLiteracy, N. I. C. E. R. C. (2018, August). *Cyberliteracy2 curriculum*. Retrieved from <https://nicerc.org/curricula/cyber-literacy-2/>
- Dasgupta, D., Ferebee, D. M., & Michalewicz, Z. (2013). Applying puzzle-based learning to cyber-security education. *Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference*, (pp. 20), New York, USA. <https://lib.ugent.be/catalog/ebk01:3780000000084192>
- Dick, W., Carey, L., & Carey, J. O. (2014). *The systematic design of instruction*. The University of Texas: Pearson Higher Ed. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.457.5828&rep=rep1&type=pdf>
- eSafety, A. G. (2018, August). *esafety website classroom resources*. Retrieved from <https://esafety.gov.au/education-resources/classroom-resources>
- GetSafeOnline, G., UK. (2018, August). *Getsafeonline campaign for children aged 6 to 9 old*. Retrieved from <https://www.getsafeonline.org/safeguarding-children/6-to-9/>
- Giannakas, F., Kambourakis, G., & Gritzalis, S. (2015). Cyberaware: A mobile game-based app for cybersecurity education and awareness. In *Interactive mobile com-*

- communication technologies and learning (imcl), 2015 international conference on (pp. 54–58), Thessaloniki, Greece.
- Giannakas, F., Kambourakis, G., Papasalouros, A., & Gritzalis, S. (2016). Security education and awareness for k-6 going mobile. *International Journal of Interactive Mobile Technologies (ijim)*, 10(2), 41–48. doi:10.3991/ijim.v10i2.5473
- Giannakas, F., Kambourakis, G., Papasalouros, A., & Gritzalis, S. (2017). A critical review of 13 years of mobile game-based learning. *Educational Technology Research and Development*, 66(2), 341–384.
- Gibbons, A. S., Boling, E., & Smith, K. M. (2014). Instructional design models. In *Handbook of research on educational communications and technology* (pp. 607–615). New York, USA: Springer.
- Gikas, J., & Grant, M. M. (2013). Mobile computing devices in higher education: Student perspectives on learning with cell-phones, smartphones & social media. *The Internet and Higher Education*, 19, 18–26. doi:10.1016/j.iheduc.2013.06.002
- Google. (2017, June). Interland: Be internet awesome. Retrieved from <https://beinternetawesome.withgoogle.com/interland/>
- Heinich, R., Molenda, M., Russell, J. D., & Smaldino, S. E. (2005). *Instructional technology and media for learning* (Vol. 141). New Jersey, Columbus: MULTI MEDIA PEM- BELAJARAN.
- Hodges, C. B. (2004). Designing to motivate: Motivational techniques to incorporate in e-learning experiences. *The Journal of Interactive Online Learning*, 2(3), 1–7.
- Kambourakis, G. (2013). Security and privacy in m-learning and beyond: Challenges and state of the art. *International Journal of U-And e-Service, Science and Technology*, 6(3), 67–84.
- Kambourakis, G. (2014). Anonymity and closely related terms in the cyberspace: An analysis by example. *Journal of Information Security and Applications*, 19(1), 2–17. doi:10.1016/j.jjsa.2014.04.001
- Kambourakis, G., Kontoni, D.-P. N., Rouskas, A., & Gritzalis, S. (2007). A pki approach for deploying modern secure distributed e-learning and m-learning environments. *Computers & Education*, 48(1), 1–16. doi:10.1016/j.compedu.2004.10.017
- Kambourakis, G., Kontoni, D.-P. N., & Sapounas, I. (2004). Introducing attribute certificates to secure distributed e-learning or m-learning services. In *Proceedings of the iasted international conference* (pp. 436–440), Innsbruck, Austria.
- Keller, J. M. (1987a). Development and use of the ARCS model of instructional design. *Journal of Instructional Development*, 10(3), 2–10. doi:10.1007/BF02905780
- Keller, J. M. (1987b). Strategies for stimulating the motivation to learn. *Performance Improvement*, 26(8), 1–7.
- Komalawardhana, N., & Panjaburee, P. (2018). Proposal of personalised mobile game from inquiry-based learning activities perspective: relationships among genders, learning styles, perceptions, and learning interest. *International Journal of Mobile Learning and Organisation*, 12(1), 55–76. doi:10.1504/IJMLO.2018.089237
- Korucu, A. T., & Alkan, A. (2011). Differences between m-learning (mobile learning) and e-learning, basic terminology and usage of m-learning in education. *Procedia- Social and Behavioral Sciences*, 15, 1925–1930. doi:10.1016/j.sbspro.2011.04.029
- Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2), 7. doi:10.1145/1754393.1754396
- Le Compte, A., Elizondo, D., & Watson, T. (2015). A renewed approach to serious games for cyber security. In *Cyber conflict: Architectures in cyberspace (cycon)*, 2015 7th international conference on (pp. 203–216), Tallinn, Estonia.
- Lebow, D. G., & Wager, W. W. (1994). Authentic activity as a model for appropriate learning activity: Implications for emerging instructional technologies. *Canadian Journal of Educational Communication*, 23, 231.
- Lee, W.-J., Huang, C.-W., Wu, C.-J., Huang, S.-T., & Chen, G.-D. (2012). The effects of using embodied interactions to improve learning performance. In *12th international conference on, advanced learning technologies (icalt)* (pp. 557–559). doi:10.1094/PDIS-11-11-0999-PDN
- Lepper, M. R., & Malone, T. W. (1987). Intrinsic motivation and instructional effectiveness in computer-based education. *Aptitude, Learning, and Instruction*, 3, 255–286.
- Malone, T. W. (1981). What makes things fun to learn? a study of intrinsically motivating computer games. *Pipeline*, 6(2), 50–51.
- Peterson, C. (2003). Bringing addie to life: Instructional design at its best. *Journal of Educational Multimedia and Hypermedia*, 12(3), 227–241.
- Rau, P.-L. P., Gao, Q., & Wu, L.-M. (2008). Using mobile communication technology in high school education: Motivation, pressure, and learning performance. *Computers & Education*, 50(1), 1–22. doi:10.1016/j.compedu.2006.03.008
- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on usable privacy and security* (pp. 88–99). ACM. doi:10.1094/PDIS-91-4-0467B
- Srikwan, S., & Jakobsson, M. (2008). Using cartoons to teach internet security. *Cryptologia*, 32(2), 137–154. doi:10.1080/01611190701743724
- Star, J. R., & Stylianides, G. J. (2013). Procedural and conceptual knowledge: exploring the gap between knowledge type and knowledge quality. *Canadian Journal of Science, Mathematics and Technology Education*, 13(2), 169–181. doi:10.1080/14926156.2013.784828
- StaySafeOnline, N. C. S. A. (2018, August). *Staysafeonline grades 3-5 teaching resources*. Retrieved from <https://staysafeonline.org/get-involved/at-school/grades-k-2/>
- Sugrue, B. (2002). *Problems with bloom's taxonomy*. Retrieved from <https://eppicinc.files.wordpress.com/2011/08/sugrue/bloom/critique/perfxprs.pdf>
- Tupsamudre, H., Wasnik, R., Biswas, S., Pandit, S., Vaddepalli, S., Shinde, A., ... Lodha, S. (2018). *Gap: A game for improving*



- awareness about passwords* (pp. 66–78). Darmstadt, Germany: Springer.
- Vieira, L., & Coutinho, C. (2017). *Urban games: How to increase the motivation, interaction and perceived learning of students in the schools* (pp. 1318–1334). Pennsylvania, USA: IGI Global.
- Visoottiviseth, V., Phungphat, A., Puttawong, N., Chantaraumporn, P., & Haga, J. (2018). Lord of secure: the virtual reality game for educating network security. In *2018 seventh ict international student project conference*, Nakhon Pathom, Thailand, (*ict-isp*) (pp. 1–6).
- Woo, J.-C. (2014). Digital game-based learning supports student motivation, cognitive success, and performance outcomes. *Journal of Educational Technology & Society*, 17(3), 291–307.
- Yang, Y.-T. C. (2012). Building virtual cities, inspiring intelligent citizens: Digital games for developing students' problem solving and learning motivation. *Computers & Education*, 59(2), 365–377. doi:10.1016/j.compedu.2012.01.012
- Yee, N. (2006). Motivations for play in online games. *CyberPsychology & Behavior*, 9(6), 772–775. doi:10.1089/cpb.2006.9.772
- Zechner, M. (2012). *Libgdx documentation initiative*. Retrieved from <http://www.badlogicgames.com/wordpress>

## Appendix

**Table A1.** Effectiveness: test questions for the security section.

Item	Question
Q1	Select and circle from the following list all the items needed to protect an Internet-connected device. List: (i) Antivirus, (ii) Image processing software, (iii) Security updates or patches, (iv) email filter, (v) Music player, (vi) Firewall, (vii) Video player.
Q2	Choose and circle from the following list all the items that justify the use of a firewall to protect an Internet-connected device. List: (i) Prevent hacking attempts against your Internet-connected device, (ii) Protect your device from downloading malware, (iii) When using it, can rest assure that their software is up-to-date, (iv) Blocks spam and other unwanted emails from entering your inbox.
Q3	Choose and circle from the following list all the items that justify the use of an antivirus to protect an Internet-connected device. List: Same options as in Q2.
Q4	Select and circle from the following list all the items that mandate the use of security updates and patches for an Internet-connected device. List: Same options as in Q2.
Q5	Choose and circle from the following list all the items that endorse the use of spam filtering. List: Same options as in Q2.
Q6	Choose and circle from the following list all the real-life scenarios where a user needs to apply at least one cybersecurity technology. List: (i) To play a game on the Web, (ii) After clicking on a web link i was prompted for an authorization approval, (iii) Unwanted advertising emails are entering my inbox, (iv) To play a music file received by email, (v) To type some sentences using the word processor, (vi) A friend of mine sent me an email that contains a web link, (vii) To visit a web site containing comics, (ix) To play music via the computer's CD player, (x) To download a game to my PC, (xi) To paint a doodle using a drawing software tool.
Q7	Choose and circle from the following list all the items that seem to be good (strong) password candidates. List: (i) Your name, (ii) At least eight alphabetical characters long, (iii) A series of alphabets, numbers, and special characters, (iv) 12345678, (v) The word "password", (vi) Five characters long, (vii) Your birth date, (ix) Your dog's name, (x) Your mobile telephone number.
Q8	Choose and circle from strongest passwords List: (i) Filip, (ii) 11111111, (iii) codeA12#\$, (iv) no password, (v) !2drg456A, (vi) may the force be with you, (vii) Hacker123.

**Table A2.** Effectiveness: test questions for the privacy section.

Item	Question
Q1	Select and circle from the following list all the pieces of information that need to be kept private. List: (i) Your favorite team, (ii) Your telephone number, (iii) Your favorite desert, (iv) Your home address, (v) Your everyday schedule, (vi) Your favorite comic, (vii) Your father's/mother's ID number, (ix) Your favorite sport.
Q2	Choose and circle from the following list all the information that can be safely posted on the Facebook. List: (i) George, the spaghetti we ate at that restaurant was delicious, (ii) Tom, i want to invite you at my home located at 4325 W. Palm Beach Rd, (iii) I am so happy because my team won the match today, (iv) Elen, do not forget our appointment today at metro station located at Syntagma, at 18:00 o'clock, (v) Give me a call on +345435325235.

**Table A3.** The questionnaire instrument regarding app usability, and user satisfaction and expectations.

Item	Question
Q1	a. Male, b. Female
Q2	a. 9, b. 10, c. 11, d. 12
Q3	Have you ever played a digital game? (Yes or No)
Q4	Have you ever played an educational game? (Yes or No)
Q5	I love playing digital games. (Yes or No)
Q6	How much do you agree with the following statements regarding the game? (check all the appropriate boxes)
(a) <input type="checkbox"/>	It was easy to use.
(b) <input type="checkbox"/>	The instructions on how to play were easy to understand.
(c) <input type="checkbox"/>	The game's information (game play and learning goals) were comprehensible.
(d) <input type="checkbox"/>	The messages displayed on the screen after a given answer were comprehensible.
(e) <input type="checkbox"/>	When a given answer was wrong, the displayed message helped me to find the correct answer.
(f) <input type="checkbox"/>	Every mini-game was easy to navigate.
(g) <input type="checkbox"/>	After an action, it was easy to understand what to do next.
Q7	Did you face any problem when using the game (e.g., small mobile screen, interactions with the touch screen, structure of learning activities, etc)? If yes, please describe it shortly.
Q8	How much do you agree with the following statements regarding the game? (check all the appropriate boxes)
(a) <input type="checkbox"/>	It was very funny to learn while playing the game.
(b) <input type="checkbox"/>	I liked that the game has a short amount of reading material and more action.
(c) <input type="checkbox"/>	I would like to play the game again in my classroom.
(d) <input type="checkbox"/>	I would like to play the game again outside the classroom in my free time.
(e) <input type="checkbox"/>	I became familiar with what is required for a personal device to be protected against basic online attacks from the Web.
(f) <input type="checkbox"/>	I realized the importance of privacy in the Internet age.
(g) <input type="checkbox"/>	I will recommend it to my friends.
Q9	Do you expect anything else from the game? if so, please describe it shortly.