Security education and awareness for K-6 going mobile

Filippos Giannakas*, Georgios Kambourakis, Andreas Papasalouros‡, and Stefanos Gritzalis
*Department of Information and Communication Systems Engineering,
University of the Aegean, Samos, Greece
Email: fgiannakas@aegean.gr, gkamb@aegean.gr, sgritz@aegean.gr
‡Department of Mathematics, University of the Aegean, Samos, Greece
Email: andpapas@aegean.gr

***Abstract*—Nowadays, due to the widespread participation of elementary school children in cyberspace activities, basic cybersecurity education and awareness is deemed necessary. Within this context, knowledge acquisition in this timely and important field has greater chances to be more fruitful when the learner is properly motivated. Also, it is anticipated to be more joyful when knowledge is acquired in the form of a digital game-based activity. The paper at hand discusses the development of a novel mobile app called CyberAware, destined to cybersecurity education and awareness. At present, the game is designed for K-6 children in order to support either or both formal or informal learning. Additionally, due to its mobile characteristics, the game can be experienced as an outdoor or classroom activity. Finally, opposite to similar studies found in the literature so far, our attention is not solely drawn to game's technological aspects but equally to the educational factor. This is achieved through the consideration and use of the ARCS motivational model already from the game's design phase.**

***Keywords*—Security education and awareness; mDGBL; motivation, ARCS.**

Note: This work is based in part on a paper presented at the IMCL 2015, The 9th International Conference on Interactive Mobile Communication, Technologies and Learning [1].

I. Introduction

It is rather undisputed that Digital Game Based Learning (DGBL) makes learning more attractive, motivating and personalized from the learner's viewpoint. Additionally, this type of games intend to improve and enhance, in a playful and enjoyable manner, some specific aspects of learning and can be met in every level of education. As such, it has been applied to numerous science education fields and curricula, more lately to cybersecurity education and awareness, which is the topic of this paper. Lately, with the advances in mobile computing, the positive outcomes of DGBL become even more reachable in the form of mobile DGBL (mDGBL).

In this direction, when creating interactive learning contexts in a mDGBL app, there is a prominent need to identify the highly motivated aspects of a game. In literature, this can be promoted by specific "design patterns". A Game Design Pattern (GDP) [2] is a method of codifying the knowledge that describes the design of game elements related to interaction. Within the context of m-Learning, the work [3] systematically reviews the GDPs for mobile platforms. A GDP pattern that is primarily well-suited to mobile platforms is that of "Quick Games", which in literature is also known as mini-games. These are considered as quick session games that can also be played casually and on-the-go. Under this mindset, the mobile app described in this paper follows the aforementioned strategy and embeds a number of mini-games in order to provide burst-knowledge experience to the learners.

Being a multidisciplinary challenge, the creation of a truly effective mDGBL platform or app for science education is far from being trivial. Technological advances and facilities should be seen and placed in conjunction with the human player in order to maximize their payoffs. Moreover, the right blending of learning theories in a (serious) game's storyline is decisive yet often neglected by designers. In some cases, this omission may be due to the undisputed difficulties designers face in applying the discrete stages of a learning theory directly to the game in a way it fulfills specific learning outcomes. Last but not least, seeing this issue from a Bring Your Own Device (BYOD) point of view, there is a need for such apps to work on arbitrary mobile devices and platforms. This is certain to not only overcome several mobile platform peculiarities, but to also increase learning independency and augment the anywhere, anytime learning experience.

Our contribution: Motivated by the aforementioned issues, the paper at hand discusses the development of a novel mDGBL app called CyberAware destined to cybersecurity education and awareness. Among others, the topics considered by CyberAware include: firewall technologies, antivirus software, security patches and updates, and email spam filters. Contrary to other works in the literature, our contribution is not solely focused on technical aspects but on the pedagogical factor as well. Thus, the design of the game is based on the Attention, Relevance, Confidence, and Satisfaction (ARCS) motivational model [4]. At present, CyberAware is designed for K-6 educators and can be used to support either or both formal or informal learning exercised as an outdoor or indoor activity. The game prototype is developed using standard software tools, including Android Development Kit (ADK) and the open-source libGDX game engine [5]. A preliminary evaluation of the game app is also performed using both pre- and post-questionnaires.

The rest of the paper is organized as follows. The next section briefly addresses related work on the topic. Section III details on CyberWare app. The conceptual framework along with the motivational model we used and as well as their interconnections with CyberAware app are discussed in section IV. The evaluation results are presented in Section VI. The last section concludes and presents future work.

II. Related Work

Nowadays, due to the Internet penetration and the popularity of social networking sites among adolescents, basic cybersecurity education and awareness is deemed necessary. In this context, digital serious games may be proved valuable for teaching security issues to this audience more effectively [6] and in a more personalised way towards cultivating security culture. Thus far, only a handful of works in the literature combine cybersecurity training and awareness with DGBL, and more scarcely with mDGBL. However, as explained further down, none of them is specially designed for K-6 or K-12 students. Also, the overwhelming majority of these works mostly neglect the educational factor and concentrate solely on the technological one, i.e., the implementation of the game.

The authors in [6] developed "PhishGuru", a personalized story-based anti-Phishing educational software aiming to alarm people about phishing attacks pertaining to email use. A similar work, namely "Anti-Phishing Phil" [7], is an online game that teaches end-users how to use cues in URLs to avoid becoming victims of "Phishing" attacks. "CyberProtect" [8] and "SecurityCartoons" [9] are both interactive online web-based games dedicated to information security assurance. Note that, all the above mentioned works have been implemented for desktop computing platforms. In the context of mDGBL the only work dedicated to cybersecurity is the one given in [10]. Specifically, the authors presented an educational mobile app designed to alert home computer users against phishing attacks.

Conclusively, and up to our knowledge, none of the existing works uses the advantages of mobile educational games in supporting learning in the field of cybersecurity awareness. This paper aims at filling this gap, given the importance of the subject for young students and the potential educational benefits of mDGBL environments.

III. CyberAware

As already pointed out, today, Internet penetration is more evident to young people, mostly due to the popularity of social networking sites and the multiplayer online games, among others. This situation makes cybersecurity education for adolescents an important and urgent issue. In this context, CyberAware is destined to support learners with an alternative, joyful and more efficient way for learning data security issues and raising security awareness. At a nutshell, the aim of the game presented in this article is to familiarize students with fundamental cybersecurity technologies that are required to keep their Internet-connected devices protected against legacy threats, including malware, cyber-attacks, and spam.

In the game scenario, the student selects a learning topic (e.g., security or privacy) and plays a series of mini-games. For providing both intrinsic and extrinsic motivation, upon the successful completion of each mini-game, the virtual "security shield" that is associated with it unlocks. If at the end of the game all the corresponding shields have been removed, the player unlocks the "Arena Security" mini-game for that topic. Lastly, upon the completion of all the game's challenges, the learner is awarded with a "CyberAware certificate".

Before starting a mini-game, the app informs the learner of how to play each quick session game and which is the current learning goal. It is to be stressed that the CyberAware app was not designed with the aim to provide the learner with pure and long-term reading material. Therefore, our design is in contrast to classical approaches, which require the student to follow a full reading process and then answer a series of questions, which is well-known to often cause boredom and inattention to students. Further, its main aim is for the student to discover new knowledge entirely by herself following a problem-based approach. For the security learning topic, the first two mini-games actively support and guide the student toward the correct answer by offering advising tips and hints, when, say, the player's answer is incorrect. Another key goal of CyberAware is to enhance learner's motivation towards an autonomous and self-directed learning process. As explained in section IV, this is achieved by problem-solving activities that promote critical thinking. In such an environment, the student is motivated to not only understand the various concepts being taught, but also to recognize their application in various real-life situations as well. In the following subsections, we detail on the conceptual framework and the ARCS motivational model on which Cyberware is built.

IV. Conceptucal Framework & Motivational Model

Motivation is considered as a theoretical construct for explaining learner's behavior. Generally speaking, motivation, both intrinsic and extrinsic, is considered as the key factor to alter or improve learning outcomes [11]. So, the effort required from the educator to capitalize on motivation during the design of the learning process is generally considered as a challenging and demanding procedure. It is also implied that the educator needs to carefully prepare the course being taught, and design it so as the instructional material to satisfy the following requirements: a) to be content-rich and, b) to be blended with appealing characteristics for "keeping learning on track".

In the literature there are numerous motivational theories. Each of them, explains the same motivational concepts and how they influence educator's learning flow from different perspectives. Therefore, we must admit that examining and understanding each of the motivational theories, may be considered a cumbersome and complex procedure due to the existence of different and inter-related factors. An attestation to this complexity is also the categorization of these theories. According to the "Elsevier's Dictionary of Psychological Theories" [12], there are free broad categories: a) "Hedonic or Pleasure Motivational Theories", b) "Cognitive or Need-to-Know Motivational Theories", and c) "Growth or Actualization Motivational Theories".

Having the above in mind, we have carefully designed our learning strategy before starting the development of the app so as to be clear content, relevant, and adapted to modern platforms, including the mobile ones. To do so, we considered that the design of CyberAware for a mobile environment should be guided by an instructional strategy based on a learning theory that should outline the learning process and guarantee the outcomes. This can be addressed by an Instructional Design Model (IDM) [13]. The latter details on how the learning experience can be orchestrated for the learner to acquire knowledge and skills in a more efficient, effective, and attractive way. In a more abstract form, such a model consists of guidelines and/or strategies for organizing clear-cut pedagogical scenarios toward the achievement of specific instructional goals.

Within the context of IDMs, in literature there are numerous instructional models such as ADDIE [14], ASSURE [15], Dick and Carey [16], ARCS, etc. Each of them examines motivation from different perspectives. Below we detail on the ARCS motivational model and how this is embedded in the conceptual framework we used during the design of CyberAware app.

A. Conceptual Framework

The conceptual framework we used in CyberAware is depicted in figure 1. It outlines the logical links among three components; the app, the learner's motivation, and the instructional design model. As already mentioned, motivation is considered as the key factor during the learning process. This is becoming more evident, when learner's motivation is kept at a high level, which in turn implies a higher positive impact during the learning process in terms of learner's engagement with the app. As a direct result, this situation is anticipated to spur the learner to keep in track and meet the expected learning outcomes.

For CyberAware we used ARCS as the IDM. Specifically, regarding the conceptual framework we used, the learner is placed in the center of knowledge acquisition, while she engages and interacts with the CyberAware Graphical User Interface (GUI) and the learning material. As explained further in this section, the ARCS model specifies all these strategies, guidelines and processes enabling us to design a suitable instructional material that sustains motivation and actively engages the learner in the learning process.

The aforementioned conceptual framework could be also seen as a continuous adjustment procedure between the app and learner's motivation. Specifically, if necessary, the developer may alter the designing characteristics of the app to embed new challenges and/or procedures towards augmenting the motivation of learners.

B. CyberAware scenarios

CyberAware is a problem-solving environment in which the student actively participates and accomplishes a series of sort challenges. This is achieved by a number of mini-games that the student mandatorily plays in a row. For instance, the security learning topic consists of 3 mini-games. As illustrated in figure 2, in the first one, the learner is presented with several relevant and irrelevant technologies pertaining to basic cybersecurity technologies and is challenged to select the correct ones and place them to the four "NEED for protection" horizontal compartments.

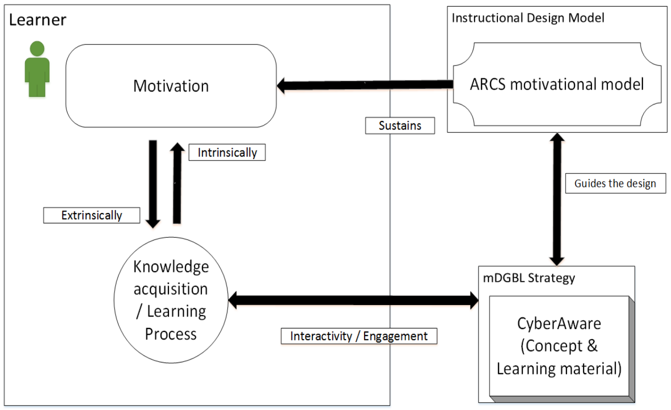

Learner
Motivation
Instructional Design Model
ARCS motivational model
Sustains
Intrinsically
Extrinsically
Guides the design
Knowledge acquisition / Learning Process
mDGBL Strategy
Interactivity / Engagement
CyberAware (Concept & Learning material)

Fig. 1. Abstract view of CyberAware conceptual framework

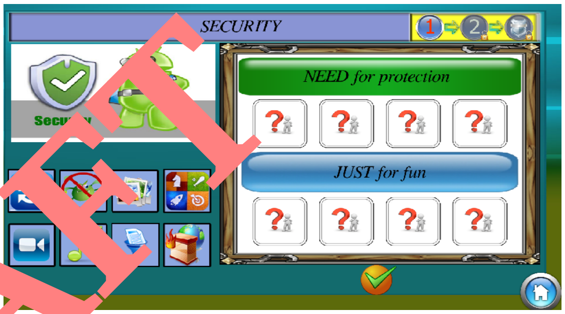
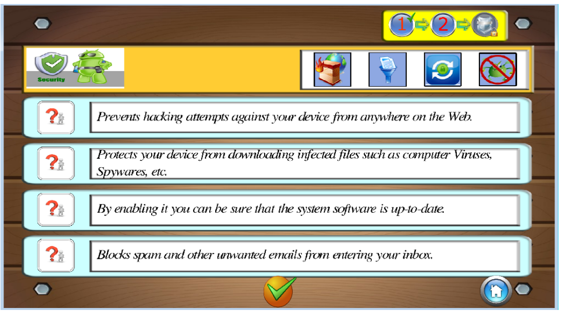


Fig. 2. First mini-game: Identify the correct cybertechnologies.

Upon the successful completion of the previous challenge, a second mini-game starts. Its goal is to teach the student to correctly associate each security technology (that she has already identified) with its specific value in keeping their device safe. This situation for the second mini-game of the security topic is illustrated in figure 3. After that, as seen in fig. 5, the "Arena Security" mini-game unlocks.



Prevents hacking attempts against your device from anywhere on the Web.

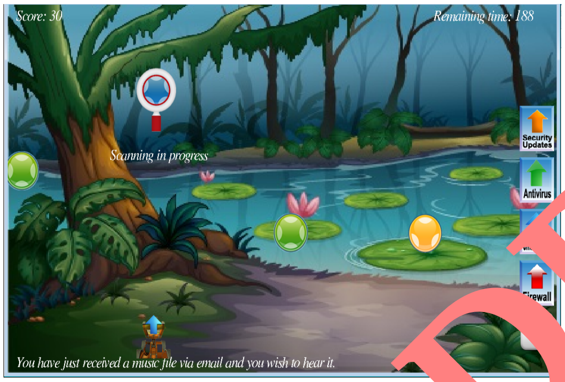
Protects your device from downloading infected files such as computer Viruses, Spywares, etc.

By enabling it you can be sure that the system software is up-to-date.

Blocks spam and other unwanted emails from entering your inbox.

Fig. 3. Second mini-game for the security topic.

The goal of this third mini-game is for the student to figure out those security technologies needed for handling specific online scenarios. These scenarios are based on typical real-life actions on the web. This challenge is crucial for a student in order to associate the knowledge she gains while interacting with the app with real scenarios she encounters while being on the web. More precisely, Arena Security consists of balls that fly from the right to the left side of the device's screen. When a ball appears on the screen it is randomly assigned to a specific scenario, e.g., “You received an email containing a music file. You should open and hear it”, “You are using a streaming app to download video files”, etc. First off, the student must use the magnifier tool to start scanning a ball in order to become aware of the parameters of the corresponding scenario. In the current version of the game, each scenario appears at the bottom of the screen. Then, based on the already acquired knowledge, the player needs to correctly identify the threat and select accordingly the right data security technology (colorful arrow on the right side of fig. 4) that eliminates it. This is achieved by selecting and throwing against the ball of interest the correct arrow, which is assigned to the appropriate cybersecurity technology (i.e., Antivirus, Firewall, Spam Filter, Security Updates and patches, and so forth). If a ball is hit by the proper cybersecurity technology (arrow), then the player collects 10 points. The learner is given 4 minutes to collect as many points as they can. Note that currently the player does not receive any negative points when she selects a wrong arrow.



You have just received a music file via email and you wish to hear it.

Fig. 4. The Arena Security mini-game: Identify the cyber-threat and face it.

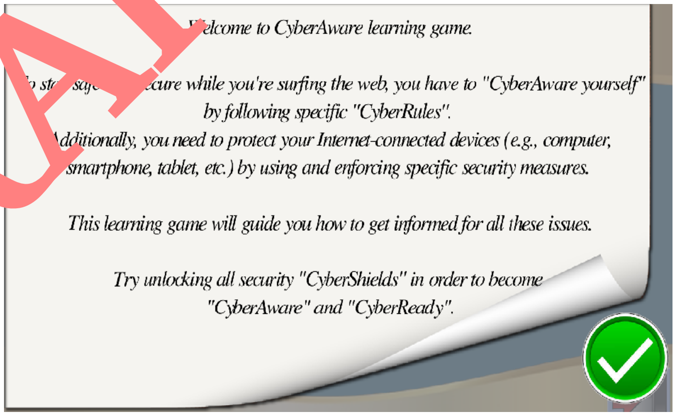
C. ARCS motivational model

ARCS [4] is a synthesis of several motivational theories, including: behavioral contingency design and management, skills and knowledge, cognitive accounting of individual abilities, and expectancy-value theory, which is met in the context of social learning theory. In this theory, the learner participates to problem-solving tasks and expects specific learning outcomes according to their behavior. Putting it another way, the model is a systematic design process for promoting and spurring motivation during the learning process. Overall, the main purpose of the model is to instruct the design of a learning app to be more intrinsically interesting to the learners. Although other models and theories for instructional design based on motivation exist, e.g. that in [17], the ARCS model was used since it provides concrete strategies for motivation based Instructional Design (ID).

The interconnection of ARCS components with the structural elements of CyberAware is depicted in figure 7. As observed from the figure, ARCS consists of 4 major components for promoting and sustaining motivation during the learning process, namely Attention, Relevance, Confidence, and Satisfaction. Each of them, consists of several other subcomponents that qualify how motivated self-directed learning can be succeeded. Within the next paragraphs, we detail on how the above mentioned qualities are involved in the design phase of CyberAware.

1) Attention: The ARCS motivational model describes the necessary stages that a learning strategy should encompass in order to keep learner's attention during learning. This quality is proved to be one of the major factors in ARCS, since the challenge is to retain learner's attention during the learning process by keeping her engagement at a high level. As observed in figure 7, this is fulfilled by the “Active Participation”, “Inquiry Arousal”, and “Maintain Attention” subcomponents.

Student's active participation is achieved when she mandatorily plays the three mini-games in a row, as illustrated in figures 2 to 4. Same, learner's stimulation in the learning process is maintained by subcomponents such as time countdown and score, which are also shown in figure 4. Finally, inquiry arousal screens are popped up before starting the main game as illustrated in figure 5, and before starting each section or a mini-game accordingly, as shown for example in figure 6.



Welcome to CyberAware learning game.

To stay safe and secure while you're surfing the web, you have to "CyberAware yourself" by following specific "CyberRules".

Additionally, you need to protect your Internet-connected devices (e.g., computer, smartphone, tablet, etc.) by using and enforcing specific security measures.

This learning game will guide you how to get informed for all these issues.

Try unlocking all security "CyberShields" in order to become "CyberAware" and "CyberReady".

Fig. 5. The initial screen for the security topic: Main inquiry.

2) Relevance: Relevance is also a key component of ARCS model. As given in figure 7, it splits into the “Present Worth” and the “Future Worth” sub-components. According to the model, it must be clear to the student why this course is worthy of being accomplished and how it is connected to real-life problems and situations. Both the aforementioned requirements are fulfilled via the mini-games discussed in the previous section as well as through a specially crafted storyline. That is, when CyberAware starts, a specific storyline inquiry is being displayed on the screen. The same procedure is followed before the initiation of an individual mini-game. This is to stimulate

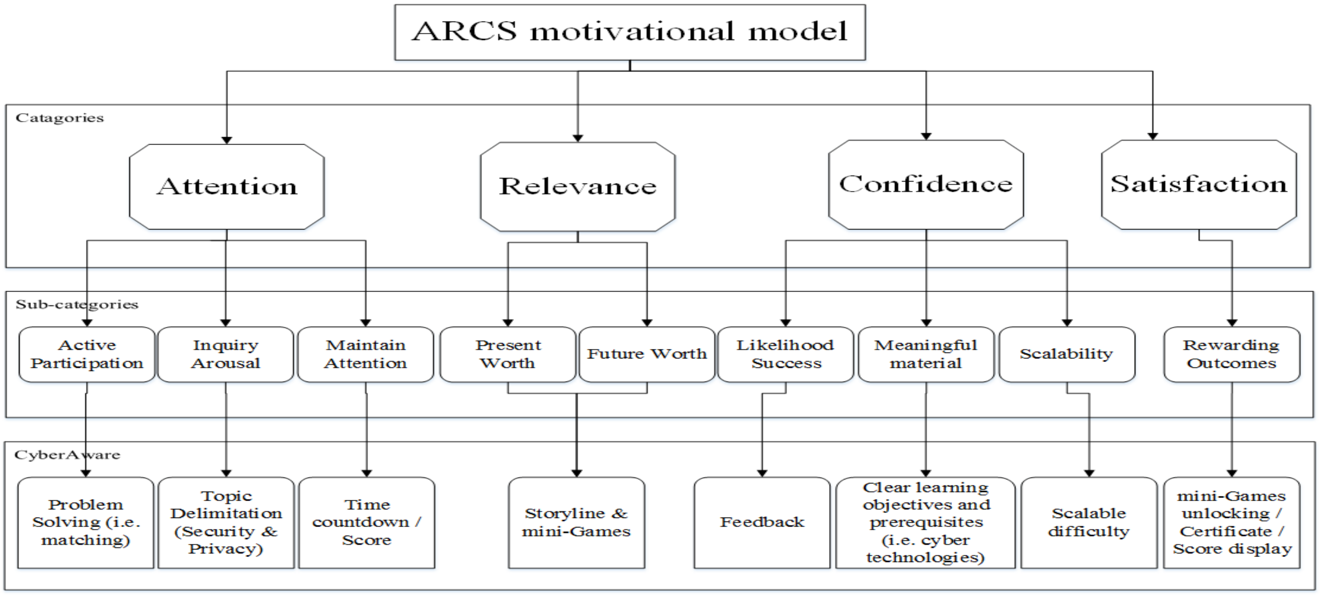
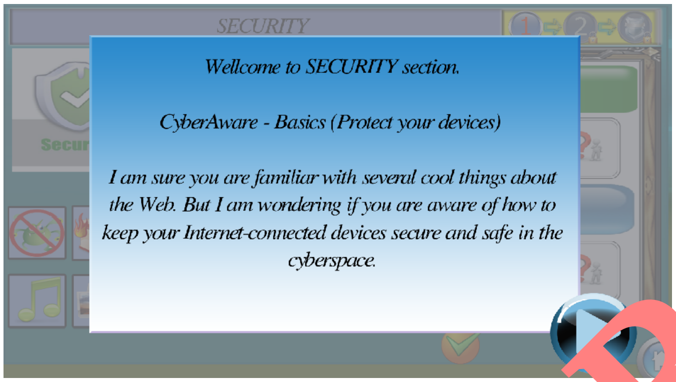


Fig. 7. CyberAware and ARCS interconnection

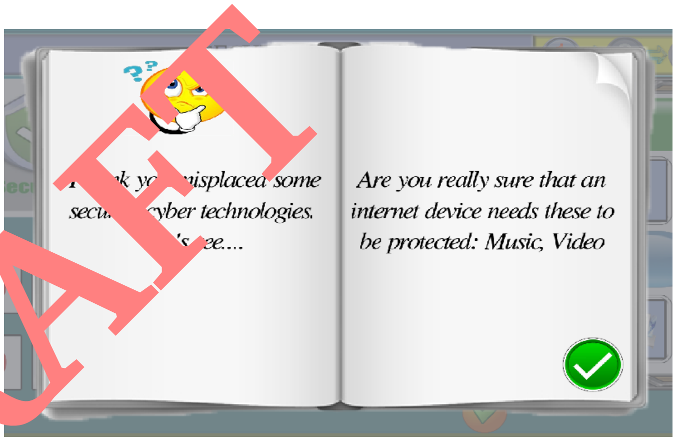


Wellcome to SECURITY section.

CyberAware - Basics (Protect your devices)

I am sure you are familiar with several cool things about the Web. But I am wondering if you are aware of how to keep your Internet-connected devices secure and safe in the cyberspace.

Fig. 6. The initial screen for the security topic: Main inquiry.


I think you misplaced some security cyber technologies. Let's see....

Are you really sure that an internet device needs these to be protected: Music, Video

Fig. 8. Advising tips and hints.

learner’s interest in exploring why it is valuable for them to attend this particular module. Precisely, as observed in figure 5, the game displays the main inquiry, indicating in this way to the student which is the present worth (interests and goals) for her to be engaged with this course/module. Similarly, upon the selection of a learning topic, a consecutive inquiry is displayed.

3) Confidence: As depicted in figure 7, confidence is split out into two subcomponents, namely “Likelihood success” and “Meaningful material”. Specifically, it is very important for the player to feel that she is capable of performing a task successfully. Hence, to increase the chances of student success, CyberAware actively supports and guides the student toward the correct answer. As depicted in figure 8, this is done by offering advising tips and hints, when, say, the player’s answer is incorrect. For instance, in the first mini-game, when the student’s answer is erroneous, a personalised message guides her in finding the correct answer.

Further, in order to cultivate confidence between the learner and the app, it is essential the learning material to be designed in such a way that its objectives are clear to them. Additionally, the learning material should place realistic expectations and if possible to accommodate scalable levels of difficulty. Under this prism, CyberAware has clear learning objectives with the aim to familiarize students with fundamental cybersecurity technologies.

Specifically, the learning objectives associated with the app can be summarized as follows:

1) Students should be able to identify the cybersecurity technologies that an internet connected device must incorporate in order for its user to stay safe in the cyberspace.
2) Students should be able to appraise and rate each cybersecurity-technology in terms of the level of protection it offers.

3) Given a series of real-life internet usage scenarios, the students should be able to identify and select the correct cubersecurity technology needed to thwart attacks.

The above objectives adhere to the first four levels of Bloom's revised taxonomy of educational objectives [18], starting from the "Remembering" level up to the "Analyzing" one. Figure 9 depicts the interlinking between the game progression and the Bloom's revised taxonomy. More precisely, during the first and the second mini-game the learner has to recall previously acquired information (e.g., that acquired after participating to traditional teaching process in their curriculum), and better understand and appraise the use and the value of each cybersecurity technology. In the third one, and after mandatorily playing the first two mini-games, the learner has to use the knowledge acquired about cybersecurity concepts in order to apply new situations and make distinguishes between facts with reference to real-life online scenarios.

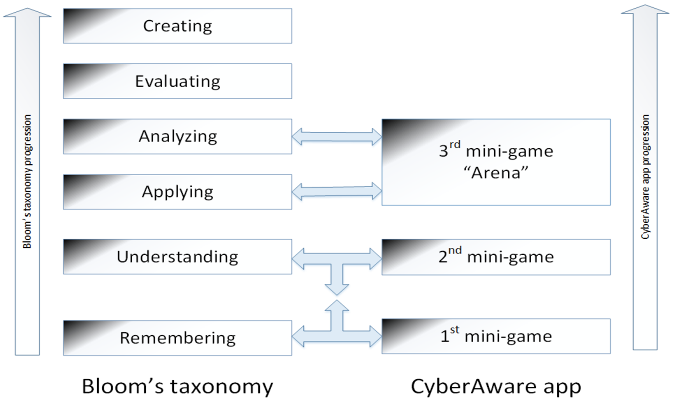


Fig. 9. CyberAware's series progression and its correspondence with Bloom revised taxonomy

Moreover, the mini-games have been designed to have a scalable difficulty which increases a mini-game after the other. Specifically, "Arena Security" is more difficult than the previous two. More precisely, in this third mini-game, the players must first think about the given scenario and then choose the correct arrow to hit and destroy the ball.

4) Satisfaction: This is the last component of the ARCS model. It is considered as a decisive component to preserve motivation, because if the student feels contented about the learning results, then she is very likely to feel the urge to play the game again. As depicted in figure 7, CyberAware fulfills this requirement by including the "Rewarding Outcomes" subcomponent. This is achieved by extrinsically rewarding the learner via unlocking security shields and new challenges such as the "Arena Security" mini-game, described in section IV. Further, it displays the player's score on the screen during the "Arena Security" mini-game. Ultimately, the game rewards the learner with the "CyberAware certificate", which certifies that she is security-aware and proficient.

V. Platform Independence and Development Technology

Another significant issue that a developer needs to take into consideration while implementing a serious app is that of the platform for which the app is destined to. Today, due to the plethora of devices of all kinds, porting an app to run on different platforms requires a significant and continuous effort in coding and testing. Consequently, most of the time, such an implementation approach is proved to be ineffective. Additionally, as pointed out in section I, platform indepedence is closely related to the BOYD concept as well. In such a case, learners are able to use their own device to play the game. This increases user's satisfaction because the player feels more comfortable using their own device. Further, seeing BYOD from an educational organization viewpoint, it needs a lot of effort from their side to develop and maintain different versions of the learning app. Therefore, it becomes clear that such a deployment creates additional costs not only for the development of the app, but also for upgrading its features and functionalities. To cope with this issue, CyberAware has been built in a way that can be run on the majority of modern platforms, ranging from desktop to mobile ones.

Specifically, for the development of CyberAware we used the Android Development Tool (ADT) plugin and libGDX game engine [5]. [illegible] with other game engines, libGDX consists of several subsystems and layered software modules. This modularised architecture focuses on code reusability and scalability as well as on the easiness of deployment of the final product in multi-platform environments. LibGDX consists of 4 modules, namely Desktop, Android, iOS, and HTML5. For more details on libGDX engine the interested reader can refer to [illegible]. Therefore, by capitalizing on such an open-source cross-platform framework, CyberAware is able to run on a variety of popular desktop and mobile platforms, including Windows, Linux, Android, and iOS.

VI. Evaluation

We performed a preliminary evaluation of CyberAware by means of both pre- and post-questionnaires (i.e., before and after the students have experienced CyberAware). Our goal was to assess both the functional characteristics of the app (user satisfaction and usability) and student learning outcomes (effectiveness). Both evaluations were conducted using a sample of 43 elementary-aged students, 20 boys and 23 girls, who ranged in age from 9 to 11 years. Before playing CyberAware all the participants had attended a security learning course in the classroom according to their curricula.

A. Usability and satisfaction

A questionnaire consisting of 12 Likert-type questions was designed to collect students' experiences about the usage of the app. Each statement consisted of 5 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 CyberAware. Table I summarises the post-questions used for the evaluation of CyberAware usability and user satisfaction properties.

Specifically, for questions Q1 to Q5 the learner had to express her opinion about the usefulness and clarity of information being provided by the app. The case where the learner plays the game in different contexts (e.g., in the classroom or elsewhere), was also examined using questions Q8 and Q9. Additionally, the usability of the app as experienced by the students was probed by questions Q3 and Q12. The app's properties related to the learning goal, the interconnection with real-life web scenarios, and the magnitude of knowledge acquisition are examined using questions Q6, Q7 and Q11, accordingly. Finally, the merit of CyberAware challenges in terms of concern to the students is also examined using question Q10.

The highlights of the findings are summarized below.

- 66.6% of the learners did not encounter any problem while playing the game.
- 74% of them did not face any problem with moving the relevant and irrelevant cybersecurity technologies in the correct place(compartment).
- 61% of the participants agreed that any message the app displays is fully informative.
- 44.4% of the learners do not prefer reading any further learning material during the game play, and 27.8% of them have a neutral opinion on the same question. This outcome also strengthens our view on designing the app to be as minimalistic as possible in terms of the volume of information provided to the student in an effort to avoid boredom and inattention.
- About 74% of the learners understand the learning objectives of each mini-game.
- 81.5% of them would play again the game in the classroom, and about 85.2% would play it at home or elsewhere.
- 37.3% agreed that the Arena Security mini-game succeeds to relate the subjects being taught with real-life online situations, while another 39% had a neutral opinion on this. After observing learners behaviour when interacting with the app, we concluded that they faced some problems in determining the scenario and selecting the correct cybersecurity technology. These problems are caused due to the ball moving speed and the time required for the learner to deactivate the magnifier before launching an arrow toward the ball of interest.
- 63% of the learners state that they understand better "what cybersecurity is all about" after playing CyberAware and 85.2% of them stated that CyberAware challenges were very interesting.

Last but not least, CyberAware is considered as a lightweight app in terms of system resources. Specifically, CPU and memory benchmarking analysis on the Android Jelly Bean platform using a 5 inch smartphone equipped with a dual-core CPU at 2GHz and 2GB of RAM reveals that the app consumes an average of 9% of CPU. Moreover, memory utilisation when the app is running fluctuates between 115 and 233 MB of RAM depending on which mini-game is active.

B. Learning/knowledge acquisition effectiveness

Knowledge delivery from external resources, such as e-Learning systems in general or m-Learning in particular, is of a major scope in learning environments. Within this context, knowledge acquisition effectiveness before and after using CyberAware, is also examined via questionnaires composed of the same 6 questions that learners answered before and after playing CyberAware. The structure of the questionnaire is given in Table II. More precisely, the learners answered the pre-questionnaire after attending their normal teaching course on security topics in the classroom according to their curricula. The post-questionnaire was answered right after a learner had interacted with the CyberAware app.

Specifically, regarding question Q1 the learners were asked to select from a provided list of answers which technologies are needed in order to protect 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 requested to identify the value of each cybersecurity technology contained in the corresponding list of answers. Finally, 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 [19].

According to our analysis, before playing the game, about 32.6% of the learners were able to recognize all 4 technologies that are required to keep their internet-connected devices protected. After playing it, this result was improved by almost 5%. An analogous improvement was also perceived for the rest of factors measured by the corresponding questions. For example, before playing the game, 18.6% of the learners were able to recognize at least 3 scenarios out of 6 that an internet-connected device needs to be protected. After playing CyberAware, this attainment rate increased to about 32.6%.

VII. Conclusion

This paper details on the design of an mDGBL app destined to cybersecurity education for students of primary education. Contrary to other works in the literature, our contribution is not focused on technical implementation only but to the pedagogical factor as well. The latter pertains to the way the ARCS motivation model is embedded in the app to maximize the learning outcomes. We show that CyberAware is simple to use and lightweight in terms of system resources. Also, it is multi-platform enabled making it ideal for the BYOD model.

Further, the current version of the game implements the "Quick Games" pattern in order to apply burst-session learning experience on cybersecurity topics. This strategic choice has been made in order to enhance learner's attention and attractiveness, and limit the existence of boredom. Therefore, there is a lot of work to be done within this challenging field, even seeing it from learners or technology perspectives. For instance, as already mentioned, adolescences experience a variety of challenges and threats when being on the web.

TABLE I. USABILITY AND SATISFACTION: QUESTIONNAIRE

Item	Question
Q1	The game's pop-up messages were fully informative, and in any case i knew what it was needed to do.
Q2	During the first and the second mini-games, i did not realize that the aim was to move the icons in their correct place.
Q3	I faced problems in moving the icons to the right place.
Q4	Before starting a mini-game, the guidelines displayed were informative enough to me for accomplishing the corresponding challenge.
Q5	Before starting a mini-game, i needed more relevant to the topic reading material because this could help me to prepare for and answer the next challenges.
Q6	The goal of each mini-game was clear enough to me.
Q7	Do you agree with the next sentence? After playing the mini-game ARENA, i learnt more on how to deal with real-life online activities.
Q8	Do you agree with the next statement? I would love to play again CyberAware for learning about security topics in the classroom.
Q9	Do you agree with the next statement? I would love to play again CyberAware outside my school.
Q10	Do you agree with the next statement? All CyberAware challenges were interesting enough.
Q11	Do you agree with the next statement? CyberAware helped me a lot to improve my knowledge about security topics.
Q12	Do you agree with the next statement? In general, during the game i did not face any usability problem.

TABLE II. LEARNING/KNOWLEDGE ACQUISITION EFFECTIVENESS: QUESTIONNAIRE

Item	Question
Q1	Choose 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 device from anywhere in the Web, (ii) Protect your device from downloading infected files such as computer Viruses, Spywares, etc., (iii) By enabling it one can rest assure that the system 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 items as given in Q2.
Q4	Choose and circle from the following list all the items that justify the use of security updates and patches for an internet-connected device. List: Same items as given in Q2
Q5	Choose and circle from the following list all the items that justify the use of spam filtering for an internet-connected device. List: Same items as given in Q2
Q6	Choose and circle from the following list all the real-life scenarios where a user needs to apply some cybersecurity technologies. List: (i) To play a game on the Web, (ii) After clicking on a web link then an authorization approval is needed, (iii) Unwanted advertising emails are entering my inbox, (iv) To play a music file that has been received by email, (v) To type a letter in the word processor, (vi) A friend of mine sent me an email that contains a web link, (vii) To visit a web site to hear music, (ix) To play music using the computer's CD player, (x) To download a game to my PC, (xi) To draw an image using a drawing software tool.

This factor pushes the research community toward the creation of more joyful and enhanced learning experiences that will support and motivate educators to learn about cybersecurity topics in a more effective way. Therefore, this challenge is not concentrated only on the creation of an effective e-Learning content, but also on finding alternatives to optimal bind the learning material with adolescences' needs and technological trends so as to create a truly effective and interactive learning experience.

As a future work, we plan to extend CyberAware functionality to integrate adaptive elements, and embrace privacy and especially anonymity topics as well.

REFERENCES

[1] F. Giannakas, G. Kambourakis, and S. Gritzalis, "Cyberaware: A mobile game-based app for cybersecurity education and awareness," in *Interactive Mobile Communication Technologies and Learning (IMCL), 2015 International Conference on*. IEEE, 2015, pp. 54–58.

[2] J. O. Borchers, "A pattern approach to interaction design," *Ai & Society*, vol. 15, no. 4, pp. 359–376, 2001.

[3] O. Davidsson, J. Peitz, and S. Björk, "Game design patterns for mobile games," *Project report to Nokia Research Center, Finland*, 2004.

[4] J. M. Keller, "Development and use of the arcs model of instructional design," *Journal of instructional development*, vol. 10, no. 3, pp. 2–10, 1987.

[5] M. Zechner. (20[illegible]) Libgdx documentation initiative.

[6] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching johnny not to fall for phish," *ACM Transactions on Internet Technology (TOIT)*, vol. 10, no. 2, p. 7, 2010.

[7] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "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*. ACM, 2007, pp. 88–99.

[8] IASE. (2014, February) Information assurance support environment (iase), dod, cyberprotect. [Online]. Available: http://iase.disa.mil/eta/Lists/IA20\Simulations/AllItems.aspx

[9] S. Srikwan and M. Jakobsson, "Using cartoons to teach internet security," *Cryptologia*, vol. 32, no. 2, pp. 137–154, 2008.

[10] N. A. G. Arachchilage and M. Cole, "Design a mobile game for home computer users to prevent from phishing attacks," in *Information Society (i-Society), 2011 International Conference on*. IEEE, 2011, pp. 485–489.

[11] C. B. Hodges, "Designing to motivate: Motivational techniques to incorporate in e-learning experiences," *The Journal of Interactive Online Learning*, vol. 2, no. 3, pp. 1–7, 2004.

[12] M. Guha, "Elsevier's dictionary of psychological theories," *Reference Reviews*, vol. 20, no. 8, pp. 10–11, 2006.

[13] A. S. Gibbons, E. Boling, and K. M. Smith, "Instructional design models," in *Handbook of research on educational communications and technology*. Springer, 2014, pp. 607–615.

[14] M. Molenda, "The addie model," *Encyclopedia of Educational Technology, ABC-CLIO*, 2003.

[15] S. E. Smaldino, D. L. Lowther, and J. D. Russell, "Instructional technology and media for learning," 2008.

[16] L. Carey, J. Carey, and W. Dick, "The systematic design of instruction," 2001.

[17] T. W. Malone, "Toward a theory of intrinsically motivating instruction," *Cognitive science*, vol. 5, no. 4, pp. 333–369, 1981.

[18] L. W. Anderson, D. R. Krathwohl, and B. S. Bloom, *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives*. Allyn & Bacon, 2001.

[19] D. Stein, "Situated learning in adult education. eric digest no. 195." 1998.