Information Security Awareness through a Virtual World: An end-user requirements analysis

Christos Mettouris[*], Vicky Maratou[**], Divna Vuckovic[***], George A. Papadopoulos[*], Michalis Xenos[**]
[*]University of Cyprus, Nicosia, Cyprus
[**]Hellenic Open University, Patra, Greece
[***]Center for the Promotion of Science, Belgrade, Serbia
mettour@cs.ucy.ac.cy, v.maratou@eap.gr, dvuckovic@cpn.rs, george@cs.ucy.ac.cy, xenos@eap.gr

Abstract—**Living in the digital era, computers and the Internet became important tools used by people to support significant parts of their everyday life such as work, education, socializing, entertainment, communication, etc. However, there are certain risks involved in using ICT technologies, and thus all ICT users should be aware of the basic principles of information security and data protection. No matter how much expertise is put into securing information assets and networks (e.g. firewalls, encryption) the human factor always remains a vulnerability. Our vision is to aid towards the development of information security awareness culture by using a 3D Virtual World Learning Environment that will simulate real-life security threat scenarios, examples and counterexamples in a way that different groups of users will experience the risks and combine critical skills, knowledge and collaboration to overcome them, without exposing their organization to real risk. In this paper we provide the results of the end user requirements collection and analysis in order to define and develop the specifications of the aforementioned 3D Virtual World Learning Environment and the specifications of the in-world activities.**

I. INTRODUCTION

The V-ALERT LLP EU project [1] aims to support the establishment of an Information Security culture in different ICT user target groups (pupils and teachers, ICT students, academics and enterprise employees) by providing awareness through an innovative and immersive e-learning tool. An online 3D Virtual World Learning Environment (VWLE) will be developed which will simulate real-life Information Security threat scenarios, allowing users to gain first-hand experience of the different risks and threats, though in a safe manner. The 3D VWLE of V-ALERT will also provide real time in-world assistance to the users through personalised recommendations. The underlying pedagogy of the V-ALERT approach is the "learning by doing" which can increase intrinsic motivation of learners and lead to deeper understanding and learning [2, 3].

The aim of this work is to present the results of the end user requirements collection and analysis which will be used to define and develop the specifications of the 3D VWLE and the specifications of the in-world activities for the V-ALERT project. The requirements collection from the end users was accomplished through an online questionnaire which end users from 5 different European countries had to complete. Following the requirements collection, an analysis of the acquired data was conducted, the outcomes of which are presented in this study.

Section 2 of this paper discusses related work. In section 3 we describe the questionnaire's aim and content, while in section 4 we discuss the results obtained. Section 5 closes the paper with conclusions, as well as a list of important user requirements based on which the 3D VWLE, its activities and the security threat scenarios will be designed and implemented.

II. RELATED WORK

Compared to other e-learning technologies, 3D virtual worlds can provide learners with a full understanding of a situation using immersive 3D experiences which allow the learner to freely wander through the learning environment, explore it, obtain sense of purpose, act, make mistakes, collaborate and communicate with other learners [4]. Indeed, immersion, that is the feeling of "actually being there", accompanied with the interaction with virtual objects can enhance learners' interest and engagement to the learning tasks and help them to develop a stronger conceptual understanding, depending on the content [5, 6]. Therefore, with the prospect of providing learners with experiences they would otherwise not be able to experience in the physical world (or in a classroom), a rapidly growing interest in 3D virtual world learning activities is observed by a large number of schools and universities worldwide [3, 7].

A number of research works aim at providing learners with experiential learning of different scientific topics through simulations or role-play games in 3D interactive virtual worlds [3, 4, 8, 9]. However, there are not many works focused on delivering Information Security issues [10, 11, 12] through 3D virtual worlds. To this direction, mostly 2D simulations and games have been developed [13].

In the context of V-ALERT, we attempt to fully exploit the possibilities of the 3D virtual world technology to create and evaluate experiential learning simulations which will address the users' real needs for Information Security awareness. To this aim, through an organised requirements collection procedure, we acquired direct feedback from more than 600 of different, in age and expertise, end users, from 5 European countries. The results of the data analysis have revealed interesting issues for educators and 3D VWLE developers who are

interested in designing educational and learning sessions on Information Security.

III. End User Requirements Collection Via Questionnaire

A. Aim of the Questionnaire

The end users requirements collection was accomplished through an online questionnaire. To the survey participated users from Cyprus, Greece, Serbia, Croatia and Bulgaria. We have categorized our end users in 4 different target groups as follows: (i) students of primary or secondary education, (ii) teachers or academic professors, (iii) ICT college or university students and (iv) enterprise staff or employees in an organisation or administrative personnel.

The questionnaire included specific questions that aimed to acquire important information regarding the user profiles, interests and activities from the perspective of Information Security. Besides basic information such as gender, age, country, etc., the aim was also to collect useful information regarding computer/smartphone usage and social network and online user activities, as well as to understand the aspects of information security that are more important to the users, based also on the particular target group of each user. In this manner, we aimed to discover the needs, preferences, habits and the level of security awareness of each target group regarding information security.

Furthermore, the questionnaire aimed to lead the process of defining the conceptual specification of the 3D VWLE. More particular, the information obtained from the end users will point to the right direction regarding the appropriate learning approach and learning activity (e.g. role-playing gaming theory, etc.) to be adopted for each target group and in relation also to the different user "roles", activities and pedagogical objectives.

In order to have a statistically correct analysis, we had aimed for 100 responses per target group. Partners sharing the same target groups were to guarantee a sum of 100 participants together.

B. Questionnaire Content

The questionnaire was launched on the official website of the V-ALERT project [1]. 5 project partners were responsible for the end users and had 2 weeks to make sure that their end users had completed the questionnaire on time. The questionnaire included 42 questions, from which 40 were multiple choice questions; the two exceptions include stating age and country in text boxes. 5 questions included text boxes for the user to provide input other than the multiple choice answers.

The first 6 questions aimed to collect user basic info. Following, questions 7 to 10 were about how often users use computers/smartphones and how confident they are while using them. Questions 11 to 19 got more into detail about online shopping, e-banking and similar activities users may perform daily. Questions 20 to 27 attempted to acquire user information about activities users perform in their routine that may involve risks, such as exchanging sensitive information via the internet with others, as well as how secure users perceive their activities to be. Questions 28 to 35 were more technical and concerned their level of knowledge and education on security awareness. The last section of the questionnaire (questions 36 to 41) included questions about users' experience regarding 3D virtual worlds and about how they perceive the involvement of 3D virtual worlds in simulating real-life security threat scenarios for educational purposes. Finally, the last question (No. 42) and probably the most important one in the questionnaire, explicitly asked users about the type(s) of security threats they would like to learn more about, by offering a list of the 13 most well-known threats to select from, as well as a text box to add more.

IV. Questionnaire Data Analysis & Results

Our analysis is based on studying the results of all end users as one large dataset, as well as analysing the results per target group in order to identify the particular characteristics of each group. In this section we discuss the most important results of our survey, providing the results in a percentage approximation.

For simplicity, in the following we will refer to: "Students of primary or secondary education" as students, "Teachers and academic professors" as teachers/profs, "ICT College and University students" as univ. students and "Enterprise staff, employees in organisations and administrative personnel" as employees.

A total of 666 responses were acquired. 361 responses - 54.2% were students, 49 responses - 7.4% were teachers (12) and academic professors (37), 194 responses - 29.1% were univ. students and 62 responses - 9.3% were employees.

A. Computer Usage and Confidence

The first few questions were about how often users use computer-smartphones and how confident they are while using them. Most of them use a computer (PC, laptop) for online activities on a daily basis, as well as a mobile device such as a smartphone. Only a very small students' minority never uses a computer for online activities, while for mobile devices the corresponding percentage includes users from all 4 target groups. 1 out of 5 teachers/profs do not use mobile devices for online activities.

More than 75% of the users are confident in using a computer for online activities, while for mobile devices the percentage drops to 70%. From a small percentage that are not confident at all with computers most are students and employees. Regarding mobile devices, 1 out of 20 users from each target group do not feel confident at all.

Regarding online shopping, more than 40% of users declare that they do not shop online, but this is mostly because most of our participants are students. Only 3 out of 10 students shop online; regarding the other target groups, the percentage is 80-98%. Almost all employees (98%) seem to shop online. Most online shoppers shop from home. However, there are a few of the online shoppers that have the risky habit of shopping from anywhere; these are mostly employees and univ. students. This may happen due to added confidence these two target groups may feel. One possibility is that employees and univ. students trust the networks and their security

software (e.g. antivirus) without a real deep knowledge as to what threats they could really be exposed to.

Regarding e-banking and m-banking, 1/3 of the adult participants manage an account. Most people have e-banking or both. Very few participants have only an m-banking account. This can lead to the conclusion that, while adult users shop online and manage e-banking accounts, they do not really trust mobile devices to manage also an m-banking account. Or, maybe m-banking is not needed, since most of them already have an e-banking account. Again, employees seem to be more risky since those that use m-banking from any location they believe is secure are more (almost twice) than the employees that use m-banking from home. Moreover, the confidence rate regarding e-banking is relatively low in all target groups. Many people have stated that they are not confident at all while performing online transactions through e-banking, except from employees: none of them has stated that they do not feel confident.

B. Routine Activities

The next part of the questionnaire acquired user information about activities users perform in their routine that may involve risks, such as exchanging sensitive information via the internet with others, as well as how secure users perceive their activities to be.

Despite that, by now, every person using computational devices (computers and smartphones) must have repeatedly heard to never disseminate personal sensitive information over the internet (email, social networks), unfortunately our users do so. A few of them even do this on a regular basis with strangers, while more than 15% do it sometimes. When being asked whether they exchange sensitive information via the internet with family or friends, the percentages rise: almost 1 out of 10 users do it regularly and 1 out of 2 do it sometimes. It is important to note that employees do it at a much lower percentage than the others.

Moreover, there are many users (almost 1 out of 5) that do not believe that shopping online may risk the exposure of sensitive data from their side, and a further 1 out of 5 that do not know. These users certainly need to be informed and educated on online information security matters. It is important to note that, while most users belonging in the latter set of users are students and univ. students, nevertheless, this set includes users from the other 2 target groups as well.

Another important result is that 1 out of 2 users believe that their home internet connection is very secure while using an Ethernet cable, and more or less the same statistic applies also for a Wi-Fi wireless connection. Of course, in reality this is not the case.

Finally, users in general do not think that using a public computer is very safe, while 1 out of 3 have stated that they do not know, mostly students. Also, 1 out of 4 participants have stated that they know very well how to protect and secure their electronic data from cyber threats when using a public Wi-Fi. 1 out of 5 do not know at all how to do that and half of them are somewhere in the middle: don't know exactly how to do it but are aware of some protective measures.

C. Technical Quiz

The following 8 questions in the questionnaire (Q28 - Q35) were more technical, aiming to determine the participants' level of knowledge and education on security awareness. The mean percentage of correct answers for all participants regarding the technical questions was 49%. Only one person responded correct to all questions. Moreover, 44.8% of the participants responded correct to at least one question (mean value). The success rate of two questions that had multiple correct answers was very low (15% and 5%), although the encouraging thing here is that a large number of participants have answered partially correct: for one question 1 out of 3 participants answered 50% correctly and for the other one almost half of them answered 66% correctly.

On the rest of the questions, the participants were correct at a rate of 65-86%, except from Q29 ("While browsing the Internet you receive a message informing you that you have become a victim of spyware and that you should click 'OK' in order to remove it. What do you do?") and Q35 ("What is phishing?"). It seems that Q29 tricked most participants and hence the low success rate, while Q35 is low mostly because of the unsuccessful participation of the students. It is interesting to observe that, although Q29 is a relatively easy question, most participants stated that they would "close the browser and scan for spyware" instead of just "ignoring the message" (correct answer). Although their response is incorrect, it would not risk their safety. Also, it is important to note that in this question students were more successful than the other target groups, perhaps due to the simple and straightforward way children are able to think as opposed to adults.

One may assume that students would have lower success rates than other target groups regarding the technical questions. Students have a higher rate regarding incorrect answers in Q31 ("To your opinion, which of the following are characteristics of a strong password?") and a lower success rate than the other target groups in Q34 ("What is a computer virus?") and Q35, but they also have a higher success rate than the other target groups in Q29.

D. User Experience

The last section of the questionnaire determined the users' experience regarding 3D virtual worlds and about how they perceive the involvement of 3D virtual worlds in simulating real-life security threat scenarios for educational purposes. These questions were set on a 5-level Likert scale, where the participants were asked to state their opinion on how much they agree to the question/statement by selecting one of the following: "Strongly agree", "Agree", "Neutral", "Disagree" and "Strongly disagree". The option "Don't know" was also included.

Half of the participants have stated that they have previous experience with computer games. As expected, students and univ. students have the highest rate in computer games experience. 1 out of 5 participants do not have previous experience with computer games. Also, more than 40% of all participants have previous experience in 3D virtual worlds through a computer (PC,

mobile device). Students, univ students and employees have the most, while teachers/profs seem to have the lowest. Almost half of teachers/profs do not have previous experience in 3D virtual worlds through a computer. In this research, the opinion of participants that have previous experience in 3D virtual worlds is important, since, through their experience, these users have become the most relevant people to respond to our questions.

In the question whether users believe that 3D virtual worlds could be effectively used for educational purposes by offering educational oriented experiences to the user, almost 27% of all participants strongly agree, while 34% agree (therefore, a total of 61% agree). Moreover, from the participants that have stated to have previous experience in 3D virtual worlds through a computer, 76% believe that 3D virtual worlds could be effectively used for educational purposes by offering educational oriented experiences to the user, and only 6% do not. Also, 50% of users who do not have previous experience in 3D virtual worlds through a computer believe that 3D virtual worlds could be effectively used for educational purposes by offering educational oriented experiences to the user, while 19% do not. Another interesting point is that very few participants strongly disagree with the statement (3.6%), and a further 6.5% disagrees. 33% of these users have stated to have previous experience with computer games and 25% have stated to have previous experience in 3D virtual worlds through a computer. 13% have both experiences.

Regarding the different target groups and whether they believe that 3D virtual worlds could be effectively used for educational purposes, students agree by more than 50% (and disagree by 13%), univ. students agree by 67% (and disagree by 8%), teachers/profs agree by more than 70% (and disagree by 4%) and employees agree by 79%. None of the employees disagrees in any way with the statement, and furthermore, none of the teachers/profs strongly disagrees with the statement.

The next question was whether the participants believe that 3D virtual worlds facilitate a 'learning by doing' educational model or not (Q39). 52% of all users agree to the statement and less than 10% do not. From the users that have previous experience in 3D virtual worlds through a computer, 67% believe that 3D virtual worlds facilitate a "learning by doing" educational model and only 7% do not agree. 45% of users who do not have previous experience in 3D virtual worlds through a computer believe that 3D virtual worlds facilitate a "learning by doing" educational model, 18% do not. Students agree to the statement by 38% (and disagree by 12%), univ. students agree by 66% (and disagree by 7%), teachers/profs agree by 64% (and disagree by 4%) and employees agree by more than 40%. None of the employees strongly agrees to the statement, as well as none of them disagrees in any way with the statement. Also, none of the teachers/profs strongly disagrees with the statement.

Question 40 explicitly asked the users whether they would like to participate in learning sessions facilitated through 3D virtual world simulations. More than half of the users (59%) agree, 17% were neutral, 13% disagree and 8% did not know. From the users that disagree, 28% have stated to have previous experience with computer games, 24% have stated to have previous experience in 3D virtual worlds through a computer and 9% stated to have both experiences. From the users that have previous experience in 3D virtual worlds through a computer, 78% would like to participate in learning sessions facilitated through 3D virtual world simulations and only 7% would not like to participate in such learning sessions. 46% of the users who do not have previous experience in 3D virtual worlds through a computer would like to participate in learning sessions facilitated through 3D virtual world simulations while 28% would not. In each one of the four target groups more than half of the participants would like to participate in learning sessions facilitated through 3D virtual world simulations. Almost 57% of students would like to participate (and 16% would not), 61% of univ. students would like to participate (and 11% would not), 50% of teachers/profs would like to participate (and 12% would not) and 69% of employees would like to participate (and 5% would not). Moreover, 27% of users who do not have previous experience in 3D virtual worlds through a computer and believe that 3D virtual worlds could be effectively used for educational purposes by offering educational oriented experiences to the user, also believe that 3D virtual worlds facilitate a "learning by doing" educational model and furthermore would like to participate in learning sessions facilitated through 3D virtual world simulations.

Regarding Q41: *"If you have any previous experience in 3D virtual worlds through a computer (PC, laptop, mobile device), for what purpose was your participation in 3D virtual worlds: 1. Educational, 2. Gaming, 3. Recreational Sports & Rehabilitation, 4. Scientific visualization and 5. Other"?* The responses of all participants show that 41.4% was Gaming and 19.1% was Educational (the other purposes were less than 10%). The purpose of participation in 3D virtual worlds of the users that have stated to have previous experience in 3D virtual worlds was 56% Gaming and 19% Educational (the other were less than 10%). Regarding the different target groups, students', univ. students' and employees' participation was mainly gaming, while teachers/profs' participation was mainly Educational, as well as Gaming.

The final question of the questionnaire and a very important one as well, is Q42: *"What type of security threats from the list below would you like to learn more about and gain knowledge in order to avoid them?"* This was a multiple choice question with 15 possible answers, 13 of which included a threat (see bars in Fig. 1 and Fig. 2 – the y-axis depict percentages): 1. Identity Theft, 2. Cyber bullying, 3. On-line Sexual Harassment, 4. Social Networking Misuse , 5. Cyber Scams, 6. Phishing/Spam, 7. Unauthorized exposure of personal information to online social networks, 8. Misuse of internet access exposing devices security, 9. Breach of Intellectual Property Rights, 10. Information leakage, 11. Social Engineering Attacks, 12. On line web security threats and 13. Unauthorized physical access to corporate facilities

The results were the following (Fig. 1): most of the participants (62%) have selected Identity Theft (bar 1 in Fig. 1) as the type of security threat they would like to learn more about. Therefore Identity Theft is the most

important security threat for the users. Second in the list of user preferences is Cyber Scams (bar 5 in Fig. 1) with 50% of users selecting it, while third is Phishing/Spam (bar 6) with a similar rate (49.8%). Note that the second and third selections are well below the first one by an important gap (12%). Then we have Unauthorized exposure of personal information to online social networks (43.7%, bar 7), Information leakage (44.6%, bar 10), Social Networking Misuse (43.5%, bar 4), On-line web security threats (42.9%, bar 12) and Social Engineering Attacks (41.3%, bar 11). The rest of the threats are below 40%: Cyber bullying (39.7%, bar 2), Misuse of internet access exposing devices security (37.5%, bar 8), On-line Sexual Harassment (33.8%, bar 3), Breach of Intellectual Property Rights (33.8%, bar 9) and Unauthorized physical access to corporate facilities (31.4%, bar 13). 9.2% of the participants did not know (bar 14) and 2.3% selected "None of the above" (bar 15).

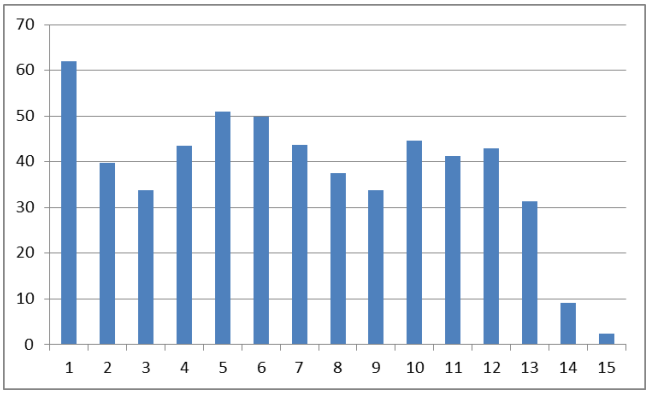

Figure 1. The responses of all participants

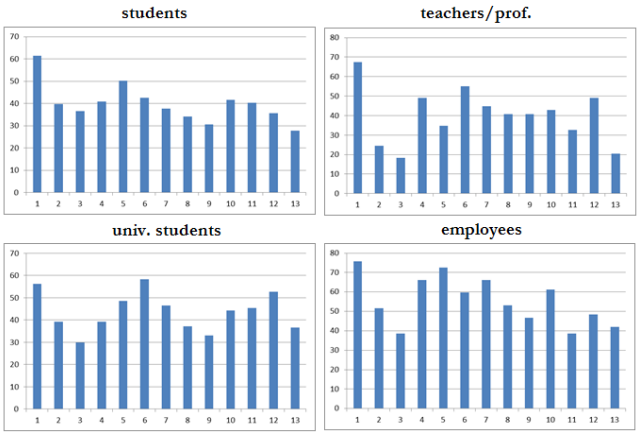

Figure 2. The responses of each target group

Quite similar to the above results are the results obtained when users with previous experience in 3D virtual worlds through a computer were asked to specify the type of security threats that they would like to learn more about: Identity Theft (66.7%) again tops the list, with Cyber Scams (50.5%) and Phishing/Spam (49.5%) following, as also above. The percentages are also quite similar.

The results obtained from each target group vary significantly. In Fig. 2 we present the selections of each target group. The top 3 for each target group are presented next. Students: Identity Theft, Cyber Scams, Phishing/Spam; univ. students: Phishing/Spam, Identity Theft, On line web security threats; teachers/profs: Identity Theft, Phishing/Spam, Social Networking Misuse; employees: Identity Theft, Cyber Scams, Social Networking Misuse. The aforementioned confirm that Identity Theft is very important for all target groups, as it is the first choice of 3 of the 4 target groups and the second choice of the remaining one. In addition, Phishing/Spam is very high in user preferences, while also Cyber Scams and Social Networking Misuse are quite popular.

V. CONCLUSIONS

Besides the specific types of security threats that users would like to learn more about, the most important result obtained from the questionnaire is the confirmation and validation of the following from all of our end user target groups: users believe that 3D virtual worlds could be effectively used for educational purposes by offering educational oriented experiences to the user, users believe that 3D virtual worlds facilitate a 'learning by doing' educational model and users would like to participate in learning sessions facilitated through 3D virtual world simulations.

Moreover, based on the questionnaire data analysis and obtained results presented in Section 4 of this paper, we close this work by describing the most important user requirements, based on which the 3D VWLE, its activities and the security threat scenarios will be implemented:

- Small minorities from all 4 target groups never use a mobile device for online activities. Hence, a security threat scenario that is only about mobile device usage should not be considered.

- 75% of the users are confident in using a computer or a mobile device for online activities. A security threat scenario should validate this information.

- 25% of students do not shop online. For students, security threat scenarios regarding online shopping could be omitted.

- A few of the online shoppers, mostly employees and univ. students shop from anywhere. Security threat scenarios regarding secure online shopping from public places should be implemented.

- Many adult users shop online and manage e-banking accounts but at the same time their confidence regarding e-banking is relatively low in all target groups. Also, very few participants have only an m-banking account, therefore users may not trust mobile devices to manage an m-banking account. E-banking and m-banking security educational scenarios can be developed to educate users on how to safely use them.

- Many users exchange personal and sensitive information over the internet with strangers and/or family members. Employees do it at a much lower percentage than the other 3 target groups. Security threat scenarios about exchanging sensitive information over the internet should be implemented - employees could be excluded from such scenarios.

- 40% of the users do not believe or do not know (mostly students and univ. students) that shopping online may risk the exposure of sensitive data from their side.

Appropriate security threat educational scenarios should be implemented that show how shopping online can be risky and how it can be done securely.

- About 50% of the users believe that their home internet connection is very secure while using an Ethernet cable or a Wi-Fi wireless connection (55% of students). Security threat scenarios regarding home internet security and potential risks should be considered.

- Users in general do not think that using a public computer is very safe but many students stated that they did not know. A security threat scenario regarding public computer usage should be considered, at least for students.

- 25% of the users have stated that they know very well how to protect and secure their electronic data from cyber threats when using a public Wi-Fi. Appropriate security threat scenarios that rate the users through their activities can determine whether this is valid. Also, 20% do not know at all how to do that and 50% don't know exactly how to do it but are aware of some protective measures.

- Security threat scenarios aiming to train users in more "technical issues" are mandatory. The mean percentage of correct answers for all users was only 49%, while only one person responded correct to all questions. Moreover, only 44.8% of the participants responded correct to at least one question (mean value).

- Regarding the technical questions, students have lower success than the other target groups in a few questions and a higher success rate only in one question. Technical oriented security threat scenarios specifically for students (small children) should be considered.

- Half of the users have stated that they have previous experience with computer games - as expected, students and univ. students have the highest rate. Gamification of security threat scenarios for students and univ. students is appropriate and desirable.

- 40% of users have previous experience in 3D virtual worlds through a computer (PC, laptop, mobile device). Students, univ students and employees have the most experience, teachers/profs have the lowest: 50% of teachers/profs do not have previous experience at all. This should be considered while designing 3D virtual world security threat scenarios for teachers/profs. An introductory video/scenario may be needed for this target group before interacting with the 3D virtual world within a real scenario.

- More than half of the users agree that 3D virtual worlds could be effectively used for educational purposes by offering educational oriented experiences to the user, that 3D virtual worlds facilitate a 'learning by doing' educational model and would like to participate in learning sessions facilitated through 3D virtual world simulations. 3D virtual world security threat scenarios for educational purposes should be developed, that will emphasize on a "learning by doing" educational model.

- Regarding the purpose of the users' participation in 3D virtual worlds, 41.4% was Gaming, 19.1% was Educational, etc. 3D virtual world security threat scenarios focused on gaming as well as education are well known to users and should be considered.

- The security threat scenarios to be implemented should include Identity Theft, Cyber Scams and Phishing/Spam. User preferences in the security threat scenarios vary little based on each user's target group.

VI. ACKNOWLEDGMENT

This work has been co-funded by the European Union under the Framework Lifelong Learning Programme / Key Activity 3 - ICT / Multilateral Project (European Commission, EACEA) for the project V-ALERT- "Virtual World for Awareness and Learning on Information Security". This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

VII. REFERENCES

[1] Virtual World for Awareness and Learning on Information Security (V-ALERT) Official Website, Online: http://v-alert.eu/, 2014.

[2] T. Lombardo, The pursuit of wisdom and the future of education. In *T. C. Mack (Ed.), Creating global strategies for humanity's future*. Bethesda, MD: World Future Society. 2006, 157–176.

[3] Daden Limited. Virtual Worlds for Education and Training. White Paper. 2010. Retrieved February 22, 2011 from http://www.daden.co.uk/media/white-papers.

[4] Daden Limited. Immersive Environments for Learning, Education and Training. White Paper. 2014. Retrieved January 30, 2014 from http://www.daden.co.uk/media/white-papers.

[5] J. Richter, L. Anderson-Inman, and M. Frisbee, Critical engagement of teachers in Second Life: Progress in the SaLamander Project. In *Proceedings of 2007 Second Life Education Workshop*. Chicago, USA, 2007.

[6] M. D. Dickey, Three-Dimensional Virtual Worlds and Distance Learning: Two Case Studies of Active Worlds as a Medium for Distance Education. British Journal of Educational Technology. 36(3), 2005, 439-451.

[7] S. de Freitas, Serious virtual worlds: A scoping study. Joint Information Systems Committee. 2008.

[8] V. Maratou, E. Chatzidaki, and M. Xenos, Enhance learning on software project management through a role-play game in a virtual world. Interactive Learning Environments. DOI: 10.1080/10494820.2014.937345, 2014.

[9] M. J. Callaghan, K. McCusker, J. Lopez Losada, J. G. Harkin, and S. Wilson, Engineering Education Island: Teaching Engineering in Virtual Worlds. ITALICS (Innovation in Teaching And Learning in Information and Computer Sciences), Vol. 8, Issue 3. 2009.

[10] J. Ryoo, A. Techatassanasoontorn, D. Lee, and J. Lothian, Game-based InfoSec Education using OpenSim. In *Proceedings of the 15th Colloquium for Information Systems Security Education Fairborn*, Ohio. 2011.

[11] J. Ryoo, A. Techatassanasoontorn, and D. Lee, Security Education using Second Life. IEEE Security & Privacy. Published by the IEEE Computer Society. (Eds.) Matt Bishop, Cynthia Irvine. 2009.

[12] B. Duffy, Network Defense Training through CyberOps Network Simulations. In *Proceedings of the Modeling, Simulation, and Gaming Student Capstone Conference*. Norfolk, Virginia. 2008.

[13] V. Pastor, P. Díaz, and M. Castro, State-of-the-art simulation systems for information security education, training and awareness. In *Proceedings of the IEEE Engineering Education 2010 – The Future of Global Learning in Engineering Education*. 2010.