Gamification to Empower Information Security Education

Alessandra Antonaci, Roland Klemke, Christian M. Stracke, Marcus Specht
Welten Institute, Open University of the Netherlands
Netherlands
alessandra.antonaci@ou.nl, roland.klemke@ou.nl, christian.stracke@ou.nl, marcus.specht@ou.nl

Mario Spatafora
Università degli Studi di Roma3
Italy
mario.spatafora@uniroma3.it

Kamelia Stefanova
University of Sophia
Bulgaria
kamelia@fmi.uni-sofia.bg

Abstract: 47% of the world population uses the internet daily, and access is growing also in less developed countries (LDCs). As a consequence, a total of almost 1 billion households in the world have internet access, of which 48 million belong from LDCs (ITU, 2016). A large proportion of internet users are teenagers, who often are not aware of all the risks related to sharing private information through the Internet using for instance social networks. This paper summarizes how much time students pass online, in what activities they prefer to be involved, which risks they are confronted with, and what can be done to reduce them. The solution we propose is an investment on the teacher level, recognized here as a key figure to be trained to become I (information) Secure Agent via an online course. The course will follow a gamified approach for empowering information security education. Our assumption is that gamification will have positive effects on participants' engagement and goal achievement.

Keywords: Gamification, Information Security, Teacher Training, Online Learning

1. Background

1.1 Internet Usage by Students-Teenagers

Based on OECD's (Organization for the Economic Cooperation and Development) report in 2012, 15-year-olds have at least five years of experience using computers (OECD, 2015). In countries like Norway, Sweden, Finland, Denmark and Israel the majority of the students starts to use the computer at about the same age they start to learn writing and reading, this means at the age of 6 years or even earlier (OECD, 2015).

"On average across OECD countries, 57% of students had accessed the Internet for the first time when they were younger than 10 (at that age, 76% of students were already using computers). In Denmark and the Netherlands, more than 30% of students had accessed the Internet for the first time before they turned 7" (OECD, 2015, p. 39).

In the PISA (programme for international student assessment) study, performed in 2012, OECD highlight that students, on average, report spending over two hours online each day on school days as well as during weekends (OECD, 2015), with students in some countries (Norway, Russian Federation, Estonia, Sweden, Australia, Denmark) even reporting over 4 hours of online activity on average (OECD, 2015).

1.2 Online Teenagers Are Busy With…

The type of activities in which students are engaged during their time online has been mapped by OECD in two PISA studies, in 2009 and 2012, with several changes being recorded. Students report that the majority of time spent in browsing is for leisure purposes, to spend time in social networks, or for downloading films or their favorite music (see figure 1 for more detailed information).

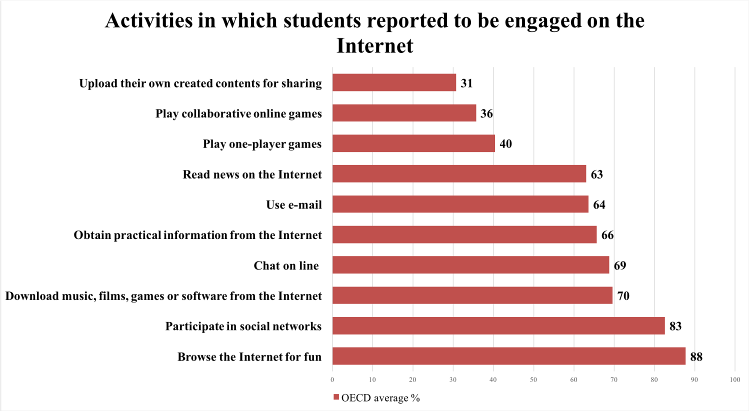


Figure 1. OECD (2015) data on the activities declared to be done online by students interviewed.

1.3 Risks for Students Online

Which risks can students, mainly teenagers and children, encounter during their online activities? In figure 2 are represented the main risks to which children are exposed while using the Internet. There are several risks, mainly connected to the access and acquisition of their personal information. Young students feel the need to socialize and they do it by using all means possible, in particularly sharing information via online social networks. Paradoxically, they are not aware of the dangers of sharing personal data online, which makes them especially vulnerable to the risks of the World Wide Web (OECD, 2012).

The risks that a student can encounter online can be roughly divided into four macro categories: (1) content; (2) contact; (3) children targeted as consumer; (4) information related to privacy and (5) security data.

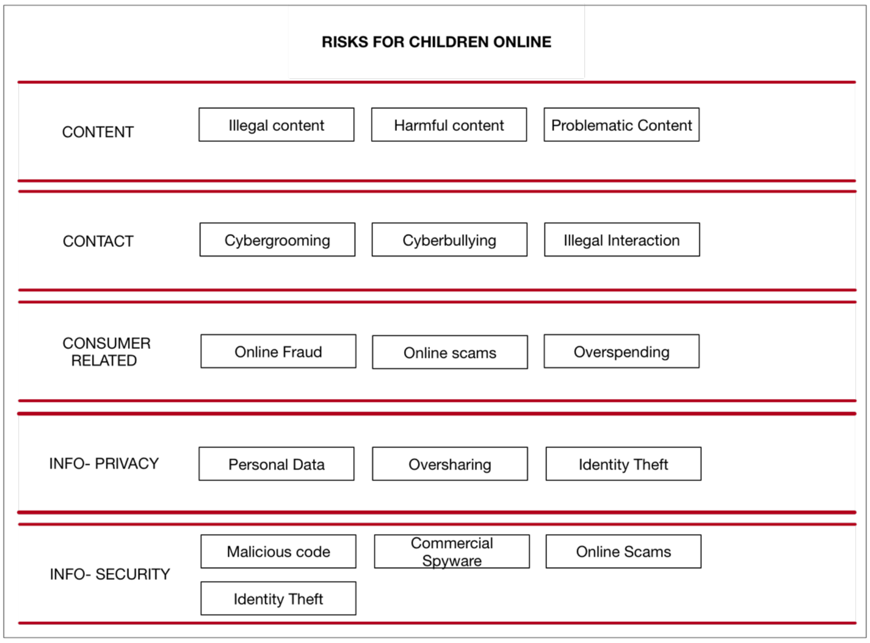
The content risk for students can occur in the following forms: *illegal content* (depending on country legislation) that generally refers to discriminative and/or sexual exploitive content; *inappropriate* for the age of the audience; *harmful advice* that can persuade a person to commit suicide, consume drugs and alcohol, develop eating disorders, such as anorexia, and problematic content that are files, generally images and or videos created by users to be shared with their peers with the initial purpose of fun, but their nature can create problems if they are captured by the wrong person (i.e., the "happy slapping" phenomenon).

The risks online also stem from the contacts whom students interact with, and "they can be further distinguished according to whether: i) the interaction takes place with the intention to harm the child; ii) children are exposed to hateful online interactions; or iii) the child inflicts harm to himself or herself by his or her conduct (e.g. liability due to illegal file sharing)" (OECD, 2012, p. 29). The first type of interaction is known as *cyber-grooming*; the second *cyberbullying* and the third *illegal interaction*. The difference between the first two is that, generally, in cyber-grooming, an adult interacts with a minor with the intent of bringing the online interaction into reality by playing on the sense of trust that the child has developed for that adult, with the intent of proceeding with illegal acts. Cyberbullying, on the other hand, is generally committed by a peer who uses information and technology to ridicule ("bully") and harm another person. Cyberbullying can also be committed by a group of people. A common definition of cyberbullying is the following: "an aggressive, intentional act or behavior that is carried out by a group or an individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself" (Moreno, 2014).

Risks more fraudulent in financial nature relate to transactions that can occur when students are approached online as consumers, in the form of online scams, fraud and overspending, if they have online access to means of payment.

The act of sharing information online implies risks for privacy, people can use personal data and even commit identity theft. Unfortunately, the risks cannot be contained only in the act of sharing, also receiving or downloading uncertain data can generate security problems such as: commercial spyware (a software that spies your internet browsing activities) or malicious code.

As mentioned at the beginning of this paragraph, children from one side put themselves at high risk of becoming a victim of online dangers, by frequently socializing with their friends and sharing their private information online, but, paradoxically, they are not aware of the potentially hazardous consequences of their online behavior. “Children may presume, incorrectly, that all information they submit remains within the boundaries of their immediate contacts, and they may fail to anticipate the possible adverse consequences of providing information to 'friends of friends'”(OECD, 2012, p. 36).



RISKS FOR CHILDREN ONLINE

CONTENT	Illegal content	Harmful content	Problematic Content
CONTACT	Cybergrooming	Cyberbullying	Illegal Interaction
CONSUMER RELATED	Online Fraud	Online scams	Overspending
INFO- PRIVACY	Personal Data	Oversharing	Identity Theft
INFO- SECURITY	Malicious code Identity Theft	Commercial Spyware	Online Scams

Figure 2. Synthesis of main risks that children can encounter online.

2. How to Contain These Risks and Support Students?

To find a possible answer in the framework of I SECURE - Empowering education systems in information security project (http://www.isecure-edu.eu/index.php/en/), a needs analysis was performed and teacher was identified as a key stakeholder for investment. A teacher can reach and support both students and their parents, and can be trained to transfer knowledge and strategies on how to reduce online risks.

The study sample consisted of 108 parents, 93 students and 89 school staff members (head masters and teachers) from four countries (see figure 3). The needs related to information security education of these target groups were investigated by means of a survey questionnaire.

By analyzing the data, we were able to determine the areas of possible intervention and define the learning objectives for a teachers’ training curriculum. Via further analysis through interviews of the school staff (19 people involved from the four countries) and focus groups involving not only school staff but also students and parents (36 people in total) we were able to investigate more deeply their needs. This led us to conclusion towards focusing our attention on teachers, recognized as the key persons on which to invest with our course.

Furthermore, from the survey data it was highlighted that the majority of the school staff members that were interviewed (73%; 65 participants out of 89) never attended a training on ICT security (see figure 4). In addition, we asked those who declared to have attended a course, to provide information on the course provider. Half of them (12 of 24), declared that the attended course was organized by their schools; the rest undertook a self-regulated learning path by looking for information on e.g., the internet or books and only one person declared to have attended private training courses organized by an external organization.

Consequently, despite the fact that some of the schools in the consortium organized training courses for their staff on ICT security, the majority of school staff has not attended them. To make the course more attractive and motivating for teachers, we aim to follow a gamified approach for the course. It will be designed and delivered in an online environment with the purpose to train our I-Secure (short for "information security") Agents.

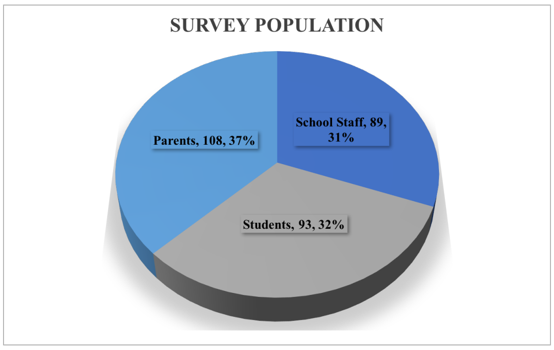


Figure 3. Survey population.

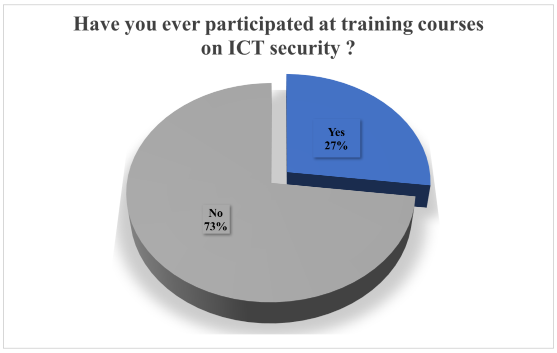


Figure 4. Investigation via surveys of the percentage of school staff who ever attended an ICT security course.

2.1 Why Gamification?

Gamification is the application of game elements in a non-game scenario to solve a problem or induce a change in the behavior of the target population (Deterding, Dixon, Khaled, & Nacke, 2011). This approach has been selected in our project because of gamification’s potential in education (Dicheva & Dichev, 2015), and for its suitability to our target audience, adults, and the topic we are aiming to deliver: information security education.

Gamification effectiveness has been studied by several authors and from these studies it has been suggested that the gamified approach can generate several effects, for instance, on users’ performance (Hakulinen, Auvinen, & Korhonen, 2015), (Bernik, Bubaš, & Radoševi, 2015), (De-Marcos, Garcia-Lopez, & Garcia-Cabot, 2016), (Hamari, 2013), (Hamari & Koivisto, 2015); motivation (Gooch, Vasalou, & Benton, 2016), (Utomo & Santoso, 2015), (Hamari, Koivisto, & Sarsa, 2014); engagement and enjoyment (De-Marcos, Domínguez, Saenz-De-Navarrete, & Pagés, 2014), (Huang & Hew, 2015), (Mazarakis, 2015).

Designing gamification is not a trivial task as it is more than just application of game elements in a non-game scenario: the mere implementation of those elements does not guarantee a result. The choice of game elements and their design needs to be related to the problem to be solved and the targeted population. In our case, teachers compose the target with a basic knowledge on information security that will be trained to cover the role of an Agent to secure their students for the online risks they can encounter.

The training will be developed in three modules: I - Protection against incorrect and aggressive behavior in social networks and personal information; II - Elements of Security Systems: firewall, anti-viruses, contactless devices; III - Intellectual Property Rights for Digital Content and ethical behavior in the legal context. Each module will be delivered with five lessons. The game elements that will be used are: scores, leaderboard, progress bar, badges, competition, collaboration, feedback and stimulated planning.

Each of these elements has been selected following a certain ratio, e.g., we want to test whether using leaderboard will positively impact on user performance by stimulating social comparison (Wu, Kankanhalli, & Huang, 2015). Studies (such as, Hamari, 2013) show that also badges can activate social comparison among users and positively influence performance.. However, in our platform we would like to use badges as "clear goals" to be achieved and as reward mechanism.
Stimulated planning is a game element described in Björk and Holopainen (2005) collection of game design patterns (GDPs) that will allow users to plan their actions and pursuit their goals (and that is mostly used in strategy games) (Björk & Holopainen, 2005). By using this game element, we aim to test whether we can positively impact users' goal achievement by stimulating them to effectively define and plan their actions. That effect could be expected following the Implementation Intention theory (Gollwitzer, 1999), (Gollwitzer & Sheeran, 2006). By using this game element, we aim to let users decide what to do during the course and help them plan how to achieve their goals.

Figure 5 shows the structure of the online course in more detail. We designed two separate course paths: a short and long version of the course. The short version presents the learner with an introduction based on the summary of the full course content that will be further detailed in the lessons. Based on this short version course, the participant can make a decision to proceed in the full course and plan it with awareness, or to continue immediately with the conclusion of the course. However, we expect that almost all users will opt for the long version of the course because it has been designed in accordance with their needs. They are free to plan which module to follow first, when and how. The success of the course will be evaluated in terms of users' learning performance (mean test scores) and users' goal achievement (completion in relation to individual intention plan).

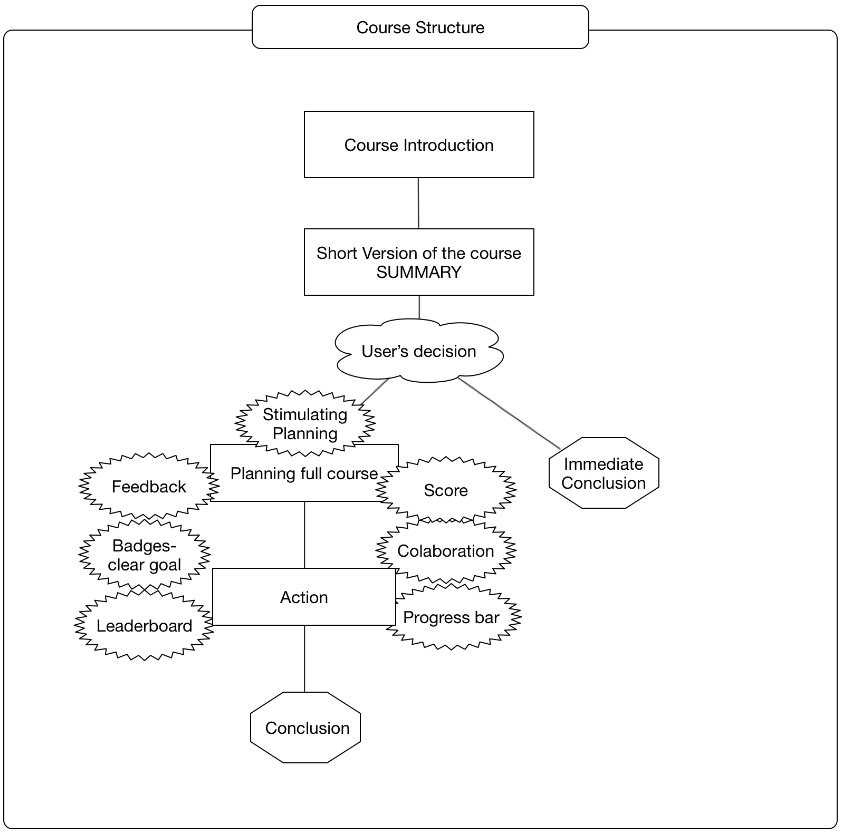


Figure 5. Gamified Online Course for Teachers.

2.2 Game Elements Selection

The selection criteria we used to identify the 21 game elements were: (1) the frequent use of a GDP in literature, (2) the applicability of a GDP in a multi-user environment, and (3) our hypothesized impact of the selected pattern on learners' engagement, goal achievement, and also on learning performance.

The tools used to validate these were questionnaire and focus group, involving 42 experts belonging from the following different fields: game design, technology enhanced learning (TEL) and learning science to validate them.

Game designers, learning scientist and TEL experts were involved because, due to the different backgrounds, they could evaluate the suitability of our selection form different perspectives: game design, didactic and TEL fit. The data of this study are being analyzed and will be presented in our future work.

3. Conclusions and Future Work

By referring to international reports from ITU and OECD, we have summarized an overview of the type and frequency of online activities that students engage in, as well as the potential risks involved.

In the framework of I Secure project, a needs analysis has been conducted among students, their parents, and school staff members with the purpose of collecting the needs of our target groups related to information security education, and designing a curriculum based on these.

The qualitative data analysis suggested that teachers are recognized as key persons: a mediator between student and parents, and point of reference for both. Furthermore, it has been underlined that despite the fact that the courses on information security were provided by the schools, the majority of school staff members did not attend them. As a consequence, to empower information security education and enhance teachers' engagement and goal achievement, a gamified online course will be designed to train the I-Secure Agent.

Our future work is aimed at (1) analyzing and presenting the data related to the GDPs validation from the experts (2) setting up a pilot course to test our assumptions and (3) in the next future scaling up the course and testing the game elements' effects on MOOC (Massive Online Open Course) users' behavior.

Acknowledgments

This study is partly founded by the I SECURE - Empowering education systems in information security project (n. 2015-1-IT02-KA201-015005) under the Erasmus + programme of the European Commission (http://www.isecure-edu.eu/index.php/en/).

References

Bernik, A., Bubaš, G., & Radoševi, D. (2015). A Pilot Study of the Influence of Gamification on the Effectiveness of an e-Learning Course. In Central European Conference on Information and Intelligent Systems (pp. 73–79). Varazdin: Faculty of Organization and Informatics Varazdin.

Björk, S., & Holopainen, J. (2005). Patterns in Game Design. ISBN1584503548 (Vol. 54). http://doi.org/10.1.1.10.4097

De-Marcos, L., Domínguez, A., Saenz-De-Navarrete, J., & Pagés, C. (2014). An empirical study comparing gamification and social networking on e-learning. Computers and Education, 75, 82–91. http://doi.org/10.1016/j.compedu.2014.01.012

De-Marcos, L., Garcia-Lopez, E., & Garcia-Cabot, A. (2016). On the effectiveness of game-like and social approaches in learning: Comparing educational gaming, gamification & social networking. Computers and Education, 95, 99–113. http://doi.org/10.1016/j.compedu.2015.12.008

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From Game Design Elements to Gamefulness: Defining "Gamification." Proceedings of the 2011 Annual Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '11, 2425. http://doi.org/10.1145/1979742.1979575

Dicheva, D., & Dichev, C. (2015). Gamification in Education: Where Are We in 2015? In E-Learn 2015 - Kona, Hawaii, United States (pp. 1445–1454).

Gollwitzer, P. M. (1999). Implementation intentions. American Psychologist, 54(7), 493–503.

Gollwitzer, P. M., & Sheeran, P. (2006). Implementation intentions and goal achievement: A meta‐analysis of effects and processes. Advances in Experimental Social Psychology, 38, 69‐119. http://doi.org/10.1016/S0065-2601(06)38002-1

Gooch, D., Vasalou, A., & Benton, L. (2016). Exploring the use of a gamification platform to support students with dyslexia. IISA 2015 - 6th International Conference on Information, Intelligence, Systems and Applications. http://doi.org/10.1109/IISA.2015.7388001

Hakulinen, L., Auvinen, T., & Korhonen, A. (2015). The effect of achievement badges on students' behavior: An empirical study in a university- level computer science course. International Journal of Emerging Technologies in Learning, 10(1), 18–30. http://doi.org/10.3991/ijet.v10i1.4221

Hamari, J. (2013). Transforming homo economicus into homo ludens: A field experiment on gamification in a utilitarian peer-to-peer trading service. Electronic Commerce Research and Applications, 12(4), 236–245. http://doi.org/10.1016/j.elerap.2013.01.004

Hamari, J., & Koivisto, J. (2015). Why do people use gamification services? International Journal of Information Management, 35(4), 419–431. http://doi.org/10.1016/j.ijinfomgt.2015.04.006

Hamari, J., Koivisto, J., & Sarsa, H. (2014). Does gamification work? - A literature review of empirical studies on gamification. Proceedings of the Annual Hawaii International Conference on System Sciences, 3025–3034. http://doi.org/10.1109/HICSS.2014.377

Huang, B., & Hew, K. F. (2015). Do points, badges and leaderboard increase learning and activity: A quasi-experiment on the effects of gamification. In Proceedings of the 23rd International Conference on Computers in Education (pp. 275–280). China: Asia Pacific: Society for Computer in Education.

ITU. (2016). ICT Facts and Figures 2016.

Mazarakis, A. (2015). Using Gamification for Technology Enhanced Learning : The Case of Feedback Mechanisms. Bulletin of the IEEE Technical Committee on Learning Technology, 17(4), 6–9.

Moreno, M. A. (2014). Cyberbullying. JAMA Pediatrics, 168(5), 500. http://doi.org/10.1001/jamapediatrics.2013.3343

OECD. (2012). The protection of children online. Raccomandation of the OECD Council. Report on risks faced by children online and polices to protect them. OECD Publishing.

OECD. (2015). Students, Computers and Learning: Making the Connection. OECD Publishing. PISA. Retrieved from http://dx.doi.org/10.1787/9789264239555-en

Utomo, A. Y., & Santoso, H. B. (2015). Development of gamification-enriched pedagogical agent for e-Learning system based on community of inquiry. Proceedings of the International HCI and UX Conference in Indonesia on - CHIuXiD '15, 1–9. http://doi.org/10.1145/2742032.2742033

Wu, Y., Kankanhalli, A., & Huang, K. (2015). Gamification in Fitness Apps: How Do Leaderboards Influence Exercise? In Icis (pp. 1–12). AIS Electronic Library (AISeL). Retrieved from http://aisel.aisnet.org/icis2015/proceedings/IShealth/14