SikkerhetsLøypa - Knowledge Toward Sustainable and Secure Paths of Creative and Critical Digital Skills

Letizia Jaccheri, Deepti Mishra, Siv Hilde Houmb, Aida Omerovic, Sofia Papavlasopoulou

SikkerhetsLøypa - Knowledge toward Sustainable and Secure Paths of Creative and Critical Digital Skills

Letizia Jaccheri[1]✉, Deepti Mishra[2]✉, Siv Hilde Houmb[3,4], Aida Omerovic[5] and Sofia Papavlasopoulou[1]

[1]Department of Computer Science,
Norwegian University of Science and Technology (NTNU), Trondheim, Norway
letizia.jaccheri@ntnu.no,spapav@ntnu.no
[2]Department of Computer Science,
Norwegian University of Science and Technology (NTNU), Gjøvik, Norway
deepti.mishra@ntnu.no
[3]Department of Information Security and Communication Technology,
Norwegian University of Science and Technology (NTNU), Gjøvik, Norway
siv.houmb@ntnu.no
[4]Secure-NOK AS, Stavanger, Norway
sivhoumb@securenok.com
[5]SINTEF Digital, Oslo, Norway
Aida.Omerovic@sintef.no

Abstract. Children spend numerous hours on the Internet daily. While online, they meet a great number of opportunities as well as risks. Of these risks, cyber bullying and privacy violations are of major concern, in addition to exploitation and child pornography. Our hypothesis is that the solution is not to keep children and teens away from the Internet, but to ensure that young citizens are empowered with the necessary knowledge and skill set to become critical consumers and creators of new secure and sustainable digital services and products. Our objective is to develop a knowledge and skill set base and offer learning through playful solutions for empowering children and young people with creative and critical digital skills, in an engaging and motivating way. The aim is to build on the method and lessons learns of Kodeløypa, one of the scientific offerings for children at the Norwegian University of Science and Technology (NTNU), and the related scientific efforts made to empower a new generation of online users to avoid risks in the modern digital society. The project, SikkerhetsLøypa, is highly inter-disciplinary and spans across the fields of information security, user experience, software engineering, and computer science education. The scientific results of this project aims at strengthen education methods and practices in secure and privacy-aware behavior in the digital world.

Keywords: Digital Society · Online Behavior · Video Games · Security · Gender.

1 Introduction

The digital literacy level of children and young adults has increased significantly in recent years. Unfortunately, their digital safety and privacy skills have not kept up with the digital literacy level. The wider use of the Internet to seek information, share ideas, consume entertainment and network using social media brings great opportunities, as well as larger risks to young users. Despite a growing body of rules and regulations implemented to enhance safe online behaviour, more efforts in this direction are still needed. Children require support to be aware of the potential risks and threats of Internet use for their online security. Staksrud and Livingstone [1] define online risks as a set of intended or unintended experiences that increase the likelihood of harm to the Internet user, and include encountering pornographic, racist or hateful content online, as well as inappropriate or potentially harmful contact via harassment and bullying. Online risks to children generally comprise a set of wanted or unwanted inappropriate activities by children (as actors, receivers, or participants) that are of concern [2]. Child pornography is addressed by the Cybersecurity SRA [3] as one of their list of serious cybercrimes and malware. Everyone, child or adult, has the right to the protection of their personal data, but many young people normalise the sharing of intimate details on social media without understanding the risks, and possibly with an overestimation of their governments ability to protect them from online risks

Parents can play an important role in providing a safe Internet environment for their children. However, it is not easy for parents to engage effectively in an instructive mediation of their child's Internet use, and co-viewing is much less likely when it comes to Internet compared with other audio-visual mediums such as television. Therefore, proper training and teaching is crucial for imparting online security-related life skills. This is further supported by Reid and Van Niekerk [4], who assert that cyber security education is becoming a necessary precaution for individuals to protect themselves against the dangers of online technologies and resources. It has also been observed that learning activities that employ gamification [5] generally lead to better learning outcomes. However, gaming brings the gender challenge to the table, which needs to be considered when using gaming as a learning platform for online security-related life skills. Although women remain under-represented in cultural representations of gamers, in the design considerations of game producers, and in the production companies themselves, the percentage of girls and women playing and creating video games is continuing to increase. Female gamers tend to play as much as male gamers or longer online, per session and per week than males [6]. As women have become more present online and in the Internet economy, this brings challenges such as becoming the prey of cybercrime and bullying, arguably at a higher level of risk or different manner of risks than for men.

The paper describes work in progress. Initially a series of workshops were conducted in the framework of Koderløypa (see section 3) with the aim to explore using gamification as a learning platform. With the above-mentioned motivations and the results of these workshops, the present study describes an ongoing project, SikkerhetsLøypa, with the aim to create new knowledge, methods, and tools that will lead to new services and products by gamifying education on online opportunities and risks with innovative gaming technologies for young online users.

The paper is organized as follows: Section 2 describes the challenges and concerns regarding digital safety and security of young users, along with gender issues in gaming. Section 3 provides a walk-through of the Kodeløpa workshop and method. The proposal to develop knowledge and offer playful solutions for empowering children and young people with creative and critical digital skills is discussed in Section 4. Section 5 provides discussion and conclusions.

2 Literature Review

A European study of 21 countries stated 75% of children are using the Internet [7]. Another study finds that more than 65% of Facebook and Myspace users are children [8]. This increasing Internet usage among children brings both opportunities and risks for those children [7]. This means that the more opportunities children gain online, the more likely they are to encounter increased risk [9].

2.1 Online Safety and Security Issues

A research network founded by the European Commission's Safer Internet Programme, known then as 'EU Kids Online' and now as 'Better Internet for Kids', developed a classification [10] of online risks comprising:
Content risks where the child is a recipient of unwelcome or inappropriate mass communication;
Contact risks where the child participates in risky peer or personal communication;
Conduct risks where the child themselves contributes to risky content or contact.
Lorenz *et al*. [11] identified that the challenges or concerns regarding digital safety and security are related to reputation (self-inflicted damage, outside damage), data (data loss, data exposure), fraud (dishonesty, money loss), health (physical and mental health factors), and freedom. Some major security risks in relation to online behaviour of children are as follows:
Children are trusting. The number of children believing everything they read on the Internet is significantly increased, according to an Ofcom study which has found that 'digital natives' are too trusting of what they find online [12].
Online grooming. Online grooming is another major problem in online communities where groomers often pretend to be children in order to become friends and establish a relationship with their young victims [13].
Unwanted exposure to sexual material. Children are more likely to experience unwanted exposure to pornography [2]. Furthermore, boys experienced more exposure to the risks compared to girls [2].
Unwanted exposure to violent content. Children are exposed to potential harmful risks such as seeing bloody movies or photos, seeing people being beaten up, and seeing hate messages [2].
Contact risks. This includes contacting someone online whom the child never met face-to-face, meeting someone face-to-face whom the child knows only online, meeting someone whom the child knows only online and being harassed [2].
Sharing personal details. Children may share and reveal personal data because they do not realize the possible consequences [14]. Minors are more likely than adults to give

out personal information in order to receive an award [15]. Eight out of 10 adolescents who use social networks share personal information about themselves to a much greater extent compared to previous years [14], revealing sensitive information about their family and friends as well as themselves [16].

Online bullying/being bullied. According to Ktoridou *et al*. [17], one in three children have experienced Internet bullying. 38% of girls and 26% boys have faced online bullying [17].

Internet addiction. Overuse and addiction to the Internet among children has been examined by many researchers [18,19,20]. Several studies [18,21,22] have also investigated online gaming addiction among school-going adolescents.

Digital safety areas are scattered across every element defined in the above list, for example: understanding internet safety trends; choosing secure devices to surf online; recognize potential insecure behaviours or threats; knowing how to act when something bad happens or how to seek help when needed; perceiving and judging the dangers of your own and others' online behaviour; knowledge about account privacy and maintenance; helping students to learn how to interact online positively and with consideration for others [11].

There are also major differences in online behavior depending on the age of children and young people. Each of these demonstrable differences in experience of the Internet and online gaming, and it is critical to take this into consideration when developing tools and techniques to improve online security skills for children.

2.2 Gender Issues in Gaming

Gender issues in technology and specifically in computer games have been a research topic for many years. Twenty years have passed since Cassel and Jenkins wrote the groundbreaking "From Barbie to Mortal Kombat" that highlighted the ways gender stereotyping and related social and economic issues characterize digital game play. Kafai *et al*. [23] have recently edited a collection of contributions around the still-relevant question about women and gaming. Video games are an important part of the life of adolescents. According to Gorriz and Medina [24], boys reported playing an average of nearly 43 h per week, or over 6 h per day, and girls reported playing nearly 30 h per week, or over 4 h per day. According to Fron *et al*. [25], 88.5% of all game development workers are male; 83.3% are white; 92% are heterosexual.

Bryce and Rutter [26] have argued that 'the popularity of domestic and online gaming among females, and the development of female gaming clans, highlights that leisure activities and spaces are becoming less gendered, and can provide sites for resistance to societal notions of the gender appropriateness of leisure activities. In the years since that study was published, female video game players have long since ceased to be a negligible minority. Women are also actively creating video games- not only as employees of computer game production companies but in a few notable cases as the owners of those companies as well. Women-owned computer game companies include HerInteractive, Girl Games, Girltech, Purple Moon (developed by Brenda Laurel, who had established Purple Moon games with the explicit goal of designing products which reflected sociological and ethnographic research into young girls' play patterns). Gorriz

and Medina [24] provides an excellent classification of games for girls from Barbie Fashion Designer to tools for boosting self-esteem such as Let's Talk About Me.

The gender aspect of Internet and online situational awareness is important, and is related to questions around users' age and maturity. It is important to understand these gender differences and to develop a training program that is both tailored to the gendered experience of learning (women learn differently than men) and the differences in the cyber situations that girls and boys (or women and men) could be exposed to.

3 Kodeløypa Workshop

Building upon several documented efforts [27, 28], we designed a one-day workshop program for 15-years old students in secondary schools in Trondheim, Norway. Students attended this five-hour workshop as part of their school day [29]. We adopted the constructionist approach as one of its main principles is learning by making. This approach was chosen because of the observation that young people of that age tend to rebel against concrete advice, and learn better through engaging with educational content in a creative and self-directed way. We have chosen to use Scratch (a digital learning environment) due to its ease of use for young students and its connection to the principles of constructionism. For a hardware platform, we selected Arduino due to its well-established and smooth integration with Scratch. We also used Scratch for Arduino (S4A), an extension of Scratch that provides extra modules for robot control.

Fig. 1. Kodeløypa workshop

Five teaching assistants facilitated the workshops and designed the process together with a researcher and an artist. In general, children who attended the workshop worked

collaboratively in triads. Digital artifacts (robots) were placed next to each of the computers, and the students had the option to select the robot they wanted (figure 1).

The workshop was organized in the following two main sections.

3.1 Playing (and Learning) with Robots

At the beginning of the workshop, one assistant welcomed the students and presented the scope of the workshop to the students. Then, the assistant demonstrated the robots and advised students to keep their attention on the tutorial placed next to each of the computers. The tutorial contained instructions with examples and pictures similar to the robots they were using. Students were asked to investigate the robots and find the exact place of their sensors and lights, write the location of the LED lights and sensors while answering some questions. Examples were deliberately sparse of text and image-rich, with images demonstrating exactly what the students were asked to do. As students had no experience with programming we wanted a smooth start that would increase their motivation to engage, so they were first asked to do a series of simple tasks making the robot react to the environment through visual effects (for example, cause a light to switch on when there was less light on the sensors). The robots were built from recycled computer parts/materials. Students could touch and play with the robots but not change any parts of them, since those robots have been constructed to support computational thinking (CT) concepts (i.e. sequences, loops, parallelism, events, conditionals, operators, variables, and lists).

During this phase, students made simple loops that could control the robots. Through this activity, students understood the metaphors and interactions between the physical design elements and the Scratch environment. The first section lasted one and a half hours.

3.2 Create Games with Scratch

In the second part of the workshop, we wanted students to be creative and implement simple game development concepts using Scratch. The students were given another tutorial with the basic CT concepts, with images arranged in an order to help them with the development of their own game. This part lasted three hours and did not use the robots.

Students were able to create their own game structure and stories by designing and programming. It is very important that students had a plan for what kind of game they want to create. Therefore, they were asked to draft a storyboard first. In order to stimulate creativity, examples of different loops and existing game characters were given to students to be used as elements of the game. Examples and visualizations of the process helped students to ideate their own original project. Help was provided anytime students asked for it and the number of assistants was enough to provide sufficient help to all teams. More complex programming concepts were introduced on an individual level when the students asked for them and those concepts were relevant to their projects. Throughout the whole process, students were iteratively testing and trying to debug their games, and they worked collaboratively according to their own pace. At the

end, each of the students' teams created a Scratch game based on their own preferences and ideas. Students' games were not presented formally, but all teams had the chance to play each other's games.

3.3 Participants

Seven KodeLøypa workshops took place during Autumn 2015, and students from four different schools participated. In total, 128 students attended, consisting of 60 male and 68 female students. All workshops followed the same structure as outlined above and each of the workshops had between 18 and 22 participants [29].

3.4 Data Collection and Measurements

A range of data was collected across the seven workshops, including surveys, photographs and observations. For the purpose of this study we focused on the quantitative data. To collect the quantitative data, we conducted a post-workshop survey based on questions adopted from similar studies in the literature. Students responded to the survey at the end of the workshop day. In summary, we collected 105 responses (53.3% males and 46.7% females). Each attitude (construct) consisted of three to four questions (items) and was measured using a seven-point Likert scale.

3.5 Lessons Learned

There were several lessons learned from the KodeLøypa workshop that form the basis for the planned SikkerhetsLøypa workshop series. In particular, the results showed that age and maturity heavily influence the learning capability. However, age and maturity level does not necessary align, which is an essential lessons learns when planning SikkerhetsLøypa workshops. For example, while 14-16 year old's have an equal need for the same level and types of online security awareness and skills, their readiness to receive and understand the workshop's training modules varied significantly based on their age and inconsistently age-linked maturity levels. The workshop could ideally be tailored to match the learning styles and maturity of each student, but the wide variability and rapid pace of change in teenagers' development makes it difficult to make useful assumptions about their learning preferences and abilities ahead of meeting the individual learners themselves.

4 Towards an Intersectional Understanding of Online Security, Gender, Creative Careers and Learning Styles

This project SikkerhetsLøypa lies at the intersection between a) the gamification of digital empowerment of children and young people and b) user-centered and adaptive training in cyber security risks and online opportunities.

4.1 Objective of the Project

The objective of the SikkerhetsLøypa project is to: create new knowledge, methods and techniques that will lead to products and services of gamified education about online opportunities and risks. This will enhance the level and competitiveness of the Norwegian education system and at the same time open up market opportunities for Norwegian publishing, gaming and e-learning industries, both nationally- and internationally-facing. The targeted end users of these products and services are children at the level of the Norwegian middle school (Ungdomskole).

The gamification of security training for youth is cross-disciplinary and the main research challenge is in the intersection between cyber security, user experience and learning science. The challenge is two-fold: (1) Identify and dynamically update the most recent knowledge on online opportunities and cyber security risks, including documented guidance on how to deal with them; and (2) Design and empirically validate the SikkerhetsLøypa products and services so that, as well as efficiently conveying the abovementioned up-to-date knowledge, they are attractive, highly motivating and entertaining to the users, so that kids actually want to use them and the teachers and policy makers want to adopt them.

4.2 Research Questions

We aim to investigate the following research questions with the aim to offer playful solutions for empowering children and young people with creative and critical digital skills, in an engaging and motivating way:

How could we develop a security knowledge tale into a video game?

How could we evaluate the video game?

The second question can be separated into two sub-questions: How do we evaluate the game after production? And how do we evaluate the game during the design and production phase to create a game that better achieves the creators' goals? The literature review will identify papers that can most usefully serve as guidance for choosing an evaluation model and methodology. Papers of relevance include examinations of evaluation methods previously applied to education-oriented video games, as well as suggestions for future evaluations of both the learning outcomes and the quality of engagement with video games among diverse audiences. It is very likely that findings related to how best to evaluate the video game will inform the methods for developing (designing and producing) the game.

The proposed work will contribute to the knowledge, methods and tools needed for: (1) acquisition of the cyber security knowledge that needs to be communicated to the user groups, (2) storytelling around the knowledge to be communicated, (3) dynamic content update of the SikkerhetsLøypa products and services with most recent knowledge and corresponding stories, and (4) adaptive learning which customizes the SikkerhetsLøypa products and services to the level and learning pace of the user.

4.3 Main Activities, Objectives and Deliverables

The main activities, objectives and deliverables of SikkerhetsLøypa are as follows:
Knowledge management regarding online opportunities and risks: Develop an approach to the acquisition of knowledge of online opportunities and risks, as well as ways of dealing with online resources associated with both.
Serious game design and user experience: Develop an approach to interactive and motivating storytelling. Develop method and metrics for evaluation of usability. Develop an approach to updating the design of serious games with new content.
Pedagogical solutions for game-based learning: Develop an approach to knowledge transfer through storytelling as well as guidance for when and how to leverage the different learning means and mechanisms. Develop method and metrics for evaluation of learning effects. Develop a method for adaptive learning.
Empirical evaluation in pilot environments: Identify requirements for SikkerhetsLøypa products and services. Evaluate the feasibility of SikkerhetsLøypa early products and services for education about online opportunities and risks. Evaluate the effect of SikkerhetsLøypa products and services on user experience and learning. Conduct an overall evaluation of the final version of the SikkerhetsLøypa products and services.
Dissemination and internationalization. Open seminars, participation in social media, scholarly articles. The pilot at NTNU and in schools will generate attention in the media. We mention that Kodeløypa has been broadcasted at NRK News and other National media channels. Kodeløypa is one of the main case studies in Horizon 2020 Umi-Sci-Ed [30], and SikkerhetsLøypa will utilize existing relationships with the international partners and previous event/activity partners of Kodeløypa.

5 Conclusions

The rapid increase over recent years in the digital literacy level of children has not been equaled by a parallel increase in online situational awareness or digital security skills. This paper has provided a brief summary of statistics outlining increasing use of the Internet by young people, including girls. This paper has also explored in brief the awareness in the literature that the Internet ecosystem, and video games especially, are increasingly inhabited by girls and women, and that although women remain underrepresented in depictions of and opportunities in the gaming industry, the percentage of girls and women playing and creating video games is continuing to increase. In summary, exposure to the Internet provides a wealth of opportunities to young people, and therefore, rather than preventing exposure to the commensurate risks and dangers by favoring restriction of access, it would be more beneficial to encourage young people to become aware of those risks and dangers, and to equip them with tools to improve their own digital safety.

A one-day workshop for school-age Norwegian children (age 15) was developed, taking a constructionist approach that used gamification to motivate students to learn about programming by playing with robots and designing their own simple video games. These “Kodeløypa” workshops were delivered to 128 students in total, with representative participation by different genders, and employed Scratch software as

well as Arduino hardware. Quantitative feedback was effectively gathered from the majority of participants and can be used to improve workshop structure and learning outcomes of similar workshops in future. The Kodeløypa workshop model developed by our team is summarized here to provide evidence of the efficacy of this model of innovative learning, and to propose that a new workshop, called SikkerhetsLøypa, be developed based on the experiences and lessons learns from the Kodeløypa's workshops. The aim of the SikkerhetsLøypa workshop is to deal specifically with issues around online safety awareness and skills. The objective of the SikkerhetsLøypa project is to create new knowledge, methods and techniques that will lead to products and services of gamified education about online opportunities and risks.

To that end, we found that a number of building block studies will need to be developed in order to deliver a workshop that addresses the intersecting needs of school-age students of different genders, ages, maturities and learning styles. These studies, which will take the form of literature reviews, original research and iterative workshops, will deliver a new knowledge base that can be used to guide pedagogy, service creation and product development around teaching internet safety to young people.

References

1. Staksrud, E., Livingstone, S.: Children and online risk. Information, Communication & Society, 12(3), 364–387, 2009. doi:10.1080/13691180802635455.
2. Teimouri, M., Hassan, M.S., Griffiths, M., Benrazavi, S. R., Bolong, J., Daud, A., Adzharuddin, N. A.: "Assessing the Validity of Western Measurement of Online Risks to Children in an Asian Context," *Child Indic. Res.*, 2015.
3. Cybersecurity Strategic Research Agenda – SRA, Produced by the European Network and Information Security (NIS) Platform http://www.kowi.de/Portaldata/2/Resources/horizon2020/coop/cybersecurity-SRA-final-v0_96-ENISA.pdf
4. Reid, R., Van Niekerk, J.: Back to Basics: Information Security Education for the Youth via Gameplay. In: Dodge R.C., Futcher L. (eds) Information Assurance and Security Education and Training. WISE 2009. IFIP Advances in Information and Communication Technology, vol 406. 2013, Springer, Berlin, Heidelberg
5. Stanescu, I. A., Stefan, A., Hauge, J. M. B: Using Gamification Mechanisms and Digital Games in Structured and Unstructured Learning Contexts. In: Wallner, G., et al. (eds.). International Conference on Entertainment Computing ICEC 2016, LNCS 9926, pp. 3-14. Springer, Heidelberg (2016)
6. Hussain, Z., Griffiths, M. D., Baguley, T., Hussain, Z., Griffiths, M. D., Baguley, T.: "Online gaming addiction : Classification, prediction and associated risk factors Online gaming addiction : Classification , prediction and associated," *Inf. Healthc.*, vol. 6359, no. September, 2012.
7. Livingstone, S., Haddon, L.: *Comparing children's online* opportunities and risks across Europe. 2009.
8. Lenhart, A.: "Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging," *Specialist*, vol. 4, p. 2010, 2009.
9. Livingstone, S., Mascheroni, G., Ólafsson, K.: "Children's online risks and opportunities: Comparative findings from EU Kids Online and Net Children Go Mobile Executive summary," 2014.

10. Hasebrink, U., Görzig, A., Haddon, L., Kalmus, V., Livingstone, S.: Patterns of risk and safety online. London: LSD, EU Kids Online network, 2011.
11. Lorenz, B., Kikkas, K., Laanpere, M., Laugasson, E.: A Model to Evaluate Digital Safety Concerns in School Environment. In: Zaphiris P., Ioannou A. (eds) Learning and Collaboration Technologies. LCT 2016. Lecture Notes in Computer Science, vol 9753. (2016).
12. Ofcom, "Children Believe Everything they Read Online," 2015.
13. Ashcroft, M., Kaati, L., Meyer. M.: A Step Towards Detecting Online Grooming -- Identifying Adults Pretending to be Children. In *Proceedings of the 2015 European Intelligence and Security Informatics Conference (EISIC)* (EISIC '15). IEEE Computer Society, Washington, DC, USA, 98-104.
14. Tsirtsis, A., Tsapatsoulis, N., Stamatelatos, M., Papadamou, K., Sirivianos, M.: "Cyber security risks for minors: A taxonomy and a software architecture," *2016 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP)*, Thessaloniki, 2016, pp. 93-99.
15. Implementing the Childrens Online Privacy Protection Act: A Report to Congress, online at: http://www.ftc.gov/reports/coppa/07COPPA Report to Congress.pdf, FTC, Feb 2007.
16. Marwick, A., Murgia-Diaz, D., Palfrey, J.: "Youth, privacy and reputations," Berkman Center Research, Tech. Rep. 2010-5, 2010. [Online]. Available: http://papers.ssrn.com/sol3/papers.cfm?abstract id=1588163
17. Ktoridou, D., Eteokleous, N., Zahariadou, A.: "Exploring parents' and children's awareness on internet threats in relation to internet safety," *Campus-Wide Inf. Syst.*, vol. 29, no. 3, pp. 133–143, 2012.
18. Gentile, D.A., Choo, H., Liau, A., Sim, T., Li, D., Fung, D., Khoo, A.: Pathological video game use amongst youths: A two-year longitudinal study. Pediatrics, 127, 319–329, (2011).
19. Huang, X., Zhang, H., Li, M., Wang, J., Zhang, Y., Tao, R.: Mental health, personality, and parental rearing styles of adolescents with internet addiction disorder. Cyber Psychology Behavior and Social Networking, 13(4), 401–406, (2010).
20. Kwisook, C., Hyunsook, S., Myunghee, P., Jinkyu, H., Kitai, K., Byungkoo, L., Hyesun, G.: Internet overuse and excessive daytime sleepiness in adolescents. Psychiatry and Clinical Neurosciences, 63(4), 455–462, (2009).
21. Lemmens, J.S., Valkenburg, P.M., Peter, J.: Development and validation of a game addiction scale for adolescents. Media Psychology, 12, 77–95, (2009).
22. Van Rooij, A.J., Schoenmakers, T.M., Vermulst, A.A., Van Den Eijnden, R.J.J.M., Van De Mheen, D.: Online video game addiction: Identification of addicted adolescent gamers. Addiction, 106, 205–212, (2011).
23. Kafai, Y. B., Richard, G. T., Brendesha, M.: Editors: Diversifying Barbie and Mortal Kombat, Intersectional Perspectives and Inclusive Designs in Gaming , ETC Press (2016).
24. Gorriz, C.M., Medina, C.: Engaging Girls with Computers through Software Games, Commun. ACM, 43(1), 42-49, 2000.
25. Fron, J., Fullerton, T., Morie, J., Pearce, C.: "The hegemony of play". In Situated Play: Proceedings of the Digital Games Research Association Conference, Edited by: Baba, A. 309–318. Tokyo, 24–28 September 2007.
26. Bryce, J. O., Rutter, J.: Gender Dynamics and the Social and Spatial Organization of Computer Gaming. Leisure studies, 22(1), 1-15, 2003. Routledge, London.
27. Giannakos, M. N., Jaccheri, L., Leftheriotis, I.: "Happy girls engaging with technology: assessing emotions and engagement related to programming activities." International Conference on Learning and Collaboration Technologies. Springer International Publishing, 2014.

28. Giannakos, M. N., Jaccheri, L.: "What motivates children to become creators of digital enriched artifacts?" Proceedings of the 9th ACM Conference on Creativity & Cognition. ACM, 2013.
29. Papavlasopoulou, S., Giannakos, M.N., Jaccheri, L.: Creative Programming Experiences for Teenagers: Attitudes, Performance and Gender Differences. In Proceedings of the The 15th International Conference on Interaction Design and Children (IDC '16). ACM, New York, NY, USA, 565-570.
30. Exploiting Ubiquitous Computing, Mobile Computing and the Internet of Things to promote Science Education, available at http://umi-sci-ed.eu/