European Crime Prevention Award (ECPA)

Annex I – new version 2014

Please complete the template in English in compliance with the ECPA criteria contained in the RoP (Par.2 §3).

General information

1. Please specify your country.

Estonia

2. Is this your country's ECPA entry or an additional project?

ECPA entry

3. What is the title of the project?

Digital Safety Game (DSG)

4. Who is responsible for the project? Contact details.

Aare Klooster, aare.klooster@gmail.com Edmund Laugasson, edmund.laugasson@gmail.com Birgy Lorenz, birgy.lorenz@gmail.com

5. Start date of the project (dd/mm/yyyy)? Is the project still running (Yes/No)? If not, please provide the end date of the project.

01/03/2013-20/06/2015

6. Where can we find more information about the project? Please provide links to the project's website or online reports or publications (preferably in English).

http://dsg.onu.ee

7. Please give a **one page** description of the project (**Max. 600 words)**

Digital Safety Game

Tallinn University Digital Safety Lab created Digital Safety Game (DSG). This card game is in English and targets university; professional higher, vocational and high school ICT students and teachers of informatics.

There was a need for a methodical material, which helps teachers to teach a variety of computer-related topics. DSG tackles learning layer to raise citizens' awareness of online crime prevention. Students and teachers will learn about a variety of topics in the field of information security, facts. Game gives students the opportunity to communicate and debate on social engineering, privacy, network, internet, hacking, and malware topics.

The idea of the game is to learn more about digital safety. The goal is to answer as many questions as possible and win after accumulating a required number of cards. The game is designed so the inquirer has to formulate a question and evaluate whether the answer is correct or not. Discussions and real life examples why this knowledge is important are encouraged. Game is designed for people who want to renew or enhance their digital safety knowledge with the help of a fun seductive game.

To play the game (54 cards, 6 topics): after shuffling the deck, each player draws one card. Each time player runs out of cards, she/he draws another one. Cards pile is at the center of table and after choosing player to start, game proceeds clockwise. At his/her turn, the player (inquirer) chooses and asks a question on the card from the next player (respondent). The inquirer evaluates whether the answer is correct or incorrect. In case of CORRECT answer the respondent keeps the card and places it in front of him/her, face up and in case of INCORRECT answer the inquirer keeps the card. Player who first collects 3 cards from one category (same color) shouts out "I'm Safe!" and wins the game!

Usually there could be 1-6 players and game duration would be around 20...25 minutes.

I. The project shall focus on prevention and/or reduction of everyday crime and fear of crime within the theme.

1. How does the project contribute to crime prevention and/or to the reduction of crime or the fear of crime? (**Max. 150 words**)

Digital Safety Game (DSG) gives students knowledge to prevent cyber crimes through learning about security issues by playing. Learning through playing is an important factor here.
As the game covers aspects about social engineering, privacy, network, internet, hacking and malware, divided into 54 questions with answers - it covers wide range of information society where cyber crimes usually happens.

Participating in information society concerns all target groups and therefore the game is suitable to all who are part of it.

2. How is the project contributing to raising citizens' awareness of crime prevention? (**Max. 150 words**)

Security experts feel digital security has three layers - learning, policies and hardware. DSG tackles the first learning layer to raise citizens' awareness of cyber crime prevention.

There are different types of cyber crimes: fraud, identity theft, sensitive data stealing. Using DSG will increase awareness how to prevent these cyber crimes. This will be achieved by keeping computer clean of malware, understanding when somebody tries to use social engineering and other cyber attacks to steal sensitive data, identity.

DSG is created by Tallinn University, Digital Safety Lab and Network of Estonian Teachers of Informatics and Computer Science (www.eiops.edu.ee) to help schoolteachers teach digital security topics. Discussions and real life examples among students why this knowledge is important, are encouraged.

There were around 10 000 students involved for research and testing - schools and youth centers are mentioned in section II.1.

II. The project shall have been evaluated and have achieved most or all of its objectives.[1]

1. What was the reason for setting up the project? What problem(s) did it aim to tackle?

After research it became clear DSG kind of security information bundle cannot be found from internet. For most topics there were dozens of different vague definitions or descriptions. We tried to gather them all, select the most important parts and squeeze them on a card the most simple way possible.

DSG can be taught in university, professional higher, vocational and high school

[1] For more information on evaluation, see Guidelines on the evaluation of crime prevention initiatives (EUCPN Toolbox No.3): http://www.eucpn.org/library/results.asp?category=32&pubdate

education programs with focus to ICT.

DSG is used for teaching purposes at Tallinn University, Tallinn School of Economics, Pelgulinna Gümnaasium.

The game has been sent to the following Estonian schools and youth centers:

- Vinni-Pajusti Gümnaasium
- Elva Gümnaasium
- Mäetaguse Põhikool
- Viljandi Kutseõppekeskus
- Kuusalu Keskkool
- Tallinna Ehituskool
- Märjamaa Gümnaasium
- Ristiku Põhikool
- Vastseliina Gümnaasium
- Tallinna Täiskasvanute Gümnaasium
- Audentese Erakool
- Elva Avatud Noortekeskus
- Harkujärve Põhikool
- Jakob Westholmi Gümnaasium

Research methods are described in written articles:

- Lorenz, Birgy;Banister, Savilla Irene;Kikkas, Kaido (2015). Impacting the Digital Divide on a Global Scale - Six Case Studies from Three Continents. In: Learning and Collaboration Technologies, Volume 9192 of the Lecture Notes in Computer Science series: The HCI International 2015, Los Angeles, CA, USA. (Toim.) Panayiotis Zaphiris; Andri Ioannou. Springer, (Lecture Notes in Computer Science; 9192).
- Lorenz, Birgy; Klooster, Aare (2013). Teacher-Student Online Relationship. In: 10th IFIP World Conference on Computers in Education: 10th IFIP World Conference on Computers in Education, 1-7. july 2013, Torun, Poland. (Toim.) N. Reynolds, M. Webb, M, Syslo, V. Dagiene. Torun, Poland:.
- Lorenz, Birgy;Sousa, Sonia; Tomberg, Vladimir (2013). Õpilaste teadlikkus e-ohutusest ja selle mõjust osalusele e-õppes . In: Open and Social Technologies for Networked Learning: IFIP WG 3.4 International Conference, OST 2012, Tallinn, Estonia, July 30 - August 3, 2012. (Toim.) Tobias Ley, Mikko Ruohonen, Mart Laanpere, Arthur Tatnall. Heidelberg [etc.]:, (FIP Advances in Information and Communication Technology,), 189 - 192.
- Lorenz, Birgy; Kikkas, Kaido; Klooster, Aare (2013). "The Four Most-Used Passwords Are Love, Sex, Secret, and God": Password Security and Training in Different User Groups. In: Human Aspects of Information Security, Privacy, and Trust: First International Conference, HAS 2013 Held as Part of HCI International 2013 Las Vegas, NV, USA, July 21-26,

2013. (Toim.) Louis Marinos and Ioannis Askoxylakis. Springer, (Lecture Notes in Computer Science; 8030), 276 - 283 .

- Lorenz, Birgy; Kikkas, Kaido; Laanpere, Mart (2013). Exploring the Impact of School Culture on School's Internet Safety Policy Development. In: HCI International 2013 – Posters' Extended Abstracts: International Conference, HCI International 2013 Las Vegas, NV, USA, July 21-26, 2013. (Toim.) Constantine Stephanidis. Springer, (Communications in Computer and Information Science,; 374), 57 - 60.
- Lorenz, Birgy; Kikkas, Kaido (2012). Lessons Learned from the Safer Internet Program in Estonia. eLearning Papers, 28, 1 - 10.
- Lorenz, Birgy; Kikkas, Kaido; Laanpere, Mart (2012). Comparing Children□s E?safety Strategies with Guidelines Offered by Adults. The Electronic Journal of e-Learning, 10(3), 326 - 338.
- Lorenz, Birgy; Kikkas, Kaido (2012). Socially engineered commoners as cyber warriors - Estonian future or present? In: 4th International Conference on Cyber Conflict: CYCON 2012: International Conference on Cyber Conflict, 5.-8. juuni, Tallinn. (Toim.) C. Czosseck, R. Ottis, K. Ziolkowski. Tallinn: IEEE, (IEEE), 221 - 234.
- Lorenz, Birgy; Kikkas, Kaido; Laanpere, Mart (2011). Bottom-Up Development of E-Safety Policy for Estonian Schools. 5th International Conference on Theory and Practice of Electronic Governance (ICEGOV2011), 26.-28.September 2011, Tallinn, Estonia. (Toim.) Estevez, E., Janssen, M.. ICEGOV '11, September 26 - 28 2011, Tallinn, Estonia: ACM, (ACM International Conference Proceedings Series), 309 - 312.
- Lorenz, Birgy (2011). E-turvalood ja lahendused paljastavad ebakõla õpilaste ja õpetajate arusaamades. In: DVD of the conference: Children's Identity, Culture and Media in Visegrad Context, Plzen 15-16 september. .
- Lorenz, Birgy (2011). Interneti turvalisuse projekt Pelgulinna Gümnaasiumis . Isehindamine (57 - 60). Tallinn: Eesti Haridusministeerium

Also there is the game shared on the mentioned conferences abroad.

2. Was the context analysed **before** the project was initiated? How, and by whom? Which data were used? (**Max. 150 words**)

The context was analysed by Digital Safety Lab with purpose to develop study and research and learning direction of digital safety at Tallinn University, Institute of Informatics. Research has been made during 2011-2015 as described in section II.1 by 6 researchers (2 scientists and 4 doctoral students). There were these 14 schools and youth centers involved as mentioned in section II.1. There were around 10 000 students involved into testing group in different schools.

The purpose of research group is to investigate digital safety area and use accomplished competence in both academic and business projects. The lab is

managed by Kaido Kikkas, PhD and Andro Kull, PhD and is still active.

Research group has been compiled of PhD students with following research areas:

Birgy Lorenz: Internet safety for teenage user

Aare Klooster: Prevention of Social Engineering in Corporate Cyber Defense Strategy

Edmund Laugasson: Free software strategies of managing information and communication technology infrastructure in Estonia

Kätlin Kalde: Security Policies and Standards in the Supply Process of Information Technology for Educational Facilities

3. What were the objective(s) of the project? Please, if applicable, distinguish between main and secondary objectives. (**Max. 150 words**)

The game meets the substantive part of the national curriculums' security section for schools. National curriculum in Estonia - https://www.hm.ee/en/national-curricula - there is appendix 10 "Informatics". This subject involves different aspects of security in personal level but also in computers and online: how to avoid threats to health, security and personal data; how to stay safe online (including: how to choose secure password, understand different security levels). All these aspects are covered also with DSG. There are sections 1.2 and 1.32 at II and III school levels at basic school curriculum of informatics, which are covered by DSG. There are also elements included from optional courses of "Mechatronics and robotics", "Computer usage at research", "Basics of programming and apps creation".

Also if to compare with international computer science curricula (http://www.acm.org/education/CS2013-final-report.pdf) then similar aspects are required (especially Assurance and Security but also Computer Systems Security part).

To use the DSG game is easy and there can be organized lessons with different topics as the game has social engineering, privacy, network, internet, hacking, and malware topics groups.

Secondary objectives are changes in teaching methods, which will help to introduce schools with modern techniques and methods. We also want to make security and technology more interesting and popularize it among students.

4. Did you build in internal goals to measure the performance of the project? If so, please describe at what stage of the project and how you measured

whether the project was moving in the planned direction. (**Max. 150 words**)

We share educative card game amongst schools, universities and youth centers. If the game is successful additional packages and changes in the content can be made.

Feedback has been always positive: IT-specialists and also regular users are playing the game and giving positive feedback. Also Estonian Information System Authority is using the game to educate their people and they even translated it into Estonian.

As described in section II.1 the gane has been shared to ICT-teachers, schools, education technologists, Estonian Information Technology Foundation for Education, International Cyber Defence Summerschool 2015, international conferences and so one.

The download statistics from DSG homepage is around 200 times by 17 highschools, 1 university, 2 vocational schools, NATO Cyber Defence Center, Microsoft, etc.

5. Has there been a process evaluation? Who conducted the evaluation (internally or externally?) and what where the main results? (**max. 300 words) -** *for more information on process evaluation, see EUCPN Toolbox No.3, p.9-10 & part 2 - section 2A*

There has been research made as described in section II.1 and after that there has been Digital Safety Lab group created with 4 students and 2 scientists. There has been participated also at NETICS (Network of Estonian Teachers of Informatics and Computer Science - around 600 ICT-teachers in community) cyber safety conference and after that we got an idea to create the Digital Safety Game (DSG) as a card game as there were lack of cyber safety information in a easy and understandable way among students. Then we wrote a project and got funding from Tiger University education project. During the DSG creation we deeply discussed several issues and finally after around two year development the game was ready.

The game was tested among community - ICT-teachers and their students. There were several iterations of DSG: we made first prototype digitally, then tested it among users, got feedback, fixed and made next prototype and tested again until feedback did not give any issues. Then we produced the game onto paper as playing cards.

6. Has there been an outcome or impact evaluation? Who conducted the evaluation (internally or externally?), which data and evaluation method where used and what were the main results? (**Max. 300 words**) - *for more information on outcome or impact evaluation, see EUCPN Toolbox No.3, p.7-9 & part 2 - section 2A*

There has been influence especially for ICT-teacher and their students: there has been learned different aspects of social engineering, privacy, network, internet, hacking, and malware topics. Evaluation has been conducted by our research team as we shared the DSG and could evaluate its impact among users. We asked feedback from users orally or by e-mail and got mainly positive feedback. There were also some criticism about the game was in English only and some proposals to add some questions. As the game size is limited then obviously we have to make tough choice, what questions to include.

III. The project shall, as far as possible, be innovative, involving new methods or new approaches.

1. How is the project innovative in its methods and/or approaches? (**Max. 150 words**)

Digital Safety Game gives students ability to learn about security issues by playing. Meaning learning can be fun!

According to the internet search nothing similar has not been done so far. Actually the term "digital security" has been created in Estonia and from our Digital Safety Lab in Tallinn University. Before that there were mostly used terms "internet security" or "computer security". There is interesting to mention that also choices of topics and description of terms are combined from different areas (social engineering, privacy, network, internet, hacking, malware) to reach most realistic, clear and instructive results.

IV. The project shall be based on cooperation between partners, where possible.

1. Which partners or stakeholders were involved in the project and what was their involvement? (**Max. 200 words**)

Tallinn University, Digital Safety Lab was mainly taking care of DSG overall creation process.
Network of Estonian Teachers of Informatics and Computer Science

NETICS (Network of Estonian Teachers of Informatics and Computer Science - around 600 ICT-teachers in community) were mainly involved as testing community with their students.

In addition also CERT Estonia was involved (CERT - Cyber Emergency Response Team) into discussion, which topics and terms needs to be covered

and how the questions needs to be formulated.

One of our research team member (Aare) had also previous experience creating similar card games (e.g. http://magic.ee/games/maade_kaardid/)

V. The project shall be capable of replication in other Member States.

1. How and by whom is the project funded? (**Max. 150 words**)

Tiger University Programme

The aim of the Tiger University programme is to support the development of highly qualified academic staff and modern infrastructure at Estonia's higher education institutions.

All those programmes contribute to educating tomorrow's university graduates so they are highly qualified and valued specialists on the Estonian and international labour markets.

http://www.hitsa.ee/it-education/educational-programmes

Project was submitted in December 2013 and was ready in June 2015.

2. What were the costs of the project in terms of finances, material and human resources? (**Max. 150 words**)

The overal project cost was 5980 € and 2000 copies printing cost were 3700 € of that. One pack cost 2,99 €.

As there were so many iterations then game got ready around a year later than preliminary expected. Almost whole game was revamped during improvements. There were around 300 working hours spent during development process.

3. Has a cost-benefit analysis been carried out? If so, describe the analysis, including how and by whom it was carried out and list the main findings of the analysis. (**Max. 150 words**)

As there are press-ready PDF-files in worldwide usable English language freely available on the web (http://dsg.onu.ee/) then the game creation cost 5980 € was actually relatively small amount if to compare with opportunity that whole world can actually download, print and use the game for free of charge. This idea has been born during the game website creation process and has been done for now.

4. Are there adjustments to be made to the project to ensure a successful replication in another Member State?

No need for adjustments can be used "as is". By default the game is in English.

Actually it is expected that cards back side remains intact with creators logo.

The game has been translated also into Estonian language by Triin Nigul from Estonian Ministry of the Environment and is also freely available for download. There is possible also ask spreadsheet files for further translation into other languages if there would be anyone interested.

5. How is the project relevant for other Member States? Please explain the European dimension of your project.

Digital Safety Game can be distributed, played and taught everywhere the same as in Estonia. The game is in English especially because it is the computing teaching language all over the world. Research group has been compiled from everyday working ICT-teachers and scientists and our experts group are aware of security issues what users have every day. The DSG has been designed so that these security issues have been covered in the game.

Also as the game has been created using also http://www.acm.org/education/CS2013-final-report.pdf requirements (especially Assurance and Security but also Computer Systems Security part) then it would be suitable also other Member States.

Whole Europe can access the website http://dsg.onu.ee/ and download the game. The website is suitable also for mobile devices.

Please provide a short general description of the project (abstract for inclusion in the conference booklet – **max. 150 words**).

Digital Safety Game

Game is designed for people who want to renew or enhance their digital safety knowledge with the help of a fun seductive game.

This game is for 1-6 people you can as individual or in teams. Recommended target audience is 16 years and up. Best suitable for vocational, professional higher and university education programs. Takes about 20...25 minutes to play a single game. ICT skills are needed. During playing real life examples, storytelling and case importance description are encouraged besides the actual fact knowledge.

The goal is to answer as many questions as possible and win after accumulating a required number (e.g. 3 if agreed so) of cards. The game is designed so the inquirer has to formulate a question and evaluate whether the answer is correct or not. Discussions and real life examples why this knowledge is important are encouraged.

There are six different categories - social engineering, privacy, network, internet, hacking, malware and 54 cards in the game.