European Crime Prevention Award (ECPA)

Annex I

Approved by the EUCPN Management Board in 2018

Please complete the template in English in compliance with the ECPA criteria contained in the Rules and procedures for awarding and presenting the European Crime Prevention Award (Par.2 §3).

General information

1. Please specify your country.

The Netherlands

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

Country's ECPA entry

3. What is the title of the project?

HackShield Future Cyber Heroes

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

Tim Murck - CEO t.murck@flavour.nl +31647096004

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.

16-11-2018 - Still running

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).

https://global.joinhackshield.com/en (main website) https://youtu.be/2cFYJuVc4Xw (English case video) https://media-and-learning.eu/type/featured-articles/hackshield-future-cyber-heroes-our-heroes-our-future/ (recent article about HackShield)

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

HackShield Future Cyber Heroes (HackShield) is on a mission to enable people to take advantage of the possibilities of the online world and thus create online equality of opportunity. We train children between the ages of 8 and 12 in cyber related topics. In contrast to the usual focus on crime prevention, focussing on the negative side of being online, HackShield's starting point is from a more positive perspective; being able to seize opportunities.

We train children to become Junior Cyber Agents and introduce them to cyber topics like passwords, phishing, cyberbullying and copyright. The children are offered knowledge and skills on our gamified platform, and are encouraged to transfer that knowledge and skills to (grand)parents, friends and classmates.

Every month, new educational material is released through the platform, which responds to the most urgent cyber topics. This (teaching) material is made available for primary education, mediapartners and libraries throughout the Netherlands.
The platform can also be reached at home via computer, tablet or smartphone, where children can continue to expand their knowledge by playing so-called quests in the HackShield game.

Additionally, we offer a connection with the offline world. Children can participate in physical events, earn shields (pins like scouting badges) and track their progress in a cyber passport.

The target group of 8 to 12 year old children has been selected with care. These children are the future and must be prepared for this future on time. They also have the curiosity, creativity, ethical compass and enthusiasm which they can use to set other people in motion.
However, in the coming years, we also want to develop content for youngsters (age 13-16) and adults (age 16+). The ultimate goal is an impactful and continuous activation towards a secure digital future for everyone.

HackShield is based on the Hero Centered Design method. In this method groups of people are set in motion as heroes within a change process. The goal of Hero Centered Design is to enable positive, meaningful and lasting change around major social issues.
Within HackShield we apply the Hero Centered Design method to realise a broad social movement. We created a story around cybercrime and put the kids in the lead role as Junior Cyber Agents.

In the municipalities affiliated with HackShield, children are summoned by mayors and local police units. These parties let the children know that their help is needed to fight cybercrime and to ensure a safe, online environment. Triggered by the call of the mayors and the police units, they simply create an account via the website www.joinhackshield.com or via the app in the Google Play or Apple Store. An account gives children access to the platform.

On the platform, they are playfully introduced to new knowledge and skills. First they are allowed to practice with this in the safe environment of the game. Then they are given real-life assignments such as: check if your neighbours have a WiFi password and give a talk about digital safety at school. With these assignments, children are motivated to take their knowledge and skills with them to reality.

Kids who do this and end up at the very top of the activation pyramid are our absolute heroes. These are also the children who will act as ambassadors. They share their

knowledge and experience with (grand)parents, friends and classmates and with their enthusiasm they ensure an increase of new potential Junior Cyber Agents. With this mechanism we also reach two vulnerable target groups; primarily children, but secondarily also elderly individuals.

In september 2022 HackShield started in Belgium, in 2023 Germany will follow.

HackShield is ready to activate all children in Europe for a secure digital future with equal opportunities for all!

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

8. Which **crime prevention/ reduction mechanisms** were used in this project to contribute to crime prevention and/or the reduction of crime or the fear of crime? Multiple answers are possible.

☐**Establishing and maintaining normative barriers to committing criminal acts**
e.g. 'Offenders, we are watching you' campaigns
☐**Reducing recruitment** to criminal social environments and activities by eliminating or reducing the social and individual causes and processes that lead to criminality
e.g. social and financial support for disadvantaged families
☒**Deterring** potential perpetrators from committing crimes through the threat of punishment
e.g. decreasing the time between arrest and punishment
☐**Disrupting** criminal acts by stopping them before they are carried out
e.g. increasing police patrols in vulnerable areas
☒**Protecting vulnerable targets** by reducing opportunities and make it more demanding to carry out criminal acts
e.g. placing locks and cameras
☒**Reducing the harmful consequences** of criminal acts
e.g. initiatives to recover stolen goods
☐**Reducing the rewards** from criminal acts
e.g. restorative justice programmes
☐**Incapacitating** (or neutralising) perpetrators by denying them the ability (capacity) to carry out new criminal acts
e.g. imprisonment of key gang members
☐**Encouraging** desistance from crime and rehabilitating former offenders so they are able to settle back into a normal life
e.g. prison rehabilitation programs

Explain how this/these crime prevention mechanisms were used ((**Max. 300 words**)

- HackShield creates awareness (deter)
    - Informing and activating children about current cyber themes
    - Ultimately strengthening the Security Mindset as part of the culture
- HackShield creates positive attention for the police and the role of the police in contributing to a (digitally) safe society
- HackShield increases risk perception (deter)
    - Provide insight into the consequences for both the perpetrators and the victims
- HackShield removes excuses (neutralising arguments) for committing cybercrime (deter)
- HackShield highlights positive alternatives (divert)
    - Show what legal options there are with which children can work on their skills
    - Retain talent (divert)

- Digital scouting: think Rangers of the WWF. But then with and for the Police.
- HackShield stimulates informed choice (divert)

Cyber security is a broad concept that encompasses technology, processes and procedures which are intended to combat or reduce the negative impact of incidents on the internet as a result of the actions of malicious or hostile parties.

Cyber security experts agree that the emphasis should be on “cultivating” a cyber security mindset among end users. Instead of establishing procedures, the mindset helps users make choices and decisions in the digital domain every day.

“Adversarial thinking is “the ability to approach system rules, operational spaces, and player actions from a hacker’s perspective.” [1]

We help and teach children to shape a sustainable digital world together. We arm young people against the lurking dangers of the digital domain.

They are the heroes who can solve the (social) problem. They see and learn new applications and learn to work together as 'future cyber heroes'. We call the underlying design strategy Hero Centered Design and it is based on a combination of storytelling (narrative content), gamification (game mechanisms) and problem solving (social challenges). It ties in with the perception of children who are entering the digital world.

II. The project shall have been evaluated and have achieved most or all of its objectives. For more information on evaluation, click here

9. What were the reasons for setting up the project? Was this context analysed before the project was initiated and in what way (How, and by whom? Which data were used?)? In what way did this analysis inform the set-up of the project? (**Max. 150 words**)

The youth of today are the adults of the future. Young people are the future. The future is largely digital and that brings new dangers and uncertainties with it. Our young people sleep, figuratively speaking, with the doors and windows wide open. Cyber criminals know the weaknesses of this target group and are constantly looking for the weakest link. **We do not adequately arm today's young people against the threats to digital life.**

The founders of HackShield want to contribute to a sustainable digital world by independently arming children against cyber risks.

[1] Seth T Hamman, et al. "Teaching game theory to improve adversarial thinking in cybersecurity students." *IEEE Transactions on Education* 60.3 (2017): 208

Based on (collected) analyses and research from TNO (https://www.tno.nl/nl/) and The Hague University of Applied Sciences the set-up of the project has been established.

Our three key insights were that we had to stimulate:

1. Adversarial thinking
2. Representational fluency[2]
3. Active knowledge sharing[3]

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

The young people of today are the adults of the future, they have the future. The future is largely digital and that brings new dangers and uncertainties with it. Hackshield arms young people against the threats of digital life. Young people who learn to be resilient in the digital domain at a young age can participate in the digital society with confidence.

Main objectives

Increasing the cyber security mindset in children aged 8-12 and their immediate environment. Understanding of digital technology, processes and procedures

Be able to think like the one who wants to attack digital technology, processes and procedures (adversarial thinking)

Secondary objectives

- Understanding that the digital world consists of data, which can be made and changed.
- Understand that digital data can be used for good and bad.
- Understanding that money is a major driver of what happens on the internet.

11. Has there been a process evaluation?[4] Who conducted the evaluation (internally or externally?) and what were the main results? Which indicators were used to measure the process? Did you make changes accordingly? (**max. 300 words)**

A process evaluation has been externally conducted by:

- Research group Social Safety - Saxion University of Applied Sciences
- Center of Expertise Cybersecurity - The Hague University of Applied Sciences

[2] The ability to create, interpret, translate between, and connect multiple representations.

[3] E. Dale (1946)

[4] **Process evaluation:** Also called *implementation evaluation*, or *monitoring*, this process documents **how the activities were implemented** in order to determine any deviations from the original planning. It facilitates finding explanations for when the results of the intervention are not as expected.

The method used was a document analysis and 30 interviews with developers, implementers and participants.

Summary

HackShield is a project, game and social movement to make children aged 8 to 12 and the Netherlands more cyber-safe.The design method of the makers is based on literature on storytelling, gamification and problem solving.

The implementation of the initiative has been standardised with room for individual (local) interpretation. Within the investigated municipalities, the initiative consisted of a promotion campaign to let children play HackShield, a period in which children play the game, and a tribute to the best players by the mayor and the police.

Participants, parents and implementers are satisfied with the progress of the project. Implementers are satisfied because there were clear instructions and good guidance and because the project is paying more attention to cybercrime. Almost all implementers would participate again in the future.

Participants all indicate that they have learned something, for example about strong passwords, recognizing phishing emails and how to prevent yourself from being hacked. Participants are enthusiastic and find the game fun and educational. All parents would recommend the game to others.

Strengths and areas for improvement. The commitment of partners involved in the initiative, the good support from the initiators and the small effort it requires for municipalities to participate ensure that the initiative runs smoothly. Profit can be made by involving schools better in the project and by adding more levels to the game.

Follow-up research in the form of an effect evaluation is a necessary next step.

https://hetccv.nl/fileadmin/Bestanden/Onderwerpen/Cybercrime/Rapportage_HackShield_in_Noord-Holland_HHs_Saxion.pdf (the full research report in Dutch)

12. Has there been an outcome[5] or impact[6] evaluation? Who conducted the evaluation (internally or externally?), which data and evaluation method were used and what were the main results? Which indicators were used to measure the impact? (**Max. 300 words**)

An impact evaluation (specifically about two 'Copy Copy' Quests on privacy and copyright) has been externally conducted by:

- Familyfactor (https://www.familyfactor.nl/)

[5] **Outcome evaluation:** Measures the **direct effect** (i.e., extent of the changes) **of the intervention on the target group, population, or geographic area**. The information produced by the outcome evaluation determines at what level the **objectives were achieved**.

[6] **Impact evaluation:** Measures **long-term effects** of the intervention on the target group, as well as **indirect effects** on the broader community. The information produced by the impact evaluation determines at what level the **ultimate goals** of the intervention were achieved.

The evaluation consisted of;

- qualitative research in the form of interviews with 20 children from groups 5 to 8
- quantitative research in the form of questionnaires with 128 children from groups 5 to 8

Summary

The most important question from this research was: What is the impact and learning effect for children in groups 5 to 8? The answer to this question is that there is certainly an impact and learning effect from groups 5 to 8!
The conclusion of this research is that the quests are educational and also very fun to do.

The children who have played the quests have significantly more understanding and knowledge than the children who have not played the quests. This means that the children who have played the quest are more likely to correctly answer questions about copyright (concepts and rules) than children who have not played the quests.

There is also a higher rating for subjects such as copyright and portrait rights among children who have played the quests, compared to children who have not played the quests.

The quest itself, in terms of content and design, is also very much appreciated. The children really enjoy doing it and give the quests an average of 8!

Both boys and girls liked the quests equally. There is also no difference in understanding among children who have played the quest for a long time (a month or more) compared to children who have played the quests recently (less than a month ago). Finally, in both quests there is no difference in the degree of understanding between children from group 5/6 and group 7/8.

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

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

HackShield:

- Sees children as heroes. We teach them cybersecurity by making them Cyber Agents that protect themselves and others around them against cybercrime, instead of telling them “to be careful” and “what (not) to do” on the internet.
- Is ahead of the education curriculum.
- Has more than 25% of the Dutch municipalities involved.
- Is free for children and schools
- Is a public-private partnership
- Uses a story and a game to activate children in the real world
- Is a high quality game. We work together with specialists and professionals to make sure that lesson materials are effective
- Is both fun and educational. The game is a balance between fun and learning cybersecurity skills
- Is surrounded with enthusiastic partners. We build a rapid growing community of Cyber Agents and professionals involved.
- Is a social intervention that motivates children to prepare themselves and the people around them for the digital future.

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

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

Collaboration has always been our starting point.

- Team HackShield Future Cyber Heroes & Flavour (serious game development), dr Barefoot & Editiem (film production) (creatives)
- SIDN Fund, Rabobank, Rabo Foundation, AFAS, ESET NL, Northwave, VOICE, the Hague Security Delta, ECP, … (private partners and knowledge experts)
- The Mediateam, Future NL, Media Literacy network (media pedagogues and educational experts)
- TNO, Saxion, Haagse, NHL Stenden, Familyfactor, Zealous Minds (researchers and science)
- Dutch police, the Dutch Ministry of Justice and Security, the association of Netherlands municipalities(VNG), the Dutch Centre for Crimeprevention and Security (CCV) and 1/3rd of all Dutch municipalities, 53 libraries, NPO/NTR (the Dutch public broadcaster), the Johan Cruijff Arena and various youth work organisations (knowledge- and distribution partners)
- 83.000 Junior Cyber Agents (active co creators)

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

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

HackShield is, and forever will be, free of kids marketing and freely available for children, parents/ guardians and schools. This is only possible with the help of our supporters and partners.

Municipalities and police contribute financially through an annual fee and help distribute the game via local (media) channels. We provide them with all the necessary materials to help activate children in their region. This leads to beautiful call-up videos of enthusiastic mayors and police officers.

https://youtu.be/h8vAbmpvTPo (Recent example)

Private partners contribute financially through a monthly fee and help distribute HackShield by giving guest lessons in primary schools using existing HackShield materials.

HackShield is a Social Enterprise with a clear focus on impact, but with an independent, sustainable and scalable revenue model.

To be able to grow organically into a successful international Social Enterprise, HackShield has received subsidies and investments from both public and private organisations.

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

Together with the public and private partners, the HackShield founders have invested almost three million euros in HackShield over the past four years.

More than 80% of the costs consist of wage costs. All technology and designs are developed in-house. Merchandise and pr materials are sold at cost prices.

Other costs mainly consist of organising events and hiring external experts.

Roughly speaking, 1/3rd is invested by the founders, 1/3rd is covered by subsidies and investments and 1/3rd is earned through annual and monthly fees from public and private partners.

17. Has a cost-benefit analysis[7] 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**)

In total, HackShield was played by 240,000 children and a much larger group, of an estimated 500,000 children, was reached at an 'awareness level'. More than 82.000 children became Junior Cyber Agent.

The contributions from the public partners are calculated at an amount of approximately 1 euro per child per year.

The actual costs are currently around 3 euros per child per year.

(3 million / 4 years = 750,000 per year) (750,000 / 240,000 = 3 euros).

By connecting more municipalities nationally and internationally, we expect to further reduce costs in the coming years.

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

- A new tenant has to be created (websites per Member State)
- All content needs to be localised (translation and cultural adjustments)
- 'Boots on the ground' via a local Powered by Partner
- Activating the local ecosystem of public and private organisations, local mediapartners, libraries and the educational system.

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

[7] **Cost-benefit analysis**: A type of economic evaluation that compares the direct and indirect cost of the resources employed in the intervention, with the equivalent economic value of the benefits.

Cybercrime is the fastest growing crime and is increasingly targeting young people. Young people are insufficiently aware of the threats when they go online. The risks such as cyberbullying, cyber exploitation and cybercrime are increasing. Young people share personal data on a daily basis, download data unsuspectingly, are good of faith, their natural competitiveness increases the dangers, and the Internet has an infinite memory. Cyber criminals are always searching for the weakest link.

HackShield is more than just a game for children and Youngsters. It creates a movement. It offers a constant stream of free to use, relevant and validated educational content on subjects that kids and youngsters need to know about, but the educational system is not providing yet.

At HackShield we have noticed increased attention in Europe for online sexual harrasment and exploitation, which is a great development and these subjects are also included in HackShield. However, there are so many other cyber related topics on which children need more education[8]. Naturally, the internet is limitless and borders are invisible, just like the EU. Furthermore, in contrast to the usual focus on crime prevention, focussing on the negative side of being online, HackShield's starting point is from a more positive perspective; being able to seize online opportunities.

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

HackShield is an educational game which trains children aged 8 to 12 years old to become Cyber Agents who protect themselves and their environment against the dangers of the online world and learn how to seize the opportunities in the online world.

By playing levels children learn about cyber security subjects and through quests they can also challenge their (grand)parents. They can even build and share their own levels with friends.

HackShield cooperates with municipalities and police who are looking for Cyber Agents to help make sure citizens will use the internet safely. Enthusiastic and active Cyber Agents even get the chance to be officially honoured!

In the Netherlands 24% of children played the game and more than 8% became Junior Cyber Agents. In august 2022 Belgium started and in 2023 Germany will join this movement towards a safe digital future with equal opportunities for everyone!

Learning goals
Students learn…
CQ1

- the Internet is a network of connections between computers. These computers are connected by cables.

[8] https://www.consilium.europa.eu/nl/policies/cybersecurity/

- that their own digital devices, in order to use the Internet, are connected to servers through an Internet service provider.
- how you can send a message to someone through the internet and that this message then travels all over the world.

CQ2

- what data are.
  The student understands that in addition to finding information, you can also leave information on the internet yourself.
- which data you can share and which you cannot (e.g. your date of birth is okay, your address not).
- why data is worth money.
  The student learns what interests people and other parties may have in obtaining possession of the data of others or in taking control of digital assets belonging to others.

CQ3

<u>Cyberbullying</u>

- online bullying, just like offline bullying, can have major consequences.
- that nasty messages can be spread very quickly to many different people using the internet.
- what they can do themselves when they are being bullied online.
- that the role of spectators is very important when it comes to online bullying, and that you also have a responsibility in this.

<u>Hacking</u>

- how to explain what cybercrime is.
- that as a hacker you can decide to join the good or the bad people.
- the parallel or link between online and offline crime (breaking into a house is illegal, breaking into a digital environment is also illegal).
- what consequences cybercrime can have for themselves and for victims.
- how they can train their digital skills safely and in a good manner.

CQ4

- to search for the right information and to check their sources.
- to consciously think about where they get their news or information from.
- to identify digital sources where useful information can be found.
- to estimate the nature of digital information sources.
- to assess whether the information acquired is useful, reliable and representative.
- the meaning of disinformation and misinformation.

CQ5

- what phishing is.
- how to recognize phishing.
- what to do when dealing with phishing.

CQ6

- what a money mule and what a money wolf is.
- what happens if a money wolf uses you as a money mule (money muling).
- what the consequences are of lending your account or accounts.
- that you should never lend out accounts, pincodes or bills.
- why a money wolf wants your data.

CQ7

- they are creators of their creative work and have (copy) rights to it
- not everything on the internet can be used just like that and why that is the case
  Learn that not all information on the internet can be used for free
- a lot of use of information is allowed if you deal with it in a media-wise way and respect the ownership of the creator

CQ8

- learn why it is important to act carefully on social media
- learn the risks of sharing personal information on (social) media
- become aware of the pros and cons of social media
- think about when information is unwanted and know who to discuss it with