European Crime Prevention Award (ECPA)
Annex I

Approved by the EUCPN Management Board in 2014

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

- Please specify your country.

Lithuania

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

It is Lithuanian ECPA entry

- What is the title of the project?

Safe Behaviour on the Internet

- Who is responsible for the project? Contact details.

Vilnius City Third Police Unit of Vilnius County Police Headquarters, Chief Investigator Vaidas Maziliauskas, e-mail: vaidas.maziliauskas@policija.lt, tel.: +370 648 04418.

- 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.

The most significant part of the project was being implemented in 2016. It was launched on 1 March 2016 and continued till February 2017. The final events took place on 6-7 February 2017 to commemorate the international **Safer Internet Day**.

- 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).

During the implementation of the project, the information was passed to the participants by various means of presenting of information (lectures, games, interactive activities, viewing of visual materials, discussions). Intermediate phases of the project were made public through social networks. Unfortunately, the substantive

part of the visual information could not be provided to the public through these social networks due to the privacy policy related to the prohibition of disclosure of personal information and images of minors.

Please find below the link to the *Facebook* post (the information provided in Lithuanian only):

https://www.facebook.com/vilniaus.treciasispolicijoskomisariatas/posts/1280957315319174

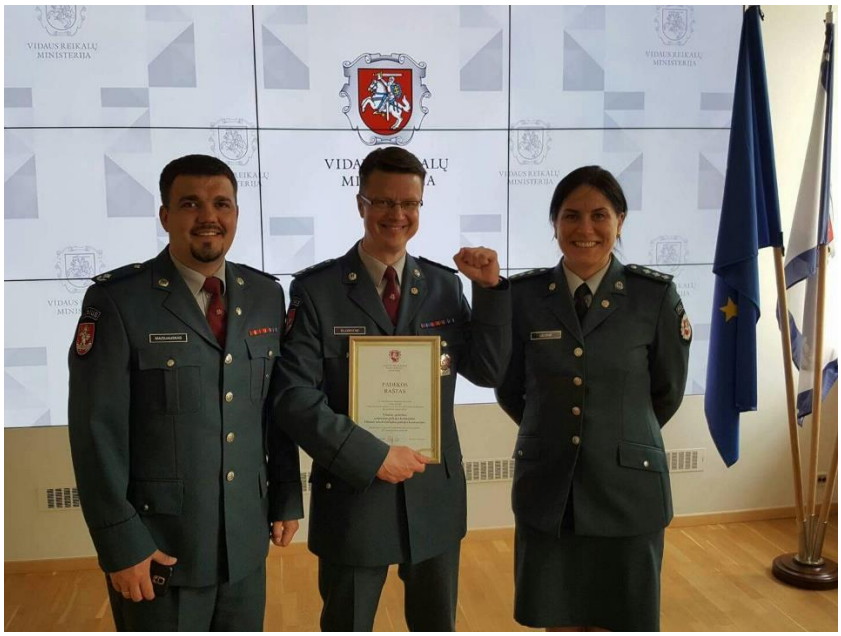
It is quite important to mention that the project received positive evaluation from the Ministry (MoI) of the Interior of the Republic of Lithuania (the link to the information about the Crime Prevention Award organized by MoI: https://vrm.lrv.lt/lt/naujienos/apdovanoti-nusikalstamumo-prevencijos-projektu-rengejai).

The information about the project is also available on the official internet website of the MoI:

http://vrm.lrv.lt/uploads/vrm/documents/files/LT_versija/Viesasis_saugumas/Konkursas/Vilniaus%20AVPK_Saugi%20kibernetine%20erdve.pdf

or

http://vrm.lrv.lt/lt/veiklos-sritys/nusikaltimu-ir-kitu-teises-pazeidimu-prevencijos-projektu-programu-konkursas-1



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

The extensive spread of computer and network technologies in the modern society at the end of the 20th century and the beginning of the 21st century determined that computers have become not only the instrument of the legal activities, but also the means for committing crimes, which occur solely in the electronic space (breaking into systems, data theft, distribution of prohibited content, copyright infringement, illegal distribution of visual materials, etc.).

The Internet is not only the source of possibilities, but also the source of possible threats. Any user, who has at least some basic skills, can find confirmation of this statement. Unfortunately, the most frequent Internet user, who has the largest potential, but very scarce knowledge of the Internet use practices and insufficient life experience, is a child. Although there is no plausible evidence yet that the Internet usage is a direct factor for negative formation of the personalities of teenagers, the results probably might not be good, if only the computer and the Internet would play the decisive role in the development of a child.

The youth (children) familiarise themselves with the world online, find friends, communicate with each other, expand their horizons, but becoming *internauts* they are not always aware that the virtual world is full of threats, just like the real world.

Social networks and the Internet pose the following threats to children:

- Sexting: a behaviour, when persons share texts and images of explicit content;
- Cyberbullying: intentional and repeated psychological humiliation of the victim before others using the means of the information technology;
- Pedophile networks: persons with no personal identification (using fake accounts/profiles) visit forums of youth (children) or groups of fans with similar interests;
- Internet and games addiction: which is expressed by excessive concern about the Internet, aimless browsing, viewing of multiple videos, spending extremely much time playing games, communicating on social networks, blogs, using online shops, spending time on pornographic websites, using the e-mail services, etc.;
- Expenditure on online games and their plug-ins: instead of saving money, for example, for buying a bicycle, which could enhance his/her physical and emotional state, give a reason to stay outdoors and meet friends in the real world, the child becomes more and more addicted to the game that he/she invested his/her pocket money in. Facing these problems results in health disorders and the growing risk of delinquent behaviour;
- Identity theft: usage of the identification data of another person (for example, data of the debit or credit cards, password of the e-mail account, social networks login data, passport information, etc.).

Considering the aforementioned threats, Vilnius City Third Police Unit of Vilnius County Police Headquarters decided to take action and to prevent the described

negative phenomena within the designated territory at the earliest stage possible. Therefore, an action plan of the project Safe Behavior on the Internet has been prepared and, once the leadership has approved it, the implementation of the project has started. It is obvious that prohibitions and restrictions of free use of the Internet can partly help to protect children from harmful online information. However, it is extremely important to speak with children about the online threats directly and to teach them the appropriate behaviour on the Internet, to raise the ability to overcome the challenges they face online by themselves. There are 18 educational institutions in the designated territory. Thus, during the implementation of the project the series of lectures were held at these institutions with the aim to have at least two project-related events at each institution. In addition, discussions with children were held, experience was shared, and situational analysis was carried out by means of visual aids and situational modelling. Upon the completion of the full cycle of lectures within the framework of the project *Safe Behaviour on the Internet* children signed the Code of Honorable Behaviour on the Internet, which was framed and hung in the classroom.

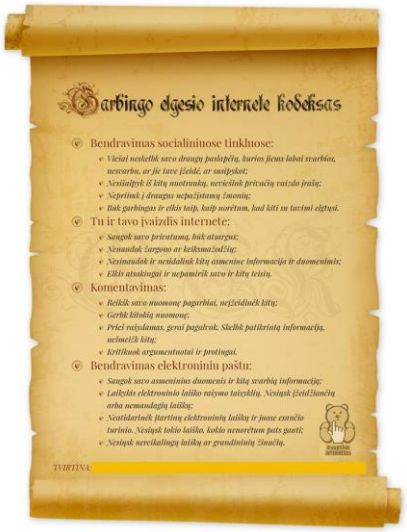
Educators and parents were also provided with recommendations about actions, which need to be taken in order to identify the problems as soon as possible and to encourage the safe behaviour on the Internet. After communication with adults, it was realised that at least 2 public events outside educational institutions for all age groups are indeed needed, because the public was poorly informed. However, due to the rapid development of the information technologies these days, the misappropriation and misuse of personal data of another person for criminal purposes becomes a mass phenomenon, which can touch anyone. Hence, the initiative within the aforementioned project titled *Protect Your Identity* was held in the shopping centres of Vilnius, which encouraged the participants in the activities to treat their personal data more responsible. Finally, the participants in the initiative shared their experience about possible ways to lose or give away personal login data while being careless; the consequences of such carelessness are usually devastating, and resulting not only in financial trouble, but also in psychological burden.

- **<u>The project shall focus on prevention and/or reduction of everyday crime and fear of crime within the theme.</u>**
  - How does the project contribute to crime prevention and/or to the reduction of crime or the fear of crime? (**Max. 150 words**)

The project *Safe Behaviour on the Internet* is classified as an action of the early prevention, one of the aims of which is to influence behaviour in order to avoid or forestall negative happenings among children/youth, so they do not become the victims of unsafe behaviour online or refrain from becoming *pests* in cyberspace (and not only there) themselves. Therefore, the results can be hardly measured in this case. The expectations are that the project was beneficial for quite a number of children/youth, their parents, and educators, other Internet users, who received information and knowledge about dangers in the cyberspace, and acquired practical skills related to this issue. Thus, they will be able to avoid breaching the law, and they will be aware of what to do and whom to approach in case of the committed criminal act, and finally, they will be capable of fostering responsible attitude towards the safe behaviour on the Internet.

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

During the implementation of the project, the information was spread in educational institutions, places of gathering of people, at shopping centres and through the social networks. The good practice was shared between various institutions and organizations. In total two project-related events were held at each of the 18 educational institutions, 2 public events took place in shopping centres, and the final closing event was held at each educational institution, with children signing the Code of Honourable Behaviour on the Internet, which was framed and hung in the classrooms. One of the intentions was to create chain reactions with people informing members of their household, friends, colleagues, because there is a severe lack of information regarding cybercrime. The more the public is aware, the less possibility is that they become a victim of the new type of crime.



- **The project shall have been evaluated and have achieved most or all of its objectives.**

  - What was the reason for setting up the project? What proble m(s) did it aim to tackle?

Nowadays new forms of crime, which are connected to the modern information technologies and new scientific achievements, appear alongside the traditional violations of law. Currently, rapidly developing information technologies are applied in almost every area of life. The development and improvement of information technologies has led to the consideration and solving of newly raised problems regarding violations of human rights and freedoms, as well as the increase of criminal offenses related to the use of information technologies. By tracking trends in cybercrime violations, we have seen that users-beginners are lacking knowledge of misleading threats in electronic space.

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

Firstly, the results of surveys performed in Lithuania and other EU countries were analysed by Community police officers of Vilnius City Third Police Unit. For instance, according to the Eurobarometer survey 2013, 81% of respondents in Lithuania believe that the risk of becoming a victim of cybercrimes is increasing, and 72% of Lithuanians are concerned about identity thefts online. The emerging fears hamper not only the expansion of online commerce and economic progress, but also slow down the transition to the use of public services online. According to the data of the representative public opinion and identity theft survey 2014 of the Lithuanian Consumer Institute the identity theft was experienced by 19% of respondents within 12 months, but over 49% of respondents did not know what identity theft meant. In general, the aforementioned survey revealed that Internet users in Lithuania think that there is not enough public information about the ways of self-protection in the cyberspace. Finally, 9.5% of the participants in the survey did not know completely who to contact in case of cybercrimes.

Secondly, the information was collected and summarized in cooperation with educational institutions, as well as performing the analysis of numbers of received police reports regarding violation of rights in the cyberspace.

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

Having analysed the context, community police officers of Vilnius City Third Police Unit drew up a plan of means and measures for the implementation of the project.

The following main objectives were defined:

- To provide Internet users, especially the beginners, with information and knowledge about dangers in the cyberspace, and also practical skills related to this issue, so they could be able to identify a cybercrime, avoid both becoming a victim and breaching the law, and they would be aware of what to do and who to approach in case of a cybercrime; finally, they would be capable of fostering responsible attitude towards the safe behaviour on the Internet;
- To increase children's and youth's safety on the Internet, providing social assistance and having positive influence on children and youth. Without a doubt, prohibitions and restrictions of use can partly help to protect children from harmful information on the Internet, however, it is extremely important to speak with children about the online dangers, to teach them the appropriate behaviour on the Internet, to raise the ability to overcome the challenges they face online by themselves.

- 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**)

Due to the fact that children and youth have vacation in summer, the implementation of the project started in at least 6 educational institutions before June 2016, and the rest of the project continued from September 2016 in the remaining 12 educational institutions. At the beginning and at the end of the project the surveys about the effectiveness of the on-going project were carried out among the employees of the educational institutions and the parents of schoolchildren. Even 92% of the respondents evaluated the initiative positively, because they gained knowledge about the dangers lurking in the cyberspace. Finally, the selected means of implementation were fully satisfactory for ensuring the favourable outcome, and did not need any significant adjustment in the process.

- 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*

Firstly, the process evaluation was carried out internally, starting with those persons, who implemented it, i.e. the community police officers of Vilnius City Third Police Unit. Secondly, the internal evaluation continued when the superiors of Vilnius City Third Police Unit (Heads of Divisions, Head of the Police Unit)

revised the project during the Annual Evaluation of Aims of the Police Unit. Since the evaluation of the leadership was positive, it was decided to participate in the competition, organised by the Ministry of the Interior of the Republic of Lithuania. The competition is related to crime prevention, and one of the topics was *Safe Cyberspace: Initiatives on Ensuring Safety in the Cyberspace*. Hence, the aforementioned institution performed the external evaluation, and the project was selected as the third best prevention project of the year. Vilnius City Third Police Unit received a reward and the acknowledgement from the Minister of Interior of the Republic of Lithuania on 01.06.2017.

- 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*

The evaluation of outcome was carried out internally only. Surveys/interviews of the employees of the educational institutions and also children and youth were carried out at the beginning and in the end of the project. The questions were given similar to those presented by the Lithuanian Consumer Institute and Eurobarometer, focusing on the definition of cybercrime, identity theft, misappropriation of login data, online swindling. Over 90% of respondents were able to identify a cybercrime and knew whom to contact after having encountered it after implementation of the project as opposed to slightly above 30% of respondents at the beginning of the project. The most important and pleasant fact was that 92% of the respondents found this project informing, useful, significant and necessary. The collected data of evaluation provided for an idea that it is worth to continue this prevention project as the next stage, another initiative or a new prevention project.

- **The project shall, as far as possible, be innovative, involving new methods or new approaches.**
  - How is the project innovative in its methods and/or approaches? (**Max. 150 words**)

The problem of the cybercrime is relatively new, but it grows rapidly becoming a global phenomenon. Currently, the most effective way to tackle cybercrime is to prevent it, and prevention is hardly possible without informing the public, especially the most vulnerable members of the public who lack life experience.

The project was the first of its kind in Lithuania, and it was created to educate children and youth (and adults) by contacting them directly, through live discussions and situation modelling. The latter required much personal involvement, was not only educating, but also entertaining, which is a useful

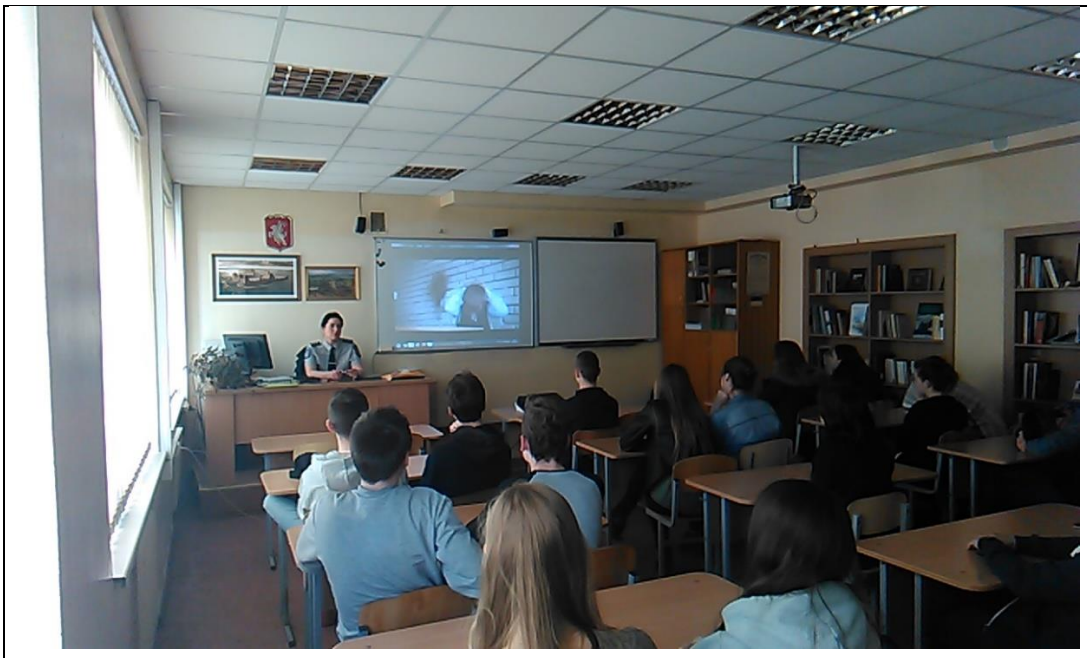
factor while trying to retain full attention of the aforementioned target group. Through situational modelling, the participants in the project learned to identify a cybercrime, because it was difficult for them to distinguish certain actions performed in cyberspace as crime. Furthermore, they learned how to react and how not to react (which can be even more important in case of a cybercrime) when dealing with crimes in the cyberspace.

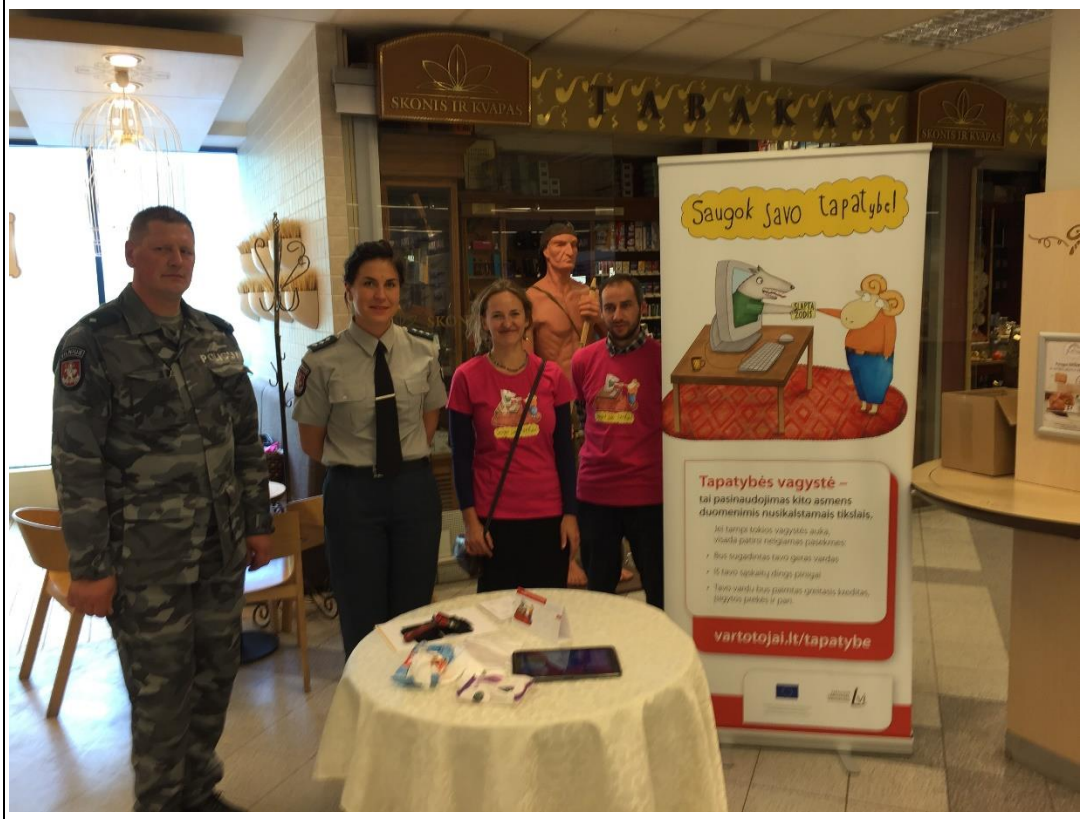
- **The project shall be based on cooperation between partners, where possible.**
  - Which partners or stakeholders were involved in the project and what was their involvement? (**Max. 200 words**)

As the project focuses on the main risk group, i.e. school age children, the main partners were the educational institutions, which regularly cooperate and provide information about negative phenomena in cyberspace among schoolchildren. The groups of pupils aged 10-16 years were selected, including teachers and parents who interact directly with children in their daily activities.

In total 18 educational institutions participated in the project, including 4 vocational education schools, 6 progymnasiums, 6 gymnasiums and 2 schools, for example, Vilnius Vocational School of Railway and Business Services, National M. K. Čiurlionis School of Art, Vilnius Antanas Vienuolis Gymnasium, Vilnius Simonas Daukantas Progymnasium, etc. When there were a possibility, social education specialists and psychologists, who were the part of the staff of the given educational institution, supervised the lectures of the project (including situational modelling activities).

The other direction of the project was dissemination of information, which is related to the protection of personal data, in public places, i.e. shopping centres *Maxima* and *Iki*, and this part was implemented together with the Lithuanian Consumer Institute. People of all ages were informed about the ways to avoid identity thefts, whom to contact in case of such crime. The participants of the project were encouraged to treat the maintenance and protection of their personal data more responsibly.





- **<u>The project shall be capable of replication in other Member States.</u>**
  - How and by whom is the project funded? (**Max. 150 words**)

The project was implemented by using budget subsidies for the general activities allocated to the institution (Vilnius City Third Police Unit of Vilnius County Police Headquarters). There was no additional funding.

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

Only human resources of the Vilnius City Third Police Unit of Vilnius County Police Headquarters were used to implement the project, and lectures, presentations and situation-modelling activities were their main tools. In total, two community police officers of Vilnius City Police Unit were implementing the project. The visual aids, namely, handouts were taken from the publicly available sources. Each officer spent up to 4 academic hours at every of the 18 aforementioned educational institution, and up to 4 hours at each of two public events in shopping centres.

- 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**)

Considering the specifics of the project, there was no need for completing such an analysis, thus, there was no analysis done.

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

The project can be implemented in its initial form but for a longer and more effective result, it is appropriate to adapt it as a curriculum for non-formal education. The advice could be given to use the means of mass media more frequently to spread the important information.

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

With the beginning of the Internet era, the fifth – cyberspace has arisen alongside the other four areas of human activities, i.e. land, air, sea and space. The phenomenon affects the majority of us, both young and elderly. The cyberspace has no walls. Thus, there are no efficient obstacles for criminal activity. The number of cybercrimes, both in Lithuania and around the world, is constantly growing, the ways and methods of committing crimes are becoming more sophisticated, a great damage is done to personal rights and massive loses are

incurred by the Internet users. The global nature of the cyberspace presupposes that nowadays a person located in a certain place of the world can commit a crime in the opposite part of the world by several presses of buttons on his/her keyboard much easier and faster than ever. Such a criminal no longer needs to travel to the country of the victim, the latter can be reached now anywhere in the world where the Internet is available.

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

With the beginning of the Internet era, the fifth – cyberspace has arisen alongside the other four areas of human activities, i.e. land, air, sea and space. The phenomenon affects the majority of us, both young and elderly. The cyberspace has no walls. Thus, there are no efficient obstacles for criminal activity. The number of cybercrimes, both in Lithuania and around the world, is constantly growing, the ways and methods of committing crimes are becoming more sophisticated, a great damage is done to personal rights and massive loses are incurred by the Internet users. The global nature of the cyberspace presupposes that nowadays a person located in a certain place of the world can commit a crime in the opposite part of the world by several presses of buttons on his/her keyboard much easier and faster than ever. Such a criminal no longer needs to travel to the country of the victim, the latter can be reached now anywhere in the world where the Internet is available.

The main risk group of the Internet users are the beginners: children, inexperienced users, who lack knowledge about the safe behaviour on the Internet. In order to provide the knowledge about the protection from the Internet threats lurking in the cyberspace, it is necessary to disseminate the information related to this issue as much as possible to protect the people from becoming the victims of cybercrimes or from becoming involved in committing a cybercrime.