Palacký University Olomouc

FACULTY OF EDUCATION

Centre for the Prevention of risky virtual communication

Czech Republic

RISKS OF ELECTRONIC COMMUNICATION 2

SURVEY RESEARCH REPORT

CONDUCTED WITHIN A PROJECT

E-BEZPEČÍ – RISKS OF ELECTRONIC COMMUNICATION FOR STUDENTS AND TEACHERS

Mgr. Veronika Krejčí
Mgr. Kamil Kopecký, Ph.D.

Olomouc 2011

1. Preface

The survey research Risks of Electronic Communication 2 follows survey researches which have been performed by the team of the Centre for the Prevention of risky virtual communication at the Faculty of Education, Palacký University Olomouc since 2008. The current survey research was conducted within a project E-Bezpečí - Risks of Electronic Communication for Students and Teachers[1] which is organized by the Centre for the Prevention of Risky Virtual Communication at Palacký University Olomouc (www.prvok.upol.cz). The research was carried out with the use of questionnaire system in E-Bezpečí portal (www.e-bezpeci.cz). 12 533 respondents from primary and secondary schools, including schools participating on Partnership Program of E-Bezpečí project, joined the research in the period from November 1, 2010 to December 31, 2010 when the questionnaire was available. Execution of the research was supported also by Vodafone Czech, Inc.

2. Research Conclusion

The goal of the survey research Risks of Electronic Communication 2 (performed in November – December 2010) was to determine following data:

A. Respondents' experience with cyberbullying from the point of view of victims and aggressors and their will to involve other people (parents and teachers) in a process of dealing with their problems.

B. Respondents' willingness to communicate with unknown persons who contact them within internet services, and their experience with meeting these people in the real world (cyber-grooming).

C. Respondents' personal data sharing within internet services (publication of personal data freely on the internet, sharing personal data with unknown persons on the internet) including respondents' experience with sexting.

D. Respondents' experience with social networks, web storages and portals focusing on children (potential environment for collecting personal data for the purpose of their possible further abuse and spreading of cyberbullying, for cyber-grooming, stalking and other dangerous practices).

[1] The project was supported by Ministry of Education, Youth and Sports Czech Republic within a program of prevention of hazardous behavior.

3. Methodology

Survey research Risks of Electronic Communication 2 is in its nature mainly descriptive, determined data are mainly quantitative. On-line questionnaire survey was chosen as the basic research method. On-line survey was monitored by questionnaire system of E-Bezpečí project and by Google Analytics system.

The questionnaire contained 67 questions of various kinds (dichotomous, leading, part, multipart, open format questions etc.).

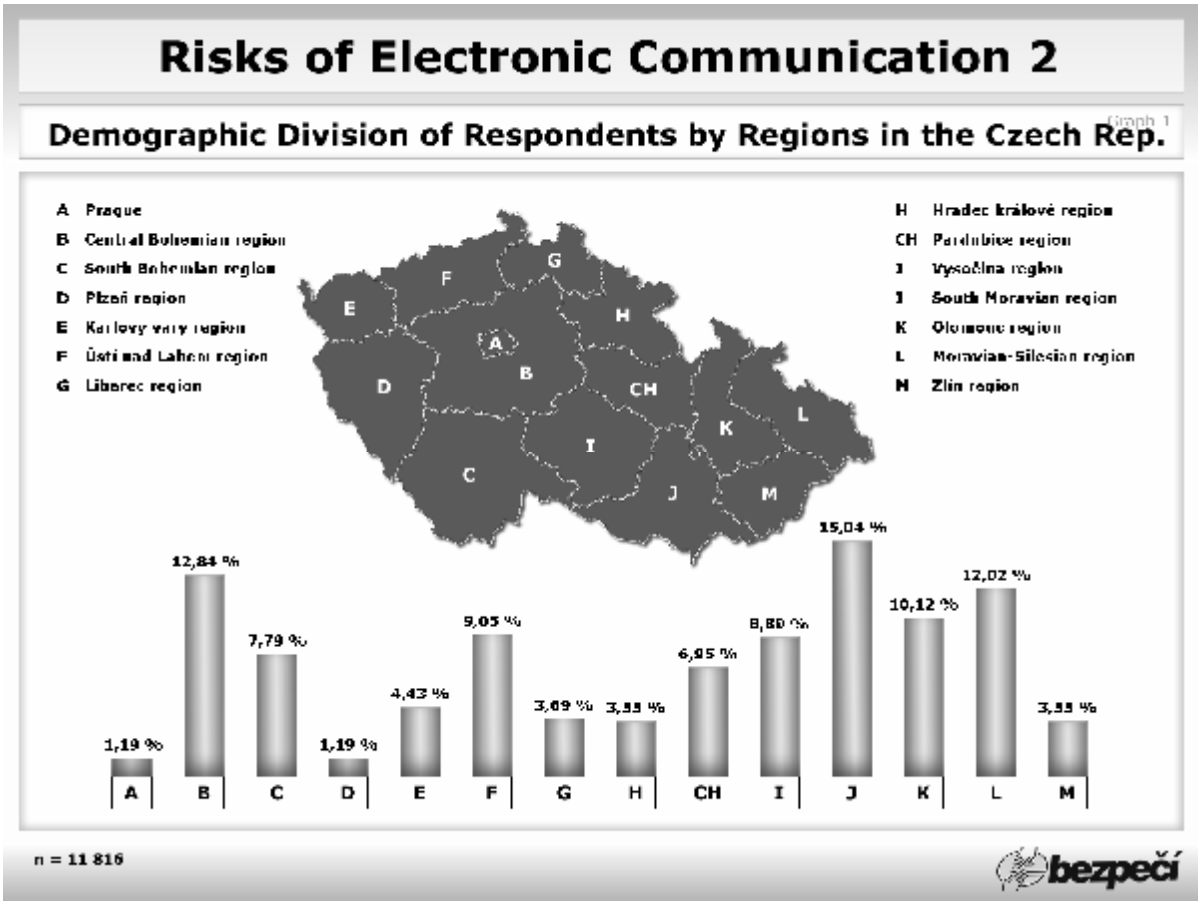
Respondents' efforts were motivated by the possibility to join a lottery with interesting prizes which we had offered as a motivational reward (T-shirts, promotional gifts, stickers etc.). Respondents interested in these prizes identified themselves by their contact e-mail.

The questionnaires were filled in anonymously.

4. Research Sample

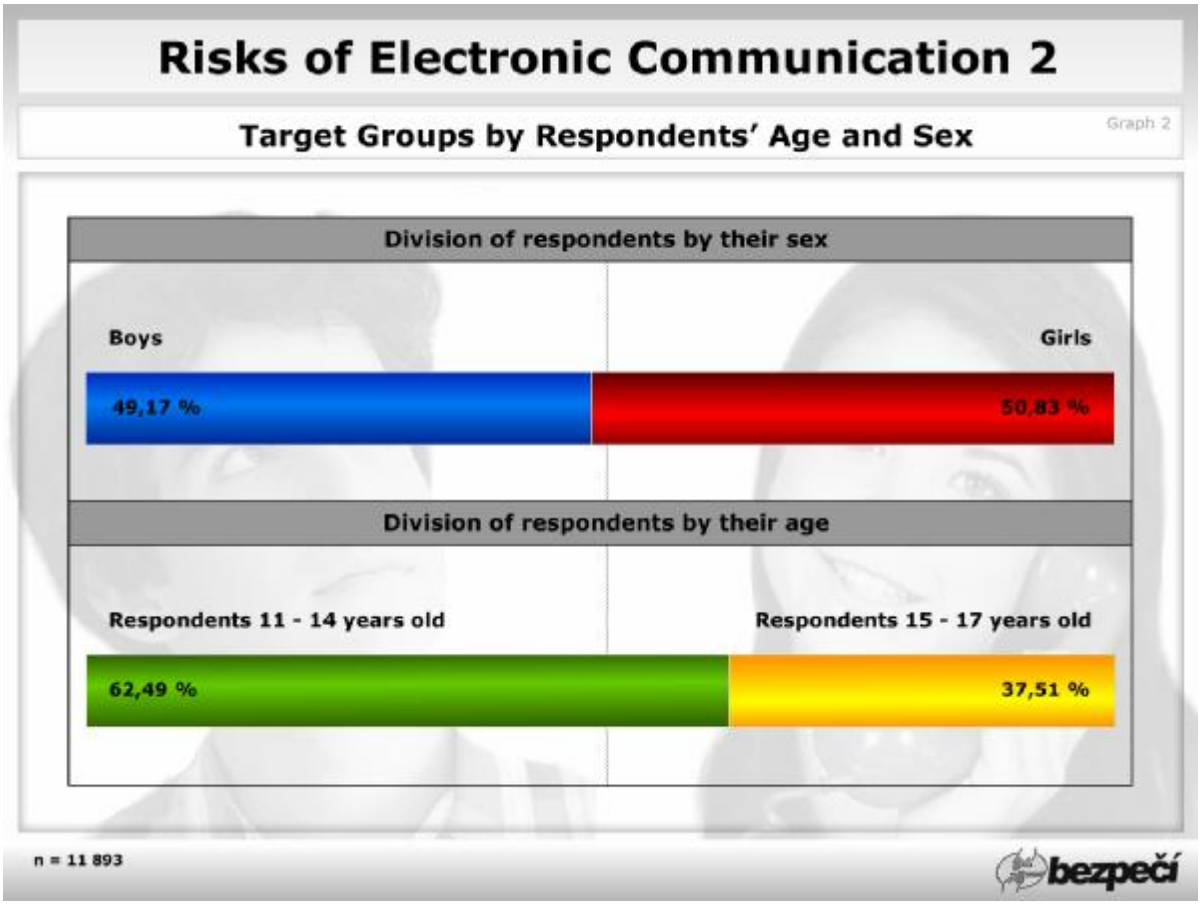
Over 4000 schools (primary and secondary schools) in all of the Czech Republic were addressed with the possibility of participation in the research. The maximum sample consisted of 12 533 respondents. The largest participation figure represented pupils from Olomouc region (15.04 %) followed by pupils from Central-Bohemian (12.84 %) and Moravian-Silesian (12.02 %) region. On the other hand, the fewest participating respondents were from Prague and Plzeň region (both 1.19 %). *(Graph 1)*

Graph 1 – Demographic Division of Respondents by Regions in the Czech Republic



The sample consisted of 47.17 % of boys and 50.83 % of girls. In terms of their age the sample was divided into 2 age categories matching the age of the 2nd and 3rd grade pupils.

Graph 2 – Target Groups by Respondents' Age and Sex



5. Research result

5.1 Cyberbullying[2]

Cyberbullying is a serious issue pupils experience quite often, which is why this topic was dealt with in the most extensive part of the survey research. There were these particular manifestations of cyberbullying monitored within the research:

- humiliation, insulting, mockery or another form of verbal ridiculing,

- publication of humiliating records (photographs, video and audio records),

- threatening and intimidation

- blackmail

- breaking in an electronic account and its possible misuse (so called identity theft),

- harassment (e.g. by phoning, giving a drop call and spamming).

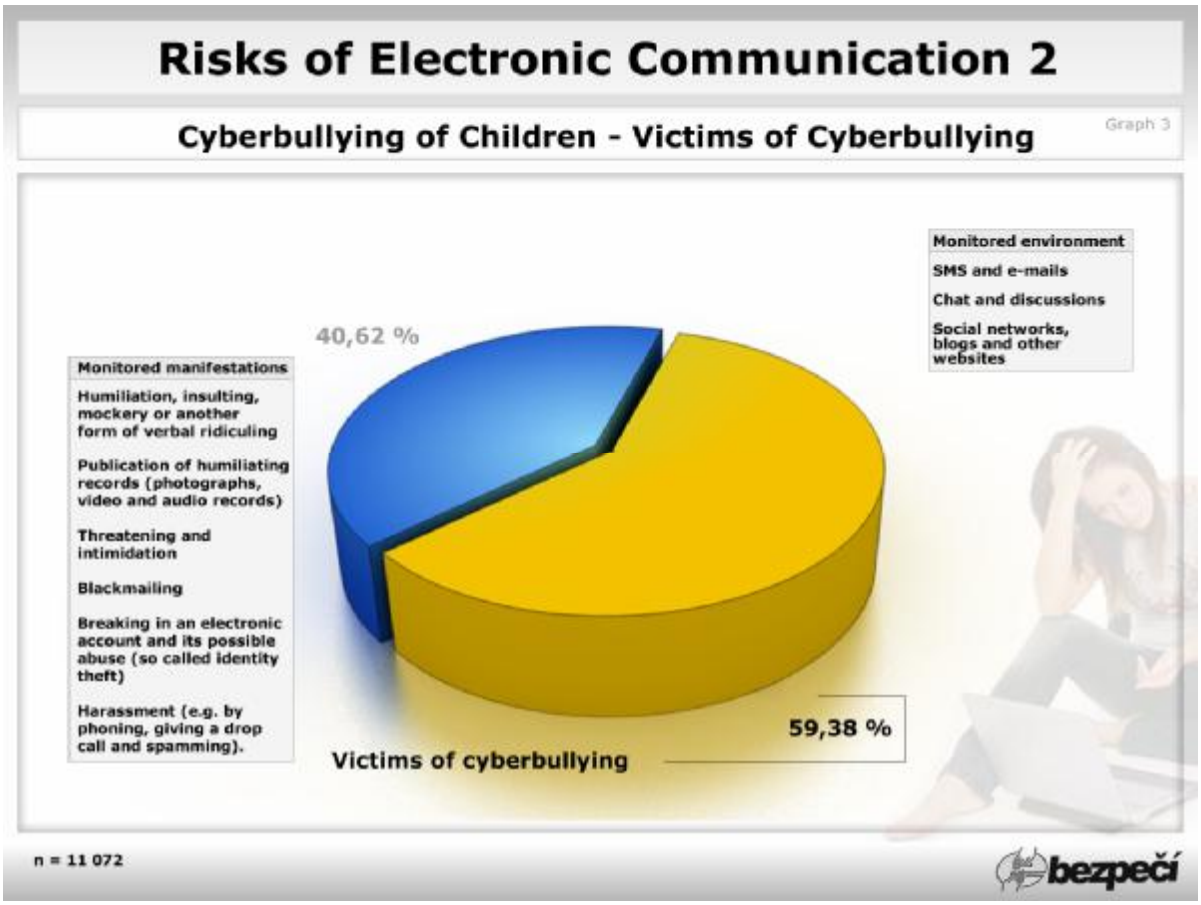
[2] Cyberbullying is a type of psychical bullying for which an information and communication technology is used by the aggressor (e.g. mobile phones, internet or pagers). There are many manifestations covered by the term cyberbullying (from Krejčí, V., 2009).

Cyberbullying of Children (Victims of Cyberbullying)

The survey research shows that more than a half of children (59.38 %) have met cyberbullying in the position of victim. *(Graph 3)* Monitored manifestations, however, can differ in their intensity and time duration.

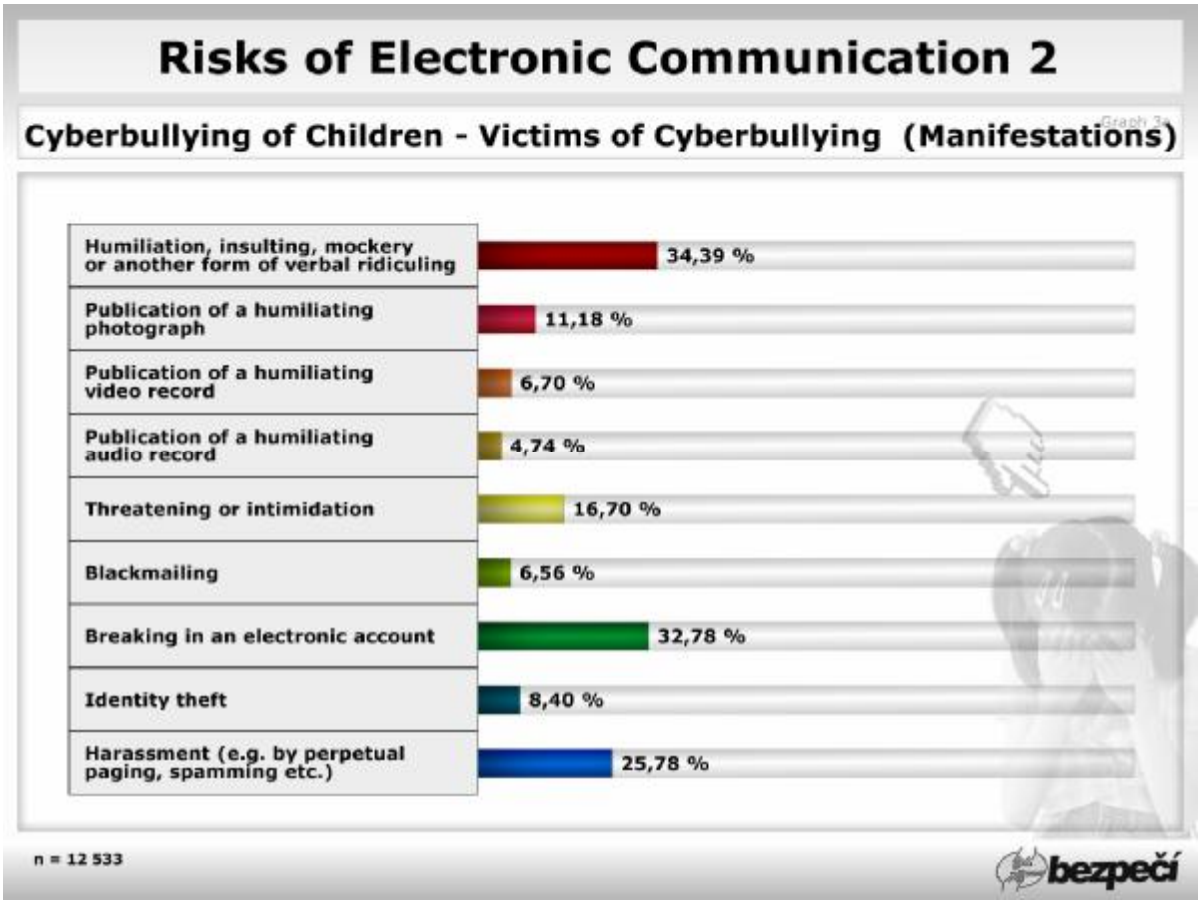
The questionnaire did not distinguish a difference between one-time and repetitive attacks. It was not monitored if a victim had experienced several attacks (by a group of unrelated aggressors) or if the attacks had been a combination of various manifestations of cyberbullying.

Graph 3 - Cyberbullying of Children - Victims of Cyberbullying



In terms of monitored manifestations of cyberbullying, the most common problem is a verbal humiliation, insulting, mockery or another form of ridiculing (34.39 %) and breaking in an electronic account (32.78 %). 25,78 % of respondents feel being harassed in the form of perpetual paging (giving a drop call), spamming etc. 16.70 % of children have encountered threatening or intimidation by means of ICT. *(Graph 3a)*

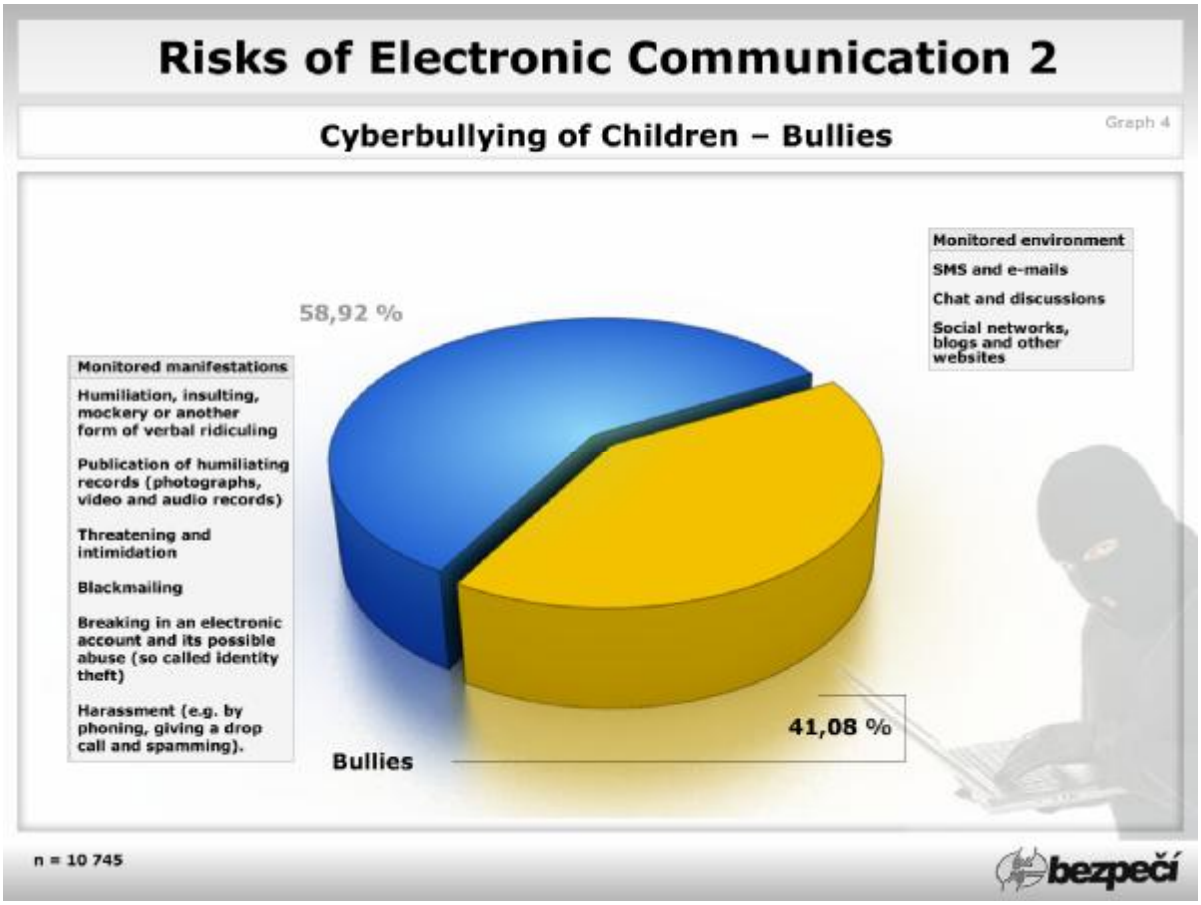
Graph 3a – Cyberbullying of Children – Victims of Cyberbullying (according to Manifestations)



Cyberbullying of Children (Bullies)

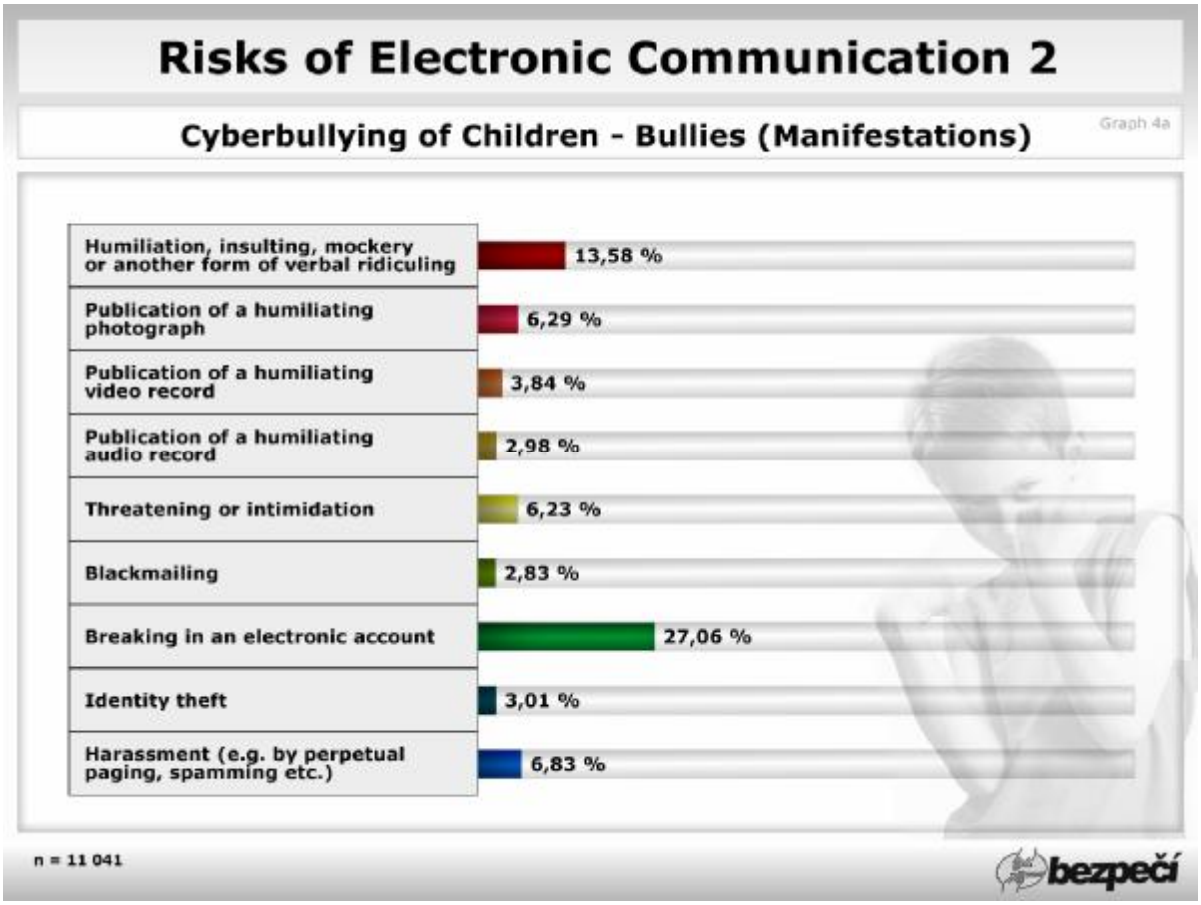
41.08 % of respondents admitted that they had tried some of the monitored cyberbullying manifestations. *(Graph 4)*

Graph 4 - Cyberbullying of Children (Bullies)



Breaking in an electronic account (27.06 %) and humiliation, insulting, mockery or another form of verbal ridiculing (13.58 %) belong to the most common forms of attacks. *(Graph 4a)*

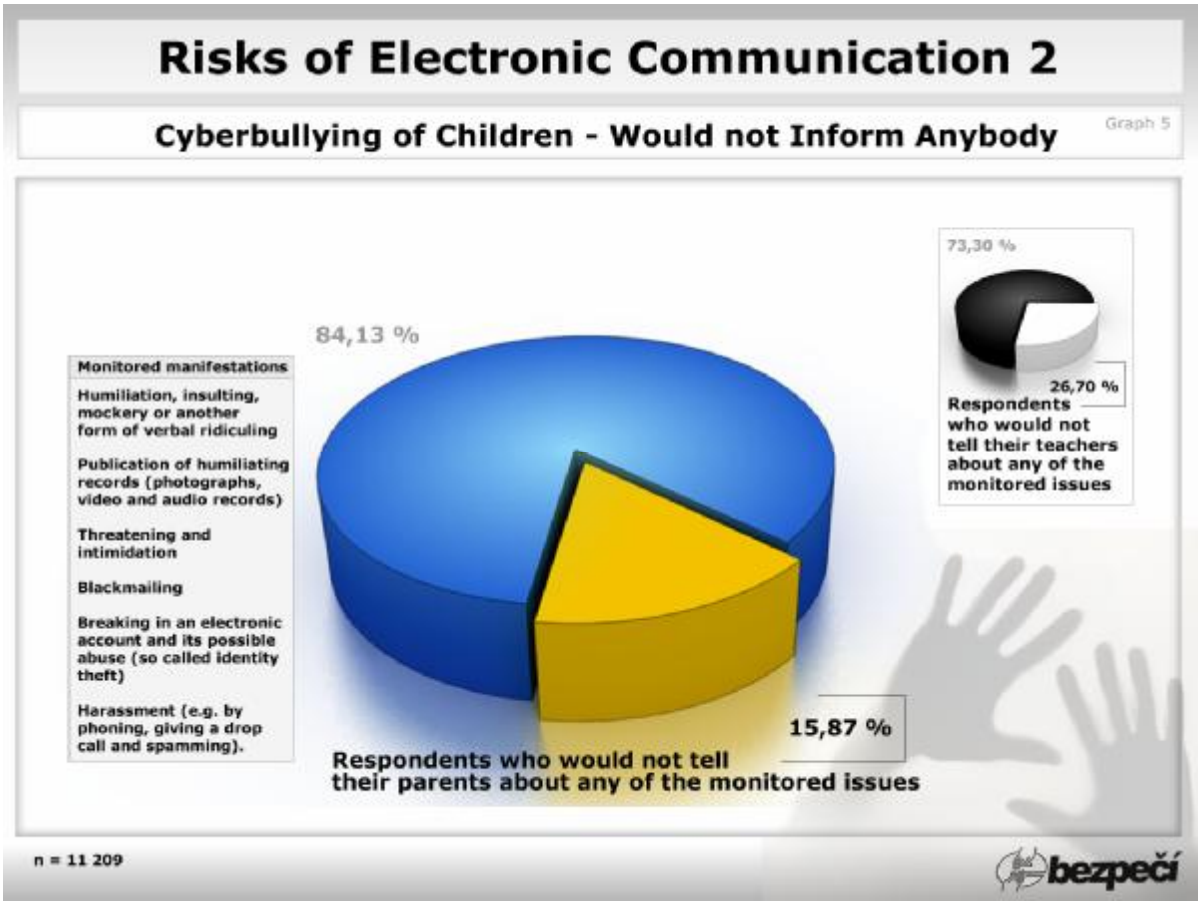
Graph 4a – Cyberbullying of Children – Bullies (According to Manifestations)



Cyberbullying of Children (Involvement of Other People in Dealing with the Issue of Cyberbullying)

15.87 % of respondents would not consult any of the monitored cyberbullying manifestations with their parents. About a third of respondents would not turn to their teachers for help with dealing with the monitored issues (26.70 %). It is obvious that most of children would turn to their parents or teachers for help in a particular problematic situation. *(Graph 5)*

Graph 5 – Cyberbullying of children – Respondents Who Would not Inform Their Parents / Teachers about Any of the Monitored Issues.

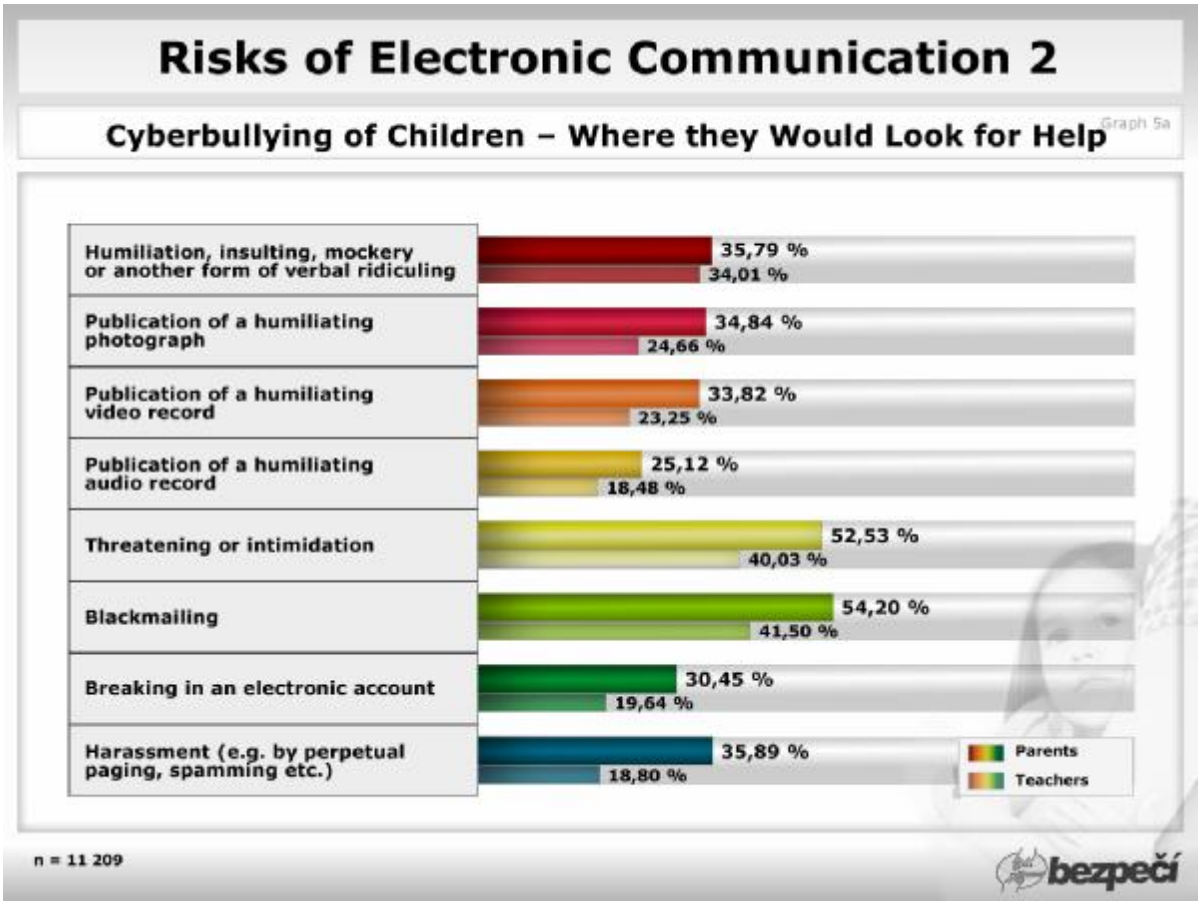


Situation in particular manifestations of cyberbullying is depicted in the graph below. *(Graph 5a)*

Children would most often tell another person if they became a victim of blackmail (54.20 % parents, 41.50 % teachers) and threatening or intimidation (52.53 % parents, 40.03 % teachers). About a third of children would communicate other problems to their parents (figures range from 25.12 % to 35.89 %). 34.01 % would tell their teachers about problems with verbal humiliation, insulting, mockery or another form of verbal ridiculing, whereas a fifth to quarter of respondents would consult their other problems (figures range from 18.48 % to 24.66 %).

Observed data show that 10.28 % more respondents, on average, would turn to their parents than to their teachers.

Graph 5a – Cyberbullying of Children – Where the Children Would Look for Help (Categorized by Manifestations)

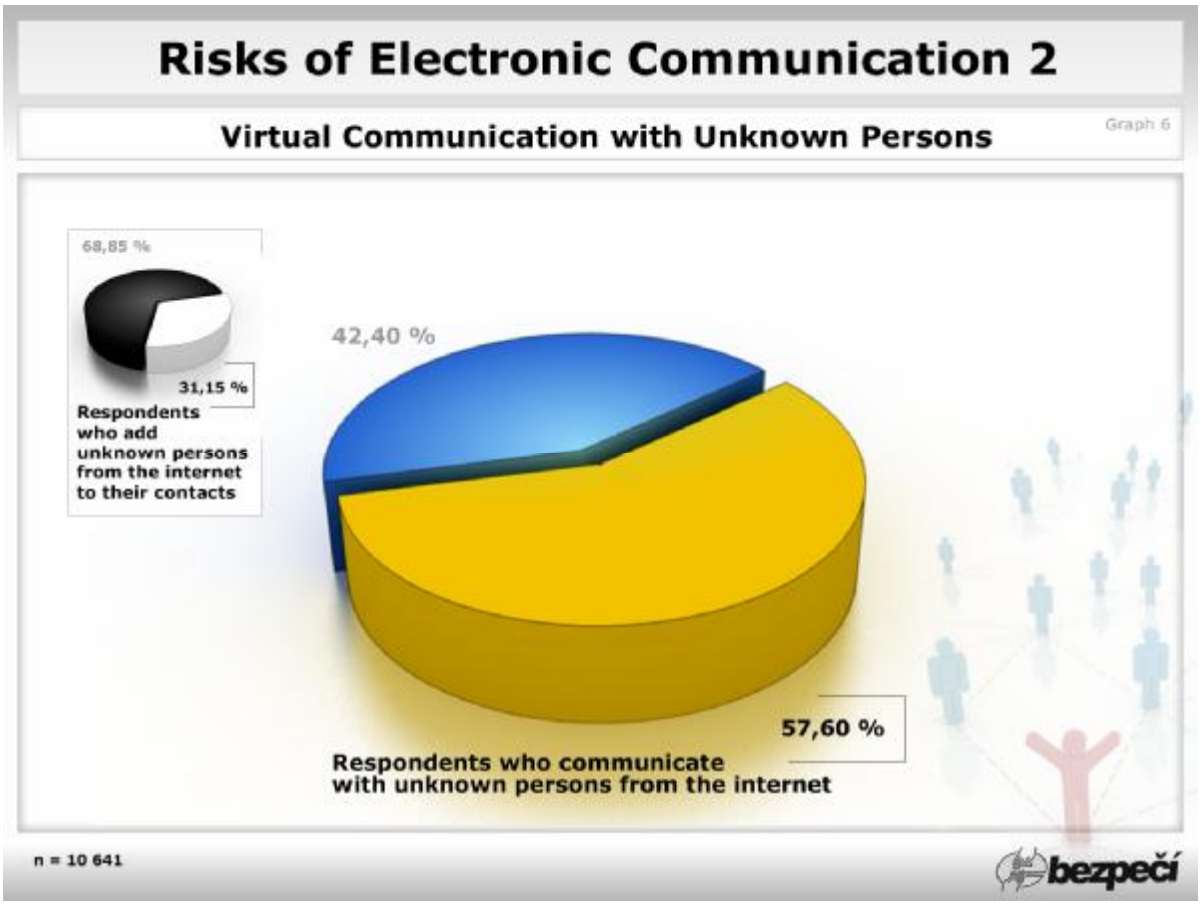


5.2 Virtual Communication with Unknown Persons

Communication with unknown persons via the internet belongs to potentially hazardous behavior for a child can be exposed to various manipulations. For instance, cybergrooming[3] is one of examples of dangerous manipulations.

It was determined in the research that the above mentioned kind of communication had been sought by 57.60 % of questioned children. 31.15 % of respondents are willing to add unknown persons to their contacts / friends etc. by request. *(Graph 6)*

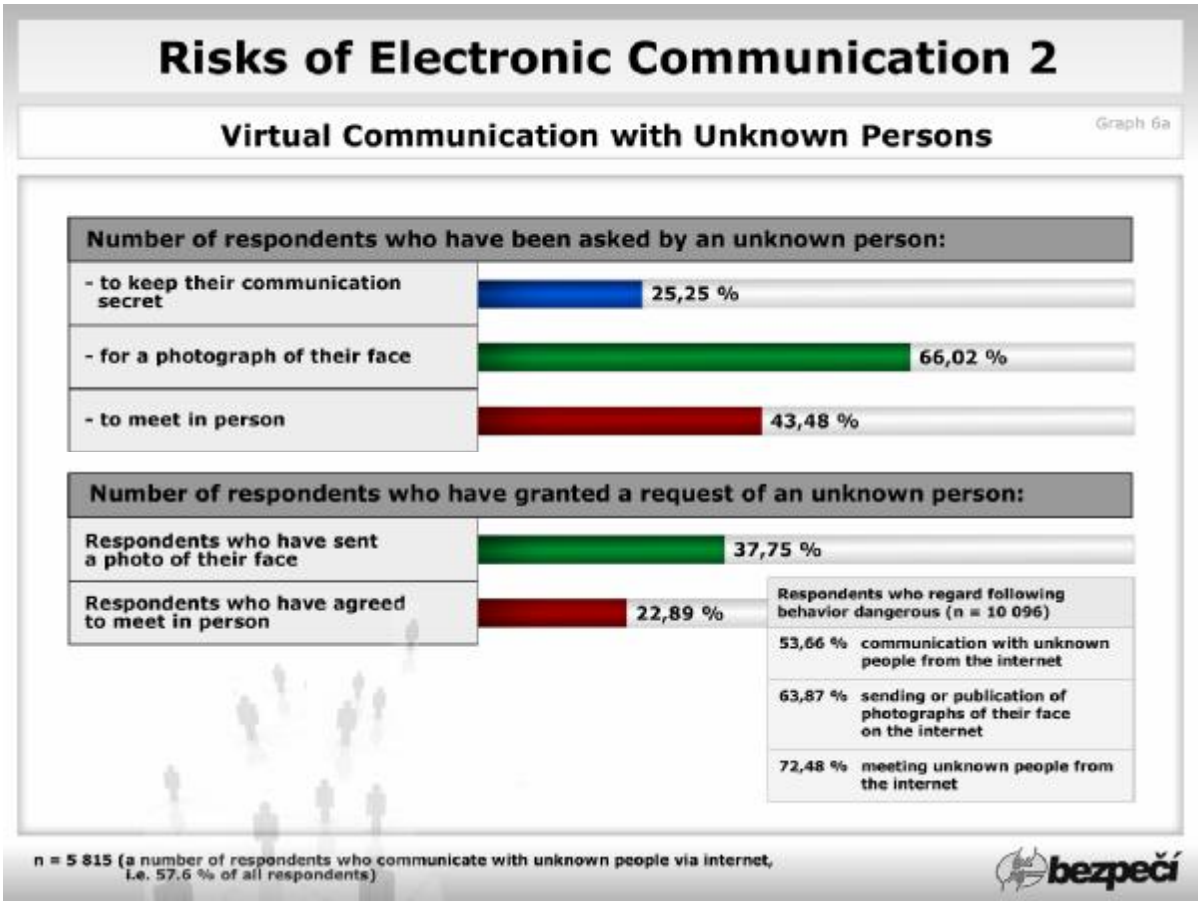
Graph 6 - Virtual Communication with Unknown Persons



[3] Cybergrooming denotes a manipulative behavior of internet users which is supposed to raise confidence and prepare the victim for a meeting where sexual abuse, torture or manipulation (forcing to stealing or terrorism etc.) can take place. (In Kopecký, K., 2008-2010).

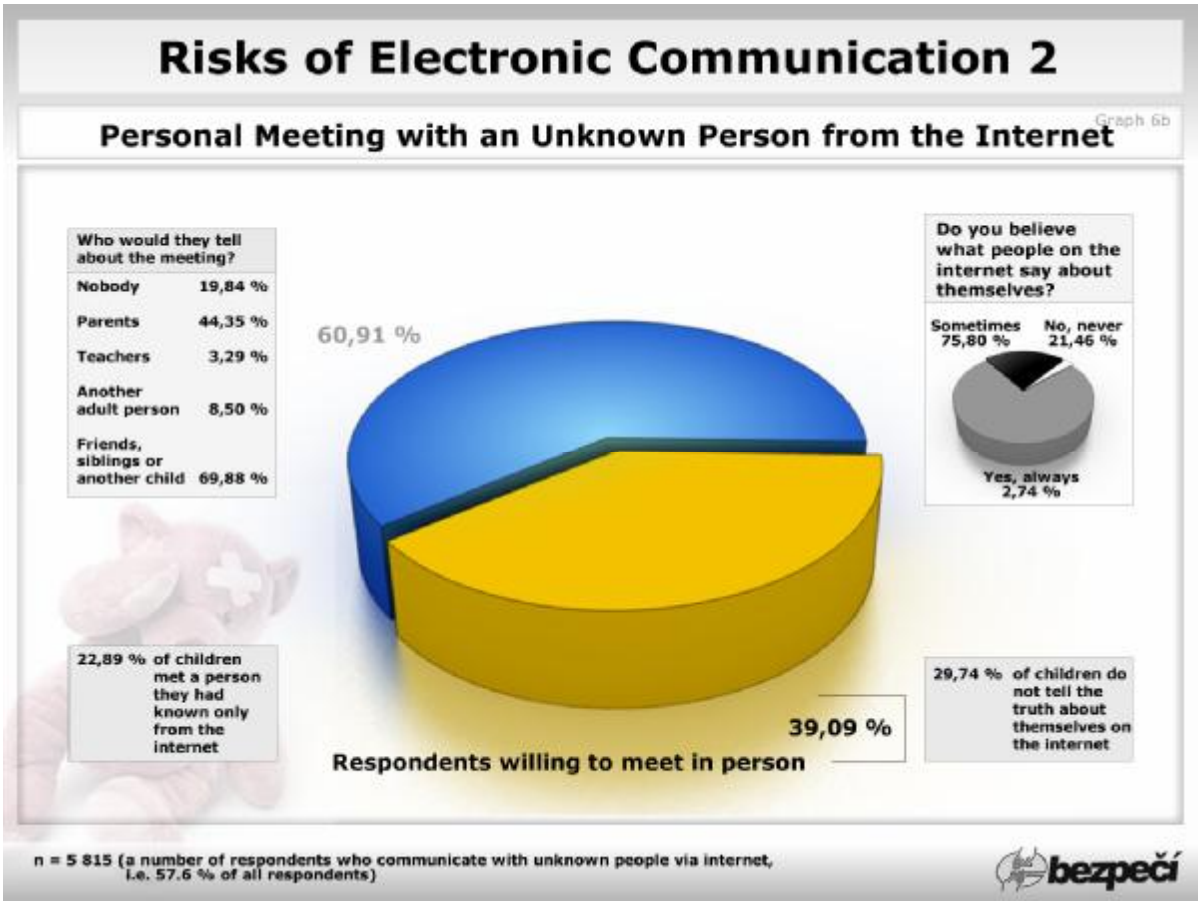
Within the course of this kind of communication, a number of respondents were asked to act in a way that could expose them to certain danger. E.g. 25.25 % of children communicating with unknown persons via internet were asked not to tell anyone that they were communicating with a particular person or what the content of their conversation was. This can be regarded a warning signal of something unsound taking place in the communication. Children communicating with unknown persons are often asked to send a photograph of their face (66.2 % of respondents). 37.75 % send such a photograph afterwards. 43.48 % of the children were asked to meet in person and 22.89 % of children agreed and met the unknown person in the real world. *(Graph 6a)*

Graph 6a – Virtual Communication with Unknown Persons



39.09 % of respondents would be willing to meet in person, in case that they were asked to. They would tell mainly their friends, siblings or another minor about the plan to meet an unknown person (69.88 % of respondents). 44.35 % would tell their parents. 19.84 % would tell nobody. *(Graph 6b)*

Graph 6b – Personal Meeting with an Unknown Person from the Internet



5.3 Sharing Personal Data within Internet Services

Sharing personal data is another risky element of virtual communication. These sensitive data can be easily misused for various pathologic communication practices, e.g. cyberbullying (especially in the form of blackmail) cybergrooming or cyberstalking, but also for pathologic, even criminal activity (e.g. using of these data by burglars).

Respondents were asked to share these data:

- their name and surname,
- photograph of their face,
- their address,
- phone number,
- e-mail address,
- contact data VoIP[4] (e.g. Skype) or IM[5] (e.g. ICQ),
- e-mail account password,
- personal identification number,
- credit card PIN.

Two forms of sharing personal data were monitored by the survey research:

1. Sharing or publishing personal data freely on the internet (hereinafter "publishing").

2. Sending or giving these data to persons within virtual communication (hereinafter "sending"). These data could be sent to an unknown person after some time of communicating, in return for reward etc.

[4] Voice over Internet Protocol (VoIP) is a technology for transfer of digitalized voice via computer net or another medium applicable for the protocol.

[5] Instant Messenger (IM) is an internet service allowing users to see which of their friends are on-line at the moment and, if they need to, send messages, chat, re-send files between users etc. Its main advantage over usage of e.g. e-mail consists in the principle of sending and receiving messages in the real time (a message is delivered in a very short time, mostly within the scope of hundreds of milliseconds.

The research shows that respondents publish a variety of risky personal data freely on the internet, which practically means that basically anyone can look through these data. In case of most monitored data the percentage of freely published data exceeds the percentage of data sent to unknown persons within virtual communication. Phone numbers, VoIP or IM contact data and PIN codes for credit cards are exceptions. *(Graph 6)*

When rating various personal data, it is necessary to consider a different risk-rate of these data and the level of danger related to their disclosure. Following data are included among risky personal data:

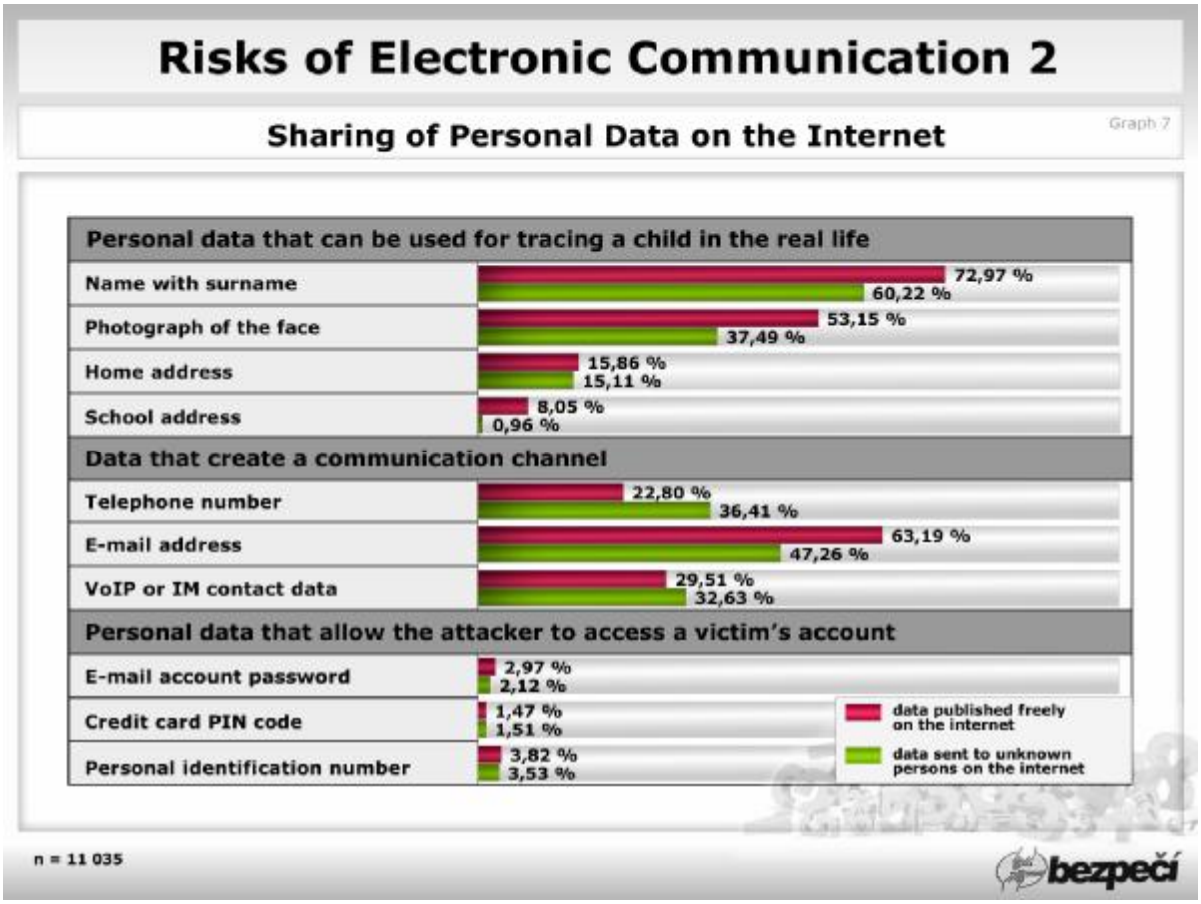
- data which can be used for tracing a child in the real life (e.g. 72.97 % of respondents publish their name and surname, 60.22 % of respondents send their name and surname. 15.86 % of respondents publish their address and 15.11 % send it),

- data that create a communication channel (e.g. e-mail address is published by 63.19 % and sent by 47.26 % of children, VoIP or IM contact data are published by 29.51 % and sent by 32.63 % of respondents, phone number is published by 22.80 % and sent by 36.41 % of respondents),

- data that allow the aggressor to access somebody else's account (these data are, compared to the previous cases, shared by much smaller number of respondents – published by 1.47 % and sent by 3.82 % of respondents). *(Graph 7)*

Special attention should be paid to sharing of photographs since a case study shows that photographs of children's faces are an efficient device used for blackmail leading to sexual violence against children etc. The survey research determined that 53.15 % share freely a photograph of their face and 37.49 % are willing to give it to an unknown person on the internet. *(Graph 7)*

Graph 7 – Sharing of Personal Data



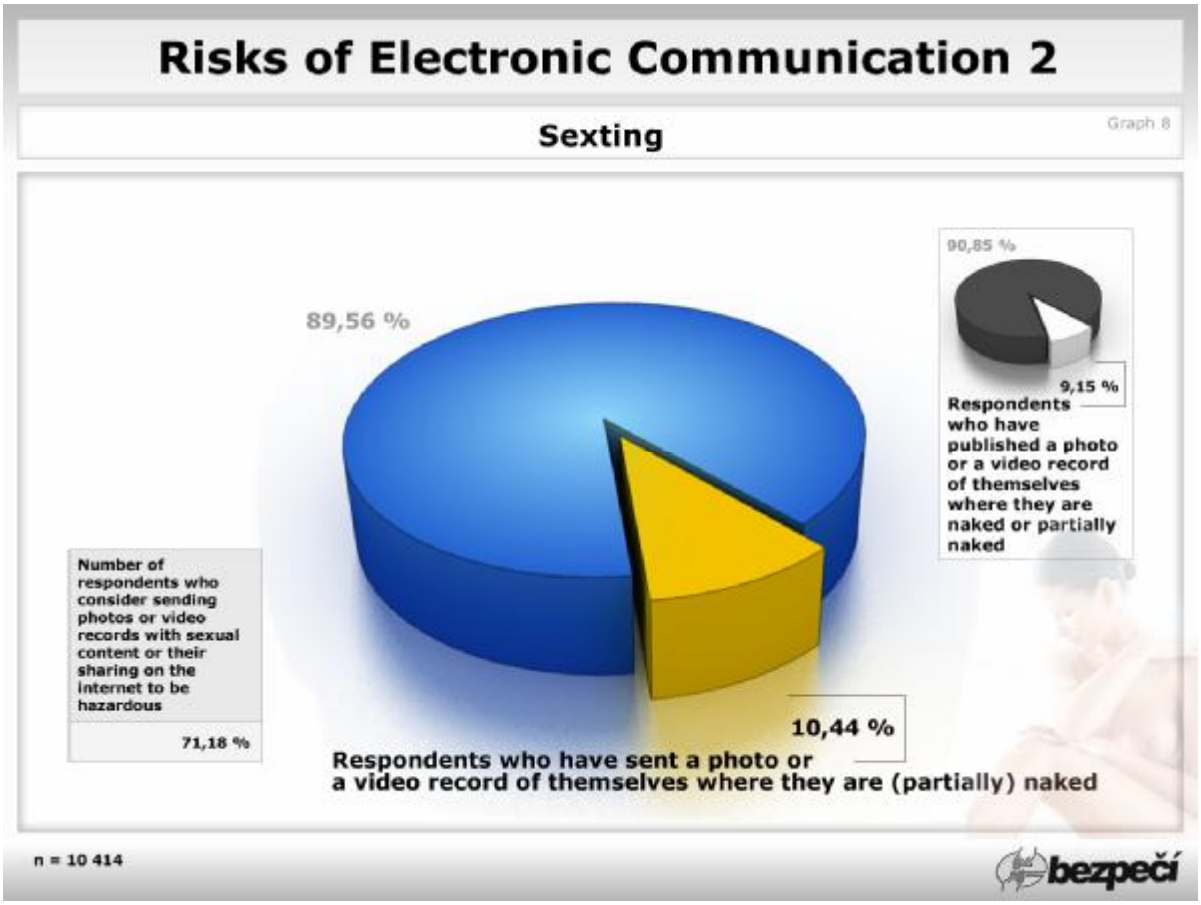
Sexting[6]

Another thing monitored in the research was respondents' willingness to share or to send a photograph or a video record with sexual content via mobile phone or an internet service. Specifically, it was a record of naked or partially naked body of the respondents. This activity is called sexting which falls within the group of hazardous activities associated with virtual communication as these materials can be used as a device for blackmail, humiliation or defacing of a victim.

Answers showed that 10.44 % of children had sent a photograph or a video record with sexual content to another person at least once. 9.15 % share this kind of depiction freely on the internet. Another fact we were interested in was whether the children regarded this behavior dangerous – that was confirmed by 71.18 % of respondents. *(Graph 8)*

[6] The term sexting denotes sending of messages, photographs or video records with sexual content, whose aim is mainly to start a relationship between the sender and receiver or to make the relationship more exciting.

Graph 8 – Sexting



5.4 Potentially Hazardous Virtual Environments

Within the survey research we directed our attention also on virtual environments which are, according to the case study, misused as devices for realization of hazardous communication practices or which are somehow associated with hazardous virtual communication.

On the basis of the analysis, 3 forms of potentially hazardous environments were chosen and we matched them to the most known and most used examples of particular portals. Those were:

- social networks,

- web storages,

- portals focused on a child-user.

Social networks[7]

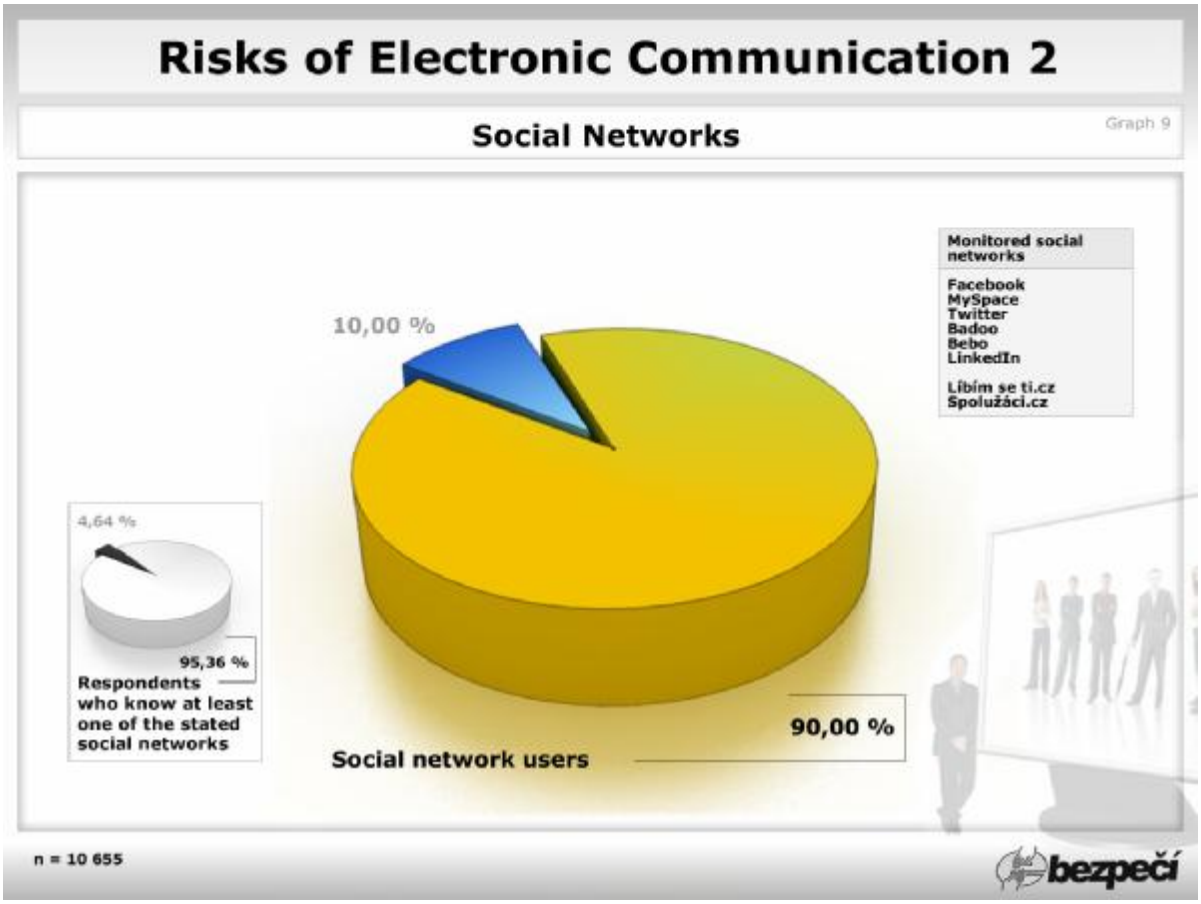
In recent years, social networks have been on the rise, they have lots of supporters and fans all over the world. Aside from advantages they provide, they pose a certain risk resulting mainly from sharing personal data, personal photographs or video records, easy access and users' anonymity. Social networks provide a great environment for social engineering[8] and dangerous communication practices; e.g. cyberbullying, sexting, cybergrooming, cyberstalking etc.

[7] Social network denotes an information network provided by internet portals which allows users to create virtual communities. Social networks offer space for presentation of people, communication, establishing of social relationships, education, commerce (advertisement, marketing, social engineering) or any other human activity that can be performed virtually.

[8] Social engineering is a way of manipulating people in order to perform a certain action or gain certain information. The term is commonly used for an illegal fraud or fraudulent behavior whose aim is to gain secret information of an organization or access to a company's information system.

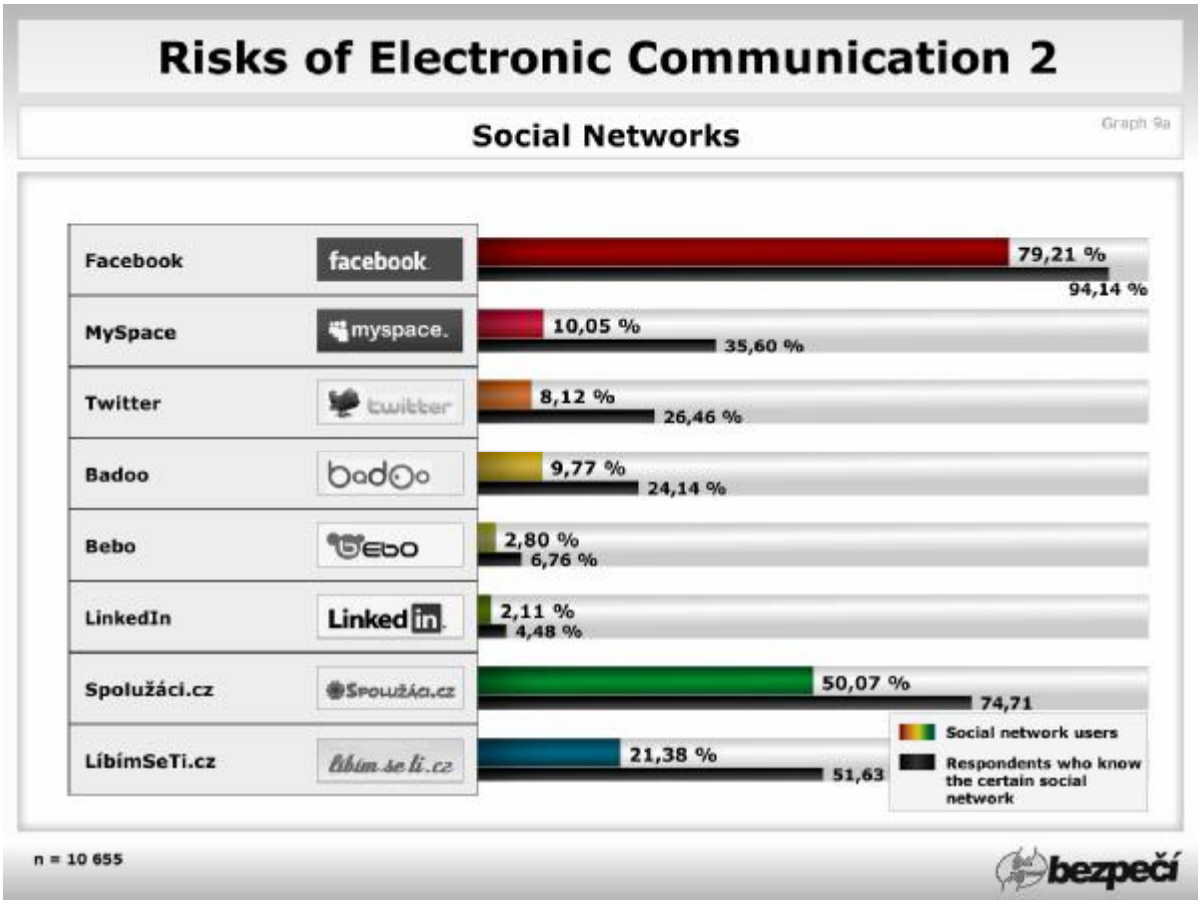
95.36 of respondents stated that they knew at least one of the mentioned social networks. Following social networks were monitored within the research: Facebook, Myspace, Twitter, Badoo, Bebo, LinkedIn, Libimseti.cz and Spoluzaci.cz. 90.00 % of children have their account on one of the mentioned social networks. *(Graph 9)*

Graph 9 – Social Networks



The most known and most spread network among users is the American network Facebook (94.14 % of respondents stated that they knew it. 79. 21 % have a Facebook account.) The most known and used social networks among Czech ones are Spoluzaci.cz (74.71 % know it and 50.07 % use it) which rated second in the overall summary and Libimseti.cz which rated third (51.63 % of children know it and 21.38 % use it). *(Graph 9a)*

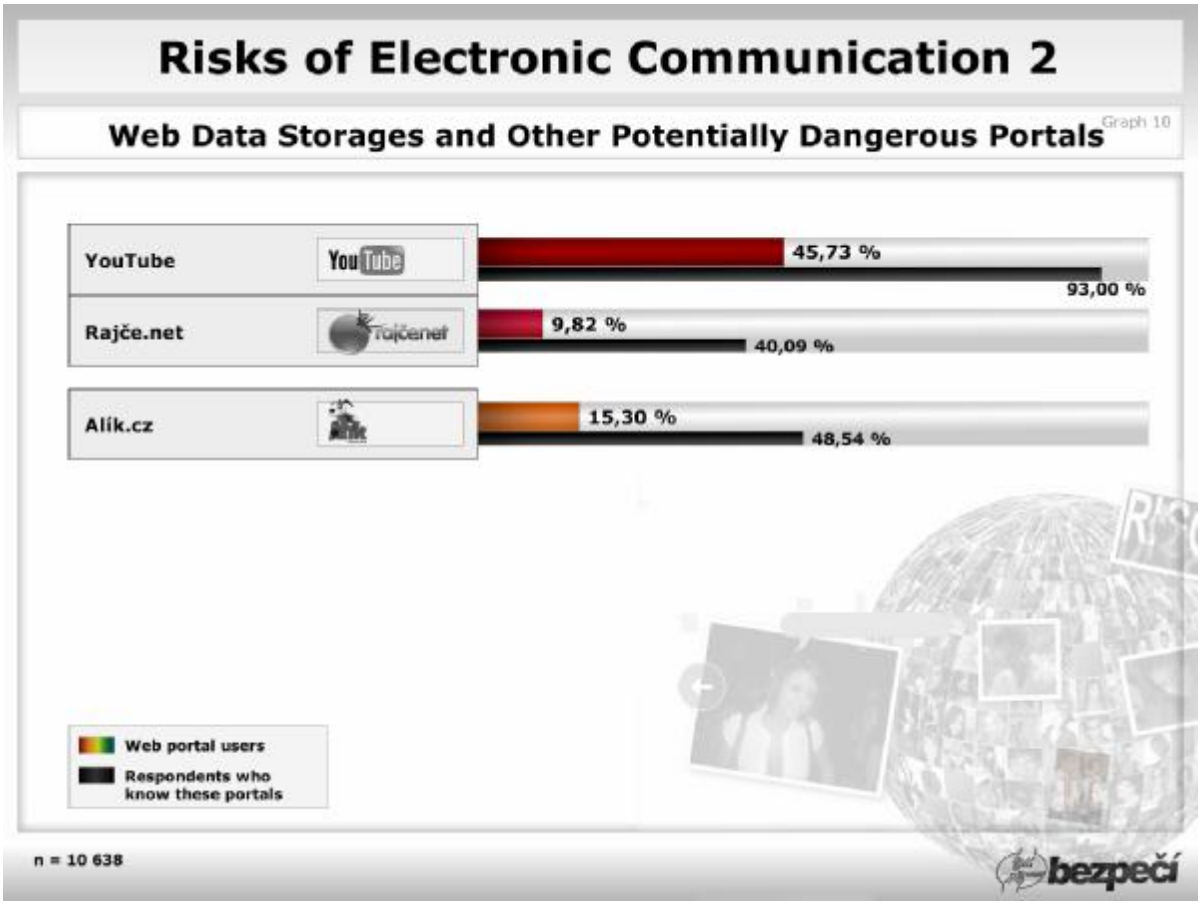
Graph 9a – Social Networks (Summary)



Web Data Storages and Other Potentially Dangerous Portals

From a group of other dangerous portals, we monitored web video storages (specifically YouTube), web photo storages (Rajce.net) and portals focused on a child-user (Alik.cz). These particular portals had been associated with manifestations of cyberbullying, blackmail and other manipulations from sexual aggressor. *(Graph 10)*

Graph 10 – Web Data Storages and Other Potentially Dangerous Portals



6. Summary

There have been certain changes in a variety of facts that are apparent in comparison with the survey research Risks of electronic communication[9] (conducted in 2009 – 2010). E.g. there has been a noticeable rise in the number of bullies; from 27.8 % to 41.08 %. The number of victims of cyberbullying has increased by 6 % (from 53.2 % to 59.38 %). On the other hand, changes in numbers concerning looking for help with dealing with cyberbullying can be seen as positive. On the average, respondents' willingness to turn to an adult person (parents / teachers) for help has doubled in all the cases of monitored manifestations.

While the number of children willing to meet an unknown person from the internet has stayed almost the same when compared to the previous research (it has slightly decreased from 39.2 % to 39.09 %), the number of children who would not inform anyone about such a meeting have gone up (from 8.7 % to 19.84 %).

Current survey research showed respondents' greater carefulness when handling their personal data on the internet. There was a decrease in numbers depicting free publication of these data on the internet and their sending by request (it was an increase by 10 % and more in case of many data). In regard to publication or sending photographs and video records with sexual content the numbers are comparable with numbers gained in the previous survey research (the number have risen from 10.1 % to 10.44 %).

A similar situation shows in respondents' knowledge of social networks and their usage; these numbers are basically the same as they were in the previous survey research.

[9] Risks of electronic communication 2009-2010 (research report) online on: http://prvok.upol.cz/index.php/ke-staeni/doc_download/5-nebezpei-internetove-komunikace-e-bezpei-prvok-2009-2010

7. Contact

Research was conducted by:

Mgr. Veronika Krejčí

Centre for the Prevention of Risky Virtual Communication

Faculty of Education, Palacký University, Olomouc

veronika.krejci@upol.cz

+420 777 588 382

Mgr. Kamil Kopecký, Ph.D.

Centre for the Prevention of Risky Virtual Communication

Faculty of Education, Palacký University, Olomouc

kamil.kopecky@upol.cz

+420 773 470 997

Contact address

Centre for the Prevention of Risky Virtual Communication

Faculty of Education, Palacký University, Olomouc

Žižkovo nám. 5

771 40 Olomouc

www.prvok.upol.cz

For information about other researches performed within the project E-Bezpečí see our websites: www.e-bezpeci.cz and www.prvok.upol.cz.