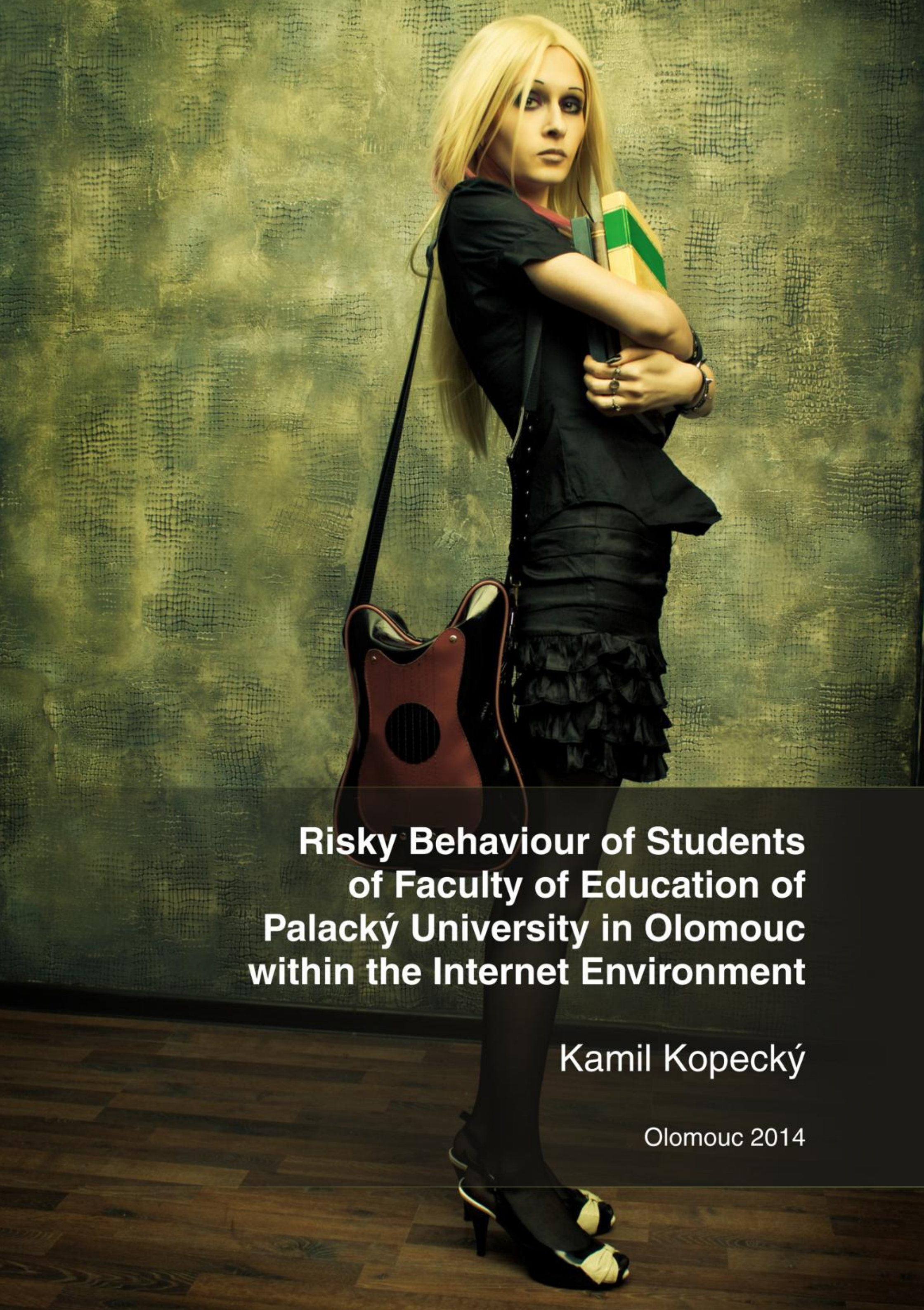


Risky Behaviour of Students of Faculty of Education of Palacký University in Olomouc within the Internet Environment

Kamil Kopecký

Olomouc 2014

Palacký University in Olomouc
Faculty of Education
Centre for the Prevention of Risky Virtual Communication

RISKY BEHAVIOUR OF STUDENTS OF FACULTY OF EDUCATION OF PALACKÝ UNIVERSITY IN OLOMOUC WITHIN THE INTERNET ENVIRONMENT

Kamil Kopecký

Olomouc 2014

Reviewers:
doc. PaedDr. Ludvík Eger, CSc.
doc. PhDr. Hana Marešová, Ph.D.

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

This publication was created within the project E-SYNERGIE - scientific network for risks of electronic communications (CZ.1.07/2.4.00/17.0062).

ISBN 978-80-244-4107-8

Content

Introduction to the problems

This publication presents research results of risky behaviour of students at Faculty of Education of Palacký University in Olomouc and it summarizes foundings that were reached during the analysis. Research monitors basic risky communication phenomena related to the use of Internet and mobile phones, namely to:

a) cyberbullying (various forms of cyberbullying connected to internet services - verbal aggression, blackmailing, threats and account attacks),
b) establishment of virtual contacts (communication with unverified Internet users, personal meetings, so-called cybergrooming or social engineering),
c) sexting (public sharing of intimate materials within the Internet environment, providing of these materials to person without verified identity, connection of sexting to other risky communication phenomena),
d) sharing of personal data on the Internet (aimed at sharing of face photos),
e) use of social networks (with relation to occurrence of particular risky communication phenomena),
f) other related phenomena.

The research was realized and guaranteed by Centre for the Prevention of Risky Virtual Communication at Faculty of Education of Palacký University in Olomouc. It follows researches Danger of electronic communication 1 and 2 (2010, 2011) and Danger of internet communication 3 (2012), further Virtual cyberbullying and its psycho-social consequences among university students (Šmahaj, J. a kol, 2011). **The research was realized within the frame of project OP VK E-Synergie - scientific network for risks of electronic communication (CZ.1.07/2.4.00/17.0062).** Presented monograph summarizes basic research results only.

1 Theoretical fundaments of observed phenomena

Research on risky behaviour of students at Faculty of Education of Palacký University in Olomouc monitored phenomena related to risky behaviour of adolescents on the Internet. In further text we will define basic theoretical fundaments of observed phenomena, i. e. cybergrooming, sexting, sharing of personal data, social engineering and cybergrooming within the Internet environment.

1.1 Cyberbullying

Definition of cyberbullying used in our research is based on existing cyberbullying definitions, where cyberbullying is understood as *aggressive, intentional, repeated action or behaviour carried out against an individual or group that cannot defend itself easily* (Whitney&Smith, 1993; Olweus, 1999). Other authors understand bullying as a *form of harassment that is based on power imbalance and systematic abuse of power* (Smith&Sharp, 1995; further Rigby, 2002). In Czech environment the bullying is defined particularly by M. Kolář and others.

Cyberbullying within this context is defined as *form of aggression, which is realized against an individual or group with usage of information and communication technologies.* This act is carried out repetitively (Belsey, B., and Smith & Slonje, 2007). Hinduja and Patchin understand the cyberbullying in a similar way when they define it as an intentional, frequently repeating and hostile behaviour that aims to harm the victim within usage of information and communication technologies. Most frequently through mobile phone or Internet. Definition is further developed and specified for example by Kowalski, Limber and others (2007-2008), who apprehend the cyberbullying as bullying carried out through e-mails, ICQ, mobile phones (text messages, MMS, phone calls), chat rooms, websites and other ICT. Dehue (2008) apprehends the cyberbullying as hazing, threats, humiliation, embarrassment and other attacks realized through Internet, interactive and digital technology or mobile phones.

Definition of cyberbullying is further elaborated also within the Czech environment (Kolář, M., Šmahel, D., Krejčí, V., Kopecký, K., Šmahaj, J., Vašutová, M. and others, 2008-2012). There are no significant divergences from foreign approaches.

Cyberbullying is often started as traditional bullying (psychical or physical). Bullying behaviours come out from the psychical bullying (e.g. dehonestation, provocation, threats, blackmailing etc.). Among the most familiar (Willard, 2007, Krejčí, 2010) we can find:

- **Distribution of humiliating recordings or photographs** (e.g. within the websites, MMS).
- **Humiliation and denigration** (within social networks, blogs or other websites).
- **Identity theft** (impersonation), **abuse of identity for cyberbullying or other social-pathologic acts** (for example electronic account theft).
- **Humiliation through fake profiles** (e.g. within social networks, blogs or other websites).
- **Provocation and attacks on users in online communication** (*flaming/bashing*) (mainly through public chats and discussions).
- **Reveal of someone else´s secrets with aim to harm the victim** (*outing*) (for example within social networks, blogs or other websites, through text messages etc.).
- **Exclusion from virtual community** (e.g. from a friend list on social network).
- **Harassment** (e.g. by repeated missed calls, phone calls or text messages).
- **Cyberbullying related to online games** (e.g. theft of virtual characters or items with consequent blackmailing, threats).

Cyberbullying also includes acts of traditional psychical bullying intensified by usage of ICT, for example:
Dehonestation (humiliation, swearing, offending).
Threats and intimidation.
Blackmailing.
Denigration.
And others.

These behaviours are carried out through SMS messages, e-mails, chat, discussions, IM (instant messenger) and VoIP (e.g. ICQ, Skype), blogs social networks or other websites in particular. These forms sporadically appear within virtual educational environments (virtual worlds) or online games (e.g. based on MMORPG). Within the framework of our research cyberbullying is monitored with respect to its individual behaviours among selected communication platforms (social networks, IM, chat and others).

It is obvious that cyberbullying presents complex phenomena and its behaviours emerge from combination of three basic constituents - *used forms of psychical bullying, forms of bullying content and tools used for its distribution (Krejčí, Kopecký, 2010).*

Tabulka 1. Cyberbullying as a ternary complex

Used forms of psychical bullying	Forms of bullying content	Tools for spread of bullying
Dehonestation (humiliation, swearing, offending) Denigration Provocation Threats, intimidation Blackmailing Harassment Stalking	Text Video recording Audio recording Graphic recording (photo, picture, caricature) Phone calls, missed calls Identity theft[1] Etc.	Public chats (textual, video chats), e-mails, instant messengers, surveys, social networks, virtual educational environment, online games, VoIP, SMS, MMS, websites, online data storage (cloud) etc.

Specific form of cyberbullying arises from the combination of particular elements, for example blackmailing through photos within social networks.

So-called *happy slapping*, or *stalking and cyberstalking* among adults are classified as associated or variant phenomena connected to cyberbullying.

[1] Considering the specific nature of the identity theft we classify it as one of the forms of bullying content, although it is not a primary psychical bullying nor technical mean or tool.

Happy slapping is one of the forms of physical and psychical aggression (Kopecký, 2008, Krejčí, 2010), which was mapped for the first time in 2005 in south London within so-called hip hop “gangsta teenagers”. Subject-matter of happy slapping is to unexpectedly physically attack a teenager or adult, whereas accomplice is recording the whole act on mobile phone or camera. Recorded video is then placed on the Internet (e.g. on YouTube, Facebook etc.). The video is meant to entertain the internet audience on victim´s account. Anybody can be a victim – a man who is just roller-skating or jogging through a park, somebody hurrying for a bus etc.

Intensity of the attacks rose along with the number of happy slapping acts and in some cases the intensity got to the real injury to health, furthermore to a death (e.g. one of the attackers shot an unsuspecting victim to the leg with an airgun, in one of the other cases attackers ignited victim´s hair or group of attackers beat a homeless to death, recorded the whole act and shared the video on the Internet).

Happy slapping is also connected to university environment. Well-known case of happy slapping was realized by students of University of Oxford who attacked and recorded one of the students of Imperial College in London, who was a member of rival rowing club (Miller, 2008). Attacker Colin Groshong was recorded by the accomplice Nick Brodie when he laughed at the rival rower Willy McFarland at first and then hit him in the face. Recording was later on posted on Facebook where other users added comments. Case details can be found in further parts of this publication.

In 2007, French Home Secretary Nicolas Sarkozy submitted a proposal to judge the happy slapping as a criminal act similar to rape or other criminal acts. His proposal was accepted and paragraph regarding happy slapping appeared in article 44, which also deals with law of robbery. Based on the above-mentioned fact, happy slapping is a criminal act that can be punished by 5 year prison sentence.

In Great Britain this form of crime was punished in 2008 for the first time. A girl who recorded a man beat to death by her accomplices on her mobile phone was sent to prison for two years. The man died in a hospital due to torn mucosa. Accomplices aged 19 - 17 were sentenced to 7 and 6-year imprisonment.

Czech law system is not familiar with term happy slapping; nonetheless happy slapping behaviours are classified as offences, misdemeanours or crimes.

Happy slapping is closely associated with **cyber-bashing**, which represents different forms of internet attacks where two groups with different opinions or attitudes attack each other on purpose. Definition of this term is relatively heterogeneous; the term can symbolize for example recordings of fights between pupils or students that are being placed on YouTube, but also psychical aggression of social network users etc. Cyber-bashing is in principle connected to term flaming.

Stalking is a term that stands for repeated, long-term, systematic and intensified harassment, which can be presented by different forms and intensities (Kopecký, 2010, further Criminal code, § 354). Stalker can for example stalk the victim for a long time, bomb the victim with text messages, e-mails, phone calls or unwanted gifts. When the attacker uses ICT we speak about cyberstalking. In this case it is sending of different messages through instant messengers (ICQ), chats, VoIP technologies, social networks etc. The attacker tries to arouse victim´s fear. Popular celebrities (singers, actors, and politicians), ex-partners and others are the most frequent victims of stalking. From January 1, 2010, stalking is considered to be a criminal act - it is qualified as dangerous stalking and it can be found in § 354 of Criminal Code.

Identifying the stalker is not such an easy thing to do and it is not very often successful. The person can behave absolutely normal within the society, even the closest neighbourhood does not have to know that the victim bothers other people through usage of internet or mobile phone. When we look at the aggressor's´ profile we will find out that the most frequent attackers are victims´ expartners (Dressing, 2005), more often men than women (87 % of male stalkers). We consider the female attackers to be more problematic, based on the weight perspective - this is mainly due to their purposefulness and systematicness. Most often, women realize the attacks through text messages.

Number of surveys realized among many Europe countries (e.g. Dressing, H. Maulk-Backer, H. Gass, P.) provides very interesting figures about stalking rate within the society. Anglo-Saxon surveys reports that 4 – 7.2 % of men and 12 – 17.5 % of women faced stalking in person. It means that stalking is relatively wide-spread phenomena. In the first German survey regarding stalking 11.6 % of questioned participants stated that they were at least once in their life in the position of stalker´s victim. According to the worldwide researches approximately 10 % of population have become victim of the stalking.

Stalking also occurs among the university students, but to a limited extent. Stalking, as a phenomenon, is not part of this research and so that we do not comment on it further.

3.1 Research of cyberbullying among university students

Researches of cyberbullying among university students prove that particular forms and behaviours of this phenomenon have become frequent part of a university life. Research by Finn (2004) presents one of the first studies focused on cyberbullying among university students. The research was realized on sample of 339 university students at University of New Hampshire. He came to the conclusion that 10 - 15 % of students have faced the cyberbullying. Occurrence of cyberbullying was within this study monitored just in relation to e-mails and instant messengers as the social networks representing basic technological platforms for realization of cyberbullying were not spread enough as it is at present. Dilmac (2009) also warns of cyberbullying among university students when he states that 55.3 % of university students confirm that they have become victims of cyberbullying at least once in their lives.

In 2008, Walker et al., who deal with the research of cyberbullying as well, realized an analysis of occurrence of cyberbullying among 120 American university students. Approximately 50 % of participants confirmed that they have already become a victim of cyberbullying.

Nursen Turan, Polat oguz et al. also deals with cyberbullying among university students. In 2011, they realized research involving sample of 579 university students (Istanbul Bilgi University Law School, Istanbul Ticaret University Law School and Marmara University Law School) at the age of 18 - 30. 59.8 % of survey participants have become the victims of cyberbullying, whereas 80% confirmed that they have been subjects to more than one form of cyberbullying.

Šmahaj, J. deals with problems of cyberbullying among university students within the Czech environment in particular and in 2011 he and his team realized research of cyberbullying within sample of 647 university students. According to the research, 14.8 % of participants stated that they have been faced to cyberbullying through mobile phone or internet at school or outside the school, whereas 6.6 % of participants have been faced to classic and cyber bullying at the same time.

Further interesting research results are presented by Vašutová (2010), who realized a research of cyberbullying together with her team among sample of 1030 students of University of Ostrava. Based on the results, 6.7 % of students at University of Ostrava have become the victims of cyberbullying.

1.2 Sharing of personal data on the Internet

Researches in the area of sharing of personal data on the Internet that have been realized abroad warn of a high percentage of children and adults sharing their personal data on the internet with no control, particularly within the environment of social networks. Within the framework of our study we will focus mainly on the target group of university students.

According to the official statistical figures of Facebook social network from 2005, 3.85 million of students of American universities had Facebook profile and this number represents 85 % of university students in the USA (Arrington, 2005). These students replied that they commonly share their basic personal data with other Facebook users, for example their name, surname and face photos, but also photos and videos.

Agazamani (2010) realized study among 595 Swedish university students when he monitored a way how the students spend their time on Facebook. The study also confirms high level of sharing of personal data within the environment of this social network. Agazamani (2013) further monitors which social networks are most often used by students. We can find Facebook, YouTube and Twitter at the first places.

Akyildiz and Argan (2011) also dealt with the use of social networks when they monitored behaviour of 1200 university students within the environment of social networks in Turkey. They confirm that Facebook is used by 93.8 % of Turkish university students (57.3 % of them have had the Facebook account active for more than 2 years). Akyildiz and Argan also reveal that average number of “friends” connected to students´ Facebook accounts varies between 101 to 300 friends (among 52.2 % of participants). Students use Facebook mostly by reasons of sharing their personal data and information, following photos, videos, events, contacting friends from a real world and also fun.

Shambare, Rugimbana and Sithole (2012) also realized research focused on usage of social networks, but this time in Republic of South Africa. According to their research, Facebook is used by 93 % of university students, further places were taken by the biggest African social network Mxit (used by 54 % of African students) and further Twitter and YouTube.

Based on the research College Students & Social Media that took place in several American universities and was realized by Tunheim company (2012), 96 % of American university students use Facebook, 84 % of students use YouTube and 20 % of students use Twitter. We also find interesting data revealed in relation to teachers: 91 % of teachers use social media (social networks and other similar platforms) as a support to their work - 57 % use Facebook, 49 % YouTube and 22 % LinkedIn. Detail information on research and other activities can be found at www.tunheim.com.

According to the Czech statistical data (Seznam.cz, May 2013) 73,771 university students share their personal data within the environment of one of the largest Czech social networks Spolužáci.cz. 20,877 of them are men (28.29 %).

1.3 Sexting

For the purposes of this publication we define sexting as *electronic distribution of text messages, own photographs or videos with a sexual content* (Kopecký, 2010-2012), *that takes place within the framework of virtual electronic media - Internet in particular.*

One of the first generally used definitions defines sexting as *act of distribution of photographs showing nudity among mobile phones or other electronic media, for example Internet* (Streichman, 2009). Other authors define sexting as sexual materials produced by young people (so-called youth-produced sexual images), which are onward distributed (Wolak, Finkelhor, Mitchell, 2011–2012). Further, sexting is defined for example by Sullivan (2011), who includes suggestive text messages or images showing nude or partially bare children or adults that are onward spread through phone or Internet. Streichman (2009-2011) supplements number of platforms and tools allowing distribution of these materials with social networks, Facebook and MySpace in particular. Within the Czech environment sexting is spreading mainly through social networks Facebook, Líbímseti.cz or through digital photo storage Rajče.net (Kopecký, 2011).

Since 2009 number of researches regarding sexting have been performed in number of countries - USA, Great Britain, Australia, Canada, China (Jolicoeur, 2010) and also the Czech Republic (Kopecký, Krejčí, 2010). Interesting results showing prevalence of sexting among young users of Internet and mobile phones are represented for example through research realized within The National Campaign to Prevent Teen and Unplanned Pregnancy (USA, 2009). Within the frame of this research realized through sample of 653 teenagers aged 13 - 19 it was proved that 38 % of them have sent sexual messages to other people and 19 % of the teenagers further sent their own photographs concerning their bare body to other people. Among adults at the age of 20 - 26 (627 respondents) more than 58 % have sent suggestive sexual sexting messages, whereas photo of their own naked body have been sent by 32 % of them. It is also interesting to follow the reasons of sexting carried out by teenagers - 71 % of girls and 67 % of boys send the sexual explicit content to their partners, sexting is then becoming a part of their intimate relationship. 21 % of girls and 39 % of boys sent the intimate photographs to person who they were about to meet with

(The National Campaign to Prevent Teen and Unplanned Pregnancy, 2010).

There have been only first probe surveys realized within the Czech environment that monitored occurrence of sexting among children population in particular. First researches monitoring current state in the area of sharing and distribution of sexual explicit content to other Internet users are represented by studies Danger of electronic communication 2 and Danger of internet communication 3 and 4 (Kopecký, Krejčí, Szotkowski, 2010-2012).

Obtained data give evidence of the fact that sexting has not been so far spread out within the Czech environment in a degree comparable to USA or other countries.

1.4 Cybergrooming and social engineering

Cybergrooming (child grooming, grooming) is represented by a behaviour of Internet users (predators, cybergroomers) that is meant to raise a fake trust of victim and force the victim to a personal meeting (Kopecký, 2010). As results of this meeting there can be sexual abuse of the victim, physical cruelty to the victim, abuse of the victim for child prostitution, creation of child pornography etc. Cybergrooming is thus a form of psychical manipulation realized through Internet, mobile phones or other related technologies[1] (Berson, I. R., 2002, O'Connell, 2001, further Kopecký, K., 2008 and others).

Cybergrooming is often connected to synchronous and asynchronous communication platforms, such as public chat, internet dating services, instant messengers and VoIP (e.g. ICQ, Skype) and for the past few years also to the social networks (Facebook, Twitter, MySpace, Bebo and others). According to the number of researches (CEOP[2], 2008 and others) cybergrooming most frequently takes place within the environment of instant messengers (56% of the cases), the next place was taken by social networks (11.4 of the cases).

We can assume that number of cybergrooming cases realized through use of social networks significantly increased. However, besides these communication environments internet predators also use advertising portals where they offer various earning or career opportunities to children (for example in the field of modelling). They often visit portals directly aimed at teenage Internet users (children portals, portals focused on free time activities, game portals and other websites).

Psychical cybergrooming manipulation is usually carried out for longer time - from approximately 3 months to several years. This time is direct dependent to the manner of manipulation and victim´s trustfulness. We can find cases when predator manipulated a child for 2 years until they met in person and the predator abused the victim sexually.

When we focus on diagnostics of the attackers, they present (according to the social status) a heterogeneous group where we can find users both with low and high social status. In many cases victim knows the attacker and the victim is dependent on the attacker (for 85-95 % of cases, see Kopecký, K., 2010). According to the recent studies, persons who do not have a criminal record present majority among the attackers, but however, attackers are sometimes represented by persons who have been previously convicted for sexual attacks against children or teenagers and we can speak about recidivism then (Choo, 2009). Among part of the attackers - sexual abusers - a disorder of sexual preference was diagnosed (paedophilia, hebophilia, ephebophilia). But it is not possible to associate the term paedophile with a term sexual abuser (Kopecký, 2010, Bartoněk, 2012)!

In some cases attackers themselves became the victims of cybergrooming or sexual abuse in their childhood, they were humiliated both by other children and teachers. Number of attackers grew up in an incomplete or non-functional family.

Within the Czech environment, cybergrooming is often associated with social engineering. However, for purposes of this publication we distinguish both terms. We understand the social engineering as a complex of strategies leading to manipulation with Internet user, to obtaining personal data and other sensitive materials from the user and others. Social engineering is thus a kind of group of techniques and strategies. However, primary goal of social engineering is not to abuse the child or adult sexually, social engineering can be aimed at for example get an access to a bank account, to obtain secret information etc. Cybergrooming then represents process using techniques of social engineering to force the victim to come for the personal meeting, whereas primary goal of cybergrooming is the sexual abuse of the victim.

With respect to the nature of target group of adult university students within the frame of this publication, we understand the cybergrooming only as **process of manipulative techniques leading to the personal meeting with the victim**, however, we do not distinguish whether the victim is a child (person younger than 18) or a student. Within the scope of manipulation of the students most of the techniques can be used for the adult Internet users too.

Basic techniques that can be used for manipulation of students are (Kopecký, 2009):

a) manipulation by means of mirroring[2], so-called mirroring,
b) sociotechnical methods for obtaining of personal data about the students, profiling of victim (phishing, pharming),
c) luring of victim,
d) manipulation using intimate students´ materials (without or with blackmailing) etc.

[2] Mirroring - manipulative technique based on imitation of victim´s behaviour. When communicating with the victim, the offender uses the same expressions and he behaves as a mirror image of the victim (therefore mirroring).

However, within university environment we also meet other forms of manipulation, particularly manipulation "from the perspective of power". It has two basic forms:

1. Student manipulates a teacher.

Relating to this form of manipulation, student (for example student in love) threatens a teacher with possible damage to the reputation (e.g. through revelation of their fictive relationship, damaging his reputation through fictive accusation etc.) if he does not meet the student. Further materials can be created at the meeting and they can be then used for blackmailing and manipulation leading to more intensive personal meeting.

2. Teacher manipulates a student.

Within this form of manipulation the teacher forces chosen victim (female student) to personal contact - a meeting - under threat of fail at exam or credit.

Both forms of manipulation can be realized both directly and through use of internet services. However, these forms of manipulation differ from the typical cybergrooming in several aspects - victim knows the attacker and an adult are manipulated by other adult person.

There is a conflict of interests for both above-mentioned forms of manipulation - specifically conflict of vocational and personal interest. Both situations are usually solved by ethical standards of a particular department/university, possibly within the criminal-law level through lodging a complaint for commission of a crime or a delict.

Cybergrooming is thus very tightly connected to so-called sexual harassment that was according to research *Sexual harassment within the university environment: occurrence and perception* (Charles University in Prague, 2008-2009) faced by approximately 3% of university students. Within the scope of this research more than 81% of students stated that they know a person who had to face the sexual harassment (Smetáčková et al., 2009). Similar results can be found within the research *Sexual harassment within university environment of Institute of Sociology of the Academy of Sciences of the Czech Republic* (2008-2009).

2 Research methodology

Description of research procedures includes research goals that are followed by research problems (questions), further description of research sample including research methodology, time schedule and method of data processing. For our research methodology proved within Danger of internet communication 3 and 4 (Kopecký et al., 2011-2012) was used.

2.1 Research goals and problems (research questions)

Research focused on occurrence of risky behaviour among the students of Faculty of Education of Palacký University in Olomouc, which is connected to information and communication technologies (Internet in particular), was at the descriptive level aimed at determination of number of victims and attackers involved in particular cyberbullying behaviours. At the same time, the research studied possibilities for help that would be used by victims in need (teacher, parent, sibling, and friend).

The research´s further task was to discover whether students communicate with unknown people on the Internet, if they were asked for personal meeting by these people and whether they are willing to meet virtual friend or familiar person in a real world. This is closely related to cybergrooming phenomenon.

Another goal was to determine forms of public sharing of intimate materials within Internet environment and to discover motivation of pubescent and adolescent people for such behaviour, it means sexting. We were also concerned in how many questioned children consider sexting to be risky and dangerous.

Regarding this, we focused on sharing of personal data of future teachers within Internet environment (particularly face photos) and on their knowledge of social networks. That is to say those social networks represent place of frequent cyber attacks that are realized through use of private information shared with particular users and also through data that are obtained by attackers thanks to the failures of social networks' security.

Research problems (research questions) were following:

A. What is the number of cyberbullying victims in relation to its individual behaviours and platforms on which the cyberbullying takes place?

B. What is the number of cyberbullying initiators in relation to its individual behaviours and platforms on which the cyberbullying takes place?

C. Which communication platform is most frequently being used for cyberbullying?

D. Who is the person contacted by a victim of cyberbullying?

E. How many university students would go to a personal meeting with internet friend if they were asked to?

F. How many university students were invited for a personal meeting by an internet user without verified identity?

G. How many university students came to a personal meeting with an internet user without verified identity?

H. How many students placed material with own sexual content on the Internet?

I. How many students sent their own materials with sexual content to other people?

J. How many students perceive sexting as risky and dangerous?

K. Which personal data are most frequently shared by students of Faculty of Education of Palacký University?

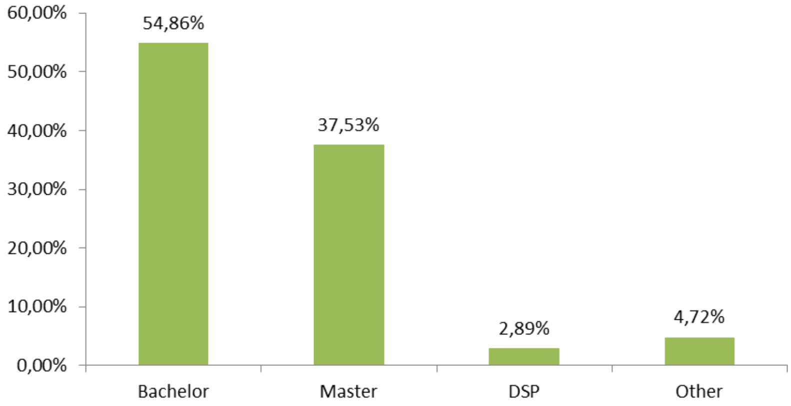
L. Which personal data are most frequently sent to other Internet users by students of Faculty of Education of Palacký University?
M. How many students were asked to send face photos by other Internet user?
N. Which social networks are known by university students?
O. Which social networks students use for their accounts?

2.2 Research sample

Basic selection was formed by students of Faculty of Education of Palacký University in Olomouc that were addressed for participation in the research through communication channels of Palacký University in Olomouc and further through E-Synergie (www.esynergie.cz) and E-Bezpečí (www.e-bezpeci.cz) project websites. These web sources are frequently being used by students of Faculty of Education.

386 students of Faculty of Education of Palacký University in Olomouc were involved in the research. From the sample, 16.75% were men, 83.25% were women. The most students were at the age of **20 - 25** (86.7% from the total sample). Sample distribution according to the individual study programmes approximately corresponds to distribution of enrolled students in 2011 and 2012 (see Annual activity report of Faculty of Education of Palacký University for the years 2011 and 2012).

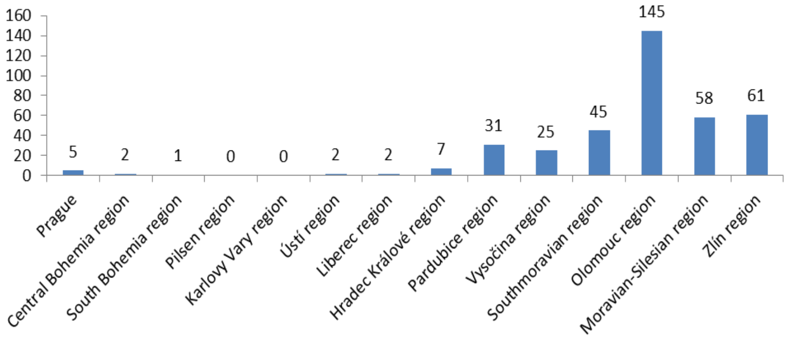
Graph No.*1 *Respondents according to the study programmes



Note:
Answer “other” involves participants of programmes of lifelong education, including students of supplementary and extending study programmes.

Graph No.* 2 *Research sample (regional distribution)

Following graph shows overview of respondents according to the particular regions. Olomoucký, Zlínský and Moravskoslezský regions prevail.



n=385

2.3 Research methodology

Research was aimed at quantitative perspective and questionnaire method was selected as an initial research procedure.

Research tool comprises of **71** items in total (40 dichotomic items, 2 polytomic items, 22 multiple answer questions and 7 open items) that were created based on the theoretical knowledge and that were arranged to reflect the set goals and arisen problems.

The questionnaire was distributed to the respondents electronically (Online) through questionnaire system of E-Bezpečí project, further through university direct email, Faculty of Education of Palacký University website and also through Facebook social network.

Anonymous questionnaire automatically verified where the questionnaire was sent from (IP address, regional citizenship, monitoring of respondents´ behaviour through Google Analytics tool etc.).

2.4 Research time schedule

Research preparation was started on the November 1 2012, data collection ran from the December 1 to January 31 2013. Data evaluation was realized during February and March of 2013.

2.5 Data and statistical tests

Obtained data were mainly at the nominal and ordinal measuring level, which corresponded to its consequent processing, used numerical operations and statistical processing.

First of all we sorted and arranged the data to the table of frequencies.

Descriptive problems were being solved through use of elementary quantities of descriptive statistics (calculation of location characteristics - central tendency rate, percentage calculation) and neither the graphic representation was missing.

To test the hypothesis we used chi-squared independence test for four-field table. The whole testing was performed at level of significance $\alpha = 0.05$.

3 Research results

3.1 Cyberbullying among university students

Basic pillar of research on risky behaviour among Czech university students within Internet environment lied in the description of forms of cyber aggression.

Within the scope of our research we focused on the following areas:

A. Victims of cyberbullying
We observed number of victims in relation to cyberbullying individual behaviours and platforms on which the cyberbullying takes place. We further observed change over the roles of victim and aggressor.

B. Initiators of cyberbullying
We observed number of attackers in relation to cyberbullying individual behaviours and platforms on which the cyberbullying takes place. We also observed change over the roles of victim and aggressor.

C. Persons involved in solving of cyberbullying
The research aimed at persons that would be contacted by the victims of cyberbullying.

D. Cyberbullying behaviours in dependence on use of social networks (Facebook in particular)
The research observes linkage between cyberbullying and use of Facebook social network.

E. Other related phenomena
Further, research follows specific forms of virtual aggression carried out for example through account breakthrough, identity theft and consequent cyberbullying.

Descriptive data are supplemented with concrete cases which were brought by students of Faculty of Education of Palacký University in Olomouc to our advisory centre. Due to the privacy protection of the clients we do not release real names of persons involved in the cases, although the case description is authentic.

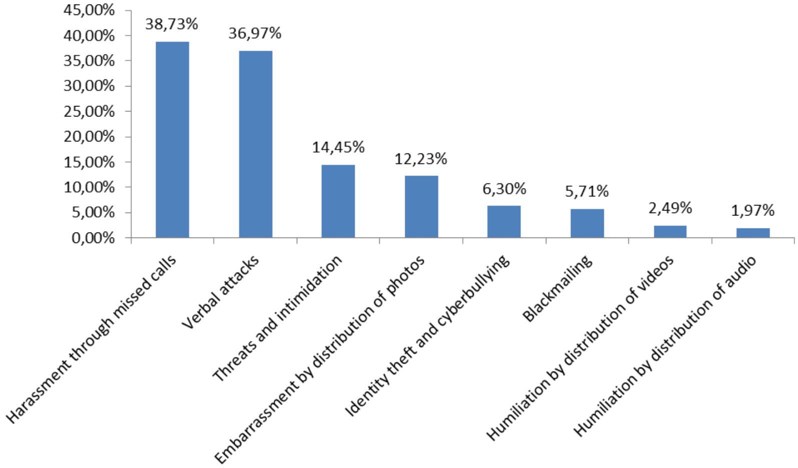
3.1.1 Cyberbullying among students of Faculty of Education of Palacký University in Olomouc - victims

Within the research, the following forms of attacks included in the area of cyberbullying were observed:

A. Verbal attacks in cyberspace - harm through humiliation, offending, taunting, embarrassing of a student (verbal aggression).
B. Threats and intimidation of a student.
C. Blackmailing a student.
D. Identity theft followed by cyberbullying.
E. Harassment through missed calls.
F. Humiliation, embarrassment realized through distribution of photography.
G. Humiliation, embarrassment realized through distribution of a video.
H. Humiliation, embarrassment realized through distribution of an audio recording.

In practice, there is a combination of particular forms of an attack - to reach the highest intensity.

Graph No.* 3 *Students as victims of cyberbullying



n=376 (detailed sums of respondents can be found further in the text)

Cyberbullying - harassment through missed calls

In spite of the fact that cyberbullying realized through harassment or missed calls is considered to be one of the modest and least dangerous forms of cyberbullying (this form is not included in the cyberbullying behaviours within the scope of some studies) we decided to include this form with respect to its range to the cyberbullying behaviours. **38.73% of students** of Faculty of Education of Palacký University in Olomouc experienced cyberbullying realized through missed calls in position of victims (namely 134 out of 346 students).

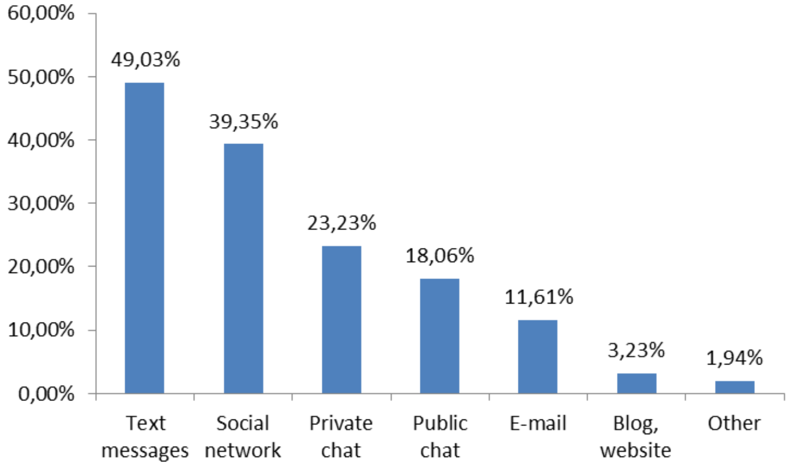
Sample situation

Denisa is a student in the second year of teaching field of study in bachelor study programme. Two months after start of summer term she began undergoing cyberbullying realized through missed calls. An unknown person repeatedly gave the student missed calls from an unknown telephone number. Missed calls were repeated 20-25 times a day on average, most frequently in the evening when she stayed at her dormitory. She answered the phone for several times but she could hear just sound of a human breathing ("puffing"). The unknown person did not respond to her questions. Consequently, Denisa tried to contact the caller through text message, but with no response. This situation lasted for more than 5 weeks. Denisa tried to identify an owner of the telephone number for several times, she tried to search on the Internet and also to contact a provider of telephone services. When she contacted E-Bezpečí advisory centre, she blocked the telephone number of an unknown person (put it to a blacklist). However, the missed calls continued for another 3 weeks using a different number, the scenario remained the same. Denisa blocked the new number once again and after 2 weeks the missed calls stopped.

Cyberbullying - verbal aggression

The most widespread "classic" cyberbullying form is represented by various aggressive behaviours that are repeatedly realized against the students in a verbal form and with increasing intensity. Cyberbullying based on this form usually takes place within the environment of social networks or through text messages, less frequently by means of email or other communication services. Cyberbullying in form of repeated long-term verbal aggression was experienced by **36.97% of respondents** (139 out of 376).

Graph No.* 4 *Platforms most frequently used for realization of cyberbullying in form of verbal aggression.



n=155

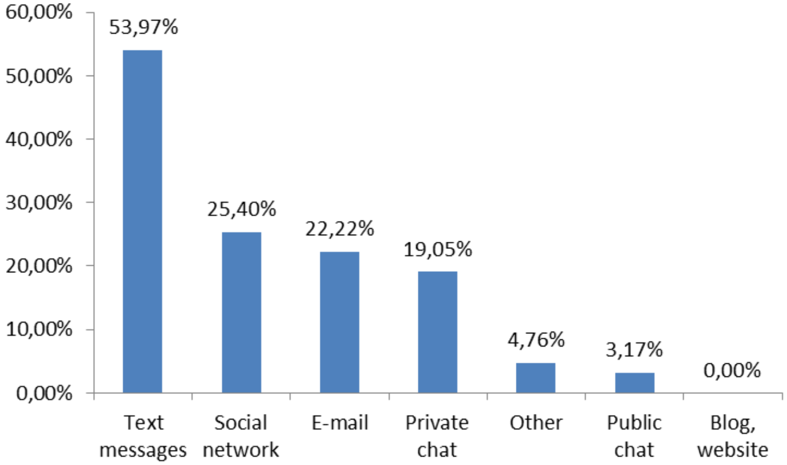
Sample situation

Jitka, student in the second year of teaching field of study on magister´s degree, was an introvert girl isolated from the rest of her study group. She almost never expressed herself at school. She was also different from the others in a way she used to dress or communicate (she spoke very standard or even hypercorrect Czech) and she exceeded others in her knowledge. Three fellow students set up a Facebook discussion group about her where they made fun of her, offended her, criticised her speech and sent abusive messages. They were also sending some of the messages to her mobile phone through anonymous website SMS gate. Discussion group originally meant to be closed became public and more than 30 additional Facebook users took part in the cyberbullying.

Cyberbullying - threats and intimidation

Another widespread form of cyberbullying is presented by threats. Threats move cyberbullying intensity to the higher level as it brings a new element to cyberbullying process - intensive fear. While verbal forms of cyberbullying focus mainly on the intensive humiliation of the victim without arousing fear (particularly fear for life, close family, pets etc.), threats and intimidation are aimed primarily at arousing fear. Threats and intimidation were experienced by **14.45% of respondents** (51 out of 353).

Graph No. 5 **Platforms most frequently used for realization of cyberbullying in form of threats and intimidation**



n=63

Sample situation

Marie, a student in the fourth year of teaching field of study on magister´s degree, was during January and February 2012 repeatedly contacted by an unknown internet user through text messages sent from an anonymous internet SMS gate. Anonymous author wrote to Marie: *I know what you are doing. I am watching you. I saw you on the street today. I will have sex with you, bitch. Do you want to feel pleasure? I will fuck you. You will know the pain etc.* The threats were intensifying and each time they were sent from the Internet. Marie received more than 300 messages during 3 months. Under this pressure she was even forced to change her telephone number. The threats were stopped.

Cyberbullying - humiliation and embarrassment through distribution of photographs

Cyberbullying realized through use of photo of a victim is quite common form of cyberbullying that belongs due to its intensity and orientation to the higher level of intensity and dangerousness than previous followed forms. This is caused particularly by existence of victim´s concrete touchy material (photos) that can be spread between large numbers of Internet users (including users who do not know the victim). Attackers often perceive this form of cyberbullying as form of teasing, as a positive way of communication which is meant to entertain the victim and at the same time make the victim tougher. However, boundary between teasing and cyberbullying is very vague and an unsuccessful joke grows into an intensive cyberbullying with wide audience on the margin of viral spreading of discriminating materials.

Compromising materials are commonly presented by photographs of drunken, vomiting students, sexual explicit photographs - images of naked victims, photographs discrediting students´ or teachers´

relationships, photographs focused on homosexual relationships, ethnical minorities and others.

Identity theft and cyberbullying

Identity theft represents a specific form of cyberbullying when an attacker firstly infiltrates victim´s account (for example e-mail account, social network account, account in MMORPG game and suchlike) and he/she then realizes attacks on other Internet users under the name of a victim. Account attacks were confirmed by **32.24%** of respondents (116 out of 349), **18.64%** also confirmed that their account was used for cyberbullying of other people. Identity theft used for cyberbullying was experienced by **6.30%** of questioned students.

Cyberbullying - blackmailing

Blackmailing represents a very intensive and dangerous form of cyberbullying that is being confirmed by approximately **5.71%** of respondents.

Cyberbullying - humiliation through distribution of video recording

2.49% of respondents stated that they experienced cyberbullying realized through distribution of a video recording. The video was spread by means of common communication channels - Internet and mobile phone.

Cyberbullying - humiliation through distribution of audio recording

At the imaginary end of our scale of the most common forms of cyberbullying we can find humiliation through distribution of audio recording that was in the position of victim experienced by **1.97% of respondents**. In this case we talk about a recording that records a victim in a humorous situation and it is possible to recognize victim´s identity. Recording can be consequently used both for humiliation or blackmailing.

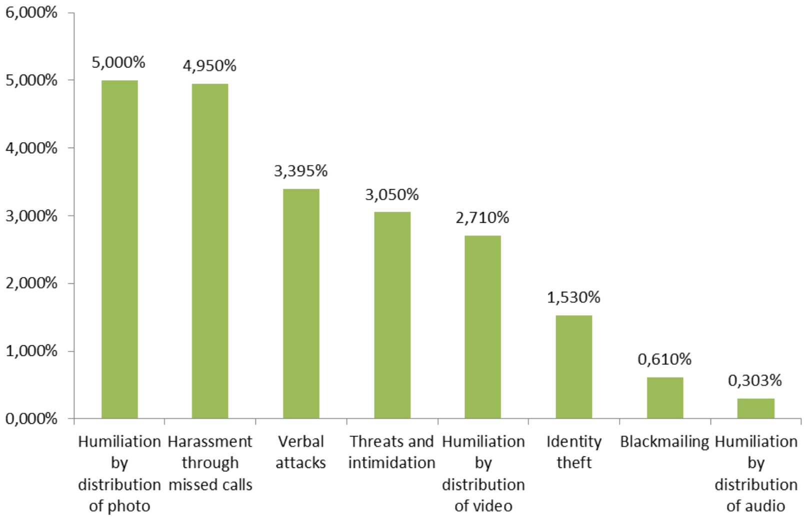
Other forms of cyberbullying

Among other forms of cyberbullying we can classify **cyberbullying focused on players of computer games** (MMORPG in particular), where the players are not only bullied by other players, but also subjects to various frauds, thefts of game characters, thefts of virtual items, trading of stolen goods etc. It is required to realize that “virtual items and game characters” are of value comparable to standard money and that they are commonly being trade. In many countries, WoW worlds are interconnected with real worlds; virtual products can be thus sold and purchased for real money. Amounts paid for unique virtual items come up to several hundred or thousand dollars per item. One of the best known virtual items that was sold for real money was (and it still is) Spectral Tiger, special kind of a mount, it means an animal used for riding in WoW. This virtual creature can be bought at EBAY auctions for price of 400 up to 9,999$ (Kopecký, 2012).

3.1.2 Cyberbullying among students of Faculty of Education of Palacký University in Olomouc - attackers

Within the scope of our research we also examined whether the students play a part in cyberbullying as the initiators. 15.00% of students confessed that they tried to realize one of the monitored cyberbullying forms. Other forms of cyberbullying from the perspective of attackers are systematically arranged within the following graph.

Graph No. *6* ***Students as initiators of cyberbullying***

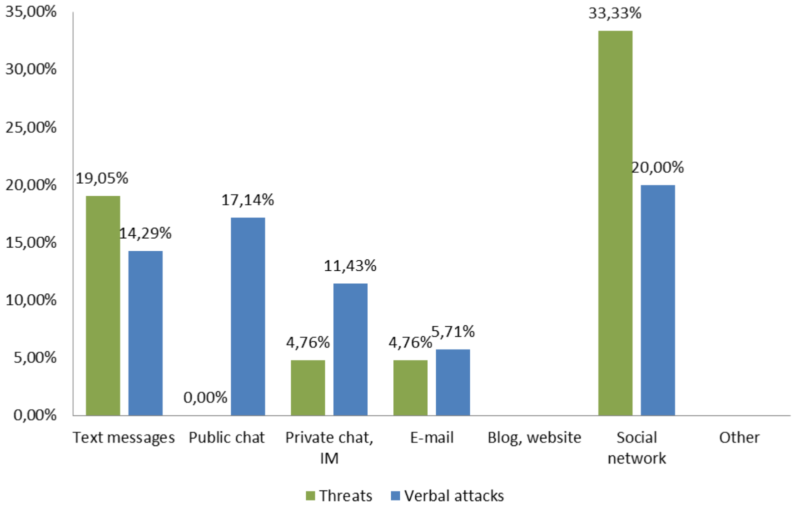


n=340

The most frequent form of cyberbullying realized by students of Faculty of Education of Palacký University in Olomouc is represented by **humiliation of a victim through distribution of photographs which was tried by 5.00%** of respondents. Other places were taken by harassment through missed calls, verbal forms of cyberbullying, threats and intimidation of a victim and humiliation through distribution of a video recording.

It is also interesting that equal **41.10% of students got into an electronic account without owner´s permission**, whereas 3.68% of them used the account to attack another person (so-called attack realized through identity theft). Based on the whole sample, 1.53% of questioned students tried an identity theft.

Graph No.* 7 *Comparison of communication platforms used for realization of verbal cyberbullying forms and for cyberbullying realized through blackmailing

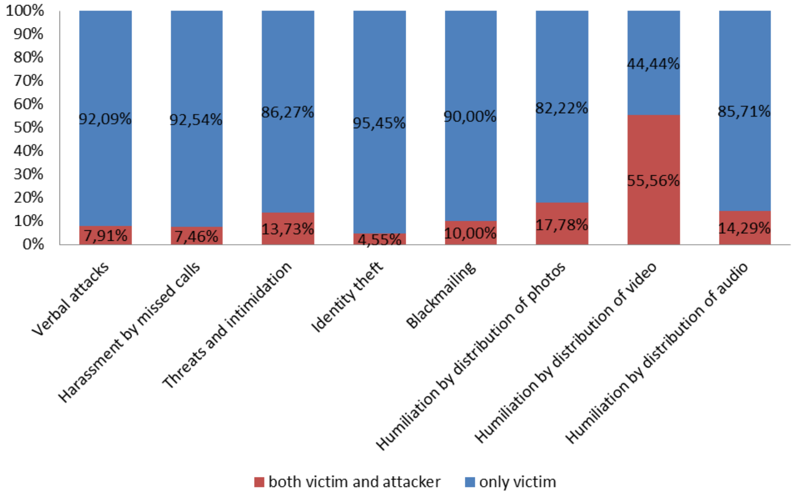


$n_{\text{blackmailing}}$=21, $n_{\text{verbal aggression}}$=35

3.1.3 Comparison between victims and attackers

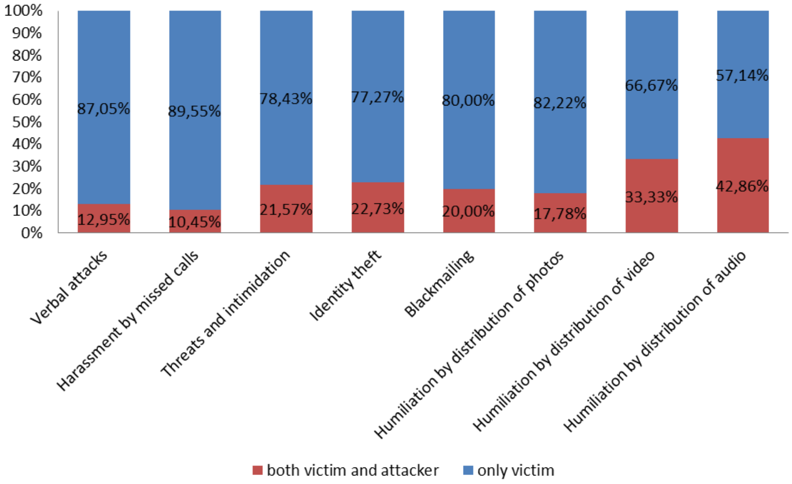
Following graph shows how many percents of victims became attackers using the same form of cyberbullying that was experienced by the victim. For example 55.56% of victims, who experienced cyberbullying realized through distribution of embarrassing video recording, tried the same in the position of attacker.

Graph No. 8 *Victims who become attackers (form of cyberbullying remains the same)*



Next graph shows how many victims of individual cyberbullying forms tried any form of cyberbullying to attack other person. In other words - in case the student experienced cyberbullying as a victim whether he/she tends to try the attack also in the position of aggressor.

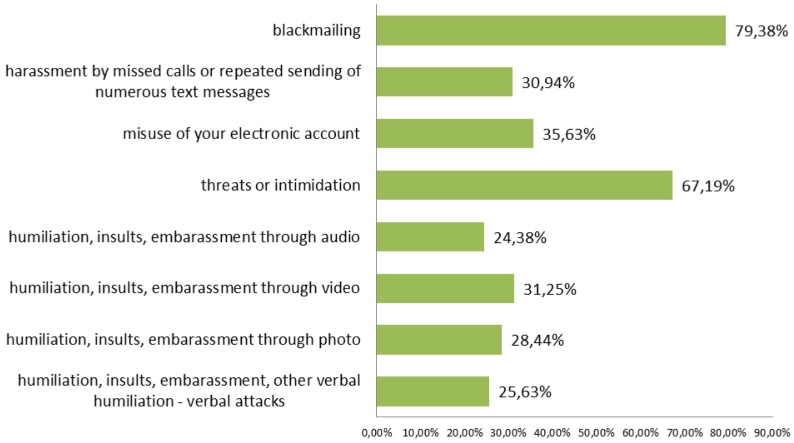
Graph No.* 9 *Victims who become attackers (random form of cyberbullying)



3.1.4 Involvement of other persons to cyberbullying solution process

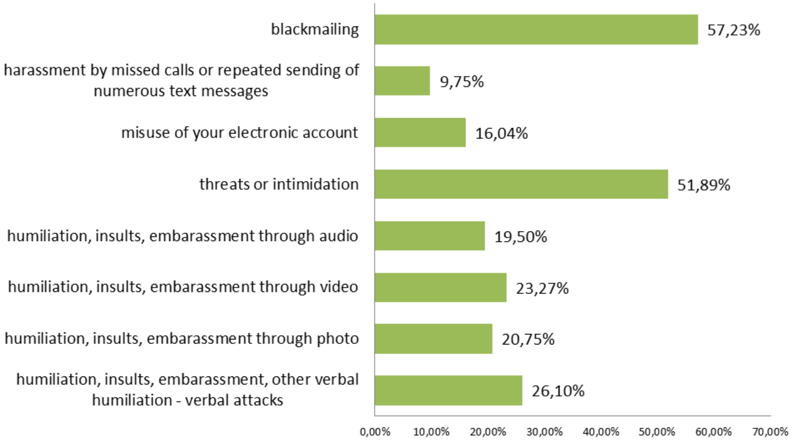
Within the frame of our research we were also interested in who would the students - victims of cyberbullying - turn to for help. Number of students contacts their own parents not before the intensity of cyberbullying attack is so high that the victim cannot solve the situation on its own. Students do not contact Police of the Czech Republic in these cases in general.

Graph No.10 Forms of cyberbullying which would be solved by students with their parents



As we expected, students would solve with their parents mainly more serious forms of cyberbullying, such as threats or intimidation (67.19%). Only ¼ of the students would commit themselves to parents with cyberbullying realized through verbal attacks.

Graph No.11 Forms of cyberbullying which would be solved by students with their teachers



3.2 Personal meetings with Internet users

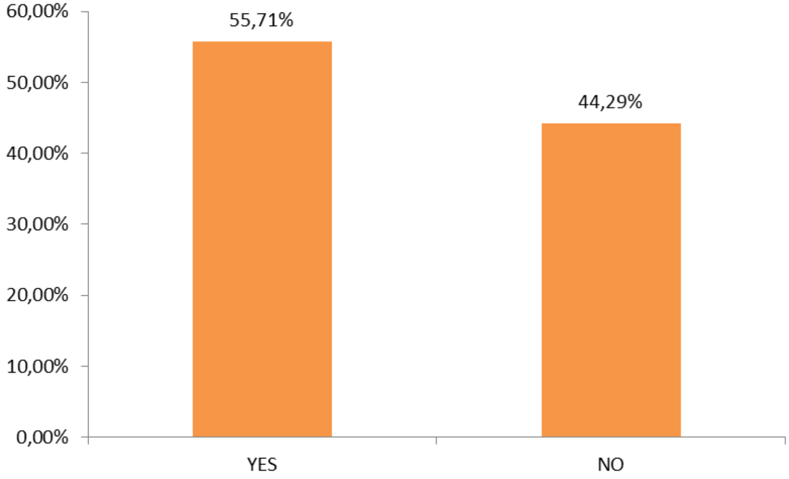
Research on risky behaviour of university students was also focused on students´ willingness to communicate with unknown persons with unverified identity within the Internet environment and also on their reactions regarding invites for personal meetings. More than half of the students communicate with unknown people without verified identity, namely **46.49%** of students of Faculty of Education of Palacký University in Olomouc.

90.94% of students stated that they **do not add unknown persons** to their social network profiles when they ask them to do so.

Not every communication with unknown people on the Internet has to be for university students a priori dangerous; it does not have to lead for example to sexual abuse. However, in number of documented cases (see Chapman case, 2010 and others) this behaviour led to sexual abuse of a student. Therefore we aimed in our research not just at the communication with people of unknown identity, but also at the process of personal meeting itself, possibly at its consequences.

First followed parameter was represented by willingness of student to come to the personal meeting. We thus asked the students whether they would be willing to come to the personal meeting with their Internet acquaintance (who they do not know from a real world). Results are presented by the following graphs.

Graph No.*12 *Willingness to come to a personal meeting with Internet acquaintance (we do not know the acquaintance in a real world)

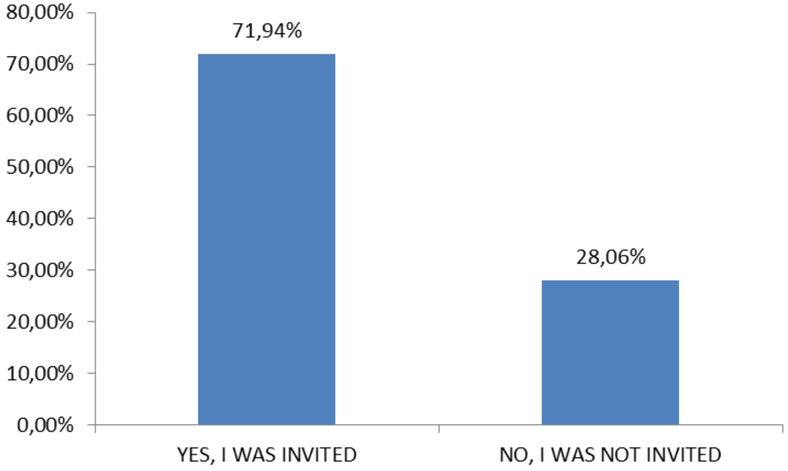


n=140

More than half of the respondents (**55.71%**) are willing to come to the personal meeting with an Internet acquaintance just on the basis of information which were provided to them through virtual Internet world.

In the next part of our research we monitor whether the students were really invited for the personal meeting and whether they attended it.

Graph No.13 Invitation for personal meeting with an Internet user

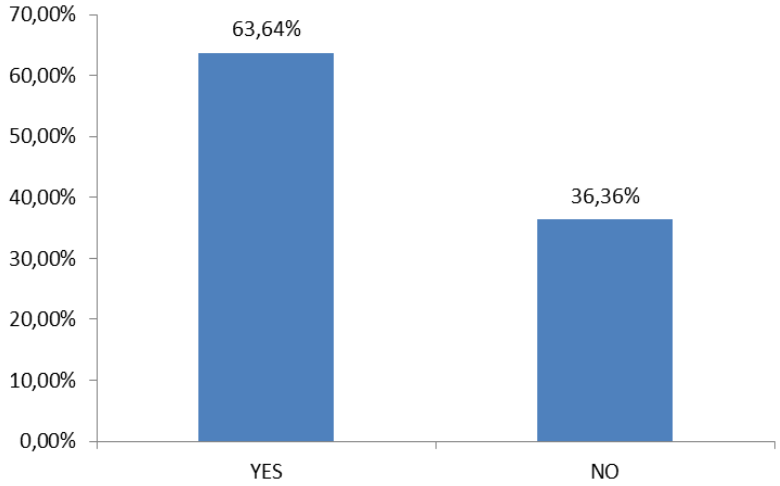


n=139

71.94% of questioned students were invited for personal meeting in 2012. This is an expected result as students of Faculty of Education of Palacký University in Olomouc comprise of more than 80% of sexually active women and many of them own social network accounts (Facebook in particular). So they present favourite and sought out targets of internet dating.

Fact that the students were invited for a personal meeting by other Internet users does not mean that the meeting has to come to sexual abuse, rape etc. Invitation for a meeting and meeting itself can be an ordinary part of interpersonal interaction, but in relation to this text we perceive personal meetings as potentially risky, not as risks themselves.

Graph No. 14 Realized personal meetings



n=99

More than half of the invited students came to the personal meeting, it means 63.64%. When we extrapolate the result towards a question focused on invitation for the personal meeting, we will find out that 45.32% of the students of Faculty of Education of Palacký University in Olomouc went to the personal meeting with unknown people. It is also interesting that 6.45% of students were asked by their Internet friends not to tell anyone that they talk to each other and also what they talk about.

To keep the research balanced we were also discovering whether our respondents invited their Internet friends for a personal meeting too and whether they asked them not to tell anyone that they talk to each other and what they talk about. About 10% of students asked their Internet acquaintance to keep their communication secret. Further, 40% of questioned students invited their Internet acquaintances for a meeting.

In case that the students would really want to come to the personal meeting, they would most frequently confide to their friends (39.51%) and parents (32.10%), no student would contact a university pedagogue. 17.28% of the students would keep the meeting in absolute secrecy and they would tell nobody about it.

Almost 3/4 (74.5%) of the respondents consider communication with unknown Internet users to be risky or dangerous, 85.99% of the students subsequently consider personal meetings to be dangerous.

3.2.1 Why we consider the personal meetings risky

As it was said, most of respondents are aware of risks connected to the personal meetings with unknown Internet users. Unverified identity of Internet users, potential deviant behaviour of a stranger, risk of an assault, kidnap or even a murder represent most often arguments for this statement.

Some of the answers of respondents
(the answers were not put through language correction)

- *We never know who can come to the meeting, it does not have to be a beautiful 18 year old lady, but for example an ugly 40 year old man.*
- *We can never know what the person is like for real, if he/she does not hurt us, steal from us and the like.*
- *The unknown person can behave pathologically and hurt me or my close friends and family.*

- *It could be a pervert.*
- *I never know what the people are like. When it is a person who neither I nor my friends know, I cannot be sure that the person will not hurt me. Therefore when I go for a meeting with somebody, I make sure that the person is telling the truth (through our mutual friends etc.). Generally speaking, I do not go for the meetings like these and I do not search anybody for purposes of this or similar character.*
- *On the internet nobody knows who is who, everybody can get a fake photo... there are many paedophiles over there.*
- *I don´t know what kind of person it could be, what he/she wants from me and if it is just an innocent date.*
- *When I don´t know the person, I cannot know what to expect and therefore I wouldn´t go for any meetings with a stranger who I know just from the Internet. It could be a rapist and I would barely defend myself if he wanted to hurt me.*
- *We never know who is hiding behind the profile, photo does not have to be real, personal life can be stolen from someone else. It is risky. The meeting should take place at a crowded cafe, possible in presence of a friend, there is a big risk when we do not know the person, his/her reactions etc.*
- *I do not know these people - it could be anyone, a rapist, murderer, paedophile, burglar. I would never meet such a person in this way, I absolutely cannot predict who will really come.*
- *Unfortunately, a lot of people are very careless, they share any information about themselves and they then cannot be surprised when something unpleasant happens. I dare to say that I have common sense and there is no danger for me.*

- *It does not have to be a person that he/she pretends to be, first of all these people are usually strangers that are known for their rich criminal records.*

- *Assault, rape, murder.*

- *These are the people I do not know in person therefore I consider the meeting risky. But when we choose an appropriate place of the meeting (it means public place) and we are cautious, then the risk of such a meeting decreases.*

- *Internet is an anonymous place. For that reason, someone different from the person showed on the social network can come to the arranged meeting. In my case I usually knew who the person I was meeting was as I got information from other people and therefore I knew what is awaiting me. But I admit that meeting with an unknown person through Internet agreement is dangerous. It is necessary to be careful.*

- *When I know the person for short time (just couple of months), it is dangerous then. He/she is untrustworthy.*

- *Name, photo and all other things stated on the Internet/Internet profile does not have to match a real person. There could be hidden some dangerous individual behind the "fictive" profile.*

- *We never exactly know what the person is like.*

- *We cannot trust somebody with whom we have a conversation just over the letters. There can be exceptions, but definitely there happen and happened many wrong things hurting people... I am not afraid of Internet communication with people who I know at least by sight although this is maybe risky as well... however, I don´t understand children at the first grade having their social network profiles... these* *kids don´t know anything about reality and they put and write anything on their profiles...,*

- *I can never know what kind of freak will turn out, nevertheless I know that I am able to defend myself and I never arrange meeting in a place where I couldn´t "escape".*

- *When communicating on Internet, social networks... anybody can pretend to be someone else (regarding visage, age, interests, character etc.). There is a risk mainly for trustful teenage girls who can agree with the meeting and many of these meetings did not come right (bodily harm, death...).*

- *One never knows who is on the other side of a monitor, it is hard to answer this question, but the given person can endanger you in many ways. In my opinion, there is a big risk for teenagers and also girls at the age of 19, 20 and as I am a guy I would sometimes go for a meeting, I have higher chance to defend myself etc.*

- *To make it clear: it depends on what communication took place and where we met. When I send an email to person who I will find information about on the Internet and the person will recommend me to contact Mr. XY on email address XZ to arrange a meeting for purposes of my research at the institution where the person works, I will do it so. When I receive an email from an unknown person who wants to join Christian prayer group that I administer, I will reply to that email and I will invite the person for personal meeting. I don´t talk to strangers and I don´t read spam emails.*

3.3 Sexting *among university students*

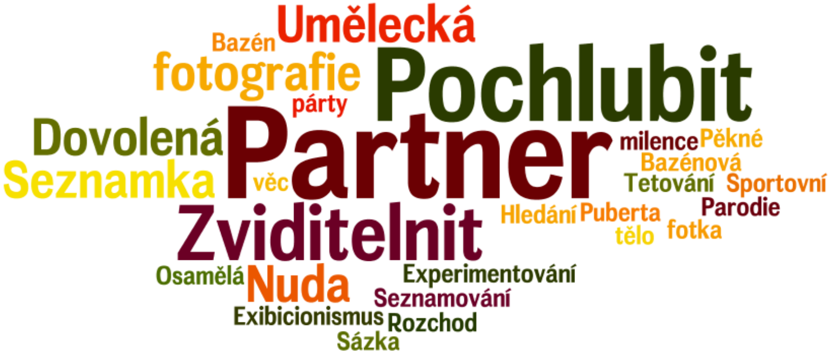
Research on risky behaviour of students at Faculty of Education of Palacký University in Olomouc also monitored problems of sexting as a specific form of sexual behaviour within cyberspace. Foreign studies prove that occurrence of sexting in the population of adolescents reach within various studies level from 20 to 70% (The National Campaign to Prevent Teen and Unplanned Pregnancy, 2010), it depends on a specific form of sexting and also on the sex of sender or receiver.

Within the scope of our survey we observe occurrence of sexting in two basic forms - in the form of public sharing of own sexually explicit materials (photographs/videos) on the Internet and in the form of sending these materials to other persons through Internet services.

Sexting in the form of sharing of own sexually explicit photographs or videos (on which student is partially or completely undressed/naked) within Internet environment is being realized by **12.42%** of students.

Reasons, which were given by the students for realization of this form, were visualized to the form of word cloud.

Graph No. 15 *Reasons for sharing of own sexually explicit materials on the Internet (Word Cloud)*



Translation of the most frequent words of word cloud:
Partner, Show off, Draw attention, Holiday, Boredom, Art, Dating service

Answers of respondents that actively perform sexting are visualized within the previous word cloud. The most frequent reasons for realization of this form of sexting are: *sharing of photograph within the frame of partnership, further desire to show off, possibly to draw attention to oneself.*

More than one fifth of the students (23.28%) also **sent their own intimate materials to other people through internet services.**

Graph No. 16 *Reasons for sending of own sexually explicit materials through Internet services (Word Cloud)*

Seznamka
Kamarád
výměna
Milenec
Profesionální
Opilost
Láskování
Vtípek
Flirt
sexu
Exibicionismus
láska
Laškování
vzdálenost
odloučení
Umění
nabídka
Přiteli
Erotika
abych
dlouhého
radost
zahraniční
Nátlak
dálku
Oboustranná
Udělat
mu
km
partnerů
stáže
Sex
vztah
Zamilovanost
dojem
důvodu
zaujmout
Partner
focení udělala
Snaha
Přítel

Translation of the most frequent words of word cloud:
Partner, Boyfriend, Mutual, Exchange, Erotic, Dating service, Flirt

The most frequent reasons for sending of own sexually explicit materials to other Internet users are: *sending the materials to a partner, friend or acquaintance, further reasons are mutual exchange of photographs (not specified with whom), application of the photo for Internet dating service, possibly flirting.*

As an illustration we provide several open answers from our respondents:

- *It should have been a professional photographing. Unfortunately it was not and my photo appeared on Lide.cz and it caused big problems to me. I suffered mentally mostly. Even today I can feel that it affected me in a certain way. I had confidence in the mentioned person. I was young and stupid.*

- *A friend of mine wanted to paint a picture of me due to entrance exams for college, I send photos of my body to him in advance to let him know what he should make provisions for.*

- *To my boyfriend by reason of long separation due to his placement abroad.*

- *I was looking for a lover.*

- *To my partner who I´ve been dating for many years and I knew that he would not use the photo for other purposes.*

- *He also sent me a photo and I wanted him to admire me.*

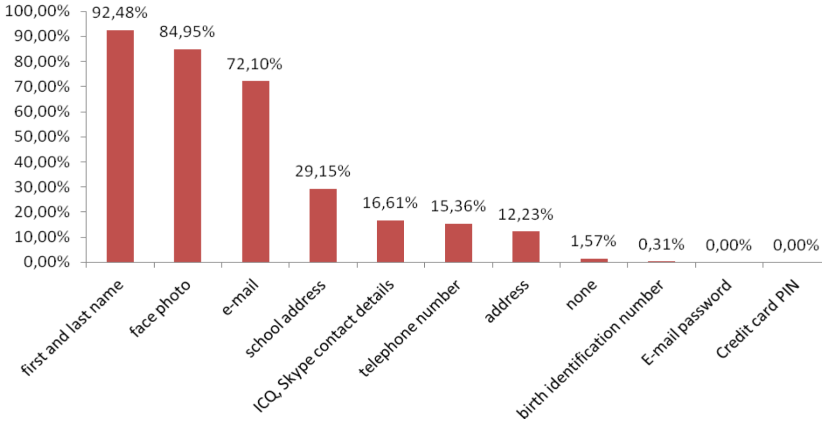
- *It was a very close person who I trusted and we couldn´t meet in person for certain time.*

3.4 Sharing of personal data among university students

Another category that was covered by our research is sharing of personal data among university students. We were concerned with personal data that students share on the Internet and that they are willing to share with people without verified identity with whom they communicate over Internet environment.

Access to personal data have considerably changed over the past years - private information have become public mainly with arrival of social networks where users started to create their real profiles containing true personal data. For example on Facebook or Google+ social networks most of the users use their real first and last name whereas estimated number of fake accounts varies between 10-15% of all accounts (data regarding Facebook social network).

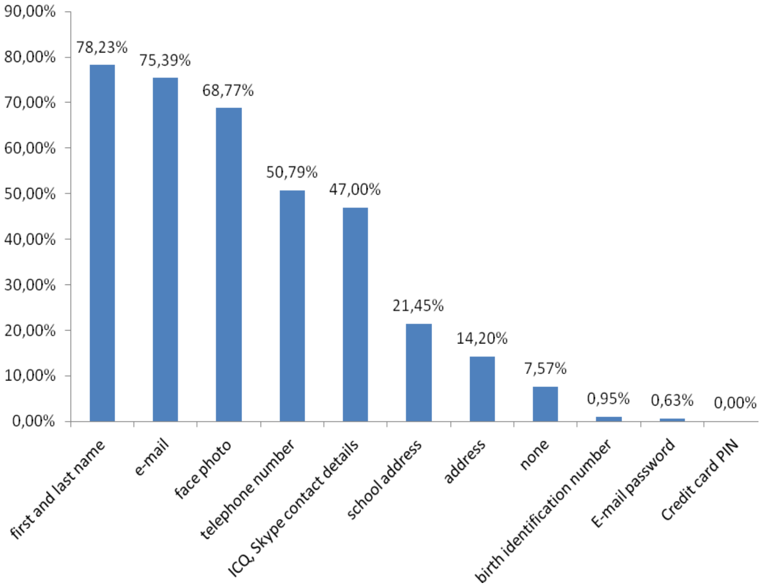
Graph No. 17 ***Personal data shared by students on the Internet***



n=319

Personal data that are mostly shared by students within the Internet environment are first and last name, face photo and e-mail. Students logically do not share personal data such as e-mail account password and credit card PIN.

*Graph No.*18 *Personal data that students are willing to send to other Internet users without verified identity*



n=317

As well as in the previous graph, the first and last name, e-mail and face photos belongs to personal data that students are willing to send to other Internet users without verified identity. In other places we can find telephone number or contact details to instant messengers. It is interesting that face photo is considered to be commonly shared and sent out personal detail although there is a high risk of its possible misuse. We were therefore concerned whether students were asked to send their face photo on the Internet and whether they responded to the request.

Sharing of face photographs

More than half of the respondents (53.65%) were **requested** by their Internet acquaintances (who they never met in a real life) **to send their face photographs.** This request was then accepted by 70.83% of respondents. These respondents also sent the real face photographs to the mentioned users.

We also followed whether the respondents of our research also ask their Internet acquaintances to send them facial photos. This request was confirmed by more than a third of them, namely 35.19%.

With respect to the fact that face photos are considered to be a highly sensitive personal detail (Kopecký, Szotkowski, Krejčí, 2010-2012) which can be quite easily misused for various attacks on a child or adult, we also focused on how the risks connected to the sharing of this photography type are perceived by our respondents. **More than 3/4 of the respondents are aware of the risks of sending or distribution of the face photos (77.19%).**

Selected opinions of the students regarding risks of sharing of face photos are introduced below:

- *It can be misused for example for some photomontage. Through this someone could for example choose a child "to be sold".*
- *By reasons of looking up and possible blackmailing, body harm.*
- *To create a fake identity.*
- *It can be misused, you can change a lot of things through Photoshop so people can be blackmailed then.*
- *On the basis of the photo I can be identified without a problem in a real life and they can hurt me personally as well.*

- *It can be misused in a way that somebody will create a caricature or other embarrassing "photo" from my face and this is not pleasing for anybody.*

- *The photo can be used to our detriment-photomontage etc. and consequent blackmailing. It does not have to be the person who I am writing to and this is a risk from the point of view of my photo,*

- *Based on the appearance I can by recognized in a real world by person from the Internet (e.g. at school, on the street). I can be for example stalked.*

- *Since the person can further distribute my photo.*

- *Takeover of identity-photo as evidence, mean for recognizing of a victim for possible accomplices in case that they are planning physical of psychical attack.*

- *By reason of misuse or later work offer (inappropriate photos, although they are imaginarily available "just" for selected users).*

- *Since we revealed our identity through the photographs, we cannot now claim that we are not the person from the profile. and the photo can be also rearranged and used to our detriment.*

- *I think that there could be a situation (and it of course was) when some unknown person can misuse the photos and for example pretend that he/she is the person from the photo!*

- *Organized crime, misuse of the photo (e.g. through photomontage).*

- *Person we are chatting with could be a mugger, paedophile etc. He/she can wait for us and harass us. You never know who´s sitting on the other side of PC network.*

- *Nowadays it is easy to edit a photo in many ways, it can be easily used for a porn movie.*

- *Somebody can pretend to be me. He can give incorrect information about me. +If it was someone dangerous, he/she could recognize me by the photo and wait for me for example near my school.*

- *Photograph (when it is a photo of a child at the age of 12 - 16 in particular), can be misused for example as a profile photo of a paedophile that is creating fake profiles to get in touch with children at the same age.*

- *It can be misused for various perversities. Photoshop can make miracles these days and if you lose someone´s favour, it can be a big problem.*

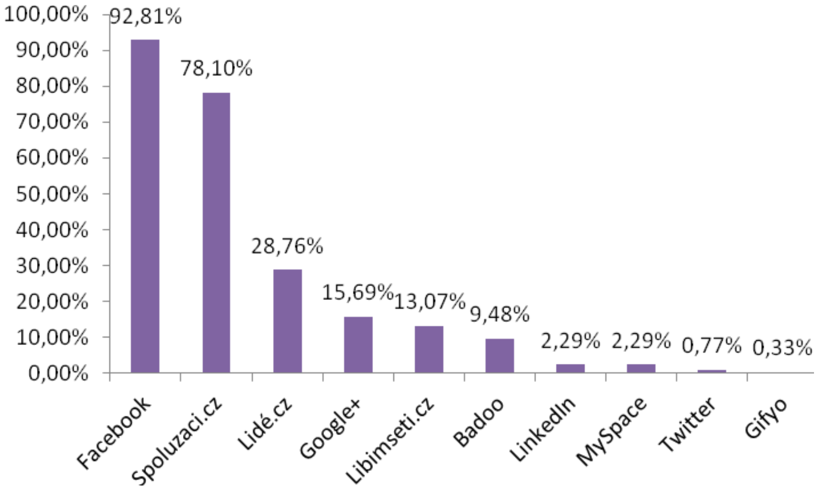
- *Through sending I am losing control over the photo, what is going to happen with the photo, how the photo is going to be used, for what purposes.*

- *Photograph can be modified - used for other photos or used on the website with morally objectionable content, advertising etc. It could be theoretically used by other person who is in contact with mafia and this person could pretend to be me within the Internet or telephone communication. In case of discovery of my contact details it does not have to turn out well... in the abstract...*

3.5 Risky communication of students within the social networks

Within the scope of the research on risky behaviour of students of Faculty of Education of Palacký University in Olomouc we also aimed at the area of social networks. We were primarily interested in what social networks are most frequently being used by the respondents (where they have active accounts) and whether they were within the social networks subjects to one of the forms of the attacks.

Graph No.19 Active social network accounts of the respondents



n=306

Most of the students have active account on Facebook social network (92.81%), Spolužáci.cz (78.10%) and Lidé.cz (28.76%), proportion of other social networks is minor. In connection with active accounts we also followed whether the students add persons without verified identity in a real world between their "virtual friends". Only 9.06% of respondents answered that they add unknown "virtual friends" to their friend lists without identity verification. We point out that "virtual friends" connected for example to Facebook account dispose of higher level of access rights to private information of a user they are connected to.

Tabulka 2. Cyberbullying and related phenomena among Facebook users

Form	*n*	*Percentage*	*ID questions*
Missed calls	117	11.62%	854
Cyberbullying - verbal attacks	108	2.11%	872
Misuse of account for cyberbullying purposes*	16	2.11%	856
Cyberbullying - threats	43	15.14%	860
Cyberbullying - distribution of photographs	33	5.99%	867
Cyberbullying - blackmailing	17	16.00%	859
Cyberbullying - distribution of video recording	6	41.20%	865
Cyberbullying - distribution of audio recording	6	38.03%	863

n=284

* Calculated figures represent combination of documented breaches to accounts and misusing the account for cyberbullying purposes. Attack was registered by 35.21% of student Facebook users.

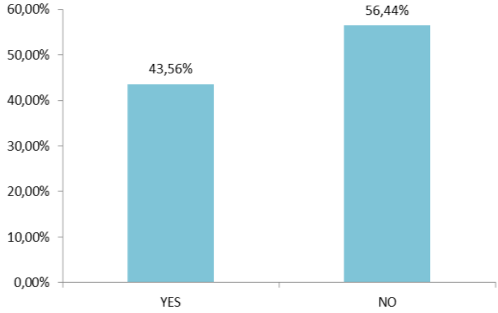
33.80% of respondents having an active Facebook account also confirmed that they were asked by their virtual friends without verified identity for personal meeting, whereas 64.58% of them really came to the meeting.

3.6 Perception of truth and lie

Important part of our research was to find out whether the students tell the truth within the Internet communication or whether it is common to lie. We were also concerned in to what extent they trust to other

Internet users. 1.69% of students trust the information that is being told by other Internet users, 98.31% do not trust the information given by virtual users. Next question was focused on determination of how many students always tell the truth within Internet communication.

Graph No. 20 Do you always tell the truth within the frame of Internet communication?



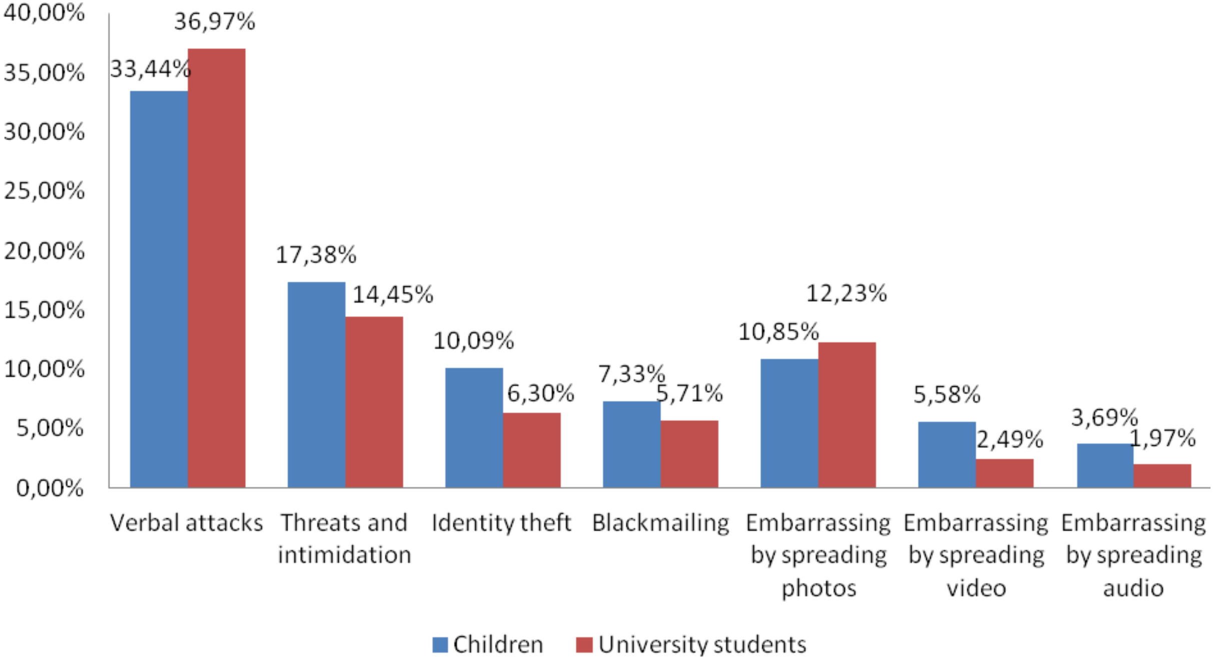
n=303

Less than half of the students (43.56%) stated that they always tell the truth about themselves within the Internet communication.

3.7 Comparison of results among university students and children

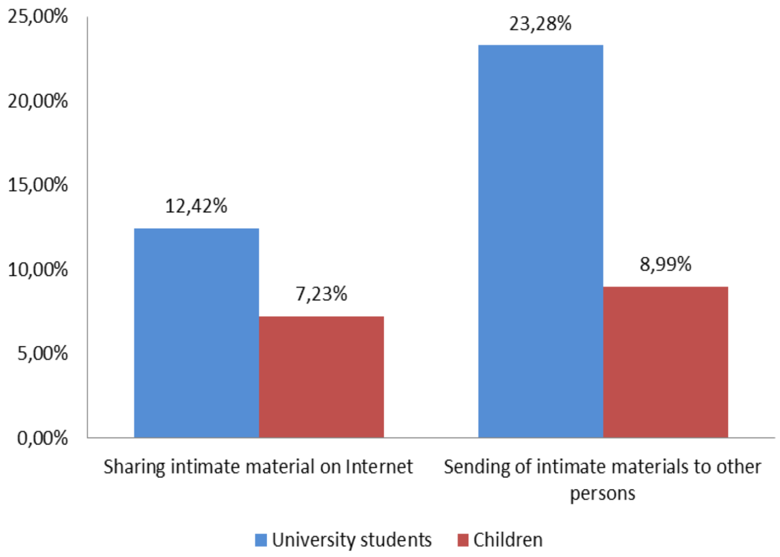
In view of the fact that in 2012 and 2013 we also realized research focused on risky behaviour of pubescents and adolescents within Internet environment, we will try to compare the finding results among key categories. First of all we will focus on occurrence of individual cyberbullying forms among children and university students where we will follow occurrence of cyberbullying within the same period - year 2012. Basic results are compared to the research Danger of internet communication 4 (Kopecký, Szotkowski, Krejčí, 2013) which was realized on sample of more than 20 000 children respondents (age spread 11-17).

Graph No.* 21 *Comparison of cyberbullying victims (university students vs children)



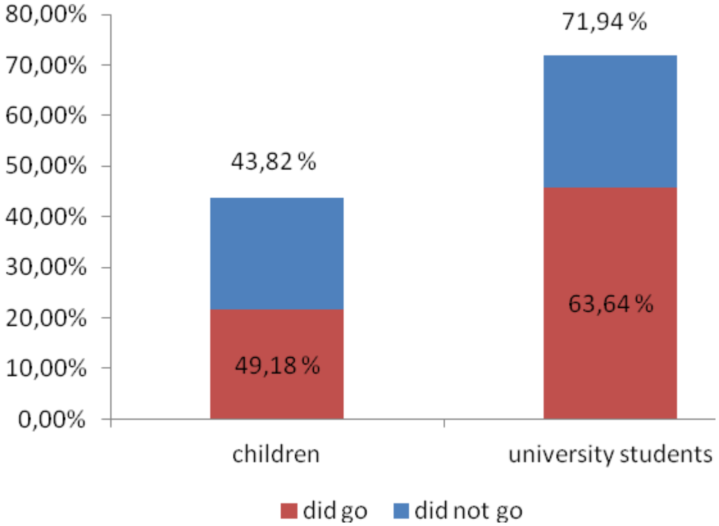
Sexting represented the next phenomenon which we focused on. Herein we followed differences at basic sexting forms - sharing of own intimate sexually explicit materials on the Internet and sending of these materials to other persons.

Graph No. 22 ***Comparison of occurrence of sexting (university students vs children)***



Based on the results we can see that occurrence of sexting among university students are in comparison with children almost twice higher for the both followed forms. It can be explained through the fact that university students live full sexual life where sharing of intimate materials is probably considered to be normal nowadays.

Graph No.* 23 *Personal meetings with people without verified identity



43.82% of children and 71.94% of university students were invited for a personal meeting with unverified Internet user and almost half of the children (49.18%) and more than half of the university students (63.64%) went for the meeting.

4 Results summary

Students of Faculty of Education of Palacký University in Olomouc confirm that they faced cyberbullying, whether in the position of a victim or an attacker. The most widespread form of cyberbullying faced by students in the position of a victim is represented by cyberbullying realized through form of repeated verbal attacks (36.97%). Another frequented form, which the respondents met, was threats and intimidation (14.45%). Cyberbullying is most often realized through text messages and social networks (Facebook in particular).

Sexting level among future pedagogues exceeds value of 12% (12.42%) for sharing of sexually explicit materials on the Internet, 23% (23.28%) for sending of intimate materials to other Internet users.

Almost half of the students (43.82%) were invited for a personal meeting with unverified Internet user, whereas almost half of the questioned respondents (49.18%) went for the meeting.

Students commonly share their personal data on Internet, most frequently the first and last name (92.48%), face photo (84.95%) and e-mail (72.10%).

5 Survey of passwords of young Internet users

Further to our research on risky behaviour of Czech university students simulated on the case of Faculty of Education of Palacký University in Olomouc we realized survey of passwords of young Internet users in 2013. During the realization of this survey we analysed more than 3700 passwords of users of Internet services, where the vast majority (more than 76%) of the file was formed by people aged 15-25. Data associated with the students of Czech universities were separated from the data file and for purposes of this research these data were analysed from the 3 perspectives:

a) *formal password analysis* (what are the formal attributes of password, alphanumerical composition of password and further formal specifics),

b) *semantic password analysis* (whether the password is contained in a dictionary, thus if it is possible to breach the password through a dictionary attack, what is the relation between a user and a password, what areas is a password chosen from etc.),

c) *password usage* (whether the password is universally used, it means one password serves for more Internet services accesses).

Average password length used by an Internet user aged 18-25 is 8.71 characters (see press release to research published on E-Bezpečí internet portal, www.e-bezpeci.cz), **average password length** among university students is **8.93** characters.

From the perspective of formal analysis the **most frequent passwords** are **alphanumerical,** which contain combination of a numerical value and a character (form 47.72% of the data file), on the contrary very few users use purely numerical passwords (only 11% from the sample).

Within the scope of semantic analysis we correlated the passwords with dictionary database of Czech vocabulary (more than 166 000 words and word forms) and we followed to what extent it is possible to "breach" the password through usage of common dictionary attacks. From the total sample of passwords **only 6.92% of passwords were able to find in the dictionary**. It thus means that by means of common dictionary attack it is possible to uncover just very few numbers of passwords. Besides, most of attacks focused on password breach use dictionaries containing English vocabulary mainly.

From the semantic perspective it is possible to divide the passwords into 6 basic categories:

1. *Passwords commonly included in the dictionaries*

   There are usually proper names - mainly first names in neutral forms, but also in forms of diminutives (*jane, janie, janet, monica, mona...*), town names (*praha, ostrava, olomouc*), but also class-nouns (for example words like *sun, locomotive, hacker, politics, studies, leaving exam)*. Among proper names there is usually not a capital letter at the beginning of the word.

2. *Passwords composed of the part derivable from the common vocabulary supplemented with a number or set of characters without specific meaning.*

   Between these passwords we can find for example combination of a name and set of ascending and descending characters without specific logical coherence (*jana123*).

3. *Passwords composed of the part derivable from the common vocabulary supplemented with a number or set of characters with specific meaning.*

   Between these passwords we can find for example combination of a name and a number that have specific meaning, for example representing user´s year of birth (*petr1980*).

4. *Passwords with modified diacritic*

   Very good password type is a password composed of Czech words containing diacritic that is replaced by numbers which represents diacritical characters on the ordinary keyboard. For example password dobrývečer can be by this simple modification rewritten to *dobr7ve4er*. With respect to the fact that dictionaries containing Czech words converted to these modified forms are not widespread so far, these passwords can be considered to be very strong.

5. *Passwords composed of numbers only*

   These passwords are very rarely used due to their quite easy breach through attacks of "brute-force" type, they are used by every 10th Internet user only. Within the frame of the brute-force attack, programme trying to breach your password uses combination of letters and numbers in all possible combinations.

6. *Alphanumerical passwords with randomly generated characters*

   Their great advantage lies in their strong resistance to automated attacks. However, their big weakness represents the fact that they are very hard to remember.

Almost half of the students (48%) use universal passwords for access to Internet services, this password is mainly used for access to main e-mail account and for access to social networks account (Facebook in particular).

Within our analysis we also followed whether Czech users use passwords that are often quoted in the lists of the least safe passwords. Among typical examples of these passwords we can find combination of numbers *12345*, word *password* etc.. These passwords are almost never used by young Internet users. We will demonstrate this fact in the following table:

Tabulka 3. Occurrence of the least safe passwords

Tested password	Occurrence rate	%
123	0	0
1234	2	0.05%
12345	1	0.03%
123456	2	0.05%
1234567	0	0
12345678	0	0
123456789	2	0.05%
word “password”	1	0.03%

n=3743

Passwords composed of descending numerical series were not presented at the table at all. **Based on the observed facts we can**

claim that frequent usage of the simple numerical series as passwords was not proved and it can be considered as a myth for the given age category.

Most frequent passwords are represented by **town names** and **first names** in particular, further words **sun**, **mummy**, **locomotive**, among students words like **studies**, **leaving exam**.

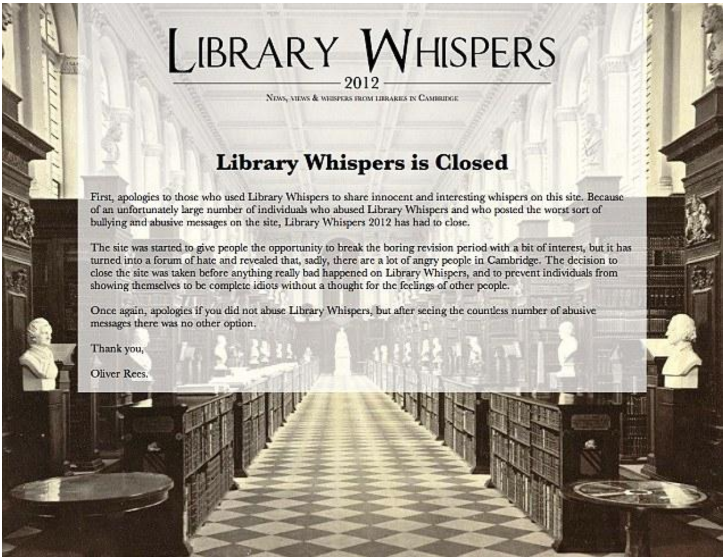
However, attackers from the Czech environment usually do not use automated forms of attacks for attacks on the Internet accounts, but they focus on the breach of the control questions for access to the accounts. These questions are frequently being underestimated and they represent crucial point for access to email accounts in particular. To reveal an answer for control question is usually significantly easier than to reveal the right password.

More information regarding this research can be found on the internet website www.prvok.upol.cz.

6 World cases of cyberbullying of students

6.1 Cyberbullying at Cambridge University (2012)

Typical example of cyberbullying among university students is represented by a case that happened at the beginning of 2012 at Cambridge University. Students of Cambridge University opened internet website focused on exchange of information about exams, teachers, study materials etc. They also used the website for communication between university libraries. Posts were published to the website in real time (similar to Twitter of Facebook). The website was called Library Whispers. However, common communication within the website very quickly developed in a discussion full of attacks on concrete students and university employees. There were more than 1000 comments registered in 5 days



LIBRARY WHISPERS

2012

News, views & whispers from libraries in Cambridge

Library Whispers is Closed

First, apologies to those who used Library Whispers to share innocent and interesting whispers on this site. Because of an unfortunately large number of individuals who abused Library Whispers and who posted the worst sort of bullying and abusive messages on the site, Library Whispers 2012 has had to close.

The site was started to give people the opportunity to break the boring revision period with a bit of interest, but it has turned into a forum of hate and revealed that, sadly, there are a lot of angry people in Cambridge. The decision to close the site was taken before anything really bad happened on Library Whispers, and to prevent individuals from showing themselves to be complete idiots without a thought for the feelings of other people.

Once again, apologies if you did not abuse Library Whispers, but after seeing the countless number of abusive messages there was no other option.

Thank you,

Oliver Rees.

Report on closure of Library Whispers website (Source: Dailymail.co.uk)

Sample of the posts within the communication (Library Whispers)

I hate this fucking library and every single person inside it. I hope you all fail your exams.

Don't worry she was a female arts student. Female x arts = second order, so can be ignored.

Just spat on a working-class person.

*I can hear you clicking at your f****** card game through my headphones you inconsiderate d***' and 'crazy laughing b**** in the corner please desist*

Case from Oxford happened just week after 2000 students threw a spectacular party in a public park where they scared local citizens, they drank themselves into oblivion, pissed on the grass, vomited in public in front of the locals. There were police patrols and medical units needed.

Photo of police striking the drunken students (Source: Dailymail.co.uk)

6.2 Tyler Clementi´s suicide (2010)

Violinist Tyler Clementi, 18 year old student from Rutgers University in New Jersey (USA), committed suicide in 2010 by jumping from George Washington Bridge after he was recorded by his roommate Dharum Ravi and his girlfriend Molly Wei, without Clementi's knowledge. They used the records for broadcasting on Internet and they allow more people to watch what is going on in Clementi´s room.

This led to revealing of Clementi´s homosexuality as he was recorded when kissing with other man. World leading media commented the case in this manner. However, this case is far more complicated that it seems.

Before the suicide, Clementi had revealed his homosexuality to his parents, he had been supported by his father but his mother could not accept it. She later explained that she was not able to deal with her son´s homosexuality because she is a religious woman and she believes that homosexuality is a sin.

Ravi Dharun tried to find information about his new roommate Tyler online and he found Tyler´s posts on Justusboys internet websites which is aimed at homosexuals. He shared this information on Twitter where he posted: *I´ve just found out that my roommate is gay.* Tyler learned about it later on.

On the nights of September 19 and 21, Clementi had asked Ravi to use their room for those evenings. On the first occasion, Ravi met Clementi's male friend, and Clementi said that the two wanted to be alone for the evening. Ravi has stated that he was worried about theft and that he left the computer in a state where he could view the webcam due to those concerns. Ravi and Wei viewed the video stream via iChat for a few seconds, seeing Clementi and his guest kissing. On September 20, Ravi then posted a message to his Twitter account: *"Roommate asked for the room till midnight. I went into Molly's room and turned on my webcam. I saw him making out with a dude. Yay."*

On September 21, Ravi posted text messages saying that there would be a viewing party to watch Clementi´s room and he asked Twitter users to watch video chat streaming from 9:30 - 12:00. Ravi had set up the webcam and pointed it towards Clementi's bed and he turned the computer to sleeping mode. Later, Ravi claimed at the court that he changed his mind about the whole action and he set up the camera pointed towards his own bed. However, Police confirmed that the webcam was still pointed towards Clementi´s bed. When Clementi returned to his room, he noticed the camera and computer being turned off and texted a friend saying he had unplugged Ravi's power strip just for sure.

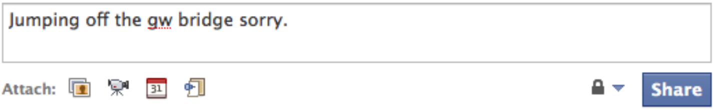
The same day Clementi complained to a resident assistant (in person and via email) that Ravi had used a webcam to video stream part of Clementi's private sexual encounter with another man and he requested punishment for Ravi. He requested a room change at the same time.

On the evening of September 22, Clementi left the dorm room, got food, and, around 6:30 p.m., headed toward the George Washington Bridge and by 8:42 p.m., Clementi had made his way to the George Washington Bridge and posted from his cell phone on Facebook: *Jumping off the gw bridge sorry.* Clementi left a suicide note which was never released to the public.

Molly Wei entered a plea agreement allowing her to avoid prosecution in exchange for her testimony against Ravi, 300 hours of community service. In 2012, Ravi was sentenced to 30 days in jail, 3 years' probation and a $10,000 fine. Ravi was released from jail after 20 days of his sentence.

Tyler Clementi (Source: Facebook.com, profile photo)

Dharun Ravi (Source: Time.com)



Jumping off the gw bridge sorry.

Last post on Clementi´s wall (Source: Facebook.com)

Although media speculated that Ravi broadcasted recordings from their room to other Internet users, it never happened and there is no existing record of sexual intercourse, also no photos showing these acts were published (there is just a photo on which it is not possible to recognize faces and both men are dressed) etc. Video broadcast ran just over corridor - to the next room where Ravi Dharum was watching it.

6.3 Happy slapping from Oxford (2008)

Cyberbullying case in form of happy slapping took place in 2008 at Oxford University as well. Nick Brodie, student and president of the university boat club, filmed a friend Colin Groshong attacking a rival rower from Imperial College in London, Will McFarland (Miller, 2008). The attack took place at the Wroclaw regatta in southern Poland, where all of them were presented.

The attack took place in the lavatory of a nightclub (Sears, 2008). Attacker Colin Groshong was taunting the rival rover at first, he yelled an obscenity before punching Mr McFarland to his face for several times.

Colin Groshong and Nick Brodie (Source: Dailymail.co.uk)

After Mr Brodie had returned to England, he posted the footage on his Facebook page where it was commented by other users. Many viewers of the footage apparently found it amusing and left online messages. Examples of the messages:

Henry Sheldon, president of the Oxford University Lightweight Rowing Club, wrote:
Thank you for posting that video of Colin. It's considerably brightened up my day in the library. I literally laughed till I cried.

Colin Brodie replied:
It's up there with the funniest things I have ever seen.'

However, after numerous complaints (including from Groshong and McFarland), Mr Brodie suddenly changed his tune, wrote that he does not really know why he filmed it and why he put it up on Facebook, and removed the video. Both students try to explain that the incident was provoked, although it may not seem on video and that they should not have reacted in the way that they did. Groshong made it up with Will and things are normal between them now.

7 Student cyberbullying cases from the Czech Republic

7.1 Cyberbullying and blackmailing of female students (2010)

In October, 2010, police station in Olomouc received a complaint from two students from Olomouc. Unknown offender breached their electronic emails and then he gained their intimate photographs which he used to blackmail them (Source: Police of the Czech Republic).

Student of information science at University of Pardubice used to create fictive internet websites, where he got e-mail addresses and passwords from people registering at the website (he done so-called phishing[3]). He for example set up various discussion groups on Facebook on which he promised interesting prizes that could be won during registration to his fake websites. Through this way he gained database with more than 1800 email addresses. As soon as he infiltrated the email addresses of his victims, he found out whether they confirm any intimate photographs. He downloaded the photos and then threatened girls by publishing of the photos within social networks (which it really happened in a few cases). Tens of thousands of girls and women were forced to send him more photographs, possibly to get naked in front of the online camera. Vast database containing several gigabytes of photographs was secured during the house search. Offender´s motive was to gain more intimate materials. Offender was put on probation of 9 months imprisonment with suspension of the sentence for 16 months for Breach of secrecy of delivered messages (§ 182/1 TZ) and Sexual constraint (§ 186/1 TZ).

7.2 Libor case (2013)

Submissive student Libor (19 years old) met through Moneyslave service (www.moneyslave.cz), which is focused on meeting with people within the frame of BDSM community[4], with 20 year old Kateřina, student of Faculty of Health Sciences at Faculty of Education of Palacký University in Olomouc. They established close communication and

[3] Phishing is a term representing communication practises focused on theft of sensitive personal data, such as passwords, bank account data, credit card numbers etc. Interpretation of phishing is not uniformed.

[4] BDSM abbreviation comes from English and stands for combination of more abbreviations, mainly S&M, for sadism and masochism, D&S for domination and submission and B&D for bondage and discipline. BDSM includes variety of unusual sexual practices.

were writing through Skype instant messenger, they also realized video calls. Gradually, they exchanged their contacts, photos, and also connected

through Facebook social network. After some time they were communicating through video chats (through use of webcam), whereas Libor fulfilled various tasks that Katka assigned to him. Tasks got more daring and the whole communication culminated at a point where Libor got naked and masturbated in front of the webcam. However, Kateřina recorded everything through the webcam, as well as Libor´s intimate video, she started blackmailing him with threats of publication of the video and she asked him to promptly pay 12,000 CZK.

Authentic communication:

Kateřina: You should try harder, you bitch, to meet my requirements, as I have your whole jerking off here on my tape.

Kateřina: I think you should go to the bank and ask for account current, you will have the money immediately. 12 grand, darling, and I will give you high rating.

Kateřina: Do you wanna see it, you bitch? If you dont meet my requirements, you could find it on YouTube.

Kateřina: If I dont get a receipt regarding the payment from the bank today, I will send the video on YouTube.

At this moment Libor contacted advisory centre of Centre for the Prevention of Risky Virtual Communication / E-Bezpečí project asking for help. Through early investigation it was found out that the user used fake profile of a female student and she also sent faked photo that was downloaded from somebody else´s profile. Team of E-bezpečí project in cooperation with other partners discovered offender´s IP address, identified her real identity through usage of bank account identification (she sent her bank account number to Libor for purposes of the payment, however the bank account number was linked to her profile on Aukro´s auction server) within combination of public profile databases. The team also located the region from which the offender sent her messages to Libor. Several social network profiles actively used by the user were subsequently uncovered. Information was passed on Libor and Police of the Czech Republic at the same time under suspicion of committing a crime of Blackmailing. At the moment Libor called the offender by her real name, she felt unsure of herself and started making excuses how she did not do anything wrong and that she was not going to publish the video. Police closed the case with suspicion on committing a crime and the case was handed over to the public prosecutor who stopped the case arguing that based on his legal opinion no criminal act nor was offence committed.

8 Cyberbullying aimed at teachers of Czech universities

Cyberbullying is within the society perceived as a topic connected mainly to pubescents and adolescents, there is just a minimum discussion about cyberbullying of adults. Nevertheless, cyberbullying of adults really exists, however it is spoken much less and employers often try - maybe for fear of discrediting of given institution - to cover it up.

Basic difference between cyberbullying of children and adults is considered to be mainly in a motive of the behaviour: while cyberbullying among children is in 95% of cases realized “for fun”, situation among adults is completely opposite - cyberbullying itself is realized to harm other persons, discredit them, possibly destroy their personal and professional lives. This behaviour leads to offences or criminal acts - particularly to a criminal act of violence against group of citizens and individuals, dangerous stalking or dangerous threatening. There are also situations at universities when an innocent joke gets out of hand and becomes a real stalking and harm of selected victim.

In this part we will reveal several cases where some of them are known through media, but numbers of cases are completely unknown for public. With respect to delicacy of these private cases and for strategic reasons we do not state name of the institutions where the given cases took place. However, all the cases took place within the last five years at one of the public or private universities.

8.1 Case of online threats at Masaryk University (2008)

Cyberbullying realized through distribution of anonymous e-mails containing death threats was running for 4 months. These emails were sent by Professor Břetislav Horyna to his colleague, professor of philosophy, Jaroslav Hroch.

For several months, Professor Hroch was receiving anonymous emails full of death threats. In December 2008, professor Hroch received a message from unknown person who was pretending to be deceased representative of catholic dissent Augustin Navrátil. There was a sentence saying "I´m coming for you soon". Professor ignored the message. However, he got far ruder anonymous message in January: "You should get a colostomy, hippo, make sure you dont have all the crap in your pants. We know you and your cunning family." (Idnes.cz) More emails followed, we shortly quote couple of them: *One injection in a trolley, complex paralysis, you will rot alive. And everyone will be happy that we get rid of a smeghead. You should go to a nuthouse, we will let you alone there, dead man. Preparation we were waiting for is in the place. But it´s not going to hurt you soon, you will wear "pampers" and have 3 sedative injections a day. It should be good for you to beat you up and make you eat the pavement.* (Source: Idnes.cz)

Horyna was accused and found guilty for committing a crime of violence against group of citizens or individuals and he was inflicted by a penalty of 50,000 CZK with substitute imprisonment for 2 months. He appealed against the sentence, nonetheless the punishment was confirmed by court of appeal in 2012.

Břetislav Horyna (photo by Otto Ballon Mierny, MAFRA)

This is not a unique case in the Czech Republic, various behaviours of bullying or cyberbullying as well as mobbing[5] occur between the pedagogues at almost all universities.

8.2 PhD. candidate Jitka (public university, January - May 2011)

Jitka was a fresh absolvent from one of the Czech public universities, she earned a master´s degree and tried to stay at her alma mater for

[5] Mobbing represents bullying that occurs in the workplace and that is longterm and repeated. Between 4-8% of workers faced mobbing as victims (Bendl, 2002). Boundary between mobbing and cyberbullying is not strictly set, mobbing can be perceived also as one of the forms of cyberbullying of adults.

some more time. She enrolled for entrance examination to full-time doctoral study programme, she was taken in the student programme and started her studies. She met her colleagues, began teaching, worked on her scientific work.

After some time she started receiving strange text messages containing threats and intimidation from a person unknown to her: I am watching you, bitch. I will come for you soon and I will enjoy it. I know where you live. Jitka at first ignored the text messages and blocked the unknown number used for sending of the messages. However, she started receiving emails with similar content later on: You cannot hide from me, I will embowel you. Clear off the faculty and our town. If you contact the police, it will be the last thing you will do in your life. The whole situation lasted for more than 5 months, emails were supplemented with messages from unknown Facebook users, and intensity got higher. Jitka started getting afraid. At the end, she contacted the Police of the Czech Republic.

During the investigation, group of Jitka´s students who did not pass the required seminar in the first term was suspected to be the unknown users. Police consequently discovered IP addresses which were used for sending of the emails containing threats and at the end one of the students plead guilty. 23 year old Petr N. decided to revenge his bad marks at university through threats sent to Jitka. He then enjoyed changes in Jitka´s behaviour during the seminars and the faculty... and he enjoyed the fear arousing in her.

Police interpreted the case as the commission of a crime of violence against a group of citizens or individuals and suspicion of commission of a crime of dangerous threatening. He appealed against the judgement and results of appeal proceedings are not public. Based on the decision of ethical commission, Petr was excluded from the faculty as well. The case was never published by the faculty; embargo was laid on any information regarding the case.

8.3 Mikeš (September 2011 to January 2012)

Mikeš had been working as lecturer for 8 years for one of the well-known Czech public universities. He earned PhD. degree and he was preparing for his habilitation. Quite young pedagogue was very popular among students, he was on the first name terms with many of them, he went to the parties with the students. Female students loved and adored him, he represented an ideal combination of handsome and successful young pedagogue. Mikeš always kept distance from the students, he did not have sex with them, he declined many offers from the students in love. He defined borderline which he did not cross.

(Illustration photo)

Unfortunately, two female students that Mikeš taught did not deal with his rejection and they decided to revenge them. Suddenly, a rumour spread between the students saying that Mikeš is refusing female students because he is a gay and he is in relationship with his colleague. At the beginning of this rumour Mikeš made an essential mistake when he tried to explain that he is not a gay and that this is a rumour. Thanks to this, he drew more attention to the rumour. His colleagues started making jokes about his homosexuality too. They speculated who could be his reputed partner... and they began making fun of him.

Furthermore, there was created a discussion group on Facebook social network, where the reputed homosexuality was discussed and where photographs from various events, that Mikeš took part in, started to appear. People then started speculating which person on the photo could be the reputed partner of Mikeš. Further, this information spread between the students (men) - who wanted to pass the exam, he had to come in a pink shirt. Mikeš began receiving text messages on his cell phone from various telephone numbers. He was offended and threatened through the messages: *We don´t want a pansy here. Departure to the warm regions, nancy boy. Poofter, you can gay in the park.*

The case was not reported on the Police of the Czech Republic. Faculty´s ethical commission and academic senate were dealing with the whole situation. Because a guilty person was unknown, students were globally warned of breaching the moral code and they were told that any concrete misconduct will be punished with assistance of Police of the Czech Republic. The Facebook discussion group was closed and consequently deleted. Mikeš was recommended to ignore the hate behaviours. Cyberbullying successively fell silent and there is none at the moment. Mikeš stayed at the faculty and he is preparing for his habilitation.

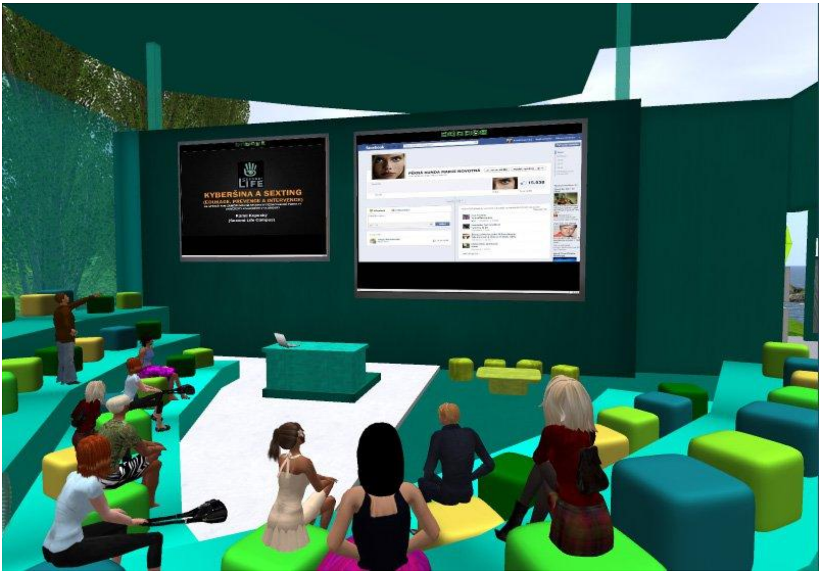
9 Education of future teachers

If we want to increase competences of future pedagogues in the area of solving of risky communication behaviours associated with ICT, it is required to integrate topics involving safer usage of the Internet and social pathological phenomena related to ICT into the academic preparation. *Combination of theoretical knowledge and practical skills,* which can be learned particularly through *direct work with endangered target group* - in our case with children, seems to be an appropriate form of this.

Knowledge, which the future teachers will gain during their practice, can be consequently brought to their common lives and used for elimination of risks that are related to them as well. Usage of *excursions or clerkships at professional institutions*, which are focused on areas of risky Internet behaviour or possibly provide Internet services or connections, represents one of the other interesting methods. Contact with such a practice can quite quickly activate students and motivate them for work with children or adults.

Another method for education of future pedagogues is to *involve them actively to activities of consulting centres* which helps to solve individual cases associated with risky Internet behaviour. In practice, it means for example to give the real cases to the students, to lead the students during the solution, teach them how to communicate with victims, make reference to the help lines etc. At Faculty of Education of Palacký University in Olomouc this task is carried out by Online advisory centre of Centre for Prevention of Risky Virtual Communication which yearly deals with approximately 150 cases of misuse of ICT for attacks to other persons. The advisory centre is available at www.napisnam.cz.

Usage of potential of multi-user virtual environments represents one of the other interesting alternatives, which allows realizing educational activities for future pedagogues within the environment of so-called virtual worlds, such as Second Life. Second life is a multi-user virtual 3D environment which is however not so popular in the Czech Republic, it is entered by no more than ten thousands of Czech users. Despite this fact it presents an interesting possibility how to draw attention to the risky behaviour within the Internet environment just through this untraditional e-learning form. Recordings from the lectures and seminars realized in Second Life world can be easily put to YouTube environment and there is then possibility to educate large number of Internet users. Lessons which take place in Second Life can be watched through E-Bezpečí portal (www.e-bezpeci.cz).



(Example of lesson about cyberbullying and sexting from the Second Life environment)

To support the education of the future pedagogues it is naturally possible to use *more traditional e-learning study forms.* So-called LMS

(Learning Management Systems), that is widespread within the university environment, represents one of these e-learning forms realized through systems for education management. Within the scope of e-learning activities there are several courses focused on social-pathological phenomena related to the Internet environment at Faculty of Education of Palacký University in Olomouc.

At number of institutions education of students and teachers is secured through various grant projects. At Faculty of Education of Palacký University in Olomouc our team runs for example a project called *E-Synergie - scientific research network for risks of electronic communications*, which is financed through funds of ESF OP VK (CZ.1.07/2.4.00/17.0062). Project is aimed at creation of working scientific research network connecting educational, research and business organizations focusing on areas of risky virtual communication within the cyberspace and related cybercrime. The network functionally interconnects both theoretical (research, stabilization of theoretical problems, psychological and legal aspects of risky communication phenomena) and practical (education, intervention, criminal solution of the problems, knowledge implementation to the commercial sphere) areas. E-Synergie project as one of the first projects integrates area of safer Internet behaviour to the system of education of future teachers, participating in training and education of new IT capable generation of new teachers who are able to solve problem situations right at the schools. E-Synergie project involves further cooperation between Centre of Prevention of Risky Virtual Communication of Faculty of Education of Palacký University in Olomouc and and team of Ministry of the Interior of the Czech Republic (department of crime prevention), Police headquarters in Olomoucký region, companies Vodafone Czech Republic, a. s., Seznam a. s. and Google Czech Republic, s. r. o. More information can be found on www.esynergie.cz.

9.1 Several insights related to education of future teachers

To ensure successful education within the university environment it is required to follow several rules and methods and obviously to respect didactic principles defined in number of expert publications (Kalhous, Obst, 2009 and further). For purposes of this text I will try to make the rules easier and adjust them to the theme of this publication.

First-rate motivation sets basis of successful education

Students have to be motivated in the appropriate manner to ensure successful education of the future pedagogues. University students motivation is usually strictly pragmatic - students get credits for passing of given lectures and seminars. However, primary motivation should come out the students´ desire for learning the unknown, getting important information, which can be used in a real life and that affect them and also their personal life. Therefore, within the education realized by team of PRVoK Centre and E-Bezpečí project we combine teacher preparations both in a "pragmatic" form of education (for which the students are rewarded with credits), and voluntary form of education, represented by selective lectures and seminars without credit evaluation.

Theory and practice must make a whole

Theory and practice, which is being interpreted to the students within the framework of their educational activities, must be interconnected to the functional unit. An ideal way is to keep balance between these two parts, possibly to interconnect these two parts into single unit. When there is an imbalance, education is less effective then. For example, when we focus on explanation of cyberbullying forms and we will not supplement each of the form with concrete practice example, process affectivity of knowledge transfer towards students will decrease. However, we will get to the same conclusion when the theory is completely absent and teacher confines himself just to the case examples, which are still not put into the needed contexts and there is no so-called fixation of theoretical knowledge.

Obtained knowledge must be applicable for practice

Knowledge, which we pass on the students, should be as applicable as possible. For example, when we present results of researches focused on occurrence of cyberbullying among university students, we will at the same time give students information about which phenomena they will mostly meet in practice, which behaviours are marginal on the contrary, how they can use the data in practice for minimization of these behaviours within society, what tools they should use etc. When we for example describe strategies of manipulation with victim realized by sexual attackers, we will at the same time give them information about defence instruments that lead to recognition and cease of these attacks. At every moment student must know what the purpose of the information passing on is.

Experience must be part of the education

If we want to maximize the educational effect, we should present the information in such a way when the student can process the information through experience, by means of his emotions. This can be reached for example through student´s active involvement to the solution of the concrete case, we can give him/her documentary evidence at his disposal, photo documentation, offender´s testimony and further information which can arouse or support the experience.

Usage of experience within so-called experience pedagogy represents very effective way of maximization of the educational process.

Experience method for solution of ethical dilemmas is one of the examples of this approach. This method was tried by our students for example within expert short term attachment or excursions realized under E-Synergie project and held at Seznam.cz Students´ task was to solve ethical dilemma regarding story About princess who was eaten by a dragon (the whole story is available on www.esynergie.cz). During the process students took active part in the solving of the given ethical problem and they argued for their opinions, they used their own arguments, they used compromise, and in number of cases students used both assertive and affective solving approaches etc. It is obvious that experience educational method is very interesting, effective and for many situations quite difficult for preparation.

Students of Faculty of Education in the training process at Seznam.cz

10 Conclusions

Area of dangerous communication phenomena related to the electronic communication represents very important and serious topic which is related to almost every Internet user. It is thus important to work actively in this area and transfer the knowledge gained for instance through a research to the practice and learn from the experience obtained during educational process.

The aim of this publication is to warn of the occurrence of risky communication behaviours within the population of university students and compare them with the occurrence of social-pathological phenomena among children. At the same time to offer possibilities of how to influence these findings mainly through pointed education and preventive influence on students, the future pedagogues.

I believe this publication gave you a lot of information which you will be able to use in your own education and prevention activities.

Kamil Kopecký
author

11 List of used sources

Aghazamani, A. (2010) How Do University Students Spend Their Time On Facebook? An Exploratory Study. Journal of American Science 2010; 6(12):730-735]. ISSN: 1545-1003

Abdelraheem Y. A. (2013) University Students Use of Social Networks Sites and Their Relation With Some Variables. WEI International Academic Conference Proceedings. Antalya: Turkey. Online: http://www.westeastinstitute.com/wp-content/uploads/2013/02/ANT13-240-Ahmed-Yousif-Abdelraheem-Full-Paper.pdf

Akyildiz, M., Argan, M. (2011) Using Online Social Networking: Students' Purposes of Facebook Usage at the University of Turkey. Online: http://www.aabri.com/LV11Manuscripts/LV11094.pdf

Amorelli, D. (2010). Parents Win Right to Block Sexting Cases. Legal News Center, 2010 (3). Online: http://www.seolawfirm.com/2010/03/parents-win-right-to-block-sexting-cases/

Arrington, M. (2005). 85% of College Students use FaceBook. TechCrunch. Online: http://techcrunch.com/2005/09/07/85-of-college-students-use-facebook/

Bartoněk, J. (2012) Dětská prostituce. E-Bezpečí. Online: http://www.e-bezpeci.cz/index.php/temata/sexting/482-dtska-prostituce

Belsey, B. (2004). Always on, always aware. Online: http://www.cyberbullying.ca/pdf/Cyberbullying_Information.pdf

Berson, I. H. (2003) Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth. University of South Florida. USA. Online: http://www.cs.auckland.ac.nz/~john/NetSafe/I.Berson.pdf

Barak, A., & King, S.A. (2000). The two faces of the internet: Introduction to the special issue on the internet and sexuality. Cyberpsychology & Behavior, 3, 517–520.

Bendl, P. (2002) Mobbing je když... Moderní vyučování. Roč. 8., čís. 3., s. 4–5.

Browker, A., & Sullivan, J.D. (2010). Sexting: Risky Actions and Overreactions. FBI Law Enforcement Bulletin, 2010 (5). Online: http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/july-2010/sexting

Catalano, R., & Junger-Tas, J. et al. (1998). The nature of school bullying: A cross-national perspective (1st ed.). London: Routledge.

Dilmac, B. (2009). Psychological needs as a predictor of cyber bullying: A preliminary report on college students [Electronic Version]. Educational Sciences: Theory & Practice, 9(3), 1307 – 1325.

Dowty, T. (2009). Sharing children's personal data. In D. Korff, & T. Dowty (Ed.) Protecting the virtual child. London: ARCH. Online: http://www.nuffieldfoundation.org/sharing-childrens-personal-data

Douglas, N., Lilley, S.J., Kooper, L., & Diamond, A. (2004) Safety and justice: sharing personal information in the context of domestic violence. Online: http://www.eurowrc.org/01.eurowrc/04.eurowrc_en/GB_UNITED%20KINGDOM/Sharing%20personal%20information%20-%20domestic%20violence.pdf

Dressing H, Kuehner C, Gass P. (2005) Lifetime prevalence and impact of stalking in a European population: Epidemiological data from a middle-sized German city. Br J Psychiatry 2005; 187: 168-172.

Englander, E. K. (2007). Is bullying a junior hate crime? Implications for interventions. American Behavioral Scientist, 51, 205–212. ISSN 00027642.

Ferguson, C. J. (2011). Sexting behaviors among young hispanic women: Incidence and association with other high-risk sexual behaviors. Psychiatric Quarterly, 82, 10.1007/s11126-010-9165-8.

Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. Deviant Behavior, 29, 129– 56. ISSN 01639625.

Choo, K. R. (2009) Online child grooming: a literature review on the minuse of social networking sites for grooming children for sexual offences. Australan Institute of Kriminology.

Chráska, M. (2007). Metody pedagogického výzkumu: základy kvantitativního výzkumu (1st ed.). Praha: GRADA.

Information Commissioner's Office. (2006). Protecting Children's Personal Information: ICO Issues Paper. Online: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/issues_paper_protecting_chidrens_personal_information.pdf

Jolicoeur, M., & Zedlewski, M. (2010) Much Ado about Sexting. Online: https://www.ncjrs.gov/pdffiles1/nij/230795.pdf

Kalhous, Z, & Obst, O. (2009) Školní didaktika. Praha: Portál.

Kolínková, E. Oběť výhrůžných e-mailů na fakultě končí, viníka propustit nemohou. Idnes.cz. Online:

http://brno.idnes.cz/obet-vyhruznych-e-mailu-na-fakulte-konci-vinika-propustit-nemohou-1d0-/brno-zpravy.aspx?c=A120611_1790747_brno-zpravy_bor

Kopecký, K. (2011). České děti o sextingu. Olomouc: E-Bezpečí. Online: http://www.e-bezpeci.cz/index.php/temata/sexting/237-eske-dti-o-sextingu

Kopecký, K. (2011). Tragický příklad sextingu z USA. Olomouc: E-Bezpečí. Online: http://www.e-bezpeci.cz/index.php/temata/sexting/254-tragicky-pipad-sextingu-z-usa

Kopecký, K. (2010). Kybergrooming – nebezpečí kyberprostoru. Olomouc: Net University. Online: http://e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie

Kopecký, K. (2011). Tragický příklad sextingu z USA. E-Bezpečí. Online: http://www.e-bezpeci.cz/index.php/temata/sexting/254-tragicky-pipad-sextingu-z-usa

Kopecký, K. (2010). Úvod do problematiky tzv. slovních mraků (Word Clouds). Net-University. Online: http://www.net-university.cz/multimedia/56-uvod-do-problematiky-tzv-slovnich-mrak-word-clouds

Kopecký, K. (2012). K pozitivním vlivům hraní World of Warcraft. Olomouc: E-Bezpečí. Online: http://www.e-bezpeci.cz/index.php/temata/dali-rizika/517-pozitivawow

Koskelainen, M., Ristkari, T., & Helenius, H. (2010). Psychosocial Risk Factors Associated With Cyberbullying Among Adolescents: A Population-Based Study. Arch Gen Psychiatry, 67, 720–728.

Kowalski, R., Limber, S., & Agatston, P. (2007). Cyber Bullying: Bullying in the Digital Age (1st ed.). Malden: Blackwell Publishers.

Krejčí, V. (2010) Kyberšikana - kybernetická šikana. Olomouc: Net University. Online: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie atd?download=14%3Akybersikana-studie

Krejčí, V., & Kopecký, K. (2010). Nebezpečí elektronické komunikace 1: zpráva z výzkumného šetření realizovaného v rámci projektu E-Bezpečí. Online: http://www.prvok.upol.cz/index.php/ke-staeni/doc_download/5-nebezpei-internetove-komunikace-e-bezpei-prvok-2009-2010

Krejčí, V., & Kopecký, K. (2011). Nebezpečí elektronické komunikace 2: zpráva z výzkumného šetření realizovaného v rámci projektu E-Bezpečí. Online: http://www.prvok.upol.cz/index.php/ke-staeni/doc_download/13-nebezpei-elektronicke-komunikace-2-centrum-prvok-2011.

Kubíčková, K. (2010) Učitelé z filozofické fakulty podpořili profesora, jemuž vyhrožoval kolega. IDnes. Online: http://brno.idnes.cz/ucitele-z-filozoficke-fakulty-podporili-profesora-jemuz-vyhrozoval-kolega-17u-/brno-zpravy.aspx?c=A101125_173526_brno-zpravy_trr

Lenhart, A. (2009). Teens and Sexting. Online: http://pewresearch.org/assets/pdf/teens-and-sexting.pdf

Lumby, C., & Funnell, N. (2011). Between heat and light: The opportunity in moral panics. Crime. Media, Cultuire, 7, 277–291.

Marešová, H. a kol. (2012). Pedagogická fakulta UP v roce 2011. Olomouc: VUP. Online: http://www.pdf.upol.cz/menu/uredni-deska/dokumenty-a-normy/

Martínek, Z. (2009). Agresivita a kriminalita školní mládeže (1st ed.). Praha: Grada.

Meacham, A. (2009). Sexting-related bullying cited in Hillsborough teen's suicide. St. Petersburg Times. Online: http://www.tampabay.com/news/humaninterest/article1054895.ece

Miller, V. (2008) Oxford students posts "happy slapping" video on Facebook. The Telegraph. Online: http://www.telegraph.co.uk/news/uknews/2020052/Oxford-student-posts-happy-slapping-video-on-Facebook.html

National Campaign to Prevent Teen and Unplanned Pregnancy. (2009). Sex and Tech: Results from a Survey of Teens and Young Adults. Online: http://www.thenationalcampaign.org/sextech/pdf/sextech_summary.pdf

North Yorkshire Children's Trust. (2009). A General Framework for Information Sharing in North Yorkshire and York. Online: http://www.northyorks.gov.uk/CHttpHandler.ashx?id=2700&p=0

Turan, N., Polat, O., Karapirli, M., Uysal, C., Turan, S.G. (2011). The new violence type of the era: Cyber bullying among university students. Neurology, Psychiatry and Brain Research. Vol. 17, Issue 1. Online: http://www.npbrjournal.com/article/S0941-9500(11)00006-6/fulltext

Olweus, D. (2006). An analysis of the Revised Olweus Bully: Victim Questionnaire using the Rasch measurement model. British Journal of Educational Psycholog, 76, 781–801.

Qing Li. (2006). Cyberbullying in Schools: A Research of Gender Differences. School Psychology International, 27, 157–170.

Rigby, K. (1997). Bullying in schools, and what to do about it (1st ed.). London: Jessica Kingsley.

Shambare, R., Rugimbana, R., Sithole, N. (2012). Social networking habits among students. African Journal of Business Management Vol. 6(2), pp. 578-786. ISSN 1993-8233

Stone, N. (2011). The „sexting" quagmire: Criminal justice responses to adolescents' electronic transmission of indecent images in the UK and the USA. Youth Justice, 11, 266–281.

Streichman, J. (2009). What is sexting? Examiner.com. Online: http://www.examiner.com/mental-health-education-in-phoenix/what-is-sexting

Shariff, S. & Churchill, A. H. (2010). Truths and Myths of Cyber-bullying: International Perspectives on Stakeholder Responsibility and Children's Safety (1st ed.). New York: Peter Lang.

Smetáčková, I., Pavlík, P., Kolářová, K. (2009). Sexuální obtěžování na vysokých školách: Proč vzniká, jak se projevuje, co lze proti němu dělat. Praha: Fakulta humanitních studií UK, 2009.

Smith, B. (2010) Social Media User Statistics. Haley Marketing. Online: http://www.haleymarketing.com/2011/06/16/social-media-user-statistics/

Smith, P. K., Mahdavi, J., Carvalho, M. (2010). Cyberbullying: It´s nature and impact in secondary school pupils. The Journal of Child Psychology and Psychiatry, 49, 376–385.

Smith, P. K., & Sharp, S. (1994). School Bullying: Insights and Perspectives (1st ed.). London: Routledge.

Sourander, A., Klomek, A. B., Ikonen, M., Lindroos, J., Luntamo, T., ion-Based Study. Arch Gen Psychiatry, 67, 720–728.

Šmahaj, J. a kol. (2012) Virtuální šikana a její psycho-sociální konsekvence u vysokoškolských studentů. Olomouc: Univerzita Palackého v Olomouci. Online: http://www.kyber-sikana.eu/o-projektu/.

Smith, G. (2012) 'Just spat on a working-class person': Cambridge University chat site taken down amid cyber-bullying accusations. London: DailyMail. Online: http://www.dailymail.co.uk/news/article-2144176/Just-spat-working-class-person-Cambridge-University-chat-site-taken-amid-cyber-bullying-accusations.html

Sullum, J. (2012). No Sex Tape, No Outing in Tyler Clementi Case. Reason.com. Online: http://reason.com/blog/2012/02/28/no-sex-tape-no-outing-in-tyler-clementi

Vašutová, M. (2010) Proměny šikany ve světě nových médií. Ostrava: Ostravská univerzita.

Weisskirch, R. S., & Delevi, R. (2011). "Sexting" and adult romantic attachment. Computers in Human Behavior, 27, 1697–1701.

Willard, N. (2007). Educator's Guide to Cyberbullying and Cyberthreats. Center for Safe and Responsible Use of the Internet. Online na http://www.cyberbully.org/cyberbully/docs/cbcteducator.pdf. Cit. 22. 4. 2010.

Wysocki, D. K., & Childers, C.D. (2011). "Let My Fingers Do the Talking": Sexting and Infidelity in Cyberspace. Sexuality and Culture, 15, 217–239.

Ybarra, M., Espelage D. L., Mitchell, & K. J. (2007). The Co-occurrence of Internet Harassment and Unwanted Sexual Solicitation Victimization and Perpetration: Associations with Psychosocial Indicators. Journal of Adolescent Health,4, 31–41.

12 About author

Mgr. Kamil Kopecký, Ph.D.

Head of E-Bezpečí project, head of Centre for the Prevention of Risky Virtual Communication of Faculty of Education of Palacký University in Olomouc, coordinator of project E-Bezpečí for teachers, coordinator of project E-Synergie - scientific network for risks of electronic communications, head of Online advisory centre of E-Bezpečí. Expert for safety research, development and innovation of Ministry of the Interior, guarantor of Methodical portal of Research Institute of Education in Prague - module Safety Internet.

Within his pedagogical activities he deals with media education and risks connected to mass media, further with communication and information systems, modern trends in electronic communication and risky communication within the virtual environment. He actively takes part in number of grant projects focused on the areas of risky behaviour in the virtual environment, crisis prevention, computer crime and safety research (cyberbullying, cybergrooming, sexting, stalking, cyberstalking, social networks, personal data protection). He is an author of many expert essays dealing with problems of risky behaviour of children within the Internet environment and mobile phones, with crisis prevention, computer crime and safety research.

He closely cooperates with the Police of the Czech Republic (consultant for cases related to the Internet crime), Google, Seznam.cz and Vodafone.

Further information about the author can be found on the following websites:
www.e-bezpeci.cz, www.prvok.upol.cz, www.sexting.cz,
www.e-nebezpeci.cz.

13 List of graphs

14 Index

15 L'Annotation (FR)

La monographie Le comportement à risque de l´usage d´internet chez les étudiants de la Faculté pédagogique de l´Université Palacký s´oriente vers la caractéristique complexe des formes particulières du comportement à risque chez les étudiants d´université et se focalise en même temps sur les effets que les étudiants rencontrent immédiatement.

Elle résume les résultats de la rechcerche orientée vers le phénomène du cyber harcèlement en observant son apparition à travers les formes fondamentales du cyber harcèlement. En plus, elle se focalise sur le domaine de grooming et elle poursuit les manières de communication et les manipulations conséquentes des étudiants, la présence des invitations aux rencontres personnelles avec les utilisateurs inconnus d´Internet et les réactions des étudiants sous ces impulsions. La monographie s´oriente aussi vers le phénomène du textopornographie, vers sa pénétration parmi la population des étudiants, vers les cas concrets du textopornographie et vers le niveau concernant le droit pénal de ce comportement.

Les chapitres suivants se focalisent sur les réseaux sociaux en rapport avec les étudiants, sur les données à caractère personnel qu´ils partagent avec les autres utilisateurs dans le milieu des réseaux sociaux et aussi sur les mots de passe, que les étudiants choississent pour leurs accès aux services d´Internet. Une partie indépéndante de la monographie est présentée par l´analyse des mots de passe choisis par les étudiants pour se connecter à leurs comptes. Les mots de passe sont caractérisés en tenant compte de la forme, du contenu et de la façon d´utilisation.

La monographie observe les cas types de l´apparition du comportement à risque sur l´Internet du monde entier et elle se focalise aussi sur les causes du cyber harcèlement des professeurs de l´université.

La partie finale de la monographie est dédiée aux possibilités diverses de l´éducation et de la prévention dans cette domaine, aux formes choisies et aux méthodes, avec lesquelles on peut soutenir l´utilisation sûre d´Internet chez cette groupe détérminée.

Les mots clés:

cyber harcèlement, grooming, textopornographie ingénérie sociale, réseaux sociaux, risques de la communication d´Internet

16 Summary (EN)

The monograph *Risky behaviour of students of Palacky University in the Internet environment* is aimed at complex characteristics of different forms of risky behaviour of students, focusing on the phenomena which students encounter.

The monograph summarizes the results of research on cyberbullying, while monitoring its occurrence across the basic forms of cyberbullying. It also focuses on the area cybergrooming, it tracks communication methods and subsequent manipulation of students and it monitors the presence of invitations to personal meetings with unknown Internet users and students reactions to this stimulus.

The monograph also focuses on the phenomenon of sexting, its penetration into the population of students; it is also aimed at specific cases of sexting and the criminal level of this behaviour.

Other chapters focus on the social networks in relation to students, personal information that users of social networks share with other users, as well as students´ passwords they choose to access the Internet services. Independent part of the monograph is the analysis of passwords chosen by the students to access their accounts. Passwords are characterized with regard to the form, content and method of use.

The monograph also monitors selected world cases of risky behaviour in the Internet and also focuses on cases of cyberbullying of university teachers.

The final part of the monograph is devoted to various possibilities of education and prevention in this area, the selected forms and methods which can support safer use of the Internet for this target group.

Keywords:
cyberbullying, cybergrooming, university students, cyberstalking, social networks, passwords

17 Аннотация (РЯ)

Монография «Рисковое поведение студентов Педагогического факультета Университета им. Палацкого в среде Интернета» сосредоточится на комплексной характеристике отдельных форм рискового поведения студентов высших школ, а также на явлениях, с которыми студенты непосредственно сталкиваются.

Данная монография подводит итоги исследования, посвященного феномену кибермоббинга и описывает места проявления данного явления насквозь всеми его формами. Работа также посвящена области кибер-груминга, в которой показываются способы коммуникации и последующая манипуляция студентов; далее перечисляются присутствия обращений с целью личной встречи с анонимными пользователями Интернета и реакции студентов на такое предложение. Монография также посвящена феномену секстинга и ему распространению в студенческой среде, конкретным случаям секстинга и характеру данного явления с точки зрения уголовного права.

Следующие главы посвящены социальным сетям в отношении ко студентам, личным данным, которые в среде социальных сетей становятся общими. Речь также идет о паролях, которые студенты используют для входа в интернетовские сайты. Самостоятельная часть монографии дополняется анализом паролей, которыми студенты используются для входа в свои аккаунты. Пароли характеризуются в отношении к форме, содержании, а также к способу назначения.

Монография также описывает некоторые мировые случаи появления рискового поведения в среде Интернета, а также сосредоточится на казусах кибермоббинга преподавателей.

Последняя часть монографии посвящена разным возможностям воспитания и профилактике в данной области, а также выбранным формам и методам, с помощью которых можно поддержать безопасность целевой группы во время использования Интернета.

Ключевые слова:

кибермоббинг, кибер-груминг, секстинг, социальная инженерия, социальные сети, риски коммуникации в Интернете

Mgr. Kamil Kopecký, Ph.D.

RISKY BEHAVIOUR OF STUDENTS OF FACULTY OF EDUCATION OF PALACKÝ UNIVERSITY IN OLOMOUC WITHIN THE INTERNET ENVIRONMENT

Publication is intended for professional community

Executive editor doc. Mgr. Miroslav Dopita, Ph.D.
Responsible editor Jana Kreiselová
Technical editor Mgr. Kamil Kopecký, Ph.D.
Cover design and edition Mgr. Kamil Kopecký, Ph.D. & Fotolia

Publication did not go through editorial finishing procedure.

Published and printed by Palacký University in Olomouc

Křížkovského 8, 771 47 Olomouc
www.vydavatelstvi.upol.cz

E-mail: vup@upol.cz

www.e-shop.upol.cz

1st Edition

Olomouc 2014

Book series - Monograph
Not for sale publication
ISBN 978-80-244-4107-8