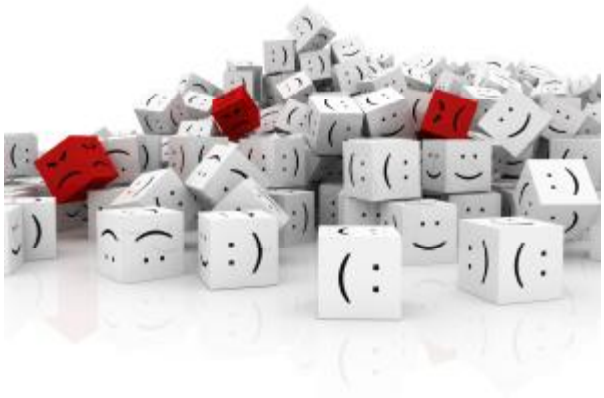
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Realized in a project:
Nebezpečné komunikační jevy pro učitele se zaměřením na
kyberšikanu, kyberstalking, kybergrooming a další sociálně-patologické jevy

Registrační číslo: CZ.1.07/1.3.13/02.0040



CYBER GROOMING
DANGER OF CYBERSPACE

(study)

Mgr. Kamil Kopecký, Ph.D.

Olomouc, 2010

ISBN 978-80-254-7573-7

A. Characteristics of Cyber Grooming 3
B. Stages of child's manipulation 5
1. Preparation of the contact 5
2. Contact with a victim, establishing and deepening the relationship 6
3. Preparing for a personal appointment 8
4. A personal Meeting 8
C. Other features of Cyber Grooming 9
D. Cases of Cyber Grooming 10
Czech Republic 10
Foreign countries 11
E. Legal Framework of Cyber Grooming in Czech Republic 14
F. Cyber Grooming Protection 15
Basic rules for children and youth 15
Rules for Parents 15
About the Author 17

Cyber Grooming – Beware of Internet Users

The Internet is an instrument used by millions of users all over the world. It serves them to search information, to work and entertain, communicate, establish social relations with other people. In the real world we meet different people, and that goes for within the Internet as well – thanks to its expansion we might communicate with the users from all over the world, even with those we would have never met in person. But these users might also be exposed to some dangers the Internet provides. In this part we will focus on one of the most dangerous Internet phenomenon – cyber grooming.

Cyber grooming (child grooming, grooming) represents the Internet users' behaviour (predators, cyber groomers) which is supposed to raise false confidence and make victim come to a secret personal meeting. The sexual abuse of the victim, physical violence or child prostitution and pornography abuse might be the results of this rendezvous which means that cyber grooming is a kind of psychological manipulation carried out through the Internet, mobile phones and other relevant technologies[1] (Berson, I. R., 2002, O'Connell, 2001, Kopecký, K., 2008).

A. Characteristics of Cyber Grooming

1. Where does cyber grooming occur

Cyber grooming is often subject to synchronous and asynchronous communication platforms, most often public chat, internet dating, instant messengers and VoIP (e.g. ICQ, Skype) and recently also social networks (Facebook, Twitter, MySpace, Bebo and others). Cyber grooming takes place by lot of researches (CEOP[2], 2008 and more) most often in instant messengers' environment (56% of cases) and social networks environment (11,4% of cases). Internet predators, however, except these communication environments use also advertising portals, where they offer various opportunities of employment or career to children (e.g. in modelling). They also often visit portals geared to infant Internet users (children's portals, leisure activities portals, gaming portals and other sites).

2. How long is the child's manipulation?

Mental manipulation within the cyber grooming is in progress usually a long time – from about 3 months to several years. This time is directly dependent on the type of manipulation and the gullibility of the victim. There are cases when a predator manipulated a child for 2 years before the personal meeting and sexual abuse.

3. Who are the victims?

Cyber grooming victims are children and young people usually aged 11-17 years, more often girls than boys[3]. It can be assumed that the victims are mainly those Internet users who spend a lot of free time in onlone communication environments (chat, instant messengers, social networks) where they establish virtual contacts with others (looking for friends and life partners here). In recent years cases

[1] Berson, I. H. 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

[2] Child Exploitation and Online Protection Centre. Online: http://www.ceop.gov.uk/mediacentre/pressreleases/2008/ceop_12092008.asp

[3] Kim-Kwang Raymond Choo. Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences. Australian Institute of Criminology, 2009.

of cyber grooming occurred at some of the social networks (Facebook, MySpace, Twitter etc.) have become more prevalent. These social networks with an elaborate system of virtual social relations provide ideal conditions for cyber grooming's realization.

Children and young people are more susceptible to manipulation because they do not yet have fully developed social skills and they have a lack of life experience (Lamb & Brown, 2006). Studies suggest that the attackers used this fact when selecting victims.

Among the most common victims are:
a) *Children with low self-esteem and lack of self-confidence* (it is easier to emotionally or physically isolate them),
b) *Children with emotional problems, victims in need* (often seeking compensation for their parents and needing a helping hand),
c) *Naive and excessively trusting children* (they are willing to engage in online conversations with strangers, it is more difficult for them to recognize the risk communication),
d) *Adolescents/teenagers* (interested in human sexuality, they are willing to talk about it).

4. Who are attackers?

Cyber attackers (predators) are a heterogeneous group in which we can find both low and high social status users (lawyers, teachers, police officers). In many cases the victim knows the offender and is dependent on him (in 85-95% of cases[4]), often the attacker is also a victim's family acquaintance. According to researches, people have not been punished yet predominate among the attackers. But sometimes even those condemned for sexual assaults against children and juveniles become cyber groomers, and they suffer a relapse. Most of the attackers were diagnosed with a pathological interest in children. The behaviour of attackers – cyber groomers - for example, is explained in the model of social skills (Emmers-Sommer, Allen 1999, Olson 2007), in which attackers make contacts with children because they fear their relationship with adults. Cyber groomers perceive relationships with children as less threatening; they feel safer than in relationships with adults.

[4] The same source.

B. Stages of child's manipulation

The process of manipulating the child goes through four basic phases (preparation of the contact - contact with the victim - a preparation for a personal appointment - a personal meeting), during which the attacker uses a large number of techniques and procedures.

1. Preparation of the contact

At this stage, the attacker prepares the ground for implementation of the victim's manipulation.

False Identity
One of the most frequently observed practices of the attacker – cyber groomer – is to create a false identity. The attacker provides false personal information about himself such as name, age or a facial picture. The attackers are usually much older than chosen victims, for that reason they adjust their age and photos as necessary to complete the matches.

The identity of the attacker can exist in several basic forms:
A. Static identity - an attacker creates one identity and by means of this identity he addresses chosen victims (e.g. Facebook user profile).

B. Dynamic identity – an attacker adjusts the identity according to his needs, and therefore he may appear under different nicknames/avatars. The attacker can intentionally adjust the hobbies and interests, or even sex and other personal information to approach chosen victim as effectively as possible. The attacker with a dynamic identity often communicates with multiple victims at once, so he must remember or record what he said and to whom. To maintain a dynamic identity is for an attacker much more challenging than to maintain the static one, and the result of this can be a replacement of the victim he currently communicates with another victim. Thus, if the victim records apparent contradictions in virtual communication (e.g. user re-enter a different age, name or other information), it may be a signal that the victim communicates with a cyber groomer.

False Authority
Sometimes attackers do not act as individuals but as companies' representatives (managers, directors), which will bring some benefit to chosen victims (children). There are cases where the attacker pretended to be a business executive specializing in financial assistance to socially disadvantaged children. On behalf of this company he then related to potential victims through Internet adverts. The authority of the company (albeit fictional) supplied the credibility to the information spread on the Internet.

Attacker's advertisement could look like this:
Hello friends. Are you under 15? Do you like computers? Do you like browsing the Internet? Take part in our competition and win fabulous prizes. Just send us your name, e-mail address and phone number and you will be included in a draw. Look forward to a fast computer, mobile phones, branded clothes and other gifts.
Email us at: soutezvip@seznam.cz.

2. Contact with a victim, establishing and deepening the relationship

In the second stage of manipulation the attacker establishes a contact with the victim and continues to work to build and sustain a virtual relationship.

The effect of mirroring

A characteristic feature of the cyber groomer's behaviour is the effect called mirroring. The predator copies the victim in an attempt to break the barrier; he behaves like a mirror reflection of the victim. If the victim tells the attacker that he feels lonely, for example, and has some troubles, the predator responds that he has similar problems and fully understands it, offering the victim that he can confide to the attacker. Thanks to the effect of mirroring the attacker creates a feeling of friendship by the victim, which helps the victim to overcome the fear of communicating with strangers[5]. Mirroring does not have to be associated only with emotional level of the relationship with the victim; it may also induce a sense of belonging to imaginary common hobbies, opinions on various topics etc.

Example of mirroring

teddy_15: Hey cutie, how are you?
cutie_13: I'm fine, I'm bored.
teddy_15: Can I get bored with you?
cutie_13: Maybe.
teddy_15: How old are you?
cutie_13: 13, and you?
teddy_15: 15, and what do you like?
cutie_13: I love Hannah Montana...
teddy_15: I totally love it!!! And do you do any sport?
cutie_13: Riding inline skates.
teddy_15: I also drive inline skates sometimes, it's great fun ... Where are you from?
cutie_13: From Prague. And you?
teddy_15: I am also from Prague. Where exactly? Any hint?
cutie_13: ... well, Smíchov.

Trying to get as much personal information about the victim (fishing)

In addition to personal data (name, age, and photo) is a predator trying to find out more information - e.g. name of the school the pupil is attending, favourite celebrities, interests and hobbies etc. These data use the attacker for building a general profile of the victim[6].

Shaping of victims

Offenders often create profiles of victims. In compiling the profiles they use the data provided by the victims within their mutual communication and also the records which they found on the web while searching.

Users of the various web portals always disclose only some personal data for fear for their safety. Therefore the attacker usually does not find all personal information at one page. But if potential

[5] Methods of Predators. iKeepSafe.org. Online: http://kids.yahoo.com/parents/online-safety/1706/4--Methods+of+Predators
[6] Methods of Predators. iKeepSafe.org. Online: http://kids.yahoo.com/parents/online-safety/1706/4--Methods+of+Predators

victims publish for example their e-mail address or other information that clearly points to them (ICQ number, phone number etc.), the attacker may be able to trace them due to these data. By means of Internet search engines (Google etc.), the offender can find out where the victim used this information, and gradually add other personal information to the profile of the victim. For example telephone number, which the victim mentioned in advertisements, school address from the victim's profile on a social network etc. The information victim told the attacker (age, sex of the child, address and other personal data) can be verified by the attacker in the same way, too.

Luring and bribing the victim

To establish as close relationship with the victim as possible, the attacker often uses various forms of bribes and "gifts" including money, mobile phone credit, modern technology (mp3 players, mobile phones), computer games, branded clothes etc. These bribes might help to verify a personal information received from the victim (e.g. a phone number or address of the victim where the bribe would be sent), and also increase cyber groomer's credibility. Another use of the bribe is to obtain the most sensitive information which is a photograph of the child's face.

The bribe could turn into a powerful weapon. This is shown by the cases of victims who came back for the bribes to the attacker for several times and allowed to be repeatedly abused by them. In this context we can talk about child prostitution.

Reducing barriers of children and young people by introducing a sexual content to the conversation

The aim of this described conduct is the effort to progressively reduce barriers of children and youth in the area of sexuality by gradually introducing sexual content to the conversation[7].. That could be primarily a discussion of human sexuality, sexual life of victim's parents, the attacker may offer a variety of erotic or pornographic material to the child, for example to arouse the interest and reduce their shyness. Of course, the attacker aims to obtain photographs or videos of naked victims (for example he is trying to force the victim to show himself at the webcam or to send him his naked photos). If the predator gets these highly sensitive materials, he can use them to blackmail the child/minor (e.g., more Berson, IR, 2002).

Attempts to isolate the victim from the vicinity

The willingness to confide in a stranger on the Internet is due to anonymity much easier than in a real life, because we do not face the immediate consequences on the Internet which could be caused by our communication (but we do face the consequences in a real physical world). The attacker uses the victim's willingness to confide the confidential information to his advantage. Gradually, the attacker becomes an irreplaceable friend for the child, the one and only who child unloads his troubles to, and becomes "the exclusive friend" for him.

Using emotional blackmail and intimidation he prohibits child to tell the parents or other people around the child certain information (Do not tell your mother, she would hate you. Do not tell anyone, the others would not understand.). The more confidential information predator knows, the more is the victim fixed and dependent on him. Initially the victim is seeking the predator voluntarily, then by force. Indeed, if the victim wanted to end this relationship, the predator could threaten and blackmail the victim with the publication of their secret communication (If you don't let me hear from you, I'll

[7] Online predators: Help minimize the risk. Microsoft Online Safety. Online: http://www.microsoft.com/protect/parents/social/predators.aspx

write your father what you have told me here). The child is then afraid of the consequences such disclosure could have in his real life (for example, parents could forbid him to use the computer.), and he preferably remains in a virtual relationship with the aggressor.

3. Preparing for a personal appointment

The aggressor has available discriminatory information and personal data of a victim and is planning a personal meeting. Even at this stage the aggressor uses a method of targeted manipulation.

The technique to overcome the age difference between an attacker and a victim

Within the case study we can find a lot of cases where a cyber attacker used specific techniques designed to overcome the age difference between him and the victim. This technique works like this: an attacker communicates with the victim for a few weeks under a false identity under which he claims to be a minor. After some time the attacker informs the victim that his father banned him from using the Internet, but his thirty years old brother (another identity of the same attacker) would like to continue with the communication. On the basis of this communication, the victim subsequently accepted the fact that he communicates with a person who is already an adult - thus much older[8].
There are also cases where a cyber groomer claimed to the victim that he would be picked up in a personal meeting by an elderly person, aggressor's father or sibling. And this person was just the attacker who drove the victim to a "safe place" and then sexually abused him there.

Threatening and blackmailing a victim

At a moment when the predator has enough information about the victim and sensitive materials, he can try to invite him to a personal meeting.
If the victim refuses to arrive to the appointment, the attacker begins to blackmail her. He threatens the victim with publication of compromising material – for example with sending of nude photos to his friends and parents, or printing the materials and posting them up around the victim's residence and school. The aggressor may also claim to publish discriminatory photos on the Internet with derogatory tags of the victim (e.g. *John Smith is gay! This is his phone number XXX-XXX, call him! Jane Novak is a dirty whore! Write to her e-mail XXX-XXX* etc.). A lot of children cannot resist to these threats. They rather attend the meeting than being subjected to humiliation by others.

However, the pressure from the attacker is not always necessary because a lot of victims are willing to go to a meeting without prior extortion.

4. A personal meeting

A personal meeting is the main cyber groomer's effort and logical ending of previous stages.

Continued manipulation

The first meeting of the attacker with the victim may be totally innocent; there does not have to be sexual or other abuse of the victim. At the meeting, the attacker can verify whether the victim is really a minor, whether there is no deployed agent (in some countries, these agents are common tools to combat abuse of minors). At the meeting the attacker may also intensify a relationship with the victim by another gift (bribe). The victim will come to believe that the attacker is harmless and that he is

[8] Berson, I. H. 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

indeed the “exclusive friend”, whom he has passed off on the Internet. Therefore, an attack could occur after up to several personal meetings.

An assault on the victim

An assault (sexual assault, physical assault etc.) has immense consequences for the victim, as in the physical and especially the psychological aspect. If a cyber groomer has plenty of powerful tools for manipulating, he may force the victim into repeated meetings at which the attacks continue.

C. Other features of Cyber Grooming

Creating of predators’ networks

A frequent phenomenon we encounter in general practice is creating organized groups of online predators – cyber groomers, who work together. These sharing networks participate for example in child kidnapping – the child is forced by manipulation to a personal meeting, then kidnapped and taken to another country, where is abused sexually, physically tortured, used for the production of child pornography etc. Predators’ networks often collect victims’ personal profiles into databases to be used by other network members.

The case from the USA

A fourteen-year-old girl received a new present from her parents – a new computer. After two months of using the internet she met an adult man in a chat room, whom she also maintained the e-mail correspondence with. When her parents learned about that, they took a number of necessary steps to prevent this contact – they removed a keyboard from her computer, monitored her e-mail and phone calls and also sought psychological counselling help. Unfortunately, the pupil maintained the communication with the attacker via a mobile phone which he sent her. After several months she disappeared from home. When police searched the girl's computer, they discovered a number of e-mails that led to a paedophile network, communicating between Europe and the USA. A paedophile user from Greece, thanks to this network, "ordered" a minor girl from the U.S., secured a false passport and provided funds to transport the girl from the U.S. to Greece. After five months the girl was returned to her parents. At first she argued that she had loved and adored the paedophile groomer, but after extensive therapeutic treatment she began to remember details of sexual and physical torture, she began to have suicidal tendencies and had to be hospitalized in a psychiatric clinic. The girl is recovering gradually, but her experience and the trauma will accompany her for the rest of her life[9].

[9] Berson, I. H. 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

D. Cases of Cyber Grooming

Cyber grooming cases can be found both abroad and in the Czech Republic itself. According to Hana Petráková, director of the Safety Line Association (Linka bezpečí), luring somebody into a personal meeting makes currently 8% of 2009 registered cases[10]. The number of cases in which an unknown person wants to arrange a personal meeting over the Internet with a minor, continues to grow (both in the Czech Republic and abroad). In the next part of our e-learning course we will focus on real cyber grooming cases that have been addressed in recent years.

Czech Republic

Pavel Hovorka

One of the most tragic known cases of cyber grooming is a case of convicted deviant Pavel Hovorka. Pavel Hovorka, a printing office porter in Prague, was sentenced in 2008 for sexual abuse, blackmail, seducing to a sexual intercourse and endangering the morals of youth. The criminal acts related to 20 minor boys, 8 of which man actually forced into sexual intercourse. He was sentenced to 6.5 years in prison (the original sentence of 8 years was mitigated by the court of appeal).

The court found porter Hovorka guilty of abusing twenty underage boys from 2005 until his arrest in 2007, who were chosen from among the children in children's homes or contacted through the Internet dating services (especially on the server Lide.cz), with some of those he was also chatting. He lured the victims into a fictional competition "The VIP Child" in which the winners were promised to spend two weeks in Prague and to win interesting prizes.

Many victims who arrived at the private meeting were forced into sexual intercourse. He offered money to children for sexual intercourse, some of them he blackmailed. Abused boys were photographed and filmed. Then he threatened boys to reveal their homosexual orientation and publish a nude photographs (the victims had sent him some photographs in return for payment, some photos he took himself), unless they would continue to visit him. Some boys resisted, and so he raped them (according to the charge) [11].

From the prosecutor's speech

"*The accused lied down from behind next to the injured person, who he first kissed all over the body, on a folding bed at the printing's office reception, where he worked as a guard, reaching anal intercourse,*" prosecutor described one of the twenty-eight Hovorka's criminal acts. Because Hovorka often photographed his victims, he used that for further meetings with the boys. "*He threatened the victim to let the neighbourhood know about his homosexuality in order to convince him to come to other meetings,*" said the prosecutor[12].

---

[10] Petráková, H. Linka bezpečí jako asistenční linka pomoci projektu SaferInternet. Online: http://konference.e-bezpeci.cz/?akce=view&id=petrakova

[11] Třeček, T., Šťastný, J. Deviant Hovorka se dočkal za zneužití dvaceti chlapců mírnějšího trestu. iDNES. Online: http://zpravy.idnes.cz/odvolaci-soud-rozhodne-o-trestu-za-zneuziti-jednadvaceti-chlapcu-p9q-/krimi.asp?c=A090526_073207_krimi_cen

[12] Bublinová, A. Za zneužití dvaceti chlapců půjde Hovorka na osm let do vězení. Mediafax. Online: http://www.mediafax.cz/krimi/2814724-Za-zneuziti-dvaceti-chlapcu-pujde-Hovorka-na-osm-let-do-vezeni

Photo: Pavel Hovorka coming to the court
Author: René Volfík, ČTK

Foreign countries

United Kingdom
Michael Wheeler

In 2003, British paedophile Michael Wheeler (35 years old, an electrical engineer) confessed to 11 sexual attacks on underage girls, two of the girls being sexually abused by him. He was sentenced to three years imprisonment[13].

Wheeler used the public chat to meet the girls. There he also made a contact with one of the abused girl who was at that time 11 years old. Gradually he manipulated her, discussed various (e.g. sexual) issues with her etc. The girl began to confide in him more and more and gradually she became emotionally dependent on him.

Shortly after her 13th birthday he began to harass her and sexually abused her.

In the case that Wheeler sexually abused the victim at the time when she was under 13 years old, he would be according to British law in danger of being sentenced to life imprisonment. The police believe that he waited for reaching of this age limit on purpose[14].

Andrew Lay
In 2003, a 35-year old locomotive driver Andrew Lay was sentenced to 6 years in prison for sexual abuse of 12-year-old girl.

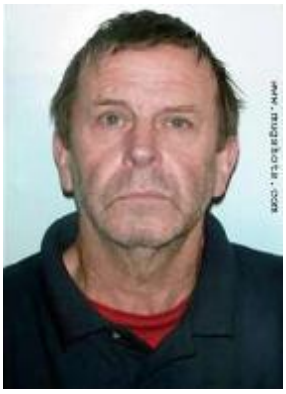
He met the minor in a chat room, where pretended to be 28 years old[15]. He began to bombard her with e-mails, exchanged phone number with her and began to send her text messages (up to several dozen

[13] Internet 'grooming' law moves closer. BBC News. Online: http://news.bbc.co.uk/2/hi/uk_news/politics/3067607.stm
[14] Chat room paedophile jailed. BBC News. Online: http://news.bbc.co.uk/2/hi/uk_news/england/2969020.stm
[15] Chat room pervert is jailed for 6 years. Milton Keynes Citizen. Online: http://www.miltonkeynes.co.uk/news/Chat-room-pervert-is-jailed.252989.jp

messages a day). He also persuaded the girl to take the photo and send him a picture of her; he was paying her phone charges and giving her gifts (alcohol, digital camera, etc.).

Gradually he convinced her to start skiving off the school and meet with him instead. He met the girl for several times personally and sexually abused her (as before her 13 birthday, and after her birthday, too).

Douglas Lindsell



In 2003, a former postman Douglas Lindsell (64) was sentenced to 5 years in prison for molesting several girls and an attempted rape.

Lindsell got acquainted with the girls through the Internet chat, where he claimed to be 15 years old. Sometimes this statement was accompanied by the information that he was dying of cancer. He even made two girls aged 13 and 14 years to come to a personal meeting. Fortunately, they managed to run away and escape the rape. Then Lindsell called them and threatened to find and rape them[16].

He was sending his nude photos to many girls as well (sometimes his own, sometimes photos of his son), he also write down his address at one of the pictures, which later led to his capture.

Lindsell kept a database of more than 70 children, which included details such as hair colour and length, eye colour, clothes, school, family information and other intimate details such as the type of bra size and what sexual practices a child likes or dislikes[17]. Through the Internet and mobile phones he communicated with more than 73 girls (54 from Great Britain, 19 from abroad, including for example Canada and New Zealand). For this purpose he bought a book about teenage slang so that his messages were more convincing.

He continued in communication with the girls even after his imprisonment.

Peter Chapman

Peter Chapman (32 years) was sentenced to life imprisonment in March 2010. Through social network Facebook he met the 17-year-old girl Ashleigh Hall. He lured her out under a false identity to a personal meeting, where he raped and murdered her.

Thirty-three-year old deviant Peter Chapman has once already been punished for sexual violence in the past. He served 7 years for the rape of prostitutes and after the release he should have been under regular police surveillance. However, he has stopped reporting to the police since April 2008. The

[16] The perfect family man who preyed on young chatroom girls. Guardian. Online: http://www.guardian.co.uk/uk/2003/oct/10/childprotection.society

[17] Lindsell 'biggest' internet grooming case. BBC News. Online: http://news.bbc.co.uk/2/hi/uk_news/3175700.stm

police announced a nationwide search as late as in September 2009, one month before 17-year-old Ashleigh Hall was murdered[18].

Within the social networks Chapman created a fake profile[19] on Facebook (he used the name Peter Cartwright and the age of 19 years, but he used also other profiles). Using Facebook he contacted the nursing care student Ashleigh Hall and after quite a long time arranged an appointment with her. He introduced himself face to face with Ashleigh as her virtual friend's father and in an isolated area near Sedgefield her first raped and then strangled her[20]. The police found out about Chapman the next day, when they stopped him by chance in connection with his suspicious license plate of his car. Chapman confessed to the murder of the girl unwittingly, assumed that the police arrested him on suspicion of murder.

When the case was made public, other girls who were visually similar to the murdered Ashleigh Hall began to contact the police. These girls were also contacted by Chapman who tried to make them come to the personal meeting[21].

Chapman's Facebook profile contained more than 3.000 virtual friends = women, age range 13-31 years. He gained personal information from his friends using different Facebook's questionnaires, and there he asked for very personal questions. He also wheedled some sensitive pictures out of some girls (in their underwear, pyjamas etc.). Chapman used other social networks besides Facebook, such as Netlog, Holabox, Profileheaven, Kazoba etc[22].

Peter Chapman. Source: Guardian

[18] Vnouček, P. Facebookový vrah má doživotí. Sociální síť sklízí kritiku. Týden. Online: http://www.tyden.cz/rubriky/media/internet/facebookovy-vrah-ma-dozivoti-socialni-sit-sklizi-kritiku_161662.html
[19] Chapman využíval více identit, uváděl věk 15, 17, 19 let, někdy tvrdil, že je DJ, někdy student, profily měnil dle potřeby.
[20] Carter, H. Merseyside police refers itself to IPCC over Facebook killer Peter Chapman. Guardian. Online: http://www.guardian.co.uk/uk/2010/mar/09/merseyside-police-peter-chapman-facebook
[21] Guy, P. Facebook suspect's ex: He 'killed my double'. The Sun. Online: http://www.thesun.co.uk/sol/homepage/news/2704262/Facebook-suspect-killed-my-double.html
[22] Stokes, P. Peter Chapman targeted thousands of young girls. Telegraph. Online: http://www.telegraph.co.uk/news/uknews/crime/7397894/Peter-Chapman-targeted-thousands-of-young-girls.html

E. Legal Framework of Cyber Grooming in Czech Republic

Cyber grooming (child grooming) as a term is unknown to criminal law (law no. 40/2009 Coll.), therefore is not defined as a criminal offense. However, following offenses[23] may be included here:

1. Human beings trafficking (§ 168) – 1st paragraph, sentence of 2-10 years.
2. Infringement of personal liberty (§ 171) - 1st paragraph, sentence of 2 years.
3. Blackmail (§ 175) - 1st paragraph, imprisonment from 6 months to 4 years.
4. Sexual abuse (§ 187) - 1st paragraph, sentence 1-8 years.
5. Production and other handling of child pornography (§ 192) - 1st paragraph, imprisonment for up to 2 years.
6. Abuse of a child to produce pornography (§ 193) - 1st paragraph, sentence 1-5 years.
7. Endangering child care (§ 201) - 1st paragraph, imprisonment for up to 2 years.
8. Fraud (§ 209) - 1st paragraph, imprisonment for up to 2 years.
9. Dangerous threats (§ 353) - 1st paragraph, imprisonment for up to 1 year.
10. Dangerous stalking (§ 354) - 1st paragraph, imprisonment for up to 1 year

[23] Vlachová, M. Trestná činnost spojená s internetovou kriminalitou. E-Bezpečí. Online: http://cms.e-bezpeci.cz/content/view/226/6/lang,czech/

F. Cyber Grooming Protection

Except for the technical possibilities the most effective defence against cyber grooming is prevention. This resides especially in good awareness of teachers and pupils about the dangers of this web manipulation. Very important preventive tool is a functioning communication between child and parent. The integration of Internet communication issues with unknown users is also significant (and logically also the issues related to risky virtual communication) in the education system (for example, through the framework of educational programs).

There are some basic rules of how to protect against cyber grooming.

Basic rules for children and youth

1. Don't le to be fooled by the promises of virtual attackers (they can promise you love, continuing relationship in the real world, money, gifts, etc.). Remember that people online may lie!

2. Pay attention to inconsistencies in communication with cyber attackers (for example, an attacker specifies a different age as the information he told you about himself before, etc.).

3. Realize why someone would want at all costs to maintain the relationship or the content of Internet communications secret.

4. Set your personal boundaries with regard to sex. Do not accept nor do send materials of a sexual nature to other users.

5. In the virtual environment do not tell anyone your personal information (especially your photos).

6. Never go to a personal meeting, without your parents knowing. Remember, what might happen to you at the meeting and how risky appointment it can be.

7. Be careful of who you talk to and about what you talk to. The Internet communication seems anonymous, but it is not. For instance, you do not want to be traced down by your "Internet acquaintance" in a real world, or forced to do something you do not want.

Rules for Parents

1. Communicate with your children about what they do on the Internet. Remember that even though your child is safe at home and sit at the computer, it does not mean it is safe!

2. Leave the child's computer at a publicly accessible location, such as in the living room, which can be randomly checked.

3. Tell children about the dangers the Internet can pose.

4. In case that your child gets into trouble with the cyber grooming, cyber bullying and other dangerous phenomena of communication, do not use non-functional method of banning your child on

computer and the Internet! Remember that if you ban the child on computer and the Internet at home, it will find another way to reach these instruments (with a friend at school, using a mobile phone, etc.).

About the Author

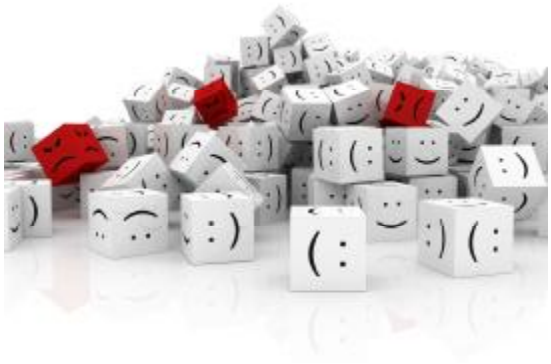
The author is Palacký University graduate (Faculty of Education, Olomouc). He is an assistant professor at Palacký University, manager of E-Bezpečí project (www.e-bezpeci.cz) and of specialized workplace: The Virtual Communication Risk Prevention Centre of Faculty of Education, Palacký University (education of students, teachers, police officers and other experts).
He is also the principal investigator of the project E-Nebezpečí for teachers (www.e-nebezpeci.cz).

He engages in basic dangerous communication phenomena associated with the use of the Internet and mobile phones, especially in cyber grooming, cyber stalking, sexting, social engineering and the risks of social networking. Other areas of interest include the use of ICT and e-learning in education, media education, crime prevention in connection with the ICT coordinator etc. He is the principal investigator of the number of grant projects at all levels (regional, national, ESF). At present he works at the Faculty of Education at Palacký University in Olomouc and in the firm NET UNIVERSITY Ltd.

He is a member of the Scientific Committee SIIN and a member of the Czech pedagogical society.

More information at www.e-bezpeci.cz or www.prvok.upol.cz.

E-mail: kamil.kopecky@upol.cz or info@e-bezpeci.cz.



CYBER GROOMING

DANGER OF CYBERSPACE

Mgr. Kamil Kopecký, Ph.D.

Publisher: NET UNIVERSITY s.r.o.

Year: 2010

ISBN 978-80-254-7573-7

Realized in a project:
Nebezpečné komunikační jevy pro učitele se zaměřením na
kyberšikanu, kyberstalking, kybergrooming a další sociálně-patologické jevy

CZ.1.07/1.3.13/02.0040

www.e-nebezpeci.cz