Rizikové chování studentů Pedagogické fakulty Univerzity Palackého v Olomouci v prostředí internetu

Kamil Kopecký

Olomouc 2013

Univerzita Palackého v Olomouci
Pedagogická fakulta
Centrum prevence rizikové virtuální komunikace

RIZIKOVÉ CHOVÁNÍ STUDENTŮ PEDAGOGICKÉ FAKULTY UNIVERZITY PALACKÉHO V PROSTŘEDÍ INTERNETU

Kamil Kopecký

Olomouc 2013

Recenzenti:

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

Publikace byla realizována v rámci projektu E-SYNERGIE – vědeckovýzkumná síť pro rizika elektronické komunikace (CZ.1.07/2.4.00/17.0062).

1. vydání

ISBN 978-80-244-3858-0
ISBN 978-80-244-3903-7 (elektronická verze)

Obsah

Úvod do problematiky

Předkládaná publikace prezentuje výsledky výzkumu rizikového chování studentů Pedagogické fakulty Univerzity Palackého v Olomouci a sumarizuje zjištění, ke kterým jsme v průběhu analýzy dospěli. Výzkum se zaměřuje na monitoring základních rizikových komunikačních jevů spojených s užíváním internetu a mobilních telefonů, konkrétně na:

a) kyberšikanu (různé formy kyberšikany vázané na internetové služby - verbální agrese, vydírání, vyhrožování, útoky na účet),
b) navazování virtuálních kontaktů (komunikace s neověřenými uživateli internetu, osobní schůzky, tzv. kybergrooming či sociální inženýrství),
c) sexting (veřejné sdílení intimních materiálů v prostředí internetu, poskytnutí těchto materiálů osobě bez ověřené identity, návaznost sextingu na další rizikové komunikační jevy),
d) sdílení osobních údajů v prostředí internetu (se zaměřením na sdílení fotografie obličeje),
e) využívání sociálních sítí (s návazností na výskyt jednotlivých rizikových komunikačních jevů),
f) další související jevy.

Výzkum byl realizován a garantován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci. Navazuje na výzkumy Nebezpečí elektronické komunikace 1 a 2 (2010, 2011) a Nebezpečí internetové komunikace 3 (2012), dále na výzkum Virtuální šikana a její psycho-sociální konsekvence u vysokoškolských studentů (Šmahaj, J. a kol, 2011). **Výzkum byl realizován v rámci OP VK projektu E-Synergie – vědeckovýzkumná síť pro rizika elektronické komunikace (CZ.1.07/2.4.00/17.0062).**

Předkládaná monografie shrnuje pouze základní výsledky výzkumu.

1 Teoretická východiska sledovaných fenoménů

Výzkum rizikového chování studentů Pedagogické fakulty Univerzity Palackého v Olomouci monitoroval fenomény spojené s rizikovým chováním adolescentů v prostředí internetu. V dalším textu proto vymezíme základní teoretická východiska sledovaných jevů, tj. kyberšikany, sextingu, sdílení osobních údajů, sociálního inženýrství a kybergroomingu v prostředí internetu.

1.1 Kyberšikana

Definice kyberšikany využitá v našem výzkumu vychází z existujících definic šikany, ve kterých je šikana vnímána jako *agresivní, úmyslné, opakované jednání či chování prováděné vůči jednotlivci či skupině, který/á se nemůže snadno bránit* (Whitney&Smith, 1993; Olweus, 1999). U dalších autorů je šikana chápána jako *forma obtěžování, které je založeno na nerovnováze sil a systematickém zneužívání moci* (Smith&Sharp, 1995; dále Rigby, 2002). V českém prostředí definuje šikanu zejména M. Kolář a další.

Kyberšikana je v tomto textu definována jako *forma agrese, která je realizována vůči jedinci či skupině s použitím informačních a komunikačních technologií*. Tento čin je prováděn opakovaně (Belsey, B., dále Smith & Slonje, 2007). Obdobně vnímá kyberšikanu Hinduja a Patchin, kteří ji definují jako úmyslné, často opakující se a nepřátelské chování, jehož cílem je ublížit oběti za použití informačních a komunikačních technologií. Nejčastěji prostřednictvím mobilního telefonu a internetu. Definici pak rozvíjí a upřesňují např. Kowalski, Limber a další (2007–2008), kteří vnímají kyberšikanu jako šikanování realizované pomocí e-mailů, ICQ, mobilních telefonů (SMS, MMS, telefonátů), chatu, webových stánek a dalších ICT. Dehue (2008) vnímá kyberšikanu jako trýznění, hrozby, ponižování, ztrapňování a další

útoky realizované pomocí internetu, interaktivních a digitálních technologií nebo mobilních telefonů.

Definice kyberšikany jsou dále rozpracovány i v českém prostředí (Kolář, M., Šmahel, D., Krejčí, V., Kopecký, K., Šmahaj, J., Vašutová, M. a další, 2008-2012), přičemž nedochází k výraznějším odchylkám od zahraničních přístupů.

Kyberšikana mnohdy začíná jako tradiční šikana (psychická nebo fyzická). Její projevy vychází z projevů psychické šikany (např. dehonestování, provokování, vyhrožování, vydírání atd.). Mezi nejznámější (Willard, 2007, Krejčí, 2010) patří:

- **Publikování ponižujících záznamů nebo fotografií** (např. v rámci webových stránek, MMS zpráv)**.**
- **Ponižování a pomlouvání** *(denigration)* (v rámci sociálních sítí, blogů nebo jiných webových stránek)**.**
- **Krádež identity** *(impersonation)***, zneužití cizí identity ke kyberšikaně nebo dalšímu sociálně patologickému jednání** (např. zcizení elektronického účtu)**.**
- **Ztrapňování pomocí falešných profilů** (např. v rámci sociálních sítí, blogů nebo jiných webových stránek)**.**
- **Provokování a napadání uživatelů v online komunikaci** *(flaming/bashing)* (především prostřednictvím veřejných chatů a diskuzí)**.**
- **Zveřejňování cizích tajemství s cílem poškodit oběť** *(outing)* (např. v rámci sociálních sítí, blogů nebo jiných webových stránek, pomocí SMS zpráv apod.)**.**
- **Vyloučení z virtuální komunity** *(exclusion)* (např. ze skupiny přátel v rámci sociální sítě)**.**
- **Obtěžování** *(harassment)* (např. opakovaným prozváněním, voláním nebo psaním zpráv)**.**

- **Kyberšikana spojená s online hrami** (např. krádeže virtuálních postav či předmětů s následným vydíráním, vyhrožováním).

Mezi kyberšikanu řadíme i projevy tradiční psychické šikany posílené využitím ICT, např.:
Dehonestování (ponižování, nadávání, urážení).
Vyhrožování a zastrašování.
Vydírání.
Očerňování (pomlouvání).
A další.

K těmto projevům jsou zneužívány především SMS zprávy, e-maily, chat, diskuze, IM (instant messengeru) a VoIP (např. ICQ, Skype), blogy, sociální sítě nebo jiné webové stránky. Ojediněle se tyto formy objevují uvnitř ve virtuálních vzdělávacích prostředích (virtuálních světech) či online hrách (např. na bázi MMORPG). V rámci našeho výzkumu je kyberšikana monitorována vzhledem k jejím jednotlivým projevům napříč vybranými komunikačními platformami (sociální sítě, IM, chat aj.).

Je zřejmé, že kyberšikana je komplex jevů a její projevy vznikají kombinací tří základních složek - *použité formy psychické šikany, formy šikanujícího obsahu* a *nástroje pro její šíření (Krejčí, Kopecký, 2010)*.

Tabulka 1. Kyberšikana jako třísložkový komplex

Použité formy psychické šikany	**Formy šikanujícího obsahu**	**Nástroje pro šíření kyberšikany**
Dehonestování (ponižování, nadávání, urážení) Pomlouvání Provokování Vyhrožování, zastrašování Vydírání Obtěžování Pronásledování	Text Videozáznam Audiozáznam Grafický záznam (fotografie, obrázek, karikatura) Volání, prozvánění Krádež identity[1] Atd.	Veřejné chaty (textové, videochaty), e-maily, instant messengery, ankety, sociální sítě, virtuální vzdělávací prostředí, online hry, VoIP, SMS, MMS, webové stránky, online datová úložiště (cloud) atd.

Kombinací jednotlivých složek pak vzniká konkrétní forma kyberšikany, např. vydírání pomocí fotografií v prostředí sociálních sítí.

Mezi přidružené či variantní jevy spojené s kyberšikanou patří tzv. *happy slapping*, u dospělých dále *stalking či kyberstalking*.

[1] Vzhledem ke specifické povaze krádeže identity tuto zařazujeme mezi formy šikanujícího obsahu, nejedná se totiž primárně o psychickou šikanu ani o technický prostředek či nástroj.

Happy slapping (v překladu zábavné fackování) je forma fyzické a psychické agrese (Kopecký, 2008, Krejčí, 2010), která byla poprvé zmapována v roce 2005 v jižní části Londýna u hiphopových tzv. „gangsta teenagerů". Podstatou happy slappingu je nečekaně fyzicky napadnout buď mladistvého, nebo dospělého člověka, přičemž komplic agresora celý čin nahrává na mobilní telefon nebo kameru. Získané video poté útočníci umístí na Internet (např. na YouTube, Facebook apod.). Takto pořízené video je určeno k tomu, aby se internetové publikum pobavilo na úkor oběti. Obětí se může stát prakticky kdokoliv – někdo, kdo se jen tak projíždí v parku na kolečkových bruslích nebo běhá, někdo kdo pospíchá na autobus, atd.

S nárůstem útoků na bázi happy slappingu rostla také jejich intenzita, která v některých případech dosáhla až skutečného ublížení na zdraví, v některých případech končícího i smrtí (např. jeden z útočníků střelil nic netušící oběť do nohy vzduchovkou, v jiném případě např. útočníci zapálili oběti vlasy, případně skupina útočníků ukopala k smrti bezdomovce a celou akci si natočila a zveřejnila v prostředí internetu).

Případy happy slappingu jsou rovněž spojené s univerzitním prostředím. Známý je např. příklad happy slappingu, který byl realizován studenty Univerzity v Oxfordu, kteří napadli a natočili jiného studenta z Imperial College v Londýně, který patřil ke konkurenčnímu veslařskému klubu (Miller, 2008). Útočník Colin Groshong, nahrávaný komplicem Nickem Brodiem, se nejdříve konkurenčnímu veslaři Willu McFarlandovi vysmíval, pak jej udeřil do obličeje. Záznam pak zveřejnili prostřednictvím Facebooku, kde jej komentovali další uživatelé. Podrobnosti o případu naleznete v dalších částech této publikace.

Francouzský ministr vnitra Nicolas Sarkozy podal v roce 2007 návrh, aby se na happy slapping pohlíželo jako na trestný čin jako je např. znásilnění. Jeho návrh byl přijat a odstavec o happy slappingu se objevil v článku 44, který se zabývá také zákonem o přepadení. Shrnutí tohoto

odstavce je takové, že happy slapping je kriminální zločin, za který hrozí až 5 let odnětí svobody.

Ve Velké Británii byl takový zločin poprvé potrestán až v roce 2008, kdy byla do vězení na dva roky poslána dívka, která na svůj mobilní telefon natočila muže, jenž byl jejími komplici ubit k smrti. Tento muž zemřel v nemocnici na následky natržené sliznice. Komplicové ve věku 19 a 17 let byli odsouzeni k 7 a 6 letům odnětí svobody.

České právo termín happy slapping nezná, nicméně jeho projevy jsou klasifikovány jako přestupky, přečiny či zločiny.

S termínem happy slapping úzce souvisí termín **cyber-bashing**, což je označení pro různé formy internetových útoků, ve kterých na sebe cíleně útočí dvě skupiny s rozdílným názorem či postojem. Definice tohoto termínu je poměrně nejednotná, termín označuje např. záznamy rvaček žáků či studentů umisťované na YouTube, ale také např. psychickou agresi uživatelů sociálních sítí apod. Cyber-bashing se ve své podstatě prolíná s termínem flaming.

Stalking (lov, pronásledování) je termín, který označuje opakované, dlouhodobé, systematické a stupňované obtěžování, které může mít řadu různých forem a různou intenzitu (Kopecký, 2010, dále Trestní zákoník, § 354). Pronásledovatel svou oběť například dlouhodobě sleduje, bombarduje SMS zprávami, e-maily, telefonáty či nechtěnými pozornostmi (dárky). Ve spojení s využitím ICT u útočníka hovoříme o termínu kyberstalking (cyber-stalking). V tomto případě jde o zasílání různých zpráv pomocí instant messengerů (ICQ), chatu, prostřednictvím VoIP technologií, sociálních sítí apod. Útočník u oběti vyvolává pocit strachu. Nejčastějšími oběťmi stalkingu jsou známé osobnosti (zpěváci, herci, politici), expartneři apod. Od 1. 1. 2010 je stalking trestným činem – je kvalifikován v § 354 TZ jako tzv. nebezpečné pronásledování.

Rozpoznat stalkera nemusí být vůbec snadné a často se to ani nepodaří. Může se jevit jako společensky naprosto normální člověk, o kterém ani jeho nejbližší okolí nemusí tušit, že např. obtěžuje jinou osobu s využitím internetu či mobilního telefonu. Podíváme-li se na profil agresorů, stávají se jimi nejčastěji bývalí partneři obětí (Dressing, 2005), častěji muži než ženy (87 % stalkerů). Z pohledu závažnosti stalkingu však považujeme za problematičtější útočníky ženy – je to zejména pro jejich cílevědomost a systematičnost. Ženy útoky realizují nejčastěji prostřednictvím SMS.

Řada studií realizovaných v mnohých zemích Evropy (např. Dressing, H. Maulk-Backer, H. Gass, P.) poskytuje velmi zajímavá čísla o četnosti stalkingu ve společnosti. Anglosaské studie udávají, že zhruba 4–7,2 % mužů a 12–17,5 % žen se alespoň jednou se stalkingem osobně setkalo. To znamená, že stalking je jev poměrně rozšířený. V první německé studii o stalkingu uvedlo 11,6 % dotázaných, že byli minimálně jednou v životě obětí stalkera. Podle celosvětových výzkumů se oběťmi stalkingu stalo přibližně 10 % populace.

Stalking se v omezené míře objevuje i u vysokoškolských studentů. Do tohoto výzkumu však stalking jako fenomén zahrnut není, proto jej dále nekomentujeme.

1.1.1 Výzkumy kyberšikany u vysokoškolských studentů

Výzkumy kyberšikany u vysokoškolských studentů dokazují, že se jednotlivé formy a projevy tohoto fenoménu staly častou součástí univerzitního života. K prvním studiím zaměřeným na kyberšikanu u vysokoškoláků patří výzkum Finna (2004), který realizoval výzkum na vzorku 339 vysokoškolských studentů na University of New Hampshire. Dochází k výsledkům, že s kyberšikanou se setkalo 10-15 % studentů. Výskyt kyberšikany je v této studii monitorován pouze ve vztahu k e-mailu a instant messengerům, neboť sociální sítě jako základní technologické platformy pro realizaci kyberšikany dosud

nebyly rozšířeny tak, jak je tomu v současnosti. Na výskyt kyberšikany u vysokoškoláků rovněž upozorňuje Dilmac (2009), který uvádí, že 55,3 % vysokoškoláků potvrzuje, že se stalo obětmi kyberšikany alespoň jednou v životě.

Výzkumem kyberšikany u vysokoškoláků se rovněž zabývá Walker, C. a kol., kteří v roce 2008 realizovali analýzu výskytu kyberšikany u 120 amerických vysokoškoláků. Přibližně 50 % respondentů potvrdilo, že se stalo obětmi kyberšikany.

Kyberšikanou u vysokoškoláků se také zabývá např. Nursen Turan, Polat Oguz a kol., kteří realizovali v roce 2011 výzkum na vzorku 579 vysokoškoláků (Istanbul Bilgi University Law School, Istanbul Ticaret University Law School and Marmara University Law School) ve věku 18-30 let. 59,8 % z nich se stalo obětmi kyberšikany, přičemž 80 % z obětí potvrzuje, že byly vystaveny více než 1 formě kyberšikany.

V českém prostředí se kyberšikanou u vysokoškoláků zabývá zejména Šmahaj, J., který se svým týmem realizoval v roce 2011 výzkum kyberšikany na vzorku 647 vysokoškolských studentů. Podle jeho výzkumu 14,8 % respondentů uvádí šikanování prostřednictvím mobilního telefonu nebo internetu ve škole nebo mimo školu, přičemž 6,6 % dotázaných bylo vystaveno souběžně klasické šikaně a zároveň kyberšikaně.

Další zajímavé výzkumné výsledky nabízí Vašutová (2010), která se svým týmem realizovala výzkum kyberšikany na vzorku 1030 vysokoškoláků Ostravské univerzity. Z výsledků vychází, že 6,7 % studentů Ostravské univerzity se stalo obětí kyberšikany.

1.2 Sdílení osobních údajů v prostředí internetu

Výzkumy v oblasti sdílení osobních údajů na internetu, které jsou realizovány v zahraničí, upozorňují na vysoké procento dětí i dospělých sdílejících nekontrolovaně osobní údaje na internetu, zejména

v prostředí sociálních sítí. V rámci naší studie se však zaměříme zejména na cílovou skupinu vysokoškolských studentů.

Podle oficiálních statistik sociální sítě Facebook z roku 2005 mělo na této sociální síti profily 3,85 milionů studentů amerických vysokých škol, což tvoří 85 % vysokoškolských studentů v USA (Arrington, 2005). Ti shodně odpověděli, že běžně s ostatními uživateli Facebooku sdílejí základní osobní údaje, jako je jméno, příjmení a fotografie obličeje, ale také fotografie a videa.

Agazamani (2010) zrealizoval na vzorku 595 švédských vysokoškoláků studii, monitorující, jak tráví svůj čas na Facebooku. Rovněž potvrzuje vysoký stupeň sdílení osobních údajů v prostředí této sociální sítě. Agazamani (2013) dále sleduje, které sociální sítě jsou studenty nejvíce využívány. Na prvních místech nalezneme Facebook, YouTube a Twitter.

Využíváním sociálních sítí se zabývali také Akyildiz, Argan (2011), kteří monitorovali chování 1200 vysokoškolských studentů v prostředí sociálních sítí v Turecku. Ti potvrzují, že Facebook využívá 93,8 % tureckých vysokoškoláků (z nich 57,3 % má aktivní účet na Facebooku déle než 2 roky). Akyildiz a Argan rovněž zjišťují, že průměrný počet „přátel“ připojených k jejich účtům na Facebooku osciluje mezi 101 až 300 přáteli (u 52,2 % respondentů). Mezi nejčastější důvody, kvůli kterým studenti Facebook využívají, patří sdílení osobních údajů a informací, sledování fotografií, videí, událostí, kontaktování přátel z reálného světa a také zábava.

Shambare, Rugimbana a Sithole (2012) realizovali výzkum zaměřený rovněž na využívání sociálních sítí, tentokrát v Jihoafrické republice. Podle jejich výzkumu Facebook využívá 93 % vysokoškoláků, na dalších místech se umístila největší africká sociální síť Mxit (využívá ji 54 %

afrických vysokoškoláků), na dalších místech se umístil Twitter a YouTube.

Podle výzkumu College Students & Social Media firmy Tunheim (2012), který proběhl na několika amerických univerzitách, využívá 96 % amerických vysokoškoláků Facebook, 84 % YouTube a 20 % Twitter. Zajímavé jsou rovněž údaje, které výzkum sleduje ve vztahu k učitelům – 91 % učitelů využívá sociální média (sociální sítě a další podobné platformy) pro podporu své práce – 57 % využívá Facebook, 49 % YouTube a 22 % LinkedIn. Detailní informace o výzkumu a dalších aktivitách naleznete na www.tunheim.com.

Podle českých statistik (Seznam.cz, květen 2013) sdílí v prostředí jedné z největších českých sociálních sítí Spolužáci.cz své osobní údaje 73 771 vysokoškoláků, z nichž 20 877 tvoří muži (28,29 %).

1.3 Sexting

Termínem sexting označujeme pro potřeby této publikace *elektronické rozesílání textových zpráv, vlastních fotografií či vlastního videa se sexuálním obsahem* (Kopecký, 2010-2012), *ke kterému dochází v prostředí virtuálních elektronických médií – zejména internetu*.

Jedna z prvních obecně užívaných definic vnímá sexting jako *akt rozesílání fotografií zachycujících nahotu mezi mobilními telefony či dalšími elektronickými médii, např. internetem* (Streichman, 2009). Sexting je dalšími autory definován jako sexuální materiály vytvářené mladými lidmi (tzv. youth-produced sexual images), které jsou dále šířeny (Wolak, Finkelhor, Mitchell, 2011–2012). Dále sexting definuje např. Sullivan (2011), která do sextingu řadí sugestivní textové zprávy a obrázky znázorňující nahé nebo částečně obnažené děti či dospělé, které jsou dále šířeny telefonem nebo internetem. Množství platforem a nástrojů, které umožňují šíření těchto materiálů, doplňuje Streichman

(2009–2011) o sociální sítě, zejména Facebook a MySpace. V českém prostředí se sexting šíří především pomocí sociálních sítí Facebook, Líbímseti.cz či digitálního úložiště fotografií Rajče.net (Kopecký, 2011).

Výzkumy sextingu probíhají od roku 2009 v celé řadě zemí – v USA, Velké Británii, Austrálii, Kanadě, Číně (Jolicoeur, 2010) a také v České republice (Kopecký, Krejčí, 2010). Zajímavé výsledky o prevalenci sextingu mezi mladými uživateli internetu a mobilních telefonů poskytuje např. výzkum realizovaný v rámci The National Campaign to Prevent Teen and Unplanned Pregnancy (USA, 2009). V rámci tohoto výzkumu realizovaného na vzorku 653 teenagerů ve věku 13–19 let bylo prokázáno, že 38 % z nich odeslalo sexuálně laděné zprávy jiným lidem a 19 % nezletilých dále odeslalo své vlastní fotografie zachycující jejich obnažené tělo jiným osobám. U dospělých ve věku 20–26 (627 respondentů) již sexuálně sugestivní sextingové zprávy odeslalo již 58 % respondentů, přičemž fotografii vlastního nahého těla odeslalo 32 % z nich. Zajímavé je rovněž sledovat důvody, proč je sexting mladistvými uživateli realizován – 71 % dívek a 67 % chlapců odesílá sexuálně laděný obsah své partnerce či partnerovi, sexting se tak stává součástí jejich intimního vztahu. 21 % dívek a 39 % chlapců odeslalo intimní fotografie osobě, se kterou si naplánovali schůzku (The National Campaign to Prevent Teen and Unplanned Pregnancy, 2010).

V českém prostředí byly realizovány pouze první sondáže, které sledují výskyt sextingu zejména v populaci dětí. K prvním výzkumům, které monitorují aktuální stav v oblasti sdílení a odesílání sexuálně laděného obsahu jiným uživatelům internetu, patří výzkum Nebezpečí elektronické komunikace 2 a Nebezpečí internetové komunikace 3 a 4 (Kopecký, Krejčí, Szotkowski, 2010-2012).

Zjištěná data vypovídají o tom, že sexting dosud není v českém prostředí rozšířen tak, jak je tomu např. v USA či dalších zemích.

1.4 Kybergrooming a sociální inženýrství

Termín kybergrooming (child grooming, grooming) označuje chování uživatelů internetu (predátorů, kybergroomerů), které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce (Kopecký, 2010). Výsledkem této schůzky může být sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod. Kybergrooming je tedy druhem psychické manipulace realizované prostřednictvím internetu, mobilních telefonů a dalších souvisejících technologií[1] (Berson, I. R., 2002, O'Connell, 2001, dále Kopecký, K., 2008 aj.).

Kybergrooming je často vázán na synchronní i asynchronní komunikační platformy, nejčastěji veřejný chat, internetové seznamky, instant messengery a VoIP (např. ICQ, Skype) a v posledních letech také na sociální sítě (Facebook, Twitter, MySpace, Bebo a další). Podle řady výzkumů (CEOP[2], 2008 a další) probíhá kybergrooming nejčastěji právě v prostředí instant messengerů (56 % případů), další pozici pak obsadily sociální sítě (11,4 % případů).

Lze však předpokládat, že počet případů kybergroomingu probíhajícího s použitím sociálních sítí několikanásobně vzrostl. Internetoví predátoři však kromě těchto komunikačních prostředí využívají také inzertní portály, na kterých nabízející dětem různé možnosti výdělku či kariéry (např. v oblasti modelingu), často navštěvují portály zaměřené přímo na nezletilé uživatele internetu (dětské portály, portály zaměřené na volnočasové aktivity, herní portály a další internetové stránky).

Psychická manipulace v rámci kybergroomingu probíhá obvykle delší dobu – od cca 3 měsíců po dobu několika let. Tato doba je přímo závislá na způsobu manipulace a na důvěřivosti oběti. Existují případy, kdy predátor manipuloval dítě po dobu 2 let, než došlo k osobnímu setkání a sexuálnímu zneužití.

Zaměříme-li se na diagnostiku útočníků, jedná se (dle sociálního statutu) o heterogenní skupinu, ve které nalezneme uživatele jak s nízkým tak i vysokých sociálním statutem. V řadě případů oběť pachatele zná a je na něm závislá (v 85-95 % případů viz Kopecký, K., 2010). Mezi útočníky převažují dle výzkumů osoby, které dosud nebyly trestány, útočníky se však někdy stávají i ti, kteří již byli za sexuální útoky proti dětem či mladistvým odsouzeni a došlo u nich k recidivě (Choo, 2009). U části z útočníků – sexuálních abuzérů – byla diagnostikována porucha sexuální preference (pedofilie, hebofilie, efebofilie). Nelze však ztotožňovat termín pedofil a sexuální abuzér (Kopecký, 2010, Bartoněk, 2012)!

V některých případech byli útočníci v dětství sami oběťmi kyberšikany či sexuálního zneužívání, byli ponižováni jak ostatními dětmi, tak i učiteli. Celá řada útočníků vyrůstala v neúplné či nefunkční rodině.

V českých podmínkách se často kybergrooming spojuje s termínem sociální inženýrství, pro potřeby této publikace však oba termíny odlišujeme. Sociální inženýrství vnímáme jako soubor strategií jak manipulovat uživatelem internetu, jak od něj získávat osobní údaje a další citlivé materiály apod. Sociální inženýrství je tedy jakýmsi souborem technik a strategií. Primárním cílem sociálního inženýrství však není sexuální zneužití dítěte či dospělého, sociální inženýrství může být zaměřeno např. na průnik na bankovní účet, na získání utajovaných informací atd. Kybergrooming je pak proces, který využívá technik sociálního inženýrství k tomu, aby donutil oběť dorazit na osobní schůzku, přičemž primárním cílem kybergroomingu je sexuální zneužití oběti.

Vzhledem k povaze cílové skupiny zletilých vysokoškolských studentů v rámci této práce vnímáme kybergrooming pouze jako **proces manipulativních technik, který vede k osobní schůzce s obětí**, nerozlišujeme však, zdali je obětí dítě (osoba mladší 18 let) či student.

V rámci manipulace studentů lze totiž většinu z technik použít i na dospělé uživatele internetu.

Mezi základní techniky, které lze využít k manipulaci studentů, patří (Kopecký, 2009):

a) manipulace pomocí mirroringu[2], tzv. zrcadlení,
b) sociotechnické metody získávání osobních údajů o studentech, profilování obětí (phishing, pharming),
c) uplácení obětí (luring),
d) manipulace využívající intimních materiálů studentů (bez prvku vydírání či s prvkem vydírání) atd.

Ve vysokoškolském prostředí se však setkáváme i s dalšími formami manipulace, zejména manipulací „z pohledu moci". Ta má dvě základní formy:
1. Student manipuluje pedagoga.
V této formě manipulace student (např. zamilovaná studentka) vyhrožuje učiteli možnou diskreditací jeho pověsti (např. zveřejněním jejich fiktivního vztahu, očerněním jeho pověsti falešným obviněním apod.), ke které dojde, pokud se společně nesejdou. Na schůzce pak mohou vzniknout další materiály, které mohou vydírání a manipulaci vedoucí k osobní schůzce zintenzivnit.

2. Pedagog manipuluje studenta.
V této formě manipulace učitel nutí vyhlédnutou oběť (studentku) k osobnímu kontaktu – schůzce – pod pohrůžkou neudělení důležitého zápočtu či zkoušky.

[2] Mirroring – manipulativní technika postavená na napodobování chování oběti. Pachatel v komunikaci s obětí používá stejné obraty, jako oběť, chová se jako zrcadlový odraz oběti (proto mirroring = zrcadlení).

Obě formy manipulace lze realizovat jak v přímém kontaktu, tak i prostřednictvím internetových služeb. Od typického kybergroomingu se však tyto formy manipulace odlišují zejména tím, že oběť zná svého útočníka a že dospělý manipuluje dospělého.

V obou výše uvedených formách manipulace dochází ke střetu zájmů – konkrétně zájmu profesního a osobního. Obě situace jsou obvykle řešeny etickými normami fakulty/univerzity, případně v trestněprávní rovině podáním trestního oznámení za podezření ze spáchání trestného činu či přestupku.

Kybergrooming je tedy velice úzce spojen s tzv. sexuálním obtěžováním, se kterým se dle výzkumu *Sexuální obtěžování ve vysokoškolském prostředí: výskyt a vnímání* (Univerzita Karlova v Praze, 2008-2009) setkalo přibližně 3 % vysokoškoláků. V rámci tohoto výzkumu více než 81 % studujících uvedlo, že znají někoho, kdo sexuální obtěžování zažil (Smetáčková a kol., 2009). Podobné výsledky nalezneme i u výzkumu *Sexuální obtěžování ve vysokoškolském prostředí Sociologického ústavu AV ČR* (2008-2009).

2 Metodologie výzkumu

Popis výzkumné procedury zahrnuje výzkumné cíle, na něž navážeme výzkumnými problémy (otázkami), dále popis výzkumného vzorku včetně metodiky výzkumu, časového harmonogramu a způsobu zpracování získaných dat. V rámci našeho výzkumu byla využita metodologie ověřená v rámci výzkumu Nebezpečí internetové komunikace 3 a 4 (Kopecký a kol., 2011-2012).

2.1 Výzkumné cíle a problémy (výzkumné otázky)

Výzkum zaměřený na výskyt rizikového chování u studentů PdF UP v Olomouci, které je spojeno s informačními a komunikačními technologiemi (zejména internetem), si v deskriptivní rovině kladl za cíl zjistit množství obětí i útočníků zapojených do jednotlivých projevů kyberšikany. Výzkum současně monitoroval, u koho by oběti hledaly pomoc v případě potřeby (učitel, rodič, sourozenec, kamarád).

Dále bylo úkolem výzkumu zjistit, zda studenti komunikují s neznámými lidmi na internetu, jestli jimi byly požádány o osobní schůzku a jestli jsou ochotni setkat se s virtuálním kamarádem či známým v reálném světě, což úzce souvisí s jevem zvaným kybergrooming.

Cílem bylo rovněž zjistit formy veřejného sdílení intimních materiálů v prostředí internetu a odhalit motivaci pubescentů a adolescentů k tomuto chování, tedy k sextingu. Také nás zajímalo, kolik dotázaných dětí považuje sexting za rizikový a riskantní.

V souvislosti s tím jsme se zaměřili na sdílení osobních údajů budoucími pedagogy v prostředí internetu (zejména na fotografii obličeje) a na jejich znalost sociálních sítí. Sociální sítě totiž představují místo četných kyberútoků, které jsou realizovány s využitím osobních

informací sdílených jednotlivými uživateli i údajů, které útočníci získají selháním zabezpečení těchto sítí.

Výzkumné problémy (výzkumné otázky) byly následující:

A. Jaké je množství obětí kyberšikany ve vztahu k jejím jednotlivým projevům a platformám, na nichž kyberšikana probíhá?

B. Jaké je množství původců kyberšikany ve vztahu k jejím jednotlivým projevům a platformám, na kterých kyberšikana probíhá?

C. Jaká komunikační platforma je nejčastěji využívaná ke kyberšikaně?

D. Koho oběť kontaktuje v případě, že zažívá kyberšikanu?

E. Kolik VŠ studentů by šlo na osobní schůzku s internetovým známým/kamarádem, kdyby je o ni požádal?

F. Kolik VŠ studentů obdrželo pozvání na osobní schůzku s uživatelem internetu bez ověřené identity?

G. Kolik VŠ studentů dorazilo na osobní schůzku s uživatelem internetu bez ověřené identity?

H. Jaké množství studentů umístilo své sexuálně laděné materiály na internet?

I. Kolik studentů odeslalo jiným osobám své vlastní sexuálně laděné materiály?

J. Kolik studentů vnímá sexting jako rizikový a riskantní?

K. Které osobní údaje sdílejí studenti PdF UP na internetu nejčastěji?

L. Které osobní údaje odesílají studenti PdF UP nejčastěji jiným uživatelům internetu?

M. Kolik studentů bylo požádáno jinou osobou na internetu o zaslání své fotografie obličeje?

N. Které sociální sítě VŠ studenti znají?

O. Na kterých sociálních sítích mají studenti své účty?

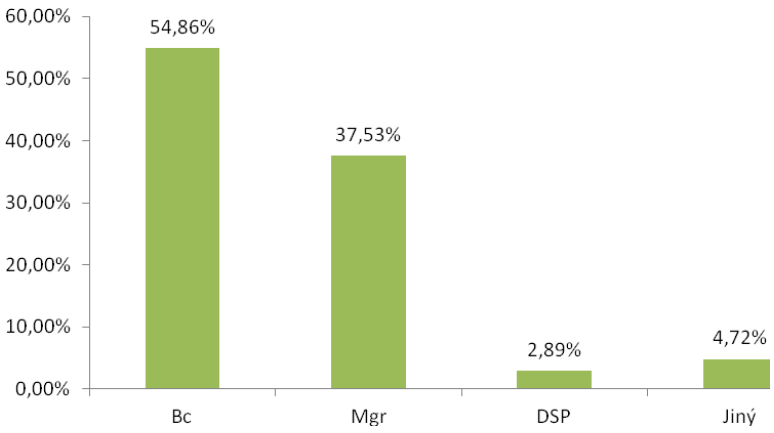
2.2 Výzkumný vzorek

Základní soubor byl tvořen studenty Pedagogické fakulty Univerzity Palackého v Olomouci, kteří byli pro účast ve výzkumu osloveni prostřednictvím komunikačních kanálů Univerzity Palackého

v Olomouci, dále prostřednictvím internetových stránek projektu E-Synergie (www.esynergie.cz) a projektu E-Bezpečí (www.e-bezpeci.cz). Tyto webové zdroje jsou studenty Pedagogické fakulty hojně využívány.

Do výzkumu se zapojilo **386** studentů Pedagogické fakulty Univerzity Palackého v Olomouci. Ze vzorku tvořili 16, 75 % muži, 83,25 % ženy. Nejvíce respondentů bylo ve věku **20 až 25 let** (86,7 % celkového vzorku). Rozložení vzorku podle jednotlivých studijních programů přibližně kopíruje rozložení počtu přijatých studentů v roce 2011 a v roce 2012 (viz Výroční zpráva o činnosti PdF UP za rok 2011 a 2012).

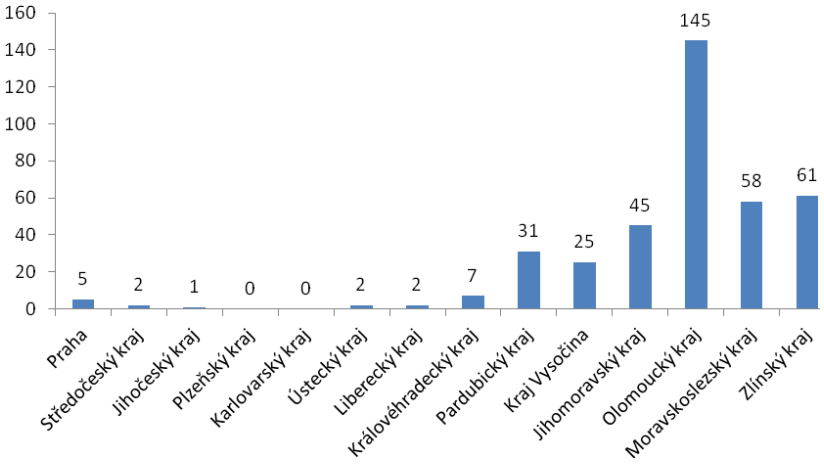
Graf č. 1 Respondenti podle studijních programů



Poznámka:
Odpověď jiný zahrnuje účastníky programů celoživotního vzdělávání, zahrnující studenty doplňujících a rozšiřujících studijních programů.

Graf č. 2 Výzkumný vzorek (regionální rozložení)

Následující graf znázorňuje přehled respondentů z jednotlivých krajů. Převažuje Olomoucký, Zlínský a Moravskoslezský kraj.



n=385

2.3 Metodika výzkumu

Výzkum byl orientován zejména kvantitativně a jako výchozí výzkumná procedura byla zvolena metoda dotazníku.

Výzkumný nástroj čítal celkem **71** položek (40 dichotomických, 2 polytomické, 22 s více možnými odpověďmi a 7 otevřených), jež vznikly na základě teoretických poznatků a byly sestaveny takovým způsobem, aby reflektovaly stanovené cíle a vzniklé problémy.

Dotazník byl respondentům distribuován elektronicky (Online) prostřednictvím dotazníkového systému projektu E-Bezpečí, dále

prostřednictvím univerzitního direct emailu, prostřednictvím www stránek PdF UP a také s využitím sociální sítě Facebook.

Anonymní dotazník automaticky ověřoval, odkud byl odeslán (IP adresa, regionální příslušnost, monitoring chování respondentů za využití nástroje Google Analytics atd.).

2.4 Časový harmonogram výzkumu

Příprava výzkumu byla zahájena 1. 11. 2012, sběr dat probíhal od 1. 12. do 31. 1. 2013. Jejich vyhodnocení bylo realizováno v průběhu února a března roku 2013.

2.5 Data a statistické testy

Získaná data byla převážně na nominální a ordinální úrovni měření, čemuž odpovídalo i jejich následné zpracování, použité numerické operace a statistické zpracování.

Data jsme nejprve uspořádali a poté sestavili do tabulek četností.

Deskriptivní problémy byly řešeny s využitím základních veličin popisné statistiky (výpočet charakteristik polohy – míry ústřední tendence, výpočet procent) a nechybělo ani jejich grafické znázornění.

K testování hypotéz jsme využili test nezávislosti chí-kvadrát pro čtyřpolní tabulku. Veškeré testování proběhlo na hladině významnosti $\alpha = 0{,}05$.

3 Výsledky výzkumu

3.1 Kyberšikana u vysokoškolských studentů

Základní pilíř výzkumu rizikového chování českých vysokoškolských studentů v prostředí internetu spočíval v popisu forem kybernetické agrese.

V rámci našeho výzkumu jsme se zaměřili na následující oblasti:

A. Oběti kyberšikany
Sledovali jsme počty obětí ve vztahu k jednotlivým projevům kyberšikany a platformám, na kterých kyberšikana probíhá. Dále jsme sledovali přepínání rolí oběti a agresora.

B. Původce kyberšikany
Monitorovali jsme množství útočníků ve vztahu k jednotlivým projevům kyberšikany a platformám, na kterých probíhá. Sledovali jsme rovněž přepínání rolí agresora a oběti.

C. Osoby zapojené do řešení kyberšikany
Výzkum se zaměřil na to, koho by oběti kontaktovaly v situaci, kdy zažívají kyberšikanu.

D. Projevy kyberšikany v závislosti na využívání sociálních sítí (zejména Facebooku)
Výzkum sleduje, jak je kyberšikana propojena s využíváním sociální sítě Facebook.

E. Další související jevy
V rámci výzkumu jsou dále sledovány specifické formy virtuální agrese realizované např. prolomením účtu, krádeží identity a následnou kyberšikanou.

Deskriptivní data doplňujeme konkrétními případy, se kterými kontaktovali studenti Pedagogické fakulty Univerzity Palackého v Olomouci naši poradnu. Z důvodu ochrany soukromí klientů nezveřejňujeme skutečná jména osob zapojených do případů, popis případu je však autentický.

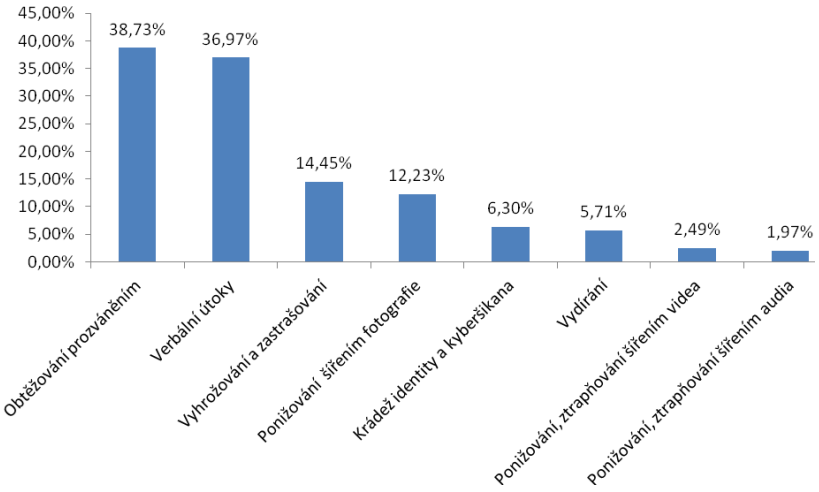
3.1.1 Kyberšikana u studentů PdF UP – oběti

V rámci výzkumu byly sledovány následující formy útoku spadajících do oblasti kyberšikany:

A. Verbální útoky v kyberprostoru – ubližování formou ponižování, urážení, zesměšňování, ztrapňování studenta (verbální agrese).
B. Vyhrožování a zastrašování studenta.
C. Vydírání studenta.
D. Krádež identity s následnou kyberšikanou.
E. Obtěžování prozváněním.
F. Ponižování, ztrapňování realizované šířením fotografie.
G. Ponižování, ztrapňování realizované šířením videonahrávky.
H. Ponižování, ztrapňování realizované šířením audionahrávky.

V praxi dochází ke kombinování jednotlivých forem útoku – tak, aby byla intenzita útoku co největší.

Graf č. 3 Studenti jako oběti kyberšikany



n=376 (sumy respondentů jsou podrobněji rozpracovány dále).

Kyberšikana - obtěžování prozváněním

Ačkoli je kyberšikana realizovaná obtěžováním či prozváněním považovaná za jednu z nejmírnějších a nejméně nebezpečných forem kyberšikany (v některých studiích není mezi projevy kyberšikany zařazena), přesto jsme se rozhodli ji vzhledem k jejímu rozsahu v populaci studentů mezi formy kyberšikany zařadit. Kyberšikanu realizovanou pomocí prozvánění zažilo v pozici oběti **38,73 % studentů** (konkrétně 134 z 346 studentů) Pedagogické fakulty Univerzity Palackého v Olomouci.

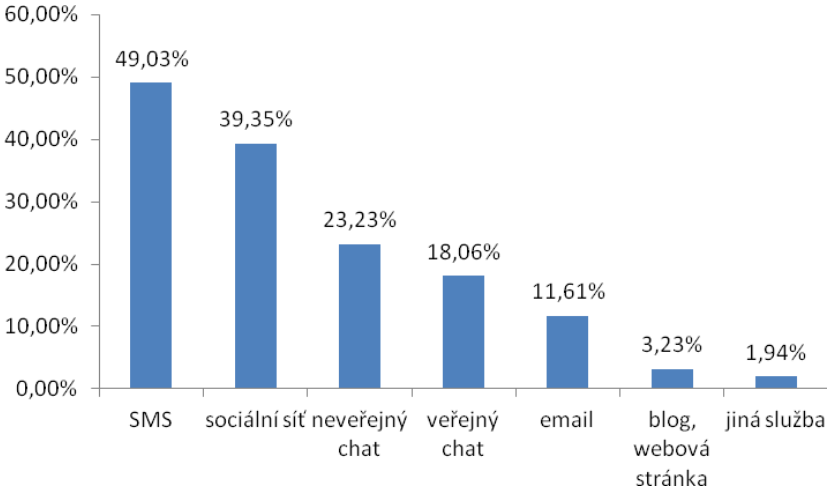
Ukázková situace

Denisa je studentkou 2. ročníku učitelského oboru v bakalářském studijním programu. Dva měsíce od počátku letního semestru začala zažívat kyberšikanu realizovanou prozváněním. Na její telefonní číslo ji opakovaně prozváněla neznámá osoba z jí neznámého telefonního čísla. Prozvánění se opakovalo v průměru 20-25x denně, nejčastěji večer, kdy byla na koleji. Několikrát hovor přijala, z telefonního přístroje však ozývaly zvuky lidského dechu („funění"), na její otázky neznámý nereagoval. Denisa se pak pokusila telefonujícího kontaktovat pomocí SMS, bez odezvy. Toto jednání probíhalo více než 5 týdnů. Denisa se pokusila několikrát zjistit majitele telefonního čísla, využila internetového vyhledávání, pokusila se kontaktovat i operátora. Po kontaktování poradny projektu E-Bezpečí si telefonní číslo neznámého zablokovala (uložila do blacklistu), přesto však po dobu dalších 3 týdnů prozvánění pokračovalo z jiného telefonního čísla, scénář se opět opakoval. Číslo bylo Denisou opět zablokováno, po dalších 14 dnech prozvánění přestalo.

Kyberšikana - verbální agrese

Nejrozšířenější „klasickou" formou kyberšikany představují různé projevy slovní agrese, které jsou vůči studentům realizovány opakovaně, a roste jejich intenzita. Kyberšikana realizovaná touto formou zpravidla probíhá v prostředí sociálních sítí či s použitím SMS, méně často je pak pro tuto formu kyberšikany využit email či další komunikační služby. Kyberšikanu ve formě opakované, dlouhodobě verbální agrese zažilo **36,97 % respondentů** (139 z 376).

Graf č. 4 Nejčastější platformy použité pro realizaci kyberšikany ve formě verbální agrese



n=155

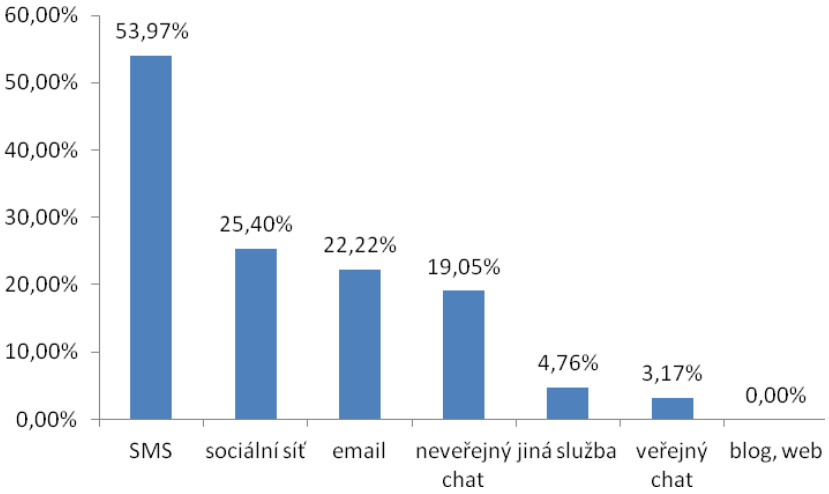
Ukázková situace

Jitka, studentka 2. ročníku magisterského studia učitelství, byla introvertní, izolovaná od zbytku studijní skupiny, ve škole se téměř neprojevovala. Rovněž se od ostatních odlišovala stylem oblékání, stylem komunikace (hovořila velmi spisovně až hyperkorektně) a svými znalostmi (vynikala nad ostatními). Tři spolužačky si o ní v prostředí sociální sítě Facebook založili diskusní skupinu, ve které se na její účet bavili, uráželi ji, napadali za její projev, psali vulgární vzkazy. Řadu vzkazů rovněž Jitce odesílali na její mobilní telefon pomocí anonymní webové SMS brány. Původně uzavřená diskusní skupina se postupně stala veřejnou a do kyberšikany se zapojilo přes 30 dalších uživatelů Facebooku.

Kyberšikana - vyhrožování a zastrašování

Další poměrně rozšířenou formou kyberšikany představuje vyhrožování. Vyhrožování posouvá intenzitu kyberšikany do vyšší úrovně, protože vnáší do procesu kyberšikany nový prvek - intenzivní strach. Zatímco verbální formy kyberšikany se zaměřují především na intenzivní ponížení oběti bez toho, aby v ní vyvolali strach (zejména strach o život, o blízké, o domácí mazlíčky apod.), vyhrožování a zastrašování je již zaměřeno především na vyvolání strachu. Vyhrožování či zastrašování zažilo **14,45 % respondentů** (51 z 353).

Graf č. 5 Nejčastější platformy použité pro realizaci kyberšikany ve formě vyhrožování a zastrašování



n=63

Ukázková situace

Marie, studentka 4. ročníku magisterského studia učitelství, byla v průběhu ledna až dubna 2012 opakovaně kontaktována neznámým uživatelem či uživatelkou internetu pomocí SMS zpráv, odesílaných z anonymní internetové SMS brány. Anonymní pisatel Marii psal: *Vim, co delas. Sleduji te. Dnes jsem te videl na ulici. Rozdam si to s tebou, ty kravo. Chces poznat rozkos? Udelam ti to. Poznas bolest atd.* Vyhrůžky se neustále stupňovaly a vždy byly odeslány z internetu. Za 3 měsíce Marie obdržela více než 300 zpráv. Pod tímto tlakem byla donucena změnit i telefonní číslo. Výhrůžky ustaly.

Kyberšikana - ponižování a ztrapňování šířením fotografie

Kyberšikana realizovaná s použitím fotografie oběti je poměrně rozšířenou formou kyberšikany, která je svou intenzitou a zaměřením na vyšším stupni intenzity a nebezpečnosti, než předcházející monitorované formy. Je to způsobeno zejména existencí konkrétního choulostivého materiálu oběti (fotografie), který lze šířit mezi velké množství uživatelů internetu (včetně těch, kteří oběť neznají). Tato kyberšikana bývá často útočníky vnímána jako forma škádlení, jako pozitivní způsob komunikace, který má za úkol pobavit a zároveň zocelit oběť, hranice mezi škádlením a kyberšikanou je však velmi neostrá a nepovedený žert často přerůstá v intenzivní kyberšikanu s širokým publikem na hranici virálního šíření diskriminujících materiálů.

Častými kompromitujícími materiály jsou fotografie opilých, zvracících studentů či studentek, fotografie zachycující sexuální obsah - fotografii obnažené oběti, fotografie kompromitující vztah studentek a pedagogů, fotografie zaměřené na homosexuální vztahy, fotografie zaměřené na etnické menšiny apod.

Krádež identity a kyberšikana

Krádež identity (identity theft) představuje specifickou formu kyberšikany, kdy útočník nejdříve pronikne na účet oběti (např. e-mailový účet, účet v sociální síti, účet v MMORPG hře apod.) a poté pod jejím jménem realizuje útoky na další uživatele internetu. Útoky na účet potvrdilo **32,24 %** respondentů (116 z 349), **18,64 %** z nich také potvrdilo, že byl jejich účet využit ke kyberšikaně jiných osob. Krádež identity využitou ke kyberšikaně zažilo **6,30 %** dotazovaných.

Kyberšikana - vydírání

Vydírání představuje velmi intenzivní a nebezpečnou formu kyberšikany, kterou potvrzuje přibližně **5,71 %** respondentů.

Kyberšikana – ponižování šířením videonahrávky

2,49 % respondentů uvádí, že zažili kyberšikanu realizovanou pomocí šíření videonahrávky. Ta byla šířena běžnými komunikačními cestami – internetem a mobilním telefonem.

Kyberšikana – ponižování šířením audionahrávky

Na pomyslném konci našeho žebříčku nejběžnějších forem kyberšikany se nachází ponižování šířením audionahrávky, které v pozici oběti zažilo **1,97 % respondentů**. V tomto případě se jedná o nahrávku, která zachycuje oběť ve směšné situaci a lze rozpoznat její identitu. Nahrávka se následně dá využít jak k ponižování, tak i k vydírání.

Další formy kyberšikany

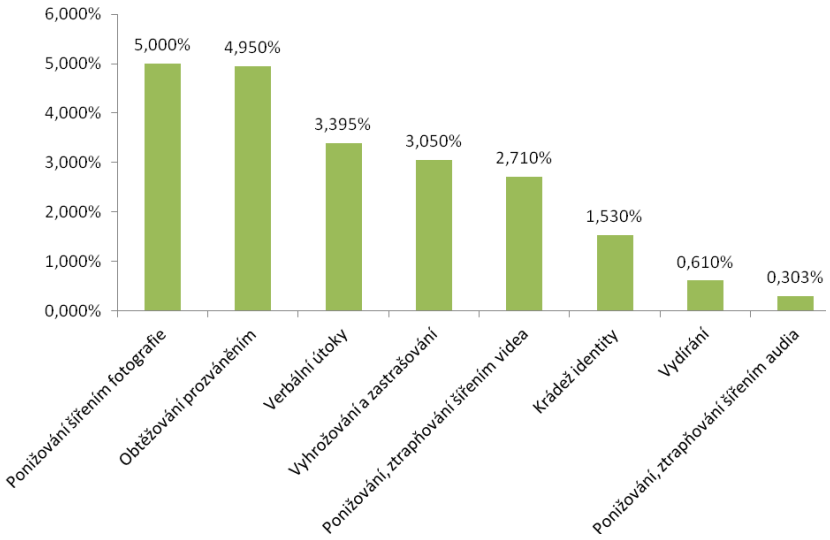
Mezi další formy kyberšikany lze zařadit **kyberšikanu zaměřenou na hráče počítačových her** (zejména MMORPG), ve kterých dochází nejen k šikanování hráčů ostatními hráči, ale také různým podvodům, krádežím herních postav, krádežím virtuálních předmětů, obchodováním s ukradeným zbožím apod. Je třeba uvědomit si, že „virtuální předměty a herní postavy“ mají hodnotu vyjádřitelnou

běžnými penězi a že se s nimi běžně obchoduje. V řadě zemí jsou virtuální světy WoW propojeny se světy reálnými, tedy virtuální produkty lze prodávat a kupovat za reálné peníze. A částky za unikátní virtuální předměty dosahují i několika stovek až tisíců dolarů za kus. Jeden z nejznámějších virtuálních předmětů, který byl prodán za skutečné peníze, byl (a je) Spectral Tiger, speciální druh mounta, tedy zvířete, které vás může po světě WoW nosit. V aktuálních aukcích na serveru EBAY dosahuje cena tohoto virtuálního živočicha od 400 do 9 999$ (Kopecký, 2012).

3.1.2 Kyberšikana u studentů PdF UP – útočníci

V rámci výzkumu jsme rovněž sledovali, zdali studenti figurují rovněž jako původci kyberšikany. 15,00 % studentů přiznalo, že si vyzkoušelo realizovat některou ze sledovaných forem kyberšikany. Další formy kyberšikany z pohledu útočníků jsou přehledně znázorněny v následujícím grafu.

Graf č. 6 Studenti jako původci kyberšikany



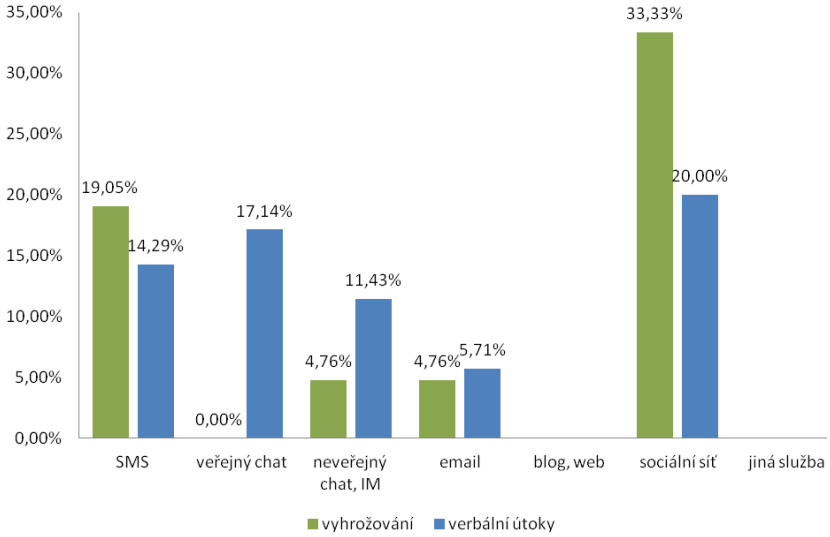
n=340

Nejčastější formu kyberšikany realizované studenty Pedagogické fakulty Univerzity Palackého v Olomouci představuje **ponižování oběti šířením fotografie, které si vyzkoušelo 5,00 %** respondentů. Na dalších místech se umístilo obtěžování prozváněním, verbální formy kyberšikany, vyhrožování a zastrašování oběti a ponižování šířením videozáznamu.

Zajímavé je rovněž zjištění, že se plných **41,10 % studentů dostalo bez svolení majitele do jeho elektronického účtu**, přičemž 3,68 %

z nich tento účet zneužilo k útoku na jinou osobu (tzv. útok realizovaný pomocí krádeže identity). Z celého vzorku si tak krádež identity vyzkoušelo 1,53 % odpovídajících.

Graf č. 7 Srovnání komunikačních platforem využitých pro realizaci verbálních forem kyberšikany a pro kyberšikanu realizovanou formou vydírání

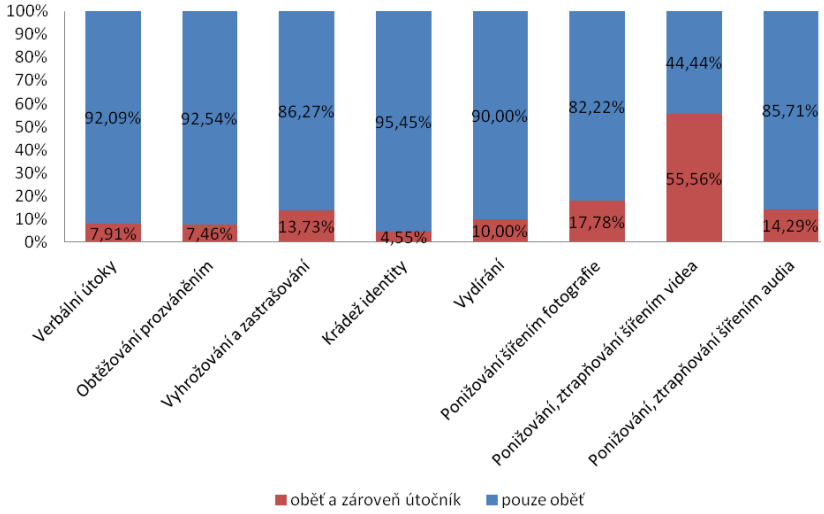


$n_{vyhrožování}=21$, $n_{verbální\ agrese}=35$

3.1.3 Komparace mezi oběťmi a útočníky

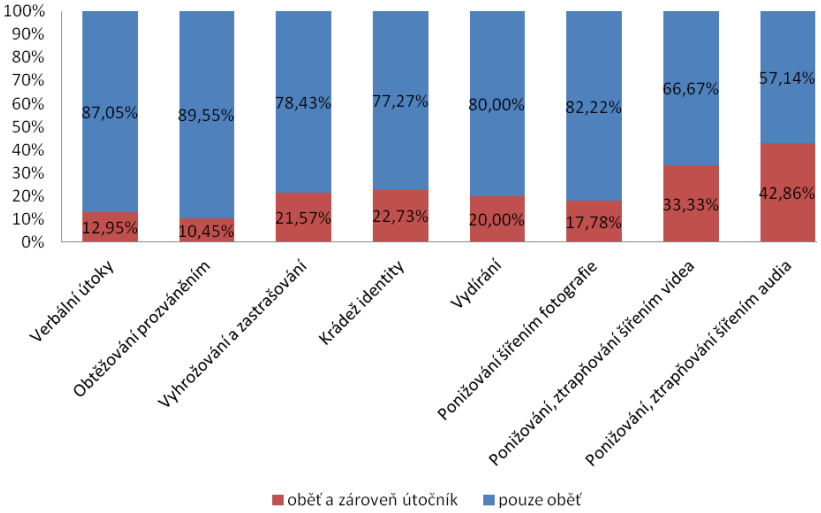
Následující graf vyjadřuje, kolik procent obětí se zároveň stalo útočníkem, který využil stejnou formu kyberšikany, jakou zažil jako oběť. Např. 55,56 % obětí, které zažily kyberšikanu realizovanou pomocí šíření ponižující videonahrávky, si totéž vyzkoušelo v pozici útočníka.

Graf č. 8 Oběti, které se stávají útočníky (při zachování stejné formy kyberšikany)



Další graf vyjadřuje, kolik obětí jednotlivých forem kyberšikany vyzkoušelo jakoukoli formu kyberšikany k útoku na jinou osobu. Jinými slovy – v případě, že student zažil kyberšikanu jako oběť, zda má tendenci zkoušet si útok také jako agresor.

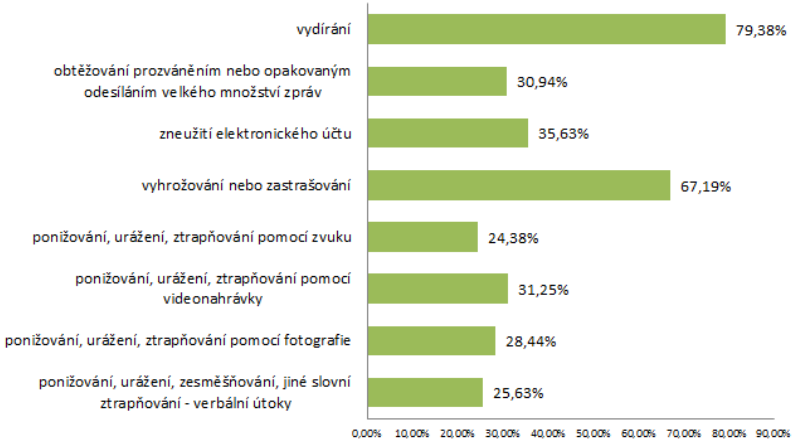
Graf č. 9 Oběti, které se stávají útočníky (při použití libovolné formy kyberšikany)



3.1.4 Zapojení dalších osob do řešení kyberšikany

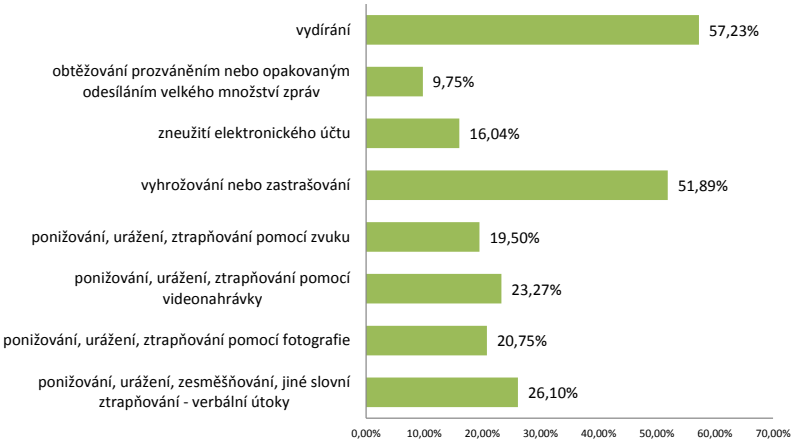
V rámci výzkumu jsme rovněž sledovali, na koho by studenti – oběti kyberšikany – obrátili s prosbou o pomoc. Řada z obětí kontaktuje své rodiče až v situaci, kdy je intenzita kybernetického útoku tak vysoká, že oběť nedokáže danou situaci řešit sama. Policii ČR studenti v těchto případech zpravidla nekontaktují.

Graf č. 10 Formy kyberšikany, které by studenti řešili s rodiči



Dle předpokladu by studenti se svými rodiči řešili především vážnější formy kyberšikany, jako je vydírání (79,38 %), vyhrožování či zastrašování (67,19 %). S kyberšikanou realizovanou ve formě verbálních útoků by se rodičům svěřila pouze ¼ studentů.

Graf č. 11 Formy kyberšikany, které by studenti řešili s pedagogy



3.2 Osobní schůzky s uživateli internetu

Výzkum rizikového chování vysokoškolských studentů se také zaměřil na ochotu respondentů komunikovat v prostředí internetu s neznámými osobami s neověřenou identitou také reakce respondentů na pozvání k osobní schůzce. S neznámými lidmi bez ověření identity komunikuje téměř polovina, tedy **46,49 %** studentů PdF UP v Olomouci.

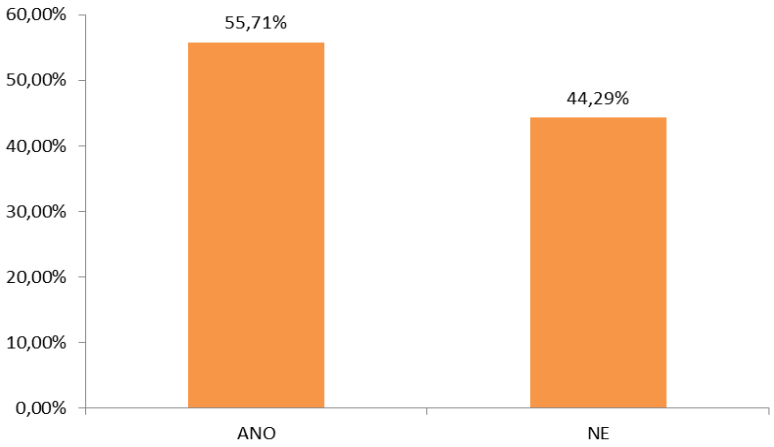
90,94 % respondentů uvedlo, že si mezi přátele do svých profilů v rámci sociálních sítí **nepřidává neznámé osoby**, pokud je o to požádají.

Ne každá komunikace s neznámými lidmi v prostředí internetu musí být pro vysokoškolské studenty apriori nebezpečná, nemusí tedy směřovat např. k jejich sexuálnímu zneužití. V celé řadě zdokumentovaných případů (viz. případ Chapman, 2010 aj.) však ke zneužití studenta či studentky došlo. Proto jsme se v rámci naší

sondáže zaměřili nejenom na komunikaci s osobami s neznámou identitou, ale také na samotný proces osobní schůzky, případně na její důsledky.

Prvním sledovaným parametrem byla ochota studenta jít na osobní schůzku. Studentům jsme tedy položili otázku, zdali by byli ochotni jít na osobní schůzku s internetovým známým (kterého neznají z reálného světa mimo internet). Výsledky shrnují následující grafy.

Graf č. 12 Ochota jít na osobní schůzku s internetovým známým (neznáme jej v reálném světě)

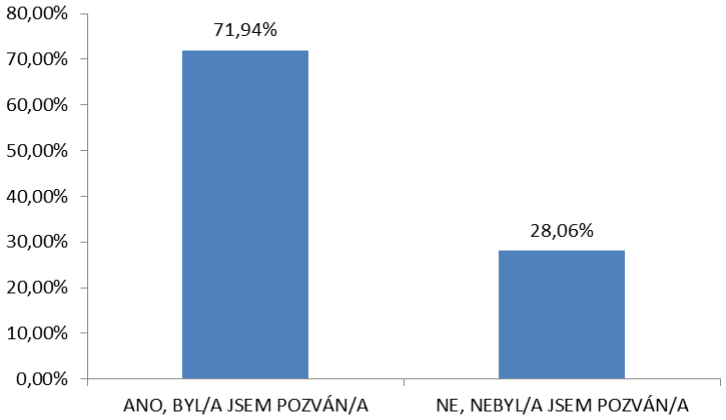


n=140

Více než polovina respondentů (**55,71 %)** je ochotna jít na osobní schůzku s internetovým známým pouze na základě informací, které jim poskytl ve virtuálním světě internetu.

V další části našeho výzkumu již sledujeme, zdali byli studenti skutečně k osobní schůzce pozváni a zda se jí zúčastnili.

Graf č. 13 Pozvání k osobní schůzce s internetovým uživatelem

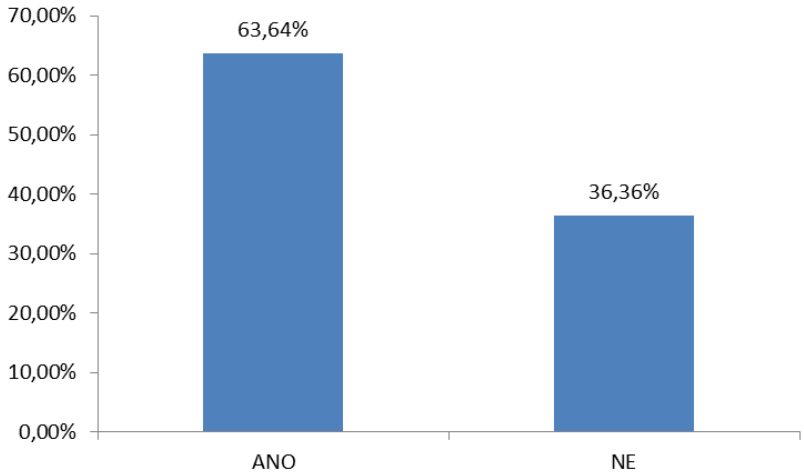


n=139

K osobní schůzce bylo v roce 2012 pozváno 71,94 % dotazovaných. Tento výsledek lze předpokládat, neboť studenty Pedagogické fakulty Univerzity Palackého v Olomouci z více než 80 % tvoří sexuálně aktivní ženy, z nichž velké množství vlastní účty na sociálních sítích (zejména Facebooku). Jsou tedy oblíbeným a vyhledávaným cílem internetového seznamování.

To, že byli studenti pozváni jinými uživateli internetu na osobní schůzku, neznamená, že by snad na schůzce muselo apriori dojít k sexuálnímu zneužití, znásilnění atd. Pozvání na schůzku a schůzka samotná může být běžnou součástí mezilidské interakce, v intencích tohoto textu vnímáme osobní schůzky jako potenciálně rizikové, nikoli rizika samotná.

Graf č. 14 Uskutečněná osobní schůzka



n=99

Na osobní schůzku dorazila více než polovina studentů z pozvaných, tedy 63,64 %. Extrapolujeme-li výsledek směrem k otázce zaměřené na pozvání k osobní schůzce, dojdeme ke zjištění, že 45,32 % studentů Pedagogické fakulty UP v Olomouci šlo v roce 2012 na osobní schůzku s neznámými lidmi. Je rovněž zajímavé, že 6,43 % studentů bylo svými internetovými přáteli požádáno, aby nikomu neříkali, že se spolu baví a o čem se spolu baví.

Pro zachování objektivity výzkumu jsme rovněž zjišťovali, zdali také naši respondenti a respondentky pozvali své internetové přátele na osobní schůzku a zdali po svých internetových známých požadovali, aby nikomu neříkali, že se spolu bavíte a o čem se bavíte. Přibližně 10 % studentů chtělo po svém internetovém známém udržet komunikaci v tajnosti. Na schůzku pak své internetové známé pozvalo 40 % oslovených.

V případě, že by studenti opravdu chtěli na osobní schůzku dorazit, svěřili by se s touto informací nejčastěji svým přátelům (39,51 %) a rodičům (32,10 %), své vysokoškolské pedagogy by nekontaktoval nikdo z nich. V naprosté tajnosti by pak schůzku uchovalo 17,28 % studentů a nikomu by o tom neřekli.

Za riskantní či nebezpečnou považuje komunikaci s neznámými uživateli internetu téměř 3/4 respondentů (74,5 %), osobní schůzky s nimi pak za nebezpečné označuje 85,99 % studentů.

3.2.1 Proč jsou osobní schůzky riskantní

Jak již bylo řečeno, většina respondentů si uvědomuje rizika spojená s osobními schůzkami s neznámými uživateli internetu. Nejčastějšími důvody pro toto tvrzení jsou neověřená identita osob na internetu, potenciální deviantní chování neznámého, riziko přepadení, únosu či dokonce vraždy.

Některé z odpovědí respondentů
(odpovědi neprošly jazykovou úpravou)

- *Nikdy nevíme, kdo na schůzku může přijít, nemusí to být krásná 18tiletá slečna, ale třeba ošklivý 40tiletý pán.*
- *Nikdy nemůžeme vědět, jaký ten člověk doopravdy je, jestli nám neublíží, neokrade nás atp.*
- *Neznámá osoba se může chovat patologicky a ublížit mi i mému okolí (rodině).*
- *Může to být úchyl.*

- *Nikdy nevím, co jsou ti lidé zač. Pokud se jedná o člověka, kterého neznám ani já, ani nikdo z mého okolí, nemohu si být jista, že mi například neublíží. Proto, jdu-li s někým na schůzku, předem si zjistím, hovoří-li o sobě pravdu (přes společné známé apod.). Obecně vzato ale na podobné schůzky nechodím a ani nikoho ke schůzkám či jiným podobným účelům nevyhledávám.*

- *Na netu člověk nikdy neví, kdo se za koho vydává, fotku si umí falešnou sehnat každý...je mnoho pedofilů.*

- *Nevím, co to může být za člověka, co po mě vlastně chce a jestli jde jen o nevinnou schůzku.*

- *Když neznám nějakého člověka, nemůžu vědět, co od něj čekat, proto bych na žádnou schůzku s cizím člověkem, kterého znám z internetu nešla. Může to být násilník a těžko se bych se sama ubránila, když by mi chtěl ublížit.*

- *Nikdy nevíme, kdo se za profilem skrývá, fotka nemusí být pravá, život osoby smyšlená. Je to riskantní. Mělo by se to odehrávat mezi lidmi v kavárně popř. přítomnost kamarádky,*
  velké riziko neznalosti člověka, jeho reakcí atd.,

- *Nevím, co to ej za lidi - může to být kdokoliv, nějaký násilník, vrah, pedofil, zloděj. Nikdy bych se takto s nikým nesešla, absolutně nemůžu předvídat, kdo doopravdy přijde.*

- *Hodně lidí je bohužel neopatrných, napíšou o sobě kde co a pak se nemůžou divit, když se něco nemilého semele. Dovolím si o sobě tvrdit, že mám zdravý rozum a tohle mi nehrozí.*

- *Nemusí se jednat o osobu, za kterou se vydává, především se jedná o cizince, kteří jsou známí svou bohatou kriminální činností.*

- *Napadení, znásilnění, vražda.*

- *Jsou to lidé co neznám osobně, proto považuji schůzku s nimi za riskantní. Pokud se však zvolí vhodné místo schůzky (tzn. na veřejném místě) a bude člověk obezřetný, pak se riziko takovéto schůzky zmenšuje.*

- *Internet je anonymní místo. Proto může na domluvenou schůzku přijít úplně někdo jiný, než je uveden na sociální síti. V mém případě jsem většinou věděl o koho se jedná přes jiné lidi a tudíž jsem věděl, do čeho jdu, ale přiznávám, že schůzka s neznámou osobou po domluvě na internetu je nebezpečná. Je třeba si dávat pozor.*

- *Pokud toho člověka znám krátce (jen několik měsíců), je to nebezpečné. Je nedůvěryhodný.*

- *Jméno, fotografie a všechny ostatní věci uvedené na internetu/internetovém profilu nemusí odpovídat skutečné osobě. Za „fiktivním" profilem se může skrývat nebezpečný jedinec.*

- *Nikdy přesně nevíme, co je to opravdu za člověka.*

- *Nemůžeme věřit někomu, s kým vedeme rozhovor pouze přes písmenka. Jsou i výjimky, ale rozhodně se takto stala i děje spousta špatných věcí, které mohly jedincům značně ublížit...nebojím se komunikovat na internetu s lidmi, které znám alespoň od vidění, i když to je možná také riskantní..nechápu však, jak mohou mít založeny účty na soc. sítích děti na prvním stupni, které absolutně neví, jaká je realita a dají si na svůj profil cokoli, napíší cokoli…,*

- *Nikdy nevím, co se z něj může vyklubat za pošuka, nicméně vím, že jsem schopna se ubránit a nikdy si nedávám schůzku někde, kde bych nemohla „utéct".*

- *Při komunikaci přes internet, sociální sítě… se člověk může prezentovat jako někdo jiný (co se týče vzhledu, stáří, zálib, povahy atd.). Riziko hrozí především u důvěřivých dospívajících dívek, které*

se schůzkou mohou souhlasit a nejedna takováto schůzka dopadla špatně (ublížení na zdraví, smrt…). ,

- *Nikdy člověk neví, kdo je na druhé straně za monitorem, je těžké na tuto otázku odpovědět, ale je mnoho rizik jak Vás může daná osoba ohrozit velké riziko je u nezletilých a také dívek ve věku 19, 20 dle mého jelikož jsem kluk a přesto bych někdy šel na schůzku mám větší šanci se bránit atd.*

- *Aby bylo jasno: záleží na tom, jaká komunikace proběhla a kde jsme se seznámili. Pakliže napíšu mail osobě, o níž si najdu na netu informaci a ona mě třeba doporučí, ať kontaktuji pana xy na mailové adrese xz, abychom se dohodli na schůzce v instituci, kde pracuje za účelem mého výzkumu, tak to tak provedu. Pakliže mi na mail napíše cizí osoba, která se chce zapojit do křesťanské modlitební skupiny, již prostřednictvím mailu animuji, tak jí taky odpovím a klidně pozvu na osobní setkání. S cizími lidmi se nebavím a spamy ani nečtu.*

3.3 Sexting u vysokoškolských studentů

Výzkum rizikového chování studentů Pedagogické fakulty Univerzity Palackého v Olomouci se rovněž zaměřil na monitoring sextingu jakožto specifické formy sexuálního chování v kyberprostoru. Zahraniční studie dokazují, že výskyt sextingu v populaci adolescentů dosahuje v různých studiích od 20 do 70 % (The National Campaign to Prevent Teen and Unplanned Pregnancy, 2010), záleží na konkrétní formě sextingu a také na pohlaví odesílatele či příjemce.

V rámci našeho šetření sledujeme výskyt sextingu ve dvou základních formách - v podobě umisťování vlastních sexuálně laděných materiálů (fotografie/video) na internet a v podobě odesílání těchto materiálů jiným osobám prostřednictvím internetových služeb.

Sexting ve formě umisťování vlastních sexuálně laděných fotografií či videozáznamů (na kterých je student částečně či úplně svlečený/nahý) do prostředí internetu realizuje **12,42 %** studentů.

Důvody, které studenti pro realizaci této formy nejčastěji uvedli, jsme vizualizovali do podoby slovního mraku (word cloud).

Graf č. 15 Důvody pro umisťování vlastních sexuálně laděných materiálů na internet (Word Cloud)

V předcházejícím slovním mraku jsou vizualizovány odpovědi od respondentů, kteří sexting aktivně provozují. Nejčastějšími důvody pro realizaci této formy sextingu jsou: *šíření fotografie v rámci partnerskému vztahu, dále touha pochlubit se, případně se zviditelnit.*

Více než pětina studentů (23,28 %) rovněž **odeslala svoje vlastní intimní materiály prostřednictvím internetových služeb jiné osobě**.

Graf č. 16 Důvody pro odesílání vlastních sexuálně laděných materiálů prostřednictvím internetových služeb (Word Cloud)

Nejčastějšími důvody pro odesílání vlastních sexuálně laděných materiálů dalším osobám na internetu jsou: *odesílání těchto materiálů partnerovi, příteli či kamarádovi, na dalších místech pak jako důvod nalezneme oboustrannou výměnu fotografií (nespecifikováno s kým), využití fotografie v rámci internetové seznamky, případně flirt.*

Pro ilustraci uvádíme i několik otevřených odpovědí našich respondentů a respondentek:

- *Mělo se jednat o profesionální focení. Bohužel se tak nekonalo a moje fotka se objevila na Lide.cz a přineslo mi to velké problémy. Psychicky jsem to odnesla nejvíce. I dnes to na sobě pociťuji, že mě to určitým způsobem poznamenalo. Věřila jsem dotyčné osobě. Byla jsem mladá a blbá.*

- *Kamarád mě chtěl namalovat kvůli přijímacím zkouškám na VŠ, poslala jsem mu předem fotografii mé postavy, aby věděl, s čím má počítat.*

- *Příteli z důvodu dlouhého odloučení z důvodu zahraniční stáže.*

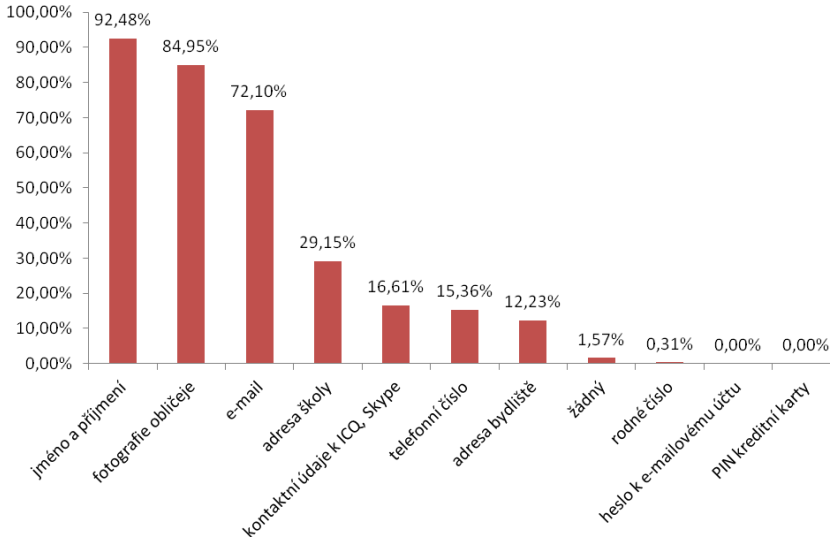
- *Hledala jsem milence.*
- *Svému partnerovi, se kterým jsem spoustu let a vím, že ji nepoužije nikde dál.*
- *Taky mi ji poslal a chtěla jsem, aby mě obdivoval.*
- *Byla to osoba velmi blízká, které jsem věřila, a nemohli jsme se nějakou dobu setkat osobně.*

3.4 Sdílení osobních údajů vysokoškolských studentů

Další kategorii, na kterou se náš výzkum zaměřil, tvořilo sdílení osobních údajů vysokoškolskými studenty. Zajímalo nás, které osobní údaje mají studenti zveřejněny na internetu a které jsou ochotni dále sdílet s lidmi bez ověřené identity, se kterými studenti komunikují právě v prostředí internetu.

Přístup k osobním údajům se v průběhu posledních deseti let poměrně razantně změnil – soukromé informace se začaly stávat veřejnými zejména s příchodem sociálních sítí, kde si uživatelé vytvářeli skutečné profily s pravdivými osobními údaji. Např. v prostředí Facebooku či sociální sítě Google+ vystupuje převážná většina uživatelů pod svým skutečným jménem a příjmením, přičemž odhadovaný počet falešných účtů se pohybuje mezi cca 10-15 % všech účtů (údaj pro sociální síť Facebook).

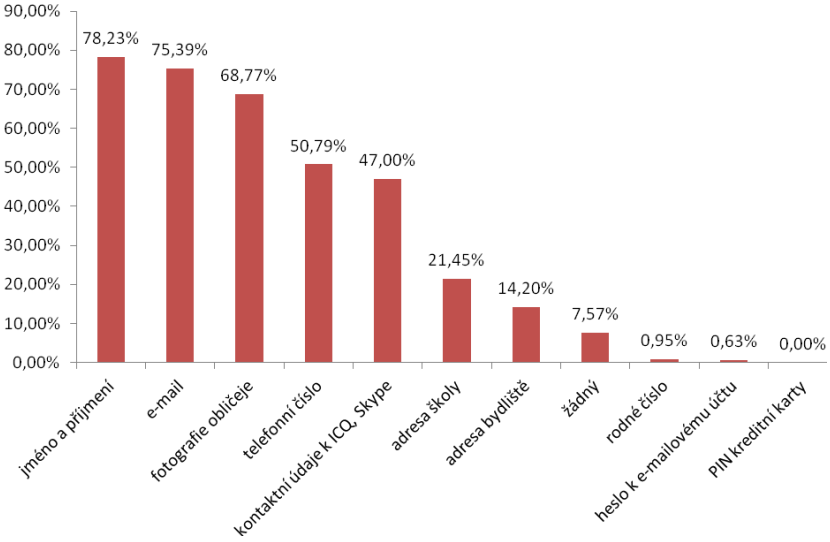
Graf č. 17 Osobní údaje sdílené studenty v prostředí internetu



n=319

Mezi osobní údaje, které jsou studenty v prostředí internetu běžně sdílené, patří jméno a příjmení, fotografie obličeje a e-mail. Mezi osobní údaje, které studenti nezveřejňují, logicky patří heslo k e-mailovému účtu a PIN kreditní karty.

Graf č. 18 Osobní údaje, které jsou studenti ochotni odeslat uživatelům internetu bez ověřené identity



n=317

Mezi osobní údaje, které jsou studenti ochotni odeslat uživatelům internetu bez ověřené identity, patří stejně jako v předcházejícím grafu jméno a příjmení, e-mail a fotografie obličeje. Na dalších místech nalezneme telefonní číslo či kontaktní údaje k instant messengerům. Je zajímavé, že fotografie obličeje je považována za běžně sdílený i běžně odesílaný osobní údaj, ačkoli je její možné zneužití vysoce rizikové. Proto nás rovněž zajímalo, zdali byli studenti osloveni v prostředí internetu s žádosti o zaslání fotografie obličeje a zdali na tuto žádost reagovali.

Sdílení fotografie obličeje

Více než polovina respondentů (53,65 %) byla **oslovena** svými internetovými známými (se kterými se nesetkali v běžném životě) **s žádostí o fotografii obličeje**. Tuto žádost pak akceptovalo a své skutečně fotografie tváře těmto osobám odeslalo 70,83 % respondentů.

Stejně tak jsme sledovali, zdali své internetové známé běžně s žádostí o zaslání fotografie obličeje oslovují také respondenti našeho výzkumu. Tuto žádost potvrdila více než třetina z nich, konkrétně 35,19 %.

Vzhledem k tomu, že fotografie obličeje je považována za vysoce citlivý osobní údaj (Kopecký, Szotkowski, Krejčí, 2010-2012), který lze poměrně snadno zneužít k variabilním útokům na dítě i dospělého, zaměřili jsme se rovněž na to, jak vnímají rizika spojená se sdílem tohoto typu fotografie naši respondenti. **Rizikovost odesílání nebo zveřejňování fotografií obličeje si uvědomuje více než 3/4 respondentů (77,19 %).**

Vybrané názory studentů na rizikovost sdílení fotografie obličeje uvádíme níže:

- *Může ji zneužít např. k nějaké fotomontáži. U dětí si takhle někdo může vyhlídnout dítě např. „k prodeji".*
- *Z důvodu vyhledání a třeba následného vydírání, ublížení na zdraví.*
- *Vytvoření falešné identity.*
- *Může se to zneužít, pomocí Photoshopu se dá mnoho přidělat, takže pak se můžou lidé vydírat.*
- *Podle toho mě pak bez problému identifikují v běžném životě a mohou mi tak nějak ublížit i osobně.*

- *Může to být zneužito tak, že někdo z mého obličeje vytvoří karikaturu či jinak zesměšňující „fotku" a to není pro nikoho příjemné.*

- *Fotografie může bát použitá v náš neprospěch-fotomontáž apod. a následné vydírání,*
  Nikdy to nemusí být ta osoba se kterou si píšu, a je to riziko z hlediska zneužití mé fotografie,

- *Podle podoby mě dotyčná osoba z internetu může poznat i v reálu. (např. ve škole, na ulici). Může mě třeba sledovat.*

- *Protože osoba může moji fotografii dále šířit.*

- *Převzetí identity-fotka jako důkaz, prostředek k rozeznání oběti pro případné komplice útočníka v případě, že plánují fyzický či psychický útok.*

- *Z důvodu zneužití, popřípadě pozdější pracovní nabídky (nevhodné fotografie, i když jsou pomyslně přístupné „jen" pro určité uživatele).*

- *Jelikož jsme tím odkryli svou identitu a nemůžeme již říci při oslovení, že to nejsme my. a také se fotografie dá přeupravit a zneužít v náš neprospěch.*

- *Myslím, že by se mohlo stát (a jistě se tak i stalo), že nějaká neznámá osoba může tyto fotografie zneužít a třeba se vydávat za osobu, která na fotce je!*

- *Organizovaný zločin, zneužití fotografie jako také (např. prostřednictvím montáže na jinou fotografii).*

- *Člověk, se kterým chatujeme, může být násilník, pedofil apod. Může si na nás počkat a obtěžovat nás. Nikdy nevíš, kdo sedí na druhé straně PC sítě.*

- *Fotka se dá dnes různě upravit, může ji klidně použit do porno snímku.*

- *Někdo se za mě může vydávat. Může o mě udávat milné informace. +Pokud by to byl někdo nebezpečný, pozná mě podle fotografie a může si na mě počkat třeba poblíž školy.*

- *Fotografie (zvlášť jestli se jedná o fotografii dítěte v letech od 12 - 16), může být zneužita například jako profilová fotka nějakého pedofila, který si vytváří falešný profil, aby mohl navazovat vztahy s dětmi v tomto věku.*

- *Může být zneužita pro různé perverznosti. Photoshop dnes dělá divy, a pokud se někomu člověk v dnešní době znelíbí, je to velký problém.*

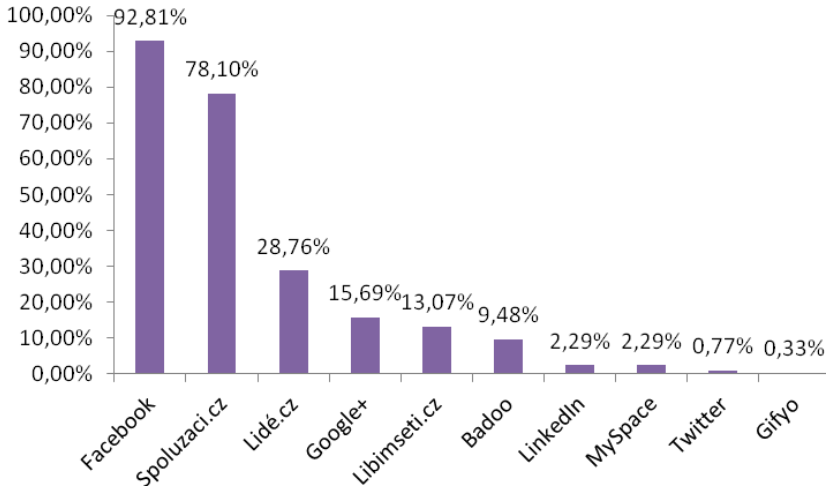
- *Odesláním ztrácím kontrolu nad tím, co se s fotografií stane, jak bude použita, k čemu bude sloužit.*

- *Fotografie může být upravena - použita v rámci jiné fotografie nebo použita na webu s mravně závadným obsahem, reklamou apod. Mohla by být teoreticky použita druhou osobou, která je v kontaktu s nějakou mafií, a tato osoba by se mohla v internetové či telefonické komunikaci vydávat za mne. V případě zjištění mých kontaktních údajů by to nemuselo dopadnout moc dobře… čistě teoreticky…*

3.5 Riziková komunikace studentů v rámci sociálních sítí

V rámci výzkumu rizikového chování studentů Pedagogické fakulty Univerzity Palackého v Olomouci jsme se zaměřili rovněž na oblast sociálních sítí, primárně nás zajímalo, na jakých sociálních sítích respondenti nejčastěji působí (mají aktivní účty) a zda byli v rámci sociálních sítí vystaveni některé z forem útoků.

Graf č. 19 Aktivní účty respondentů v rámci sociálních sítí



n=306

Nejvíce studentů má aktivní účet na sociální síti Facebook (92,81 %), Spolužáci.cz (78,10 %) a Lidé.cz (28,76 %), podíl ostatních sociálních sítí je minoritní. V souvislosti s aktivními účty jsme rovněž sledovali, zdali si studenti přidávají mezi své „virtuální přátele" osoby bez identity ověřené v reálném světě. Pouze 9,06 % respondentů odpovědělo, že si neznámé „virtuální přátele" přidává do svého seznamu přátel bez ověření jejich identity. Upozorňujeme, že „virtuální

přátelé“ připojení např. k účtu na Facebooku mají vyšší stupeň přístupu k osobním informacím na profilu uživatele, ke kterému jsou připojeni.

Tabulka 2. Kyberšikana a související jevy u uživatelů Facebooku

Forma	***n***	***Procento***	***ID otázky***
Prozvánění	117	11,62 %	854
Kyberšikana - verbální útoky	108	2,11 %	872
Zneužití účtu ke kyberšikaně*	16	2,11 %	856
Kyberšikana - vyhrožování	43	15,14 %	860
Kyberšikana šířením fotografie	33	5,99 %	867
Kyberšikana - vydírání	17	16,00 %	859
Kyberšikana šířením videonahrávky	6	41,20 %	865
Kyberšikana šířením audionahrávky	6	38,03 %	863

n = 284

* Vypočítané hodnoty jsou kombinací zaznamenaných průniků na účet a zneužití účtu ke kyberšikaně. Útok na účet zaznamenalo 35,21 % studentských uživatelů Facebooku.

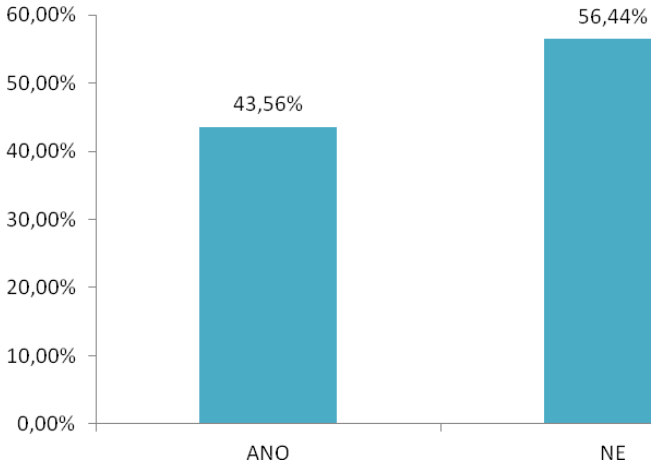
33,80 % respondentů s aktivním účtem na Facebooku rovněž potvrdilo, že byli osloveni svými virtuálními přáteli bez ověřené identity k osobní schůzce, přičemž 64,58 % na tuto schůzku skutečně šlo.

3.6 Vnímání pravdy a lži

Důležitou částí našeho výzkumu bylo zjistit, zdali studenti na internetu hovoří v rámci komunikace vždy pravdu nebo zda je běžné, že lžou. Stejně tak nás zajímalo, nakolik věří ostatním uživatelům internetu. 1,69 % studentů věří tomu, co jim o sobě sdělují ostatní lidé na

internetu, 98,31 % informacím od virtuálních uživatelů nevěří. Další otázka byla zaměřena na zjištění, kolik studentů při komunikaci na internetu říká vždy pravdu.

Graf č. 20 Říkáš při komunikaci na internetu vždy pravdu?



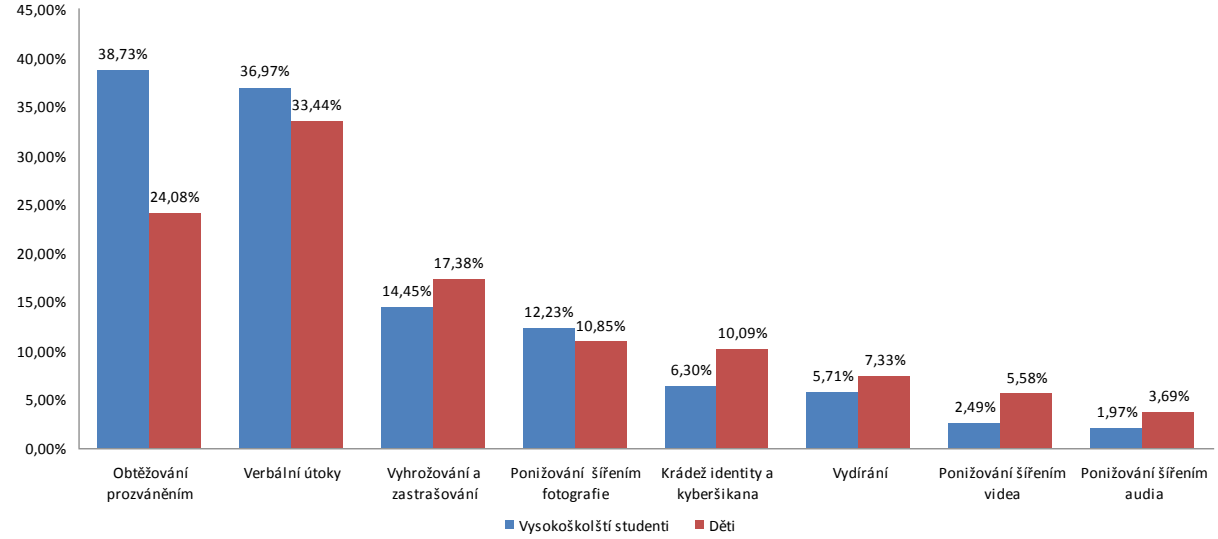
n=303

Necelá polovina studentů (43,56 %) uvedla, že o sobě při komunikaci na internetu vždy říká pravdu.

3.7 Komparace výsledků vysokoškolských studentů a dětí

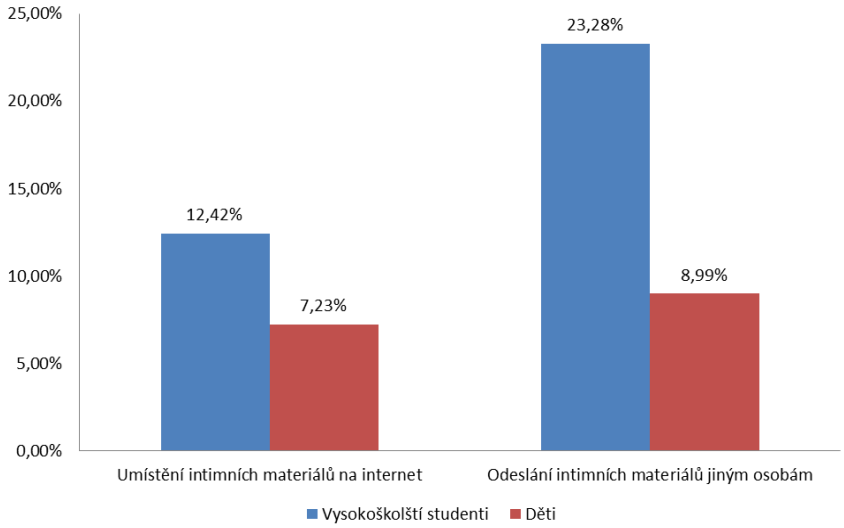
Vzhledem k tomu, že jsme v roce 2012 a 2013 realizovali rovněž výzkumy zaměřené na rizikové chování pubescentů a adolescentů v prostředí internetu, pokusíme se výsledky zjištění v klíčových kategoriích porovnat. Nejdříve se zaměříme na výskyt jednotlivých forem kyberšikany u dětí a u vysokoškolských studentů, přičemž budeme sledovat výskyt kyberšikany ve stejném období – v roce 2012. Základní výsledky komparujeme s výzkumem Nebezpečí internetové komunikace 4 (Kopecký, Szotkowski, Krejčí, 2013), který byl realizován na vzorku více než 20 000 dětských respondentů (věkové rozpětí 11-17 let).

Graf č. 21 Komparace obětí kyberšikany (vysokoškolští studenti vs. děti)



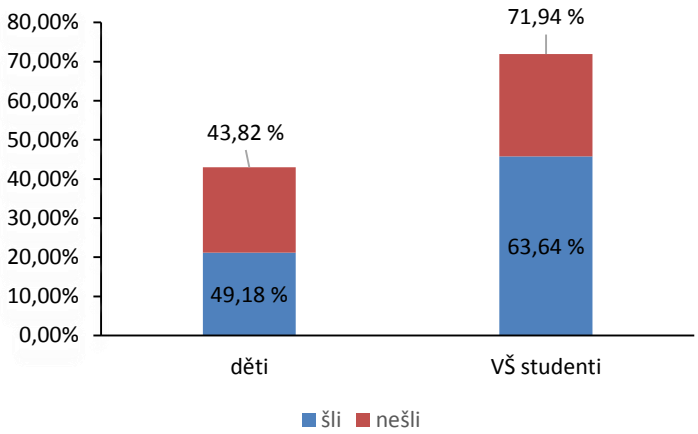
Dalším fenoménem, na který jsme se zaměřili, byl sexting. Zde jsme sledovali rozdíly u základních forem sextingu – sdílení vlastních intimních sexuálně laděných materiálů v prostředí internetu a odesílání těchto materiálů jiným osobám.

Graf č. 22 Komparace výskytu sextingu (vysokoškolští studenti vs. děti)



Z výsledků lze vyčíst, že výskyt sextingu u vysokoškoláků je oproti dětem v obou sledovaných formách téměř dvojnásobný. To lze vysvětlit tím, že vysokoškoláci plně žijí sexuálním životem, ke kterému v současnosti pravděpodobně sdílení intimních materiálů patří.

Graf č. 23 Osobní schůzky s lidmi bez ověřené identity



Na osobní schůzku s uživateli internetu bez ověřené identity bylo pozváno 43,82 % dětí a 71,94 % vysokoškolských studentů, přičemž téměř polovina dětí (49,18 %) a více než polovina vysokoškolských studentů (63,64 %) na schůzku šla.

4 Shrnutí výsledků

Studenti Pedagogické fakulty Univerzity Palackého v Olomouci potvrzují, že se s kyberšikanou setkali ať již na pozici oběti či útočníka. Nejrozšířenější formou kyberšikany, se kterou se studenti na pozici oběti setkali, je kyberšikana realizovaná formou opakovaných verbálních útoků (36,97 %). Další frekventovanou formou, se kterou se respondenti setkali, je vyhrožování a zastrašování (14,45 %). Kyberšikana byla nejčastěji realizována prostřednictvím SMS zpráv a sociálních sítí (zejména Facebooku).

Úroveň sextingu u budoucích pedagogů přesahuje hranici 12 % (12,42 %) u umisťování sexuálně laděných materiálů na internet, 23 % (23,28 %) u odesílání intimních materiálů jiným osobám v prostředí internetu.

Téměř polovina studentů (43,82 %) byla pozvána na osobní schůzku s neověřenými uživateli internetu, přičemž téměř polovina z oslovených (49,18 %) na tuto schůzku šla.

Studenti v prostředí internetu běžně sdílejí své osobní údaje, nejčastěji jméno a příjmení (92,48 %), fotografii obličeje (84,95 %) a e-mail (72,10 %).

5 Výzkum hesel mladých uživatelů internetu

V návaznosti na výzkum rizikového chování českých vysokoškoláků modelovaných na případu Pedagogické fakulty Univerzity Palackého v Olomouci jsme v roce 2013 zrealizovali výzkum hesel mladých uživatelů internetu. V průběhu realizace tohoto výzkumu jsme zanalyzovali více než 3700 hesel uživatelů internetových služeb, přičemž převážnou většinu (více než 76 %) souboru tvořili lidé ve věku 18-25 let. Ze souboru dat jsme oddělili data spojená se studenty českých vysokých škol a ty jsme pro potřeby této monografie zanalyzovali z 3 hlavních hledisek:

a) *formální analýza hesla* (jaké jsou formální vlastnosti hesla, délka hesla, alfanumerické složení hesla a další formální specifika),

b) *sémantická analýza hesla* (zdali je heslo obsaženo ve slovníku, tedy zda jde prolomit útokem slovníkového typu, jakou má heslo vazbu uživatele, z jakých oblastí se hesla volí apod.),

c) *užití hesla* (zdali je heslo užíváno univerzálně, tj. jedno heslo slouží k přístupům do více internetových služeb).

Průměrná délka hesla uživatele internetu ve věku 18-25 let je 8,71 (viz tisková zpráva k výzkumu zveřejněná na internetovém portálu E-Bezpečí www.e-bezpeci.cz), u vysokoškolských studentů má **průměrné heslo délku 8,93** znaků.

Z hlediska formální analýzy jsou **nejčetnější hesla alfanumerická**, která obsahují kombinaci číselné hodnoty a znaku (tvoří 47,72 % souboru), naopak velmi málo uživatelů používá čistě číselná hesla (pouze 11 % vzorku).

V rámci sémantické analýzy jsme provedli korelaci hesel se slovníkovou databází české slovní zásoby (více než 166 000 slov a slovních tvarů) a

sledovali, nakolik je heslo možné „prolomit“ s použitím běžných slovníkových útoků. Z celkového vzorku hesel **bylo ve slovníku možné dohledat pouze 6,92 % hesel**. To tedy znamená, že běžným slovníkovým útokem lze odhalit pouze velmi malé množství hesel. Kromě toho většina útoků zaměřených na prolomení hesel využívá slovníky obsahující zejména anglickou slovní zásobou.

Ze sémantického pohledu lze hesla rozdělit do 6 základních kategorií:

1. *Hesla běžně obsažená ve slovnících*

   Nejčastěji se jedná o vlastní jména – zejména křestní jména v neutrálních tvarech, ale také v podobě zdrobnělin (*jana, janička, jaňule, monika, monička…*), názvy obcí (*praha, ostrava, olomouc*), ale také jména obecná (např. slova typu *sluníčko, lokomotiva, hacker, politika, studium, maturita*)). U vlastních jmen se v heslech obvykle nerespektuje velké písmeno na začátku slov.

2. *Hesla složená z části pocházející z běžné slovní zásoby doplněná o číslice či série znaků bez specifického významu*.

   Mezi tato hesla patří např. kombinace jména a série vzestupných a sestupných znaků bez specifické logické souvislosti (*jana123*).

3. *Hesla složená z části pocházející z běžné slovní zásoby doplněná o číslice či série znaků se specifickým významem*.

   Mezi tato hesla patří např. kombinace jména a číslic, která mají specifický význam, označují např. rok narození uživatele (*petr1980*).

4. *Hesla s modifikovanou diakritikou*

   Velmi dobrým typem hesla je heslo složené z českých slov obsahující diakritiku nahrazenou číslicemi, které označují diakritické znaky na běžné klávesnici. Např. heslo dobrývečer lze pomocí této jednoduché modifikace přepsat jako *dobr7ve4er*. Vzhledem k tomu, že dosud nejsou rozšířené slovníky obsahující česká slova převedená do těchto modifikovaných podob, lze tato hesla považovat za velmi silná.

5. *Hesla složená výhradně z číslic*

   Tato hesla se vzhledem k jejich poměrně snadnému prolomení útoky typu „brute-force" téměř neužívají, užívá je pouze každý 10. uživatel internetu. V rámci útoku brute-force program, který se snaží prolomit vaše heslo, využívá k prolomení logické kombinace písmen a číslic ve všech kombinacích.

6. *Alfanumerická hesla s náhodně generovanými znaky*

   Jejich velkou výhodou je jejich silná odolnost proti automatizovaným útokům, jejich velkou slabinou je však jejich nezapamatovatelnost.

Téměř polovina studentů (48 %) používá pro přístup k internetovým službám univerzální heslo, toto heslo se využívá zejména k přístupu do hlavní emailové stránky a pro přístup k účtu v sociální síti (nejčastěji na Facebook).

V naší analýze jsme rovněž sledovali, zda čeští uživatelé využívají hesla, která jsou často citovaná v seznamech nejméně bezpečných hesel. Mezi typické příklady těchto hesel patří kombinace číslic *12345*, slovo *heslo*

apod.). Tato hesla mladí uživatelé internetu téměř nepoužívají. Tutu skutečnost budeme demonstrovat v následující tabulce:

Tabulka 3. Výskyt nejméně bezpečných hesel

Testované heslo	Počet výskytů	%
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
slovo „heslo“	1	0,03

n=3743

Hesla složená ze sestupné číselné řady se nevyskytovala v souboru vůbec. **Na základě zjištěných skutečností lze tvrdit, že časté používání jednoduchých číselných řad jako hesel nebylo prokázáno a v dané věkové kategorii jej lze považovat za mýtus**.

Mezi nejvíce frekventovaná hesla patří zejména ***názvy měst*** a ***křestní jména***, dále slova ***sluníčko, maminka, lokomotiva,*** *u studentů dále slova* ***studium, maturita***.

Při běžném útoku na internetový účet však útočníci v českém prostředí zpravidla nevyužívají automatické formy útoku, ale soustřeďují se na

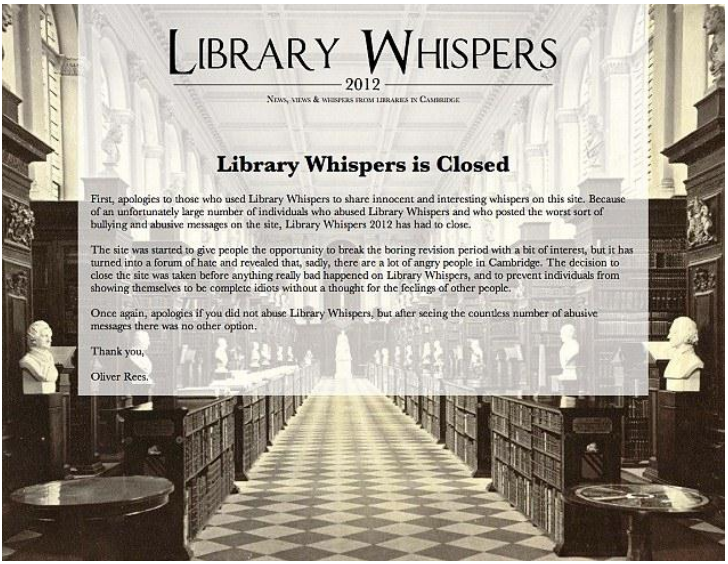
prolamování kontrolních otázek pro přístup k účtům. Ty jsou často podceňovány a stávají se kritickým místem pro přístup zejména k emailovým účtům. Odhalit odpověď na kontrolní otázku je totiž zpravidla podstatně jednodušší, než zjistit správné heslo.

Další informace k tomuto výzkumu lze nalézt na internetových stránkách www.prvok.upol.cz.

6 Světové kauzy kyberšikany studentů

6.1 Kyberšikana na Cambridžské univerzitě (2012)

Typickým příkladem kyberšikany u vysokoškolských studentů představuje kauza, která proběhla počátkem roku 2012 na Cambridge University. Studenti si zde založili internetové stránky zaměřené na výměnu informací o zkouškách, učitelích, studijních materiálech, apod. Využívaly se pak také pro komunikaci mezi univerzitními knihovnami. Záznamy se na webu zveřejňovaly v reálném čase (podobně jako na Twitteru či Facebooku). Webové stránky měly název Library Whispers („knihovna šeptá“ či „šepoty knihovny“). Běžná komunikace uvnitř stránek však velmi rychle přerostla v diskusi plnou útoků na konkrétní studenty a zaměstnance univerzity. Za 5 dnů zaznamenaly tyto internetové stránky přes 1000 příspěvku



Zpráva o uzavření webu Library Whispers (Zdroj: Dailymail.co.uk)

Ukázkové záznamy z komunikace (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*

Případ z Oxfordu proběhl jen týden poté, co téměř 2000 studentů uspořádalo velkolepou party ve veřejném parku, při které děsili místní obyvatele, opíjeli se do bezvědomí, močili na trávník, zvraceli na veřejnosti před místními. Na akci zasahovalo několik policejních hlídek a zdravotnických jednotek.

Fotografie ze zásahu na opilé studenty (Zdroj: Dailymail.co.uk)

6.2 Sebevražda Tylera Clementiho (2010)

Houslista Tyler Clementi, 18letý student Rutgers University v New Jersey (USA) v roce 2010 spáchal sebevraždu skokem z mostu George Washingtona poté, co jej bez jeho vědomí spolubydlící Dharun Ravi a jeho přítelkyně Molly Wei s použitím webkamery nahrávali, záznam z kamery vysílali na internet a umožnili dalším lidem sledovat, co se děje v Clementiho pokoji. Vyšla tak najevo Clementiho homosexualita, protože byl natočen, jak se líbá s jiným mužem. Takto komentovala případ přední světová média. Případ je však podstatně složitější, než se zdá.

Clementi se již před sebevraždou se svou homosexualitou svěřil rodičům, otec ho pochopil, matka se však nechtěla s Tylerovou homosexualitou smířit. Později v rozhovorech vysvětlovala, že se nemohla s homosexualitou svého syna vyrovnat, protože je silně věřící a věří, že je homosexualita hřích.

Ravi Dharun si o svém novém spolubydlícím Tylerovi hledal na internetu informace a na internetové stránce Justusboys zaměřené na homosexuály objevil Tylerovy příspěvky. S tímto se podělil na Twitteru, na kterém zveřejnil příspěvek: *Právě jsem zjistil, že je můj spolubydlící gay.* O tom se také později Tyler dozvěděl.

Ve dnech 19. a 21. září 2010 Tyler poprosil Raviho, zdali by mohl mít pokoj na večer pro sebe. Ravi se seznámil s Tylerovým přítelem a Tyler Ravimu řekl, že chtějí být večer spolu sami. Ravi se však obával, že by mu Tylerův přítel mohl něco ukrást, proto svůj počítač a webkameru umístil tak, aby mohl dění v místnosti sledovat. Ravi a Wai poté sledovali skrze službu iChat dění v pokoji a viděli, že se Clementi a jeho host líbají. Ravi pak 20. září umístil na svůj Twitter zprávu*: Spolubydlící mě požádal, abych mu až do půlnoci půjčil pokoj. Šel jsem do pokoje k Molly, zapnul kameru. Viděl jsem ho, jak to dělá s klukem. Jó.*

Dne 21. září Ravi zveřejnil zprávu, že uspořádá živý přenos z Clementiho pokoje, a pozval uživatele Twitteru na videochat, který proběhne od 21:30 do 0:00. Odpoledne Ravi namířil kameru na Clementiho postel, přepnul počítač do režimu spánku (sleeping mode). U soudu pak Ravi tvrdil, že si celou akci rozmyslel a kameru namířil na svou vlastní postel, policie však potvrdila, že webkamera byla stále namířena na postel Clementiho. Když se Tyler vrátil do pokoje, viděl, že je počítač a kamera vypnutý, a napsal svému příteli, že pro jistotu vytáhl počítač ze zásuvky.

Ten den oznámil Tyler správci koleje (osobně i emailem), že jej Ravi webkamerou šmíruje, že jej natočil při sexu s jiným mužem a žádal, aby byl Ravi potrestán. Zároveň požádal o jiný pokoj.

V noci 22. září 2010 opustil Clementi kolej, zamířil k mostu George Washingtona a v 20:42 přidal na svou zeď na Facebooku zprávu: *Skáču z mostu George Washingtona, promiňte*. Zanechal dopis na rozloučenou, který však nebyl nikdy zveřejněn.

Mooly Wei nakonec výměnou za svědectví proti Ravimu nebyla trestně stíhána, bylo jí uděleno 300 hodin obecně prospěšných činností. Dharun Ravi byl v roce 2012 odsouzen k 30 dnům vězení, 3 letům probačního dohledu a pokutě 10 000 $. Po 20 dnech byl z vězení propuštěn.

Tyler Clementi (Zdroj: Facebook.com, profilová fotografie)

Dharun Ravi (Zdroj: Time.com)

Poslední zpráva na zdi Clementiho (Zdroj: Facebook.com)

Ačkoli média spekulovala o tom, že Ravi vysílal záznamy z jejich pokoje jiným uživatelům internetu, nikdy se tak nestalo, v případu neexistuje žádná dostupná nahrávka sexuálního aktu, nebyly zveřejněny žádné fotografie zachycující tyto události (existuje pouze fotografie, ve které nelze rozeznat tváře aktérů a oba jsou oblečeni) apod. Videopřenos proběhl pouze přes chodbu – do vedlejšího pokoje, ve kterém dění pozoroval Ravi Dharun.

6.3 Happy slapping z Oxfordu (2008)

Případ kyberšikany ve formě happy slappingu se v roce 2008 odehrál také na Oxfordské univerzitě. Student Nick Brodie, prezident univerzitního veslařského klubu, natočil svého přítele Colina Groshonga při útoku na jiného studenta z Imperial College v Londýně, Willa McFarlanda, který patřil ke konkurenčnímu veslařskému klubu (Miller, 2008). Celý útok se odehrál v Polsku, kde se všichni účastnili Wroclavské regaty, veslařského závodu.

Celá akce proběhla na WC v nočním klubu (Sears, 2008). Útočník Colin Groshong se konkurenčnímu veslaři nejdříve vysmíval, předváděl obscénní gesta, pak McFarlanda udeřil několikrát do obličeje.

Colin Groshong a Nick Brodie (Zdroj: Dailymail.co.uk)

Po návratu do Anglie Brodie záznam zveřejnil na Facebooku, kde jej komentovali další uživatelé. Celé řadě uživatelů připadala nahrávka zábavná a začali ji komentovat. Ukázky z komentářů:

Henry Sheldon, prezident veslařského klubu Oxfordské univerzity:
Díky Colinovi za sdílení tohoto videa, úplně mi to rozzářilo můj nudný den v knihovně. Smál jsem se, až jsem plakal.

Colin Brodie:
Je to jedna z nejzábavnějších věcí, co jsem kdy viděl.

Po četných stížnostech (včetně stížností od Groshonga a McFarlanda) však Brodie změnil svůj postoj k celé akci, napsal, že neví, proč záznam nahrál a zveřejnil, a celý záznam smazal. Oba aktéři se snažili vysvětlit, že incident byl vyprovokovaný, ačkoli to na videu není vidět, a že

neměli reagovat tak, jak reagovali. Groshong se za celou akci omluvil McFarlandovi a usmířili se.

7 Kauzy kyberšikany studentů z České republiky

7.1 Kyberšikana a vydírání studentek (2010)

V říjnu 2010 olomoucká policie přijala trestní oznámení od dvou olomouckých studentek, že se tehdy ještě neznámý pachatel naboural do jejich elektronické pošty. Zde získal jejich intimní fotografie, jejichž pomocí je potom vydíral (Zdroj: Policie ČR).

Student informatiky na Univerzitě Pardubice z Nymburska na internetu zakládal fiktivní internetové stránky, v rámci kterých od lidí, kteří se na ně zaregistrovali, získával e-mailové adresy a přístupová hesla (realizoval tzv. phishing[3]). Zakládal např. různé diskusní skupiny na Facebooku, ve kterých sliboval zajímavé výhry, pokud se zaregistrujete na jeho podvržené stránky. Celkově tímto způsobem získal databázi více než 1800 emailových adres. Jakmile do e-mailových schránek svých obětí pronikl, zjistil, zdali neobsahují nějaké intimní fotografie. Ty si stáhl a vyhrožoval dívkám, že jejich fotografie zveřejní na sociálních sítích (což se rovněž v několika případech stalo). Desetitisíce žen a dívek tak nutil, aby mu posílaly další fotografie, případně se svlékaly před online kamerou. Při domovní prohlídce byla zajištěna rozsáhlá databáze, kterou tvořilo několik gigabytů fotografií. Motivem pachatele bylo získávání dalších intimních materiálů. V roce 2011 byl pachatel podmínečně odsouzen na 9 měsíců odnětí svobody s odkladem na 16

[3] Phishing je označení pro komunikační praktiky, které jsou zaměřeny na krádež citlivých osobních údajů, jako jsou hesla, údaje k bankovním účtům, čísla platebních karet atd. Výklad vzniku termínu phishing je nejednotný.

měsíců za Porušení tajemství dopravovaných zpráv (§ 182/1 TZ) a Sexuální nátlak (§ 186/1 TZ).

7.2 Případ Libor (2013)

Submisivní student Libor (19 let) se prostřednictvím služby Moneyslave (www.moneyslave.cz), která je orientována na seznamování v rámci komunity BDSM[4], seznámil s 20letou Kateřinou, studentkou Fakulty zdravotnických věd Pedagogické fakulty Univerzity Palackého v Olomouci. Navázali spolu úzkou komunikaci, psali si prostřednictvím instant messengeru Skype, realizovali rovněž videohovory. Postupně si vyměnili svoje kontakty, fotografie, rovněž se vzájemně propojili pomocí sociální sítě Facebook. Po čase spolu začali realizovat videochaty (s použitím webkamery), přičemž Libor plnil nejrůznější úkoly, které mu Kateřina zadávala. Úkoly byly stále odvážnější a celá komunikace mezi oběma aktéry vyvrcholila tím, že se Libor před webkamerou obnažil a masturboval. Kateřina si však celou dobu veškeré záznamy z webkamery nahrávala, stejně tak si nahrála Liborovo intimní video a začala Libora vydírat zveřejněním videa a požadovala na něm okamžité zaplacení 12 000,- Kč.

Autentická komunikace:

Kateřina: Měl by ses snažit, ty čubko, abys mi vyhověl, neboť celé tvoje honění tady mám na videu.

Kateřina: Myslím, že když zajdeš do banky a požádáš o kontokorent, máš prachy okamžitě. 12 tisíc, milánku, a dokonce ti dám dobré hodnocení.

[4] Zkratka BDSM pochází z angličtiny a je kombinací více zkratek, zejména S&M, tedy sadismus a masochismus, D&S tedy dominance a submisivita a B&D tedy bondage (svazování) a disciplína. Termín BDSM samotný zahrnuje pestrou paletu neobvyklých sexuálních praktik.

Kateřina: Chceš to vidět, ty čubko? Pokud mi nevyhovíš, mohl bys to vidět na YouTube.

Kateřina: Pokud dneska nedostanu doklad potvrzený od banky o poslání, video poputuje na YouTube.

V tomto okamžiku Libor kontaktoval poradnu Centra prevence rizikové virtuální komunikace / projektu E-Bezpečí s prosbou o pomoc. Prvotním šetřením bylo zjištěno, že uživatelka použila falešný profil studentky, stejně tak Liborovi poslala podvrženou fotografii, kterou stáhla z cizího profilu. Tým projektu E-Bezpečí ve spolupráci s dalšími partnery zajistil IP adresu pachatelky, identifikoval její skutečnou identitu s použitím identifikace bankovního účtu (pachatelka Liborovi zaslal číslo účtu, na který má složit peníze, ten účet však měla zároveň spárovaný s profilem na aukční serveru Aukro) v kombinaci s veřejně dostupnými databázemi profilů, rovněž byl zaměřen region, ze kterého pachatelka s Liborem komunikovala. Následně bylo odkryto několik profilů na sociálních sítích, které pachatelka aktivně využívala. Informace byly předány Liborovi a zároveň Policii ČR s podezřením z trestného činu Vydírání. Jakmile Libor pachatelku oslovil jejím skutečným jménem, znejistěla a začala se vymlouvat, že vlastně nic neudělala a že video nezveřejní. Případ byl policií uzavřen s podezřením na spáchání trestného činu a předán státnímu zástupci, ten však případ zastavil s tím, že podle jeho právního názoru nedošlo ke spáchání trestného činu či přestupku.

8 Kyberšikana zaměřená na pedagogy českých vysokých škol

Kyberšikana je ve společnosti vnímána jako téma spojené zejména s pubescenty a adolescenty, jen minimálně je v tomto kontextu diskutováno o kyberšikaně dospělých. Přitom kyberšikana dospělých reálně existuje, hovoří se o ní však podstatně méně a zaměstnavatelé se ji - snad z obavy z diskreditace dané instituce - často snaží tutlat.

Základní rozdíl mezi kyberšikanou dětí a dospělých lze spatřovat především v motivu tohoto jednání: zatímco u dětí je kyberšikana v cca 95 % realizována „z žertu“, u dospělých je situace zcela opačná - zde vlastní kyberšikana probíhá ve většině případů za účelem ublížit jiné osobě, zdiskreditovat ji, případně jí zničit její osobní i profesní život. V těchto případech pak chování útočníků přechází v přestupky či trestné činy - zejména v trestný čin násilí proti skupině obyvatel a proti jednotlivci, nebezpečné pronásledování či nebezpečné vyhrožování. Stejně tak ovšem i na vysokých školách dochází k situacím, kdy se zpočátku nevinný žert zvrhne do skutečného pronásledování a ubližování vyhlédnuté oběti.

V této odhalíme několik případů, z nichž některé jsou mediálně známé, řada z nich je však veřejnosti zcela neznámá. S ohledem na citlivost těchto neveřejných případů ze strategických důvodů neuvádíme jména institucí, ve kterých se daný případ odehrál. Všechny z případů se však odehrály v posledních pěti letech na některé z veřejných či soukromých vysokých škol.

8.1 Případ online vyhrožování z Masarykovy univerzity (2008)

Čtyři měsíce probíhala kyberšikana realizovaná rozesíláním anonymních e-mailů s výhrůžkami smrti, které zasílal profesor Břetislav Horyna svému kolegovi, profesoru filozofie, Jaroslavu Hrochovi.

Profesor Hroch dostával anonymy plné výhrůžek smrtí celé měsíce. V prosinci roku 2008 mu kdosi skrytý za identitu zesnulého představitele katolického disentu Augustina Navrátila napsal, že už brzy „si pro něj přijde". Profesor zprávu ignoroval, v lednu ale dorazil další anonym, o poznání drsnější: „Nech si udělat vývod bokem, hrochu, ať nemáš všechno v gatích – teď už se z toho nedostaneš. Víme o tobě i o té tvé podařené famílii." (Idnes.cz) Následovaly další emaily, ze kterých krátce citujeme: *Jedna injekce v trolejbusu, celkové ochrnutí, shniješ zaživa. A všichni budou rádi, že se zbavili magora. Nech se zavřít do blázince, tam tě necháme na pokoji, mrtvolo. Přípravek, na který jsme čekali, je už na místě. Ale brzo už tě to bolet nebude, budeš mít pempersky a tři injekce sedativ denně. To by ti prospělo, pár ti jich naflákat, až budeš žrát chodník.* (Zdroj: Idnes.cz)

Horyna byl obžalován a uznán vinným za spáchání trestného činu násilí proti skupině obyvatel nebo jednotlivci a byl mu uložen peněžitý trest ve výši 50 000 Kč s náhradním trestem odnětí svobody na 2 měsíce. Proti rozsudku se odvolal, nicméně trest mu byl v roce 2012 potvrzen i odvolacím soudem.

Břetislav Horyna (foto Otto Ballon Mierny, MAFRA)

Případ není v České republice ojedinělý, různé projevy šikany či kyberšikany, stejně jako mobbingu[5] se vyskytují mezi pedagogy téměř na všech vysokých školách.

8.2 Doktorandka Jitka (veřejná vysoká škola, leden – květen 2011)

Jitka byla čerstvou absolventkou jedné české veřejné vysoké školy, získala titul magistr a usilovala o to, aby na své alma mater ještě nějaký čas zůstala. Přihlásila se tedy k přijímacím zkouškám do prezenčního

[5] Mobbing je druh šikany realizované na pracovišti, která je dlouhodobá a opakovaná. Obětí mobbingu je 4-8 % pracujících (Bendl, 2002). Hranice mezi mobbingem a kyberšikanou není ostře vyhraněna, mobbing lze vnímat jako jednu z forem kyberšikany dospělých.

doktorského programu, byla přijata a na fakultu nastoupila. Seznámila se s kolegy, začala vyučovat, pracovala na své vědecké práci.

Po čase jí však na její telefon začaly chodit podivné SMSky, ve kterých jí někdo neznámý začal vyhrožovat a zastrašovat: Sleduji tě, ty děvko. Brzy si pro tebe přijdu a vychutnám si tě. Vím, kde bydlíš. Jitka SMSky zpočátku ignorovala, zablokovala si neznámé telefonní číslo, ze kterého chodily, po čase se však začaly objevovat první e-maily podobného ražení: Přede mnou se neschováš, vykuchám tě. Zmiz z fakulty i z našeho města. Jestli budeš kontaktovat policajty, bude to to poslední, co v životě uděláš. Celé jednání probíhalo více než 5 měsíců, emaily začaly doplňovat vzkazy od neznámých lidí na Facebooku, intenzita se stupňovala. V Jitce postupně narůstal strach. Nakonec Jitka kontaktovala Policii ČR.

V průběhu prověřování případu se mezi podezřelé dostala skupina studentů, které Jitka vyučovala v seminářích a kteří u ní v rámci semestru řádně neukončili povinný seminář. Postupně došlo k zjištění IP adresy, ze které byly odesílány výhružné emaily, a nakonec se jeden ze skupiny studentů přiznal. 23letý Petr N. se rozhodl, že se za svůj školní neúspěch Jitce pomstí a začal Jitce vyhrožovat. V seminářích a na fakultě si pak užíval toho, jak se chování Jitky měnilo… a užíval si strachu, který v Jitce vyvolal.

Policie případ vyhodnotila jako spáchání trestného činu násilí proti skupině obyvatel nebo jednotlivci a podezření ze spáchání trestného činu nebezpečné vyhrožování. Proti rozhodnutí se odvolal, výsledky odvolacího řízení nejsou známé. Etickou komisí fakulty byl Petr rovněž vyloučen z fakulty. Fakulta případ nikdy nezveřejnila, na sdělování jakýchkoli informací o případu bylo uvaleno embargo.

8.3 Mikeš (září 2011 až leden 2012)

Mikeš pracoval již 8. rokem na jedné ze známých českých veřejných vysokých škol jako odborný asistent. Získal titul Ph.D., postupně se připravoval na habilitaci. Poměrně mladý pedagog byl mezi studenty oblíben, s řadou z nich si tykal, chodil se studenty na nejrůznější party. Studentky ho milovaly a zbožňovaly, byl pro ně ideální kombinací hezkého a úspěšného mladého pedagoga. Mikeš si však ve vztahu ke studentkám vždy udržoval odstup, neoddával se s nimi sexuálním hrátkám, odmítl řadu nabídek od zamilovaných studentek. Definoval si hranice, které nepřekročil.

(Ilustrační foto)

Bohužel dvě studentky, které Mikeš vyučoval, jeho odmítnutí nezvládly a rozhodly se, že se mu pomstí. Mezi studenty se náhle začala šířit pověst, že Mikeš odmítá studentky, protože je homosexuálně

orientovaný, a že má vztah se svým kolegou. Mikeš v počátku šíření této fámy udělal zásadní chybu, začal vysvětlovat, jak je to s jeho údajnou homosexualitou, a snažil se vysvětlit, že se jedná o fámu. Nicméně snahou o svou obhajobu na fámu upozornil stále více lidí. Na téma Mikešova homosexualita začali žertovat i jeho kolegové, kteří začali spekulovat, kdo by mohl být jeho údajným partnerem... a pak se začali na jeho úkor bavit.

Navíc v rámci sociální sítě Facebook vznikla diskusní skupina, ve které se Mikešova údajná homosexualita intenzivně probíhala a ve které se náhle začaly objevovat nejrůznější fotografie z akcí, kterých se Mikeš zúčastnil. Následně se začalo spekulovat, kdo z osob na fotografiích je Mikešovým údajným partnerem. Dále se začala fakultou šířit mezi studenty – muži - informace, že kdo chce u Mikeše udělat zkoušku, musí na ni přijít v růžové košili. Na Mikešovo telefonní číslo začaly z nejrůznějších čísel chodit SMSky, ve kterých ho jejich pisatelé uráželi a vyhrožovali mu: *Buzika tu nechceme. Odlet do teplych kraju, ty buzno. Buzerante, jdi si teplit do parku*.

Případ se k Policii ČR nedostal. Celou situací se zabývala etická komise fakulty a její akademický senát. Protože nebyl známý viník, studenti byli plošně důrazně upozorněni na to, že porušují etický kodex chování a že jakékoli konkrétní prohřešky budou trestány a k řešení situace bude přizvána Policie ČR. Facebooková skupina byla uzamčena a následně smazána. Mikeši bylo doporučeno projevy nenávisti ignorovat. Kyberšikana postupně utichla, v tuto chvíli již neprobíhá. Mikeš na fakultě zůstal a chystá se na habilitaci.

9 Edukace budoucích pedagogů

Pokud chceme zvýšit kompetence budoucích pedagogů v oblasti řešení rizikových komunikačních jevů spojených s ICT, je nutné integrovat do vysokoškolské přípravy témata spojená s bezpečnějším užíváním internetu a sociálně patologickými fenomény spojenými s ICT. Jako vhodná forma se jeví *kombinace teoretických poznatků s praktickými dovednostmi*, které je možné získat zejména s *přímou prací s ohroženou cílovou skupinou* – v našem případě dětmi.

Znalosti, které budoucí učitelé získají kontaktem s praxí, pak mohou přenášet do svého běžného života a využít je k eliminaci rizik, která se týkají rovněž jich samotných. Další zajímavou metodou je využití *exkurzí a stáží u odborných institucí*, které se na oblasti rizikového chování na internetu zaměřují, případně např. provozují internetovou službu či poskytují internetové připojení. Kontakt s tímto typem praxe dokáže poměrně rychle aktivizovat studenty a motivovat je pro práci s dětmi i dospělými.

Dalším způsobem edukace budoucích pedagogů je *zapojit je aktivně do činnosti poradenských center*, které pomáhají řešit jednotlivé případy spojené s rizikovým chováním na internetu. Prakticky to znamená např. zadávat jim ke zpracování skutečné případy, vést studenty v rámci jejich řešení, naučit je komunikovat s oběťmi, odkazovat je na krizové linky apod. Na Pedagogické fakultě Univerzity Palackého v Olomouci tuto úlohu plní Online poradna Centra prevence rizikové virtuální komunikace, která ročně zpracuje přibližně 150 případů zneužití ICT k útokům na jiné osoby. Poradna je k dispozici na www.napisnam.cz.

Zajímavou alternativu představuje rovněž *využití potenciálu multiuživatelských virtuálních prostředí* a realizovat vzdělávací akce pro budoucí pedagogy v prostředí tzv. virtuálních světů, např. světa Second Life. Second Life je multiuživatelské virtuální 3D prostředí, které však není v České republice příliš rozšířené, navštěvují jej maximálně

desítky tisíc českých uživatelů. Přesto však představuje zajímavou možnost, jak si témata rizikového chování v prostředí internetu přiblížit právě pomocí této netradiční e-learningové formy. Záznamy přednášek a seminářů ze Second Life je pak snadné umístit např. do prostředí YouTube a poskytnout tak možnost vzdělávat se velkému počtu internetových uživatelů. Lekce realizované v Second Life můžete sledovat prostřednictvím portálu E-Bezpečí (www.e-bezpeci.cz).

(Ukázka z lekce o kyberšikaně a sextingu z prostředí Second Life)

Pro podporu vzdělávání budoucích pedagogů je samozřejmě možné využít i *tradičnějších e-learningových forem studia*, zejména v prostředí univerzit velmi rozšířené formy e-learningu realizovaného prostřednictvím systémů pro řízení vzdělávání, tzv. LMS (learning management system). Na Pedagogické fakultě UP v Olomouci je v rámci e-learningu realizováno hned několik kurzů zaměřených na sociálně-patologické jevy spojené s internetovým prostředím.

Na řadě institucí je edukace žáků, studentů či pedagogů zajištěna rovněž nejrůznějšími grantovými projekty. Na Pedagogické fakultě Univerzity Palackého v Olomouci náš tým realizuje např. projekt *E-Synergie - vědeckovýzkumná síť pro rizika elektronické komunikace,* který je dotován z prostředků ESF OP VK (CZ.1.07/2.4.00/17.0062). Cílem projektu je vytvořit funkční vědeckovýzkumnou síť, propojující vzdělávací, výzkumné a podnikatelské organizace zaměřující se na oblast rizikové virtuální komunikace v kyberprostoru a související kyberkriminalitu. Síť funkčně propojuje jak oblast teoretickou (výzkum, teoretické ukotvení problematiky, psychologické a právní aspekty rizikových komunikačních fenoménů), tak i oblast praktickou (vzdělávání, intervence, trestně-právní řešení problematiky, implementace znalostí do komerční sféry). Projekt E-Synergie jako jeden z prvních integruje oblast bezpečnějšího chování na internetu do systému edukace budoucích učitelů, podílí se tak na výchově a vzdělávání nové generace informačně gramotných učitelů schopných řešit problémové situace přímo na úrovni škol. Na projektu E-Synergie s Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci dále spolupracuje tým Ministerstva vnitra ČR (odbor prevence kriminality), Krajské ředitelství policie Olomouckého kraje, firmy Vodafone Czech Republic, a. s., Seznam a. s. a Google Czech Republic, s. r. o. Více o projektu naleznete na webu www.esynergie.cz.

9.1 Několik postřehů z edukace budoucích pedagogů

K tomu, aby byla edukace v univerzitním prostředí úspěšná, je třeba dodržet několik důležitých pravidel a postupů a samozřejmě respektovat didaktické zásady, definované v řadě odborných publikací (Kalhous, Obst, 2009 a dále). Pro potřeby tohoto textu se pokusím tyto zásady zjednodušit a přizpůsobit tématu této práce.

Kvalitní motivace je základem úspěšné edukace

Aby bylo vzdělávání budoucích pedagogů úspěšné, musí být studenti vhodně motivováni. Motivace vysokoškolských studentů je v řadě případů většinou ryze pragmatická – za absolvování příslušných přednášek či seminářů student získává kredity. Primárně by však motivace měla vycházet z touhy studentů poznávat dosud nepoznané, získat důležité informace, které mohou využít v reálném životě, které se jich osobně týkají a ovlivňují jejich život. Proto v rámci edukace realizované týmem Centra PRVoK a projektu E-Bezpečí kombinujeme v rámci učitelské přípravy jak „pragmatickou" formu edukace (v rámci které jsou studenti odměněni kredity), tak dobrovolnou formu edukace, představovanou výběrovými přednáškami a semináři bez kreditového ohodnocení.

Teorie a praxe musí tvořit funkční celek

Teorie a praxe, která je studentům představována v rámci vzdělávacích aktivit, musí být vždy propojena ve funkční celek. Ideální je zachovat mezi těmito dvěma složkami rovnováhu, případně obě složky synergicky propojit v jednotný celek. V případě, že dojde k nerovnováze, pak se stane edukace méně efektivní. Např. pokud se zaměříme na výklad forem kyberšikany a každou z forem nedoprovodíme konkrétním případem z praxe, pak se sníží efektivita procesu přenosu poznatků směrem ke studentům. Ke stejnému jevu však dojde i tehdy, pokud teorie absentuje zcela a pedagog se omezuje pouze na ukázky případů, které však nedává do potřebných souvislostí, tedy nedochází k tzv. teoretickému ukotvení poznatků.

Získané poznatky musí být využitelné v praxi

Poznatky, které budoucím pedagogům předáváme, by měly být co nejvíce uplatnitelné v praxi. Např. prezentujeme-li jim výsledky výzkumů zaměřených na výskyt kyberšikany u vysokoškoláků, zároveň jim vysvětlíme, se kterými jevy se setkají v praxi nejvíce, které jevy jsou naopak marginální, k čemu tedy v praxi data využít pro minimalizaci těchto jevů v populaci, jaké nástroje lze použít apod. Popisujeme-li studentům např. strategie manipulace obětí sexuálními útočníky, zároveň jim nabízíme obranné prostředky pro rozpoznání či zastavení těchto typů útoku. Student tedy musí v každém okamžiku vědět, k čemu informace, které mu pedagog předává, může využít.

Edukace musí obsahovat prožitek

Chceme-li maximalizovat edukační efekt, je vhodné prezentovat informace tak, aby je student mohl zpracovat prožitkově, s pomocí emocí. Toho lze dosáhnout například tím, že studenta aktivně zapojíme do řešení konkrétního případu, dáme mu k dispozici důkazní materiál, fotodokumentaci k případu, výpovědi pachatelů a další informace, které v něm prožitek mohou probudit či podpořit. Využití prožitku v rámci tzv. zážitkové pedagogiky je velmi efektivní cesta maximalizace procesu vzdělávání.

Příkladem tohoto přístupu je *zážitkový způsob řešení etických dilemat*, který si naši studenti vyzkoušeli např. na odborných stážích a exkurzích realizovaných v rámci projektu E-Synergie u firmy Seznam.cz. Jejich úkolem bylo vyřešit etické dilema v příběhu O princezně, kterou sežral drak (celý příběh je dostupný na www.esynergie.cz). V průběhu procesu se studenti velmi aktivně zapojili do řešení vzniklého etického problému a obhajovali svá stanoviska, argumentovali, využívali kompromisu, v řadě způsobů využili asertivních ale také afektivních přístupů k řešení atd. Je zjevné, že zážitkový způsob vzdělávání je

velmi zajímavý, efektivní, ale také v řadě situací poměrně náročný na přípravu.

Studenti pedagogické fakulty v tréninku u Seznam.cz

10 Závěr

Oblast nebezpečných komunikačních jevů spojených s elektronickou komunikací je velmi důležité a závažné téma, které se týká téměř každého uživatele internetu. Je tedy důležité v této oblasti aktivně preventivně působit a přenášet znalosti získané např. prostřednictvím výzkumu do praxe a poučit se ze zkušeností získaných v procesu vzdělávání.

Cílem této publikace je upozornit na výskyt rizikových komunikačních jevů v populaci vysokoškolských studentů a srovnat jej s výskytem sociálně-patologických jevů u dětí. Zároveň nabídnout možnosti ovlivnit tato zjištění zejména cílenou edukací a preventivním působením na studenty, budoucí pedagogy.

Věřím, že Vám tato publikace poskytla řadu informací, které budete moci přenášet do své vlastní edukační a preventivní činnosti.

Kamil Kopecký
autor

11 Seznam použitých zdrojů

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 O autorovi

Mgr. Kamil Kopecký, Ph.D.

Vedoucí projektu E-Bezpečí, vedoucí Centra prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci, koordinátor projektu E-Bezpečí pro učitele, koordinátor projektu E-Synergie – vědeckovýzkumná síť pro rizika elektronické komunikace, vedoucí Online poradny E-Bezpečí. Expert bezpečnostního výzkumu, vývoje a inovací Ministerstva vnitra, garant Metodického portálu Výzkumného ústavu pedagogického Praha – modul Bezpečný internet.

Ve své pedagogické činnosti se zabývá mediální výchovou a riziky masmédií, dále komunikačními a informačními systémy, moderními trendy v elektronické komunikaci a rizikovou komunikací ve virtuálním prostředí. Aktivně se zapojuje do množství grantových projektů orientovaných na oblasti rizikového chování ve virtuálních prostředích, krizové intervence, počítačové kriminality a bezpečnostního výzkumu (kyberšikana, kybergrooming, sexting, stalking, kyberstalking, sociální sítě, ochrana osobních údajů). Je autorem řady odborných statí pojednávajících o problematice rizikového chování dětí v prostředí internetu a mobilních telefonů, o krizové intervenci, počítačové kriminalitě a bezpečnostním výzkumu.

Úzce spolupracuje s Policií ČR (konzultant v oblasti případů internetové kriminality), firmami Google, Seznam.cz a Vodafone.

Další informace o autorovi naleznete na:
www.e-bezpeci.cz, www.prvok.upol.cz, www.sexting.cz,
www.e-nebezpeci.cz.

13 Seznam grafů

14 Rejstřík

15 Anotace

Monografie Rizikové chování studentů Pedagogické fakulty Univerzity Palackého v prostředí internetu se zaměřuje na komplexní charakteristiku jednotlivých forem rizikového chování vysokoškolských studentů, přičemž se zaměřuje na jevy, se kterými se studenti bezprostředně setkávají.

Shrnuje výsledky výzkumu zaměřeného na fenomén kyberšikany, přičemž sleduje její výskyt napříč základními formami kyberšikany. Dále se zaměřuje na oblast kybergroomingu, sleduje způsoby komunikace a následné manipulace studentů, monitoruje přítomnost výzev k osobním schůzkám s neznámými uživateli internetu a reakci studentů na tento podnět. Monografie se také zaměřuje na fenomén sextingu, na jeho penetraci do populace studentů, na konkrétní případy sextingu a na trestněprávní rovinu tohoto chování.

Další kapitoly se zaměřují na sociální sítě ve vztahu ke studentům, na osobní údaje, které v prostředí sociálních sítí s ostatními uživateli sdílejí, a také na hesla, která si studenti k přístupu do svých internetových služeb volí. Samostatnou část monografie doplňuje analýza hesel, která si studenti pro přístup do svých účtů volí. Hesla jsou charakterizována vzhledem k formě, obsahu a také způsobu využití.

Monografie dále sleduje vybrané světové případy výskytu rizikového chování v prostředí internetu a také se zaměřuje na kauzy kyberšikany vysokoškolských učitelů.

Závěrečná část monografie je věnována různým možnostem edukace a prevence v této oblasti, na vybrané formy a metody, kterými lze podpořit bezpečnější používání internetu u této cílové skupiny.

Klíčová slova:
kyberšikana, kybergrooming, sexting, sociální inženýrství, sociální sítě, rizika internetové komunikace

16 Summary

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

KATALOGIZACE V KNIZE - NÁRODNÍ KNIHOVNA ČR

Kopecký, Kamil
Rizikové chování studentů Pedagogické fakulty Univerzity Palackého v Olomouci v prostředí internetu / Kamil Kopecký. – 1. vyd. – Olomouc : Univerzita Palackého v Olomouci, 2013. – 110 s. – (Monografie)
Anglické resumé
Nad názvem: Univerzita Palackého v Olomouci, Pedagogická fakulta, Centrum prevence rizikové virtuální komunikace. – Pub. je určena pro odbornou veřejnost
ISBN 978-80-244-3858-0

316.772:004.738.5 * 316.624 * 364.636:004 * 378.096:37.01 * 378.011.3-052 * 316:303 * (437.325)
– Univerzita Palackého. Pedagogická fakulta
– 2012–2013
– internetová komunikace
– rizikové chování
– kyberšikana
– kyberšikana – Česko
– pedagogické fakulty – Česko
– vysokoškolští studenti – Česko
– sociologický výzkum – Česko – 2011–2020
– Olomouc (Česko)
– monografie

364 – Sociální problémy vyžadující podporu a pomoc. Sociální zabezpečení [18]

Mgr. Kamil Kopecký, Ph.D.

RIZIKOVÉ CHOVÁNÍ STUDENTŮ PEDAGOGICKÉ FAKULTY UNIVERZITY PALACKÉHO V OLOMOUCI V PROSTŘEDÍ INTERNETU

Publikace je určena pro odbornou veřejnost

Výkonný redaktor doc. Mgr. Miroslav Dopita, Ph.D.
Odpovědná redaktorka Jarmila Kopečková
Technický redaktor Mgr. Kamil Kopecký, Ph.D.
Návrh a úprava obálky Mgr. Kamil Kopecký, Ph.D., & Fotolia

Publikace ve vydavatelství neprošla redakční úpravou.

Vydala a vytiskla Univerzita Palackého v Olomouci
Křížkovského 8, 771 47 Olomouc
www.vydavatelstvi.upol.cz
e-mail: vup@upol.cz
www.e-shop.upol.cz

1. vydání

Olomouc 2013

Ediční řada – Monografie

ISBN 978-80-244-3858-0
ISBN 978-80-244-3903-7

Neprodejná publikace

Více informací o projektu naleznete na www.esynergie.cz
a na www.e-bezpeci.cz

VUP 2013/779

Univerzita Palackého v Olomouci, Pedagogická fakulta
Centrum prevence rizikové virtuální komunikace
2013

Publikace byla realizována v rámci projektu
E-SYNERGIE - vědeckovýzkumná síť pro rizika elektronické komunikace
(CZ.1.07/2.4.00/17.0062).
Více informací o projektu naleznete na www.esynergie.cz.