UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
FAKULTA HUMANITNÍCH STUDIÍ
Institut mezioborových studií Brno

Preventivní bezpečnostní programy v rámci internetové sítě

BAKALÁŘSKÁ PRÁCE

Vedoucí bakalářské práce:
doc. Ing. Antonín Řehoř, CSc.

Vypracoval:
Monika Pelcová

Brno 2012

Prohlášení

Prohlašuji, že jsem bakalářskou práci na téma „Preventivní bezpečností programy v rámci internetové sítě“ zpracovala samostatně a použila jsem literaturu uvedenou v seznamu použitých pramenů a literatury, který je součástí této bakalářské práce.
Elektronická a tištěná verze bakalářské práce jsou totožné.

V Brně dne 24. 4. 2012 …….

Podpis

Poděkování

Děkuji panu doc. Ing. Antonínu Řehořovi, CSc., za velmi užitečnou metodickou pomoc, kterou mi poskytl při zpracování mé bakalářské práce.

Také bych chtěla poděkovat svému příteli Filipovi, kamarádce Radce a naší malé žabce Barušce za morální podporu a pomoc, kterou mi poskytli při zpracování mé bakalářské práce, a které si nesmírně vážím.

Monika Pelcová

OBSAH

Úvod

Internet a jeho užívání se stalo fenoménem dnešní doby a kdo nemá mezi určitou věkovou skupinou uživatelů alespoň jeden účet v sociální síti, není takzvaně „in“. Na druhou stranu pro mnoho lidí je jeho využívání nepostradatelnou součástí dne ať již osobního nebo pracovního charakteru. Pravdou zůstává také fakt, že pro mnohé uživatele je cestou k obživě a výdělku. Bohužel užívání Internetu je z velké části anonymní a tento fakt skrývá také různé nástrahy pro jeho uživatele, především začátečníky nebo méně znalé těchto nástrah. Uživatelé jsou různých věkových skupin a míra uživatelských dovedností, znalostí, ostražitosti a třeba i určité naivity je velmi rozdílná.

O budoucnosti internetové sítě a sdílení soukromých dat s nadsázkou píše sloupkař Miloš Čermák: *„Dřív nebo později bude běžné, že do Googlu místo textového dotazu pošlete fotografii - a vyhledávač vám zjistí všechno o lidech, kteří na ní jsou. Od toho už je jen kousek ke speciálním googlovským brýlím. Nasadíte si je na ulici … a nad každým člověkem, kterého potkáte, bude „obláček“ s informacemi. Uvidíte pohlednou dívku a budete číst: „Z maturity čtyřka z češtiny, dvakrát zasnoubená, jedno erotické video na YouTube, neplatí televizní poplatky, vysokou školu nedokončila.“ Ježišimarjá, řeknete si, rychle pryč. Ale pak si uvědomíte, co v obláčku nad sebou máte vy sami.“*[1]

Můžeme se aktivně podílet na rozvoji uživatelských vědomostí? Je možno chránit sebe a své soukromí před těmi, kteří rádi tato soukromí, bez ohledu na své pohnutky, odkrývají a zneužívají pro sebe nebo třetí stranu? Mají uživatelé internetu i přes různorodost věkového zastoupení povědomí o těchto možnostech a pokud ano, jaké jsou to možnosti a jak a kde získat tyto informace? Podobné otázky si můžeme klást nejen ve vlastním zájmu. Malé nahlédnutí do světa ne/bezpečnosti Internetu a zodpovězení několika zmíněných otázek je cílem mojí bakalářské práce.

Poslední dobou se v rámci různých finančně podporovaných projektů situace na poli informovanosti a vzdělávání v oblasti rizik online komunikace razantně mění. Existují různé preventivní bezpečnostní programy, ať již v rovině vzdělávací nebo informační, a ráda bych provedla jejich výčet a popis.

---

[1] ČERMÁK, M. *Nikomu to neříkejte!, (aneb, Proč píšu Internet s velkým písmenem na začátku)*. 1. vyd. Praha: Extra Média, 2008, s. 169. ISBN 978-80-903994-6-4.

Já osobně jsem aktivní nadšenec užívání Internetu a proto mne toto téma lákalo ke zpracování. Zároveň jsem čerstvě matkou dítěte, čímž se zvýšil můj zájem o vytvoření přehledu a získání zmiňovaných informací, které mohou být v budoucnu užitečné nejen při vzdělávání a výchově odborníkům z řad pedagogiky a školství, ale především také rodičům. Neboť právě rodiče jsou osoby mající výrazný podíl vlivu na trávení volného času vlastních dětí.

„Používání počítačů a na nich postavených nových komunikačních médií představuje bezesporu novou kulturní techniku. Avšak její hodnotu vzhledem k již existujícím kulturním technikám musíme velmi dobře uvážit. Východiskem všech úvah, právě s ohledem na technické inovace, musí být člověk. Technika má sloužit jednotlivému člověku i lidskému společenství a napomáhat možnostem jednotlivce, a tím i všech lidí. Jen to je pak technika humánní.“[2]

První část bakalářské práce popisuje stručně historii Internetu a vysvětluje několik základních pojmů virtuálního světa. Zároveň se také věnuje pojmům především sociálně-patologických jevů, které ohrožují uživatele internetové komunikace.

Druhá část bakalářské práce je podrobnou analýzou současného stavu zmiňovaných preventivně bezpečnostních programů v rámci internetové sítě. Mezi tyto programy jsou zahrnuty různé projekty a kampaně věnující se informování a vzdělávání odborníků a široké veřejnosti před rizikovými jevy, které se při online komunikaci objevují.

Třetí, empirická část bakalářské práce se zaměřuje na rodiče, kdy dotazníkovým výzkumem zjišťuji aktuální stav rozsahu jejich informovanosti o eventuálních rizicích online komunikace a především o možnostech vzdělávání.

[2] BUERMANN, U. *Jak (pře)žít s médii*: *příležitosti a hrozby informačního věku a nové úkoly pedagogiky*. Vyd. 1. Hranice: Fabula, 2009, s. 194-195. ISBN 9-788086-600581.

1. Internet a základní pojmy

Tato kapitola je věnována stručnému popisu historie Internetu nejen v zahraničí, ale i v České republice. Dále se seznámíme s trendy moderního virtuálního světa jako jsou, sociální sítě a komunikační programy. Představené virtuální prostředí Second Life zaujme možnostmi využití v praxi.

1.1 Historie Internetu

Rozvoj Internetu

V Sovětském svazu byla v roce 1957 vyvinuta první družice, která obíhala Zemi. Nesla název Sputnik. Reakcí na tuto skutečnost bylo v roce 1958 založení agentury s názvem ARPA, jenž měla za cíl udržení technologického pokroku neboli náskoku ozbrojených sil USA před ostatními. Tato agentura je organizací zřízenou americkým ministerstvem obrany a věnuje se především, v rámci svého již výše zmiňovaného cíle, vývoji nových vojenských technologií při krátkodobých projektech.

Počítačová experimentální síť ARPANET byla financována a vybudována v roce 1969 agenturou ARPA a je považována za to, co dnes označujeme pojmem Internet. Jejím cílem bylo umožnění vzdáleného přístupu k nejvýkonnějším počítačům tehdejší doby a měla fungovat bez cílové složky, tedy i tehdy, pokud by byla její část zničena. Jejím základem se postupně staly univerzitní počítače UCLA (University of California Los Angeles), SRI (Stanford Research Institute), UCSB (University of California Santa Barbara) a University of Utah.

První pokus o propojení sítě mezi počítačem SRI a UCLA proběhl na základě protokolu NCP (Network Control Protocol) roku 1969. Síť se postupně rozrůstala po celé USA a do Evropy se elektronická komunikace rozšířila přes Norsku a Spojené království v roce 1973.

V roce 1983 byl po oddělení počítačové sítě armády USA MILNET již využíván protokol TCP/IP (Transmission Control Protocol/Internet Protocol, hlavní komunikační protokol, který je souborem pravidel určující například význam jednotlivých zpráv při komunikaci v celosvětové počítačové síti) a na jaře roku 1990 byl projekt ARPANET ukončen.

Zatímco v roce 1984 využívalo připojení k Internetu jen 1000 počítačů, v roce 1992 to bylo již více než jeden milion.[3]

Myšlenka hypertextu, tedy způsob strukturace textu s obsahem odkazů, je různými zdroji datována k rokům 1945, 1965 a později k roku 1980, kde měl tento způsob usnadnit ve švýcarském institutu CERN sdílení a aktualizaci mezi zaměstnanci institutu. V roce 1991 byly spuštěny první webové stránky, první browser (webový prohlížeč) s názvem World Wide Web, nejznámější systém hypertextu.

Rok 1993 byl velkou expanzí Internetu v USA a v roce 1995 bylo připojeno již přes dva milióny počítačů. Na celém světě v roce 1995 bylo počítáno na dvacet miliónů uživatelů Internetu a v roce 2000 více než 300 miliónů.

Jak bývá často uvedeno, nastává na planetě Zemi doba internetová. Zároveň se také objevují závislosti na Internetu a možná nebezpečí sociálně-patologických fenoménů online komunikace.

Internet je globálním systémem vzájemně propojených počítačových sítí, které umožňují vzájemnou komunikaci mezi počítači. Jeho nejrozšířenější aplikací je WWW neboli web, přirovnávaná k celosvětové pavučině, systému propojených hypertextových dokumentů. Služba, která je kombinací textu, grafiky, audiovizuálních technických prostředků, vzájemně propojenými textovými odkazy.

Další velmi rozšířenou aplikací Internetu je například e-mail neboli elektronická pošta, VoIP (Voice over Internet Protocol) telefonování pomocí Internetu, IM (Instant messaging), online komunikace mezi uživateli, například ICQ, Jabber, Skype, Miranda, Trillian, Google Talk a FTP (File Transfer Protocol) přenos souborů.

Dále také dnes stále oblíbenější sociální sítě různých zaměření, například Facebook, Google+, Lidé.cz, MySpace, Twitter a další. Každý k Internetu připojený počítač má svoji takzvanou IP adresu (Internet Protocol), tedy protokol, který je podstatou komunikace všech zařízení Internetu.

[3] VRABEC, V. Co bylo, než vznikl český Internet?: Historie Internetu. *Lupa.cz* [online]. 13. 8. 2002 [cit. 2012-03-12]. Dostupné z: http://www.lupa.cz/clanky/co-bylo-nez-vznikl-cesky-internet/

Rozvoj Internetu v ČR

Sedmdesátá léta minulého století dávala českým vysokoškolským studentům možnost učit se používat výpočetní techniku v podobě sálových počítačů pracujících v dávkovém režimu, kdy bylo potřeba úkol předem připravit na děrné pásce nebo štítcích, předat do výpočetního střediska a po určité době si vytištěný výsledek vyzvednout.

Větším průlomem byl rok 1976 instalací britského systému ICL-4-72 na ČVUT, UK, VŠE a v Ústavu školských informací. Propojení počítačů a terminálů dálnopisného typu telefonními linkami, které byly umístěny na českých vysokých školách nejen v Praze, bylo nejvýkonnějším výpočetním systémem tehdejší doby.[4]

Díky politické situaci v České republice se internetová historie počíná v polistopadovém období. Kromě prolomení politických bariér bylo potřeba překonat i nedostatečné technické podmínky. V květnu roku 1990 se zde objevuje síť EUnet, v říjnu pak EARN a v listopadu roku 1991 proběhly první pokusy s připojením k Internetu. Formální slavnostní připojení Československa k Internetu proběhlo v Praze na ČVUT 13. února 1992. První sítí byl FESNET a po rozpadu federace CESNET.

Původním cílem Internetu bylo propojení akademického zázemí, ale později se rozšířil mezi soukromou a také veřejnou sféru. Největší rozmach Internetu potom probíhá od roku 1995, dále pak v letech 1998, 2000 a jeho podoba oproti dnešnímu je již nostalgií.[5]

„Člověk je tvor sociální. Svoje psychické potřeby naplňuje v mnoha ohledech prostřednictvím vztahu s druhými lidmi. Komunikace hraje v tomto procesu klíčovou roli, ať už ve své verbální nebo neverbální podobě.…Internet se stal novým komunikačním prostředím, na jehož základně dochází k sociální interakci a které slouží k mezilidské komunikaci - v dyádě, skupině či masově.“[6]

---

[4] PETERKA, J. Internet u nás: Internet. *EArchiv.cz* [online]. 1995 [cit. 2012-03-12]. Dostupné z: http://www.earchiv.cz/a95/a504c504.php3

[5] PETERKA, J. Kolikáté narozeniny slaví Internet?. *Lupa.cz* [online]. 6. 1. 2003 [cit. 2012-03-12]. Dostupné z: www.lupa.cz/clanky/kolikate-narozeniny-slavi-internet

[6] HORSKÁ, B., LÁSKOVÁ A. a PTÁČEK L.. *Internet jako cesta pomoci*: *internetové poradenství pro pomáhající profese*. Vyd. 1. Praha: Sociologické nakladatelství (SLON), 2010, s. 17-19. Studijní texty (Sociologické nakladatelství), sv. 49. ISBN 978-80-7419-034-6.

1.2 Sociální sítě a komunikační programy

Sociální sítě

Sociální síť je v moderním pojetí služba poskytující vytvoření a sdílení osobního, nebo firemního profilu. Uživatelé spolu mohou navzájem nejen komunikovat a sdílet různé soubory, ale i hledat či nabízet zaměstnání, číst a psát články, odborné texty, vytvářet rodokmen, studovat různé žebříčky a statistiky, hodnotit koncerty, festivaly a jiné kulturní akce, plánovat akce a srazy nebo například sledovat intimní aktivity uživatelů. Tyto možnosti jsou pak rozdílné v závislosti na jejich zaměření.

Po celém světě existují servery – portály sociálních sítí rozšířené buď globálně nebo úzce zaměřené na kontinent, státy, koníčky, profese a další členění. Jedná se o fenomén posledních let na Internetu, uživatelé těchto sítí musí být většinou registrovaní, aby ji mohli používat v plném rozsahu.[7]

Facebook je sociální sítí, kterou dnes využívají již celé generace a slouží ke komunikaci mezi lidmi, přenosu souborů jako jsou fotky, videa a například i ke hraní her. Původně byla sítí studentů Harvardské univerzity.

V současné době je registrováno v této síti již přes 800 miliónů soukromých profilů – záměrně se nebavíme o soukromých osobách, protože Facebook umožňuje, jako spousta jiných on-line služeb, registraci na e-mailovou adresu a zbytek údajů si člověk může upravit dle svého uvážení a již nejsou ověřitelné.

Proč je Facebook tolik lákavý pro zakládání falešných profilů? Protože je největší a zcela zdarma, pokud mluvíme o základních funkcích. Díky masivní návštěvnosti se podařilo firmě vlastnící Facebook rozjet mnoho rozličných funkcí a dalších aplikací, přizpůsobení prostředí programátorům třetích stran, které umožňují tvorbu her, soutěží, kvizů a mnoho dalších komerčních i privátních služeb. Bohužel s tím souvisí i nekalá činnost osob nebo uskupení jedinců s cílem poškození, nebo vylákání dat z nic netušících fanoušků (osoba, která v rámci svého profilu schválila a podporuje konkrétní výrobek, myšlenku, názor nebo službu).

Obecně má Facebook problémy se zajištěním dat svých uživatelů, neboť technologicky je prostředí natolik náročné na provázaní dat, navíc definice ochrany osobních údajů dává většinu trumfů do rukou provozovatele.

[7] Sociální sítě. *Socialnisite.123abc.cz* [online]. 2011 [cit. 2012-03-12]. Dostupné z: http://www.socialnisite.123abc.cz

Vrátíme se k falešným profilům – ty představují na Facebooku jedno z největších rizik pro děti a dospívající mládež. Systém umožňuje registraci uživatele vázaného na unikátní znění e-mailové adresy, kterou si můžeme pořídit, kolikrát chceme. Dalším krokem je vytvoření falešného profilu, který se celkově tváří uživateli, ale spíše uživatelce, jako dokonalé ztvárnění jejích představ o protějším virtuálním příteli. Nebo snad nepříteli?

Prenatální profil není sám o sobě sociální sítí, ale je její součástí. Tento jev se objevil v nedávné době, kdy se na sociální síti Facebook začaly objevovat vznikající profily dosud nenarozených miminek. Maminky tyto profily zakládaly zajisté v dobré víře a radosti z tak veselého očekávání, ale neuvědomily si, že tím porušují několik pravidel bezpečného užívání Internetu současně. Na tento profil vkládaly maminky fotky nejprve nenarozeného a později již narozeného miminka.

Následně sdělovaly zároveň citlivé osobní a zdravotní údaje již narozeného dítěte a také především samotné založení toho uživatelského účtu probíhá jednak bez souhlasu dotčené osoby a zároveň je porušením pravidel sociální sítě Facebook, tedy založení účtu uživatelem před dovršením 13 let. Tyto profily jsou proto administrátorem mazány.

Google+ je sociální síť veřejnosti zpřístupněná v loňském roce, spadající do projektů největší internetové firmy na světě Google se sídlem v USA. Tato síť má podobný model využití a cílových skupin jako Facebook a bývá považována za konkurenci. Oproti Facebooku má více jak patnáctkrát méně registrovaných uživatelů a obecně je vnímána jako serióznější sociální sít především pro větší podíl firemních a serióznějších obsahů.

MySpace je sociální síť sloužící především ke sdílení hudby a videa, mnohdy její služby využívají jak profesionální umělci, tak amatérské hudební skupiny, jednotliví interpreti a různí umělečtí perfomeři.

Twitter je sociální síť, kterou využívají uživatelé píšící blogy, tedy příspěvky, kde píší svoje myšlenky a informace. Je využíván i z řad mediálních osob nebo odborníků, například IT technologií.

LinkedIn je sociální sítí v oblasti profesní profesionální prezentace a personalistiky, její služby využívají nejen zaměstnanci a zaměstnavatelé, ale i personalisté a personální agentury. Pokud uživatel ve svém profilu zvolí možnost, může získat i pracovní nabídku. Síť funguje celosvětově, nedávno byla lokalizována i do českého jazyka.

Mezi další světově proslulé sociální sítě různých zájmů, rozdílných věkových skupin uživatelů a regionálních lokalit jsou například **Last.fm** – zaměřena na hudební fanoušky, **Bebo** – síť podporující blogování uživatelů, **Classmates** – mezinárodní síť určená pro sdílení s bývalými nebo stávajícími spolužáky, **Friendster** – síť zaměřená na hraní her, **Hi5** – další síť propojující setkávání uživatelů a hraní her, **Songkick** – síť zaměřená na sdílení zájmů o kultuře, **Blackplanet** – síť zaměřená na afroamerickou populaci a nespočet dalších platforem, které vznikají, působí a mění se v rámci celosvětového Internetu každým okamžikem.

Na poli českého Internetu vznikly také rozsáhlé projekty sdružující a socializující velké množství internetových uživatelů.

Lidé.cz patří do skupiny projektů největší české internetové firmy Seznam.cz, a.s. Jedná se o české komunitní fórum, kde mohou uživatelé chatovat, psát blogy, sdílet soubory, seznamovat se a zároveň je uživatelsky propojen s následující sítí. V současné době již dlouhodobě klesá návštěvnost.

Spolužáci.cz, opět patřící pod firmu Seznam.cz, a.s., jsou českou sociální sítí se stejnými možnostmi jako předchozí, navíc zde uživatelé sdružuje prostor pro spolužáky ať již současné nebo bývalé.

Líbímseti.cz patřilo mezi nejoblíbenější české seznamovací portály, web obsahuje i interaktivní sekci, jako je chat v reálném čase a mnoho dalších komunikačních nástrojů pro sdílení názorů, textů, multimédií mezi uživateli. Je znám a populární především u mládeže.

Jagg.cz je neobvyklý projekt, umožňující sdílení hyperlinků – odkazů na jiné webové stránky pro další uživatele jako potenciálně přínosný.

Zmíněn byl velký výčet světových sítí a diskuzních stránek, podobně velký seznam lze vytvořit i v případě českého Internetu jako jsou česká fóra: **Ukazse.cz**, **Stesti.cz**, **Forum.lide.cz**, **Superforum.cz**, **Rodina.cz** a mnohá další.

Specifickou skupinou z hlediska zneužití důvěry uživatelů nebo jejich dat jsou komunitní – sociální platformy zaměřené na děti, například **Emimino.cz**, **Modrykonik.cz**, **Babyweb.cz** a další. Důvod je prostý – velmi často se stává, a maminky jsou na podobné situace upozorňovány, že jsou vystavovány fotky nemluvňat. Maminky to obvykle myslí dobře, ale již byly objeveny případy, kdy se cíleně infiltrovaly do skupin maminek i lidé, kteří neměli ty nejlepší úmysly – jejich cílem bylo získávání takových fotek, kde je například odhalena většina tělíčka, případně i genitálie. Tito lidé nemusejí nutně trpět formou sexuální deviace, tedy pedofilie, ale mají z toho profit v podobě sestavování fotografických bookletů, které potom prodávají na černém trhu buď organizovaným skupinám pedofilů, nebo samotným jednotlivcům.

Stejný problém hrozí u jakékoliv služby na Internetu, která umožňuje zveřejňování multimédií soukromých osob. Může se jednat i o zabezpečenou službu, kdy pachatelé používají hackerských technik, nebo metod sociálního inženýrství. Mezi takové služby obecně patří specializované portály na zveřejňování fotografií nebo videí, např. **Flickr.com**, **Picasso.com**, **Youtube.com** nebo české projekty **Stream.cz** a **Rajce.net** a mnoho dalších.

Komunikační programy

Specifickou skupinou jsou tzv. instantní komunikační programy, anglicky označované jako Instant messaging. Postupně vznikly celosvětově známé programy, jako je **ICQ**, **MSN Messenger**, **IBM Lotus SameTime** pro firemní použití, nebo aplikace chatovacích klientů například **Jabber**, **Trillian**, **Miranda**, nebo **Meebo**, dnes je to již i Facebook a další sociální sítě s integrovanými messengery, které umí používat až desítky rozličných komunikačních rozhraní a odlišných technologií na přenos nejen zvuku, ale také videa, případně souborů.

Dále také sdružují databázi kontaktů, podle kterých si může uživatel najít dle vlastních preferencí přátele z druhé strany planety. Rozhodně je to jedna z výhod těchto komunikačních nástrojů a Internetu vůbec.

Čím je populární tento způsob komunikace? Probíhá přes Internet v reálném čase, dnes i v mobilní podobě jako aplikace v chytrých telefonech, a tím se odlišuje například od telefonní, nebo e-mailové komunikace. Účastníci mohou vidět dopředu, zdali je protější uživatel přihlášený do aplikace, a tím dává najevo, že je ochoten ihned komunikovat.

Obecně mezi mládeží a dětmi je tento nástroj velmi populární, neboť nabízí rychlou a velmi levnou alternativu oproti klasickému telefonnímu volání, navíc může vést hovor více osob najednou, což se využívá například při hraní počítačových her po síti. Bohužel tyto technologie jsou stejně tak dobře zneužitelné.

Byly zaznamenány pravidelné hromadné útoky počítačových hackerů právě přes chatovací služby, velmi často se stává, že koncový uživatel ani netuší, že právě otevírá soubor nebo odkaz na webové stránky, kde se nachází druh počítačového viru, nebo dalšího škodlivého softwaru.[8]

V kontextu zaměření této práce je zde ještě jedna velká skupina představující nebezpečí. Tím je zneužití chatování ve prospěch strany, která skrývá svou identitu a vydává se za někoho jiného. Obvykle se můžeme setkat s projevy kyberstalkingu v různých podobách. Nejobvyklejším případem jsou starší muži, kteří si vyhlídnou nezletilou dívku, anebo také chlapce, a začínají rozjíždět intimní a zároveň anonymní hru na tenkém ledě. Jejich cílem je po několika sezeních u internetového chatování navodit takový pocit důvěrnosti, sympatií a emocí, že oběť – nezletilá dívka či chlapec uvěří, že nalezli někoho, s kým mohou sdílet své starosti, pohled na svět a mohou se někomu na plno svěřit. Pachatel se snaží často získat i kontaktní údaje, případně začíná komunikaci cíleně vést k osobnímu setkání. Zde vzniká skutečné nebezpečí reálného zneužití nic netušící důvěřivé oběti, bohužel se setkáváme i s tragickými následky jako jsou znásilnění nebo vraždy.

[8] FAQ-PC Help: Programy pro internetovou komunikaci. *PC-HELP.cz*: *České diskuzní fórum* [online]. 2006 [cit. 2012-03-12]. Dostupné z: http://www.pc-help.cz/viewtopic.php?f=72&t=6891

1.3 Second Life

Second Life, projekt společnosti Linden Lab z roku 2002, není hra, uživatelé zde vzájemně nesoupeří ani neplní žádné stanovené úkoly. Kreativita uživatelů není omezena. SL je trojrozměrný virtuální svět, jehož obyvatelé (uživatelé) život žijí.

Obyvatelé SL cestují, vzájemně komunikují, navazují nové kontakty, budují hodnoty, vyrábí, mohou obchodovat, staví domy, nakupují, vzdělávají se, chodí na přednášky, baví se v kavárnách a barech, mohou tancovat, sportovat, relaxovat. Lze zde směnit reálné peníze za herní měnu (Linden dolary) a jejich hodnotu třeba i navýšit.

V roce 2007 vzniklo v Second Life československé virtuální město Bohemia, kde se mluví česky nebo slovensky a vyučuje se zde například anglický jazyk.

Pro firmy je SL vnímán jako internet nové generace, mohou zde použít prostor k obchodním jednáním, školením nebo pro schůzky. SL zde zmiňuji záměrně ačkoliv nesouvisí přímo s tématem, nicméně existence SL je spjata s aktivitou Centra PRVoK na webu www.sl.e-bezpeci.cz. Ukázka virtuálního prostoru SL je součástí přílohy č. 3.[9]

[9] RYLICH, J. Second Life – život ve virtuální realitě. *Lupa.cz* [online]. 17. 5. 2007 [cit. 2012-03-12]. Dostupné z: http://www.lupa.cz/clanky/second-life-8211-zivot-ve-virtualni-realite/

2. Rizika virtuální komunikace

Online komunikace překonává hranice a její možnosti nejsou vzdáleností omezeny. Její pozitiva však narušují možná rizika, která uživatele ohrožují a se základními pojmy těchto rizik se nyní seznámíme.

Virtuální svět může být pro některé lidi svoji poutavostí velkou časovou investicí, proto se věnujeme krátce pojmu netholismus, který souvisí se závislostí na Internetu.

2.1 Vybrané pojmy

Ve virtuálním světě se setkáme s mnoha podobami zneužití osobních informací, vedoucích k obtěžování anebo přímo napadení obětí. Obecně můžeme rozdělit pojmy na dvě skupiny.

První skupina pojmů se týká sociálního inženýrství a hackerských útoků s cílem poškodit technologicky nebo finančně předem vyhlédnuté oběti nebo celé množiny obětí. V tomto případě nevzniká bližší pouto mezi obětí a útočníkem, i když tyto metody mohou být také založeny na získání důvěry.

Druhá skupina pojmů se týká činů, které buď přímo nebo nepřímo poškozují oběti psychicky či fyzicky a následky bývají nezřídka dlouhodobé až celoživotní, v některých případech situace vrcholí následkem činu sebevraždou oběti. Vzniká zde většinou citové pouto mezi útočníkem a obětí, např. navázáním kontaktu pod falešnou identitou útočníka.[10]

Netiketa

Skupina doporučení pro slušné chování v síti. Existuje i RFC dokument (základní technický dokument bez právní síly) z roku 1995, který sice nezahrnuje nejnovější vývoje, ale pořád jsou pravidla platná pro vzájemné vztahy mezi uživateli. Například doporučení: adresátem sdílení je člověk a berte na něj ohled.

[10] Nebezpečné komunikační praktiky. *E-bezpeci.cz* [online]. 2010 [cit. 2012-03-12]. Dostupné z: http://cms.e-bezpeci.cz/content/blogcategory/33/54/lang,czech/

Google Bombing

Zneužití jmenovaného internetového vyhledávače k vyhledání webu s určitou frází, přestože ji neobsahuje, a zároveň ji tak posouvá výše v seznamu doporučených odkazů. I když tato aktivita nepůsobí destruktivním dojmem a důvod bývá humorný nebo politický, mohou se obětí stát také děti.

Flaming

Flamingem se rozumí nepřátelské chování uživatelů na Internetu. Může se jednat o urážky , ale i o vyhrožování, většinou v prostředí diskuzních fór.

Trolling

Trollové jsou uživatelé, kteří se snaží v online prostředí záměrnou diskuzí nebo vkládáním nevhodného obsahu vyprovokovat ostatní uživatele k rozhořčení, což může vést až k odklonění původních témat fóra.

Kybernalita

„Kybernetickou kriminalitou, neboli kybernalitou, rozumíme takovou činnost, kterou je porušován zákon nebo je v rozporu s morálními pravidly společnosti. Tato kriminalita může být namířena přímo proti počítačům, jejich hardwaru, softwaru, datům, sítím apod., nebo v ní vystupuje počítač pouze jako nástroj pro páchání trestného činu, případně počítačová síť a k ní připojená zařízení jsou prostředím, v němž se taková činnost odehrává. Obtížnost sledování projevů kybernality spočívá v tom, že se odehrávají v prostředí, jenž je objektivně pouze velmi obtížně vnímatelné. Dění v tomto prostředí můžeme pozorovat pouze pomocí strojů a přístrojů, které nám přístup do kyberprostoru umožní. Útočník, nebo pachatel pracuje v globálním prostředí, může se v kyberprostoru velmi rychle a nepozorovaně pohybovat, měnit identity nebo i mizet. Může vytvářet, předstírat nebo realizovat různé hrozby a vždy bude o krok napřed.“[11]

[11] JIROVSKÝ, V. *Kybernetická kriminalita*: *nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s. 19. ISBN 978-80-247-1561-2.

Spam

Nevyžádaná pošta, obdržená do e-mailové schránky většinou z reklamních důvodů. Zahlcuje místo a uživatel stráví nemálo času jejím promazáváním.

Hoax

Je šíření poplašných, zbytečných a nebezpečných zpráv v rozporu s Netiketou. Mezi nejznámější patří například „Psík - 7 štěňat retrívrů“ nebo „Cibule proti chřipce“.

SMS Spoofing

Je v podstatě nevyžádanou poštou. V tomto případě ale formou sms na mobil, odeslané z webového formuláře. Může mít vtipný obsah, ale také může ohrozit dítě svojí anonymitou, kdyby jej například sms vyzývala k osobní schůzce pod falešnou identitou v domnění, že se jedná o rodinu.

Hacking

Jedná se o porušování zákona s cílem prolomit bezpečnostní ochrany informačních systémů. Počítačové pirátství porušuje soukromí osob nebo jejich majetky. Zároveň ale posouvá vývoj softwaru, protože bývá nejčastěji využíváno při napadení jejich slabých stránek.

Phishing

Tato metoda je používána dnes a denně v oblasti především e-mailové komunikace, kdy se útočníci snaží vylákat z obětí citlivé údaje, jako jsou čísla bankovních kont, údaje k platebním a kreditním kartám. V České republice jsou známy opakované útoky na e-mailové adresy klientů českých bank.

Obdobou phishingu jsou klasické **podvodné e-maily**, často ze zahraničí, případně i exotických destinací, které se zaměřují na běžnou soukromou korespondenci v souvislosti s každodenní rutinou, jako je soukromá inzerce na bazarových portálech a podobných webech. Jedinci zde slibují lámaným „mateřským“ jazykem poslání peněz předem, kdy žádají například zaslání zboží na adresu do zahraničí. Trik spočívá v tom, že podvodník peníze dopředu nepošle, ale zaslané zboží je na cestě a oběť již nemůže ovlivnit ztrátu na své straně.

Pharming

„Pharming je náročnější variantou Phishingu. Internetové prohlížeče si v rámci urychlení práce a spojení vytváří v lokálním (místním=vašem) počítači paměť s navštěvovanými IP adresami. A právě data v této lokální paměti jsou pharmingem upravena - správná IP adresa je upravena na IP adresu škůdce a vy se pak připojujete na nesprávný server, na nesprávnou stránku, vypadající velmi podobně jako ta, na kterou se chcete připojit.“[12]

Sociální inženýrství

Je způsobem manipulace lidí ke stanovenému cíli, například získání nevědomě určité informace, dle rozsahu důvěřivosti poškozeného. Je tak velmi kvalitně využíváno znalostí o lidské povaze. Útočník může s obětí i navázat dlouhodobý kontakt za účelem jejího poznání.

Kyberšikana

Jedná se o různé možnosti a kombinace obtěžování, nejčastěji používané mezi dětmi a mládeží školou povinné. K obtěžování se zneužívá elektronických médií, jako jsou foto a videokamery, e-mail, chat, sociální sítě, falešné a očerňující webové stránky a další možné prostředky. Takové jednání může vést až k páchání trestného činu nebo i více trestných činů najednou. U nezletilé mládeže nastává často problém v situaci, kdy se jedinec takového jednání dopustí, často v rámci z počátku nevinné hry jako zábavy k zahnání nudy.

Nejčastěji se setkáme s natáčením fyzické, psychické a v posledních letech i sexuální šikany. Pachatelé takové činnosti anonymně zveřejní video nebo fotky, případně zvukový záznam na internet v rámci veřejně populárních portálů nebo sociálních sítí. Zaručí tím dosažení svého cíle: co největší počet shlédnutí choulostivého materiálu běžnými uživateli. Tím ještě více podtrhnou provedený zločin nebo přestupek. Následky bývají tragické – nezřídka se pokusí oběť i o sebevraždu.

Takový čin má totiž ničivé dopady na zachování práva o soukromí, které je zcela podlomeno, a oběť má pocit, že se tak již každý člověk dozvěděl o nesnesitelném ponížení, které bylo na oběti spácháno, a oběť se v takovém případě nemá šanci ubránit,

[12] KRÁL, M. *Bezpečnost domácího počítače*: *prakticky a názorně*. 1. vyd. Praha: Grada, 2006, s. 230. ISBN 80-247-1408-6.

pokud není pachatel, nebo celá skupina pachatelů, ihned odhalena a potrestána. I když se oběť nepokusí o sebevraždu, často na ní takový útok zanechá následky v psychice osobnosti. Zde je zapotřebí podpora odborníka psychologa. Poslední dobou se rozšířila i kyberšikana, která je zaměřena na učitele.[13]

Happy Slapping

Je jedna z dalších forem šikany, poměrně nová, poprvé se objevila před 3 lety v Londýně. Útočník si vybere náhodnou oběť, například kolemjdoucího na ulici, bez ohledu zda se jedná o dítě nebo dospělou osobu, ta je přihlížející osobou při napadení nahrána na mobil nebo kameru, a video je poté zveřejněno na internetu pro širokou veřejnost za účelem pobavení diváků.

Sexting

Materiály s intimním a sexuálním podtextem jsou posílány dnes a denně mezi partnery, kteří využívají moderních metod komunikace. Problém nastává v případě, kdy jsou takové materiály zneužity a pachatel je například zveřejní na svém profilu v sociální síti, anebo založí falešný profil na komunitních a dalších portálech za účelem veřejného ponížení oběti. Nejčastějším důvodem bývá pomsta kvůli ukončení důvěrného vztahu, anebo vylákání citlivých dat za účelem dalšího zneužití.

Cyberstalking

Obecně se jedná o variantu stalkingu, neboli nebezpečné patologické a chorobné pronásledování vybrané osoby, která si nepřeje takovou pozornost. V této kategorii převažují z 80 % muži ve věku 30–40 let, což je rozdíl oproti například kyberšikaně.

Dnes je v rámci české legislativy upraven zákonem 40/2009 Sb. dle paragrafu §354, který vešel v platnost až v roce 2010 jako důsledek naléhavé změny narůstajících případů stalkingu. Nezřídka je tato aktivita provozována útočníkem i díky rozmachu moderních komunikačních technologií, kdy jsou využívány telefony, elektronická korespondence, natáčení multimédií a další metody.

Kybergrooming

Tento pojem označuje patologický jev, který souvisí s vyvoláním falešného pocitu a důvěry dětí a mladistvých ze strany pachatele. Cílem bývá pod záminkou

[13] *Nebuď oběť!*: *Rizika Internetu a komunikačních technologií o.s.* [online]. 2010 [cit. 2012-03-12]. Dostupné z: http://nebudobet.cz/

falešné a nereálné představy o pachateli (pro oběť se prezentující jak důvěrný přítel, nebo ideální partner) vylákat k osobnímu setkání nebo intimní schůzce.

Opět je zneužito anonymní internetové komunikace (chatovací nástroje, fóra, sociální sítě, emailová korespondence a další oblasti Internetu). Tuto formu zneužití osobní důvěry páchají především osoby s určitým rysem deviace, často se jedná o pedofilii. Z toho vyplývá i vyšší počet mužů coby útočníků. Následky těchto činů mohou být opět velmi tragické. Častým druhem útoku bývá znásilnění, fyzické napadení nebo také psychické zneužití, jako je vydírání k dětské prostituci a další nelegální aktivity.

Pornografie a Dětská pornografie

Dětská pornografie není spojena pouze s virtuálním prostředím, nicméně rozvoj těchto technologií k jejímu rozšíření výrazně přispěl. Její šíření je často spojováno s Internetem, ať již se jedná o zvukové nebo obrazové materiály.

2.2 Netholismus

„Počítače se zajisté nevyskytují mezi návykovými látkami. Ale možná vás napadlo, že i u počítačů lze uvažovat o příznacích jako „silná touha nebo pocit puzení užívat (si počítače, Internetu), potíže v sebeovládání užívání, a to pokud jde jak o začátek a ukončení, tak i o množství (času tráveného u počítače nebo na Internetu), průkaz tolerance jako vyžadování vyšších dávek (času u počítače nebo Internetu), postupné zanedbávání jiných potěšení nebo zájmů ve prospěch (počítače či Internetu) a pokračování v užívání (počítače, Internetu) přes jasný důkaz zjevně škodlivých následků (např. na pohybový systém nebo mezilidské vztahy).“[14]

V obecné rovině můžeme mluvit o netholismu jako jedné z forem nezdravé závislosti na určitém podnětu. V tomto případně se jedná o Internet jako virtuální svět, ve kterém člověk najde vše, co kdy lidská civilizace vytvořila – má to jednu zásadní nevýhodu – nemůžeme si na nic sáhnout, pouze to v nás vyvolává pocity uspokojení. Spoustu věcí máme na dosah a dovytváříme si vlastní ulitu, vlastní svět. Oficiálně ale nebyla závislost na hrách a internetu uznána a diagnostikována.

[14] NEŠPOR, K. *Počítače a zdraví.* Vyd. 1. Praha: BEN, 1999, s. 29. ISBN 80-86056-71-6.

„Jak tedy vypadá typický „závislák na Internetu“? … Na téma závislosti na Internetu bylo provedeno mnoho výzkumů, žádný však nepřinesl nijak překvapivá či obzvlášť významná zjištění. To, že na internetu jsou závislí častěji muži než ženy, bychom snad mohli očekávat, stejně jako fakt, že ti, kteří jsou na internetu závislí, jej využívají v daleko větší míře než lidé nezávislí k vyhledávání nových přátel, bavení se, hraní interaktivních her či virtuálnímu sexu.“[15]

Sklon k netholismu mohou mít děti a mládež, kteří nenašli jiné možnosti volnočasového uspokojení nebo vhodné náplně, mají sklon k sebepodceňování a nemají dostatek vhodných kamarádů, případně je ovlivněna jejich emoční nebo sociální inteligence v důsledku nezdravých rodinných nebo výchovných vztahů.

Jedním z projevů netholismu je neustálé hraní počítačových her. U velmi silně závislých jedinců taková závislost způsobila i smrt, obvykle na totální vyčerpání organismu, kdy závislá osoba nebyla již vůbec schopna rozpoznat příznaky ohrožení a realitu kolem sebe. Dalším projevem je přílišná závislost na dopisování nebo chatování se svými přáteli, nebo naopak cizími lidmi.

Projevy netholismu definujeme podobně jako u jiných závislostí. Bohužel tento druh závislosti je těžko odhalitelný nebo identifikovatelný, neboť Internet je současně považován za fenomén lidstvu prospěšný, slouží k podnikání, správě věcí veřejných, informovanosti celé populace. Proto se obtížně stanovuje hranice závislosti.

U dětí a mládeže můžeme pozorovat abstinenční příznaky, pokud jsou odloučeny od počítače, projevy jsou v oblasti emoční, následuje zhoršená pozornost, schopnost učení, osoba bývá podrážděná vůči okolí, přestává dbát o svůj zevnějšek, ustává zájem o jiné druhy koníčků a zábavy mimo počítače, přibývají výchovné problémy. Pomocnou ruku může podat odborná psychologicko pedagogická poradna, školní psycholog, rodinná poradna a další odborné subjekty. Léčba spočívá v dlouhodobé psychoterapii, obvykle se zapojením i nejbližší rodiny, tedy rodičů.

Hlavním cílem bývá přehodnocení vnitřních postojů a žebříčku hodnot směrem k pozitivnějším návykům v rámci životního stylu a dlouhodobému udržení takového cíle.

---

[15] ŠMAHEL, D. *Psychologie a internet*: *děti dospělými, dospělí dětmi*. Praha: Triton, 2003, s. 143. Psychologická setkávání, sv. 6. ISBN 80-7254-360-1.

3. Preventivní a bezpečnostní vzdělávací programy

Rizikové jevy, které se mohou objevit v rámci online komunikace ohrožují uživatele. Uživatelé mají však možnosti se chránit. Kde najít informace o hrozících nebezpečích a kde např. nahlásit nevhodný obsah seznamuje tato kapitola. Následující přehled webových portálů také seznamuje se svými vzdělávacími programy pro děti, rodiče a pedagogy.

3.1 Centrum prevence rizikové virtuální komunikace

Centrum PRVoK neboli Centrum prevence rizikové virtuální komunikace (dále pouze Centrum) realizuje a financuje od roku 2009 Katedra českého jazyka a literatury PdF UP v Olomouci ve spolupráci s Ministerstvem vnitra ČR a MŠMT. V rámci této spolupráce realizuje Centrum na území ČR projekt proškolování policistů a projekt proškolování žáků.

Dále pak spolupracuje s Preventivně-informační skupinou Policie ČR Olomouc a Odborem prevence kriminality Ministerstva vnitra ČR. Svoji činností navazuje na předchozí projekt E-Bezpečí.

Vedoucí Centra je jmenován vedoucím Katedry českého jazyka a literatury PdF UP a je odpovědný za jeho chod, odbornou způsobilost a postupy v souladu s etickými a právními normami. Partnery Centra jsou firmy Český rozhlas Olomouc a Vodafone.

V současnosti se Centrum věnuje ve spolupráci se školami na celém území ČR problematice sociálně-patologických jevů spojených s užíváním internetu a mobilních telefonů, kterými jsou například sexting, kyberstalking, kyberšikana, kybergrooming, hoax, spam, sociální inženýrství, zneužití osobních údajů a další rizika sociálních sítí. Cílem Centra je: vzdělávání, výzkum, prevence, intervence a poradenství. Centrum se také věnuje online poradenství a má i vlastní rozhlasový pořad. Centrum zajišťuje prevenci primární, viktimní a situační.

Při vzdělávání se věnuje ve spolupráci s Policií ČR vzdělávacím akcím a přednáškám, které jsou zaměřeny na školy, studenty učitelských i neučitelských oborů na PdF, pracovníky orgánů sociálně-právní ochrany, PIS Policie ČR a veřejnost. V rámci prevence pořádá mimo jiné i soutěže pro žáky ZŠ a SŠ zaměřené na nebezpečné komunikační činnosti.

Vzdělávání pro žáky, učitele, členy PIS Policie ČR nebo jiné pracovníky Policie ČR či MVČR a pracovníky orgánů sociálně-právní ochrany je interpretováno pomocí portálu www.e-bezpeci.cz.

Centrum má vytvořen systém komplexních preventivních programů pro oblast rizikového chování. Provozuje na svých internetových stránkách www.napisnam.cz a přes aplikaci pro mobilní telefony online poradnu ve spolupráci s organizacemi jako je Bílý kruh bezpečí, Policie ČR, pedagogicko psychologické poradny a zajišťuje tak pětivrstevné poradenství: primární, právní, psychologické, sociálně právní a policejní.

Umožňuje například i pomoc s nastavením ochrany proti rizikům v sociální síti Facebook. Zároveň se také věnuje regionálně i celorepublikově výzkumným programům zaměřených na sociálně patologické jevy. Další činností Centra je samotná realizace a provoz portálu E-bezpečí. Aktivity Centra a spolupracujících institucí či firem jsou realizovány převážně bezplatně a Centrum je začleněno zároveň bezplatně i do poradenského systému fakulty a univerzity.

V současnosti realizuje Centrum, například projekt E-Bezpečí - nebezpečí elektronické komunikace pro žáky i učitele 2. etapa, projekt E-Synergie, vědeckovýzkumná síť pro rizika elektronické komunikace a online projekt webového portálu Sexting.cz.

K červnu 2010 bylo Centrem proškoleno 4210 žáků a studentů SŠ a 200 učitelů a policistů.

V rámci projektu The Virtual Anti-Violence-Campus at Second Life na portále www.sl.e-bezpeci.cz realizuje vzdělávací a informační aktivity zaměřené na oblast rizikové komunikace spojené s internetem. Virtuální areál Centra v prostředí Second Life je provozován taktéž univerzitním pracovištěm PdF UP a je určen pro realizaci vzdělávacích, preventivních a informačních aktivit zaměřených na oblast rizikové komunikace spojené s internetem a souvisejícími jevy.

Centrum zde v areálu prezentuje svoje projekty Projekt E-Bezpečí, Projekt Online poradny projektu E-Bezpečí a Projekt E-Synergie. Areál je zázemím také pro další vzdělávací aktivity PdF UP, čímž rozšiřuje e-learningové studium jako jsou přednášky vědeckých expertů a významných pedagogů.[16]

3.2 Národní centrum bezpečnějšího internetu

České Národní centrum bezpečnějšího internetu je neziskové nevládní sdružení, založené v roce 2006 jako Online Safety Institute. Současný název NCBI nese od ledna 2011.

Cílem centra je podílet se na bezpečnějším užívání internetu, moderních informačních a komunikačních technologiích, prevenci a minimalizaci možných sociálních rizik spojených s jejich užíváním.

Centrum je členem celoevropské sítě národních osvětových center bezpečnějšího internetu INSAFE a spolupracuje s mezinárodní sítí horkých linek INHOPE. NCBI je realizátorem řady projektů se zaměřením na vzdělávání, především dětí, pomoc, zamezení šíření škodlivého a nevhodného obsahu a v rámci prevence počítačové kriminality pořádá semináře, přednášky, konference a školení.

Projekt provozuje tematicky vymezené portály: www.saferinternet, www.bezpecne-online.cz, www.horkalinka.cz, www.pomoconline.cz, www.payseccup.bezpecne-online.cz.

NCBI je zřizovatelem kamenného Informačního centra pro mládež, které poskytuje informace o bezpečném užívání internetu, možnostech volnočasových aktivit, vzdělávacích a pracovních aktivitách, které potom zveřejňuje na portálech www.saferinternet.cz a www.bezpecne-online.cz.[17]

[16] *Centrum prevence rizikové virtuální komunikace* [online]. 2012 [cit. 2012-03-12]. Dostupné z: http://www.prvok.upol.cz/

[17] O nás. *Saferinternet.cz*: *... pro bezpečnější internet* [online]. 2011 [cit. 2012-03-12]. Dostupné z: http://www.saferinternet.cz/

3.3 E-bezpečí, E-Synergie, Napiš nám, E-nebezpečí, Sexting

Projekt E-Bezpečí

Projekt E-Bezpečí neboli Prevence nebezpečných komunikačních praktik spojených s elektronickou komunikací pro pedagogy a nepedagogy byl zrealizován v roce 2008-2009 za podpory grantové dotace Grantové agentury ČR a Statutárního města Olomouc. Cílem byla především prevence sociálně patologických jevů virtuálního prostředí.

Projekt byl pak v průběhu roku 2009 doplněn projekty jednotlivých regionů. Jednalo se například o projekt „Bezpečný internet“ (Město Lipník nad Bečvou), projekt „Patron bezpečného internetu“ (Olomoucký kraj), projekt „E Bezpečí“ pro Olomouc. Projekty byly především zaměřeny na prevenci kyberkriminality a cílovými skupinami byli nejen děti, ale i dospělí především z řad rodičů, učitelů nebo policistů. Více než 60 škol z celé ČR se do tohoto programu aktivně zapojilo.

Projekt získal v roce 2009 3. místo v národním kole Evropské ceny prevence kriminality MVČR. Cílem projektu je informovat, zkoumat, pomáhat, podpora prevence a snižování rizik.

Nyní je projekt nadále realizován Centrem PRVoK a stále se věnuje nebezpečím vznikajících v rámci elektronické komunikace. Mediálním partnerem je Vodafone a Český rozhlas Olomouc. Cílem projektu jsou prevence a informace.

Cíleně edukuje žáky a učitele, vytváří edukační materiály, preventivní kampaně a realizuje výzkumná šetření. Rizikovou skupinou jsou především děti a mládež ve věku 6 až 15 let, tedy žáci ZŠ. Samotný portál www.e-bezpeci.cz slouží také k sumarizaci poznatků z výzkumů pro učitele a studenty učitelských oborů, které pak mohou využít ve vlastní praxi. Zveřejňování těchto informací je součástí kvalitní prevence před možnými sociálně-patologickými jevy. Portál má také svoji podobu na sociální síti Facebook.

Projekt na svém portále disponuje i poradnou. Najdete zde i příspěvky partnerských škol projektu s případy a způsoby řešení přímo z praxe. Nejen žáci zde mají k dispozici edukační materiály. V neposlední řadě je portál studnou informací pro rodiče, od vysvětlení pojmů, přes konkrétní rizika a doporučené postupy v případě již

vzniklého problému. Portál zároveň zveřejňuje výsledky výzkumných šetření, například „Kyberšikana u českých dětí“ - závěry z výzkumného šetření projektu E-Bezpečí a Centra PRVoK 2009, „České děti a mobilní telefony“ (výsledky výzkumu E-Bezpečí).

Jednotlivé podsekce portálu obsahují aktuální zprávy z ČR i ze světa týkající se konkrétních rizik. Další jsou pak děleny na sekci pro rodiče, žáky a učitele a je možno se zapojit i do partnerského programu.

Součástí portálu je pak mapa proškolených institucí a počet proškolených žáků, aktuální anketní otázka, knihovna multimédií a rozpis vzdělávacích akcí s názvem „Rizikové chování na internetu“.

Vzdělávací akce jsou děleny na 4 kategorie. V kategorii pro žáky 1. stupně ZŠ (5. třída) se jedná o dvouhodinovou přednášku s diskuzí ve skupině do 30 osob, zaměřenou na rizikové chování na internetu. Předmětem jsou především kyberšikana, kybergrooming, rizika sociálních sítí (se zaměřením na Facebook) a ochrana osobních údajů. Přednášejícími jsou lektoři projektu a eventuelně i policista. Nechybí ani edukační materiály.

V kategorii pro žáky 2. stupně ZŠ a studenty SŠ se také jedná o přednášku s diskuzí ve skupině maximálně 50 osob. Předmětem jsou stejné jevy a kyberstalking. Zbylý průběh přednášky je totožný.

Další kategorií je série přednášek pro maximálně 50 člennou skupinu učitelů ZŠ a SŠ. Předmětem jsou kyberšikana, kybergrooming, sexting, happy slapping, kyberstalking, rizika sociálních sítí, ochrana osobních údajů, prevence v oblasti IT technologií, právo, kasuistika, obrana a ochrana.

Poslední kategorie pro policisty PIS a městské policisty je totožná s kategorií předchozí.

Projekt ve své výroční zprávě za rok 2011 zveřejnil informaci o realizaci 111 vzdělávacích akcí pro děti a 39 vzdělávacích akcí pro dospělé. Celkově pak bylo proškoleno 4738 dětí a 1214 dospělých. Zároveň se zapojili do řešení 130 případů spojených s rizikovými jevy na internetu.

Ukázka propagačního letáku projektu je součástí přílohy č. 2.[18]

[18] *E-bezpečí* [online]. 2012 [cit. 2012-03-12]. Dostupné z: http://www.e-bezpeci.cz/

Projekt E-Synergie

Projekt E-Synergie je vědeckovýzkumná síť pro rizika elektronické komunikace Centra PRVoK se zaměřením na boj proti kyberkriminalitě a rizikovému chování spojenému s virtuálním prostředím. Partnery projektu jsou Odbor prevence kriminality MVČR, Krajské ředitelství policie Olomouckého kraje a firma Vodafone.

Cílem projektu je vytvoření vědeckovýzkumné sítě vzájemně propojující vzdělávací, výzkumné a podnikatelské organizace věnující se rizikové virtuální komunikaci v kyberprostoru včetně související kyberkriminality. Síť má být propojením teorie a praxe, přičemž teorie je zastoupena výzkumem a praxe vzděláváním, intervencí a trestně právní problematikou. Aktivita probíhá díky stážím, odbornou praxí a interaktivní komunikační technikou.

Zatímco projekty E-bezpečí a E-nebezpečí se věnují žákům, rodičům a učitelům, projekt E-Synergie je zaměřen na studenty učitelských a dalších souvisejících oborů PdF UP v souvislosti s budoucí pomocí řešení krizových situací. Studenti absolvují cyklus stáží, workshopů a přednášek pod týmem projektu E-Synergie, kde získají znalosti a dovednosti uplatnitelné při vlastní budoucí praxi.

Přednáška Rizikové chování na internetu pohledem projektu E-Bezpečí se po seznámení s projektem věnuje rizikovým situacím jako kyberšikana, happy slapping, sexting, kybergrooming. Dvoudenní akce „Rizikové chování na internetu a prevence kriminality pohledem Ministerstva vnitra ČR“ realizuje exkurzi v Muzeu policie a operačním středisku, seznámení s činností Policie ČR v rámci informační kriminality a legislativou v oblasti kybernetického prostředí. Zajímavostí je poté kazuistika konkrétních případů. Přednáška „Trestná činnost dětí a trestná činnost páchaná na dětech pohledem Policie ČR“ je zaměřena na trestně právní odpovědnost dětí, trestné činy páchané v souvislostí s elektronickou komunikací, statistiky, zvláštní kauzy, kriminalistické postupy, identikit, prostředky policejní techniky, včetně ukázek. Seminář „Vodafone a jeho aktivity v oblasti ochrany uživatelů mobilních sítí“ je představením firmy Vodafone, která se věnuje i ochraně dat.

Dvoudenní akce „Sociálně-právní ochrana dětí pohledem Olomouckého kraje“ se věnuje modelovým situacím sociálně-právní ochrany dětí, například krizová situace dítěte, počínající a vážné výchovné problémy dítěte. V druhé části probíhá setkání

s kurátorem pro mladistvé a exkurze v P-centru a Středisku sociální prevence Olomouc. Tímto programem se projekt snaží přispět k prevenci kriminality páchané na dětech.

Klíčovou aktivitou projektu je také networking, jehož základem je tvoření sítě kontaktů pro sdílení názorů, znalostí a zkušeností v dané oblasti.

Ačkoliv byl projekt realizován ke konci loňského roku, do první fáze vzdělávání se dle výroční zprávy zapojilo více jak 140 studentů.[19]

Poradna Napiš nám

Portál www.napisnam.cz je online poradnou projektu E-bezpečí a je realizován portál Centrem PRVoK ve spolupráci specialistů a Policie ČR. Poradenství probíhá anonymně a zdarma za finanční podpory Statutárního města Olomouc. Poradna funguje i pod aplikací pro některé moderní telefony. [20]

Projekt E-Nebezpečí

Projekt s vlastním portálem a aktualizovanou verzí na sociální síti Facebook má identifikační název „Nebezpečné komunikační jevy pro učitele se zaměřením na kyberšikanu, kyberstalking, kybergrooming a další sociálně-patologické jevy“ je realizován s podporou Evropských sociálních fondů a státního rozpočtu ČR. Cílem projektu E-Nebezpečí pro učitele je poskytování vzdělávání pro učitele ZŠ a SŠ pro orientaci v sociálně patologických jevech, které vznikají v souvislosti s internetovou a mobilní komunikací.

Konkrétní zaměřením jsou především jevy kyberšikana, sexting, kybergrooming, stalking a kyberstalking, ochrana osobních údajů, zneužívání sociálních sítí. Vzdělávání zajišťuje tým projektu E-bezpečí, Centra PRVoK a pracovníci PIS Policie ČR Olomouc. Vzdělávací aktivity jsou zdarma, mají akreditaci v rámci systému DVPP MŠMT a jsou podpořeny kvalitním edukačním materiálem použitelným pro vlastní praxi. Vzdělávání probíhá formou prezenčního kurzu nebo e-learningového studia pro absolventy předchozího kurzu.

[19] O projektu. *E-Synergie*: *vědeckovýzkumná síť pro rizika elektronické komunikace* [online]. 2011 [cit. 2012-03-12]. Dostupné z: http://esynergie.upol.cz/

[20] Poradna E-Bezpečí. *Poradna E-Bezpečí*: *pro oblast rizikové chování na internetu* [online]. 2008 [cit. 2012-03-12]. Dostupné z: http://napisnam.cz/

Prezenční kurz v rozsahu 4-6 hodin představuje základní téma, vysvětlení pojmů, statistiky, kazuistiky, prevence a seznamuje s e-learningovou částí vzdělávání. E-learningový kurz probíhá dva měsíce v systému LMS Unifor, speciální vzdělávací aplikaci, jejíž součástí je i propracovaná komunikace, diskusní fóra a jiné uživatelské možnosti. Samotný kurz se dále věnuje konkrétním sociálně patologickým jevům a krizovým situacím vznikající při internetové a mobilní komunikaci. Součástí tohoto kurzu je vypracování pracovního listu a vlastního projektu v rámci uvedených témat. Po absolvování obou částí vzdělávacího kurzu obdrží absolvent certifikát. [21]

Portál Sexting

Webový portál www.sexting.cz realizovaný projektem E-bezpečí a Centrem PRVoK varuje a především seznamuje širokou veřejnost s fenoménem sexting. Jednoduše vysvětluje právní problematiku sextingu a dětské pornografie. Je zde zveřejněn výsledek výzkumu v ČR a zahraničí, včetně videa australské kampaně. V závěru seznamuje s konkrétními případy u nás i v zahraničí, bohužel mnohdy s tragickým koncem. [22]

3.4 Další vzdělávací a informační portály, kampaně

Seznámíme se s webovými portály, které se věnují poskytování informací, metodikám a nabídce vzdělávacích aktivit. Patří sem:

- portál Saferinternet
- portál Bezpečně-online
- portál Horká linka
- organizace INHOPE
- portál Pomoc online
- portál Nebuď oběť!
- projekt Minimalizace šikany
- metodický portál RVP
- metodický portál Komunikační výchova
- portál projektu Internetová ambasáda

[21] O projektu. *E-nebezpečí pro učitele* [online]. 2010 [cit. 2012-03-12]. Dostupné z: http://e-nebezpeci.cz/

[22] Klikni. *Sexting.cz*: *nebezpečný fenomén* [online]. 2009 [cit. 2012-03-12]. Dostupné z: http://sexting.cz/

- portál Bezpečný internet
- projekt Internet Hotline
- portál Kyberšikana
- portál Ewa má problém
- portál Mobil Story
- kampaň Seznam se bezpečně
- kampaň Proti šikaně
- kampaň Skrytá identita

Tématům bezpečnější online komunikace se také věnují:

- konference „Rizika internetové komunikace“
- konference „Den bezpečnějšího internetu“ - „Safer Internet Day“
- konference „Trendy v internetové bezpečnosti“
- připravovaný „Zákon o kybernetické bezpečnosti“

Portál Saferinternet

Portál www.saferinternet.cz (Czech Safer Internet Combined Node) s Facebook verzí je český projekt podporovaný Evropskou komisí v rámci programu Safer Internet Plus. Cílem tohoto projektu je zvyšování povědomí uživatelů, dětí, pedagogů a rodičů o možných hrozbách Internetu a také iniciace diskuze, která by napomohla definovat význam pojmů nežádoucí a škodlivý obsah a vysvětlila, jak se vyhnout možným hrozbám.

Zaměřuje se také na realizaci výukových materiálů, konferencí, seminářů a výchovně vzdělávacích soutěží. Partnery jsou například Google, UPC, ERA, Centrum.cz, NIDM. Na portále jsou dále zveřejněny mediální ohlasy, informace o kampani Get Online Week k minimalizaci digitálního vyloučení, informace o ICM, které je součástí centra, edukační a metodické materiály pro vlastní potřebu, aktivity souvisejících portálů, newsletter informací.

Portál informuje také o aktuálně plánovaných nebo uskutečněných konferencích , například říjnová konference „Praha bezpečně online – podněty pro praxi“, jejímž cílem byla osvěta v rámci prevence a konkrétní případy kyberkriminality nebo konference Ústavně-právního výboru Senátu Parlamentu ČR „Prevence internetové kriminality a děti: technologie, edukace, legislativa“, věnující se praktickým

zkušenostem pedagogů, právníků, odborníků informačních technologií a dětí s užíváním internetu.

Zajímavostí jsou také pořádané soutěže pro děti, jako jsou vědomostní soutěž pro školní třídy „PaySecCup“ nebo soutěž vlastní fantazie u příležitosti „Dne ochrany osobních údajů“ pro děti a mládež „Moje soukromí! Nekoukat, nešťourat!“. Nechybí ani pravidelné aktuální články a také rozdělení sekce pro děti a rodiče, kde jsou s přihlédnutím k čtenáři vysvětleny pojmy kyberkriminality a uvedeny možnosti řešení.

Nejdůležitější součástí portálu je Safer Internet Akademie organizující semináře, přednášky, školení a konference v rámci prevence kyberkriminality a sociálně psychologických rizik vznikajících v kyberprostoru. Vzdělávací akce jsou realizovány pro pedagogy, školní metodiky, sociálním pracovníkům, policistům, pracovníkům veřejné správy, rodičům a veřejnosti. Program je dělen na kategorii workshopy, projekty a kurzy.

Workshopy určené rodičům mají názvy „Pozor na kyberšikanu“, „Pozor na kybergrooming“ a „Co číhá na děti na internetu“. Témata workshopů vyplývají z vlastních názvů. Součástí je seznámení se s jmenovaným fenoménem, prevence, dopady, právní otázky a následně samotné řešení vzniklých situací. Na závěr třetí výukové hodiny pro maximálně 15 účastníků obdrží rodiče výukové materiály a pracovní sešit pro děti.

Další kategorií jsou regionální projekty. Projekt Praha bezpečně online byl organizován městem Praha a NCBI. Byl zaměřen na prevenci před riziky používání internetu a online technologií, pražské dětské veřejnosti, formou osmihodinových seminářů pro odbornou veřejnost a pracovníky úřadů města Prahy.

Evropský projekt „Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání Internetu v Pardubickém kraji“ je podporován Evropským sociálním fondem v rámci Operačního programu Vzdělávání pro konkurenceschopnost ve spolupráci se SOŠE, SOU v Pardubicích a NCBI.

Cílem tohoto projektu je výchova k bezpečnému a etickému užívání internetu na ZŠ a SŠ v rámci bezplatného vzdělávacího programu pro pedagogické pracovníky ZŠ a SŠ, školní metodiky a výchovné poradce se zaměřením na ochranu dětských uživatelů internetu a následné využití poznatků ve vlastní výukové praxi. Součástí výuky je seznámení se s jevy kyberšikana školní a vůči učiteli, kybergrooming, rizika sociálních

sítí, nevhodný a protizákonný obsah, závislosti ve spojení s užíváním internetu, ochrana osobních údajů, autorská práva, právní postavení škol a řešení konkrétních situací. V závěru 40 vyučovacích hodin je třeba vytvořit vlastní školní projekt nebo modelovou lekci. Souběžně probíhá také projektová soutěž.

Cílem projektu „Region bezpečného internetu: Rozvoj kompetencí pracovníků škol v oblasti ICT a online bezpečnosti ve Středočeském kraji“ je rozvoj pravomocí pedagogických pracovníků, tvorba a realizace vzdělávacích programů v rámci DVPP, získání kvalifikace a didaktických schopností. Projekt je realizován městem Mladá Boleslav za podpory Operačního programu „Vzdělávání pro konkurenceschopnost“ financován z Evropského sociálního fondu a Státního rozpočtu ČR, NCBI a Obce Líbezníce. Metodiky vzniklé při realizaci projektu budou celostátně využity v budoucí výuce online bezpečnosti a etiky na ZŠ a SŠ.

Projekt "E-Crime" je dvoudenní seminář realizovaný Vysočina Education, odborem informatiky Krajského úřadu Kraje Vysočina, pod vedením NCBI se zaměřením na nejnovější poznatky v rámci e-bezpečnosti, včetně nových edukačních a metodických materiálů ke vzdělávání týmu poradců pro školy a další instituce.

Poslední kategorií vzdělávání NCBI je 8 otevřených kurzů, které jsou akreditované MŠMT pro DVPP, zakončené vydáním osvědčení o absolvování.

Kurz „Elektronická šikana a jak ji řešit“ je 8 hodinový seminář věnující se tématům: kyberšikana, prevenci, právním otázkám, řešením situací. Závěrem je obdržení edukačních, výukových materiálů a metodických podkladů pro praxi.

Kurz „Kybergrooming“ je 6 hodinový seminář věnující se tématům: kybergrooming, prevenci, řešením situací. Závěrem je obdržení edukačních, výukových materiálů a metodických podkladů pro praxi.

Kurz „Rizika sociálních sítí a co by děti měly vědět“ je 6 hodinový seminář věnující se tématům: sociální sítě, rizika, prevence. Závěrem je obdržení edukačních, výukových materiálů a metodických podkladů pro praxi.

Kurz „Nebezpečný a nezákonný obsah na internetu a jak s ním naložit“ je 6 hodinový seminář věnující se tématům: nezákonný a nebezpečný obsah, dětská pornografie, extremismus, technické bariéry, prevence a aktivní prostředky obrany. Závěrem je obdržení edukačních, výukových materiálů a metodických podkladů pro praxi.

Kurz „Práva učitele a nová média ve vyučování (PC, mobil, herní konzole)“ je 6 hodinový seminář věnující se tématům: nové technologie, připojení k internetu, kyberšikana proti učiteli, právo učitele se bránit, metodika právních aspektů, využití moderních technologií při výuce. Závěrem je obdržení edukačních, výukových materiálů a metodických podkladů pro praxi.

Kurz „Závislost na internetu a jak ji řešit“ je 6 hodinový seminář věnující se tématům: sociální sítě, hry online a jejich rizika, závislosti, možnosti pomoci. Závěrem je obdržení edukačních, výukových materiálů a metodických podkladů pro praxi.

Kurz „Dětská delikvence v prostředí internetu“ je 6 hodinový seminář věnující se tématům: nové technologie, aktuální situace v ČR a Evropě, aktuální výstupy z výzkumů, porušování autorských práv na internetu, šíření pornografie a dětské pornografie dětmi a teenagery, osobnostní práva na internetu, hacking, trestní odpovědnost dětí a mládeže, prevence. Závěrem je obdržení edukačních, výukových materiálů a metodických podkladů pro praxi.

Kurz „Jak vyučovat bezpečné a etické užívání online technologií na ZŠ a SŠ (metodické postupy)“ je 6 hodinový seminář věnující se tématům: představení metodických materiálů a pracovních listů, jak zacházet s metodickými materiály, přehled témat pracovních listů, workshop s ukázkou použití pracovních listů ve vzorové vyučovací hodině. Závěrem je obdržení edukačních, výukových materiálů a metodických podkladů pro praxi.[23]

Portál Bezpečně Online

Portál www.bezpecne-online.cz s Facebookovou verzí je aktivitou NCBI. Projekt je podporován Poštovní spořitelnou. Sekce všeobecná a sekce pro rodiče a učitele je souhrnem všech podstatných informací: newsletter, aktuální články ze světa a ČR, slovník, vysvětlení pojmů kyberkriminality a možných rizik v rámci online komunikace, výukové materiály, prezentace z kurzů, diskuze, poradenství, PaySecCup, informace jak surfovat bezpečně týkající se samotné komunikace a možných rizik, online hráčství, hledání informací, nakupování na internetu, internetbanking, sdílení dat,

[23] O nás. *Saferinternet.cz*: *... pro bezpečnější internet* [online]. 2011 [cit. 2012-03-12]. Dostupné z: http://www.saferinternet.cz/

technické zabezpečení počítače, autorský zákon, rodičovská kontrola, netiketa, sociální sítě a závislosti.[24]

Portál Horká linka

Portál www.horka-linka.saferinternet.cz s Facebookovou verzí je aktivitou NCBI ve spolupráci s Policií ČR, INHOPE za spolufinancován Evropskou unií. Projekt je kontaktním centrem pro příjem hlášení o nezákonném a nevhodném obsahu na internetu, kterým je například dětská pornografie, pedofilie, nelegální sexuální praktiky, rasismus, xenofobie, extremismus, šíření drog, sebepoškozování, nepovolená věková hranice a další. Po nahlášení informace Horká linka přešetří, vyhodnotí v souladu s aktuálními předpisy a předá odpovídajícím orgánům. Funguje i vzájemná spolupráce s mezinárodními linkami Internet Hotline. Hlášení probíhá e-mailem, formulářem na portále nebo „Červeným tlačítkem“. Červené tlačítko je software, který pohodlně umožňuje podat hlášení. Nechybí rady hlášení stížností na Facebook, popis, co je nezákonné a co nevhodné, zákony, statistika a případy z policejní praxe.[25]

Organizace INHOPE

INHOPE je mezinárodní organizace podporovaná Evropskou komisí, sdružující všechny horké linky. Cílem je vzájemná podpora horkých linek po celém světě a společné úsilí o bezpečnější Internet všem. Hlavním dokumentem je Etický kodex (Code of Practice) definující zázemí horkých linek, metodologii postupů, soubor doporučení vzájemné spolupráce.[26]

Portál Pomoc Online

Portál www.pomoc-online.saferinternet.cz je aktivitou NCBI. V úvodu dělen na věkové kategorie, posloupnost uživatelských znalostí. V sekci do 10 let jsou informace: vysvětlení pojmů internet, e-mail, chat, hry, sociální sítě, na co si dát pozor, Listina dětských práv, modelový případ a návod na pomoc. V sekci nad 10 let najdeme informace: vysvětlení pojmů internet, e-mail, chat, hry, sociální sítě, blogy, sdílení obsahu a dat, nakupování a telefonování, na co si dát pozor, modelový případ a návod

---

[24] Jsi na internetu jako doma?. *Bezpečně-online.cz* [online]. 2011 [cit. 2012-03-12]. Dostupné z: http://www.bezpecne-online.cz/

[25] Horká linka. *Horká linka.cz*: *bojujeme proti internetové kriminalitě* [online]. 2012 [cit. 2012-03-12]. Dostupné z: www.horka-linka.saferinternet.cz

[26] INHOPE Homepage. *INHOPE*: *International Association of Internet Hotlines* [online]. 2010 [cit. 2012-03-12]. Dostupné z: http://www.inhope.org/gns/home.aspx

na pomoc. Poslední sekce je věnována rodičům a pedagogům, přičemž prezentuje informace: vysvětlení pojmů, internet, rady jak ochránit nejen své děti, katalog otázek a rady kam se obrátit o pomoc.[27]

Portál Nebuď oběť!

Portál www.nebudobet.cz je provozován Občanským sdružením s názvem „Rizika internetu a komunikačních technologií“ a je podporován Statutárním městem Ostrava, NAEP, Alvit s.r.o. a knihovnou města Ostravy. Cílem portálu je zvýšit informovanost dětí ZŠ, rodičů a pedagogů o možných nebezpečích v rámci internetové komunikace, při využívání informačních technologií a na ochranu osobních dat. Portál nemá jen informační, ale i vzdělávací charakter. Úvodní část vysvětluje pojmy kyberšikana, sexting, stalking, happy slapping, netholismus, kybergrooming, hoax, včetně konkrétních případů ze života.

Dále jsou zde uvedeny informace z výzkumů, „Desatero bezpečného internetu“, pravidla chování, netiketa, Listina dětských práv, informace z legislativy a o asociaci INHOPE. Dále zde uživatel najde anglický překlad stránek, související odkazy, články, závěry domácích a zahraničních studií, novinky aktivit, dotazy a odpovědi uživatelů nebo posluchačů přednášek, videa z akcí, edukační a instruktážní videa a komiksy k tématům bezpečnosti internetu. Sdružení se dále věnuje především prevenci ve formě přednášek na ZŠ, pořádá ankety, workshopy, diskuze a semináře, například informativní seminář „Bezpečný internet“ nejen pro děti, ale i rodiče především v rámci Severomoravského kraje. [28]

Projekt Minimalizace šikany

Projekt portál www.minimalizacesikany.cz, realizovaný občanským sdružením Aisis za podpory Nadace 0_2, a MŠMT přidělením grantu z Evropských sociálních fondů má hlavní cíl snížení šikany na ZŠ a SŠ ČR, především svým vzdělávacím programem. Grant umožní projít vzdělávacím programem MiŠ zhruba 600 učitelům z ČR. Portál je také souhrnem informací jako jsou tiskové zprávy, aktivity projektu, online poradenství, souhrn a nabídka literatury vydané ve vzájemné spolupráci při projektu, podrobné

[27] Linka bezpečí: Úvodní strana. *Pomoconline.cz*: *Pomáháme dětským obětem internetové kriminality* [online]. 2010 [cit. 2012-03-12]. Dostupné z: www.pomoc-online.saferinternet.cz

[28] Nebuď oběť!: Novinky. *Nebuď oběť!*: *Rizika Internetu a komunikačních technologií o.s.* [online]. 2010 [cit. 2012-03-12]. Dostupné z: http://www.nebudobet.cz/

informace o šikaně, rady pro rodiče, školu, konkrétní případy, podrobné informace o kyberšikaně, výsledky soutěže kampaně „MIŠí děti říkají STOP kyberšikaně“, výběr vzdělávání.

Vzdělávání má podobu 4 dvoudenních seminářů pro celý pedagogický sbor školy, včetně vedoucích pracovníků a vytvoření vlastního plánu prevence šikany dané školy. Nově je pořádán seminář pro rodiče „Jak poznám, že je moje dítě šikanováno“ a jednodenní seminář „Kyberšikana ve školním prostředí“, který účastníky seznamuje s fenoménem kyberšikana, vysvětlí bezpečný pohyb ve virtuálním světě a je určen pro pedagogy, asistenty, výchovné poradce, vychovatele a vedení ZŠ a SŠ.[29]

Metodický portál RVP

Metodický portál www.rvp.cz je metodickou podporou učitelů v rámcových vzdělávacích programech škol. V sekci vzdělávání najdou zájemci vzdělávací článek s názvem „Stručný úvod do problematiky bezpečného internetu“ a věnuje se tématům: sdílení osobních údajů, internetová komunikace a otevřenost uživatelů, porušování pravidel služeb, závislostní chování a slabá ochrana hesel k internetovým účtům.[30]

Metodický portál Komunikační výchova

Portál www.komunikacnivychova.upol.cz je projektem Příprava a realizace výukových materiálů pro podporu komunikační výchovy RVP ZV ve výuce českého jazyka a literatury na základních školách a víceletých gymnáziích. Projekt je realizován Univerzitou Palackého v Olomouci za podpory MŠMT, spolufinancováním Evropských sociálních fondů a státním rozpočtem ČR.

Cílem projektu je příprava výukových materiálů, výukových listů tvořených odbornými profesionály. Portál se věnuje konferencím Komunikační výchova v teorii a praxi, všeobecným informacím projektu a soutěži Mladý Demosthenes. Podstatou

[29] Šikana: projekt Minimalizace šikany. *Minimalizace šikany*: *Informační portál o šikaně na školách* [online]. 2008 [cit. 2012-03-12]. Dostupné z: http://www.minimalizacesikany.cz/

[30] KOPECKÝ, K. Stručný úvod do problematiky bezpečného internetu: Základní vzdělávání. In: *Metodický portál*: *inspirace a zkušenosti učitelů* [online]. 22. 10. 2010 [cit. 2012-03-12]. Dostupné z: http://clanky.rvp.cz/clanek/c/Z/9673/strucny-uvod-do-problematiky-bezpecneho-internetu.html/

portálu jsou aktuální a zajímavé informace týkající se komunikační a mediální výchovy v teorii a praxi, tedy jak například vybavit žáka základní úrovní mediální gramotnosti.[31]

Portál projektu Internetová ambasáda

Portál www.internetembassy.cz je koncepcí pilotní fáze projektu patřící NCBI za finanční podpory Think Big Nadace O2. Cílem projektu je vzdělání za metodické podpory zhruba 10 členného týmu středoškolských studentů, tito členové se následně stanou ambasadory bezpečnějšího internetu.

Poté budou navštěvovat ZŠ, víceletá gymnázia za účelem prezentace preventivního programu peer learningu, jehož principem je zapojení proškolených studentů při realizaci vzdělávacích akcí skupinám vrstevníků, což působí věrohodněji. Projekt si klade za důležité rozšířit povědomí o nebezpečích a podpoření pozitivního online chování. Portál dále uvádí novinky z oblasti a pozvánky na konference, kontakty včetně Facebookové podoby.[32]

Portál Bezpečný Internet

Portál www.bezpecnyinternet.cz je projektem ve vzájemné spolupráci firem Seznam.cz, Microsoft, Česká spořitelna, Policie ČR, advokátní kancelář Pierstone a Quantasoft. Je dělen na sekce začínající a pokročilý uživatel, rodiče, děti a školy a má svoji Facebookovou podobu. Hned v úvodu je možné přesměrování na online diskuzi a poradnu, kde jsou zveřejněny i nejčastěji řešené problémy.

Cílem projektu je informovanost veřejnosti o možných rizicích a způsobech ochrany. Uživatelé zde najdou vysvětlení pojmů rizik online komunikace, informace o zabezpečení počítače a v závěru konkrétního tématu si může udělat test znalostí. Pokročilý uživatel má ve svojí sekci větší zřetel na zabezpečení počítače. V sekci informací pro rodiče jsou základní informace o možných rizicích a test znalostí. Sekce pro děti obsahuje výukové komiksové příběhy, dále pak například desatero bezpečného internetu, rady o zveřejňování osobních informací, a odkaz na kampaň Seznam se

[31] Vítejte na našich internetových stránkách: Aktuální informace. *Komunikační výchova*: *Příprava a realizace výukových materiálů* [online]. 2009 [cit. 2012-03-12]. Dostupné z: http://www.komunikacnivychova.upol.cz/

[32] Internetová ambasáda: Novinky. *Internetová ambasáda* [online]. 2011 [cit. 2012-03-12]. Dostupné z: www.internetembassy.cz

bezpečně a kde hledat pomoc. Poslední sekce pro školy obsahuje tip do výuky a přehled zákonů.[33]

Projekt Internet Hotline

Portál www.internethotline.cz je realizací stejnojmenného projektu, který je realizován a financován Nadací Naše dítě ve spolupráci s Policií ČR, pod záštitou MŠMT za podpory společností RWE, Livebox a Seznam.cz. Mimo všeobecných informací v rámci projektu, aktualit, slovníčku a formuláře pro nahlášení nelegálního obsahu, je portál dělen na tři sekce. Sekce s informacemi pro děti a mládež vysvětluje základní pojmy s nelegálním obsahem na internetu, zabývá se bezpečností a dětskými právy. Sekce pro rodiče zahrnuje vysvětlení rizik v rámci internetové bezpečnosti, věnuje se pojmům kyberstalking, kyberšikana, desateru rad a zabezpečení počítače. Sekce pro pedagogy uvádí navíc výsledky výzkumu internetové komunity Habbo.[34]

Portál Kyberšikana

Portál www.kyber-sikana.eu je realizací projektu Virtuální šikana a její psycho-sociální konsekvence u vysokoškolských studentů, což bylo umožněno účelovou podporou na specifický vysokoškolský výzkum udělené Univerzitě Palackého v Olomouci MŠMT. Projekt mapuje virtuální šikanu mezi studenty vysokých škol, realizuje výzkum a zveřejňuje výsledky, což je předmětem tohoto portálu. Nechybí zde informace o projektu, aktuality a diskusní fórum.[35]

Portál Ewa má problém

Portál www.ewamaproblem.cz má informační charakter pro rodiče a děti. Tento projekt vznikl za spolupráce Sdružení Linky bezpečí s patronkou Ewou Farnou, populární zpěvačkou mezi mládeží. V rodičovské sekci zmiňuje problémy výchovy, rozvodu, šikanu a zneužívání. Tyto fakta popisuje i v sekci pro děti, kde jsou přidány i témata týrání, útěk, sebepoškozování a šikana. Vždy je rodič nebo dítě odkázán na poradenství webu Sdružení Linky bezpečí.[36]

---

[33] Bezpečný internet. *Bezpečný internet.cz*: *Rady pro vaši bezpečnost* [online]. 2011 [cit. 2012-03-12]. Dostupné z: http://www.bezpecnyinternet.cz/

[34] Internet Hotline Nadace Naše dítě: Smysl a význam Internethotline.cz. *Internet Hotline.cz* [online]. 2009 [cit. 2012-03-12]. Dostupné z: www.internethotline.cz

[35] Vítejte. *Kyberšikana.cz*: *kyber-sikana.eu, cyberbullying.eu* [online]. 2012 [cit. 2012-03-12]. Dostupné z: www.kyber-sikana.eu

[36] Ewa má problém. *Ewa má problém.cz* [online]. 2009 [cit. 2012-03-12]. Dostupné z: www.ewamaproblem.cz

Portál Mobil story

Portál www.mobil-story.saferinternet.cz provozovaný NCBI má za partnery projektu společnosti Microsoft, 0_2, T-mobile a Vodafone. Portál slouží dětem a rodičům informacemi o mobilních telefonech, bezpečném užívání internetu, mobilní etiketě a nevhodném obsahu.[37]

Kampaň Seznam se bezpečně

Portál www.seznamsebezpecne.cz obsahuje 30 minutové video s totožným názvem, které seznamuje poutavým způsobem s možnými riziky na internetu a zaměřuje se především na anonymitu identit.

Cílovou skupinou diváků jsou děti především ve věku 12-16 let, rodiče, pedagogové a po získání akreditace MŠMT bylo distribuováno do všech ZŠ v ČR. Projekt realizovala společnost Seznam.cz za podpory Nadace Naše dítě, Linky bezpečí, Policejního prezidia. Portál dále uvádí „Desatero bezpečného internetu“, diskuzi k videu, vyhledání pomoci a nahlášení závadného obsahu. Nový druhý díl bude poprvé prezentován na konferenci RIK.[38]

Kampaň Proti šikaně

Portál www.proti-sikane.saferinternet.cz provozovaný NCBI je součástí evropské kampaně, do které je zapojeno 29 zemí. Portál poskytuje informace: popis šikany a kyberšikany, rozdíly, jak se bránit proti šikaně, rady rodičům, odkazy, dětská práva a následky, aktuality, soutěž, „Charta proti šikaně“.[39]

Kampaň Skrytá identita

Mediální kampaň „Skrytá identita“ je realizována NCBI ve spolupráci s Poštovní spořitelnou a Centrum Holdings. Cílem je aktivace zájmu veřejnosti o informovanosti v oblasti rizik online komunikace. Kampaň bude probíhat v rámci celé ČR prostřednictvím plakátů, které mají vyvolat potřebné zamyšlení o skutečné identitě

---

[37] Úvodní strana. *Mobilstory.cz*: *Používáme mobil bezpečně* [online]. 2011 [cit. 2012-03-12]. Dostupné z: www.mobil-story.saferinternet.cz

[38] Domů. *Seznam se bezpečně.cz*: *Jsou děti na internetu v bezpečí?* [online]. 2011, 2012 [cit. 2012-03-12]. Dostupné z: www.seznamsebezpecne.cz

[39] Úvodní strana. *Saferinternet.cz*: *Národní centrum bezpečnějšího internetu* [online]. 2009 [cit. 2012-03-12]. Dostupné z: www.proti-sikane.saferinternet.cz

lidí, pohybujících se v kyberprostoru. Pro základní orientaci doporučuje desatero online bezpečnosti.[40]

Konference „Rizika internetové komunikace“

Internetová stránka mezinárodní vědecké konference „Rizika internetové komunikace – teorie, praxe, prevence a edukace“ www.konference.e-bezpeci.cz informuje zájemce o programu, účastnících a bližších podrobnostech. Cílem jsou současné trendy v problematice nebezpečných komunikačních jevů, spojených s užíváním internetu a mobilních technologií. Nebudou chybět případy z praxe, uveřejnění výsledků výzkumných šetření, souhrn činnosti Policie ČR a ostatních institucí.

Konference je zaměřena na pedagogy, studenty učitelství, dále je určena psychologům, psychoterapeutům a policistům. Část teorie a praxe je finančně realizována projektem E-Synergie a část prevence a edukace projektem E-nebezpečí. Záštitu převzala PdF UP a vstup je zdarma. Přítomni budou i členové Linky bezpečí, firmy Vodafone, Seznam.cz a Google. V rámci konference proběhne také premiérové promítnutí druhého dílu edukačního projektu Seznam se bezpečně 2. Konference se koná 10. 5. 2012 v Olomouci.[41]

Konference „Den bezpečnějšího internetu“ - „Safer Internet Day“

Letošní „Den bezpečnějšího internetu“ vyšel na 7. února s mottem "Objevujte digitální svět spolu bezpečně!". Loňský „Den bezpečnějšího internetu“ proběhl 8. února a jeho mottem bylo "Víc než hra, je to tvůj život!" SID je organizován každým rokem mezinárodní sítí INSAFE. Cílem je propagace bezpečnějšího a zodpovědnějšího využívání online a mobilních technologií, především dětmi a mládeží, nejen u nás, ale i po celém světě. Každý rok se mohou školy formou soutěže zapojit do kampaně daného tématu a získat hodnotné ceny. Letošní motto se zároveň stalo celoročním programem osvěty Národního centra bezpečnějšího internetu, snažíc se

[40] Mediální osvětová kampaň "Skrytá identita": O kampani. In: *Bezpecne-online.cz*: *Skrytá identita* [online]. 2012 [cit. 2012-03-12]. Dostupné z: http://www.bezpecne-online.cz/skryta-identita

[41] O konferenci: Úvod. *Mezinárodní vědecká konference*: *Rizika internetové komunikace* [online]. 2010, 2012 [cit. 2012-03-12]. Dostupné z: www.konference.e-bezpeci.cz

o uvědomění si potřeby moderních technologií generací rodičů a prarodičů, a zároveň se snaží vzájemnou informovaností a spoluprácí poukázat na možná rizika.[42]

Konference „Trendy v internetové bezpečnosti“

Letos se konal čtvrtý ročník konference „Trendy v internetové bezpečnosti“ věnující se technickým bezpečnostním rizikům. Konferenci zahájila se statistickým výstupem členka Národního bezpečnostního institutu CSIRT, který ve spolupráci se sdružením CZ.NIC, zřízené Ministerstvem vnitra, dohlíží, kontroluje a zachycuje bezpečnostní incidenty. Globální rizika zmínil svojí přednáškou Miloš Balabán, vedoucí Střediska bezpečnostní politiky CESES na Fakultě sociálních věd UK.

Další přednášená témata se věnovala Internetu jako klíčové infrastruktuře, zamýšlela sen nad svobodou Internetu, zmiňovala možností zabezpečení IT struktury a počítačových sítí, význam čipů v dokladech, nastavování bezpečnostních certifikátů. Zdůrazněna byla rizika sociálních sítí, internetová kriminalita, bezpečnost mobilních transakcí a průřez aktuálních hrozeb, neboli havětí, zakladatelem serveru www.viry.cz.[43]

Připravovaný „Zákon o kybernetické bezpečnosti“

Národní bezpečnostní úřad vypracoval návrh věcného záměru zákona o kybernetické bezpečnosti, který byl do 29. února v připomínkovém řízení, kdy se mohla vyjádřit i nejširší veřejnost. Zákon řeší například vybudování „Národního centra kybernetické bezpečnosti ČR“ do konce roku 2015.

Do konzultace se zapojila i Pirátská strana, která svůj odmítavý postoj zveřejnila v tiskové zprávě dne 2. března.[44]

---

[42] Aktivity: Safer Internet Day 2012. In: *Saferinternet.cz*: *... pro bezpečnější internet* [online]. 2007, 2012 [cit. 2012-03-12]. Dostupné z: http://www.saferinternet.cz/sid-2012

[43] REDAKCE. Trendy v bezpečnosti 2012: soukromí, Facebook, mobilní platby a stará dobrá havěť. In: *Lupa.cz* [online]. 2. 3. 2012 [cit. 2012-03-12]. Dostupné z: http://www.lupa.cz/clanky/trendy-v-bezpecnosti-2012-soukromi-facebook-mobilni-platby-a-stara-dobra-havet/

[44] PIRÁTI. Piráti odmítají chystaný zákon o kybernetické bezpečnosti: Tisková zpráva České pirátské strany ze dne 2. března 2012. In: *Pirátské noviny.cz* [online]. 2. 3. 2012 [cit. 2012-03-12]. Dostupné z: http://piratskenoviny.cz/?c_id=33650

4. Vlastní výzkumné šetření

Praktická část se věnuje popisu cíle výzkumného šetření, stanovení hypotéz, popisu výběrového souboru a metodě sběru dat. Následně jsou získaná data analyzována a hypotézy ověřovány. Dílčí závěr tyto poznatky shrnuje.

4.1 Cíl empirické části, stanovení hypotéz, výběrový soubor, metodologie

Téma mého průzkumného šetření navazuje na teoretickou část, která je zmapováním existence webů, které se věnují informacím, prevenci a vzdělávání v oblasti rizikové komunikace internetového prostředí. Cílem je zjištění rozsahu informovanosti a přístupu rodičů v souvislosti s těmito jevy.

Stanovení hypotéz

Otázky jsem vytvářela s cílem pokusit se potvrdit či vyvrátit stanovené hypotézy. Mimo hypotézy mne ale zajímaly i další statistické informace a vzájemné souvislosti, které zmíním při samotném zpracování dat.

Hypotézy jsou označeny zkratkou H a číselným označením.

H_1: Rodiče neznají možná rizika online komunikace na internetu

H_2:Rodiče nejsou dostatečně informováni o možnostech preventivního vzdělávání v oblasti rizikové online komunikace na internetu

Charakteristika výběrového souboru

Cílovou skupinou výběrového souboru byli náhodní rodiče s alespoň jedním dítětem. Věk dítěte nebyl stanoven, důležité pro můj výběrový soubor byl pohyb na internetu, kde jsem předpokládala alespoň minimální znalost rodiče, tj. co je počítač, jak se používá, dále pak vědomost, co je Internet a co jsou webové stránky.

Výběr cílové skupiny byl tedy založen na dobrovolnosti a dostupnosti, přesněji tzv. samovýběrem a výsledky nejsou zobecnitelné pro celou populaci.

„Mechanismus samovýběru je dán způsobem distribuce podnětu. … Výsledky tohoto šetření nejsou zobecnitelné, resp. jsou zobecnitelné pouze na populaci těch, kteří odpověděli. Takže je nelze jakkoli vztahovat na ostatní populaci.“[45]

Metoda sběru dat

V závislosti na stanoveném cíli jsem si vybrala kvantitativní metodu výzkumu. Vytvořila jsem pro tento účel standardizovaný dotazník.

„Vysoce efektivní technika, která může postihnout veliký počet jedinců při relativně malých nákladech. …Anonymita je relativně přesvědčivá.“[46]

V první části dotazníku jsem zvolila otázky statistické a ve druhé pak otázky konkrétní sloužící k vyvrácení nebo potvrzení stanovených hypotéz nebo sloužící k bližšímu prohloubení informací dotýkajících se zvoleného tématu. Celkem je použito 25 uzavřených otázek. Otázky jsem se snažila formulovat srozumitelně a výstižně.

Před zveřejněním dotazníku jsem jej nejprve několikrát sama zkoušela vyplnit a odstranit přitom případné nedostatky a chyby. Potom jsem požádala dva rodiče 1 muže a 1 ženu k jejich vyplnění z důvodu opětovné kontroly chyb a k vytvoření připomínek. Před oficiálním zveřejněním byly všechny pokusy vynulovány.

Dotazník byl šířen po schválení administrátorem elektronickým zadáním na webový server www.vyplnto.cz a jeho vlastním nástrojem nabízení vyplnění a závěrečného statistického zpracování.

Dále jsem vyplnění dotazníku nabídla rodičům, uživatelům sociální sítě Facebook a především rodičům pohybujících se na rodičovských webech www.emimino.cz, www.modrykonik.cz, www.babyweb.cz a www.spoluzaci.cz. Další respondenti byli osloveni také prostřednictvím e-mailových dopisů. Respondentům byl vysvětlen cíl dotazníku a nabídnuta možnost zveřejnění výsledků.

Na vyplnění dotazníku měli respondenti 7 dní. Tento způsob vyplnění dotazníku má i výhodu nemožnosti přeskočení vyplnění otázky, ať již úmyslné, nebo nedbalostní.

---

[45] REICHEL, J. *Kapitoly metodologie sociálních výzkumů*. Vyd. 1. Praha: Grada, 2009, s. 84. Sociologie (Grada). ISBN 978-80-247-3006-6.

[46] DISMAN, M. *Jak se vyrábí sociologická znalost*: *Příručka pro uživatele*. 3.vyd. Praha: Karolinum, 2000, s. 141. ISBN 978-80-246-0139-7.

Nákladem na průzkumné šetření byla pouze platba poskytovateli internetového připojení. Vzor dotazníku je součástí přílohy č. 1.

4.2 Analýza dat

Mého výzkumného šetření se zúčastnilo 127 respondentů, respektive tito respondenti vyplnili celý dotazník. Návratnost je zde hodnocena 81 %, což je rozdíl mezi fakticky vyplněnými a zobrazenými dotazníky. Průměrná doba vyplnění jednoho dotazníku byla 5 minut a 22 sekund. Zjištěné přístupy zobrazení dotazníků jsou z webových serverů www.facebook.com (30 %), www.emimino.cz (13,7 %), www.spoluzaci.cz (9,7 %), www.vyplnto.cz (7,2 %), ve 39,4 % není přístup zřejmý, např. z důvodu použití poštovního klienta.

Grafy zveřejňuji pouze k otázkám týkajících se tématu práce a hypotéz, u ostatních otázek by v textu bakalářské práce pouze zaplnily prostor.

1) **Jste?**

Dotazník vyplnilo 111 žen (87,4 %) a 16 mužů (12,6 %). Z tohoto výsledku usuzuji, že uvedené formy oslovení respondentů pravděpodobně více oslovily ženy než muže, z důvodu např. jejich přítomnosti na uvedených webových fórech.

2) **Kolik je Vám let?**

Téměř vyrovnaně jsou zastoupeni rodiče věkové hranice 31-40 let (53 respondentů 41,73 %) a věkové hranice 21-30 let (52 respondentů 40,94 %). Dále pak ve věku 41-50 let 17 respondentů (13,39 %), 4 respondenti ve věku 16-20 let (3,15 %) a 1 respondent ve věkové kategorii 51 a více (0,79 %).

3) **Jaké je Vaše nejvyšší dosažené vzdělání?**

Dotazem na vzdělání bylo zjištěno, že 77 respondentů (60,63 %) má středoškolské vzdělání, 46 respondentů (36,22 %) vysokoškolské vzdělání a 4 respondenti (3,15 %) základní vzdělání. Podrobnější rozbor vzdělání nebyl pro cíl dotazníku nutný. Z uvedených 4 respondentů se základním vzděláním vyplnili svůj věk v kategorii 3 respondenti 16-20 let, ale zároveň 2 uvedli v otázce věku vlastního dítěte kategorii 13-17 let, což není možné. Je tedy zřejmé, že minimálně ve 2 případech nebyla

buď otázka pochopena, nebo byla odpověď úmyslně či neúmyslně špatně zvolena, což je jedna z nevýhod kvantitativní metody anonymního dotazníku.

4) **Jste momentálně na mateřské dovolené?**

Ano odpovědělo 61 respondentů (48,03 %) a 66 respondentů (51,97 %) odpovědělo ne. Zde jsem spíše očekávala opačný poměr, ale zřejmě si našli čas na vyplnění dotazníku i zaměstnaní rodiče.

5) **Místo Vašeho bydliště?**

Respondentů z Jihomoravského kraje bylo 51 (40,16 %), Středočeského kraje 13 (10,24 %), Ústeckého kraje 9 (7,09 %), Moravskoslezského kraje 9 (7,09 %), hlavního města Prahy 8 (6,3 %), Pardubického kraje 7 (5,51 %), Plzeňského kraje 5 (3,94 %), Zlínského kraje 5 (3,94 %), Olomouckého kraje 5 (3,94 %), zahraničí 5 (3,94 %), Libereckého kraje 4 (3,15 %), kraje Vysočina 3 (2,36 %), Jihočeského kraje 2 (1,57 %) a 1 (0,79 %) kraje Královéhradeckého. Nesporná výhoda dotazníku šířeného online byla, že se rozšířil i za hranice Jihomoravského kraje.

6) **Kolik máte dětí?**

Od této otázky následuje blok otázek, týkajících se dětí respondentů. Respondentů s 1 dítětem bylo 86 (67,72 %), se dvěma 35 (27,56 %) a 6 (4,72 %) respondentů uvedlo 3 a více dětí.

7) **Věk Vašeho dítěte?** (V případě, že máte víc než 1 dítě, vyplňte prosím tuto informaci vztažnou k dítěti, které stráví u počítače nejvíce času).

Respondenti uvedli věk dítěte 0-6 let v 83 případech (65,35 %). Dále pak 18 respondentů (14,17 %) uvedlo stáří dítěte 13-17 let, věkovou hranici 7-12 let uvedlo 14 respondentů (11,02 %) a 12 respondentů (9,45 %) uvedlo věk 18 a více let. Z výsledku lze konstatovat, že více než polovina respondentů elektronicky oslovených jsou rodiče s nejmladšími dětmi, což ale nemá zkreslující efekt na cíl dotazníku.

8) **Hlídají Vaše děti minimálně 1x týdně po dobu minimálně 2 hodin jiní rodinní příslušníci?**

Tato otázka byla vytvořena záměrně, pokud by bylo převládající množství odpovědí ano, dalo by se předpokládat, že je důležité, aby i oni měli přehled o rizicích

online komunikace, protože jsou dozorem v době volna dítěte, a je důležité vědět, zda nějaké povědomí mají či ne. Ne odpovědělo 67 respondentů (52,76 %) a ano 60 respondentů (47,24 %). Dá se tedy z výsledku usuzovat, že již dřívější model hlídání pomocí babiček a dědečků nefunguje jako dříve, především z důvodu prodloužení věku odchodu do důchodu a zvýšené potřebě finančního přivýdělku i v důchodovém věku. Jedná se pouze o moji domněnku, skutečný stav by bylo potřeba zjistit jiným šetřením.

9) **Kolik času průměrně denně Vaše dítě stráví u počítače mimo aktivit spojených se školou?** (V případě, že máte víc než 1 dítě, vyplňte prosím tuto informaci vztažnou k dítěti, které stráví u počítače nejvíce času).

Počítač zatím neovládá 75 dětí (59,06 %) respondentů. Dalších 41 dětí (32,28 %) respondentů stráví u počítače 0-3 hodiny, 5 dětí respondentů (3,94 %) stráví u počítače 7 a více hodin. U počítače stráví 4-6 hodin 4 děti respondentů (3,15 %) a 2 respondenti (1,57 %) nevědí, kolik času u počítače jejich děti stráví. Největší zastoupení odpovědí, že dítě počítač neovládá, je dáno největším počtem dětí respondentů ve věku 0-6 let. Z počtu 75 dětí počítač neovládajících je 73 dětí ve věku 0-6 let a pouze 2 děti ve věku 7-12 let.

10) **Víte co dělají Vaše děti na počítači mimo školních povinností?**

Respondenti mohli vybírat více položek. V souladu s předchozími výsledky odpovědělo, že počítač zatím dítě neovládá 78 respondentů (61,42 %). Předpokládala jsem stejný počet jako u předchozí otázky, tedy 75 odpovědí respondentů, ale 3 respondenti uvedli v předchozí otázce místo neovládání počítače dítětem rozsah používání počítače v kategorii 0-3 hodin. Dále zhruba vyrovnaně odpovědělo 32 respondentů (25,2 %) o využití počítače dítětem k hledání informací, 27 respondentů (21,26 %) k chatování a telefonování, 27 respondentů (21,26 %) k pohybu na sociálních sítích a fórech, 16 respondentů (12,6 %) k prohlížení a ukládání fotek a videí. Poslední 3 (2,36 %) respondenti uvedli, že nevědí, jak tráví čas jejich děti na počítači mimo školní povinnosti. Respondenti mohli vybírat více odpovědí a minimálně jednu. Dle výsledků je zřejmé, že se děti respondentů věnují vícero činnostem na počítači mimo školní aktivity.

11) **Používá Vaše dítě při online komunikaci webkameru?**

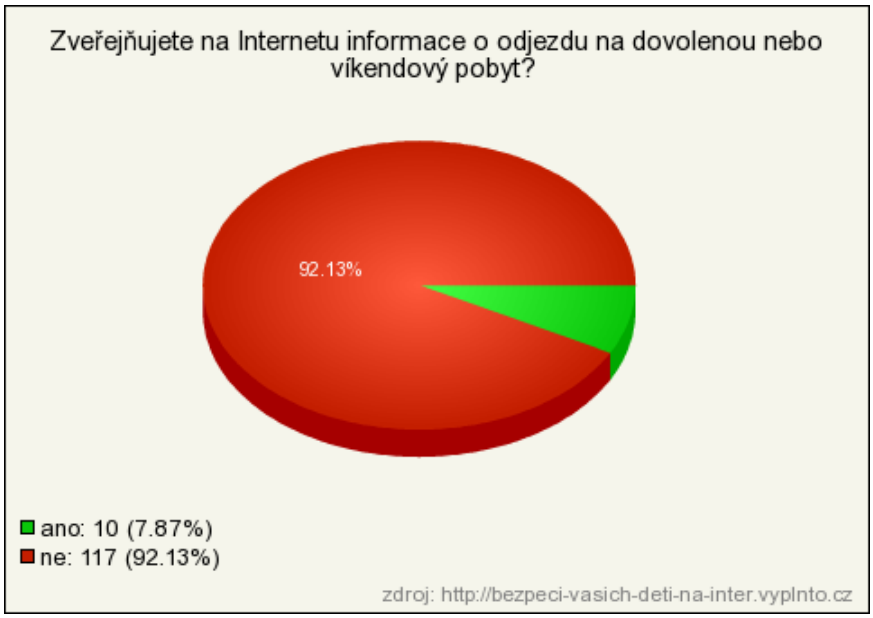
Respondenti uvedli ve 105 případech (82,68 %), že jejich děti nepoužívají při online komunikaci webkameru. Dalších 17 respondentů (13,39 %) uvedlo, že ji děti používají a 5 respondentů (3,94 %) nevědělo, zda jejich dítě při online komunikaci kameru využívá. Tato otázka byla uvedena z důvodu zjištění rizik online komunikace, kde přes záběry webkamery může např. potencionální zloděj tipovat prostory za hlavou komunikujícího nebo může webkamera sloužit k natáčení videa.

12) **Jaké jsou Vaše počítačové dovednosti?**

Touto otázkou se vrací pozornost dotazníku zpět k rodiči. Respondenti ohodnotili svoje počítačové dovednosti v 70 odpovědích (55,12 %) jako uživatelsky dobré se schopností nastavit i některé bezpečnostní prvky, v 36 případech (28,35 %) bez schopnosti nastavit bezpečnostní prvky. Ve 14 případech (11,02 %) ohodnotili svoje schopnosti respondenti jako profesionální se schopností nastavení veškerých bezpečnostních prvků. Žádné dovednosti charakterizovali 4 respondenti (3,15 %) a 3 respondenti (2,36 %) ohodnotili své dovednosti jako minimální. Otázkou je do jaké skutečné míry dovednosti respondentů dosahují a zda byla otázka dostatečně pochopena svým obsahem nebo jednotlivými rozdíly, což je nevýhoda chybějícího osobního vysvětlení při vyplňování.

13) **Zveřejňujete na internetu informace o odjezdu na dovolenou nebo víkendový pobyt?**

Respondenti odpověděli, že ve 117 případech (92,13 %) informace o odjezdu na dovolenou nebo víkendový pobyt nezveřejňují a v 10 případech (7,87 %) tyto informace zveřejňují. Tato otázka byla zajímavá pro zjištění rizika těch, kteří uvedenou informaci zveřejňují, např. riziko vytipování vykradení bytu pachatelem ať přímo nebo přes zprostředkovatele informace. Zajímavá je také skutečnost, že 7 respondentů z 10 tuto informaci zveřejňující jsou respondenti ve věku 21-30 let. Výsledek je podstatný pro ověření $H_{1.}$



Graf č. 1

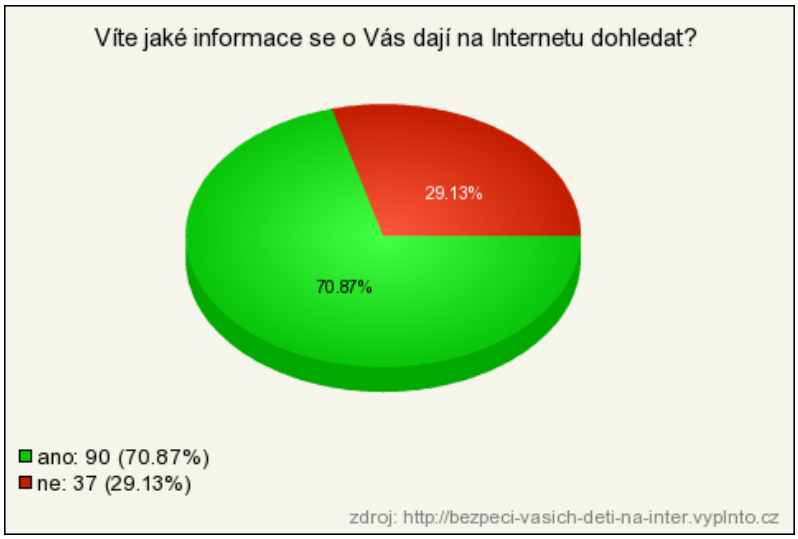
14) **Využíváte sociální síť Facebook?**

Převážná většina odpověděla, že sociální síť Facebook využívá a zároveň umí nastavit soukromí uživatelského profilu a to v 91 případech (71,65 %), v dalších 10 případech (7,87 %) toto soukromí nastavit respondenti neumí a 26 respondentů (20,47 %) sociální síť Facebook nevyužívá. Opět je nedostatkem chybějící osobní kontakt při vyplňování dotazníku, míra pochopení nastavení bezpečnosti uživatelského programu může být rozdílná.

Graf č. 2

15) **Víte, jaké informace se o Vás dají na internetu dohledat?**

V 90 případech (70,87 %) uvádí respondenti, že vědí, jaké informace se o nich na internetu dají dohledat a ve 37 případech (29,13 %) uvádí respondenti, že toto nevědí. Problémem otázky může být rozdílné pojetí obsahu dohledatelných informací. Výsledek je podstatný pro ověření H_1.



Graf č. 3

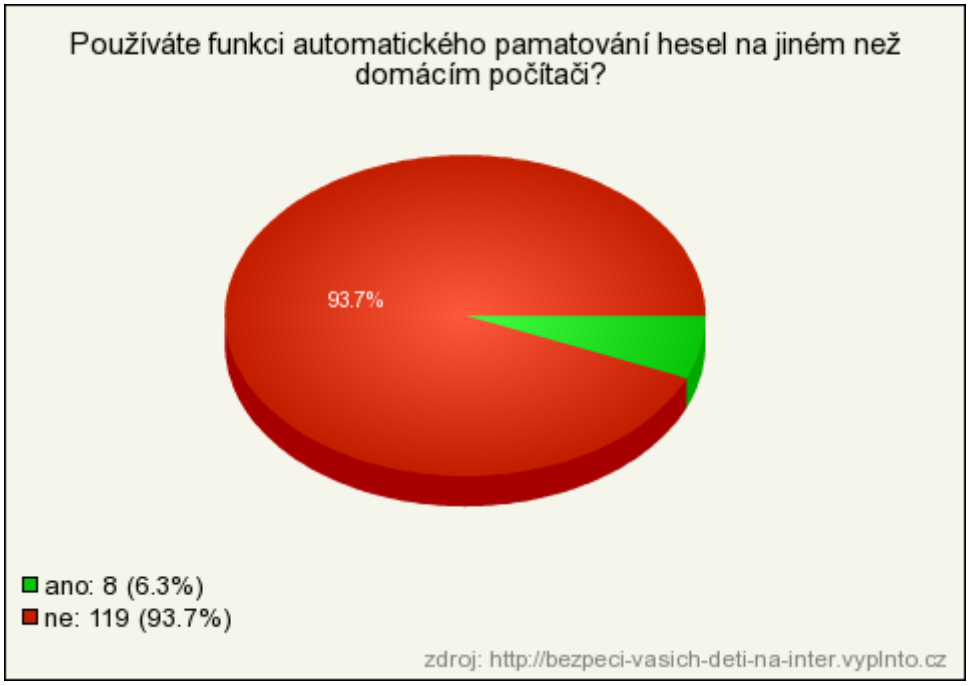
16) **Máte rozdílná hesla na různých uživatelských profilech?**

Zde uvedlo 101 respondentů (79,53 %), že má rozdílná hesla na uživatelských profilech a 26 respondentů (20,47 %) uvedlo, že nemá rozdílná hesla. Tato otázka byla zajímavá k přihlédnutí stavu, jak respondenti, potažmo uživatelé počítače přistupují k tématu bezpečnosti, protože tento fakt je jednou z rad bezpečného užívání internetu. Výsledek je podstatný pro ověření H_1.

Graf č. 4

17) **Používáte funkci automatického pamatování hesel na jiném než domácím počítači?**

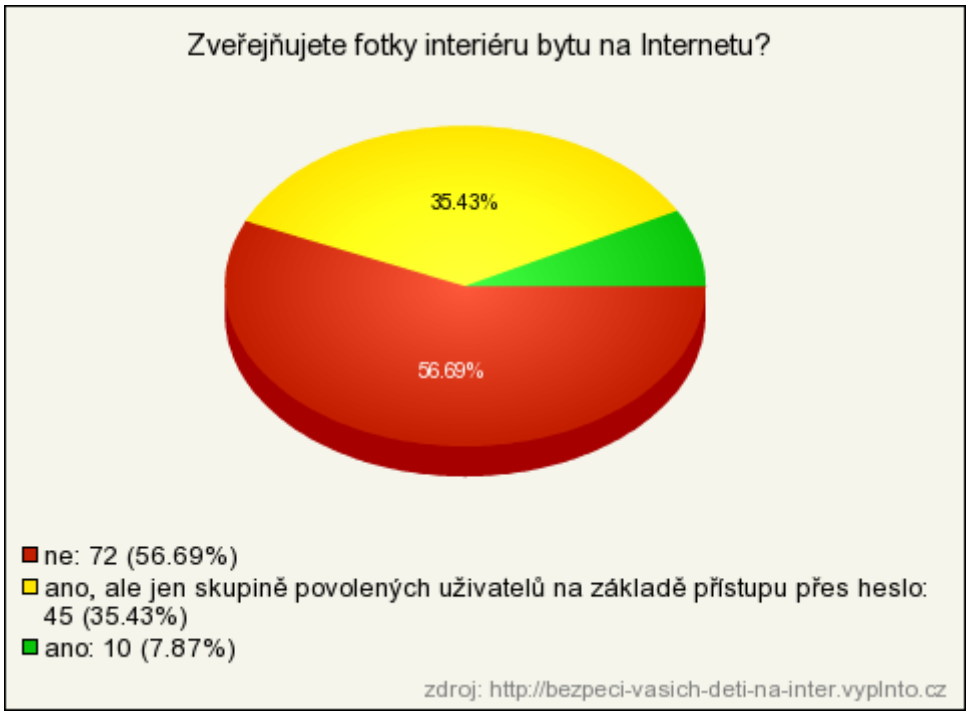
Překvapivě odpovědělo 119 respondentů (93,7 %), že funkci automatického pamatování hesel nepoužívá na jiném než domácím počítači a 8 respondentů (6,3 %) ji používá. Moje dosavadní zkušenost v pracovním životě ukazovala na obrácený výsledek výpovědí respondentů, protože ale výsledky nejsou zobecnitelné, je možné, že tato skupina je uživatelsky vzdělanější, může to být ale i věkovým rozdílem respondentů dotazníku a pracovním kolektivem. Výsledek je podstatný pro ověření H_1.



Graf č. 5

18) **Zveřejňujete fotky interiéru bytu na internetu?**

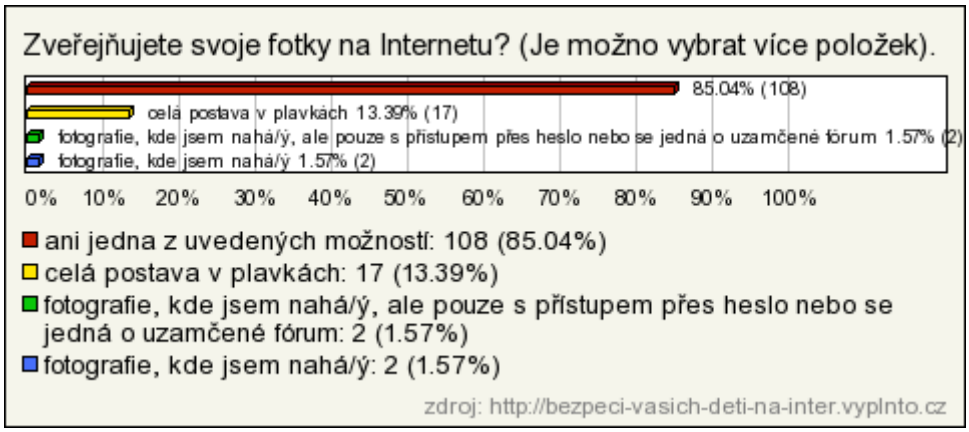
Větší část respondentů, konkrétně 72 (56.69 %) odpověděla, že fotky interiéru bytu nezveřejňuje, což je z bezpečnostního hlediska vhodnější, např. z důvodu vytipování interiéru ke krádeži, mnohdy i když samotný interiér není hlavním předmětem fotografie. Tato má otázka souvisí i s otázkou č. 13. Dalších 45 respondentů (35,43 %) tyto fotografie zveřejňuje, ale jen ve skupině povolených uživatelů na základě přístupu přes heslo, což koresponduje s odpověďmi otázky č. 12, kdy si jsou respondenti schopni nastavit i určité bezpečnostní prvky. Skupina 10 respondentů (7,87 %) uvedla, že fotografie zveřejňuje. Lépe by asi vystihovala možnost otevřené otázky ano, všem. Předpokládejme ale, že byly odpovědi respondenty správně pochopeny. Výsledek je podstatný pro ověření H_1.



Graf č. 6

19) **Zveřejňujete svoje fotky na Internetu?**

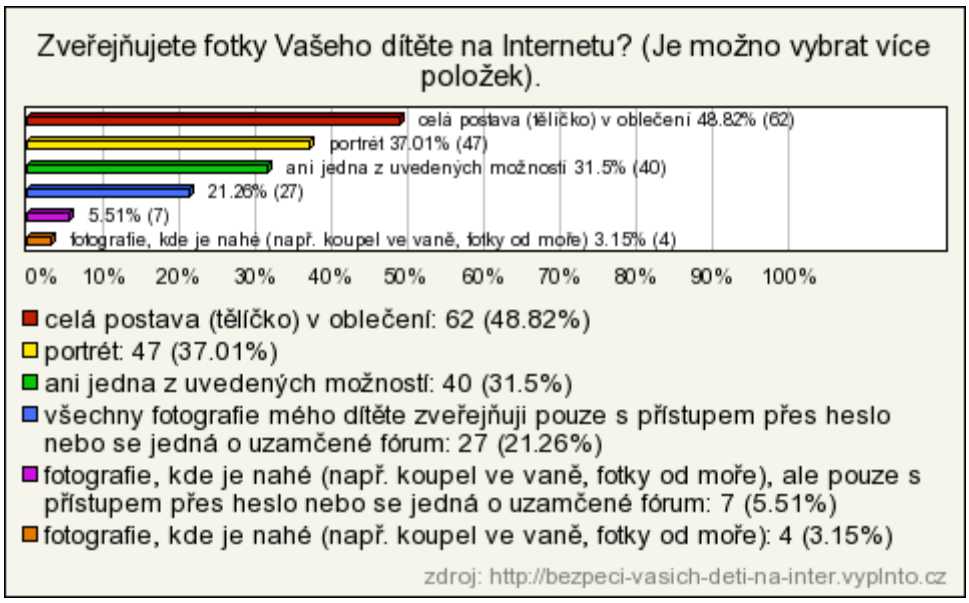
Při této otázce mohli respondenti vybírat více možností, přičemž většina respondentů 108 (85,04 %) zvolila výběr ani jedné z uvedených možností. Lze předpokládat, že z důvodu zachování intimity zvolilo pouze 17 respondentů (13,39 %) možnost výběru odpovědi, kdy zveřejňuje celou postavu v plavkách a 2 respondenti (1,57 %) i fotografie nahé postavy, ale pouze s přístupem přes heslo a 2 respondenti (1,57 %) fotografie nahé postavy bez omezení. Jistě by bylo zajímavé tyto dotazy položit paralelně i dětem a mladistvým. Výsledek je podstatný pro ověření H_1.



Tabulka četností č. 1

20) **Zveřejňujete fotky Vašeho dítěte na Internetu?**

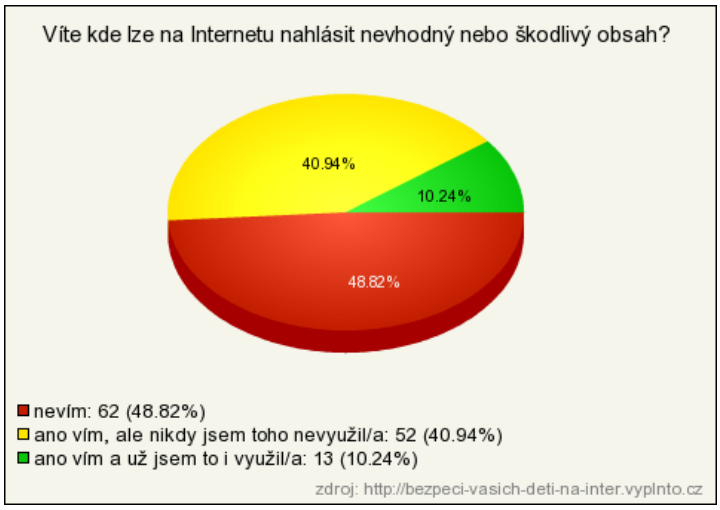
Respondenti mohli u dotazu opět volit více možností. Více jak polovina respondentů zveřejňuje fotografie celé postavy svých dětí, konkrétně 62 respondentů (48,82 %). Dalších 47 respondentů (37,01 %) zveřejňuje portrét svých dětí. 40 respondentů (31,5 %) nezveřejňuje jmenované fotografie. Všechny fotografie svého dítěte zveřejňuje pouze pod přístupem přes heslo 27 respondentů (21,26 %). Také přes zabezpečený přístup zveřejňuje fotografie nahého těla svého dítěte 7 respondentů (5,51 %). Stejné fotografie, ale bez bezpečnostního omezení v přístupu zveřejňují 4 respondenti (3,15 %). Dle odpovědí otázek č. 19 a č. 20 lze usuzovat, že uvedení respondenti nad bezpečností nebo možnými riziky, které souvisí se zveřejňováním intimních partií na fotografiích minimálně přemýšlí nebo znají možná rizika a chrání se před nimi. Výsledek je podstatný pro ověření H_1.



Tabulka četností č. 2

21) **Víte kde lze na Internetu nahlásit nevhodný nebo škodlivý obsah?**

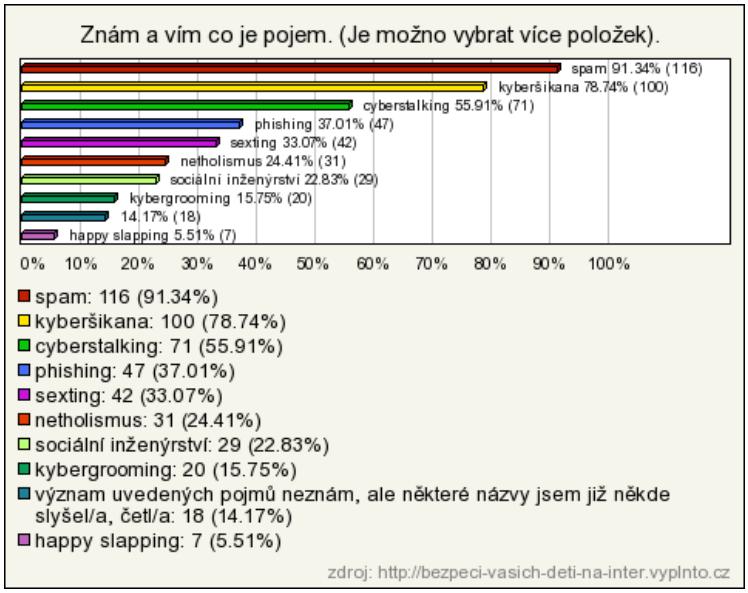
Tuto informaci nemá více jak polovina respondentů, tedy 62 (48,82 %). Dalších 52 respondentů (40,94 %) tuto informaci má, ale možnost hlášení nikdy nevyužila a 13 respondentů (10,24 %) tuto informaci má a dokonce hlášení i podala. Předmětem dalšího šetření by mohlo být zajímavé zjištění o jaký nevhodný nebo škodlivý obsah se jednalo, jaká možnost hlášení byla využita a zda došlo k následné nápravě či sankcionalizaci odpovědného. Výsledek je podstatný pro ověření H_1.



Graf č. 7

22) **Znám a vím co je pojem (dle následujícího výčtu).**

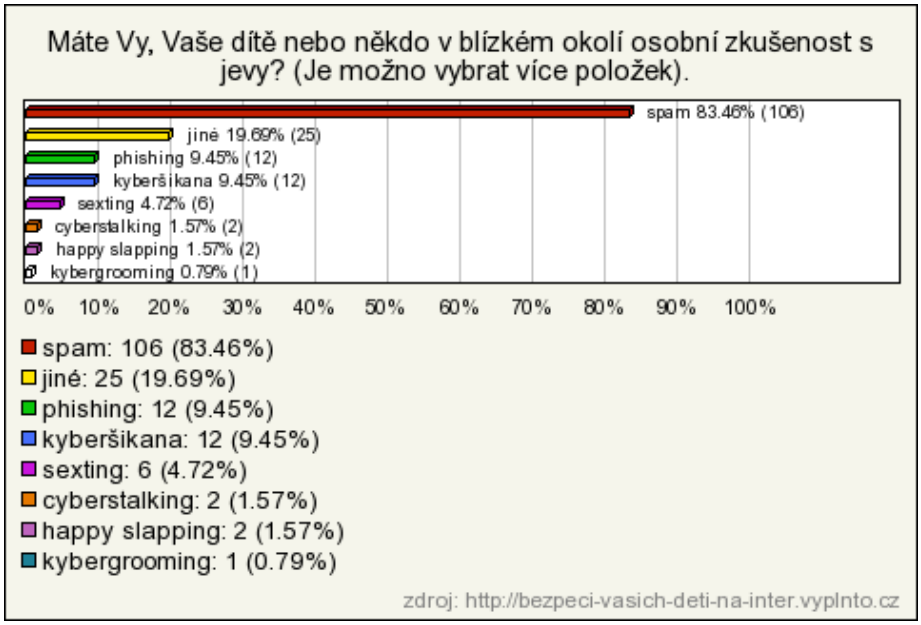
Respondenti mohli vybírat z vícero možností, přičemž nejvíce respondentů zná pojem spam 116 (91, 34 %) a pojem kyberšikana 100 (78,74 %). Dalším hodně známým pojmem byl pro respondenty pojem cyberstalking a to u 71 respondentů (55,91 %). Pojem phishing znalo 47 respondentů (37,01 %) a pojem sexting 42 respondentů (33,07 %). Pojem netholismus je znám 31 respondentům (24,41 %), pojem sociální inženýrství 29 respondentům (22,83 %) a pojem kybergrooming zná 20 respondentů (15,75 %). Význam uvedených pojmů nezná, ale někde se s nimi již setkalo 18 respondentů (14,17 %). Pojem happy slapping zná pouze 7 respondentů (5,51 %). Zajímavé by jistě bylo šetření u starší věkové hranice, která ale podle všeho stráví času u počítače méně, než zde oslovená skupina respondentů. Výsledek je podstatný pro ověření H_1.



Tabulka četností č. 3

23) **Máte Vy, Vaše dítě nebo někdo v blízkém okolí osobní zkušenost s jevy?**

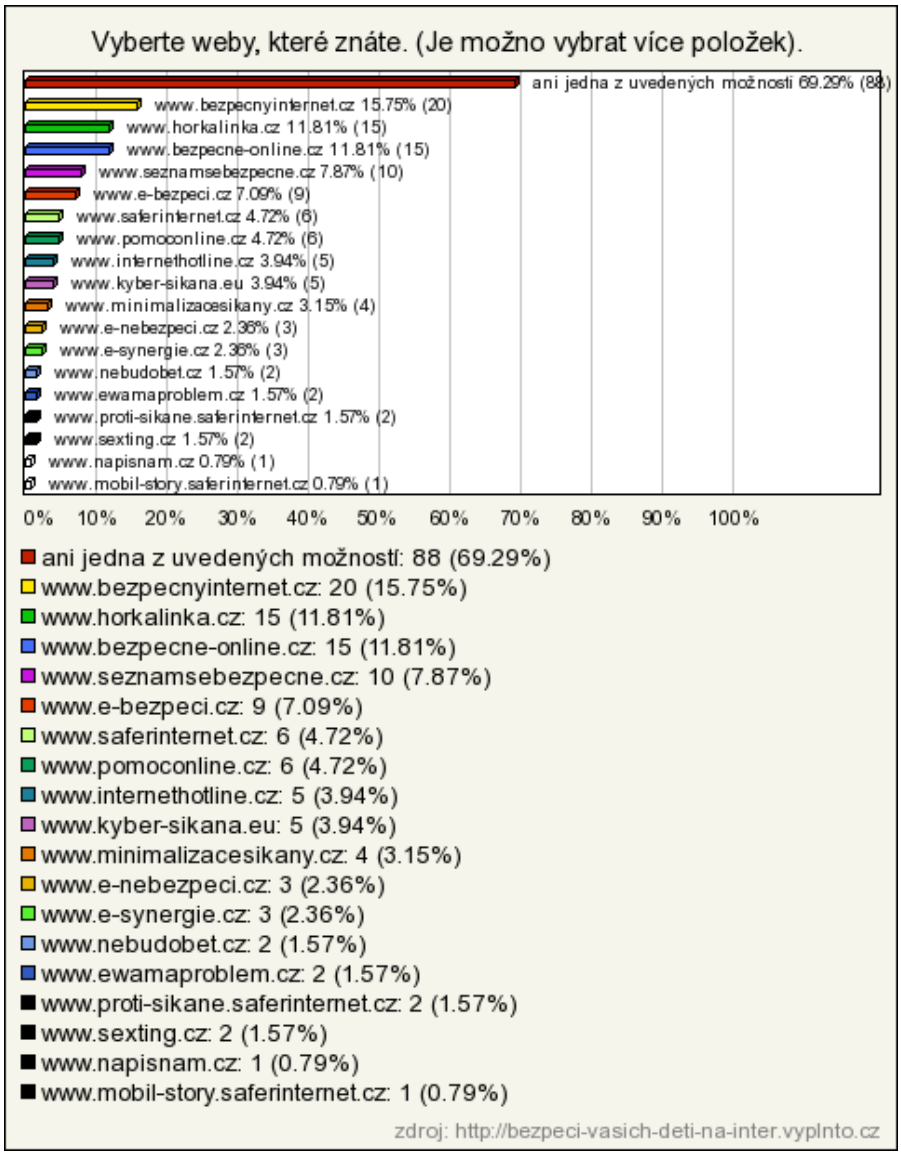
Respondenti mohli vybírat opět více možností. Se samotným jevem spam, ať osobně či z okolí, má zkušenost 106 respondentů (83,46 %). Jiný jev zažilo 25 respondentů (19,69 %). Phishing a kyberšikanu zažilo 12 respondentů (9,45 %). Sexting 6 respondentů (4,72 %). Rizikové jevy cyberstalking a happy slapping zažilo po 2 respondentech (1,57 %) a kybergrooming 1 respondent (0,79 %). Bohužel nebyla možnost „jiné“ upravena k doplnění konkrétního jevu, se kterým má respondent zkušenost, tudíž není tato zajímavá informace k dispozici.



Tabulka četností č. 4

24) **Vyberte weby, které znáte.**

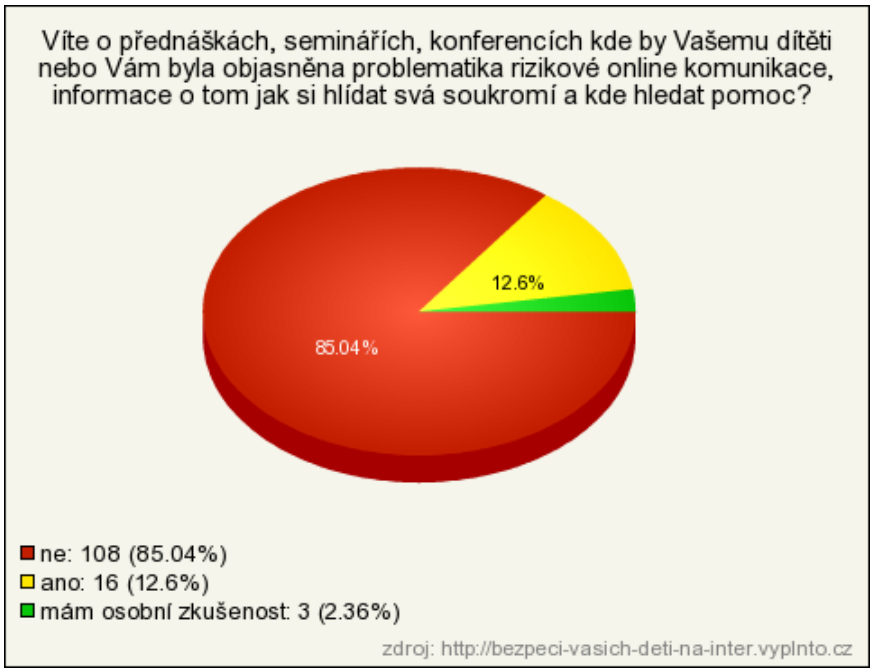
Respondenti mohli vybírat více odpovědí. Většina, přesněji 88 respondentů (69,29 %), nezná ani jeden z uvedených webů. Web www.bezpecnyinternet.cz zná 20 respondentů (15,75 %). Weby www.horkalinka.cz a www.bezpecne-online.cz pak 15 respondentů (11,81 %). Web www.seznamsebezpecne.cz zná 10 respondentů (7,87 %) a www.e-bezpeci.cz 9 respondentů (7,09 %). Weby www.saferinternet.cz a www.pomoconline.cz 6 respondentů (4,72 %) a weby www.internethotline.cz a kybersikana.eu 5 respondentů (3,94 %). Web www.minimalizacesikany.cz znají 4 respondenti (3,15 %). Weby e-nebezpeci.cz, e-synergie.cz znají 3 respondenti (2,36 %) a weby www.nebudobet.cz, www.ewamaproblem.cz, www.proti-sikane.saferinternet.cz, sexting.cz znají vždy 2 respondenti (1,57 %). Pouze po 1 respondentu (0,79 %) jsou známy weby www.napisnam.cz a www.mobil-story.safeinternet.cz. Výsledek je podstatný pro ověření H_2.



Tabulka četností č. 5

25) **Víte o přednáškách, seminářích, konferencích, kde by Vašemu dítěti nebo Vám byla objasněna problematika rizikové online komunikace, informace o tom, jak si hlídat svá soukromí a kde hledat pomoc?**

108 respondentů (85,04 %) o těchto vzdělávacích možnostech neví, 16 respondentů (12,6 %) o nich ví a 3 respondenti (2,36 %) mají s tímto vzděláváním osobní zkušenost. Výsledek je podstatný pro ověření $H_{2.}$



Graf č. 8

4.3 Ověřování hypotéz

H_1: Rodiče neznají možná rizika online komunikace na Internetu

Pro ověření nebo vyvrácení hypotézy jsem provedla analýzu otázek s čísly 13,15, 16, 17, 18, 19, 20, 21, 22. Respondenti ve 117 případech (92,13 %) informace o odjezdu na dovolenou nebo víkendový pobyt nezveřejňují. V 90 případech (70,87 %) uvádí respondenti, že vědí, jaké informace se o nich na Internetu dají dohledat. Rozdílná hesla na uživatelských profilech potvrdilo 101 respondentů (79,53). Funkci automatického pamatování hesel nepoužívá na jiném než domácím počítači 119 respondentů (93,7 %). Fotky interiéru bytu nezveřejňuje 72 respondentů (56.69 %). Své fotky na internetu nezveřejňuje 108 respondentů (85,04 %). Fotografie celé postavy svých dětí zveřejňuje 62 respondentů (48,82 %) a fotografie portrétní zveřejňuje 47 respondentů (37,01). Nevhodný a škodlivý obsah neví kde nahlásit 62 respondentů (48,82 %). Dalších 52 respondentů (40,94 %) tuto informaci má, ale možnost hlášení nikdy nevyužila. Respondenti znají nejvíce pojmy rizikových jevů spam 116 respondentů (91, 34 %), kyberšikana 100 respondentů (78,74 %), cyberstalking 71 respondentů (55,91 %).

Respondenti si hlídají své soukromí chováním dle pravidel bezpečného užívání Internetu a znají nejznámější pojmy rizikového chování na Internetu, pouze dostatečně neví, kde např. hlásit nevhodný či škodlivý obsah.

Předpokládám, že rozdílný výsledek by mohl být v jiné věkové kategorii respondentů, ale tento překlad by musel být ověřen v jiném výzkumném šetření.

Po analýze uvedených otázek se moje hypotéza nepotvrdila.

H_2: Rodiče nejsou dostatečně informováni o možnostech preventivního vzdělávání v oblasti rizikové online komunikace na Internetu

V teoretické části bakalářské práce jsem se věnovala zmapování a popisu existujících webů a projektů informující a vzdělávající v oblasti rizikové online komunikace. V otázce č. 24 více než polovina respondentů (88 respondentů 69,29 %) uvedla neznalost těchto vyjmenovaných webů. Weby www.e-bezpeči.cz a www.saferinternet.cz, které jsou na poli informovanosti, vzdělávání a výuky nejaktivnější, zná pouze minimum dotazovaných respondentů (www.e-bezpeci.cz 9 respondentů 7,09 % a www.saferinternet.cz 6 respondentů 4,72 %). V otázce č. 25 uvedla většina respondentů (108 respondentů 85,04 %) nevědomost existujících vzdělávacích programů v oblasti rizikové online komunikace. Po analýze uvedených otázek se moje hypotéza potvrdila.

4.4 Dílčí závěr

Mého šetření se zúčastnilo 127 rodičů, především ženy. Nejvíce respondentů zastupovaly věkové kategorie 21-40 let. Výběr byl proveden elektronickým oslovením a podmínkou bylo rodičovství minimálně jednoho dítěte.

Tito respondenti jsou především aktivními uživateli Internetu, návštěvníci internetových fór a sociálních sítí. Mají většinově dítě ve věku 0-6 let. Respondenti jsou převážně středoškolského vzdělání a nejvíce respondentů pochází z Jihomoravského kraje. Mají uživatelsky dobré dovednosti nastavení bezpečnostních funkcí v souvislosti s užíváním Internetu a uživatelských profilů.

Dotazník byl standardizovaný s 25 uzavřenými otázkami. Protože byl výběr proveden na základě dobrovolnosti, samovýběrem, nelze výsledky šetření zobecnit na celou populaci.

H_1: Rodiče neznají možná rizika online komunikace na Internetu

Tato hypotéza nebyla po analýze dat potvrzena.

H_2: Rodiče nejsou dostatečně informováni o možnostech preventivního vzdělávání v oblasti rizikové online komunikace na Internetu

Tato hypotéza byla po analýze dat potvrzena.

Zajímavé by zajisté byly výsledky dotazníkového výzkumu s porovnáním krajů bydliště respondentů, zda existence vzdělávacích programů v určitém kraji zvyšuje povědomí rodičů o vzdělávání. Také by bylo možným návrhem dalšího dotazníkového výzkumu zaměření se na děti a následné srovnání odpovědí. V přípravách projektu jsem původně tento záměr měla, ale během psaní bakalářské práce jsem došla k závěru, že srovnání takového rozsahu by bylo spíše předmětem diplomové práce.

Závěr

Cílem teoretické části mé bakalářské práce bylo popisné zpracování existujících vzdělávacích bezpečnostních programů v rámci internetové sítě a další související body, např. vysvětlení pojmů. Cílem empirické částí bylo zjištění, zda jsou rodiče informováni o možných rizicích online komunikace a zda vědí, že existují možnosti vzdělávání v této oblasti. Tento cíl byl podložen ověřením nebo vyvrácením stanovených hypotéz.

Po základním seznámení s historií Internetu jsem se v první části teoretického celku věnovala popisu základních sociálních sítí a komunikačních programů.

Ve druhé části práce jsem stručně vysvětlila pojmy nejčastěji se vyskytujících nebezpečí internetové komunikace.

Ve třetí části jsem podrobně monitorovala existenci vzdělávacích programů, zaměřených nejen na vzdělávání, ale i na informační prevenci různých webových projektů v rámci možných rizik internetové komunikace.

V empirické části jsem si stanovila cíl zjistit, jak jsou rodiče informovaní o možných rizicích online komunikace, a zda vědí o možnostech sebevzdělávání v programech, které se zaměřují na bezpečnost při užívání Internetu. Pro tento cíl jsem si vytvořila dvě hypotézy, přičemž jedna byla vyvrácena a druhá potvrzena.

Rodiče tedy možná rizika internetové komunikace znají, ale nejsou dostatečně informovaní, kde se v této oblasti dále vzdělávat. Jsem si vědoma, že výsledek mého šetření není zobecnitelný na celou populaci.

„Není pochyb o tom, že nevídaný rozvoj individuálních a masmediálních prostředků nepřímé sociální komunikace nám otevírá dříve nepředstavitelné možnosti získávání znalostí… Byli jsme při tom, když první člověk přistál na Měsíci, jsme při tom, když někde na Zemi vybuchla sopka, jsme informovanější, znalejší, vzdělanější. Ale současně jsme vlastně jen „jakoby“ při tom. Jsme v zajetí znakové symbolické kultury, kterou jsme si vytvořili. Jsme stále více izolováni od reálného světa.“[47]

[47] CEJPEK, J. *Informace, komunikace a myšlení*: *úvod do informační vědy*. 2. přeprac. vyd. Praha: Karolinum, 2005, s. 72. ISBN 978-80-246-1037-5.

Je zřejmé, že s přibývajícím vzděláním lidstva přicházejí na svět nové technologie, nejen v oblasti samotné techniky. Člověk je tvorem, který potřebuje pro svůj zdárný vývoj a rozvoj především komunikaci. Rozvojem Internetu se tato potřeba naplnila, komunikace může probíhat globálně bez ohledu na vzdálenosti. Mnohdy je ale tato komunikace náhražkou komunikace reálné, tedy osobní ve svém životním okolí. Různá nebezpečí skýtá reálný život, ale i tenhle nový virtuální svět. Nebezpečí nabrala novou podobu a z tohoto reálného světa se přenesla do světa virtuálního. Vždy byli, jsou a budou na jedné straně ti, co přečiny neetické nebo trestné činy páchají a ti, co jejich následky trpí. Smutné je, když se týkají dětí a ještě smutnější, mají-li závažné tragické následky.

Samotná sociální pedagogika je na pomezí obou těchto skupin. Snaží se působit preventivně, ale zároveň pomáhat resocializačně. Oblast působení sociální pedagogiky není vymezena pouze v prostorách kamenné instituce. Myslím, že je důležité věnovat pozornost těmto možným rizikům virtuálního světa stále více. Vzdělávání se v této oblasti je zásadní především pro pedagogy, odborníky spolupracující na různých projektech spojených se vzděláváním nebo osvětou, např. pro sociální pedagogy, ale mělo by být ve větším rozsahu doporučeno i rodičům. Ti mají vliv na volnočasové aktivity dětí a děti k nim mají největší důvěru v případě potíží a potřebě pomoci. Mám na mysli samozřejmě ideální situaci, bohužel takto to nebývá vždy. Pokud jsou ale rodiče dobře informováni, mohou své děti lépe chránit, a nejen své děti, ale i jejich kamarády a také sebe. Nástrahy se netýkají jen dětí, ale i dospělých.

Samotné téma je velmi rozsáhlé a skýtá mnoho možností dalších různých výzkumů a následných analýz a srovnání. V posledních letech se v oblasti tohoto konkrétního vzdělávání mnoho změnilo, tedy pozitivním směrem. Většina aktivit je spojena s dobrovolnictvím, vzájemnou spoluprácí různých týmů a podporou projektů. Mezera je dle mého především v regionální podpoře a v nedostatečném působení silnou realitou na rodiče.

Při práci jsem využila jako zdroje konkrétní weby jednotlivých poskytovatelů. Při e-mailovém oslovení se mi kontakt nepodařilo navázat, osobní kontakt nebyl pro vzdálenost možný. Internetové zdroje byly podstatou mojí práce v rámci splnění jejího cíle a byly doplněny také o literární myšlenky. Samotná práce pro mne byla nabytím informací, které mohu zúročit při výchově vlastních dětí.

Má bakalářská práce nabízí sumarizaci existence možností, kde najít informace v oblasti prevence i vzdělání v rámci rizikové internetové komunikace. Mohla by být rádcem nejen pro sociální pedagogy v oblasti školství, poraden, ale také rodičům, kterými to vše začíná a končí.

V závěru zde uvádím citaci, která dle mého názoru, velmi jednoduše, ale výstižně shrnuje dvě nejdůležitější zásady ochrany soukromí dítěte a měla by být malou inspirací či ochutnávkou vlastního rozšíření povědomí rodičů jak lze na dítě působit.

„První a prvořadé pravidlo, které je potřeba při používání služeb typu online dítěti neustále vštěpovat, je neuvádět žádné osobní informace. Žádná telefonní čísla, žádné adresy či konkrétní podrobnosti, které by komukoli umožnily zjistit, kam dítě chodí do školy, na nákup či za zábavou.

Najde-li si vaše dítě prostřednictvím Sítě nového kamaráda a poté se snaží s ním osobně sejít, vždy ho doprovoďte. K setkání by mělo dojít na místě, kam může veřejnost, kde se dá dobře pozorovat a za denního světla.“[48]

[48] KEHOE, B. P. *ZEN a umění Internetu*. 1. vyd. Praha: BEN, c1997, s. 116. ISBN 80-86056-31-7.

Resumé

Téma mé bakalářské práce je „Preventivní bezpečnostní programy v rámci internetové sítě“. Hlavním cílem teoretické části bylo zmapování existence vzdělávacích bezpečnostních programů v rámci internetové sítě. Toto bylo doplněno o historii a vysvětlení souvisejících pojmů v oblasti sociálních sítí a komunikačních programů. Část práce byla věnována rizikovým jevům v rámci internetové komunikace. Cílem empirické částí bylo na základě potvrzení nebo vyvrácení hypotéz zjištění, jsou-li rodiče informováni o možných rizicích online komunikace a existenci vzdělávání v této oblasti.

Po základním seznámení s historií Internetu jsem se v první části teoretického celku věnovala popisu základních sociálních sítí a komunikačních programů. Ve druhé části práce jsem stručně vysvětlila pojmy nejčastěji se vyskytujících nebezpečí internetové komunikace. Ve třetí části jsem podrobně monitorovala existenci vzdělávacích programů, zaměřených nejen na vzdělávání, ale i na informační prevenci různých webových projektů v rámci možných rizik internetové komunikace. V empirické části jsem si stanovila cíl zjistit, jak jsou rodiče informováni o možných rizicích online komunikace a zda ví o možnostech sebevzdělávání v programech, které se zaměřují na bezpečnost při užívání internetu. Pro tento cíl jsem si vytvořila dvě hypotézy, přičemž jedna byla vyvrácena a druhá potvrzena. Rodiče možná rizika internetové komunikace znají, ale nejsou dostatečně informováni o tom, kde se dále vzdělávat.

Téma jsem si zvolila z důvodu vlastního zájmu o danou problematiku. Myslím, že je aktuální, a především rizika virtuálního světa budou nadále stoupat s rozvojem technologií.

Za podstatné považuji se neustále v dané oblasti vzdělávat pro zabezpečení vlastního soukromí a k ochraně sebe, rodiny před možnými negativními jevy. V případě poškození ke snížení rozsahu následků nebo vzájemné pomoci. Vzdělávání v rámci internetové komunikace by dle mého názoru mělo být také součástí osnov povinné školní docházky.

Anotace

Téma bakalářské práce je „Preventivní bezpečnostní programy v rámci internetové sítě“. Účinná ochrana před rizikovými jevy je spojena se vzděláváním formou samostudia nebo pod vedením odborníků. Teoretická část práce se věnuje historii Internetu, vysvětlení pojmů z oblasti sociálních sítí, komunikačních programů a rizikových jevů. Podstatou je zmapování existence webů, které se dané problematice věnují, ať již na úrovni informací nebo vzdělávání. V praktické části za pomoci kvantitativní metody sběru dat zjišťuji, zda jsou rodiče o možných rizicích internetové komunikace informování a zda vědí, kde se v dané oblasti mohou preventivně vzdělávat. Analýzou dat jsem zjistila, že rodiče informovaní jsou, ale nevědí, kde se mohou dále vzdělávat. Výsledky nejsou zobecnitelné na celou populaci.

Klíčová slova

Internet, sociální síť, kybernetická bezpečnost, virtuální svět, komunikace.

Annotation

The chosen topic of my thesis is "Preventive safety programs in the Internet network." This issue is currently associated with the rapid development of information technology. The communication in the online environment has been accompanied by hazardous socio-pathological phenomena. They threaten us, our immediate and surrounding area. Effective protection of private persons is associated with the need for self-education through or under the guidance of experts. The theoretical part is devoted to the history of the Internet, explains the concepts of social networks, and risk communication programs. The essence is to map the existence of websites that are devoted to the issue at the level of information or education. In the practical part, using quantitative methods of data collection, namely a standardized questionnaire, we try to find out whether the parents have knowledge about the potential risks of Internet communication and where they can get the information about safety prevention. In analyzing the data we found, parents are informed, but do not know where they can continue to educate. The results are not generalizable to the entire population.

Keywords

Internet, social network, cyber security, virtual world, communications.

Seznam použité literatury

1. BUERMANN, U. *Jak (pře)žít s médii*: *příležitosti a hrozby informačního věku a nové úkoly pedagogiky*. Vyd. 1. Hranice: Fabula, 2009, s. 239. ISBN 9-788086-600581.

2. CEJPEK, J. *Informace, komunikace a myšlení*: *úvod do informační vědy*. 2. přeprac. vyd. Praha: Karolinum, 2005, s. 233. ISBN 978-80-246-1037-5.

3. ČERMÁK, M. *Nikomu to neříkejte!, (aneb, Proč píšu Internet s velkým písmenem na začátku)*. 1. vyd. Praha: Extra Média, 2008, s. 171. ISBN 978-80-903994-6-4.

4. DISMAN, M. *Jak se vyrábí sociologická znalost*: *Příručka pro uživatele*. 3.vyd. Praha: Karolinum, 2000, s. 372. ISBN 978-80-246-0139-7.

5. HORSKÁ, B., LÁSKOVÁ A. a PTÁČEK L. *Internet jako cesta pomoci*: *internetové poradenství pro pomáhající profese*. Vyd. 1. Praha: Sociologické nakladatelství (SLON), 2010, s. 197. Studijní texty (Sociologické nakladatelství), sv. 49.
ISBN 978-80-7419-034-6.

6. JIROVSKÝ, V. *Kybernetická kriminalita*: *nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, s. 284.
ISBN 978-80-247-1561-2.

7. KEHOE, B. P. *ZEN a umění Internetu*. 1. vyd. Praha: BEN, c1997, s. 168.
ISBN 80-86056-31-7.

8. KRÁL, M. *Bezpečnost domácího počítače*: *prakticky a názorně*. 1. vyd. Praha: Grada, 2006, s. 334. ISBN 80-247-1408-6.

9. NEŠPOR, K. *Počítače a zdraví*. Vyd. 1. Praha: BEN, 1999, s. 96.
ISBN 80-86056-71-6.

10. REICHEL, J. *Kapitoly metodologie sociálních výzkumů*. Vyd. 1. Praha: Grada, 2009, s. 184. Sociologie (Grada). ISBN 978-80-247-3006-6.

11. ŠMAHEL, D. *Psychologie a internet*: *děti dospělými, dospělí dětmi*. Praha: Triton, 2003, s. 158. Psychologická setkávání, sv. 6. ISBN 80-7254-360-1.

Odkazový a poznámkový aparát

VRABEC, V. Co bylo, než vznikl český Internet?: Historie Internetu. *Lupa.cz* [online]. 13. 8. 2002 [cit. 2012-03-12].
Dostupné z: http://www.lupa.cz/clanky/co-bylo-nez-vznikl-cesky-internet/

PETERKA, J. Internet u nás: Internet. *EArchiv.cz* [online]. 1995 [cit. 2012-03-12].
Dostupné z: http://www.earchiv.cz/a95/a504c504.php3

PETERKA, J. Kolikáté narozeniny slaví Internet?. *Lupa.cz* [online]. 6. 1. 2003 [cit. 2012-03-12]. Dostupné z: www.lupa.cz/clanky/kolikate-narozeniny-slavi-internet

Sociální sítě. *Socialnisite.123abc.cz* [online]. 2011 [cit. 2012-03-12].
Dostupné z: http://www.socialnisite.123abc.cz

FAQ-PC Help: Programy pro internetovou komunikaci. *PC-HELP.cz*: *České diskuzní fórum* [online]. 2006 [cit. 2012-03-12].
Dostupné z: http://www.pc-help.cz/viewtopic.php?f=72&t=6891

Nebezpečné komunikační praktiky. *E-bezpeci.cz* [online]. 2010 [cit. 2012-03-12].
Dostupné z: http://cms.e-bezpeci.cz/content/blogcategory/33/54/lang,czech/

RYLICH, J. Second Life – život ve virtuální realitě. *Lupa.cz* [online]. 17. 5. 2007 [cit. 2012-03-12].
Dostupné z: http://www.lupa.cz/clanky/second-life-8211-zivot-ve-virtualni-realite/

Nebuď oběť!: *Rizika Internetu a komunikačních technologií o.s.* [online]. 2010 [cit. 2012-03-12]. Dostupné z: http://nebudobet.cz/

Centrum prevence rizikové virtuální komunikace [online]. 2012 [cit. 2012-03-12].
Dostupné z: http://www.prvok.upol.cz/

E-bezpečí [online]. 2012 [cit. 2012-03-12]. Dostupné z: http://www.e-bezpeci.cz/

O projektu. *E-Synergie*: *vědeckovýzkumná síť pro rizika elektronické komunikace* [online]. 2011 [cit. 2012-03-12]. Dostupné z: http://esynergie.upol.cz/

Poradna E-Bezpečí. *Poradna E-Bezpečí*: *pro oblast rizikové chování na internetu* [online]. 2008 [cit. 2012-03-12]. Dostupné z: http://napisnam.cz/

O projektu. *E-nebezpečí pro učitele* [online]. 2010 [cit. 2012-03-12].
Dostupné z: http://e-nebezpeci.cz/

Klikni. *Sexting.cz*: *nebezpečný fenomén* [online]. 2009 [cit. 2012-03-12].
Dostupné z: http://sexting.cz/

O nás. *Saferinternet.cz*: *... pro bezpečnější internet* [online]. 2011 [cit. 2012-03-12].
Dostupné z: http://www.saferinternet.cz/

Jsi na internetu jako doma?. *Bezpečně-online.cz* [online]. 2011 [cit. 2012-03-12]. Dostupné z: http://www.bezpecne-online.cz/

Horká linka. *Horká linka.cz*: *bojujeme proti internetové kriminalitě* [online]. 2012 [cit. 2012-03-12]. Dostupné z: www.horka-linka.saferinternet.cz

INHOPE Homepage. *INHOPE*: *International Association of Internet Hotlines* [online]. 2010 [cit. 2012-03-12]. Dostupné z: http://www.inhope.org/gns/home.aspx

Linka bezpečí: Úvodní strana. *Pomoconline.cz*: *Pomáháme dětským obětem internetové kriminality* [online]. 2010 [cit. 2012-03-12]. Dostupné z: www.pomoc-online.saferinternet.cz

Nebuď oběť!: Novinky. *Nebuď oběť!*: *Rizika Internetu a komunikačních technologií o.s.* [online]. 2010 [cit. 2012-03-12]. Dostupné z: http://www.nebudobet.cz/

Šikana: projekt Minimalizace šikany. *Minimalizace šikany*: *Informační portál o šikaně na školách* [online]. 2008 [cit. 2012-03-12]. Dostupné z: http://www.minimalizacesikany.cz/

KOPECKÝ, K. Stručný úvod do problematiky bezpečného internetu: Základní vzdělávání. In: *Metodický portál*: *inspirace a zkušenosti učitelů* [online]. 22. 10. 2010 [cit. 2012-03-12]. Dostupné z: http://clanky.rvp.cz/clanek/c/Z/9673/strucny-uvod-do-problematiky-bezpecneho-internetu.html/

Vítejte na našich internetových stránkách: Aktuální informace. *Komunikační výchova*: *Příprava a realizace výukových materiálů* [online]. 2009 [cit. 2012-03-12]. Dostupné z: http://www.komunikacnivychova.upol.cz/

Internetová ambasáda: Novinky. *Internetová ambasáda* [online]. 2011 [cit. 2012-03-12]. Dostupné z: www.internetembassy.cz

Bezpečný internet. *Bezpečný internet.cz*: *Rady pro vaši bezpečnost* [online]. 2011 [cit. 2012-03-12]. Dostupné z: http://www.bezpecnyinternet.cz/

Internet Hotline Nadace Naše dítě: Smysl a význam Internethotline.cz. *Internet Hotline.cz* [online]. 2009 [cit. 2012-03-12]. Dostupné z: www.internethotline.cz

Vítejte. *Kyberšikana.cz*: *kyber-sikana.eu, cyberbullying.eu* [online]. 2012 [cit. 2012-03-12]. Dostupné z: www.kyber-sikana.eu

Ewa má problém. *Ewa má problém.cz* [online]. 2009 [cit. 2012-03-12]. Dostupné z: www.ewamaproblem.cz

Úvodní strana. *Mobilstory.cz*: *Používáme mobil bezpečně* [online]. 2011 [cit. 2012-03-12]. Dostupné z: www.mobil-story.saferinternet.cz

Domů. *Seznam se bezpečně.cz*: *Jsou děti na internetu v bezpečí?* [online]. 2011, 2012 [cit. 2012-03-12]. Dostupné z: www.seznamsebezpecne.cz

Úvodní strana. *Saferinternet.cz*: *Národní centrum bezpečnějšího internetu* [online]. 2009 [cit. 2012-03-12]. Dostupné z: www.proti-sikane.saferinternet.cz

Mediální osvětová kampaň "Skrytá identita": O kampani. In: *Bezpecne-online.cz*: *Skrytá identita* [online]. 2012 [cit. 2012-03-12].
Dostupné z: http://www.bezpecne-online.cz/skryta-identita

O konferenci: Úvod. *Mezinárodní vědecká konference*: *Rizika internetové komunikace* [online]. 2010, 2012 [cit. 2012-03-12]. Dostupné z: www.konference.e-bezpeci.cz

Aktivity: Safer Internet Day 2012. In: *Saferinternet.cz*: *... pro bezpečnější internet* [online]. 2007, 2012 [cit. 2012-03-12].
Dostupné z: http://www.saferinternet.cz/sid-2012

REDAKCE. Trendy v bezpečnosti 2012: soukromí, Facebook, mobilní platby a stará dobrá havěť. In: *Lupa.cz* [online]. 2. 3. 2012 [cit. 2012-03-12].
Dostupné z: http://www.lupa.cz/clanky/trendy-v-bezpecnosti-2012-soukromi-facebook-mobilni-platby-a-stara-dobra-havet/

PIRÁTI. Piráti odmítají chystaný zákon o kybernetické bezpečnosti: Tisková zpráva České pirátské strany ze dne 2. března 2012. In: *Pirátské noviny.cz* [online]. 2. 3. 2012 [cit. 2012-03-12]. Dostupné z: http://piratskenoviny.cz/?c_id=33650

Seznam symbolů a zkratek

ARPA - Advanced Research Projects Agency

ARPANET - Advanced Research Projects Agency Network

CERN - Conseil Européen pour la recherche nucléaire

CESES - Centrum pro sociální a ekonomické strategie

CESNET - Czech Educational and Scientific Network

cit. - citováno

CSIRT - Computer Security Incident Response Team

CZ.NIC - Správce domén

ČR - Česká republika

ČVUT - České vysoké učení technické v Praze

DVPP - Další vzdělávání pedagogických pracovníků

EARN - European Academic and Research Network

ERA - Poštovní spořitelna Era účet

EUnet - Správce domén

FAQ - Frequently Asked Questions

FESNET - Federal Educational and Scientific Network

FTP - File Transfer Protocol

H - Hypotéza

IBM - International Business Machines Corporation

ICL-4-72 - Střediskový počítač

ICM - Informační centrum pro mládež

ICQ - I Seek You

ICT - Information and Communication Technologies

IM - Instant messaging

INHOPE - Mezinárodní asociace internetových horkých linek

INSAFE - Evropská síť osvětových center

IP - Internet Protocol

ISBN - International Standard Book Number

IT - Information technology

LMS Unifor - Learning Management System

MILNET - Military Network

MiŠ - Minimalizace šikany

MSN - The Microsoft Network

MŠMT - Ministerstvo školství, mládeže a tělovýchovy
MVČR - Ministerstvo vnitra České republiky
NAEP - Národní agentura pro evropské vzdělávací programy
NCBI - Národní centrum bezpečnějšího internetu
NCP - Network Control Protocol
NIDM - Národní institut dětí a mládeže
PC - Personal computer
PdF - Pedagogická fakulta
PIS - Preventivně informační oddělení
PRVoK - Centrum prevence rizikové virtuální komunikace
Přeprac. - Přepracováno
RFC - Request for comments
RIK - Konference Rizika internetové komunikace
RVP ZV - Metodický portál
RWE - Německá energetická společnost
s. - strana
Sb. - Sbírka zákonů
SID - Safer Internet Day
SL - Second Life
SMS - Short message service
SOŠE - Střední odborná škola elektrotechnická
SOU - Střední odporné učiliště
SRI - Stanford Research Institute
SŠ - Střední škola
TCP/IP - Transmission Control Protocol/Internet Protocol
tzv. - takzvaně
UCLA - University of California Los Angeles
UCSB - University of California Santa Barbara
UK - Univerzita Karlova
UP - Univerzita Palackého v Olomouci
UPC - Provozovatel telekomunikačních služeb v ČR
USA - United States of America
ÚŠI - Ústav školských informací
VoIP - Voice over Internet Protocol
VŠE - Vysoká škola ekonomická

Vyd. - Vydání

WWW - World Wide Web

ZŠ - Základní škola

.com - specifikace domény

.cz - specifikace domény

.fm - specifikace domény

.net - specifikace domény

.org - specifikace domény

Seznam příloh

Příloha č. 1: Dotazník

Milí rodičové,

dovoluji si Vás požádat o vyplnění tohoto dotazníku, který je určen rodičům s minimálně jedním dítětem.

Získané údaje budou především podkladem pro zpracování praktické části mojí bakalářské práce na téma „Preventivní bezpečnostní programy v rámci internetové sítě“. **Cílem dotazníku je zjistit údaje o informovanosti rodičů v rámci bezpečnosti internetové komunikace.**

Děkuji za Váš čas a ochotu k vyplnění dotazníku. Děkuji i těm, kteří dotazník doporučí k vyplnění dalším rodičům ☺

1) Jste?

- žena
- muž

2) Kolik je vám let?

- 16-20
- 21-30
- 31-40
- 41-50
- 51 a více

3) Jaké je Vaše nejvyšší dosažené vzdělání?

- základní
- středoškolské
- vysokoškolské

4) Jste momentálně na mateřské dovolené?

- ano
- ne

5) Místo Vašeho bydliště?

- Praha
- Středočeský
- Ústecký
- Jihomoravský
- Pardubický
- Královéhradecký
- Vysočina
- Zlínský
- Moravskoslezský
- Plzeňský
- Olomoucký
- Karlovarský
- Liberecký
- Jihočeský
- Zahraničí

6) Kolik máte dětí?

- 1
- 2
- 3 a více

7) Věk Vašeho dítěte? (V případě, že máte víc než 1 dítě, vyplňte prosím tuto informaci vztažnou k dítěti, které stráví u počítače nejvíce času)

- 0-6
- 7-12
- 13-17
- 18 a více

8) Hlídají Vaše děti minimálně 1x týdně po dobu minimálně 2 hodin jiní rodinní příslušníci?

- ano
- ne

9) Kolik času průměrně denně Vaše dítě stráví u počítače mimo aktivit spojených se školou? (V případě, že máte víc než 1 dítě, vyplňte prosím tuto informaci vztažnou k dítěti, které stráví u počítače nejvíce času)

- počítač zatím neovládá
- nevím
- 0-3 hodiny
- 4-6 hodin
- 7 hodin a více

- **10) Víte co dělají Vaše děti na počítači mimo školních povinností? (Je možno vybrat více položek)**
- počítač moje dítě zatím neovládá
- nevím
- chatování (např. přes ICQ) a telefonování (např. přes Skype)
- hledání informací
- stahování souborů (hudba, filmy)
- sociální sítě a fóra (např. Facebook.com, Lide.cz, Spoluzaci.cz)
- prohlížení a ukládání fotek a videí (např. Rajce.cz, Youtube.cz)

11) Používá Vaše dítě při online komunikaci webkameru?

- nevím
- ano
- ne

12) Jaké jsou Vaše počítačové dovednosti?

- žádné, počítač neumím ani zapnout
- minimální
- uživatelsky dobré, ale neumím nastavit bezpečnostní prvky
- uživatelsky dobré a umím nastavit i některé bezpečnostní prvky
- profesionální úroveň a umím nastavit veškeré bezpečnostní prvky

13) Zveřejňujete na Internetu informace o odjezdu na dovolenou nebo víkendový pobyt?

- ano
- ne

14) Využíváte sociální síť Facebook?

- ne
- ano, ale neumím nastavit soukromí uživatelského profilu
- ano a umím nastavit soukromí uživatelského profilu

15) Víte, jaké informace se o Vás dají na Internetu dohledat?

- ano
- ne

16) Máte rozdílná hesla na různých uživatelských profilech?

- ano
- ne

- **17) Používáte funkci automatického pamatování hesel na jiném než domácím počítači?**
- ano
- ne

18) Zveřejňujete fotky interiéru na Internetu?

- ano, ale jen skupině povolených uživatelů na základě přístupu přes heslo
- ano
- ne

19) Zveřejňujete svoje fotky na Internetu? (Je možno vybrat více položek).

- celá postava v plavkách
- fotografie, kde jsem nahá/ý
- fotografie, kde jsem nahá/ý, ale pouze s přístupem přes heslo nebo se jedná o uzamčené fórum
- ani jedna z uvedených možností

20) Zveřejňujete fotky Vašeho dítěte na Internetu? (Je možno vybrat více položek)

- portrét
- celá postava (tělíčko) v oblečení
- celá postava v plavkách
- fotografie, kde je nahé (např. koupel ve vaně, fotky od moře)
- fotografie, kde je nahé (např. koupel ve vaně, fotky od moře), ale pouze s přístupem přes heslo nebo se jedná o uzamčené fórum
- všechny fotografie mých dětí zveřejňuji pouze s přístupem přes heslo nebo se jedná o uzamčené fórum
- ani jedna z uvedených možností

21) Víte kde lze na Internetu nahlásit nevhodný nebo škodlivý obsah?

- ano vím, ale nikdy jsem toho nevyužil/a
- ano vím a už jsem to i využil/a
- nevím

22) Znám a vím co je pojem. (Je možno vybrat více položek)

- spam
- phishing
- kyberšikana
- happy slapping
- sexting
- cyberstalking
- kybergrooming
- sociální inženýrství
- netholismus
- význam uvedených pojmů neznám, ale některé názvy jsem již někde slyšel/a, četl/a

- **23) Máte Vy, Vaše dítě nebo někdo v blízkém okolí osobní zkušenost s jevy? (Je možno vybrat více položek)**
- spam
- phishing
- kyberšikana
- happy slapping
- sexting
- cyberstalking
- kybergrooming
- jiné

24) Vyberte weby, které znáte. (Je možno vybrat více položek)

- www.e-bezpeci.cz
- www.e-nebezpeci.cz
- www.e-synergie.cz
- www.sexting.cz
- www.napisnam.cz
- www.saferinternet.cz
- www.bezpecne-online.cz
- www.horkalinka.cz
- www.pomoconline.cz
- www.nebudobet.cz
- www.minimalizacesikany.cz
- www.bezpecnyinternet.cz
- www.internethotline.cz
- www.kyber-sikana.eu
- www.ewamaproblem.cz
- www.mobil-story.saferinternet.cz
- www.seznamsebezpecne.cz
- www.proti-sikane.saferinternet.cz
- ani jedna z uvedených možností

25) Víte o přednáškách, seminářích, konferencích, kde by Vašemu dítěti nebo Vám byla objasněna problematika rizikové online komunikace, informace o tom, jak si hlídat svá soukromí a kde hledat pomoc?

- ano
- mám osobní zkušenost
  nevím

V případě dotazů, připomínek nebo zájmu o výslednou práci mne prosím kontaktujte na emailu: pelcova.monika@email.cz.

Všem přeji pěkný den,

Pelcová Monika

Příloha č. 2: Leták E-bezpečí

Příloha č. 3: Virtuální Centrum PRVoK v Second Life