Pedagogická fakulta
Faculty of Education
Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta
Katedra informatiky

Bakalářská práce

Výukové materiály pro prevenci nežádoucích e-jevů působících na děti ve školách i domácím prostředí

Vypracoval: Jan Kopecký
Vedoucí práce: RNDr. Hana Havelková

České Budějovice 2013

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a všechny citace a prameny řádně vyznačil v textu. Veškerou použitou literaturu a podkladové materiály uvádím v přiloženém seznamu literatury. Současně souhlasím s tím, aby tato práce byla zpřístupněna v knihovně MUP a používána ke studijním účelům v souladu s autorským právem.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v plném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě, elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly, v souladu s uvedeným ustanovením zákona č. 111/1998 Sb., zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích, dne ……..……. ……

Jan Kopecký

Poděkování

Za odbornou pomoc při zpracování předkládané práce chci na tomto místě poděkovat vedoucí práce paní RNDr. Haně Havelkové.

Úvod 1
Teoretická část 3
1 Komunikace v prostředí Internetu 3
1.1 Elektronická komunikace 3
1.1.1 Asynchronní komunikace 3
1.1.2 Synchronní komunikace 3
1.2 Komunikační technologie 4
1.2.1 Chat 4
1.2.2 Elektronická pošta 4
1.2.3 Instant Messaging 6
1.2.4 VoIP 7
1.2.5 Sociální sítě 7
1.3 Virtuální prostředí 9
2 Nežádoucí jevy 11
2.1 Obecná problematika 11
2.2 Kyberšikana 11
2.2.1 Co je to kyberšikana 11
2.2.2 Nejčastější projevy 13
2.2.3 Čím se vyznačuje 13
2.2.4 Kde se vyskytuje 15
2.2.5 Důvody ke vzniku 16
2.2.6 Prevence před kyberšikanou 17
2.2.7 Následky 17
2.3 Kybergrooming 19
2.3.1 Co je to kybergrooming 19
2.3.2 Čím se vyznačuje 19
2.3.3 Kde se vyskytuje 21
2.3.4 Následky 22
2.4 Kyberstalking 22
2.4.1 Co je to kyberstalking 22
2.4.2 Nejčastější projevy 23

2.4.3 Čím se vyznačuje ... 24
2.4.4 Důvody ke vzniku ... 24
2.5 Sexting ... 26
2.5.1 Co je to sexting ... 26
2.5.2 Nejčastější projevy ... 26
2.5.3 Čím se vyznačuje ... 27
2.6 Ostatní nebezpečí ... 28
2.6.1 Počítačové viry ... 28
2.6.2 Spyware ... 28
2.6.3 Adware ... 29
2.6.4 Spam ... 29
2.6.5 Phishing ... 30
2.6.6 Sociální inženýrství ... 31
2.6.7 Hoax ... 31
2.6.8 SMS Spoofing ... 31
2.7 Prevence ... 32
3 Portály a projekty ... 34
3.1 Seznam se bezpečně ... 34
3.2 E-bezpečí ... 34
3.3 E-nebezpečí ... 35
3.4 Saferinternet ... 36
3.5 Bílý kruh bezpečí ... 36
Praktická část ... 37
4 Cíle a metodika práce ... 37
4.1 Cíl práce ... 37
4.1.1 Primární cíle ... 37
4.1.2 Sekundární cíle ... 37
4.2 Metodika ... 37
4.3 Zdroje informací ... 38
4.3.1 Primární zdroje dat ... 38
4.3.2 Sekundárná zdroje dat ... 38

5 Stanovení hypotéz 39
6 Dotazníky 42
6.1 Příprava a realizace dotazníkového šetření 42
6.2 Vyhodnocení prvního dotazníkového šetření 43
6.3 Vyhodnocení druhého dotazníkového šetření 48
7 Ověření hypotéz 50
8 Tvorba výukového materiálu 55
8.1 Volba programu pro vývoj 55
8.2 Struktura programu 56
8.3 Návrh grafického prostředí 57
8.4 Příprava dat 59
8.5 Zhodnocení 59
9 Návrh možných preventivních opatření 60
9.1 Opatření pro rodiče 60
9.2 Opatření pro studenty 61
10 Závěr 62
11 Přehled použité literatury 64
12 Přílohy 67
12.1 Seznam tabulek 67
12.2 Seznam grafů 67
12.3 Seznam obrázků 67
12.4 Použité vzorce pro ověření hypotéz 68
12.5 Dotazníky 70

Úvod

S rozvojem internetu a komunikace, kterou nám poskytuje, se rozmáhá i internetová kriminalita. Tento pojem je poměrně nový. Mnozí lidé ani netuší, jaká nebezpečí na ně v prostředí internetu čekají. Pro omezení šíření internetové kriminality je nutno informovat uživatele o možných rizicích. Proto je velmi důležité před používáním určité služby seznámit uživatele s možnými riziky. Uvést, jak se před napadením bránit a jaká podniknout bezpečností opatření. Pro uživatele, kteří se do potíží dostali, je nutné uvedení řešení vzniklých situací. Také je nutné uvedení míst či osob, na které se v případě potíží mohou obrátit.

Portál e-nebezpeci poukazuje i na nízkou informovanost učitelů: *„Učitelé mají v současnosti o sociálně-patologických jevech spojených s ICT velmi málo informací, jsou odkázáni na informace z médií, případně ze specializovaných zdrojů (ty však neposkytují systematickou edukaci). Učitelé navíc nevědí, jak v případných krizových situacích reagovat, které instituce zabezpečují řešení problémových situací, jak postupovat, v jakém případě se obrátit na Policii ČR apod.“*[1].

Obecně platí, že schopnost přizpůsobovat se novým technologiím je bližší dětem než dospělým, neboť objevování je nedílnou součástí jejich života. Děti se s novinkami virtuálního světa seznamují rychleji než dospělí, kteří mají svůj čas vázaný na jiné aktivity a na ono objevování jim už tolik času a energie nezbývá. Rodiče většinou nemají čas neustále zjišťovat, jaké nové služby virtuální prostředí poskytuje, jak fungují nebo jakými pravidly se řídí. O dané problematice tak mají méně informací než děti, což jim značně ztěžuje jejich pozici v oblasti prevence. O tom, co by se jejich dítěti ve virtuálním světě mohlo stát nebo jaký problém může způsobit, se tak mnohdy dovídají až ve chvíli, kdy tato situace opravdu nastane a oni jsou nuceni hledat řešení.

---

[1] E-bezpeci. *Další témata* [online]. 2008 [cit. 2013-01-18]. Dostupné z: http://www.e-bezpeci.cz

V této bakalářské práci se budu zabývat prevencí nežádoucích jevů působících na děti ve škole, ale i v domácím prostředí. O většině nebezpečí, které v prostředí internetu na děti čekají, nemá veřejnost dostatek informací. Pachatelé neinformovanosti využívají ke svému prospěchu, a proto bych chtěl upozornit na mnohá nebezpečí, která se v prostředí internetu vyskytují.

Bakalářská práce je rozdělena do dvou částí: na část teoretickou a praktickou. Teoretická část je rozdělena do více částí.

V první části teorie se zabývám specifikací internetové komunikace, elektronické komunikace i virtuálním prostředím. Uvádím zde přehled komunikačních technologií, jež jsou nejčastěji prostředkem internetové kriminality. Ve druhé části uvádím nejčastěji se vyskytující nežádoucí jevy v prostředí internetu. Dále se zaměřím na jednotlivé pojmy. Poukazuji, čím se vyznačují, jak dané útoky probíhají a jaké následky sebou nesou na obětech. Ke konci druhé kapitoly uvádím obecnou prevenci proti těmto jevům. V poslední teoretické části představuji internetové portály, jež se v současné době zabývají danou problematikou.

V praktické části proběhne marketingové šetření. Na základě provedeného terénního šetření dojde k vymezení negativních jevů působících na děti prostřednictvím internetu. Dále vymezení míry uvědomění potenciálního nebezpečí včetně četnosti i druhy jevů, s nimiž se respondenti skutečně setkali. Na základě vyhodnocení zjištěných dat z terénního šetření dojde k navržení možných preventivních řešení.

Teoretická část

1 Komunikace v prostředí Internetu

S velmi rychle se rozvíjejícím a rozšiřujícím internetem jsou stále více kladeny nároky na komunikaci. Především je důraz kladen na hlasovou, video komunikaci, ale i na textovou komunikaci. S novými technologiemi se stále zdokonaluje rychlost a kvalita přenosu, také se snižuje časová odezva.

1.1 Elektronická komunikace

Jako elektronická komunikace je považována komunikace prostřednictvím počítačových sítí. Do této komunikace lze zařadit internet, ale může sem patřit i komunikace prostřednictvím mobilních telefonů atd.

1.1.1 Asynchronní komunikace

Během asynchronní komunikace komunikují uživatelé bez okamžité odezvy. Komunikace nemá odezvu v reálném čase. Zpráva je odeslána a čeká, až si ji příjemce vyzvedne. Příkladem asynchronní komunikace je například e-mail, SMS zpráva, různé fórum a webové nástěnky.

1.1.2 Synchronní komunikace

Během synchronní komunikace komunikují uživatelé s okamžitou odezvou v reálném čase. Tedy oba uživatelé, jež spolu komunikují, musí být ve stejnou dobu online (přítomní). Synchronní komunikace je realizována prostřednictvím mobilní nebo počítačové sítě, do takovéto komunikace můžeme zahrnout například IM, chat, internetové či mobilní telefonování, Facebook chat, Windows Messenger, Twitter, MySpace, Team Speak, apod.[2]

[2] KOPECKÝ, Kamil. *Moderní trendy v e-komunikaci*. Olomouc: Hanex, 2007, 98 s. ISBN 978-808-5783-780.

1.2 Komunikační technologie

1.2.1 Chat

Chat patří mezi druhy online internetové komunikace. Svůj vzestup zaznamenal tento druh komunikace zejména na přelomu tisíciletí, kdy ho využívalo velké množství mladých lidí. Pro zapojení se do chatu lze použít portál, z českých portálů například www.xchat.cz nebo www.lide.cz. Na některém z konkrétních portálů si uživatel vybere „konferenční místnost" (místo v prostředí internetu, kde lidé se stejnými zájmy či koníčky provozují konverzaci, vystupují zde pod svým jménem, nebo uživatelskou přezdívkou)[3]. V dnešní době se ke klasickému chatu přidala i audio komunikace a video komunikace - videochat a audiochat. Mezi hlavní představitele audio chatu se řadí TeamSpeak, Mumble a Ventrilo.[4]

1.2.2 Elektronická pošta

E-mail neboli elektronická pošta je určena pro zasílání textových zpráv s možností přidání přílohy. Zasílání zpráv je realizováno mezi počítači elektronickou cestou.[5]

První e-mail byl odeslán pracovníkem firmy Bolt Beranek Newmann a to R. Tomlinsonem v roce 1971. E-mail byl součástí výzkumu firmy pro americkou vládu, projekt se jmenoval ARPANET.[6]

---

[3] PROCHÁZKA, David. *První kroky s internetem*. 3., aktualiz. vyd. Praha: Grada, 2010, 108 s. Snadno a rychle (Grada). ISBN 978-80-247-3255-8.

[4] JONES, Dennis. *Jak využívat Internet*. Praha: SoftPress, c2001, 398 s. ISBN 80-864-9712-7.

[5] VITOVSKÝ, Antonín. *Anglicko-český a česko-anglický výkladový slovník Internetu.* Vyd. 1. Praha: AV software, 2004, 300 s. ISBN 80-901-4287-7.

[6] ŽEMLIČKA, Martin. *E-mail, chat, sms: praktický průvodce elektronickou komunikací.* Vyd. 1. Brno: Computer Press, 2003, 110 s. ISBN 80-722-6928-3.

Jako nejznámější české provozovatele e-mailových služeb bych uvedl například Seznam.cz, Centrum.cz, Atlas.cz a jako globální například Gmail.com.

Ačkoli e-mail v dnešní době využívají miliony uživatelů na celém světě, myslím si, že kromě výhod, jež tato služba poskytuje, má i pár záporů, a to například v tom že není velmi důvěryhodný. Jak uvádí ve své prácí Taťána Milošová: „*Uživatel si může pořídit více účtů s různými uživatelskými jmény a klamat tak ostatní uživatele. Hodně se také objevují podvodné e-maily, případně řetězové zprávy, spamy nebo e-maily, které mají za úkol pouze získat aktivní e-mailové adresy, na něž jsou pak tyto podvody páchány*."[7]

Mezi přednosti e-mailu patří:

- **Rychlost doručení zprávy -** Zpráva je doručena příjemci během několika sekund po odeslání, přičemž nezáleží na tom, kde se příjemce nachází a zda je právě online či offline, zpráva je uložena na serveru a čeká na své vyzvednutí.
- **Multimediální zprávy -** Možnost ke zprávě připojit přílohu. Příloha může být textový dokument, obrázek, video, audio soubor a jakýkoliv jiný typ souboru.
- **Nezávislost -** Přijímat a odesílat lze zprávu na jednom e-mailu z jakéhokoliv místa na světě, kde je přístup k internetu.
- **Ovládání -** Velmi jednoduché a velice snadné uživatelské prostředí. Využívání e-mailu zvládne i méně zkušený uživatel.

[7] MILOŠOVÁ, Taťána. *Kybergrooming jako nebezpečný jev v informačních a komunikačních technologiích*. Zlín, 2011. Bakalářská práce. Univerzita Tomáše Bati.

1.2.3 Instant Messaging

Druh internetové komunikace, jenž je mnohdy označován zkratkou jako (IM). Jedná se o druh okamžité internetové komunikace. Před příchodem Facebooku se jednalo o jednu z nejvíce využívaných internetových aplikací, jež umožňovala dialog mezi uživateli, kteří byli připojeni. Instant Messaging umožňuje svým zaregistrovaným a přihlášeným uživatelům sledovat, kteří jejich přátelé jsou momentálně online a kteří offline, odesílat jim zprávy, nebo posílat soubory. Mezi instant messengery používající IM protokoly patří např. ICQ, ruský QIP, Yahoo Messenger, Windows Live Messenger a v USA nejpoužívanější Jabber.

ICQ

Název programu v sobě nese zkratku z anglického jazyka, a to (I Seek You) neboli „hledám tě“. Komunikace probíhá v reálném čase, každý uživatel po registraci získá jedinečné identifikační číslo neboli UIN (Unixe identification number). Zadáním příslušného čísla je možno uživatele vyhledat v databázi a přidat mezi své přátele. Od počátku až do současnosti byl a je program volně šiřitelný. Program disponuje velkým množstvím funkcí, ačkoliv je využíváno jen minimum z toho, co nabízí. V roce 1996 ho vytvořili čtyři mladí izraelští programátoři, kteří si následně založili vlastní firmu se jménem Mirabilis. Krátce po založení firmy ji zakoupil americký gigant - firma AOL. ICQ bylo v roce 2001 nepoužívanějším komunikačním nástrojem na světě, používalo ho více než 100 milionů uživatelů.

QIP

Je to obdoba ruského ICQ, která používá komunikační protokoly ICQ. Lze se tedy připojit s jeho pomocí k účtu vytvořenému na ICQ a komunikovat s uživateli, jež jsou připojeni na ICQ, ale i na qipu. Program je volně šiřitelný a lze ho zdarma stáhnout na stránkách výrobce. Mezi jeho přednosti patří schopnost komunikovat s americkým Jabberem pomocí protokolu XIMSS. Existuje verze pro PDA a pro mobilní telefony.

1.2.4 VoIP

Voice over Internet Protocol je technologie, pomocí které je možno telefonování prostřednictvím počítačové sítě. Tato technologie využívá ke své komunikaci pakety z rodiny IP a UDP.

Skype

Původními autory programu jsou dva programátoři z Estonska, a to Niklas Zennström a Janus Friis. Program umožňuje zdarma telefonovat mezi uživateli programu (SpyeIn) a za poplatek je možno ze Skype telefonovat do klasických telefonních sítí (SkypeOut). Skype nepodporuje volání na linky záchranného systému. Pomocí programu lze však i chatovat, odesílat soubory a vést konferenční hovory mezi více uživateli.

TeamSpeak

Program umožňuje hlasovou komunikaci mezi více uživateli, a to v reálném čase. Pro svou nenáročnost na systém se používá především při komunikaci lidí během hraní online multiplayerových her. Program lze využívat i pro jiné účely, je zdarma a volně šiřitelný. Firma poskytuje i TeamSpeak server, který lze snadno nainstalovat na jakémkoliv PC a při veřejné IP adrese daného PC se mohou uživatelé volně připojovat a komunikovat. Oproti klasickému VoIP programu lze nastavovat citlivost mikrofonu elektronicky jednotlivě zesilovat a zeslabovat konkrétní uživatele, nebo nastavit klávesovou zkratku pro zapnutí mikrofonu. Hlas je komprimován velmi kvalitními kodeky pro nízké využití internetového připojení při velmi čistém hlasovém přenosu. Obdobou TeamSpeaku jsou programy Mumble a Ventrilo.

1.2.5 Sociální sítě

Sociální sítě začaly vznikat už v USA v polovině 90. let minulého století. Dnes díky Facebooku a G+ dosáhly obrovského rozmachu mezi uživateli internetu.

Sociální sítě jsou kombinací specializované webhostingové služby a specializovaného vyhledávače. Po vyplnění strukturovaného profilu může uživatel hledat a být hledán. Tyto systémy obvykle sdružují lidi stejných zájmů a jsou stále

více populární, tím tedy narůstá i počet jejich uživatelů. V rámci těchto služeb mohou uživatelé nalézat své přátele, seznamovat se s novými lidmi, diskutovat na diskusních fórech nebo přispívat do nejrůznějších blogů.[8] Jako nejznámější a nejpoužívanější sociální sítě bych uvedl Facebook a G+, v USA také velmi často používaný Twitter.

Google+

Neboli také zkráceně G+ je internetová sociální síť provozovaná společností Google. Konkurence Facebooku, neboli snaha firmy Google proniknout na pole sociálních sítí. Nabízí stejné služby jako Facebook a přidává k nim navíc některé nové prvky např. Kruhy, Témata či Setkání. Sociální síť Google+ byla uvedena 28. června 2011 a zpřístupněna byla jen na pozvánky a pro omezený počet uživatelů. V polovině října 2011 pak Google ohlásil 40 milionů registrovaných uživatelů, v dnešní době se množství aktivních uživatelů propadlo o 60 % oproti červenci 2011.

Facebook

Zakladatelem Facebooku je programátor Mark Zuckerberg, který tento sytém založil původně jen pro studenty Harvardovy univerzity, během roku se připojily další univerzity. Od 11. srpna 2006 se může dle licence používání připojit kdokoli starší 13 let. Dnes je Facebook největší sociální sítí na světě. Uživatelé se v systému mohou připojovat k různým skupinám uživatelů, kteří působí například v rámci jedné školy, firmy nebo geografické lokace.

[8] PROCHÁZKA, David. *První kroky s internetem*. 3., aktualiz. vyd. Praha: Grada, 2010, 108 s. Snadno a rychle (Grada). ISBN 978-80-247-3255-8.

Twitter

Twitter založil programátor Jack Dorsey v roce 2006. Umožňuje uživatelům posílat a číst příspěvky zaslané jinými uživateli, známé jako tweety (textové zprávy dlouhé maximálně 140 znaků, jež se zobrazují na uživatelově profilové stránce a na stránkách jeho odběratelů). V roce 2011 bylo ke Twitteru zaregistrováno přes 200 milionů uživatelů.[9]

1.3 Virtuální prostředí

Virtuální prostředí nám umožňuje komunikovat s lidmi, s kterými bychom se v běžném životě třeba ani nepoznali. Můžeme zde velice snadno změnit svou identitu nebo ji lehce poupravit. Na své profily vkládáme pouze to, co chceme vkládat. Nelze tedy spoléhat pouze na to, co zde můžeme o dané osobě zjistit. Většina lidí se tedy přetvařuje a uvádí lživé informace. Virtuální realita může člověku nahrazovat, co mu v reálném životě chybí, nebo prostředí, do kterého utíkáme před realitou.

Jedním ze znaků virtuálního prostředí jako je například internet, je otevřenost, která umožňuje uživatelům větší výřečnost a odvážnost. Uživatelé se odhalují a takzvaně „odhazují masku“. Dívky se zde mnohem více než v reálním světě setkávají se sexuálními narážkami, ačkoliv mnohé z nich tvrdí, že to pro ně není nepříjemné a berou narážky jako součást flirtování.

Na většinu lidí působí také jako prostředí, ve kterém se posouvá hranice jeho zábran. Lidé jsou při komunikaci odvážnější, protože velmi často předpokládají, že za své činy ve virtuálním prostředí nemusí nést žádnou zodpovědnost. Cítí se bezpečně, protože osoby, s kterými komunikují, nejsou fyzicky v jeho blízkosti a nemohou je

[9] TAYLOR, Chris. *Twitter Has 100 Million Active Users. Mashable* [online]. 2011 [cit. 2011-10-12]. Dostupné z: www.mashable.com/2011/09/08/twitter-has-100-million-active-users/

tedy ohrozit. Pocit bezpečí může také navozovat fakt, že komunikaci vždy lze velmi snadno ukončit odpojením se.

Prostředí internetu slouží také k povyražení a odreagování či relaxaci, nebo pro zkrácení dlouhé chvíle. Většina dětí, mládeže a v dnešní době také dospělých, ale i seniorů za tímto účelem internet využívá. Při pobytu na internetu jsou do své činnosti tak zabráni, že nevnímají okolní svět. Hodiny se zde mění v minuty a člověk stráví spousty času sezením u počítače. Tento jev se v psychologii nazývá: „flow", neboli stav kdy je člověk pohlcen činností, kterou právě provádí, natolik, že nevnímá čas, únavu a jiné potřeby.

Na některé osoby může také působit jako prostředí, ve kterém je šťastný. Taková osoba může internet vnímat jako prostředí štěstí, uvolněné atmosféry, bezstarostnosti či emoční podpory. Nepřichází se do virtuálního prostředí pouze pobavit, je to pro něho místo, kde může ventilovat své pocity, cítit sounáležitost s ostatními, sdílet své problémy.[10]

[10] ŠMAHEL, David. *Psychologie a internet: děti dospělými, dospělí dětmi*. Praha: Triton, 2003, 158 s. Psychologická setkávání, sv. 6. ISBN 80-725-4360-1.

2 Nežádoucí jevy

2.1 Obecná problematika

Nízká informovanost dětí, rodičů a učitelů o problematice nebezpečných komunikačních jevů má za následek rizikové chování dětí ve virtuálním prostředí, tedy počet obětí. Může ale také souviset s množstvím útočníků, kteří nejsou dostatečně seznámeni s důsledky svého jednání.

Nejprve proběhne analýza nejčastěji se vyskytujících negativních jevů na internetu (např. kyberšikana, kybergrooming, atd.). Následující jevy představují ohrožení pro děti i mládež.

2.2 Kyberšikana

V poslední době nastal opravdový boom v oblasti informačních komunikačních technologií. Tyto technologie nám nabízí obrovské možnosti a podstatně ulehčují náš život. Ovšem je třeba si uvědomit, že s sebou přináší také četná rizika. Technologie se totiž mohou stát mocnou zbraní, kterou může někdo obrátit proti nám. Jedním z rizik, které nám hrozí, je kybernetická šikana, tzv. kyberšikana.[11]

2.2.1 Co je to kyberšikana

Kyberšikana úzce souvisí s šikanou. Zatímco klasická šikana se může projevovat jak fyzickými útoky, tak útoky psychickými. Kyberšikana se odehrává pouze v psychické rovině, je tedy druhem psychické šikany.

Pojem kyberšikana (někdy se používají i cizí výrazy kyber-mobbing, e-mobbing apod.) představuje úmyslné urážky, vyhrožování, zesměšňováni, pomlouvání,

[11] KYBERŠIKANA: *KYBERNETICKÁ ŠIKANA* [online]. Olomouc, 2010 [cit. 2013-01-24]. ISBN 978-80-254-7791-5. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd. Studie. UP.

vydírání nebo obtěžování druhých prostřednictvím moderních komunikačních prostředků většinou v delším časovém období. Kyberšikana se odehrává na internetu (např. prostřednictvím e-mailů, chatovacích aplikací jako je ICQ, v sociálních sítích, na videích umístěných na internetových portálech), nebo prostřednictvím mobilního telefonu (např. SMS zprávami nebo nepříjemnými telefonáty). Pachatel často jedná anonymně, takže oběť netuší, od koho útoky pochází. Mezi kyberšikanu také lze zahrnout „Happy Slapping", nejedná se o nic šťastného, jak by mohl napovídat název. Happy Slapping je novým druhem šikany, který se poprvé objevil v jižní části Londýna v roce 2005 u hiphopových „gangsta teenagerů". Účelem happy slappingu je nečekané tělesné napadení mladistvého nebo dospělého člověka, přičemž spolupachatel agresora celý čin nahrává na mobilní telefon nebo kameru. Získané video je poté umístěno na internet k pobavení ostatních uživatelů. Obětí takového útoku se může stát prakticky kdokoliv, kdo se útočníkovi naskytne.[12]

Právě v případech kyberšikany mezi dětmi a dospívajícími se většina obětí a pachatelů navzájem zná i v „reálném" světě. Téměř vždy mají oběti alespoň podezření, kdo by se mohl za útoky skrývat. Kyberšikanu většinou páchají lidé z okolí oběti: ze školy, ze čtvrti, ze stejné vesnice nebo např. etnické komunity. Případy kyberšikany mezi zcela neznámými lidmi nejsou příliš časté.[13]

---

[12] E-bezpeci. *Ebezpečí* [online]. 2008 [cit. 2013-01-18]. Dostupné z: http://www.e-bezpeci.cz.

[13] Co je to kyberšikana a jak se projevuje?. *Bezpecne-online* [online]. 2006 [cit. 2013-03-30]. Dostupné z: http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html?highlight=YToxOntpOjA7czoxMjoia3liZXLFoWlrYW5hIjt9

2.2.2 Nejčastější projevy

- Publikování ponižujících záznamu nebo fotografií (v rámci webových stránek, MMS zpráv).
- Ponižování a pomlouvání v rámci sociálních sítí, blogu nebo jiných webových stránek.
- Krádež identity, zneužití cizí identity ke kyberšikaně nebo dalšímu sociálně patologickému jednání (zcizení elektronického účtu).
- Ztrapňování pomocí falešných profilů v rámci sociálních sítí, blogu nebo jiných webových stránek.
- Provokování a napadání uživatelů v online komunikaci (především v rámci veřejných chatu a diskuzí).
- Zveřejňování cizích tajemství s cílem poškodit oběť (v rámci sociálních sítí, blogu nebo jiných webových stránek, pomocí SMS zpráv apod.).
- Vyloučení z virtuální komunity (ze skupiny přátel v rámci sociální sítě).
- Obtěžování (opakovaným prozváněním, voláním nebo psaním zpráv).[14]

2.2.3 Čím se vyznačuje

Kyberšikana se od klasické šikany liší v mnoha ohledech. Kyberšikana se vyznačuje především následujícími charakteristikami jako je např. anonymita pachatele, žádné časové omezení či velmi rychlé šíření, atd.

[14] WILLARD, N. *Educator's Guide to Cyberbullying and Cyberthreats: Center for Safe and Responsible Use of the Internet. In: Cyberbully.org* [online]. 2007 [cit. 2013-01-24]. Dostupné z: http://www.cyberbully.org/cyberbully/docs/cbcteducator.pdf

Žádné časové omezení

Pachatel není nijak časově vázán, může pronásledovat svou oběť doma, ale i v práci.

Na svou oběť může útočit prostřednictvím mobilního telefonu, či internetu. Oběť se nemůže cítit bezpečně ani ve svém domově, je pronásledována neustále bez ohledu na to, kde se zrovna nachází.

Anonymita pachatele

Prostřednictvím internetu a mobilu může pachatel na svou oběť útočit anonymně. U většiny případů pachatel a oběť jsou spolu v určitém sociálním vztahu, nelze však určit, o koho se jedná, neboť se snaží svou identitu utajit. To dělá pachatele vytrvalého.

Pachatel a oběť

U kyberšikany nehraje věk, ani vzhled žádnou roli. Může tedy docházet ke kyberšikaně mezi spolužáky, ale i mezi učitelem a žáky. Pachatel si velmi snadno může vytvořit svou novou elektronickou identitu.[15]

Neúmyslná kyberšikana

Jako neúmyslný případ kyberšikany lze brát zveřejnění fotografie videa či jiného média. Pachatel nedomyslí následky svého činu nebo prostě jen nevidí reakce oběti a ze špatně pochopeného vtipu může vzniknout neúmyslná kyberšikana.

Velmi rychlé šíření

Pomocí sociálních sítí sdílením odkazů fotografií videí a webových adres dochází k masovému šíření obsahu. Takovéto šíření inkriminujícího matriálu je následně nekontrolovatelné a šíří se lavinově.

---

[15] Kyberšikana. *Bezpecne-online* [online]. 2006 [cit. 2013-03-30]. Dostupné z: http://www.bezpecne-online.cz

Velmi široké publikum

Díky sociálním sítím dochází k velmi rychlému předávání a sdílení informací, publikum sledující inkriminující materiály se zvětšuje s každým dalším členem o všechny jeho přátele, kontrolovat všechny v publiku je velice obtížné.

2.2.4 Kde se vyskytuje

Kyberšikana v žádném případě není problém, který zůstává skryt v soukromém životě. Stále častěji se dějištěm kyberšikany stává škola a cílem veřejných útoků jsou jak žáci, tak učitelé. V roce 2009 organizace E-Bezpečí a Centrum prevence rizikové virtuální komunikace Univerzity Palackého provedly výzkum. Dle výzkumu 2,3 % dětí se přiznalo k tomu, že se někdy aktivně podílelo na kyberšikaně namířené proti učiteli. Přitom nezáleží na věku nebo pohlaví, profil oběti nebývá příliš schematický. Co se týče pachatelů, zhruba dvě třetinu útočníků kyberšikany tvoří chlapci. A i když existují případy kyberšikany mezi kolegy, šikanu proti učiteli mají v drtivé většině na svědomí žáci. Přesto by ale měla pozornost zůstat u toho, že většinu obětí kyberšikany tvoří žáci, a že kyberšikana se odehrává především mezi vrstevníky.

Oběti většinou při prvních projevech kyberšikany prožívají vztek a nejistotu nebo mají strach. Z počátku obvykle nevědí, kdo se za obtěžováním skrývá. Pokud pachatel vyjde najevo, nemívá to pro něj žádné vážnější důsledky (jako např. trestní oznámení nebo vyloučení ze školy). Případy kyberšikany by se ale měly řešit a nemusí přitom zůstat jen u klasických prostředků, jako je rozhovor s učitelem nebo s vedením školy nebo běžné školní tresty. Při vyvozování důsledků z kyberšikany nelze opomenout širší souvislosti: Kde jsou příčiny šikany? Jaká je na škole atmosféra? Mluví se o problémech ve třídě, existuje třídní výbor nebo nějaký

kultivovaný způsob řešení podobných problémů? Které okolnosti přispěly k šikaně? [16]

2.2.5 Důvody ke vzniku

Nuda – Ke vzniku kyberšikany může přispět také nuda, pachatel z dlouhé chvíle píše nevhodné komentáře, poznámky k příspěvkům i fotografiím svých známých či přátel na sociálních sítích. Vše může vyvrcholit až ke sporu, který se může nestále více vyhrocovat.

Konflikt dvou osob – Konflikt mezi osobami s různým názorem bývá často také jednou z příčin vzniku kybešikany.

Vztahy ve třídě či pracovní skupině – Napětí mezi lidmi v určité skupině může vést k posměchu či urážkám slabšího jedince neboli "otloukánka". Posměch a urážky se mohou nadále přesunout do SMS či na internet a pronásledovat daného jedince.

Rozchod nebo ukončení přátelství – Velmi často při rozchodu se objevuje nenávist jednoho k druhému. Nenávist nebo pomstychtivost veliče často bývá impulz k pronásledování.

Potřeba uznání - Kyberšikanu pachatelé využívají k tomu, aby si získali pověst „frajerů".

Potřeba síly – Pomocí kyberšikany se mnohdy snaží ostatním pachatel dávat na jevu svou sílu ostatním.

Následování skupiny – Slabší jedinci mnohdy jen nechtějí vybočovat z davu a sami přispívají k šikaně jiné osoby.

---

[16] Kyberšikana II. *Bezpecne-online* [online]. 2006 [cit. 2013-03-30]. Dostupné z: http://www.bezpecne-online.cz

2.2.6 Prevence před kyberšikanou

Před kyberšikanou se nelze na 100 % ochránit, ale existuje velké množství rad, jak snížit riziko napadení.

Informovanost

Pro prevenci před vznikem kyberšikany je velice důležitá informovanost. Žáci ve školách by měli být informováni, co vše kyberšikana je, čím se vyznačuje a jaké má dopady na šikanovanou osobu. Také informovat žáky o možných postizích útočníků. Klást důraz na to, že i když ke kyberšikaně nedochází přímo v budově školy, tak škola je schopna oběti pomoci a v případě potíží se lze na ni obrátit.

2.2.7 Následky

Vzhledem k době trvání kyberšikany mohou být následky velmi vážné a dlouhotrvající.

Oběť kyberšikany může cítit rozčílení, frustraci, rozpaky, a tak dále. To může mít za následky:

Změny chování - Zhoršení koncentrace ve výuce, pokles školní výkonnosti, ale i záškoláctví a absence ve škole mohou být důsledky kyberšikany. Oběť se může cítit v pozici podřízenosti vůči agresorovi nebo skupině agresorů, rovněž vnímá negativní nebo nízké hodnocení od svých vrstevníků, spolužáků, což obvykle nadále prohlubuje jeho pocity osamělosti a nízkého sebehodnocení.

- **Negativní myšlení -** Vzhledem k tomu, že kyberšikana může trvat po velmi dlouhou dobu, než se agresora podaří vypátrat nebo alespoň zabránit projevům, způsobuje často také dlouhotrvající negativní emoce oběti. Následkem kyberšikany nezřídka bývají i sebevražedné myšlenky, dlouhotrvající depresivní stavy apod. Kyberšikana může způsobit také duševní nestabilitu oběti.
- **Vyhýbavost -** Když se děti stanou oběťmi kyberšikany, často to může vést ke změnám v jejich dosavadních zvycích a chování. Může u nich dojít k útlumu

používání sociálních sítí, které měly dříve v oblibě. Mohou přestat používat i mobilní telefon, aby se tak vyhnuly opakování negativních incidentů. U obětí, zejména u dívek, dochází také vlivem prožité kyberšikany k vytvoření si nedůvěry vůči okolí, snížení kontaktů s dosavadními přáteli, k nechuti seznamovat se s novými lidmi apod.

- **Pocit ohrožení -** Ztráta pocitu bezpečí může být výraznější, než je tomu u klasické šikany. Oběť kyberšikany je dosažitelná po dobu 24 hodin denně. Na rozdíl od oběti tradiční šikany, která často reaguje stažením se do sebe, pasivitou, úzkostí, u obětí kyberšikany obvykle dochází k projevům slovní i fyzické agresivity, slabému ovládání hněvu. Jedná se o obrannou reakci, vyrovnání se se stresem, kdy oběť není schopna postavit se útočníkovi tváří v tvář, neboť se s ním fyzicky nesetkává.
- **Změna fyzických projevů -** Zejména u déletrvající kyberšikany může dojít následkem zvyšující se úzkostnosti oběti až ke změnám fyzických projevů, mezi které patří například dlouhodobé vyčerpání organismu, změny váhy, nechutenství, nevolnost, oslabená imunita. Důsledkem frustrace z nemožnosti řešení vzniklé situace může u jedince postiženého kyberšikanou docházet k sebepoškozování, v nejhorším případě i k pokusu o sebevraždu.[17]

[17] MGR.JANA GAJDOŠOVÁ. *Zdravotní a psychické následky kyberšikany mezi dětmi a dospívající mládeží. In: E-bezpeci.cz* [online]. Pedagogická fakulta MU v Brně, 2008 [cit. 2013-01-27]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/dali-rizika/355-zdravotni-a-psychicke-nasledky-kyberikany-mezi-dtmi-a-dospivajici-mladei

2.3 Kybergrooming

Internet je nástroj, který využívají milióny uživatelů z celého světa. Slouží jim k vyhledávání informací, práci i zábavě, ke komunikaci, k navazování sociálních vztahů s dalšími lidmi. V reálném světě se potkáváme s různými lidmi, totéž platí i v rámci internetu – díky jeho rozšíření lze komunikovat s uživateli z celého světa, i s těmi, se kterými bychom se pravděpodobně osobně nikdy nesetkali. Internet však skýtá také řadu nebezpečí, kterým mohou být jeho uživatelé vystaveni.

2.3.1 Co je to kybergrooming

Termínem kybergrooming neboli „grooming“ se označuje chování pachatelů neboli „predátorů“, kdy si v prostředí internetu vytipují oběť, následně se snaží u oběti vybudovat důvěru. Pachatelé jsou velmi často velice trpěliví, co se týká získání základních informací o oběti, jako je například místo bydliště, zda oběť bydlí s rodiči, telefonní číslo nebo jiný kontakt, sociální vztahy apod. Vydrží velmi dlouho, mnohdy až řádově v měsících budovat vztah s obětí, posilovat důvěru oběti, to vše pomocí komunikace s obětí, posíláním drobných dárků jako například kredit do mobilního telefonu. Pachatelé se velmi často vydávají za úplně někoho jiného, než ve skutečnosti jsou. Většinou se vydávají za osobu, která má největší šanci u oběti získat důvěru, u malé dívenky za kamarádku ve stejném věku, u starší slečny za chlapce, jež je o něco málo starší než ona. Po získání důvěry a vybudování vztahu se pachatelé snaží vylákat oběť na osobní schůzku za účelem sexuálního zneužití, dětské pornografie, dětské prostituce, fyzického násilí atd. V některých případech pachatel po získání intimních fotografiích oběť vydírá. Hrozí zveřejněním získaného materiálu a nutí oběť například k opakované osobní schůzce, na které oběť zneužívá.

2.3.2 Čím se vyznačuje

Falešná identita - U většiny případů jsou útočníci starší než jejich oběť, jsou nuceni pro získání důvěry u oběti změnit svou identitu, uvádějí pak falešný věk, pohlaví, koníčky, jméno a velmi často i svůj vzhled pomocí cizích fotografií. Útočník si vytvoří svůj profil na některé ze sociálních sítí a snaží se vyhledávat oběti podle určitého pravidla, například podle věku, pohlaví,

nebo mění svou identitu podle potřeby tak, aby co nejlépe oslnil oběť a co nejsnáze získal její důvěru.

Efekt zrcadlení - Charakteristickým rysem chování kybergroomera je tzv. *„efekt zrcadlení“* (mirroring). Predátor napodobuje oběť ve snaze prolomit zábrany, chová se jako její zrcadlový odraz. Pokud oběť útočníkovi sdělí, že se cítí například osamělá a má nějaké problémy a starosti, predátor odpoví, že má podobné problémy a plně ji chápe. Nabízí jí, že se mu může s důvěrou svěřit. Díky efektu zrcadlení útočník u oběti navozuje pocit přátelství či kamarádství, který oběti pomůže překonat strach z komunikace s neznámou osobou. Zrcadlení nemusí být spojeno pouze s emoční rovinou vztahu s obětí, může také navodit sounáležitost například fiktivními společnými koníčky, názory na různá témata apod.[18] Efekt zrcadlení využívá pachatel ke snadnému získání osobních údajů a vytvoření si obrazu o oběti. Pomocí zrcadlení také pachatel upevňuje svůj vztah s obětí a buduje vzájemnou důvěru.

Zasílání dárků - Jako další velmi účinný nástroj k posílení vztahu mezi pachatelem a obětí je takzvané uplácení oběti. Pachatel zasílá oběti malé dárečky. Dárečky mohou být ve formě peněz, mobilního kreditu, oblečení, elektroniky a spousty jiných předmětů, které udělají na oběť dojem. Výsledkem snahy zasílat oběti dárečky, je velmi často ověření získaných osobních údajů jako je telefonní číslo, jméno a také adresa, nebo vyžadování nějaké satisfakce, jako je například zaslání intimních fotografií, osobní schůzka apod. V mnoha případech, které jsou známy, se oběti za vidinou odměny často k útočníkovi dobrovolně vracely, i přesto že byly na setkáních zneužívány. V takových případech se dá hovořit o dětské prostituci.

---

[18] KOPECKÝ, Kamil. *KYBERGROOMING: NEBEZPEČÍ KYBERPROSTORU* [online]. Olomouc, 2010 [cit. 2013-01-29]. ISBN 978-80-254-7573-7. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie. Studie. UP.

Intimní konverzace – Pachatel se postupně snaží snižovat zábrany své oběti a zvyšovat důvěru. Zavádí do konverzací sexuální témata, mnohdy zasílá oběti pornografii, vše s cílem získat intimní materiály oběti. Pachatel se snaží vytvářet iluzi nejlepšího přítele či partnera. Díky internetovému prostředí, kde neneseme bezprostřední důsledky, které může naše komunikace přinášet, jsme více ochotní sdělovat intimní informace než například v reálném životě.

Snaha o osobní schůzku – Vyvrcholením kybergroomingu je osobní schůzka pachatele s obětí, na které se pachatel ve většině případů dopouští násilí na oběti.

2.3.3 Kde se vyskytuje

Kybergrooming je často vázán na synchronní i asynchronní komunikační platformy, nejčastěji veřejný chat, internetové seznamky, instant messengery a VoIP (např. ICQ, Skype) a v posledních letech také na sociální sítě (Facebook, Twitter, MySpace, Bebo a další). Podle řady výzkumů (CEOP[19], 2008 a další) probíhá kybergrooming nejčastěji právě v prostředí instant messengerů (56 % případů), další pozici pak obsadily sociální sítě (11,4 % případů). Internetoví predátoři však kromě těchto komunikačních prostředí využívají také inzertní portály, na kterých nabízející dětem různé možnosti výdělku či kariéry (např. v oblasti modelingu), často navštěvují portály zaměřené přímo na nezletilé uživatele internetu (dětské portály, portály zaměřené na volnočasové aktivity, herní portály a další internetové stránky).[20]

---

[19] BERSON, I. H. *Cybervictims: The Psychosocial Effects of Online Exploitation for Youth. In: Cs.auckland.ac.nz* [online]. 2008 [cit. 2013-01-29]. Dostupné z: http://www.cs.auckland.ac.nz/~john/NetSafe/I.Berson.pdf.

[20] KOPECKÝ, Kamil. *KYBERGROOMING: NEBEZPEČÍ KYBERPROSTORU* [online]. Olomouc, 2010 [cit. 2013-01-29]. ISBN 978-80-254-7573-7. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie. Studie. UP.

2.3.4 Následky

Útok na oběť (fyzický útok, sexuální útok apod.) má dalekosáhlé následky, jak v oblasti fyzické i psychické. Pokud kybergroomer vlastní dostatek účinných nástrojů pro manipulaci, může oběť přinutit k opakovaným schůzkám, na kterých útoky pokračují.[21]

2.4 Kyberstalking

Kyberstalking je typ pronásledování, při němž stalker využívá informační a komunikační technologie (internet, mobilní telefony). Kyberstalkeři využívají diskusní fóra, na kterých se pod falešnou identitou snaží kontaktovat oběť, případně získat informace o oběti od ostatních uživatelů internetu. K tomuto účelu mohou využívat také různé typy spywarových programů. Kyberstalkeři, kteří k pronásledování využívají pouze informační a komunikační technologie, se nikdy neuchýlí k fyzickému útoku. Kyberstalking jako doprovodný jev můžeme nalézt u všech výše uvedených kategorií. Každý stalker tedy může být zároveň ikyberstalkerem.[22]

2.4.1 Co je to kyberstalking

Kyberstalking vznikl z termínu *„stalking“* neboli pronásledování či lov. Stalkingem se označuje dlouhodobé, opakované a systematické obtěžování oběti, které se může stupňovat. Stalking se může vyskytovat v různé podobě a intenzitě. Oběť je dlouhodobě pronásledována či sledována pachatelem, je pod neustálým bombardováním zprávami jako například SMS, e-maily či nechtěné dárky, které

[21] MILOŠOVÁ, Taťána. *Kybergrooming jako nebezpečný jev v informačních a komunikačních technologiích*. Zlín, 2011. Bakalářská práce. Univerzita Tomáše Bati.

[22] KOPECKÝ, Kamil. *STALKING A KYBERSTALKING: NEBEZPEČNÉ PRONÁSLEDOVÁNÍ* [online]. 2010[cit. 2013-02-12]. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu

pachatel zasílá. Odehrává-li se stalking v prostředí informačních technologií, hovoříme o kybestalkingu. Při kyberstalkingu využívá pachatel například ICQ, VoIP, sociální sítě, e-mail apod. Oběti stalkingu a kyberstalkingu se cítí pachatelem ohroženy, mají strach o své bezpečí.

Za trestný čin bylo pronásledování poprvé označeno v Kalifornii roku 1990. Od okamžiku zveřejnění také vzrostlo procento ohlášených případů. Z USA pochází zatím také většina výzkumných prací zabývajících se různými typy stalkingu, osobnostmi pachatelů a poškozených, prevencí a kriminologickými aspekty takového jednání.[23]

2.4.2 Nejčastější projevy

Z počátku může být komunikace příjemná a nic nenaznačující, tyto zprávy jsou většinou zasílané s úmyslem získání kontaktu na oběť. Následně pachatel bombarduje oběť zprávami prostřednictvím SMS, telefonátů, dárků a v prostředí IT to mohou být zprávy přes IM jako ICQ nebo QIP, Skype, prostřednictvím chatu, e-mailu apod. Ve snaze kontaktovat svou oběť používá pachatel různé metody, jako je například vyvolávání kladných pocitů, soucitu, viny, vyhrožování, vydírání atd.

Velmi často se stalker snaží od sebe odvrátit pozornost. Nejprve se tváří jako ten, komu je ubližováno a obviňuje svou oběť. Předstírá, že se mu oběť mstí, v některých případech na ní podá i trestní oznámení.

Oproti klasickému stalkerovi se kyberstalker většinou omezuje na různé druhy výhrůžek, které opírá o poznatky o oběti (vím, kde jsi, co děláš, vidím tě, vím, co máš na sobě…).

---

[23] ŠTĚPÁNKA, *Tůmová. Nová forma psychického teroru.: Asociace forenzních psychologů*. [online]. Praha, 2007 [cit. 2013-03-07]. Dostupné z: http://afp.wz.cz/clanky.doc/Stalking.doc

Mezi velmi časté praktiky kyberstalkeru patří také pošpiňování oběti. Šíří mezi přáteli, rodinou či známými nepravdivé informace. Například vytvořením profilu na některé ze sociálních sítí či vytvoření blogu, na těchto profilech uvádí lživé informace o oběti s cílem jí zesměšnit, ztrapnit či snížení důvěryhodnosti. Odkaz na takto vytvořený profil následně rozesílá známým a přátelům oběti.

2.4.3 Čím se vyznačuje

Stalker či Kyberstalker je u většiny případů společenský a na první pohled normální, nijak se neliší od ostatních, proto je ho velmi těžké odhalit. I když většinu kyberstalkingu a stalkingu má na svědomí mužská populace, ženy jsou mnohem větší hrozba jejich pronásledování je mnohem promyšlenější a to díky jejich cílevědomosti a systematičnosti.

2.4.4 Důvody ke vzniku

Rozchod

Jedná se o osobu, která se nepřenesla přes ukončení vztahu a to nejen partnerského, ale i pracovního či obchodního, nebo rozpad přátelství. Snaha o obnovení vztahu, nebo pomsta za rozpad přátelství motivuje pachatele k činu. Mohou se přidat pocity frustrace, žárlivosti či hněvu, zvláště když někdo nahradí místo pachatele.

Uctívání

Pachatel slepě touží po vztahu s osobou, jež ho zaujala. Doufá, že se dostane do přízně této osoby, nemusí primárně usilovat o sex, spíše o navázání kontaktu a opětování svých citů. Jakákoliv reakce oběti na uctívačovu snahu působí jako motivace pro další pronásledování. Pachatel vynakládá veškeré úsilí a doufá, že jeho snaha nepřijde vniveč. Při dlouhodobém odmítání či znemožnění vztahu, například svatbou nebo jiným nahrazením jeho vysněné pozice, může dojít k přechodu na vyhrožování, pachatel se v takovém případě snaží pomstít a oběť poškodit.

Posedlost

Pachatel touží po intimním partnerském vztahu s obětí. Většinou se jedná o osobu, která má problémy se seznamováním, obtížně vyjadřuje své city a projevuje ostatním lidem své emoce. Vzhledem k těmto okolnostem velmi špatně navazuje kontakt, přesto se domnívá, že je pro ostatní neodolatelný. Velmi často se jedná o osoby se sklonem k narcismu, jež neumějí vnímat pocity druhých lidí. Pachatel se pokouší navázat kontakt s obětí. Po několika neúspěších či kontaktování policie obětí od pronásledování ustupují. Jedná se tedy o méně nebezpečný druh kyberstalkerů.

Pronásledování

Pachatel usiluje o pomstu oběti, a to ať už kvůli skutečnému ublíženi či domnělému. Pachatel jedná paranoidně a nedomýšlí své činy. Jedná se o útoky slovní, poškozování majetku oběti, jako například poškození automobilu vloupání do bytu, vyhrožování či zastrašování oběti. Takovýmto pronásledováním si kompenzuje pocit ublížení, pocitem moci a výhrou nad obětí. Ačkoliv u většiny pronásledovatelů nedochází k fyzickému napadení, pachatel je velmi vytrvalý.

Sexuální motiv

Pachatel je velmi agresivní a snaží se o fyzický či sexuální útok, je poháněn základními pudy a touhou po takovémto útoku či uspokojení sexuálních potřeb. Velmi často se jedná o sexuální delikventy s poruchou osobnosti či nižší inteligencí. Při útocích se také projevují jejich pohnuté sklony k sadismu, masochismu či exhibicionismu. K takovýmto útokům dochází velmi zřídka.

Poblouznění

Pachatel je beznadějně zamilován do své oběti a myslí si, že oběť jeho city opětuje. Jakékoliv chování své oběti si vykládá tak, aby utvrdil své přesvědčení o opětování jeho lásky. Pachatel může trpět akutní paranoiou. Veškeré vnější podměty, jež

objasňují city oběti k pachateli, jsou pachatelem ignorovány. Pachatele zpravidla nezastaví právní jednání proti jeho osobě. Pokud se nedostane do péče psychologa, pokračuje v pronásledování oběti.[24]

2.5 Sexting

Je složenina slov Sex a Texting. Posílání SMS se v angličtině říká „texting", „sexting" je tedy nové slovo, které vystihuje nový trend: posílání erotického obsahu prostřednictvím mobilních telefonů, patří mezi nejrozšířenější jevy v komunikaci mladých lidí. Ačkoliv je strašáků, kteří upozorňují na nebezpečí této aktivity, čím dál víc, zdá se, že to pořád nestačí. Jakoby se tvrdé pády obětí šíření fotek týkaly jen zahraničních kauz.[25]

2.5.1 Co je to sexting

Termínem *„sexting"* je označováno rozesílání a šíření materiálů obsahujících sexuální kontext. Jedná se o textové zprávy, fotografie, videa a ostatní materiály se sexuálním obsahem.

2.5.2 Nejčastější projevy

Stále více dospívajících pořizuje erotické fotky, ať už sebe nebo i někoho dalšího, natáčejí různá odvážná videa a ty pak mobilním telefonem posílají kamarádům a známým. Takové obrázky často skončí i na Internetu např. na stránkách sociálních sítí nebo na různých portálech pro zveřejňování fotek a odtamtud se dostávají k širokému publiku. Často se lechtivé obrázky posílají nejdřív „jen" v páru nebo nejlepším kamarádům a kamarádkám např. jako důkaz lásky nebo přátelství, někdy

[24] MULLEN, P. E. a kol. *The management of stalkers: Advances in Psychiatric Treatment. In: Apt.rcpsych* [online]. 2001 [cit. 2013-03-07]. Dostupné z: http://apt.rcpsych.org/cgi/content/full/7/5/335.

[25] E-bezpečí. LETOCHOVÁ, Kateřina. *Sexting aneb Černobílá budoucnost* [online]. 2008 [cit. 2013-03-07]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/sexting.

jsou takové fotky i formou flirtování. Když se ale vztah nebo kamarádství rozpadne, intimní fotky mohou skončit jako pomsta v mobilech dalších známých nebo se veřejně pověsí na Internet. Někdy se původně důvěrné osobní fotky stanou i prostředkem vydírání.

Jakmile se takové obrázky jednou dostanou do oběhu, neexistuje žádná možnost, jak spolehlivě zastavit jejich šíření. I když jsou fotky na internetu původně zpřístupněny například jen kamarádům, nedá se vyloučit, že se dostanou do nesprávných rukou. Fotky nebo videa, která se jednou objevila někomu v mobilním telefonu nebo na internetu, se mohou znovu vynořit i po létech a napáchat závažné škody například v kariéře nebo v soukromých vztazích.[26]

2.5.3 Čím se vyznačuje

- Pachatel vlastní citlivé materiály, které mohou při zveřejnění poškozovat oběť.
- Díky internetu mohou materiály kolovat na webu velmi dlouhou dobu, je velmi obtížné je úplně odstranit či dohledat všechny kopie.
- Citlivé materiály mohou být zveřejněny i velmi dlouhou dobu od jejich vzniku.
- Oběti sextingu mohou být vystaveny tzv. harašení či sexuálním útokům.
- Pachatelé dopouštějící se sextingu páchají přestupek a v některých případech dokonce i trestný čin (šíření dětské pornografie, ohrožování výchovy dítěte).[27]

---

[26] Sexting & Kybergrooming. *Saferinternet* [online]. 2011 [cit. 2013-03-13]. Dostupné z: http://www.saferinternet.cz/pro-rodice/sexting-kybergrooming.

[27] Sexting. PEDAGOGICKÁ FAKULTA UNIVERZITY PALACKÉHO. *Sexting* [online]. Olomouc, 2009 [cit. 2013-03-07]. Dostupné z: www.sexting.cz.

2.6 Ostatní nebezpečí

2.6.1 Počítačové viry

Počítačový virus je malý softwarový program, který se šíří z jednoho počítače do druhého a překáží provozu počítače. Počítačový virus může poškodit nebo odstranit data v počítači, pomocí e-mailového programu se rozšířit do dalších počítačů, nebo dokonce odstranit celý obsah pevného disku.

Počítačové viry se nejsnáze šíří prostřednictvím rychlých zpráv nebo příloh e mailových zpráv. Viry mohou být maskovány jako přílohy obsahující vtipné obrázky, pohlednice nebo zvukové soubory či soubory videa. Počítačové viry se také šíří při stahování z Internetu. Mohou se skrývat v nelegálním softwaru či v jiných souborech nebo programech, které stáhnete.[28]

2.6.2 Spyware

Spyware je program, který využívá internetu k odesílání dat z počítače bez vědomí jeho uživatele. Někteří autoři spyware se hájí, že jejich program odesílá pouze data jako je přehled navštívených stránek či nainstalovaných programů za účelem zjištění potřeb nebo zájmů uživatele a tyto informace využívá pro cílenou reklamu. Existují ale i spyware odesílající hesla a čísla kreditních karet nebo spyware fungující jako zadní vrátka. Protože lze jen těžko poznat, do které skupiny program patří, vzhledem k postoji, k reklamě řada uživatelů nesouhlasí s existencí a legálností jakéhokoliv spyware.

Spyware se často šíří jako součást shareware, a to jako adware nebo bez vědomí uživatelů (ale s vědomím autorů programu). Jakmile si takový program nainstalujete

[28] Počítačové viry: popis, prevence a obnovení. JOHNSON, Eric. *MCITP: Microsoft Windows Vista desktop support enterprise study guide* [online]. Indianapolis: Wiley, c2007 [cit. 2013-03-07]. Dostupné z: http://support.microsoft.com/kb/129972/cs.

a spustíte, nainstaluje se do systému také spyware. Často se to týká například klientských programů pro peer to peer sítě umožňujících stahování hudby a videa od ostatních uživatelů.

Spyware patří mezi malware, tedy programy které na počítači běží bez vědomí uživatele a nějakým způsobem jej poškozují, nebo zhoršují jeho funkci. Spyware představuje z hlediska bezpečnosti dat velkou hrozbu, protože odesílá různé informace (historii navštívených stránek, hesla) z vašeho počítače určenému uživateli, který tyto informace dále zpracovává.

2.6.3 Adware

Neboli (advertising-supported software) je označení pro produkty znepříjemňující práci nějakou reklamní aplikací. Ty mohou mít různou úroveň agresivity - od běžných bannerů až po neustále vyskakující pop-up okna nebo ikony v oznamovací oblasti. Další nepříjemnou věcí je např. změna domovské stránky ve Windows Internet Exploreru, aniž by o to uživatel měl zájem.

Většinou nejsou přímo nebezpečné jako spyware, ale jsou spojeny s nějakým programem, který je freeware. To se dělá z důvodu toho, že díky těmto reklamám mohou vývojáři financovat dál svůj program. Nebo když se jedná o placený produkt, může se díky těmto reklamám prodávat program se slevou. Nějaký adware je také shareware, ale není to totéž. Rozdíl mezi adware a shareware je ten, že u adware je reklama podporovaná. Některé produkty nabízejí uživateli možnost odstranění reklam po zaplacení.

2.6.4 Spam

Spam je nevyžádané sdělení (nejčastěji reklamní) masově šířené internetem. Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace – např. diskusní fóra, komentáře nebo instant messaging. Používá se též zkratka UBE/UCE (Unsolicited Bulk/Commercial Email).

Společným znakem těchto e-mailů je to, že je spameři posílají v obrovských kvantech na všechny e-mailové adresy, které seženou. Nejde vůbec o cílenou reklamu na určitý okruh vytipovaných lidí, které by daný výrobek mohl zajímat. Prostě pošlou reklamu na viagru všem, mužům, ženám, dětem, na kontaktní adresy úřadů, na adresy dávno zrušené.

Dalším znakem spamu je to, že zpáteční adresa v něm uvedená bývá z 99 % falešná. Rozesílání spamu lze totiž chápat jako obtěžování ostatních a je možné toho, kdo to udělá, od Internetu odpojit. Proto spameři nikdy neposílají spam ze své vlastní adresy ani z adresy firmy, pro niž dělají reklamu. Pro přístup k Internetu využívají většinou různé "připojení k Internetu přes telefon zadarmo" a pro rozesílání využívají cizí špatně zabezpečené servery nebo hacknuté počítače.[29]

2.6.5 Phishing

Phishing je druh internetového podvodu, kterým se podvodníci snaží z uživatelů internetového bankovnictví vylákat přístupové údaje k účtům a zneužít je pro svoje obohacení.

K získání těchto důvěrných informací využívají podvodné e-maily, které na první pohled vypadají, že jsou odeslány přímo z banky a snaží se přesvědčit uživatele, aby kliknul na odkaz. Jestliže neopatrný uživatel na tento falešný odkaz klikne, dostane se na podvodné stránky, kde jsou po něm požadovány přístupové údaje k účtům, platebním kartám nebo jiné důvěrné informace. Pokud je uživatel naivně vyplní, získají tato data podvodníci, kteří je následně využijí pro svůj prospěch.[30]

---

[29] HORÁK, Vladimír. Spam. *Spam* [online]. 2006 [cit. 2013-03-07]. Dostupné z: http://uvt1.cuni.cz/email/spam/uvod.html.

[30] DŽUBÁK, Josef. PHISHING. *HOAX* [online]. 2000 [cit. 2013-03-07]. Dostupné z: http://www.hoax.cz/phishing/.

2.6.6 Sociální inženýrství

Sociální inženýrství je způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace. Termín je běžně používán ve významu podvodu i podvodného jednání za účelem získání utajených informací organizace nebo přístupu do informačního systému firmy. Ve většině případů útočník nepřichází do osobního kontaktu s obětí.[31]

2.6.7 Hoax

V počítačovém světě slovem HOAX nejčastěji označujeme poplašnou zprávu, která varuje před neexistujícím nebezpečným virem. Hoax (anglické slovo hoax označuje podvod, mystifikaci či žert) je nevyžádaná e-mailová nebo IM zpráva, která uživatele varuje před nějakým virem, prosí o pomoc, informuje o nebezpečí, snaží se ho pobavit apod. Hoax většinou obsahuje i výzvu žádající další rozeslání hoaxu mezi přátele, příp. na co největší množství dalších adres, proto se někdy označuje také jako řetězový e-mail.

2.6.8 SMS Spoofing

Je rozesílání falešných SMS zpráv. Tyto falešné zprávy jsou nebezpečné, protože mohou zmást děti, ale i dospělé.

Útočník odešle SMS zprávu nebo zprávy, které po přijetí vypadají, jako by zpráva byla od jednoho z našich kontaktů.

Útočník se tak může vydávat za někoho z našich blízkých. Toto může být hodně nebezpečné pro děti, které se tak mohou stát obětí únosu, pedofilního člověka nebo

---

[31] KUČERA, Radek. *Pojem Sociální inženýrství. ABZ.cz: slovník cizích slov - on-line hledání* [online]. 2005 [cit. 2013-03-07]. Dostupné z: http://slovnik-cizich-slov.abz.cz/web.php/slovo/socialni-inzenyrstvi.

dalších jiných osob s nebezpečnými úmysly. Avšak existují právě i oběti mezi dospělými. [32]

2.7 Prevence

To znamená informovat veřejnost o daných problematikách a uvést případné postihy pro pachatele. Ve školách jasně stanovit výchovného poradce, který bude žákům v případě potíží k dispozici.

Důvěřivost – Absence mimoverbálních znaků komunikace připravuje dítě o možnost rozeznat pravdu od lži jako při reálné komunikaci. Je důležité si uvědomit, že osoba na druhé straně nemusí vždy mluvit pravdu.

Citlivé informace – Vždy zvážit, zda data zveřejnit či odeslat. Jedná se především o osobní údaje, osobní fotografie, problémy, hesla k elektronickým účtům apod. To platí i o informacích, fotografiích atd. příbuzných a známých.

Ve virtuálním prostředí by dítě mělo používat nejlépe obecnou, nic neříkající přezdívku, nikde neuvádět své jméno a příjmení, adresu atd., podle nichž by jej mohl útočník vystopovat. Důležité je také uvědomit si, že útočník si může „poskládat" uvedené údaje z různých zdrojů (ve vyhledávači může např. podle e-mailu zjistit, jaké informace uvede dítě ve svých profilech na Facebook nebo jiných sociálních sítích, na XChatu či jiných diskuzních fórech, v inzerátech na internetu, internetových aukcích apod.).

K citlivým osobním údajům patří také hesla k elektronickým účtům, která by měla být důvěrná minimálně stejně jako PIN kreditní karty. Na svých virtuálních účtech (např. účtu k e-mailu, k chatu, účtu do vzdělávacího prostředí apod.) sice nejsou

---

[32] SMS Spoofing. JAVORČÍK, Tomáš. *Elektronická komunikace* [online]. 2010 [cit. 2013-03-07]. Dostupné z: http://bezpecna-komunikace.budnet.eu/web/spoofing.php.

uložené peníze, ale útočník se jejich prostřednictvím může dostat k osobním údajům a ty zneužít, může s účtem manipulovat, popř. může zneužít virtuální totožnost k nezákonné činnosti. K velmi rizikovému chování patří také zveřejňování osobních fotografií. Ty totiž patří k nejcitlivějším osobním údajům. Jako jedinečný identifikátor směřují ke konkrétní osobě (na rozdíl od jména, příjmení nebo např. adresy bydliště). V řadě kauz byla fotografie oběti účinným nástrojem k vydírání nebo jiným manipulacím.[33]

Seznámit se s riziky – Pokud bude dítě předem vybaveno souborem informací o dané problematice, v tomto případě o kyberšikaně (tj. co přesně je kyberšikana, jak se projevuje, jak ji řešit, koho požádat o pomoc apod.), bude mít mnohem větší šanci problém zvládnout. V tomto směru hraje klíčovou roli prevence, která by měla nastoupit samozřejmě ve chvíli, kdy dítěti poprvé pořídí rodiče mobilní telefon nebo kdy se poprvé připojí na internet. Na prevenci by se měly podílet všechny složky, které se podílí na výchově dítěte, tedy rodina, škola i celá společnost. Tak jako připravují rodiče své děti na to, aby zvládly nástrahy skutečného světa, musí je naučit překonávat i problémy, se kterými se mohou setkat ve světě virtuálním.[34]

[33] KYBERŠIKANA: KYBERNETICKÁ ŠIKANA [online]. Olomouc, 2010 [cit. 2013-01-24]. ISBN 978-80-254-7791-5. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd. Studie. UP.

[34] KYBERŠIKANA: KYBERNETICKÁ *ŠIKANA* [online]. Olomouc, 2010 [cit. 2013-01-24]. ISBN 978-80-254-7791-5. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd. Studie. UP.

3 Portály a projekty

3.1 Seznam se bezpečně

Koncem roku 2008 pořádal Seznam.cz ve Švandově divadle v Praze konferenci pro učitele, která mimo jiné účastníkům přiblížila rizika, s nimiž se mohou děti setkat na internetu. O akci byl velký zájmem a měla nečekaný úspěch. Proto se o bezpečnosti na internetu natočil film, který by mohl zasáhnout širší skupinu lidí a nejvíce ohrožených - dětí. Pár týdnů uteklo a 10. dubna 2009 zazněla poslední klapka prvního dílu „*Seznam se bezpečně 1*“. Od té doby se leccos na internetu změnilo a první díl dokumentárně vzdělávacího filmu dostal po třech letech pokračování. Druhý díl *„Seznam se bezpečně! 2“* byl představen v březnu 2012. Mimo jiné se zabývá otázkou, jestli se nejčastější oběti - děti, nestaly i částečně pachateli. Poukazuje na největší hrozbu sociálních sítí tzv. sociální inženýrství a dětskou prostituci. Zároveň otevírá téma, že kyberšikana je přeceňovaný problém a mýtus.[35]

Portál také nabízí pomoc uživatelům internetu. Po kliknutí na odkaz, který je umístěn na stránkách www.seznamsebezpecne.cz lze zvolit hned tři možnosti pomoci. Jako první z nabídky je nahlásit policii, druhá možnost nahlásit závadný obsah na internetu a jako poslední možnost požádat o pomoc pracovníky projektu.

3.2 E-bezpečí

Projekt jako celek byl zahájen v roce 2008 (předcházelo mu období sběru a systematizace dat spojených s online kriminalitou v českém prostředí) díky grantové podpoře Grantové agentury ČR. Grantová podpora trvala do roku 2009, kdy se projekt osamostatnil a začal fungovat jako jeden z klíčových projektů Pedagogické fakulty UP v Olomouci.

---

[35] O projektu. *Seznam se bezpečně!* [online]. 1996-2011 [cit. 2013-03-13]. Dostupné z: http://www.seznamsebezpecne.cz/o-projektu.

Základním východiskem činnosti projektu je terénní práce s nejrůznějšími cílovými skupinami, přednášková činnost, preventivní vzdělávací akce apod. Přednášky/besedy mapují jak konkrétní nebezpečné jevy, tak možnosti prevence a obrany proti útočníkům. Představa o problematice je vytvářena na základě modelových situací i skutečných kauz. Besedy jsou multimediální, jsou doprovázeny prezentací a videoukázkami.

Mezi cílové skupiny projektu E-Bezpečí patří žáci a studenti (od 1. stupně ZŠ), učitelé, preventisté sociálně patologických jevů, metodice prevence, policisté (městská policie, Policie ČR), manažeři prevence kriminality, vychovatelé, pracovníci OSPOD a v neposlední řadě také rodiče.

Kromě vzdělávacích akcí realizuje projekt E-Bezpečí také pravidelná celorepubliková výzkumná šetření zaměřená na rizikovou komunikaci v online prostředí, provozuje také online poradnu, vydává řadu zajímavých tiskovin pro žáky/učitele a realizuje řadu dalších aktivit.

V současnosti je projekt E-Bezpečí dynamicky fungujícím preventivním projektem, který poskytuje pomoc velkému množství uživatelů internetu – dětem i dospělým na adrese www.e-bezpečí.cz . Zároveň nabízí pomocnou ruku všem, kteří se dostali díky některému z online nebezpečí do obtížné situace.[36]

3.3 E-nebezpečí

Projekt je zaměřen na vzdělávací aktivity pro učitele všech typů škol, kteří potřebují získat nové znalosti a dovednosti v oblasti rizikového chování spojeného s využíváním informačních a komunikačních technologií – zejména internetu a mobilních telefonů.

---

[36] O projektu. *E-bezpečí* [online]. 2008-2013 [cit. 2013-03-13]. Dostupné z: http://www.e-bezpeci.cz/index.php/o-projektu/oprojektu.

Portál slouží především pro propagaci a objednání placených kurzů v dané problematice.

3.4 Saferinternet

Národní centrum bezpečnějšího internetu je neziskové nevládní sdružení, založené v roce 2006 jako Online Safety Institute. V lednu 2011 bylo sdružení přejmenováno na Národní centrum bezpečnějšího internetu (NCBI). Jeho cílem je přispívat k bezpečnějšímu užívání internetu, k moderním informačním a komunikačním technologiím, k osvojování etických norem v online komunikaci a napomáhat předcházení i snižování možných sociálních rizik spojených s jejich užíváním. Sdružení je členem celoevropské sítě národních osvětových center bezpečnějšího internetu INSAFE a spolupracuje s mezinárodní sítí horkých linek INHOPE.

NCBI pro uskutečnění svých cílů realizuje řadu projektů, z nichž nejdůležitější je Saferinternet.cz, který usiluje o zvyšování povědomí o bezpečnějším užívání internetu. Podporuje vzdělávání v této oblasti, a to zejména dětí, kterým ubližuje nevhodné a závadné chování na internetu. Poskytuje pomoc, působí proti šíření ilegálního, zejména pedofilního a extremistického obsahu na internetu. Projekt je spolufinancovaný Evropskou komisí.[37]

3.5 Bílý kruh bezpečí

Bílý kruh bezpečí poskytuje odbornou, bezplatnou a diskrétní pomoc obětem a svědkům trestných činů. BKB poskytuje tři druhy sociálních služeb: odborné sociální poradenství, telefonickou krizovou pomoc a službu intervenčního centra.[38]

---

[37] O nás. *Safer internet* [online]. 2011 [cit. 2013-03-13]. Dostupné z: http://www.saferinternet.cz/o-nas.

[38] Poslání a činnost. *Bílý kruh bezpečí* [online]. 2007 [cit. 2013-03-13]. Dostupné z: http://www.bkb.cz/

Praktická část

4 Cíle a metodika práce

4.1 Cíl práce

Cílem práce je provedení analýzy negativních vlivů působících na děti ve školách i domácím prostředí pomocí dotazníkového šetření. Dále pak zhotovení prezentací na nejčastěji se vyskytující negativní vlivy na internetu, jenž působí na děti. Prezentace budou obsahovat názorné ukázky problematiky. Dále také vizualizace výsledků šetření, statistické zpracování a analýzy zjištěných dat, formulace a ověření hypotéz.

4.1.1 Primární cíle

- Vytvoření výukového materiálu

4.1.2 Sekundární cíle

- Provedení dotazníkového šetření ke zjištění nejčastěji se vyskytujících negativních jevů
- Vizualizace výsledků dotazníkového šetření
- Statistické zpracování
- Analýza zjištěných dat
- Formulace a ověření hypotéz
- Návrh možného preventivního řešení

4.2 Metodika

Nejprve proběhlo dotazníkové šetření mezi studenty druhého stupně základních škol. Na základě provedeného výzkumu byly stanoveny nejčastěji se vyskytující negativní vlivy působící na děti v prostředí internetu. Dále byly zhotoveny přehledy nejrůznějších typů nežádoucích jevů na Internetu, jenž působí na děti ve škole i domácím prostředí a také byly zmíněny možné důsledky a dopady na studenty, kteří se s těmito jevy na vlastní kůži setkali.

Následně proběhlo vybrání nejčastějších negativních jevů a zhotovení výukového materiálu, jenž bude obsahovat animace a jiné mediální prostředky pro názorné ukázky daných jevů. Výukový materiál byl zhotoven tak, aby uvedl dítě do problematiky a předcházel případnému problému při používání internetu.

Dále byla provedena marketingová šetření, a to pomocí marketingového nástroje - dotazník. Na základě provedených výzkumů byly stanoveny míra uvědomění potenciálního nebezpečí; četnosti a druhy jevů, s nimiž se respondenti skutečně setkali, a to se zaměřením na cílovou skupinu 2. stupeň ZŠ - učitele i žáky. V neposlední řadě byla provedena vizualizace výsledků šetření, statistické zpracování a analýza zjištěných dat, formulace a ověření hypotéz.

4.3 Zdroje informací

4.3.1 Primární zdroje dat

Data byla nově získána pomocí dotazníkového šetření a konzultací s učiteli informačních technologií na vybraných základních školách, a to především na Táborsku. Pro sběr dat byla využita technika osobního dotazování, ale také forma elektronického dotazování. Dále byla data získána individuálními rozhovory a konzultacemi se samotnými učiteli. Elektronický dotazník byl po dohodě s vedením škol vyplněn žáky během vyučování, a to pod vedením vyučujících učitelů informačních technologií. Elektronický dotazník byl vytvořen na portálu www.vyplnto.cz. Získané údaje byly statisticky zpracovány a shrnuty do konkrétního závěru.

4.3.2 Sekundárná zdroje dat

Mezi sekundární zdroje lze zařadit data, která byla již jednou publikována. Ze sekundárních zdrojů jsem v práci použil převážně zdroje externí pocházející především z webových portálů uvedených v použité literatuře. Dále byla některá data získána z propagačních materiálů projektu bezpečný kraj.

5 Stanovení hypotéz

Hypotéza je tvrzení o podstatě určité situace ve světě, je to vědecky zdůvodněný předpoklad možného stavu skutečnosti. Na počátku vědeckého poznání stojí domněnka, kterou hypotéza rozpracovává. Hypotéza vzniká, když pátráme po nutné souvislosti mezi fakty, vyžaduje práci badatele, aby mohla být potvrzena či vyvrácena. Můžeme-li na základě faktů vytyčit více hypotéz, upřednostňujeme tu hypotézu, která vysvětluje větší počet faktů. Hypotézu nelze nikdy dokázat, pouze potvrdit nebo vyvrátit.

Byly stanoveny následující hypotézy:

1. Hypotéza

V dotazníkovém šetření zjišťuji setkání s nežádoucími jevy, jež působí na chlapce i dívky v prostředí internetu. Jako nežádoucí jev je brána alespoň jedna kladná odpověď na jednu z pěti otázek 9-13 v dotazníku podaném studentům. Budu posuzovat, zda existuje závislost mezi pohlavím a výskytem nežádoucího jevu. Předpokládám, že mezi výskytem nežádoucího jevu a pohlavím existuje závislost

H_0: Mezi pohlavím a výskytem nežádoucího jevu neexistuje žádná závislost.

H_A: Mezi pohlavím a výskytem nežádoucího jevu existuje závislost.

Odůvodnění

Potvrzení hypotézy předpokládám vzhledem k velmi odvážným módním trendům oblékání, které se dnes velmi často objevují již mezi žákyněmi základních škol. Také mnohdy špatně myšlené či provedené snaze chlapců stáhnout na sebe pozornost dívky. Předpokládám, že většina dotazovaných studentů druhého stupně, kteří se setkali s nežádoucími jevy, které v úvodu práce popisuji, budou právě dívky. Předpokládám, že mezi činností prováděnou na internetu a výskytem nežádoucích jevů existuje nějaká závislost.

2. Hypotéza

Následující hypotéza zkoumá, zda činnost, kterou student stráví většinu času na internetu, souvisí s výskytem nežádoucích jevů. Jako nežádoucí jev je brána alespoň jedna kladná odpověď na jednu z pěti otázek 9-13 v dotazníku podaném studentům.

> **H_0:** Mezi činností prováděnou na internetu a výskytem nežádoucích jevů neexistuje závislost.
>
> **H_A:** Mezi činností prováděnou na internetu a výskytem nežádoucích jevů existuje závislost.

Odůvodnění

Předpokládám, že při většině stráveného času na internetu chatováním a komunikací s ostatními uživateli je mnohem větší pravděpodobnost ke vzniku zárodku internetové kriminality než například při hraní her. U většiny zaznamenaných případů pachatel vyhledával svou oběť právě na sociální síti, či chatové místnosti.

3. Hypotéza

Dále v dotazníkovém šetření zjišťuji, jakou dobu stráví studenti na sociálních sítích. Posuzuji, zda existuje závislost mezi časem stráveným na sociálních sítích a výskytem nežádoucích jevů, které na studenty působí. Jako nežádoucí jev je brána alespoň jedna kladná odpověď na jednu z pěti otázek 9-13 v dotazníku podaném studentům. Předpokládám, že mezi časem stráveným na sociálních sítích a výskytem nežádoucích jevů existuje nějaká závislost.

> **H_0:** Mezi množstvím času stráveným na sociálních sítích a výskytem nežádoucích jevů neexistuje závislost.
>
> **H_A:** Mezi množstvím času stráveným na sociálních sítích a výskytem nežádoucích jevů existuje závislost.

Odůvodnění

Čím více času strávím v rizikovém prostředí, tím větší je riziko vzniku problému, předpokládám tedy že, čas strávený na sociální síti bude mít nějakou souvislost s výskytem nežádoucího jevu.

4. Hypotéza

Vzhledem k rozmachu výskytu nežádoucích jevů na internetu, předpokládám, že většina studentů se zúčastnila přednášky nebo jiné formy prezentace, na které byli poučeni o bezpečném používání internetu. Předpokládám, že studenti se zúčastnili přednášky nebo jiné formy prezentace zaměřené na bezpečné používání internetu.

> **H:**Většina studentů se zúčastnila přednášky nebo jiné formy prezentace zaměřené na bezpečné používání internetu.

Odůvodnění

Dnes velmi diskutované téma, základní školy by se měly stavět k problému zodpovědně a žáky včas varovat. Předpokládám tedy že, se tak u většiny stalo.

5. Hypotéza

Vzhledem k zájmu o dané téma jsem se rozhodl zařadit i hypotézu ověřující, zda existuje závislosti mezi infikováním počítače virem a pohlavím jeho uživatele. Předpokládám, že mezi infikováním studentova počítače virem během používání internetu a studentovým pohlavím existuje nějaká závislost.

> **H_0:** Mezi infikováním studentova počítače a studentovým pohlavím neexistuje závislost.
>
> **H_A:** Mezi infikováním studentova počítače a studentovým pohlavím existuje závislost.

Odůvodnění

Nejvíce zavirované bývají webové stránky obsahující pornografii a většina těchto stránek je tvořena pro klienty mužského pohlaví. Tento fakt by se mohl v závislosti projevit.

6 Dotazníky

6.1 Příprava a realizace dotazníkového šetření

Dotazníkové šetření proběhlo na základních školách i na sociální síti za pomoci Domu dětí a mládeže. Z pěti kontaktovaných škol na Táborsku spolupracovaly dvě základní školy (ZŠ Chýnov a ZŠ Choustník) a střední odborné učiliště ve Stodu. Nástrojem k získání potřebných informací byl elektronický dotazník. Důvodem použití elektronického dotazníku byla jeho snadná dostupnost výsledných dat k dalšímu zpracování a dobrá vypovídací schopnost. Dotazník zkoumal nejčastěji se vyskytující negativní vlivy působící na děti, dále četnosti jevů a míru uvědomění potencionálního nebezpečí. Druhý výzkum byl zaměřen na učitele - nejčastěji řešené problémy vzniklé v prostřednictvím internetu a také míru četnosti konání školení a kurzu pro učitele v dané problematice.

Dotazníkové šetření mezi žáky bylo zaměřeno především na druhý stupeň základních škol, ovšem ke zjištění úplnějšího přehledu, byli dotazováni i studenti středních a vysokých škol.

Výzkum mezi učiteli byl zaměřen především na učitele informačních technologií. Úvodem rozhovoru byl vysvětlen účel, jeho smysl a jakým způsobem má být proveden.

Dotazník podaný mezi studenty obsahoval celkem 14 otázek. U dotazníku podaného studentům byl zvolen kvantitativní druh výzkumu. Úvodní otázky se týkaly osobních údajů. Cílem otázek bylo zjistit nejčastěji se vyskytující negativní vlivy působící na žáky, dále zjistit četnosti jevů a míru uvědomění potencionálního nebezpečí. Otázky byly uzavřené a otevřené.

Druhý výzkum byl proveden mezi učiteli informatiky na základních školách. Byl zvolen kvalitativní druh výzkumu. Výzkum byl proveden formou přímého dotazování učitelů informatiky na základních školách. Rozhovor podstoupili učitelé ze dvou základních škol (ZŠ Chýnov, ZŠ Choustník), jedné školy střední (SOU Stod)

z jedné školy specializované (ZŠ Radenín) a také z výchovného zařízení (Dům dětí a mládeže). Strukturovaný rozhovor byl uskutečněn v měsíci březnu roku 2013. Sloužil především k zjištění nejčastěji řešených problémů vzniklých prostřednictvím internetu a také míru četnosti konání školení a kurzů pro učitele se zaměřením na internetová nebezpečí, také formu konání prezentací pro školení žáků v dané problematice. Rozhovor měl celkem 11 otázek. Úvodní otázky se týkaly osobních údajů.

6.2 Vyhodnocení prvního dotazníkového šetření

Vzhledem k faktu, že u odpovědí na dotazy týkající se nežádoucích jevů působících na děti, nelze určit, zda se jedná například o přítele, který vyžadoval intimní fotografie (tyto fotografie nebyly nikdy nijak zneužity), nebo fotografie, které byly zneužity. Proto budu všechny pozitivní odpovědi pokládat jako nežádoucí jev, jenž může k internetové kriminalitě vést.

Celkem bylo vyplněno 283 dotazníků. První dotazník byl vyplněn pomocí webového portálu www.vyplnto.cz. Návratnost dotazníku činila 90,6 %. Tento dotazník zkoumal nejčastěji se vyskytující negativní vlivy působící na děti, dále četnosti jevů a míru uvědomění potencionálního nebezpečí.

Návratnost dotazníků je dána poměrem vyplněných a zobrazených dotazníků. Jedná se o orientační údaj, který nebere v potaz oslovené respondenty, kteří ani nezobrazili úvodní text (neklikli na odkaz na dotazník). Takto stanovená návratnost dotazníku činila u provedeného dotazníkového výzkumu 90,6 %.

Přehled respondentů

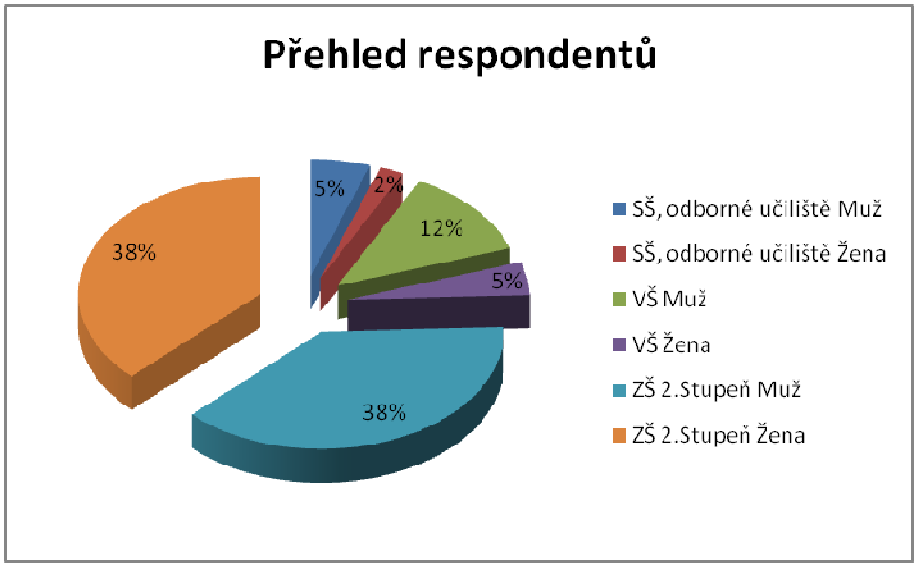
Tabulka 1: Počet odpovídajících studentů

Student	Pohlaví		Celkový počet
	Ženy	Muži	
ZŠ 2. stupeň	106	108	214
SŠ a OU	6	15	21
VŠ	13	35	48
Celkem	158	125	283

Zdroj: vlastní 2013

Grafický přehled respondentů

Graf 1: Přehled respondentů



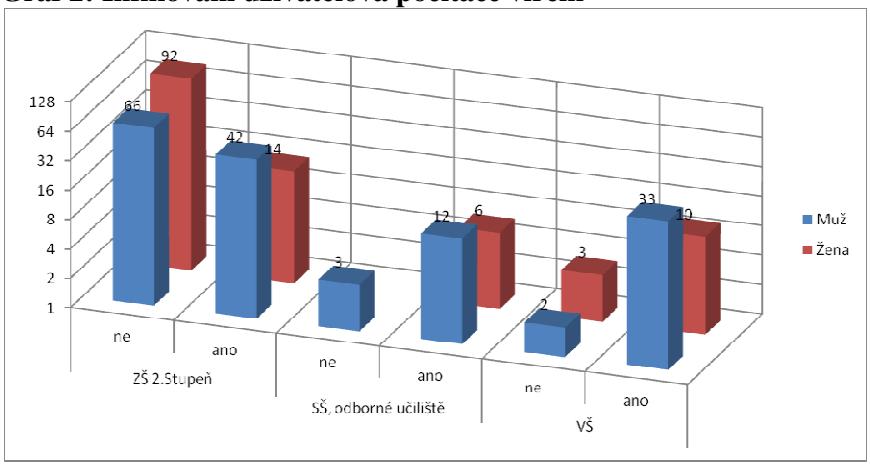
Zdroje: Vlastní výzkum, 2013

Infikování uživatelova počítače virem

Graf č. 2 znázorňuje, jak odpovídali studenti základních, středních i vysokých škol na otázku, zda byl jejich počítač infikován virem. Dále rozděluje respondenty podle pohlaví. Je patrné, že se stářím studentů rostou i zkušenosti s infikováním

uživatelova počítače virem. Většina vysokoškoláků se s infekcí počítače viru již setkala, zatímco na základní škole se převážná část oslovených žáků zatím s virem nesetkala.

Graf 2: Infikování uživatelova počítače virem

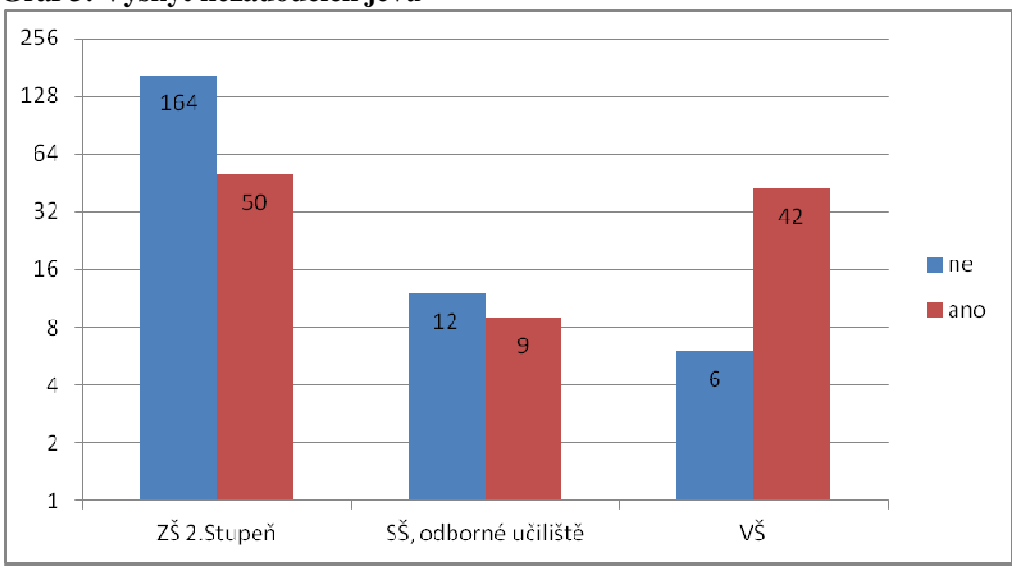


Zdroje: vlastní, 2013

Výskyt nežádoucích jevů mezi studenty

Graf č. 3 zobrazuje výskyt nežádoucích jevů u studentů vysokých a středních škol, ale také u studentů druhého stupně základních škol. Jako nežádoucí jev je brána alespoň jedna kladná odpověď na jednu z pěti otázek 9 -13 v dotazníku podaném studentům. Je zde patrný stejný jev jako u předchozího grafu č. 3. Studentů základních škol, kteří se setkali s potencionálními nežádoucími jevy, je méně jak 30%, zatímco studentů vysokých škol více jak 70 %.

Graf 3: Výskyt nežádoucích jevů

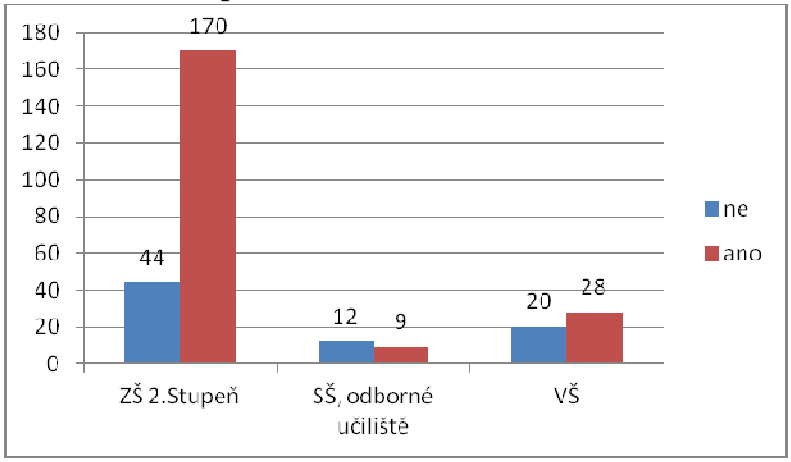


Zdroje: vlastní, 2013

Konání přednášky o bezpečném používání internetu

V dnešní době se informace o internetové zločinnosti a nebezpečí, jež přináší internet, šíří velmi rychle. Jak je patrné z grafu č. 4, školy se snaží na tuto hrozbu reagovat a řešit v porovnání s tím jak tomu bylo v minulosti.

Graf 4: Účast na přednášce



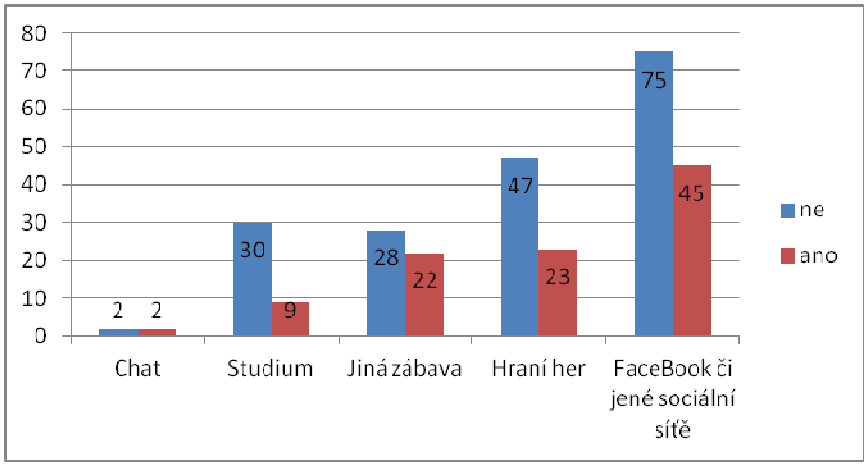
Zdroje: vlastní, 2013

Činnosti na internetu a výskyt potencionálních nežádoucích jevů

Graf č. 5 znázorňuje souvislost mezi výskytem potencionálních nežádoucích jevů a činností, kterou se dotazovaný student zabývá na internetu většinu svého času,

který na něm stráví. Je zřejmé, že nejvíce času věnuje mládež sociálním sítím a počítačovým hrám, kde se také častěji s těmito nežádoucími jevy setkala, což je patrné z grafu č 5.

Graf 5: Výskyt nežádoucích jevů ve vztahu k činnosti

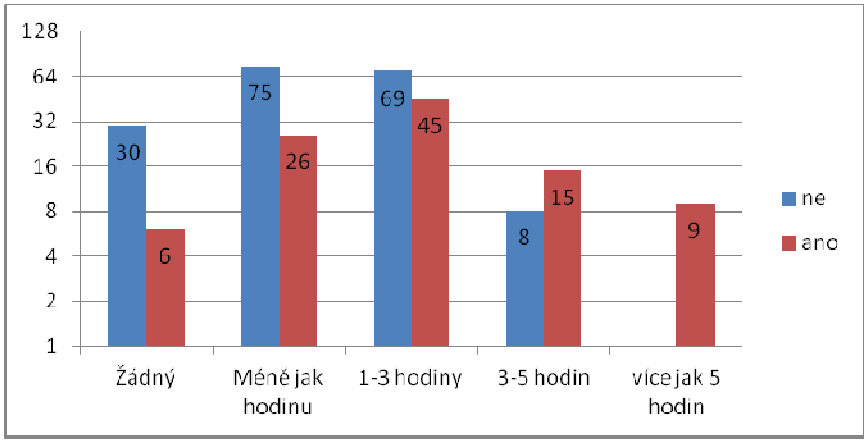


Zdroje: vlastní, 2013

Výskyt potencionálních nežádoucích jevů a čas strávený na sociální síti

Graf č. 6 zobrazuje souvislost mezi výskytem potencionálních nežádoucích jevů a časem stráveným na sociální síti. Je patrné, že s rostoucím časem stráveným na internetu je více výskytu potencionálních nežádoucích jevů.

Graf 6: Výskyt nežádoucích jevů ve vztahu s časem stráveným na sociální síti



Zdroje: vlastní, 2013

6.3 Vyhodnocení druhého dotazníkového šetření

Celkem bylo uskutečněno 6 rozhovorů s následujícími učiteli informatiky a odborných předmětů: Mgr. Vladana Radová, Mgr. Petr Dvořák a Josef Vandělík (ZŠ Chýnov), Ing. Jana Kopecká (SOU Stod), Mgr. Blanka Šimáková (ZŠ Radenín) a Mgr. Hercíková (ZŠ Choustník). Dotazník byl vyplněn na základě odpovědí učitelů během strukturovaného rozhovoru. Návratnost dotazníku činila 100 %. Tento rozhovor zkoumal nejčastěji řešené problémy vzniklé prostřednictvím internetu a také míru četnosti konání školení a kurzů pro učitele se zaměřením na internetová nebezpečí. Dále se zabýval formou konání prezentací pro školení žáků v dané problematice.

V následující tabulce č. 2 je znázorněn přehled dotazovaných učitelů, jejich pohlaví a jaké studenty vyučují.

Tabulka 2: Počet odpovídajících učitelů

Učitel	Pohlaví		Celkový počet
	Ženy	Muži	
ZŠ 1. stupeň	1	0	1
ZŠ 2. stupeň	2	2	4
SŠ a OU	1	0	1
Celkem	4	2	6

Zdroj: vlastní výzkum, 2013

Ze všech dotazovaných učitelů pouze jediný podstoupil školení ve formě přednášky se zaměřením na bezpečné používání internetu. Ostatní učitelé se podobné přednášky nikdy nezúčastnili.

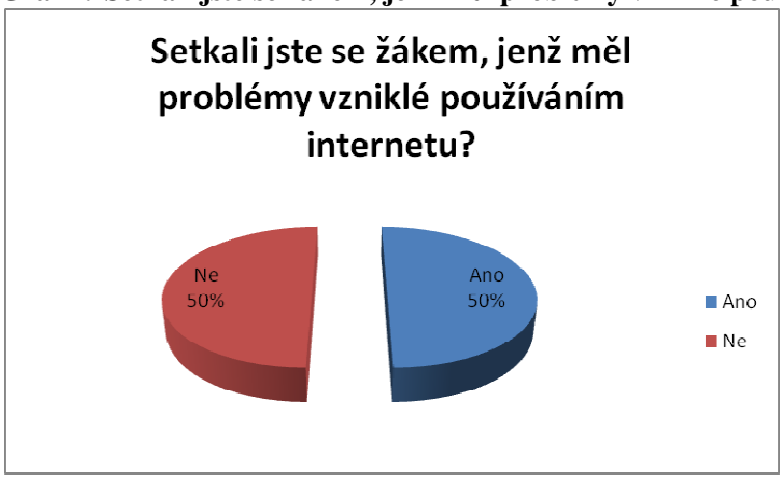
Ačkoliv z dotazníku, který byl podán studentům, vyplynulo, že více jak polovina studentů základních škol druhého stupně se zúčastnila přednášky či jiného druhu prezentace zaměřeného na bezpečné používání internetu. Rozhovor s jejich učiteli

odhalil, že se jednalo o přednášku, která byla uskutečněna prostřednictvím samotných učitelů.

Další z otázek byla zaměřena na zdroje informací, které učitelé použili ke svým prezentacím. Zde jeden dotazovaný učitel uvedl jako zdroj jeho předchozího kolegu, který mu materiály pro přednášku poskytl, jeden z učitelů čerpal z přednášky, která proběhla na předchozí škole, kde vyučoval. Tato přednáška byla zajištěna vedením školy. Ostatní učitelé uvedli jako zdroj informací internet bez konkrétní adresy či názvu webu. Jako klíčové zdroje u dotazovaných učitelů lze tedy považovat internet.

Předmětem otázky, zda se učitel setkal se situací, kdy byl nucen řešit se studentem problém vzniklý během studentova používání internetu, bylo zjistit, zda se u studentů které učí, vyskytly problémy jako je například kyberšikana, sexting, grooming, nebo jakýkoliv jiný problém, z těch které jsem úvodem práce stanovil.

Graf 7: Setkali jste se žákem, jenž měl problémy vzniklé používáním internetu?



Zdroj: vlastní výzkum, 2013

Ze zbylých odpovědí, které se týkaly řešení problémů u studentů vzniklých z používání internetu, reagovali tři ze šesti učitelů kladně. Jeden z učitelů uvedl jako řešený problém zveřejnění intimních fotografií a následné obtěžování žákyně posíláním dotěrných a urážejících zpráv. Ostatní učitelé řešili stejný problém, a to obtěžování zasíláním vulgárních zpráv a vyhrožování.

7 Ověření hypotéz

Při ověřování hypotéz byla data filtrována. Vybráni byli pouze žáci základních škol, jelikož analýza dat prokázala několikanásobně větší výskyt nežádoucích jevů u starších studentů.

1. Hypotéza

Za výskyt nežádoucího jevu u jednoho respondenta považuji alespoň jednu kladnou odpověď u pěti otázek v dotazníku tázajících se na danou problematiku.

Výpočty provádím s 0,05 hladinou významnosti, tedy na 95% předpokládám H_0 .

H_0: Mezi pohlavím a počtem nežádoucích jevů neexistuje žádná závislost.

H_A: Mezi pohlavím a počtem nežádoucích jevů existuje závislost.

Tabulka 3: Hypotéza 1. zjištěné četnosti

Zjištěné četnosti	ne	ano	Celkový součet
Muž	82	26	108
Žena	82	24	106
Celkový součet	164	50	214

Zdroje: vlastní 2013

Tabulka 4: Hypotéza 1. vypočtené četnosti

Vypočtené četnosti	ne	ano	Celkový součet
Muž	82,7663551	25,2336449	108
Žena	81,2336449	24,7663551	106
Celkový součet	164	50	214

Zdroje: vlastní 2013

Tabulka 5: Hypotéza 1. Chí kvadrát pro jednotlivé pole

Chí kvadrát	
0,00709588	0,02327449
0,00722977	0,02371363

Zdroje: vlastní 2013

Chí kvadrát vypočtený	0,06131377
Hladina významnosti	0,05
Stupně volnosti	1
Kritická hodnota z tabulek	3,84145915

3,841 > 0,0613

Závěr:

Vypočítaná hodnota je menší než hodnota z tabulek. H_0 nelze odmítnout, proto nelze ze zjištěných údajů vyvozovat, že by pohlaví mělo vliv na výskyt nežádoucích jevů.

2. Hypotéza

Za výskyt nežádoucího jevu u jednoho respondenta považuji alespoň jednu kladnou odpověď u pěti otázek v dotazníku tázajících se na danou problematiku.

Výpočty provádím s 0,05 hladinou významnosti, tedy na 95% předpokládám H_0.

H_0: Mezi činností prováděnou na internetu a výskytem nežádoucích jevů neexistuje závislost.

H_A: Mezi činností prováděnou na internetu a výskytem nežádoucích jevů existuje závislost.

Tabulka 6: Hypotéza 2. zjištěné četnosti

Zjištěné četnosti	Soc. sítě	Hraní her	Jiná zábava	Studium	Chat	Celkový součet
ne	72	40	22	28	2	164
ano	24	16	10	0	0	50
Celkový součet	96	56	32	28	2	214

Zdroje: vlastní 2013

Tabulka 7: Hypotéza 2. vypočtené četnosti

Vypočtené četnosti	Soc sítě	Hraní her	Jiná zábava	Studium	Chat	Celkový součet
ne	73,570093	42,915888	24,523364	21,457944	1,5327103	164
ano	22,429907	13,084112	7,4766355	6,5420561	0,4672897	50
Součet	96	56	32	28	2	214

Zdroje: vlastní 2013

Tabulka 8: Hypotéza 2. Chí kvadrát pro jednotlivé pole

Chí kvadrát				
0,0335081	0,1981178	0,259645	1,9945293	0,1424664
0,1099065	0,6498264	0,8516355	6,5420561	0,4672897

Zdroje: vlastní 2013

Chí kvadrát vypočtený	11,248981
Hladina významnosti	0,05
Stupně volnosti	4
Kritická hodnota z tabulek	9,487729

9,488 < 11,249

Závěr:

Vypočítaná hodnota je větší než hodnota získaná z tabulek.

H_0 zamítáme, přijímáme H_A tedy ze zjištěných údajů lze vyvozovat, že by činnost prováděná na internetu měla mít vliv na výskyt nežádoucího jevu.

3. Hypotéza

Za výskyt nežádoucího jevu u jednoho respondenta považuji alespoň jednu kladnou odpověď u pěti otázek v dotazníku tázajících se na danou problematiku.

Výpočty provádím s 0,05 hladinou významnosti, tedy na 95% předpokládám H_0.

H_0: Mezi množstvím časem stráveným na sociálních sítích a výskytem nežádoucích jevů neexistuje závislost.

H_A: Mezi množstvím časem stráveným na sociálních sítích a výskytem nežádoucích jevů existuje závislost.

Tabulka 9: Hypotéza 3. zjištěné četnosti

	Výskyt nežádoucích jevů		
Čas na soc. síti	ne	ano	Celkový součet
1-3 hodiny	60	30	90
3-5 hodin	8	2	10
Méně jak hodinu	68	10	78
více jak 5 hodin	0	4	4
Žádný	28	4	32
Celkový součet	164	50	214

Zdroje: vlastní 2013

Tabulka 10: Hypotéza 3. vypočtené četnosti

	Výskyt nežádoucích jevů		
Čas na soc. síti	ne	ano	Celkový součet
1-3 hodiny	68,9720	21,0280	90
3-5 hodin	7,6636	2,3364	10
Méně jak hodinu	59,7757	18,2243	78
více jak 5 hodin	3,0654	0,9346	4
Žádný	24,5234	7,4766	32
Celkový součet	164	50	214

Zdroje: vlastní 2013

Chí kvadrát vypočtený	25,13088
Hladina významnosti	0,05
Stupně volnosti	4
Kritická hodnota z tabulek	9,487729

9,488 < 25,131

Závěr:

Vypočítaná hodnota je větší než hodnota získaná z tabulek.

H_0 zamítáme, přijímáme H_A tedy ze zjištěných údajů lze vyvozovat, že čas strávený na sociálních sítích má vliv na výskyt nežádoucího jevu.

4. Hypotéza

Jako většina studentů je bráno 90% studentů z celkového počtu dotazovaných.

H: Většina studentů se zúčastnila přednášky nebo jiné formy prezentace zaměřené na bezpečné používání internetu.

Dotazovaných studentů se zúčastnilo přednášky nebo jiné formy prezentace zaměřené na bezpečné používání internetu pouze 79%.

Závěr:

Hypotéza byla vyvrácena, většina dotazovaných studentů se kursu či prezentace zaměřené na bezpečné používání internetu nezúčastnila.

5. Hypotéza

H_0: Mezi počtem případů infikování studentova počítače virem během používání internetu a studentovým pohlavím neexistuje závislost.

H_A: Mezi počtem případů infikování studentova počítače virem během používání internetu a studentovým pohlavím existuje závislost.

Tabulka 11: Hypotéza 5. zjištěné četnosti

Zjištěné četnosti	Infikování počítače virem		
Jaké je vaše pohlaví?	ne	ano	Celkový součet
Muž	66	42	108
Žena	92	14	106
Celkový součet	158	56	214

Zdroje: vlastní 2013

Tabulka 12: Hypotéza 5. vypočtené četnosti

Vypočtené četnosti	Infikování počítače virem		
Jaké je vaše pohlaví?	ne	ano	Celkový součet
Muž	79,73831776	28,26168224	108
Žena	78,26168224	27,73831776	106
Celkový součet	158	56	214

Zdroje: vlastní 2013

Tabulka 13: Hypotéza 5. Chí kvadrát pro jednotlivá pole

Chí kvadrát	
2,36700974	6,67834891
2,411670301	6,804355493

Zdroje: vlastní 2013

Chí kvadrát vypočtený	18,26138444
Hladina významnosti	0,05
Stupně volnosti	1
Kritická hodnota z tabulek	3,841459149

3,841 < 18,261

Závěr:

Vypočítaná hodnota je větší než hodnota získaná z tabulek. H_0 zamítáme, přijímáme H_A tedy ze zjištěných údajů lze vyvozovat, že pohlaví má vliv na infikování studentova počítače virem během používání internetu.

8 Tvorba výukového materiálu

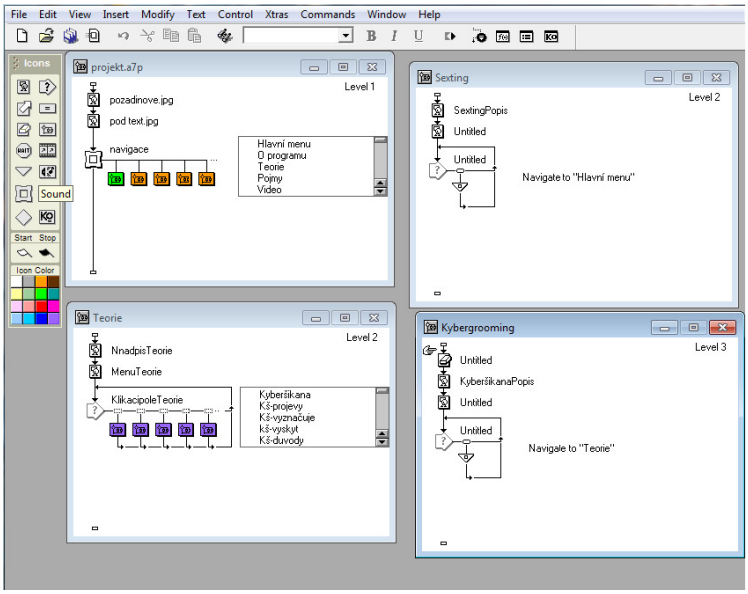
Cílem mé bakalářské práce bylo vytvořit prezentace upozorňující poutavou formou na nežádoucí jevy na Internetu. Na základě provedeného výzkumu mezi žáky a učiteli základních škol jsem se rozhodl vytvořit materiály v programu, jenž by umožňoval více funkcí než obyčejná prezentace a byl tak vhodnějším nástrojem pro tvorbu multimediální formy. Vzhledem k faktu že většina učitelů z dotazovaných škol své žáky školí sama a k tvorbě prezentací využívají materiál umístěný na internetu. Na základě této skutečnosti jsem vytvořil aplikaci, která je vhodná nejen k samotnému prezentování, ale i zároveň obsahuje fakta a materiály navíc. Následující materiály by sloužily nejen učitelům jako podklady pro výuku a školení, ale i samotným žákům, kteří by projevili zájem o dané téma.

8.1 Volba programu pro vývoj

Macromedia Authorware, který je určen k tvorbě výukových materiálů a je jedním z nejpoužívanějších autorských systémů pro tvorbu e-learningových aplikací, integruje grafiku, zvuk, animace, text a video. Tím vznikají velmi přesvědčivá multimediální řešení online výukových kurzů. Umožňuje nejen publikování aplikace přímo pro webové prohlížeče, ale i pro Mac OS a operační systém Windows jako klasická desktopová aplikace. Důvody vedoucí k tvorbě aplikace v prostředí Authorware jsou především rychlé a snadné prostředí pro vývoj interaktivních aplikací, které Authorware nabízí. Dále možnost využití již předpřipravených modulů pro rychlou a intuitivní aplikaci bez nutné znalosti programovacího jazyka. V neposlední řadě skutečnost, že je určen učitelům k tvorbě výukových materiálů, ale i můj vlastní zájem po absolvování krátkého kursu tvorby aplikací v tomto programu vyzkoušet si tvorbu aplikace z pohledu učitele. Jak je patrné na obrázku č. 1. program se může zdát na první pohled jako velmi jednoduchý nástroj na tvorbu aplikací. Nicméně nám nabízí širokou možnost využití. Do programu lze vpisovat vlastní kód, což vytváří nový rozměr tvory v Autorware výsledný program je pak funkcemi omezen pouze na znalosti a zkušenosti programování jeho tvůrce. Začínající tvůrci mohou využít tzv. „Knowledge Objects“, které pomocí průvodce do programu vloží kusy aplikací snadno a rychle. Knowledge Objekty jsou také

nástrojem pro zkušené vývojáře, protože pomocí nich můžeme zjednodušit práci při tvorbě často se opakujících částí aplikace.

Obrázek 1: Prostředí Authorwaru



Zdroje: vlastní 2013

8.2 Struktura programu

Pro navigaci v programu byla vytvořena dvě menu. První menu je znázorněno na obrázku č. 3, kde v levé části je tvořeno z textu, za kterým je tzv. „Hot Spot“ neboli oblast horkého textu, který funguje v principu stejně jako tlačítko. Položky v tomto menu odkazují na jednotlivé prezentace, které jsou určeny pro prezentaci daného pojmu zejména žákům. Druhé menu je umístěno ve spodní části a to v podobě čtyř tlačítek odkazujících na teorii, pojmy, videa a informace o programu. Navigační struktura je tedy velmi jednoduchá a orientace v ní by neměla dělat žákům problém.

Dále v pravé horní části jsou další 4 tlačítka jak, můžeme vidět na obrázku č. 4. Tlačítka ve tvaru šipek slouží k postupnému listování celým programem. Tlačítko s obrázkem dalekohledu slouží pro vyhledávání nejen ve všech textech programu, ale také v názvech jednotlivých snímků a zobrazovaných oken. Poslední z této řady tlačítek je tlačítko pro ukončení aplikace, které po stisku zobrazí dialogové okno, zda

chceme skutečně aplikaci ukončit. Po stisknutí tlačítka ano je aplikace ukončena a po stisknutí tlačítka ne je navrácena do hlavního menu programu.

8.3 Návrh grafického prostředí

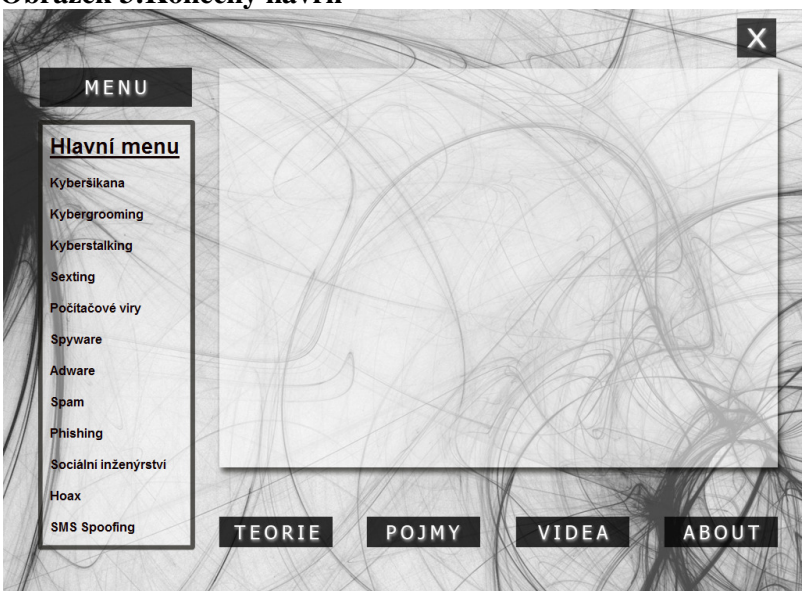
Grafický návrh byl vytvořen v prostředí programu Adobe Photoshop CSS5. V programu byl navržen jednak vzhled aplikace, tak i vzhled tlačítek, která měla být původně bílá s černým ohraničením a stínem na spodní a pravé straně, jak můžeme vidět na obrázku č. 2. Při realizaci grafického vzhledu aplikace jsem ovšem narazil na problém kompatibility při použití formátu PNG - tlačítka po vložení do Authorware byla zobrazena bez stínů a bez alfa kanálu neboli průhlednosti. Při pokusech odstranit tento problém jsem se pokusil použít formát obrázků pro tlačítka TIF, nicméně ani tento formát nebyl podporován. Jako poslední možnost zbýval formát obrázků GIF. Tento formát sice v autorware byl podporován, nicméně jsem se ho rozhodl nepožít z důvodu ztráty kvality při převodu na tento formát.

Obrázek 2: Prvotní návrh

Zdroje: vlastní 2013

Vzhledem k tomu, že do aplikace nemohla být vložena první verze grafického návrhu, rozhodl jsem se vytvořit verzi, v které jsem odstranil stíny a průhlednost, jak můžeme vidět na obrázku č 3. Konečný návrh

Obrázek 3:Konečný návrh



Zdroje: vlastní 2013

Na obrázku č. 4 je vidět konečný grafický vzhled vložený již do aplikace v Authorware. Tlačítka obsahující průhlednost a stíny byla nahrazena tlačítky, která se mohou na první pohled zdát také průhledná, nicméně je to efekt vzniklý v programu Photoshop a do Authorware byly vložené jako obrázky ve formátu JPG. Pozadí, které lze vidět za tlačítkem je pevné, a efekt průhlednosti vzniká přesným umístěním tlačítka oproti textuře na pozadí.

Obrázek 4:Grafika aplikace

Zdroje: vlastní 2013

8.4 Příprava dat

Většina použitých textů jsou materiály zpracovány pro mou bakalářskou práci vzniklé ze zdrojů, jež jsou uvedeny v programu po stisknutí tlačítka about. Jako zdroje, z nich jsem nejvíce čerpal, bych uvedl například portál Seznamsebezpecne.cz, Enebezpeci.cz, It-slovnik.cz a také práce magistra Kamila Kopeckého Ph.D, jež se značnou mírou podílí při tvorbě materiálu na témata bezpečné používání internetu.

8.5 Zhodnocení

Po prvních pár hodinách tvorby mi práce v prostředí programu Macromedia Authorware připadala velmi chaotická a pro učitele, kterým je tento program určen velmi neefektivní a náročná. V počáteční fázi tvorby bych program učitelům, jež s Authorwarem nemají vůbec žádné zkušenosti, nedoporučoval.

Po uplynutí několika hodin následné tvorby jsem pochopil základní strukturu programu a význam jednotlivých ikon a práci s nimi. Program je navržen tak, aby většinu času zabrala spíše příprava textů a odborného materiálu. Nicméně bych tento program učitelům doporučil spíše pro tvorbu jednoduchých aplikací vzhledově

připomínající spíže prezentace a pouze se základními funkcemi, které Authorware nabízí. Aplikace obsahující například texty obrázky videa a základní interakce s nimi. Authorware sice nabízí mnohem více než jen tvorbu jednoduchých výukových aplikací, ale k vytvoření složitější aplikace je nutnost znalosti programování. S největšími problémy jsem se potýkal při vkládání předem vytvořeného grafického návrhu pro vzhled celé aplikace včetně tlačítek. Konkrétně při vytváření vlastního vzhledu tlačítek. Program podporuje průhlednost u tlačítek pouze při vložení obrázků ve formátu GIF. Ovšem při převodu na tento formát dochází ke ztrátě kvality. U tlačítek s importovaným vzhledem nelze měnit jejich velikost. Při vložení webového prohlížeče do programu a použití metody „Navigate“ pro zobrazení konkrétní stránky, následně nelze odstranit či skrýt okno s webovým prohlížečem. Tento problém nastal pouze při použití metody „Navigate“ při ostatních testech s oknem lze běžně pracovat.

Program hodnotím jako velmi účinný nástroj k tvorbě jednoduchých aplikací. Učitelům, jež mají zájem vytvořit výukové materiály ve formě aplikace, a to bez znalosti programování, bych authorware doporučil, nicméně si myslím, že absolvování kursu ovládání tvorby v tomto programu je nutností.

Program je nahrán na CD přiloženém k práci.

9 Návrh možných preventivních opatření

Obecně platí, že čím více informací o rizicích, následcích či průběhu útoků máme, tím větší je šance se případnému útoku ubránit nebo dokonce vyvarovat. Na paměti musíme také mít, že málokterý student bude z vlastní iniciativy vyhledávat rizika určité služby na internetu před jejím použitím. Důraz při prevenci bych kladl na rodiče studentů a také na učitele škol, do kterých studenti docházejí.

9.1 Opatření pro rodiče

Jako jeden z nejdůležitějších bodů prevence v domácím prostředí spatřuji rodičovskou kontrolu činnosti studenta na internetu. Je jasné, že dítě nelze

kontrolovat svou přítomností za jeho zády po celou dobu, kdy je na internetu. Nicméně existuje spoustu velmi účinných metod, které bych se pokusil přiblížit.

Jako první metodu bych uvedl umístění počítače do prostoru, kde se během dne rodiče pohybují nejvíce například do obývacího pokoje. Získají tak kontrolu nad činností, kterou dítě provádí a zároveň svou stálou přítomností či náhodným, ale častým výskytem v místnosti nezíská dítě pocit soukromí. Ze strachu z náhodné kontroly sám bude svou činnost regulovat.

Dále bych doporučil nastavení přístupového hesla do operačního systému počítače. Zamezí se tak používání počítače za zády rodičů, například v době kdy se nacházejí v práci. Dále je potřeba mít kontrolu nad tím, kdy dítě počítač používá.

Výrobci síťových prvků jako je například router či switch jdou rodičům v tomto ohledu vstříc. Při zakoupení a zapojení získají možnost nastavit různé filtry pro používání internetu. Rodiče mají možnost různého nastavení pro více počítačů. Mezi ty nejúčinnější a mnou doporučené patří nastavení filtrování, zákaz používání určitých webů, například stránky, které v názvu obsahují slovo sex nebo jakékoliv jiná zvolená slova. Tento filtr lze také použít obráceně a nastavit pouze ty webové stránky, na které dítě bude mít přístup. Také nastavení času od kdy do kdy zpřístupnit internet. Router vidím jako jeden z nepostradatelných prvků, když chce rodič kontrolovat dobu strávenou na internetu či navštěvované webové stránky.

Před zpřístupněním internetu dítěti bych doporučil si s dítětem sednout a například pomocí mé aplikace s ním projít všechna možná rizika, která na něho v prostředí internetu čekají. Dále jak případné útoky probíhají a jaké mají následky, čemu se vyvarovat a jak rizikům předejít. Věřím, že při dostatečné informovanosti o dané problematice bezpečného používání internetu, mohou rodiče útokům předcházet.

9.2 Opatření pro studenty

Možná opatření pro studenty spatřuji v informovanosti o možných rizicích například pomocí mého programu. Prostudovat průběh útoků a praktiky útočníků. Vždy být podezřívavý. Nevhodný obsah či chování ostatních uživatelů hlásit rodičům či učiteli

ve škole. Počítač zabezpečit pomocí antivirového programu a firewallu. Svůj osobní e-mail na neověřených místech neuvádět, zřídit si pro tyto případy email, který bude vkládat na pochybné webové stránky či aplikace. Používat nejlépe obecnou, nic neříkající přezdívku, nikde neuvádět své jméno a příjmení, adresu atd. Důležité je také uvědomit si, že útočník si může „poskládat“ uvedené údaje z různých zdrojů.

10 Závěr

Cílem bakalářské práce bylo vymezit negativní vlivy působící na děti ve školách i domácím prostředí pomocí dotazníkového šetření. Na základě zjištěných dat zhotovit prezentaci na nejčastěji se vyskytující negativní vlivy na internetu, jež působí na děti.

S rozvojem internetu se rozmáhá i internetová kriminalita. Převážně v dnešní době nemají lidé tušení, jaká nebezpečí na ně v prostředí internetu čekají. Proto je velmi důležité informovat uživatele o možných rizicích.

Portál e-nebezpeci poukazuje na nízkou informovanost učitelů o sociálně-patologických jevech spojených s internetem. Toto se potvrdilo i v mém výzkum prováděném na Táborsku. Ze šesti dotazovaných učitelů pouze jediný podstoupil školení ve formě přednášky se zaměřením na bezpečné používání internetu. Polovina studentů ze základních škol druhého stupně uvedla, že se zúčastnila přednášky či jiného druhu prezentace zaměřeného na bezpečné používání internetu. Avšak rozhovor s jejich učiteli odhalil, že se jednalo o přednášku, která byla uskutečněna prostřednictvím samotných učitelů, kteří převážně čerpali informace z internetu. Proto by byla vhodná a prospěšná mnou navrhnutá prezentace upozorňující na negativní vlivy působící na děti při používání internetu.

Při používání internetu hrozí uživateli různá nebezpečí, ať již kyberšikana, kyberstalking, kybergrooming či sexting. Na Táborsku bylo prokázáno jako nejčastěji řešený problém zveřejnění intimních fotografií, obtěžování zasíláním vulgárních zpráv a vyhrožování. Sami žáci uvedli jako nejčastější problém, s kterým se setkali na internetu, infikování počítače virem. Téměř většina z dotazovaných

žáků nebyla obtěžována neustálým zasíláním zpráv, nesetkala se s pedofilem, či nebyla zastrašována ani ohrožována pomocí internetu.

Nejvíce času věnuje mládež sociálním sítím a počítačovým hrám, kde se také častěji s těmito nežádoucími jevy setkala. Je patrné, že s rostoucím časem stráveným na internetu je více výskytu potencionálních nežádoucích jevů. Největší rizika na internetu spatřují žáci v ohrožení své identity, ztráty soukromí, využití osobních dat i fotografií, dále se obávají infikování počítače virem, atd.

Jako jeden z nejdůležitějších bodů prevence je informovat se o možných rizicích například pomocí mého programu. Prostudovat průběh útoků a praktiky útočníků. Vždy být podezřívavý. Nevhodný obsah či chování ostatních uživatelů hlásit rodičům či učiteli ve škole. Počítač zabezpečit pomocí antivirového programu a firewallu. Svůj osobní e-mail na neověřených místech neuvádět, zřídit si pro tyto případy email, který bude vkládat na pochybné webové stránky či aplikace. Používat nejlépe obecnou nic neříkající přezdívku, nikde neuvádět své jméno a příjmení, adresu atd. Důležité je také uvědomit si, že útočník si může „poskládat“ uvedené údaje z různých zdrojů.

11 Přehled použité literatury

1. E-bezpeci. *Další témata* [online]. 2008 [cit. 2013-01-18]. Dostupné z: http://www.e-bezpeci.cz
2. KOPECKÝ, Kamil. *Moderní trendy v e-komunikaci*. Olomouc: Hanex, 2007, 98 s. ISBN 978-808-5783-780.
3. PROCHÁZKA, David. *První kroky s internetem*. 3., aktualiz. vyd. Praha: Grada, 2010, 108 s. Snadno a rychle (Grada). ISBN 978-80-247-3255-8.
4. JONES, Dennis. *Jak využívat Internet*. Praha: SoftPress, c2001, 398 s. ISBN 80-864-9712-7.
5. VITOVSKÝ, Antonín. *Anglicko-český a česko-anglický výkladový slovník Internetu*. Vyd. 1. Praha: AV software, 2004, 300 s. ISBN 80-901-4287-7.
6. ŽEMLIČKA, Martin. *E-mail, chat, sms: praktický průvodce elektronickou komunikací*. Vyd. 1. Brno: Computer Press, 2003, 110 s. ISBN 80-722-6928-3.
7. MILOŠOVÁ, Taťána. *Kybergrooming jako nebezpečný jev v informačních a komunikačních technologiích*. Zlín, 2011. Bakalářská práce. Univerzita Tomáše Bati
8. PROCHÁZKA, David. *První kroky s internetem*. 3., aktualiz. vyd. Praha: Grada, 2010, 108 s. Snadno a rychle (Grada). ISBN 978-80-247-3255-8.
9. TAYLOR, Chris. *Twitter Has 100 Million Active Users. Mashable* [online]. 2011 [cit. 2011-10-12]. Dostupné z: www.mashable.com/2011/09/08/twitter-has-100-million-active-users/
10. ŠMAHEL, David. *Psychologie a internet: děti dospělými, dospělí dětmi*. Praha: Triton, 2003, 158 s. Psychologická setkávání, sv. 6. ISBN 80-725-4360-1.
11. KYBERŠIKANA: *KYBERNETICKÁ ŠIKANA* [online]. Olomouc, 2010 [cit. 2013-01-24]. ISBN 978-80-254-7791-5. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd. Studie. UP.
12. E-bezpeci. *Ebezpečí* [online]. 2008 [cit. 2013-01-18]. Dostupné z: http://www.e-bezpeci.cz
13. Co je to kyberšikana a jak se projevuje?. *Bezpecne-online* [online]. 2006 [cit. 2013-03-30]. Dostupné z: http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html?highlight=YToxOntpOjA7czoxMjoia3liZXLFoWlrYW5hIjt9
14. WILLARD, N. *Educator's Guide to Cyberbullying and Cyberthreats: Center for Safe and Responsible Use of the Internet. In: Cyberbully.org* [online]. 2007 [cit. 2013-01-24]. Dostupné z: http://www.cyberbully.org/cyberbully/docs/cbcteducator.pdf

15. Kyberšikana. *Bezpecne-online* [online]. 2006 [cit. 2013-03-30]. Dostupné z: http://www.bezpecne-online.cz
16. Kyberšikana II. *Bezpecne-online* [online]. 2006 [cit. 2013-03-30]. Dostupné z: http://www.bezpecne-online.cz
17. MGR.JANA GAJDOŠOVÁ. *Zdravotní a psychické následky kyberšikany mezi dětmi a dospívající mládeží. In: E-bezpeci.cz* [online]. Pedagogická fakulta MU v Brně, 2008 [cit. 2013-01-27]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/dali-rizika/355-zdravotni-a-psychicke-nasledky-kyberikany-mezi-dtmi-a-dospivajici-mladei
18. KOPECKÝ, Kamil. *KYBERGROOMING: NEBEZPEČÍ KYBERPROSTORU* [online]. Olomouc, 2010 [cit. 2013-01-29]. ISBN 978-80-254-7573-7. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie. Studie. UP.
19. BERSON, I. H. *Cybervictims: The Psychosocial Effects of Online Exploitation for Youth. In: Cs.auckland.ac.nz* [online]. 2008 [cit. 2013-01-29]. Dostupné z: http://www.cs.auckland.ac.nz/~john/NetSafe/I.Berson.pdf
20. KOPECKÝ, Kamil. *KYBERGROOMING: NEBEZPEČÍ KYBERPROSTORU* [online]. Olomouc, 2010 [cit. 2013-01-29]. ISBN 978-80-254-7573-7. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie. Studie. UP.
21. MILOŠOVÁ, Taťána. *Kybergrooming jako nebezpečný jev v informačních a komunikačních technologiích.* Zlín, 2011. Bakalářská práce. Univerzita Tomáše Bati.
22. KOPECKÝ, Kamil. *STALKING A KYBERSTALKING: NEBEZPEČNÉ PRONÁSLEDOVÁNÍ* [online]. 2010[cit. 2013-02-12]. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu
23. ŠTĚPÁNKA, *Tůmová. Nová forma psychického teroru.: Asociace forenzních psychologů.* [online]. Praha, 2007 [cit. 2013-03-07]. Dostupné z: http://afp.wz.cz/clanky.doc/Stalking.doc
24. MULLEN, P.E. a kol. The management of stalkers: Advances in Psychiatric Treatment. In: Apt.rcpsych [online]. 2001 [cit. 2013-03-07]. Dostupné z: http://apt.rcpsych.org/cgi/content/full/7/5/335
25. E-bezpečí. LETOCHOVÁ, Kateřina. Sexting *aneb Černobílá budoucnost* [online]. 2008 [cit. 2013-03-07]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/sexting
26. Sexting & Kybergrooming. *Saferinternet* [online]. 2011 [cit. 2013-03-13]. Dostupné z: http://www.saferinternet.cz/pro-rodice/sexting-kybergrooming
27. Sexting. PEDAGOGICKÁ FAKULTA UNIVERZITY PALACKÉHO. *Sexting* [online]. Olomouc, 2009 [cit. 2013-03-07]. Dostupné z: www.sexting.cz.

28. Počítačové viry: popis, prevence a obnovení. JOHNSON, Eric. *MCITP: Microsoft Windows Vista desktop support enterprise study guide* [online]. Indianapolis: Wiley, c2007 [cit. 2013-03-07]. Dostupné z: http://support.microsoft.com/kb/129972/cs
29. HORÁK, Vladimír. Spam. *Spam* [online]. 2006 [cit. 2013-03-07]. Dostupné z: http://uvt1.cuni.cz/email/spam/uvod.html
30. DŽUBÁK, Josef. PHISHING. *HOAX* [online]. 2000 [cit. 2013-03-07]. Dostupné z: http://www.hoax.cz/phishing/.
31. KUČERA, Radek. Pojem Sociální inženýrství. *ABZ.cz: slovník cizích slov - on-line hledání* [online]. 2005 [cit. 2013-03-07]. Dostupné z: http://slovnik-cizich-slov.abz.cz/web.php/slovo/socialni-inzenyrstvi
32. SMS Spoofing. JAVORČÍK, Tomáš. *Elektronická komunikace* [online]. 2010 [cit. 2013-03-07]. Dostupné z: http://bezpecna-komunikace.budnet.eu/web/spoofing.php
33. KYBERŠIKANA: *KYBERNETICKÁ ŠIKANA* [online]. Olomouc, 2010 [cit. 2013-01-24]. ISBN 978-80-254-7791-5. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd. Studie. UP.
34. KYBERŠIKANA: *KYBERNETICKÁ ŠIKANA* [online]. Olomouc, 2010 [cit. 2013-01-24]. ISBN 978-80-254-7791-5. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd. Studie. UP.
35. O projektu. *Seznam se bezpečně!* [online]. 1996-2011 [cit. 2013-03-13]. Dostupné z: http://www.seznamsebezpecne.cz/o-projektu
36. O projektu. *E-bezpečí* [online]. 2008-2013 [cit. 2013-03-13]. Dostupné z: http://www.e-bezpeci.cz/index.php/o-projektu/oprojektu
37. O nás. *Safer internet* [online]. 2011 [cit. 2013-03-13]. Dostupné z: http://www.saferinternet.cz/o-nas
38. Poslání a činnost. *Bílý kruh bezpečí* [online]. 2007 [cit. 2013-03-13]. Dostupné z: http://www.bkb.cz/
39. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

12 Přílohy

12.1 Seznam tabulek

Tabulka 1: Počet odpovídajících studentů 44
Tabulka 2: Počet odpovídajících učitelů 48
Tabulka 3: Hypotéza 1. zjištěné četnosti 50
Tabulka 4: Hypotéza 1. vypočtené četnosti 50
Tabulka 5: Hypotéza 1. Chí kvadrát pro jednotlivé pole 50
Tabulka 6: Hypotéza 2. zjištěné četnosti 51
Tabulka 7: Hypotéza 2. vypočtené četnosti 51
Tabulka 8: Hypotéza 2. Chí kvadrát pro jednotlivé pole 52
Tabulka 9: Hypotéza 3. zjištěné četnosti 52
Tabulka 10: Hypotéza 3. vypočtené četnosti 53
Tabulka 11: Hypotéza 5. zjištěné četnosti 54
Tabulka 12: Hypotéza 5. vypočtené četnosti 54
Tabulka 13: Hypotéza 5. Chí kvadrát pro jednotlivé pole 54

12.2 Seznam grafů

Graf 1: Přehled respondentů 44
Graf 2: Infikování uživatelova počítače virem 45
Graf 3: Výskyt nežádoucích jevů 46
Graf 4: Účast na přednášce 46
Graf 5: Výskyt nežádoucích jevů ve vztahu k činnosti 47
Graf 6: Výskyt nežádoucích jevů ve vztahu s časem stráveným na sociální síti 47
Graf 7: Setkali jste se žákem, jenž měl problémy vzniklé používáním internetu? 49

12.3 Seznam obrázků

Obrázek 1: Prostředí Authorwaru 56
Obrázek 2: Prvotní návrh 57
Obrázek 3:Konečný návrh 58
Obrázek 4:Grafika aplikace 59

12.4 Použité vzorce pro ověření hypotéz

Stanovení hladiny významnosti

Máme možnost vybrat si buď 0,05 nebo 0,01.

Při 0,05 na 95% předpokládáme, že nastane situace v H_0.

Výpočet testovaného kritéria

Vypočítaná hodnota, která se porovnává s hodnotou tabulkovou je suma všech χ^2 z každého řádku tabulky.

$$\chi^2 = \sum [(P - O)^2 : O]$$

P = pozorované četnosti

O = očekávané četnosti podle H_0

Stupeň volnosti

Stupeň volnosti získáváme odečtením jednotky od počtu řádků v tabulce, je li v tabulce 5 řádků supen volnosti je 4.

Stanovení hladiny významnosti

Obvykle máme možnost vybrat si buď 0,05 nebo 0,01.

Při 0,05 na 95% předpokládáme, že nastane situace v H_0.

Stupeň volnosti

Stupeň volnosti získáváme odečtením jednotky od počtu řádků a odečtením jednotky od počtu sloupců v tabulce, výsledné hodnoty spolu vynásobíme, je li v tabulce 5 řádků a 3 sloupce supen volnosti je 8.

$$f = (\check{r} - 1) * (s - 1)$$

ř = počet řádků

s = počet sloupců

12.5 Dotazníky

Příloha 1: Dotazník 1

1. Jaké je vaše pohlaví?

- Muž
- Žena

2. Máte sourozence?

ANO NE

3. Jste žákem či studentem?

- ZŠ 1.stupeň
- ZŠ 2.Stupeň
- SŠ, odborné učiliště
- VŠ

4. Používáte internet?

ANO NE

5. Většinu času, který trávíte na počítači využíváte k ?

- ICQ či jiný AIM client
- FaceBook či jené sociální síťě
- Chat
- Hraní her
- Studium
- Jiná zábava

6. Zůčastnili jste se na vaší škole přednášky nebo jiné formy prezentace zaměřené na bezpečné používání internetu?

ANO NE

7. Byl váš počítač infikován virem během používání internetu?

ANO NE

8. Kolik času průměrně za den trávíte na sociálních sítích jako je Facebook, G+, Twitter...?

- Žádný
- Méně jak hodinu
- 1-3 hodiny
- 3-5 hodin
- více jak 5 hodin

9. Psali (chatovali) jste si s někým, kdo po vás požadoval vaší fotografii, či jiné osobní údaje?

ANO NE

10. Zval vás někdo neznámý na internetu na osobní schůzku?

ANO NE

11. Obtěžoval vás někdo neustálým zasíláním zpráv, emailů, SMS..?

ANO NE

12. Dostal se k vám odkaz na intimní fotografievašeho kamaráda či kamarádky, nebo přímo fotografie?

ANO NE

13. Byli jste ztrapňováni, ohrožováni, nebo zastrašováni někým prostřednictvím internetu? například(zveřejněním fotografie, situace nebo jiných intimních informací?)

ANO NE

14. Co vidíte jako riziko, které na vás čeká na internetu?