

Kyberšikana na základních a středních školách

Cyber Bullying at Primary and Secondary Schools

Bc. Jana Horáková



ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Jana HORÁKOVÁ**
Osobní číslo: **A10705**
Studijní program: **N 3902 Inženýrská informatika**
Studijní obor: **Učitelství informatiky pro střední školy**

Téma práce: **Kyberšikana na základních a středních školách**

Zásady pro vypracování:

1. Zmapujte základní publikované zkušenosti z výskytu kyberšikany na základních a středních školách.
2. U jednotlivých popsáných projevů kyberšikany zhodnoťte jak dopad na příjemné pracovní prostředí, tak způsob realizace kyberšikany z hlediska informatických nástrojů.
3. Popište a vzorově realizujte informatické metody používané v kyberšikaně.
4. Navrhněte možnosti bezpečnostních opatření na informatické úrovni zamezujících realizaci kyberšikany.
5. Posudte míru nebezpečí vyplývající z kyberšikany pro třídní kolektivy.
6. Definujte možná organizační opatření zamezující negativnímu působení kyberšikany.
7. Zhodnoťte komplexně problematiku v kontextu informatických a výchovných aspektů.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. MCQUADE, S., COLT, J., MEYER, N. **Cyber Bullying: Protecting kids and adults from online bullies**. 1st ed. Westport, Conn.: Praeger Publishers, 2009. ISBN 978-0-313-35193-8.
2. PARSONS, L. **Bullied teacher, bullied student: how to recognize the bullying culture in your school and what to do about it**. Markham, ON: Pembroke Publishers, 2005. ISBN 15-513-8190-7.
3. ROGERS, V. **Kyberšikana: pracovní materiály pro učitele a žáky i studenty**. 1. vyd. Překlad Ondřej Vágner. Praha: Portál, 2011. ISBN 978-807-3679-842.
4. E-bezpečí [online]. 2008 [cit. 2012-01-30]. Dostupné z: <http://www.e-bezpeci.cz>.
5. Rady a doporučení proti šikaně [online]. 2011 [cit. 2012-01-30]. Dostupné z: <http://www.proti-sikane.cz>.


Vedoucí diplomové práce: **doc. RNDr. Zdeněk Botek, CSc.**

Ústav krizového řízení

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **21. května 2012**

Ve Zlíně dne 24. února 2012


prof. Ing. Vladimír Vašek, CSc.
děkan




doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá jedním z nejrozšířenějších problémů současné společnosti – kyberšikanou, jež využívá informační a komunikační technologie k tyranizování obětí. Práce je rozdělena na teoretickou a praktickou část. Teoretická část definuje pojmy a problémy týkající se kyberšikany a současně se zabývá zneužíváním a kyberšikanováním pomocí elektronických a komunikačních prostředků. V praktické části je provedena realizace metody kyberšikany z hlediska informačních nástrojů a dále jsou navržena opatření zamezující realizaci kyberšikany.

Klíčová slova: kyberšikana, kyberšikanování, kyberprostor, znaky kyberšikany, druhy kyberšikany, kyberpronásledování, informatické prostředky, informatické metody, kyberagresor, oběť, dopad, prevence.

ABSTRACT

This diploma thesis deals with one of the most common problems of contemporary society - cyberbullying, which uses information and communication technologies to torture victims. The work is divided into the theoretical and the practical part. The theoretical section defines the concepts and issues relating to cyberbullying and at the same time dealing with abuse and cyberbullying by electronic means of communication. In the practical implementation of the method is performed in terms of cyberbullying and information tools are designed to implement measures to prevent cyberbullying.

Keywords: cyberbullying, cyberspace, cyberbullying characters, types of cyberbullying, cyberstalking, IT resources, informatics methods, cyber - attacker, victim, impacts, prevention.

Poděkování:

Mému vedoucímu diplomové práce, panu doc. RNDr. Zdeňku Botkovi, CSc., bych chtěla touto cestou poděkovat za jeho pomoc, odborné náměty, připomínky a konzultace, které mi během zpracování diplomové práce poskytl.

Dále bych chtěla poděkovat všem, kteří se podíleli na tvorbě videa během realizace kyberšikany.

Motto:

„Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.“

Čl. 10 odst. 1 Listiny základních práv a svobod

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD.....	9
I TEORETICKÁ ČÁST	11
1 TEORETICKÉ POJETÍ KYBERŠIKANY	12
1.1 VYMEZENÍ KYBERŠIKANY.....	12
1.1.1 Pojem kyberšikana	12
1.1.2 Kyberšikana ve škole.....	13
1.1.2.1 Kyberšikana na ZŠ	14
1.1.2.2 Kyberšikana na SŠ	14
1.1.3 Zákon a legislativa	15
1.2 ŠIKANA VERSUS KYBERŠIKANA	16
1.2.1 Definice šikany.....	16
1.2.2 Rozdíl mezi šikanou a kyberšikanou.....	17
1.3 DĚLENÍ A ZNAKY KYBERŠIKANY	19
1.3.1 Dělení kyberšikany.....	19
1.3.2 Znaký kyberšikany	20
1.4 PROSTŘEDKY A FORMY	22
1.4.1 Prostředky.....	22
1.4.2 Formy	24
1.5 DRUHY KYBERŠIKANY.....	25
1.5.1 Nářez	26
1.5.2 Obtěžování	26
1.5.3 Pomlouvání	27
1.5.4 Předstírání	27
1.5.5 Prozrazení.....	27
1.5.6 Podvod.....	28
1.5.7 Vyloučení	28
1.5.8 Kyberstalking	28
1.6 DALŠÍ PODOBY KYBERŠIKANY	30
1.6.1 Kybergrooming	30
1.6.2 Sexting.....	32
1.6.3 Happy slapping.....	33
1.6.4 SMS spoofing.....	34
1.6.5 Hoax	34
1.6.6 Phishing.....	35
1.6.7 Pharming	36
1.7 TYPOLOGIE KYBERAGRESORA A OBĚTI	36
1.7.1 Kyberagresor	36
1.7.2 Oběť a netholismus	39
1.8 DOPADY	40
1.8.1 Dopad na oběť	40
1.8.2 Dopad na prostředí	41

1.9	ORGANIZAČNÍ OPATŘENÍ ZAMEZUJÍCÍ KYBERŠIKANĚ.....	42
2	HYPOTÉZY.....	44
II	PRAKTICKÁ ČÁST.....	45
3	REALIZACE A ZAMEZENÍ KYBERŠIKANY.....	46
3.1	ZPŮSOBY REALIZACE KYBERŠIKANY	46
3.1.1	Nářez	47
3.1.2	Obtěžování	48
3.1.3	Pomlouvání	49
3.1.4	Předstírání	49
3.1.5	Prozrazení.....	50
3.1.6	Podvod.....	52
3.1.7	Vyloučení	52
3.1.8	Hoax	53
3.1.9	Happy Slapping	54
3.1.10	Sexting.....	56
3.1.11	Kybergrooming	57
3.1.12	Kyberstalking	59
3.2	ZAMEZENÍ REALIZACE KYBERŠIKANY	61
3.2.1	Vytvoření uživatelského účtu.....	61
3.2.2	Firewall.....	65
3.2.3	Centrum akcí	68
3.2.4	Zabezpečení internetu	71
3.2.5	Antiviry	76
3.2.6	Uzamčení složek	77
3.2.7	Programy pro ochranu dětí na internetu	80
	ZÁVĚR	84
	CONCLUSION	86
	SEZNAM POUŽITÉ LITERATURY	88
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	91
	SEZNAM POJMŮ	92
	SEZNAM OBRÁZKŮ	93
	SEZNAM TABULEK.....	96
	SEZNAM PŘÍLOH.....	97

ÚVOD

Kyberšikana, pro mnoho dětí a mladistvých hrůzostrašný pojem, patří mezi nejčastěji vyskytujícími se problémy dnešního světa, plného stále nových technických vymožeností a technologií. Příčinou je snadná dostupnost internetu, mobilních telefonů a dalších informačních a komunikačních technologií. To způsobuje, že se šikana přesouvá ze tříd, škol a dětských hřišť do kyberprostoru, kde se oběť nemůže agresorovi fyzicky vzepřít a ubránit se.

Kyberšikana v obecném slova smyslu znamená ubližování a terorizování obětí prostřednictvím informačních a komunikačních technologií (ICT). Mezi ICT patří např. mobilní telefon, internet, Skype, atd. Díky těmto technologiím nelze snadno zjistit identitu pachatele, což umožňuje oběť kdykoliv a kdekoliv kyberšikanovat.

Dle dostupných výzkumů se kyberšikana v poslední době rozšířila a bývá tak nečastěji spojována se školním prostředím, neboť nejčastějšími oběťmi jsou právě děti a mládež. Je proto nutné uvědomit si, že děti a mládež mají odlišnou povahu, cítění a myšlení než dospělí jedinci.

Ve společnosti všeobecně panuje několik otázek a hypotéz v oblasti kyberšikany. Je to dáno neustálým rozvojem technických a technologických vymožeností a chápavostí dětí. Zatímco rodiče a prarodiče mnohdy přemýšlí a neví si rady s technikou, děti je v tomto chápání dalece převyšují. Snadněji ovládají a využívají informačních technologií. Nic jim proto nebrání těchto technologií zneužít ke špatným způsobům (chování).

Ve své práci jsem si stanovila následující cíle. Prvním krokem je vyhledat a prostudovat základní poznatky z výskytu kyberšikany na základních a středních školách. Pomocí získaných poznatků z publikací a odborných článků pak budu mít možnost zmapovat výskyt kyberšikany na základních a středních školách.

V druhém kroku cíle zhodnotím dopad na školní prostředí a klima třídy u všech jednotlivých projevů kyberšikany.

V praktické části provedu vzornou realizaci kyberšikany. Po získání poznatků z teoretické části a poznatků z praktické části se pokusím navrhnout bezpečnostní a organizační opatření na informatické úrovni, jež zamezují realizaci kyberšikany.

V předposledním kroku cíle zhodnotím několik hypotéz, které by v této práci měly být prošetřeny. Na základě hypotéz v práci znázorním postupy při realizaci kyberšikany a postupy při zamezení kyberšikany. Mezi takové hypotézy patří např. otázka, jestli se děti a mládež s kyberšikanou již setkali, zda je kyberšikana častějším týráním než šikana, zda se kyberšikana týká výhradně starších žáků či zda kyberšikana probíhá pouze ve škole.

V posledním kroku vyhodnotím celou problematiku kyberšikany.

I. TEORETICKÁ ČÁST

1 TEORETICKÉ POJETÍ KYBERŠIKANY

1.1 Vymezení kyberšikany

1.1.1 Pojem kyberšikana

Kyberšikana (cyberbullying) bývá definována jako trýznění, hrozby, obtěžování, ponižování, ztrapňování nebo jiné útoky mezi mladistvými pomocí internetu, interaktivních a digitálních technologií nebo mobilních telefonů. Má stejné charakteristiky jako nepřímé tradiční šikanování - stává se opakovaně, zahrnuje psychické násilí a je záměrná. [3]

Je to tedy úmyslné, nepřátelské chování, které se opakuje. Cílem je ublížit oběti pomocí informačních a komunikačních technologií. Obecně se dá říci, že je to psychické šikanování. Další definicí může být, že kyberšikana je šikanování jiné osoby, čili ubližování, obtěžování, ztrapňování, zastrasování atd., a to za použití internetu, mobilních telefonů či ostatních informačních a komunikačních technologií (ICT).

Ublížení či poškození může být jak záměrem útočníka, tak důsledkem např. nevhodného vtipu, nedorozumění mezi obětí a útočníkem, nedomyšlením důsledků jednání ze strany útočníka atd. Oběť je poškozována opakovaně, ať už původním útočníkem či osobami, které se do kyberšikany zapojí později. [5]

Kyberšikana probíhá vždy v kyberprostoru, neboli ve virtuálním světě, ve kterém se uživatelé chovají jinak než ve skutečném světě. Uživatelé internetu jsou odvážnější, více riskují a experimentují, aniž by si uvědomili rizika, která jejich chování přináší. Dovedou napsat a šířit v kyberprostoru takové věty, intimnosti a hlášky, které by se nikdy neodvážili povědět lidem tváří v tvář.

Být napaden kvůli svému vzezření nebo původu a ještě k tomu na veřejnosti, je skutečnou agresí. Tentokrát bolest nezpůsobí případné modřiny, ale ponížení, a to pálí úplně stejně. Ponížení znamená něco daleko silnějšího a hlubšího než jen být zesměšněn, dotčen ve své ješitnosti nebo hrdosti. Došlo k zasažení identity, dotyčný se cítí ponížený, bezvýznamný a má pocit, že v očích ostatních neexistuje a ztratil své místo. [1]

Kyberútoky velmi často souvisí s rozvojem šikany ve třídě a často závisí i na věku, neboť s věkem roste mediální vybavenost dětí. V dnešní době dokáže dítě v nízkém věku užívat různé digitální technologie a pracovat na počítači. Není proto divu, že už dnešní žáci čtvrtých tříd na základních školách natáčejí své spolužáky, kamarády a učitele na svůj mobilní telefon. Mnoho z nich si ale neuvědomuje, že v případě nesouhlasu nebo bez vědomí natáčení dotyčné osoby se dopouští porušení zákona o ochraně osobnosti.

Děti a mladí lidé v mnoha případech projevy kyberšikany nevidí. Neví totiž, že se v jejich případě jedná o jednu z forem šikanování a neumí se s ní ani vypořádat. Myslí si, že jim nikdo nemůže pomoci a připadají si tak osamělí.

1.1.2 Kyberšikana ve škole

Poslední dobou je kyberšikana velmi aktuálním tématem, které je ve školách řešeno. Znalost pojmu kyberšikana je mezi dětmi malá, což vyplývá z výzkumů, již byly provedeny několika výzkumnými týmy. Dle některých autorů odborných článků je pro vznik kyberšikany podstatné postavení dítěte ve třídě. Mnoho žáků se kyberšikany příliš nebojí. Myslí si totiž, že se to právě jim nemůže stát i přesto, že kyberšikanu považují za poměrně nebezpečnou.

Nejčastěji ve školách, ať už při výuce informatiky či o přestávkách, děti posílají urážlivé textové zprávy, píší ponižující a nevhodné e-maily. Taktéž ponižují oběti prostřednictvím chatů a ještě mnohem více je ponižují přes sociální sítě, jako jsou Facebook, Twitter, Líbímseti, Lidé a Spolužáci.

Z důvodu stále narůstající agresivity tohoto typu šikany mnoho škol pořádá přednášky, prevence a vytváří letáky a plakáty určené žákům základních a střední škol. Nejvíce proti kyberšikaně bojují právě školy, neboť bylo zjištěno, že téměř polovina kyberagresorů je ze stejné třídy jako jejich oběť, zhruba čtvrtina agresorů je ze stejné školy. Proto mnoho škol využívá projektu minimalizace šikany, ve kterém jsou k dispozici informace a rady vztahující se k této problematice. V neposlední řadě školy zavádí do školního řádu pravidla použití informačních a komunikačních technologií (ICT), mezi které patří používání mobilních telefonů a internetu během vyučování a přestávek.

Žáci staršího věku nebo středoškoláci obvykle vytváří blogy namířené proti svým pedagogům. Na sociálních sítích píší nevhodné a negativní komentáře o učitelích. Mstí se jim i za špatné známky, které dostali na vysvědčení.

1.1.2.1 Kyberšikana na ZŠ

Díky výzkumům bylo zjištěno, že se kyberšikana objevuje častěji na základních než na středních školách. Je to proto, že na základních školách se kyberšikanují děti navzájem, neboť mají velmi malé zkušenosti, jsou důvěřivé, bojí a stydí se někomu staršímu o problému říct.

Polovina letáků a plakátů týkající se kyberšikany jsou orientovány právě pro žáky 3. až 9. tříd. V letácích jsou zveřejněna důležitá telefonní čísla a kontakty na poradenské linky, Linku bezpečí nebo na Policii. Jsou tam také informace, které mají odstranit bojácnost a povzbudit tak dítě ke svěření se někomu s problémem.

1.1.2.2 Kyberšikana na SŠ

Na středních školách se kyberšikana žáků vyskytuje v menším poměru než na základních školách. Velmi znepokojivé je na středních školách, že v mnoha případech jsou oběťmi samotní učitelé. Důvodem mnohdy bývá nuda žáků nebo touha pomstit se a zesměšnit jejich pedagoga.

Bylo zjištěno, že pokud pedagog dodržuje pravidla a je spravedlivý, stává se pro žáka autoritou, a tak obvykle tento učitel nebývá šikanován. V praxi to funguje tak, že se žáci mezi sebou domluví a snaží se pedagoga vydírat a vyprovokovat až k nepřičetnosti, přičemž se žáci navenek tváří klidně a neustále jej provokují urážlivými výroky. Tuhle situaci ostatní spolužáci natáčejí na mobilní telefon a vše vyvěsí na internetové stránky pro pobavení všech lidí. Tyto jevy jsou nejčastěji vystaveny ke zhlédnutí na serveru YouTube.



Obr. 1. *Kyberšikana učitele.* [18]

1.1.3 Zákon a legislativa

V České republice kyberšikana není trestným činem, ale toto chování může nabýt skutkovou podstatu některých trestných činů, může se jednat o vydírání, vyhrožování, utiskování, šíření pornografie, podněcování k nenávisti jednotlivce nebo skupiny osob, stalking (pronásledování) nebo hanobení národa a rasy. [10]

V oblasti školské legislativy jsou základní informace obsaženy v Metodickém pokynu MŠMT č. j. 24 246/2008-6, který upravuje i zásady prevence a řešení kyberšikany. Na základě tohoto dokumentu musí mít každá škola vypracován Program proti šikanování, který je součástí tzv. preventivního programu. [10]

O tom, že se o problematiku kyberšikany zajímá stále širší část odborné veřejnosti, dokazuje, že se v roce 2011 konala konference nazývaná se “Prevence internetové kriminality a děti: technologie, edukace, legislativa.”. V roce 2010 se konala konference na půdě Senátu Parlamentu České republiky s názvem “Kyberšikana a ochrana osobních údajů aneb Kam až to může zajít na internetu”.

Jestliže se kyberšikana vyskytne během vyučování, za její následky zodpovídá škola, jež za chování žáka během školního vyučování a přestávek zodpovídá. Škola či pedagog, jenž kyberšikanu odhalil, má povinnost oznámit policii výskyt a odhalení kyberšikany.

K tomu, aby byl pachatel dopaden, musí dosáhnout 15 let. K trestní odpovědnosti agresorů mladších 15 let nedochází, mohou být ale postiženi jinak nebo jejich rodiče. [10]

Porušení zákona č. 40/1964 Sb., občanského zákoníku, se dopustí ten, kdo natáčí, fotografuje či zveřejňuje snímky bez souhlasu a vědomí dotyčné osoby.

Zákon č. 40/2009 Sb., trestního zákoníku, obsahuje několik paragrafů, které se kyberšikany dotýkají. Právní řád ČR pojem kyberšikana nezná, nicméně poškození se na něj mohou odvolat, neboť obsahuje trestné činy, mezi které se řadí například:

- § 175 Vydírání,
- § 182 Porušování tajemství dopravovaných zpráv,
- § 184 Pomluva,
- § 192 Výroba a jiné nakládání s dětskou pornografií,
- § 230 Neoprávněný přístup k počítačovému systému a nosiči informací,
- § 352 Násilí proti skupině obyvatelů a proti jednotlivci,
- § 353 Nebezpečné vyhrožování,
- § 354 Nebezpečné pronásledování atd.

Zákon č. 127/2005 Sb., o elektronických komunikacích obsahuje mimo jiné i paragrafy týkající se kyberšikany:

- § 67 Identifikace zlomyslných nebo obtěžujících volání,
- § 93 Zneužití elektronické adresy odesílatele atd.

1.2 Šikana versus kyberšikana

1.2.1 Definice šikany

Je to fyzické a psychické týrání, jehož cílem je ublížit, týrat, zastrašovat či omezovat jedince nebo skupinu lidí. Agresor má obvykle převahu nad obětí jak fyzickou, tak početní.

Podle Michala Koláře je šikana systematické zneužívání moci. Je to nemoc skupinové demokracie a má svůj zákonitý vnitřní vývoj. [4]

Se šikanou se lze setkat v rodině, škole, školských zařízeních, sportovním klubu a v zaměstnání. Slovo šikana je odvozeno z původního francouzského slova „chicane“, které znamená zlomyslné obtěžování, pronásledování a týrání.

Ministerstvo školství definuje kyberšikanu jako: *„Šikanování je jakékoliv chování, jehož záměrem je ublížit jedinci, ohrozit nebo zastrašovat jiného žáka, případně skupinu žáků. Je to cílené a obvykle opakované užití násilí jedincem nebo skupinou vůči jedinci či skupině žáků, kteří se neumí nebo z nejrůznějších důvodů nemohou bránit. Zahrnuje jak fyzické útoky v podobě bití, vydírání, loupeží, poškozování věcí druhé osobě, tak i útoky slovní v podobě nadávek, pomluv, vyhrožování či ponižování. Může mít i formu sexuálního obtěžování až zneužívání. Šikana se projevuje i v nepřímé podobě jako nápadné přehlížení a ignorování žáka či žáků třídní nebo jinou skupinou spolužáků.“* [12]

1.2.2 Rozdíl mezi šikanou a kyberšikanou

Podle Michala Koláře není třeba hledat zásadní rozdíl mezi šikanou a kyberšikanou, neboť je jejich podstata stejná. V obou případech existuje násilí, záměrnost a opakování. Školní šikana se přenáší do kyberprostoru, kde role agresorů a obětí zůstávají stejné. [4]

Šikana umožňuje, že oběť a agresor jsou v přímém kontaktu, přesněji řečeno tváří v tvář. V případě kyberšikany si agresori zachovávají odstup od svých obětí, která jim umožňuje anonymitu a pocit bezpečí před odhalením. Pokud agresor oběť šikanuje fyzicky, postižený se mu může fyzicky vzepřít a ubránit, což v kyberprostoru nelze.

Pro agresory je zároveň jednodušší zapomenout na své chování a zmenšit pocit viny, neboť nevidí újmy, které napáchali. Oběť tak snadno ztratí důvěru ke všem lidem, protože nezná pravou identitu pachatele. Pro oběť může tímto způsobem být pachatelem i kdokoliv z jeho blízkých.

Šikana obvykle probíhá za dne např. během školní docházky, zato kyberšikana probíhá kdykoliv během dne i noci a proniká i do jinak bezpečných míst. To všechno způsobuje pocit oběti bezmoci, že se nemá kam schovat a že nikde není v bezpečí.

Před kyberšikanou není úniku, nemusí opakovaně probíhat jako v případě šikany, stačí pouze jednou vyvěsit inkriminovanou fotografii nebo video na internet, odkud ji může kdykoli a kdokoli na světě vidět, tím se mnohonásobně zvyšuje utrpení a trauma oběti.

V kyberprostoru si agresor může vytvořit falešnou identitu a za někoho se vydávat, v případě šikany oběť vždy ví, kdo jej šikanuje.

V neposlední řadě může kyberšikana na rozdíl od šikany vzniknout i v generačním rozdílu, kde školou povinní žáci mohou šikanovat dospělé osoby, lidi z okolí, rodiče či učitele. Je známo několik případů, kdy dospělí lidé kyberšikanovali děti, spolužáky a kamarády svých dětí kvůli pomstě a zesměšnění.



Obr. 2. *Prostředek ICT.* [21]

1.3 Dělení a znaky kyberšikany

1.3.1 Dělení kyberšikany

Podle několika autorů odborných článků se do projevů verbální šikany řadí i kyberšikana, jež se děje pomocí ICT, neboť se za verbální projev považuje psychické týrání. U verbální, neboli slovní agrese je oběti vyhrožováno pomocí mobilního telefonu nebo e-mailu zabitím, mučením a násilím.

Kyberšikana by se teoreticky mohla dělit na skrytou a otevřenou, jež je popsána níže.

Skrytá kyberšikana

Skrytá kyberšikana (Covert Cyberbullying) poukazuje na nepříjemné sociální chování a vztahy, které vedou k izolaci a manipulaci v případě pomluv a obrázků, které se šíří mezi ostatními bez uvědomění oběti. Dále se sem řadí anonymní urážlivé internetové stránky a zneužití anonymity uživatelů k zastrašování oběti.

Otevřená kyberšikana

Otevřená kyberšikana (Overt Cyberbullying) záměrně zneužívá ICT za účelem způsobení újmy a zesměšnění, mezi které patří úmyslné pořizování intimních a inkriminujících fotografií, videí pro trápení a vydírání oběti.

Kyberprávnička Parry Aftab dělí kyberšikanu na dvě kategorie, a to na přímou a nepřímou kyberšikanu.

Přímá kyberšikana

Přímá kyberšikana je posílání zákeřných kódů, kterými jsou viry nebo škodlivé programy, které útočník posílá a které oběti poškozují počítač. Tímto způsobem pak může agresor získat heslo či sledovat svou oběť.

Nepřímá kyberšikana

Nepřímá kyberšikana, neboli kyberšikana pomocí prostředníka, funguje tak, že si agresor pro svůj útok na oběť vybere druhou osobu. Druhá osoba v mnohých případech vůbec netuší, že se dopouští kyberšikany. Takovými prostředníky mohou být i partneři a rodiče oběti, kteří oběť trestají za něco, co ve skutečnosti provedl kyberagresor sám. Mezi další prostředníky se řadí chatovací místnosti, kde agresor svou oběť označí kvůli porušování pravidel a nahlásí ji provozovateli sítě. Agresor dosáhne toho, že provozovatel sítě oběť vyloučí v domněnku, že pravidla skutečně porušuje.

1.3.2 Znaky kyberšikany

Mezi specifické znaky kyberšikany patří:

- Anonymita,
- těžko rozpoznatelná,
- proměna agresora,
- proměna oběti,
- znalosti PC a ICT,
- široké publikum,
- místo,
- čas.

Anonymita

V případě anonymity se velká většina obětí nikdy nedozví, kdo je kyberšikanoval. Agresorovi je umožněno pomocí přezdivek, anonymních (jednorázových) telefonních čísel a e-mailů zachovat si anonymitu. Díky tomu je kyberagresor těžko polapitelný.

Anonymita může být někdy i zdánlivá, neboť lze pomocí vhodné technologie kyberagresora odhalit.

Těžká rozpoznatelnost

Kyberšikana je těžko rozpoznatelná, neboť rodiče a škola nemá k dispozici přímé důkazy, kterých by si na první pohled mohli všimnout, např. modřiny, roztrhané sešity apod.

Není snadné poznat ihned výskyt kyberšikany, neboť se jedná o psychické týrání a oběť se mnohdy o svém problému nikomu nesvěří.

Proměna agresora

Proměna agresora znamená, že agresorem může být kdokoliv na světě. Někdo, kdo nemusí být fyzicky silný, ale navenek vypadá nenápadně a křehce. Kyberagresor ovládá informační a komunikační technologie a někdy se sám stal obětí.

Proměna oběti

Proměnou oběti se rozumí, že agresor si své oběti náhodně vybírá, a to pouze v kyberprostoru. Často se oběťmi stávají děti, které jsou na mobilních telefonech, počítačích a internetu závislé.

Publikum

Publikum pomáhá šířit kyberšikanu tím, že videa, zprávy a fotografie rozesílá dál. Útočník svou oběť opakovaně nekyberšikanuje, stačí vystavit na internet prostředky kyberšikany a publikum bude sledovat utrpení oběti, bavit se tím a šířit dál.

Místo

Před kyberšikanou není úniku. Agresor má možnost týrat kdekoliv a na jakémkoliv místě. Oběť se před ním nikde neschová, ani v bezpečí domova, poněvadž vlastní mobilní telefon nebo může připojit k internetu.

Čas

Oběť se může v případě času neustále vracet k urážlivým SMS, e-mailům či odkazům na internetu. Naopak agresor může svou oběť terorizovat i 24 hodin denně.

1.4 Prostředky a formy

1.4.1 Prostředky

Nejčastějšími prostředky, které pachatelé užívají, patří mobilní telefony a internet. Pomocí mobilního telefonu lze psát výhružné zprávy, fotit a zároveň i natáčet útoky. Tyto snímky jsou pak přes bezdrátovou síť uloženy do počítače a vystaveny na internetu.

Pomocí prostředků lze provádět kyberšikanu následujícím způsobem:

1. Mobilní telefonáty,
2. textové zprávy (SMS),
3. fotografie nebo videa pořízené mobilním telefonem,
4. e-maily,
5. internetové stránky,
6. chat,
7. instant messaging,
8. sociální síť.

Mobilní telefonáty

Mobilními telefonáty je míněno obtěžování neustálými telefonáty, opakované prozváněním a při zvednutí telefonu neodpovídáním. V několika případech útočníci své oběti mobilní telefon ukradnou a vydávají se za něj, tím je oběť omylem považována za agresora.

Textové zprávy

Jsou to zprávy s výhružným nebo útočným obsahem, které mohou být opakovaně posílány oběti z jednorázové SIM karty, kterou lze vyměnit.

Fotografie nebo videa pořízené mobilním telefonem

Fotografie nebo videa pořízené mobilním telefonem lze poslat dál na internet nebo na další mobilní telefon. Pachatel může snadno oběť vydírat, neboť má k dispozici v mobilním telefonu nahrané útoky nebo fotografie, na nichž je oběť zachycena.

E-mailly

E-mailové účty lze jednoduše pořídit pod cizí identitou a pseudonymem, což vede k posílání útočných, hanlivých a zastrašujících zpráv.

Internetové stránky

Internetovými stránkami mohou být hanlivé blogy a osobní stránky o oběti, na které lze vystavit fotografie a videa s obětí. Mnoho služeb na internetových stránkách je zdarma, útočníci mají snadnější cestu vytvářet ankety a pokládat otázky o svých obětech.

Chat

Chat nebo chatovací místnost je prostředek, v němž komunikace probíhá mezi dvěma nebo více lidmi v reálném čase. Prostřednictvím chatu lze zastrašovat a vyhrožovat oběti.

Chat v překladu znamená pokec, přátelský rozhovor a klábosení. Původně se jednalo o textovou podobu, při které se jen psaly znaky.

Instant messaging

Instant messaging je druh internetové komunikace, která probíhá v reálném čase. Patří sem ICQ (I Seek You), Skype, MSN (MicroSoft Network), Miranda atd.

Instant messaging se dá přirovnat k rozhovoru mobilním telefonem v textové formě. V případě potřeby lze připojit webkameru a komunikovat s dalším uživatelem přímo tváří v tvář. Programy lze na internetu zdarma stáhnout a bezplatně jimi komunikovat. Komunikace pomocí IM probíhá v kratším čase než pomocí e-mailu.

Sociální síť

Sociální síť umožňuje spojení s lidmi na celém světě. Mezi tyto síť patří Facebook, Twitter, Google+, Lidé.cz, Líbímseti.cz apod. Síť bývají často zneužívány k rozšiřování pomluv a kyberšikanování. V neposlední řadě si na nich lze vytvořit falešný účet a vydávat se tak za oběť.

Pro lepší pochopení podstaty sociálních sítí je vhodné popsat ty nejrozšířenější v České republice:

Facebook a Twitter jsou nejrozšířenějšími celosvětovými sítěmi, které umožňují komunikovat s ostatními „přáteli“ a sdílet s nimi informace, fotografie a videa.

Google+ patří mezi nově spuštěné sociální síť. Umožňuje poznat nové lidi a být v kontaktu s přáteli a známými. V tomto případě se nemusí vyplnit osobní údaje. Lze sem nahrát fotografie, přidat alba z Google Web Albums atd.

Lidé.cz je sociální síť, kterou využívají uživatelé převážně z České republiky. Zde si vyplní svůj profil, nahrají fotografie a videa a komunikují s jeho dalšími uživateli.

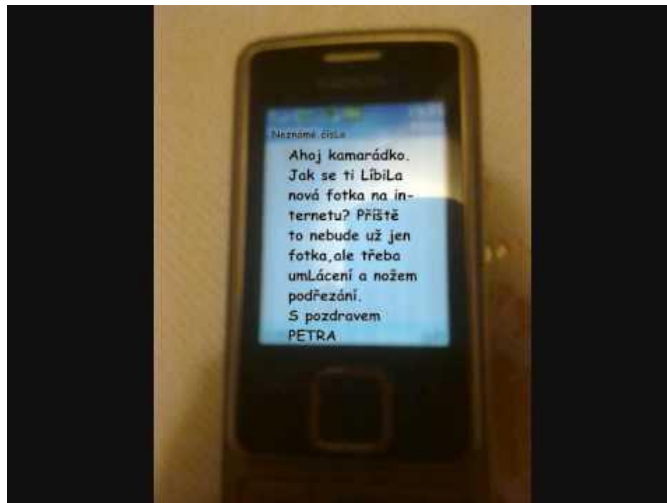
Líbímseti.cz vznikl jako seznamka lidí, kam se uloží fotografie, které ostatní hodnotí a píšou k nim komentáře.

1.4.2 Formy

Formami kyberšikan jsou:

- Falšování identity,
- obtěžování,
- pomlouvání a ponižování,

- ztrapňování,
- provokování a napadení uživatelů v online komunikaci,
- fotografování bez souhlasu nebo vědomí,
- vystavení nahrávek a snímků,
- vyloučení z virtuální komunity,
- zveřejnění cizích tajemství.



Obr. 3. Útočná sms. [25]

1.5 Druhy kyberšikany

Podle Vanessy Rogers [10] mezi druhy kyberšikany patří:

- Nářez (Flaming),
- obtěžování (Harassment),
- pomlouvání (Denigration),
- předstírání (Impersonation),
- prozrazení (Outing),
- podvod (Trickery),

- vyloučení (Exclusion),
- kyberpronásledování (Cyberstalking).

1.5.1 Nářez

Definice a skutečný případ nářezu

Flaming, čili nářez, je odvozen od slova flame, jež znamená hořet. Označuje nepřátelské chování uživatelů na internetu. Jsou to internetové diskuse, které se uskutečňují pomocí elektronických zpráv, které používají útočný jazyk nebo kód. Útočník, flamer, neustále umísťuje do diskusních fór urážlivé vzkazy. Útoky stále stupňuje a své názory hájí.

V tomto případě jde i o provokování. Agresor chce oběť vyprovokovat urážlivými zprávami a přinutit ji podobně komunikovat.

Jeden muž se z nudy přihlásil do diskusního fóra fanoušků fotbalového klubu Slávie. Byl fanouškem konkurenčního klubu a pro své pobavení chtěl popíchnout fanoušky slávistického klubu. Urážel jejich fotbalové hráče i ostatní diskutéry. Po chvíli se k němu přidali ostatní uživatelé a na diskusi mezi nimi vypukla hádka. [7]

1.5.2 Obtěžování

Obtěžování, neboli harassment, je opakované posílání urážlivých nebo nevyžádaných zpráv prostřednictvím mobilních telefonů, e-mailů atd. Jde o jednosměrnou komunikaci a spočívá v tom, že oběť dostává útočné zprávy po připojení se do virtuálního světa nebo při kontrole svého mobilního telefonu.

Obtěžování se nejčastěji objevuje ve škole nebo v zaměstnání a může snadno přejít až ke kyberstalkingu.

Nejčastěji je s termínem harassment spojováno sexuální harašení, které znamená úmyslné obtěžování se sexuálním motivem a které oběť uráží.

1.5.3 Pomlouvání

Definice a skutečný případ pomlouvání

Denigration, neboli pomlouvání, je rozšiřování pomluv a lží o oběti za účelem poškodit ji. Je to informace o druhém, která je zkreslená a nepravdivá. [11]

Pomlouvání může být šířeno pomocí e-mailu, sociálních sítí a instant messaging (IM). Kyberagresor chce získat přátele oběti na svou stranu.

Třináctiletý Ryan z USA se stal obětí šikany. Aby se agresorovi vzepřel, naučil se kickbox a pak se útočníkovi úspěšně vzepřel. To agresora naštvalo a veřejně ho označil za gaye. Aby Ryan dokázal, že je to lež, navázal vztah přes internet s oblíbenou dívkou ve škole. Bohužel, dívka byla domluvena s agresory a Raynova tajemství a informace přeposílala dál ostatním žákům školy. Za jeho zády se mu všichni posmívali. Ryan tento podraz neunesl a oběsil se. [6]

1.5.4 Předstírání

Předstírání, nebo impersonation, je situace, ve které se agresor vydává za oběť – vytvoří falešný profil z jejích fotek nebo používá heslo oběti, aby se dostal k jejím účtům, a následně komunikuje negativně či zveřejňuje nevhodné informace. [6]

Agresor tedy posílá komentáře a vzkazy pod identitou oběti. Přátelé oběti nebo ostatní uživatelé si myslí, že se jedná skutečně o jejich známého, neboť agresor vytvoří falešný profil z fotek oběti nebo získá její přístupové heslo k jeho účtu a komunikuje s nimi.

1.5.5 Prozrazení

Prozrazení je zveřejňování a odhalení osobních a intimních informací uživatelům, pro které původně neměly být určeny. [11]

Je to sdělování cizích a intimních tajemství a informací bez souhlasu dotčené osoby. Termín „Outing“ znamená také úmyslné a veřejné oznámení homosexuální orientace konkrétní osoby bez jejího souhlasu nebo proti její vůli.

1.5.6 Podvod

V případě podvodu je oběť klamána natolik, že považuje konverzaci za soukromou a svěří se, popř. pošle své fotografie agresorovi, který je následně zneužije veřejně. [12]

Oběť je kyberagresorem podváděna kvůli zjištění jejích tajemství a informací, které ji můžou ztrapnit nebo znemožnit. Je to tedy přesvědčení oběti, aby byly citlivé informace a tajemství prozrazeny a zveřejněny na internetu.

1.5.7 Vyloučení

Exclusion, neboli vyloučení, je záměrné vyloučení z virtuální skupiny, skupiny přátel na sociální síti atd. Pro děti a teenagery je přátelství a komunikace s ostatními velmi důležitá, proto má vyloučení pro ně emocionální dopad. K vyloučení může nastat v online hrách, skupinovém blogu nebo IM komunikaci tím, že se oběť vymaže ze seznamu kontaktů.

Vyloučení je úzce spojeno i se skutečným světem, neboť v případě vyloučení jedné osoby ze skupiny na internetu často způsobí i vyloučení ze skutečné skupiny, např. třídy.

1.5.8 Kyberstalking

Definice a skutečný případ kyberstalkingu

Termín kyberstalking poprvé v roce 1999 použil Deirmenjian. Popsal jej jako stalking, neboli pronásledování, v kybernetickém prostoru – „cyberspace“. [2]

Stalking znamená pronásledování, opakované a stupňované obtěžování, které může mít různou podobu a intenzitu.

Kyberpronásledování je opakované posílání ubližujících zpráv, které zahrnují výhrůžky a obsahují množství extrémně útočných a zastrahujících vyjádření včetně vydírání. [12]

V tomto případě se oběť obává o své bezpečí, neboť ji agresor může pronásledovat. Kyberstalking je zneužívání internetu, mobilních telefonů či jiných informačních a komunikačních technologií ke stalkingu.

Patří sem zejména:

- Zasílání obtěžujících e-mailů,
- negativní zprávy o oběti v různých chat-roomech,
- nevyžádané, zlovolné prezentace oběti na různých místech v internetovém prostoru,
- vyhrožování prostřednictvím internetu, elektronická sabotáž (zavirování počítače, slídění v počítači oběti atd.). [2]

Kyberpronásledovatelé se snaží získávat informace od uživatelů diskusních fór o oběti a pod falešnou identitou ji kontaktovat.

Nejčastějšími útočníky jsou muži, přičemž oběťmi jsou častěji ženy. Mnohdy se kyberstalker a oběť znají a měli dříve i blízký nebo intimní vztah.

Kyberstalking je snadno dostupný díky nízkým nákladům, které umožňují oběť neustále terorizovat.

Formy útoků podle Čírtkové [2]:

- Telefonování oběti - 85%,
- pokus kontaktování oběti přes třetí osobu - 65%,
- posílání SMS - 47%,
- posílání e-mailů - 35%,
- objednávání zboží či služby jménem oběti - 10%,

- skryté sledování a fotodokumentace pohybu oběti - 3%.

Jistý Petr H. si vyhlédl za svou oběť - kolegyni z práce na letišti. Ona však jeho zájem a city neopětovala. To jej rozzuřilo a začal ji kyberpronásledovat SMS, e - maily, špehoval ji, dokonce i fyzicky napadl. Za tyhle útoky byl odsouzen ke 250 hodinám veřejně prospěšných prací. Trest nesplnil, a tak mu soud zpřísnil trest k pobytu v vězení na 125 dní. Agresor si ale nástup do vězení odložil kvůli špatnému psychickému stavu. Poškozená upozornila na jeho trestné činy policii, ti se tím nepříliš nezabývali. Petr H. ji nakonec před jejím domem ubil k smrti. Teprve pak po tomto trestném činu byl odsouzen na 15 let. [13]

1.6 Další podoby kyberšikany

Dalšími podobami kyberšikany jsou také:

- Kybergrooming,
- sexting,
- Happy Slapping,
- SMS spoofing,
- hoax,
- phishing,
- pharming.

1.6.1 Kybergrooming

Definice a skutečný případ kybergroomingu

Termín kybergrooming označuje chování uživatelů internetu (predátorů, kybergroomerů), které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce. Kybergrooming je druhem psychické manipulace realizované prostřednictvím internetu, mobilních telefonů a dalších souvisejících technologií. [5]

Je to chování na internetu, které v dítěti vyvolá falešný pocit důvěry. Po získání důvěry pachatel dítě přemluví na schůzku, kde jej pohlavně zneužije. Pachateli jsou často pedofilové.

Nejčastěji se kybergrooming provozuje pomocí chatu, ICQ, seznamky a e-mailu. Oběťmi jsou častěji dívky než chlapci ve věku od 11 do 17 let.

Za kybergrooming se také v širším pojetí považují jakékoliv způsoby manipulace dětí a mladistvých prostřednictvím ICT (např. ve spojení s terorismem a spol.). [17]

Několik etap kybergroomingu:

1. Vzbuzení důvěry a snaha izolovat oběť od okolí (především od rodičů).
2. Vytváření důvěry a podplácení oběti.
3. Vyvolání závislosti oběti na útočníkovi, který se navenek tváří jako důvěryhodný a láskyplný, jehož oběť považuje za jedinečného a výjimečného.
4. Sexuální komunikace, zatahování oběti do komunikace o sexu.
5. Získání diskriminačních materiálů k možnému vydírání (video, fotografie, spodní prádlo, atd.).
6. Osobní setkání (park, ZOO, kino atd.).
7. Sexuální zneužití.

Vrátný v tiskárnách Pavel Hovorka se seznamoval s oběťmi přes chat, inzeráty apod. Všem namluvil, že vybírá děti z dětských domovů do soutěže pro děti atd. Díky tomuto předstírání získal od dětí informace a fotografie, pomocí nichž je následně vydíral a přiměl je k osobním schůzkám. Na schůzkách znásilnil a zneužil 20 chlapců. [13]

1.6.2 Sexting

Definice a skutečný případ sextingu

Je to elektronické rozesílání SMS zpráv, e-mailů, fotografií či videí se sexuálním obsahem. Sexting s využitím ICT nejčastěji provozují děti a mladiství.

Sexting je elektronické šíření textových zpráv, vlastních fotografií či vlastního videa se sexuálním obsahem, ke kterému dochází v prostředí virtuálních elektronických médií - zejména internetu. Mezi platformy, které umožňují šíření těchto materiálů, patří v dnešní době zejména sociální sítě – Facebook, MySpace, Libimseti.cz nebo digitální úložiště fotografií Rajče.net. [23]

Tento druh kyberšikany podporuje šíření dětské pornografie, která je celosvětově zakázána.

Inkriminující a velmi intimní fotografie nebo nahrávky bývají často zveřejněny na internetu. Velmi často v případě rozchodu mladistvého páru.

Není ani vhodné zveřejňovat fotografie v plavkách nebo ve spodním prádle. Nevhodné jsou také fotografie z dětství, na nichž jsou malé děti nahé, mohou být totiž zneužity pedofilem. Je třeba pamatovat i na to, že v případě zveřejnění fotografie na internetu ji už nelze vrátit zpět ani odstranit. Zůstane tam navždy, i když ji autor smaže. Někdo mohl využít chvíle a fotografii si stáhl, nebo byla fotografie uložena někde do databáze.

Třináctiletá žákyně z USA Hope chtěla upoutat pozornost jednoho chlapce, který se jí líbil tím, že mu prostřednictvím mobilního telefonu poslala svou nahou fotografii. Jedna spolužačka chlapce si jeho mobilní telefon půjčila a našla v něm tuto fotografii, kterou posléze přeposlala dalším kamarádkám a kamarádům ze školy. Fotografie se pak rozšířila do dalších škol, přičemž se vedení školy o tom dozvědělo a vyloučilo Hope ze školy. Všichni se jí posmívali a neslušně osočovali. Na jedné akci ji oslovilo několik chlapců, aby jim poslala svou fotografii, na které by byla nahá. Ignorovala je. Po nějaké době ji v kavárně oslovila další skupina chlapců s tím, že má její inkriminovanou fotografii, že přijdou za ní do školy a pak že jí začne peklo. To ji velmi rozrušilo a po tomto incidentu se začala sebepoškozovat. Jednou po večeři s rodiči se jí ozval chlapec, Hope se navenek před rodiči tvářila, že jí volala kamarádka. Odešla do svého pokoje, ve kterém se následně oběsila. [13]

1.6.3 Happy slapping

Definice a skutečný případ happy slappingu

Jde o agresivní chování, kdy si agresor vybere náhodnou oběť a fyzicky ji napadne. Celý útok je natočen nebo vyfocen a záznamy jsou následně umístěny na internetu, kde je může vidět téměř každý. [15]

V překladu „*spokojené fackování*“ je tedy fyzický útok na nic netušící osobu a její reakce, ať už překvapená nebo zděšená, je nahrána na mobilní telefon a poté zveřejněna na internetu, nejčastěji na portálech YouTube, Stream a Ulozto.

Původně se jednalo o vytváření zábavných videí na způsob „skryté kamery“ – tomu odpovídá také náhodný výběr obětí. Tyto „nevinné“ útoky však brzy přerostly v opravdu závažné násilné trestné činy, které v některých případech končily dokonce smrtí obětí. [6]

V některých státech je happy slapping trestným činem.

V roce 2008 napadli dva útočníci neznámého a nic netušícího muže. Útočníkům bylo sedmnáct a devatenáct let. Muž na následky natržení sleziny v nemocnici zemřel. Celý útok natočila na mobilní telefon sedmnáctiletá dívka a nahrávku zveřejnila na internet. Dívka byla odsouzena na 2 roky a útočníci na 6 a 7 let nepodmíněně. [13]



Obr. 4. Útočníci – veselé fackování. [26]

1.6.4 SMS spoofing

SMS spoofing je posílání falešných SMS zpráv z internetu. Oběť zprvu nepozná, že přijatá zpráva je odeslána z internetu, neboť vypadá stejně jako SMS zpráva, jež je odeslána z mobilního telefonu. To znamená, že se kyberagresor může vydávat za jinou osobu či zamýšlenou oběť.

V dnešní době je v České republice SMS spoofing blokován všemi mobilními operátory. Posílání falešných SMS zpráv poskytoval server smsspoofing.com. První dvě SMS zprávy byly posílány z tohoto serveru zdarma, což napomáhalo kyberšikanování.



Obr. 5. Sms spoofing. [24]

1.6.5 Hoax

Termín hoax v překladu znamená falešná zpráva, novinářská kachna nebo poplašná zpráva. Je to nevyžádaná pošta, neboli spam, která varuje před neexistujícím nebezpečím a obsahuje i žádost nebo výzvu o přeposlání. Jedná se o řetězový e-mail kvůli množství dalších adres, na které je hoax přeposílán.

Působí na city příjemce a využívá principy mediální komunikace. Často obsahuje fotografie s postiženými osobami, oběťmi autohavárie, zvířaty atd. Nejznámějším hoaxem je poplašná zpráva s infikovanými injekčními jehlami v tramvaji.

Podle výzkumů hoaxy nejčastěji přeposílají děti, které si zprávy přečtou. Poplašné zprávy u nich ale vyvolají paniku a strach.

Hoax škodí tak, že zaplavuje e-mailové schránky, nebezpečně radí, prozrazuje o uživateli e-mailu důvěrné informace, poškozují firmy a vyvolává zbytečnou paniku a strach.

Poplašné zprávě je třeba nevěřit a všechny nepodložené informace si ověřit.



Obr. 6. Hoax – injekční jehly. [16]

1.6.6 Phishing

V překladu phishing znamená rhybaření. Je to nebezpečná podvodná technika používaná na internetu, jež je zaměřená na získávání citlivých údajů, jako jsou hesla, PIN kódy, informace a údaje k bankovnímu účtu.

Principem je posílání e-mailů nebo zpráv v IM, které vyzývají uživatele, aby zadal své osobní údaje na falešnou internetovou stránku. Stránky jsou velmi podobné těm oficiálním. Příkladem je přihlašovací okno internetového bankovníctví, kam oběť zadá své přihlašovací údaje a heslo. Pachatel na základě těchto údajů vykrade oběti peníze z účtu, nebo uživateleovy údaje prodá.

Proti phishingu lze bojovat specializovanými nástroji, které útoky detekují a upozorní na ně. Dále je potřeba dodržovat i bezpečnostní pravidla.

1.6.7 Pharming

Pharming je nástupce phishingu a v českém jazyce znamená farmaření. Je to podvodný postup na internetu, jak získat citlivá data a údaje od oběti. Princip spočívá v napadení DNS (Domain Name System) a následně přepsání IP (Internet Protocol) adresy oběti. To způsobuje, že je uživatel přesměrován na falešné stránky. Internetové stránky jsou takovým způsobem k nerozeznání od oficiálních, že je ani zkušený uživatelé nerozeznají.

Proti pharmingu lze bojovat antivirovými systémy, správně nakonfigurovanými firewally kvůli ztížení cesty útočníka a specializovanými aplikacemi, např. Netcraft Toolbar.

1.7 Typologie kyberagresora a oběti

1.7.1 Kyberagresor

U kyberšikany nemusí být agresor nutně starší, fyzicky silný a mít kolem sebe partu, která při něm stojí. V kyberprostoru agresorem může být i dívka z dobrého rodinného zázemí. V tomto případě může být útočníkem kdokoliv. Agresor si své oběti mnohdy vybírá náhodně a neustále si vytváří nové identity.

Cílem agresorů je šířit nežádoucí informace o svých obětech tak, že se snaží hlavně narušit pevné přátelství nebo zničit reputaci své oběti. [12]

Kyberagresor je k oběti lhostejný, neboť na vlastní oči nevidí emoční utrpení jeho oběti. V důsledku toho cítí v menší míře vinu, stud nebo strach. Mnohdy je takové chování agresora považováno za zbabělé, protože se schovává za obrazovkou svého počítače nebo notebooku.

Útočníci šikanující ve škole nebo školském zařízení mohou i po zazvonění školního zvonku pokračovat v trýznění - kyberšikanovat, neboť je pro ně internet dalším rozšiřujícím prostorem.

Podle Kopeckého a Krejčí [5] existují tzv. sekundární útočníci, neboli šířitelé, kteří posílají dál odkazy na výskyt kyberšikany, čímž se vědomě nebo nevědomě také zapojují do kyberšikanování.

Existují čtyři typy útočníků, které mají typický různý styl kyberšikanování. Každý z nich má svůj motiv k těmto útokům. Důvodem může být nuda, vytahování se před kamarády, posílení svého ega, snaha ponížit a zastrašit oběť, chuť vyzkoušet něco nového a neznámého. Naopak některé dívky chtějí dát vidět své vůdčí postavení v dívčí skupině. Důvodem kyberšikanování může být i snaha vyzkoušet, zda je oběť tak odolná, jak tvrdí.

Čtyři typy kyberagresorů:

1. „Pomstychtivý andílek“.
2. Toužící po moci.
3. „Sprostý holky“.
4. Neúmyslný kyberagresor.

„Pomstychtivý andílek“

Tento typ útočníka se za agresora vůbec nepovažuje. Myslí si o sobě, že napravuje zlo a chrání jak sebe, tak i ostatní před zlým kyberagresorem, který díky jeho zásahu trpí, jak ve skutečnosti má.

Velmi často kyberšikanu sám prožil a teď to vrací zpět. Nejspíše je rozzlobený na svou oběť kvůli tomu, co provedla a myslí si, že pomstou jí uloží správnou lekci. Snaží se tak ochránit svého kyberšikanovaného kamaráda a obvykle jedná sám za sebe bez pomoci ostatních.

Tomuto typu agresora je potřeba nastínit jeho špatné chování a vysvětlit mu, že nikdo nemá právo to řešit právě tímto způsobem - kyberšikanu přebýt další kyberšikanou, protože to situaci ještě zhoršuje. Musí si totiž uvědomit, že se ve skutečnosti chová jako agresor.

Toužící po moci

Kyberagresori toužící po moci chtějí, aby ostatní dělali, co po nich chtějí. Dávají tak najevo svou autoritu a chtějí ostatní ovládat pomocí strachu. Tento typ potřebuje publikum z přátel nebo spolužáků.

Svémi útoky se chlubí, a pokud publikum nereaguje, své útoky stupňuje, dokud publikum nezačne reagovat. V kyberprostoru nejvíce využívá anonymity a velmi málokdy si uvědomí, co provedl.

Typ toužící po moci patří mezi nejnebezpečnější ze čtyř typů.

„Sprostý holky“

Typické agresorky – děvčata hledají zábavu nebo jsou znuděná. Kyberšikana se nejčastěji děje ve skupině a jejich útokům někdy neuniknou ani chlapci. Útoky se můžou dít ve škole, na večírku nebo po skončení vyučování.

Tento typ vyžaduje publikum, aby bylo vidět, jak jsou silné. Chtějí, aby je ostatní obdivovali. Kyberšikanovat přestanou, když zjistí, že je zábava neuspokojila tak, jak si „*spřstý holky*“ představovaly.

Neúmyslný agresor

Tohoto typu kyberagresora v žádném případě nenapadne, že je vůbec agresorem. Předvádí a vydává se za silného „borce“, někoho jiného nebo odpovídá na negativní zprávy plné nenávisti a násilí, aniž by si uvědomil následky svého chování.

Obvykle odpovídá ve vzteku nebo rozmrzelosti kvůli přijatým zprávám, které ho naštvaly nebo i kvůli online videu, jež viděl.

Má sklon se vydávat na internetu za jiné osoby a posílat obětem kyberšikanující zprávy, aniž si uvědomí podstatnost problému. Své útoky realizuje sám a velmi jej překvapí, když je z kyberšikany obviněn.

1.7.2 Oběť a netholismus

Čím má uživatel méně znalostí v oblasti počítačové a mediální gramotnosti, tím se snadněji může stát obětí kyberšikany. Jedná se hlavně o děti a mladistvé, kteří tráví na internetu a počítači mnoho času. Některé zdroje uvádí, že děti mluví s rodiči 50 hodin ročně, ve škole jsou 850 hodin, ale před osobním počítačem sedí až 1500 hodin ročně. Z těchto čísel se dá usoudit, že právě děti, které jsou internetu závislé, jsou snadnějšími oběťmi kyberšikany.

Případné oběti obvykle nejsou seznámeny s riziky, které ICT přináší. Riskují při seznamování se s cizími lidmi na sociálních sítích nebo IM a svěřují jim osobní informace, které se můžou proti nim obrátit. Myslí si, že jim agresor rozumí a že je nezradí. Neuvědomují si přitom, že osoba na druhé straně kyberprostoru může být falešná a zákeřná nebo je to pedofil.

V případě kyberšikany může být obětí jak učitel, tak i oblíbená osoba, jež nemusí být nutně ze sociálně slabé komunity nebo „outsider“. Obětí tedy může být kdokoliv na světě. Mnoho obětí vůbec neví, že mají na internetu internetové stránky a blogy mířené proti nim. Taktéž neví, že je někdo natočil na mobilní telefon a zkradené a upravené video zveřejnil na internet. Většinou se to dozví od blízkých přátel nebo rodiny.

Jak bylo zmíněno výše, nejčastějšími oběťmi kyberšikany jsou děti závislé na internetu. Proto je vhodné v této souvislosti zmínit termín netholismus.

Netholismus je závislost na internetu a na všem, co s tím souvisí. Patří tam hry, psaní e-mailů, chatování, surfování atd.

Hlavními příznaky jsou:

- Ignorování okolí,
- při absenci internetu nervozita nebo agrese,
- špatný stravovací a pitný režim,
- neschopnost odtrhnout se od internetu.

Pokud je uživatel závislý, může postupně ztratit reálné přátele, hobby, zhoršit studijní výsledky a přivodit si zdravotní potíže.



Obr. 7. *Netholismus*. [19]

1.8 Dopady

1.8.1 Dopad na oběť

Kyberšikana může způsobit, že některé oběti ponесou psychické následky až do konce života. Některé oběti přestanou důvěřovat okolí a nikomu nevěří, sociálně se izolují, uzavrou se do sebe, mají snížené sebevědomí, trápí je noční můry, mají strach, sebepoškozují se, přiberou nebo uberou na váze a v horším případě spáchají sebevraždu.

Oběť se cítí v ohrožení, a tak se obvykle projevuje agresivně jak slovně, tak i fyzicky. Nedokáže totiž plně ovládnout svůj hněv. Toto rozpoložení způsobuje obranná reakce a vyrovnávání těla se stresem. Výjimkou není ani kouření, opilství a drogování.

Dopady z psychického hlediska:

- Frustrace,
- úzkost,
- sebevražedné myšlenky,
- dlouhodobá deprese,
- duševní nestabilita,

- sociální izolace,
- nedůvěra k okolí,
- nechť se seznamovat se s novými lidmi,
- pocit osamělosti,
- nízké sebevědomí,
- záškoláctví,
- zhoršení studijních výsledků atd.

Dopady z fyzického hlediska:

- Vyčerpání organismu,
- nechutenství,
- nevolnost,
- bolest hlavy
- kolísavost váhy,
- oslabená imunita,
- sebepoškozování,
- sebevražda.

Oběť si kyberútoky neustále v hlavě přemítá a opakuje, což způsobuje mimo jiné i nesoustředěnost, poruchu spánku, lekavost, zakřiknutost atd. Bojí se otevírat a číst elektronickou poštu, zúčastňovat se komunikace v internetovém kolektivu a má strach z budoucnosti.

1.8.2 Dopad na prostředí

Klima třídy má vliv na chování žáků a jejich studijní výsledky. Kyberšikana má špatný vliv na děti a mladistvé a kazí jinak příjemné klima prostředí.

V negativním školním prostředí nevládne spravedlnost, tolerance a bezpečí. Nepotrestané kyberútoky mají špatný vliv na morální citění žáků a na psychiku obětí.

V prostředí nastávají špatné sociální vztahy a objevují se křivdy, frustrace a osočování. Taková třída často vykazuje horší chování, školní výsledky a výkon.

Motivace žáků se snižuje, často se kvůli pomstě z některých obětí stávají kyberagresoři.



Obr. 8. Facebook – ponížení. [14]

1.9 Organizační opatření zamezující kyberšikaně

Pro prevenci platí několik zásad, kterými by se měli uživatelé ICT řídit, aby snižovali případné kyberútoky. Je třeba nevěřit všem informacím, které se na internetu vyskytují, mohou být nepravdivé. V kyberprostoru uživatel totiž neví, kdo je na druhé straně – pedofil, hacker atd.

Několik důležitých zásad, kterými by se měli žáci řídit:

- Nevěřit neznámé osobě,
- neudávat věk, adresu, číslo na mobilní telefon,

- nevolat zpět na neznámá telefonní čísla ze zahraničí,
- chránit svá hesla a často je měnit,
- opustit pochybné webové stránky,
- nezveřejňovat na profilu věty typu „Příští týden jsem sám doma.“,
- nikdy nevystavovat fotky v plavkách, spodním prádle, fotografie z dětství, domu atd.

Aby se kyberútokům předešlo, je třeba mít počítač v místnosti, kde se nejčastěji zdržuje celá rodina. Dítě tak nemá možnost trávit čas u počítače o samotě. Pokud dítě nedodržuje pravidla, která byla společně s dospělými stanovena, je potřeba mu uložit postih. V neposlední řadě je důležité zabezpečit počítač. V něm lze nastavit rodičovskou kontrolu a také kontrolovat historii navštívených stránek.

Ve školách by organizační opatření měla být popsána ve školním řádu, ve kterém jsou popsány postihy při porušení. V řádu by měl být napsán zákaz používání mobilních telefonů během vyučování. Dále by měly být na všech počítačích školy nastavena práva uživatelů a zablokovány přístupy na nepožadované internetové stránky.

2 HYPOTÉZY

Existuje mnoho hypotéz zaměřující se na palčivou tematiku kyberšikany. Ne vždy jsou vyřčené hypotézy pravdivé.

Z mnoha hypotéz bylo vybráno pět nejpodstatnějších hypotéz, jež vyjadřují podstatu celého problému. Na základě hypotéz budou vytvořeny postupy pro zamezení kyberšikany.

Hypotézy a výsledky:

1. Kyberšikana se rozšiřuje a je častější formou než šikana.

Ano, kyberšikana se rozšiřuje a je častější formou než šikana. Dokazují to mimo jiné i výzkumy, jež byly provedeny. V roce 2010 bylo obětí kyberšikany téměř 50% dětí [5], v roce 2011 se stalo obětí už téměř 60% dětí [27].

2. Starší žáci více kyberšikanují než mladší žáci.

Ano, starší obvykle více kyberšikanují. Podle výzkumu téměř 37% starší žáků kyberšikanuje [5].

3. Na internetu všechny děti komunikují pouze s tím, koho znají.

Ne, téměř 60% dětí komunikuje s cizími osobami [27].

4. Děti se s projevem kyberšikany svěří rodičům.

Ne, 77% dětí uvedlo, že by se s projevem kyberšikany rodičům nesvěřili [5].

5. Mnoho dětí má na několika sociálních sítích založený účet.

Ano, téměř 90% dětí má založen účet na sociální síti [5].

Z hypotéz, které jsou výše uvedeny, lze vyvodit, že se kyberšikana skutečně rozšiřuje a že mnoho dětí komunikuje s cizími osobami. Zarážející je také fakt, že se drtivá většina dětí s projevem kyberšikany svým rodičům nesvěří. Je proto nutné popsat a znázornit projevy realizace kyberútoků. Dále je nutno vytýčit postupy při zamezení realizace kyberšikany.

II. PRAKTICKÁ ČÁST

3 REALIZACE A ZAMEZENÍ KYBERŠIKANY

3.1 Způsoby realizace kyberšikany

Realizace kyberšikany probíhá mnoha způsoby za pomoci použití ICT. Postupy a ukázky realizace kyberšikany jsou popsány níže. Aby realizace kyberšikany proběhla co nejlépe, bylo potřeba nejprve načrtnout na zkušební papír algoritmus a sled všech průběhů kyberšikany. K inspiraci posloužily skutečné příběhy, jež jsou na internetu nebo v publikacích popsány. Neméně důležité bylo i vžít se do role kyberútočníka kvůli uvědomění si jeho myšlení a postupů útoků pro jednotlivé druhy kyberšikany.

Poté byly vytvořeny čtyři fiktivní osoby, z nichž v mnoha případech obětí byla Anička Nováková a kyberagresorem Tadeáš Jedlička. Zbylé dvě postavy byly v některých případech kamarádkami obětí, případně byly účastníky kyberšikany. Následovalo vytvoření e-mailových účtů a účtů na sociální síti Facebook a IM Skype.

Fiktivní osoby	Datum narození	Účet E-mail	Účet Skype	Heslo k e-mailu a Skype	Nick
Anička Nováková	7. 5. 1996	aninka070596@seznam.cz	aninka070596	pora569	Aninka
Tadeáš Jedlička	23. 2. 1995	jedlickastromek@email.cz	jedlickastromek	teda456	Jedlička
Romana Rybičková	1. 8. 1996	rybickarybnik@seznam.cz	rybickarybnik	vega123	Rybička
Pepina Procházková	12. 4. 1996	pepinapepova1@email.cz	pepinapepova	depo789	Pepina

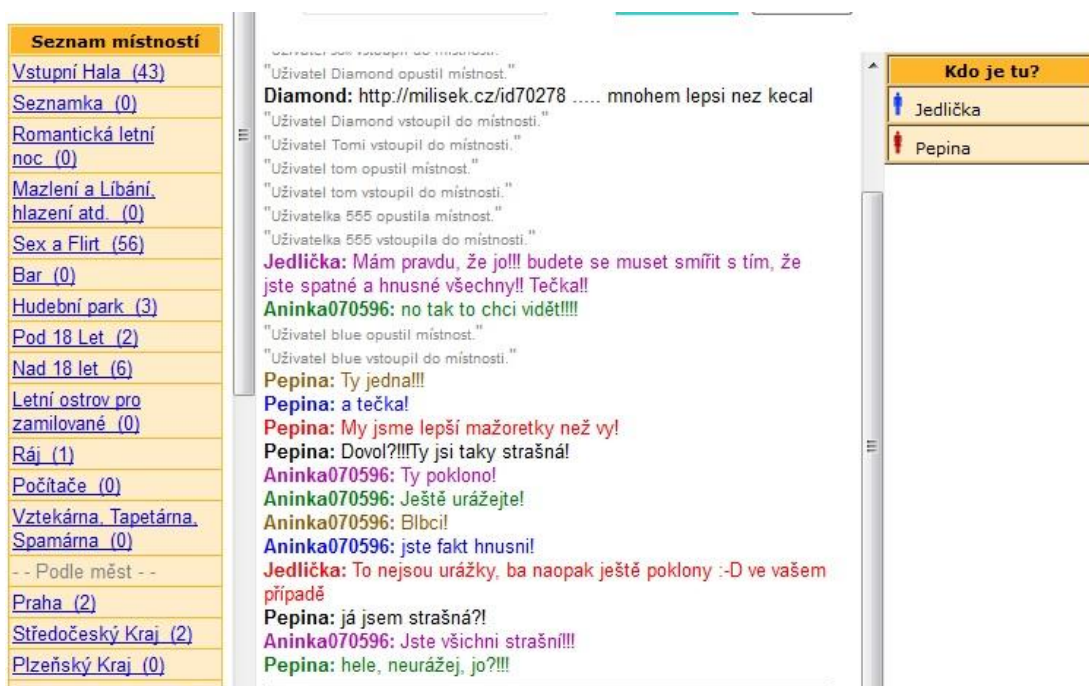
Tab. 1. Vytvořené fiktivní osoby.

3.1.1 Nářez

V případě nářezu chce kyberútočník své oběti vyprovokovat hanlivými a negativními výroky a přinutit je komunikovat podobným způsobem.

Postup u realizace nářezu:

1. Nejprve je potřeba na internetovém prohlížeči vyhledat chatovací místnost, diskusní fórum apod. Pro ukázkou byl vybrán chat na serveru www.kecal.cz.
2. Pro přihlášení do chatovací místnosti je nutné zadat přezdívku, pod kterou bude kyberagresor vystupovat.
3. Na chatu [kecal.cz](http://www.kecal.cz) lze vybrat několik chatovacích místností ze „*Seznamu místností*“. Pro komunikaci byla vybrána místnost „*Zlínský Kraj*“.
4. Po přečtení několika komentářů mezi diskutujícími se může kyberagresor vložit do jejich diskuze a začít psát hanlivé a urážlivé komentáře.
5. Aby oběti kyberútočník vyprovokoval a přinutil je podobně komunikovat, své útoky zvyšoval. Tímto způsobem dosáhl kýženého výsledku – poštvál proti sobě diskutující, které se navzájem znaly.



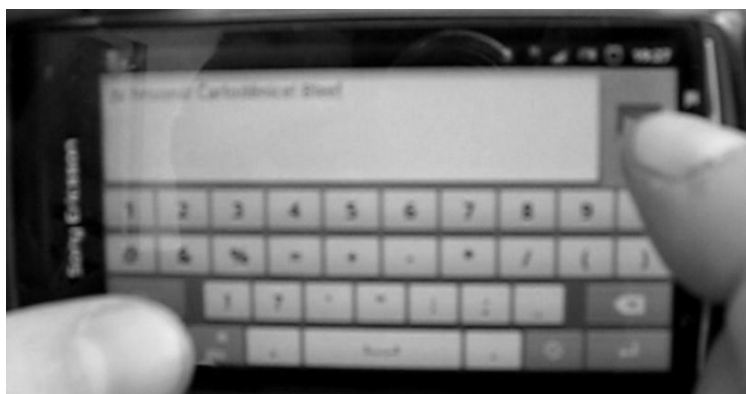
Obr. 9. Flaming na chatu [kecal.cz](http://www.kecal.cz).

3.1.2 Obtěžování

Kyberagresor opakovaně posílá urážlivé textové a e-mailové zprávy. Těmito útoky ponižuje, zesměšňuje a zastrašuje svou oběť. Způsobuje mi nechuť přihlašovat se do virtuálního světa.

Postup u realizace obtěžování:

1. V případě, že kyberútočník nemá telefonní číslo své vyhlédnuté oběti, je nucen si telefonní číslo zjistit. Teprve pak může opakovaně a kdekoliv posílat oběti SMS s urážlivým obsahem. Viz obr. 10.



Obr. 10. *Obtěžování prostřednictvím SMS.*

2. Obtěžovat svou oběť může neustálým telefonováním nebo i prozváněním.
3. Své oběti může mimo jiné neustále posílat negativní e-maily a také zprávy na sociální účet nebo do IM. Viz Obr. 11.



Obr. 11. *Obtěžování prostřednictvím elektronických zpráv.*

3.1.3 Pomlouvání

Pokud chce kyberagresor poškodit oběť a získat její přátele na svou stranu, použije techniku pomlouvání. Jedná se o rozšiřování nepravdivých pomluv a lží.

Postup u realizace pomlouvání:

1. V kyberprostoru lze pro pomluvy a lži využít mobilních telefonů, pomocí nichž lze pomlouvat v telefonním rozhovoru, SMS a MMS.
2. Použit pro pomluvy lze i sociální sítě, IM, blogy a webové stránky.
3. Pro znázornění - kyberútočník Tadeáš Jedlička vyvěsil na svůj profil facebooku lež o Aničce Novákové. Oběti způsobil přetrhání přátelských vazeb mezi ní a jejími virtuálními přáteli díky nařčení o krádeži, viz Obr. 12.



Obr. 12. Pomlouvání na sociální síti FB.

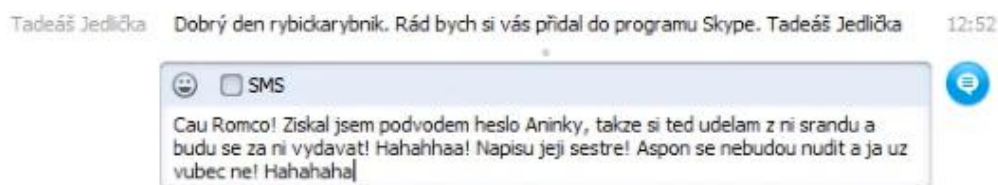
3.1.4 Předstírání

Kyberagresor může svou oběť poškodit a znepřátelit její přátele a rodinu i prostřednictvím techniky předstírání.

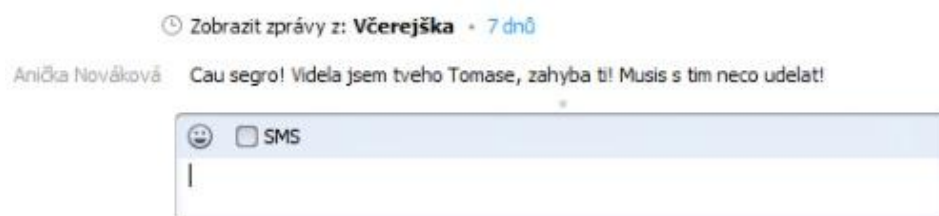
Postup u realizace předstírání:

1. Pro realizaci tohoto způsobu kyberšikany je potřeba získat přístupová hesla oběti.
2. Po přihlášení se do účtu oběti lze negativně komunikovat s jejími přáteli a rodinou.
3. Kromě negativní komunikace může kyberagresor zveřejňovat i citlivé informace.

4. Předstírat a vydávat se za oběť se dá také vytvořením jejího falešného účtu na sociálních sítích. Pro iluzi pravosti profilu oběti lze využít její získané fotografie, ukázky a informace.



Obr. 13. Chlubení se získáním hesla oběti.



Obr. 14. Předstírání prostřednictvím účtu Skype.

3.1.5 Prozrazení

Dalším druhem kyberšikany je technika prozrazení. Kyberagresor prozradí a zveřejní osobní a intimní informace o oběti, aniž by s tím oběť souhlasila či o tom věděla.

Postup u realizace prozrazení:

1. Kyberútočník může vytáhnout od oběti její osobní informaci. Informaci se může dozvědět náhodně nebo od někoho jiného.
2. Tuto intimní informaci prozradí prostřednictvím mobilního telefonu - hovorem, SMS, MMS a nahraným záznamem.
3. Nahraný záznam je zveřejněn na internetové síti, např. na YouTube, Stream, Ulozto.
4. Pro zveřejnění záznamu na serveru youtube.com se musí kyberagresor zaregistrovat a pak záznam do serveru nahrát.

5. Zjištěnou informaci lze prozradit i díky elektronickým zprávám, sociálních sítí apod.
6. V tomto případě techniky kyberagresor, Tadeáš Jedlička, náhodně slyšel soukromý rozhovor. Bez vědomí oběti její intimní informaci všem zveřejnil na svém profilu sociální sítě, viz Obr. 15. a Obr. 16.



Obr. 15. Prozrazení intimní informace o oběti.



Obr. 16. Prozrazení informace na Facebooku.

3.1.6 Podvod

Techniky podvodu se dosáhne klamáním oběti za účelem svěření informací, které ji mohou znemožnit.

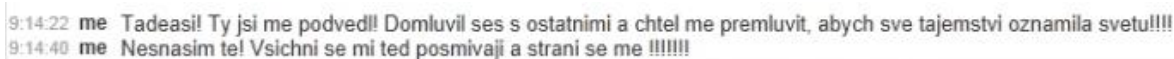
Postup u realizace podvodu:

1. Vytvořit v kyberprostoru příjemné klima a klamat oběť tak, aby měla pocit soukromé konverzace a bezpečí.
2. Během konverzace musí kyberútočník dát oběti najevo, že mu může důvěřovat a svěřit se s tajemstvím, viz Obr. 17.
3. Nyní zbývá oběť přesvědčit, aby své tajemství prozradila a zveřejnila.



16:08:07 me Ahoj Aničko!
16:08:12 me Jak jde život?
16:08:34 Anička Nováková ahoj! Blbě. Mám strach
16:08:49 me Z čeho máš strach?
16:09:01 Anička Nováková to je jedno, prostě je to sobní
16:09:31 me Co může být tak osobního? Mně můžeš důvěřovat, já nic neřeknu, jsem jako vrba
16:09:45 Anička Nováková já vím, ale je to důvěrné
16:10:02 me prosím tě, ničeho se neboj a řekni mi to, já ti určitě pomůžu
16:10:33 Anička Nováková no, ségra je vážně nemocná, je autista.
16:10:45 me co? Určitě to víš jistě?
16:11:03 Anička Nováková jo, zrovna dnes řekli výsledky a já se bojím, že je to dědičné
16:11:15 me to je smůla.
16:11:28 me ale čeho se bojíš? Myslíš si, že tě lidi budou odsuzovat?
16:11:50 Anička Nováková bojím se posměchu, nikdo se se mnou nebude chtít bavit
16:12:15 me neboooj, normálně to napiš na FB a uvidíš, že tě ještě děcka ze třídy podpoří
16:12:29 Anička Nováková já nevím, co kdyby něco...

Obr. 17. Vytvoření soukromé konverzace.



9:14:22 me Tadeasi! Ty jsi me podved!! Domluvil ses s ostatními a chtel me premluvit, abych sve tajemstvi oznamila svetu!!!!
9:14:40 me Nesnasim te! Vsichni se mi ted posmivaji a strani se me !!!!!!!

Obr. 18. Odhalení podvodu.

3.1.7 Vyloučení

Kyberútočník může svou oběť potrestat či znemožnit záměrným vyloučením z online skupiny či smazat ji ze seznamu kontaktů.

Postup u realizace vyloučení:

1. V případě, že online skupina není vytvořená, ji lze jednoduše vytvořit na sociální síti či IM v tomto případě se jedná o třídní skupinu na Skype.
2. Ten, kdo skupinu vytvořil, v tomto případě kyberagresor, pozve účastníky konverzace, které chce ve skupině mít.
3. Pro vyloučení oběti z online skupiny oběť označí a odstraní ji ze skupiny.

17:21:20 Pepina prudi me, ale hodne, mam chut vyloucit, co si o sobe myslis?

17:21:44 Pepina Tak tak, Tadeášku :-DDD

17:21:53 Pepina co navrhujes?

17:22:09 jedlickastromek Romanko klid, ja jsem uplne O.K.

17:22:10 Pepina myslim, co navrhuje Tadeášek :-)

17:22:33 me co tim vyloucenim myslis????

17:22:46 me a co ma navrhnout? Nechapu.....

17:23:04 jedlickastromek Meli by jsme se domluvit jak zatocime s Ancinym ritolectvím!!! Kazi nam povest rebelu na skole!!!

17:23:19 Pepina moje rec! Mas recht

17:23:29 Pepina at si pak nevyskakuje, Kaca jedna

17:23:51 rybickarybnik Ani hlavne klid, za rozcilovani to nestoji!!!!

17:23:52 me proc? Co jsem vam udelala?..-(

17:24:21 jedlickastromek Já bych ti ukázal co stojí, ale to bys nerozchodila princezno!!!

17:24:24 jedlickastromek :-D

17:24:40 Pepina :-D

17:24:48 Pepina tak co, co provedem?

17:25:04 jedlickastromek Nic co bys udelala? my ti taky nic nedelame!!!! Zatím

17:25:17 Pepina vyloučíme Anči

17:25:22 Pepina já ji tu nechci

17:25:25 Pepina at si dela, co chce

17:25:43 jedlickastromek jj jsem pro, tak Romus delej vyhod ji!!!!

17:25:54 Pepina joool

17:26:02 me jste hnusní!

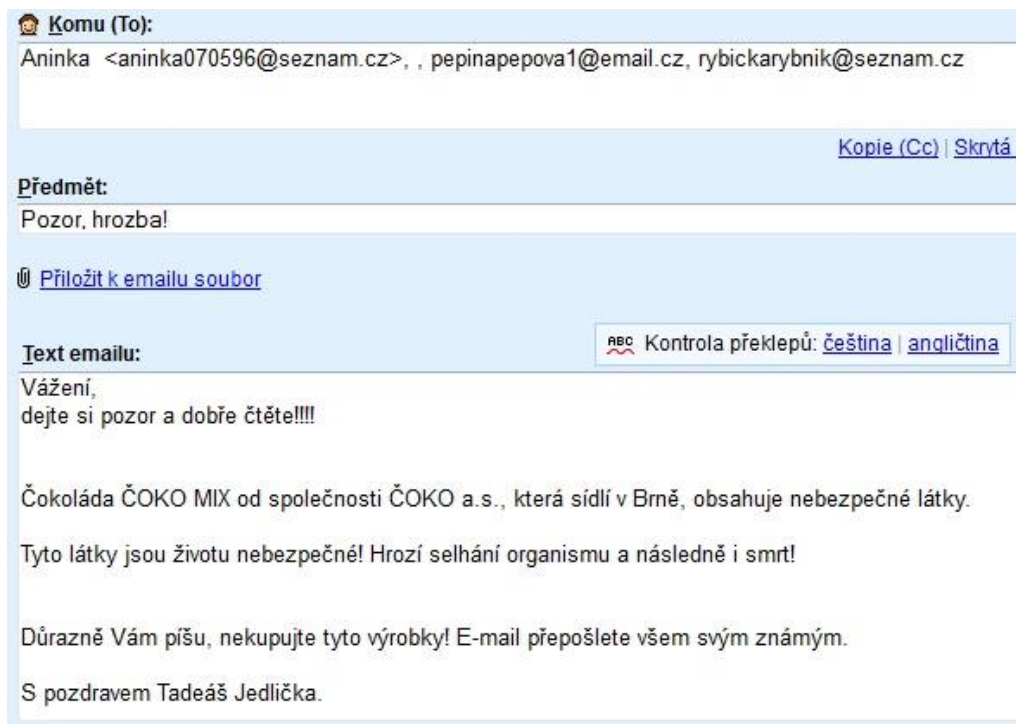
Obr. 19. Vyloučení oběti.

3.1.8 Hoax

Hoax, nevyžádanou poštu a poplašnou zprávu může kyberútočník využít v případě, že chce někoho či něco poškodit. Hoax je vhodný i pro poplazení a vyvolání paniky obětí.

Postup u realizace vytvoření hoaxu:

1. Pro odeslání spamu je nejprve otevřen e-mailový účet a vytvořena nová zpráva.
2. Do seznamu doručitelů jsou zadány e-mailové kontakty a do textu e-mailu je napsána poplašná zpráva, viz Obr. 20.



Obr. 20. Poslání poplašné zprávy.

3. Aby se hoax poslal dál, na konec zprávy se dopíše výzva nebo žádost o další přeposlání.
4. Pokud chce kyberagresor zatlačit na city a emoce doručitele, vloží do přílohy fotografii nebo snímek, např. postižené osoby atd.

3.1.9 Happy Slapping

Prostřednictvím této techniky lze na kteroukoliv náhodnou oběť fyzicky zaútočit, její reakci nahrát na mobilní telefon a pak video nahrát na internet pro pobavení ostatních lidí.

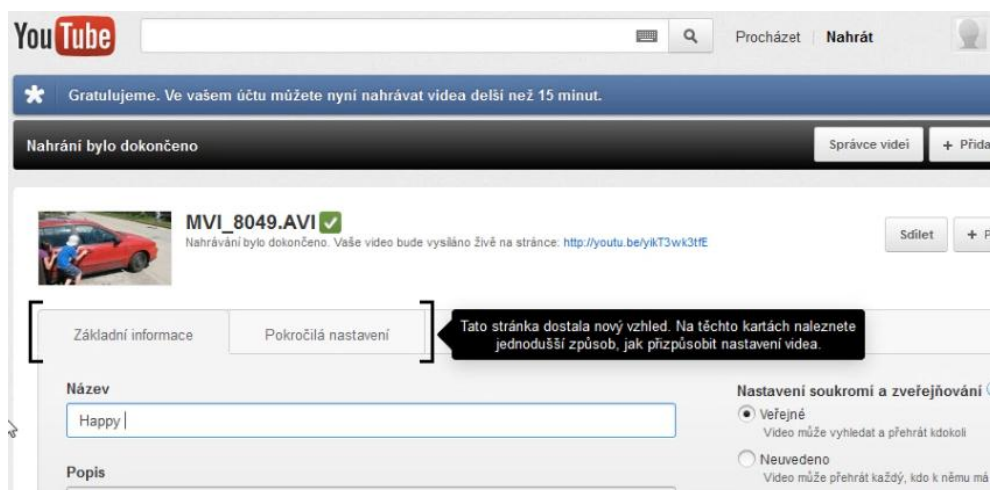
Postup u realizace Happy slappingu:

1. Domluvit se s partou na roli útočníka a na roli nahrávajícího útoku.
2. Na ulici si vyhlédnout jakoukoliv oběť a nečekaně na ni zaútočit, přičemž nahrávající nahrává reakce na mobilní telefon, viz Obr. 21.



Obr. 21. Útok na náhodnou oběť.

3. Dokud se oběť nevzpamatuje, rychle od místa činu uprchnout.
4. Poté je potřeba nahrát video s útokem a reakcí na server YouTube, viz Obr. 22.



Obr. 22. Vložení videa do YouTube.

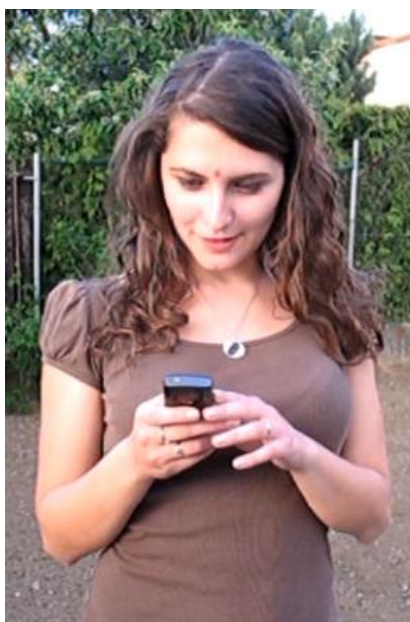
5. Nyní zbývá video veřejně zveřejnit a odkaz na video poslat přátelům.

3.1.10 Sexting

Fotografie, MMS nebo videa se sexuálním obsahem lze zneužít, přeposlat dál nebo zveřejnit na internetu. V případě, že kyberútočník získá tento materiál známé osoby, může ji pro pobavení všech ponížit a zesměšnit.

Postup u realizace sextingu:

1. V případě obdržení MMS s obsahem nahé nebo spoře oděné oběti lze MMS přeposlat dál přátelům. Obsah MMS lze poslat i přes bezdrátovou síť, viz Obr. 23.



Obr. 23. Rozeslání MMS všem kamarádkám.

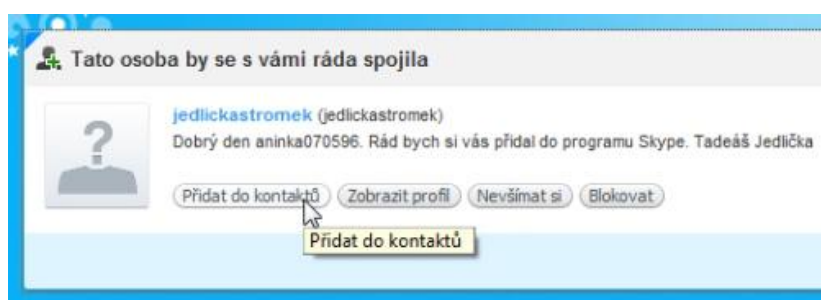
2. Pokud kyberútočník obdrží e-mailovou zprávu se sexuálním obsahem, zprávu s přílohou je možné přeposlat dál všem požadovaným kontaktům.
3. Fotografie nebo video lze také přeposlat prostřednictvím IM.
4. Pomocí těchto materiálů a způsobu rozesílání lze snadno oběť ponížovat, zesměšňovat a manipulovat s ní.

3.1.11 Kybergrooming

Kyberagresor pomocí techniky kybergroomingu vyvolá v oběti pocit důvěry a pochopení. Tak dosáhne toho, že s obětí manipuluje a přiměje ji k osobní schůzce.

Postup u realizace kybergroomingu:

1. Kyberagresor, Tadeáš Jedlička, si vybere v IM náhodnou oběť, Aninku070596, a požádá ji o přidání do seznamu kontaktů, viz Obr. 24.



Obr. 24. Žádost o přidání do kontaktů.

2. Ze začátku svou oběť otestovat, zda je pro kyberšikanování vhodná.
3. Po otestování Jedlička zjistí její věk a záliby, aby mohl použít efekt „zrcadlení“. Tzn., že kyberagresor má stejné hobby a názory jako oběť, viz Obr. 25.

Tadeáš Jedlička	Ahoj Aninko!	15:59
	Jmenujes se Aninka?	15:59
Anička Nováková	Ahoj! Ano, jmenuji se tak, přesne Anicka. A ty?	15:59
Tadeáš Jedlička	ja se jmenuju Tadeas. Mas hezke jmeno :_)	16:00
Anička Nováková	dik, taky se mi tve jmeno libi	16:00
Tadeáš Jedlička	koli ti je?	16:00
Anička Nováková	13. A tobe?	16:00
Tadeáš Jedlička	mne 15. Odkud jsi?	16:00
Anička Nováková	z uherskeho hradiste. A ty?	16:01
Tadeáš Jedlička	ja taky! To je nahoda!	16:01
	Co te vlastne bavi?	16:01
Anička Nováková	mam rada hudbu. A rada kreslim a tak. Ty?	16:01
Tadeáš Jedlička	Ja taky rad posloucham hudbu. Takze rada kreslis, jo? To je supr: _))))	16:02

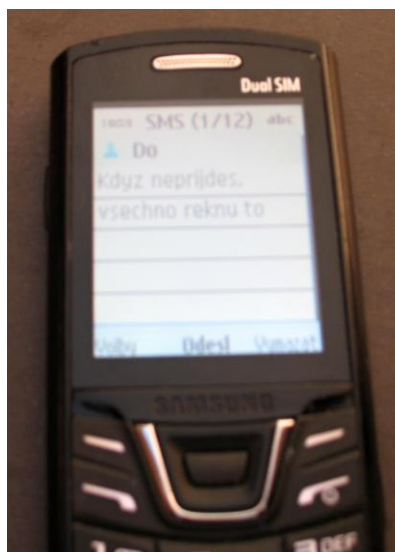
Obr. 25. Efekt zrcadlení.

4. V další etapě kybergroomingu by měl útočník navodit pocit důvěry a svou oběť izolovat od okolí, především od rodičů, viz Obr. 26.

Tadeáš Jedlička Jak se mas?
Anička Nováková Bibe, nasi mi dali zaracha kvuli bibe znamce
Tadeáš Jedlička strasne! Proc ti rodice vzdycky prudi? Oni nas vubec nechapu a vse zakazuji!
Anička Nováková mas pravdu
Tadeáš Jedlička ja te ale chapu
Anička Nováková aspon ty mi rozumis. Jeste, ze jsme se seznamili
Tadeáš Jedlička posles mi svou fotku?
Anička Nováková jo, hned to bude

Obr. 26. Navozování důvěry.

5. Aby Tadeáš Jedlička vyvolal závislost Aničky Novákové, měl by budit dojem láskyplnosti a podplácet ji různými dárky, např. dobítím kreditu.
6. Po určité době by kyberagresor měl snadno Aničku přemluvit k poslání jejích intimních fotografií.
7. Pokud bude mít kyberútočník k dispozici její fotky, může je nyní vydírat a přimět k osobní schůzce, viz Obr. 27.



Obr. 27. Donucení k osobní schůzce.

3.1.12 Kyberstalking

Pokud chce kyberagresor neustále sledovat a pronásledovat svou oběť odkudkoliv a v jakoukoliv dobu, potřebuje mít k dispozici ICT. Pomocí nichž ji může přemluvit či donutit ke schůzce. V horším případě ji může dohnat k hlubokým depresím.

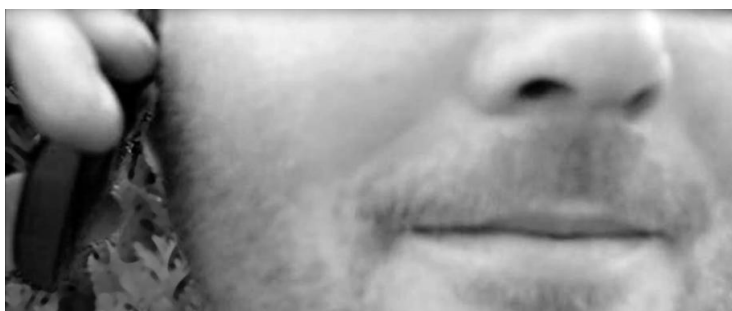
Postup pro realizaci kyberstalkingu:

1. V případě, že kyberútočník nezná telefonní číslo nebo kontakt na účty e-mailu a IM své oběti, je nucen si číslo zjistit na internetu, od přátel oběti nebo přímo od samotné oběti, viz Obr. 28.



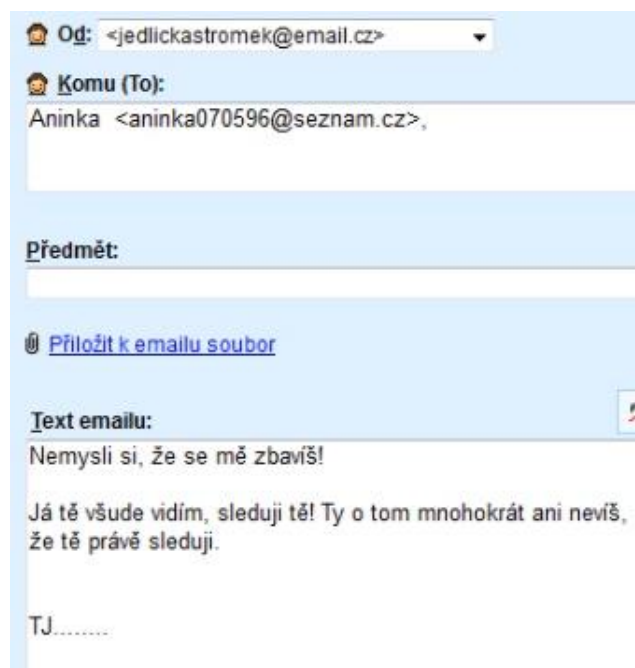
Obr. 28. *Kontaktování přes další osoby.*

2. Oběti lze neustále telefonovat nebo ji pouze prozvánět, viz Obr. 29.



Obr. 29. *Kyberpronásledování telefonním hovorem.*

3. Prostřednictvím IM lze oběť vydírat, zastrašovat nebo ji zvát na osobní schůzky.
4. Vyhrožovat oběti a popisovat jí své pocity může kyberútočník také prostřednictvím SMS nebo elektronických zpráv, viz Obr. 30.



Obr. 30. Kyberpronásledování pomocí e-mailu.

3.2 Zamezení realizace kyberšikany

Z hlediska informačních technologií lze zamezit realizaci nebo šíření kyberšikany několika způsoby. V případě zjištění výskytu kyberšikany nebo pochybného obsahu lze nejprve nahlásit administrátorovi sítě negativní projevy, a tím agresora zablokovat. Lze tak zakázat nebo zrušit webové stránky a kyberšikanující profil na sociální síti.

Aby žáci během výuky z nudy nekyberšikanovali oběti, zejména na sociálních sítích, je potřeba během výuky blokovat internetové stránky, které s výukou nesouvisí.

Vhodné je i vytvoření uživatelského účtu, ve kterém uživatelé nemají veškeré pravomoce jako administrátor. Pro uživatele účtu lze mimo jiné i nastavit povolené a zakázané internetové stránky a také pomocí programů chránit děti před kyberútoky. Takovými programy jsou např. iProtectYou, We-Blocker, Anti-Porn, Naomi 3.2.90 atd.

Nelze opomenout ani antivirové programy, které detekují a odstraňují útoky a viry napadávající PC. Nejvíce používanými antivirovými programy v České republice jsou AVG, ESET NOD32, avast!, Norton Antivirus atd.

Vhodným způsobem zamezení přístupu dětí do složek s důležitými daty uloženými v PC, je složky skrýt nebo ještě lépe uzamknout heslem. Pro uzamčení složky existuje několik programů, které lze z internetu stáhnout.

Následující postupy zamezení realizace kyberšikany jsou vytvořeny v operačním systému Windows 7.

3.2.1 Vytvoření uživatelského účtu

Uživatelský účet umožňuje pracovat s omezením, např. zákaz prohlížení dokumentů správce PC, nemožnost upravovat a rušit další uživatelské účty nebo zákaz instalování softwaru (SW), který by ovlivnil OS.

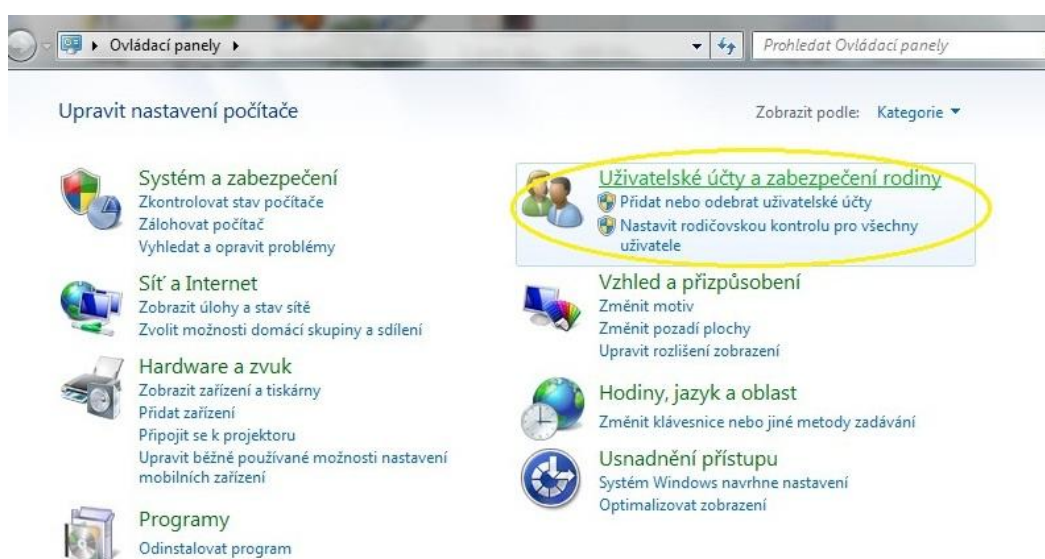
Postup pro vytvoření uživatelského účtu:

1. Pro vytvoření uživatelského účtu je třeba nejprve kliknout na tlačítko „Start“, při kterém se zobrazí hlavní menu. Poté se klikne na složku „Ovládací panely“. Viz Obr. 31.



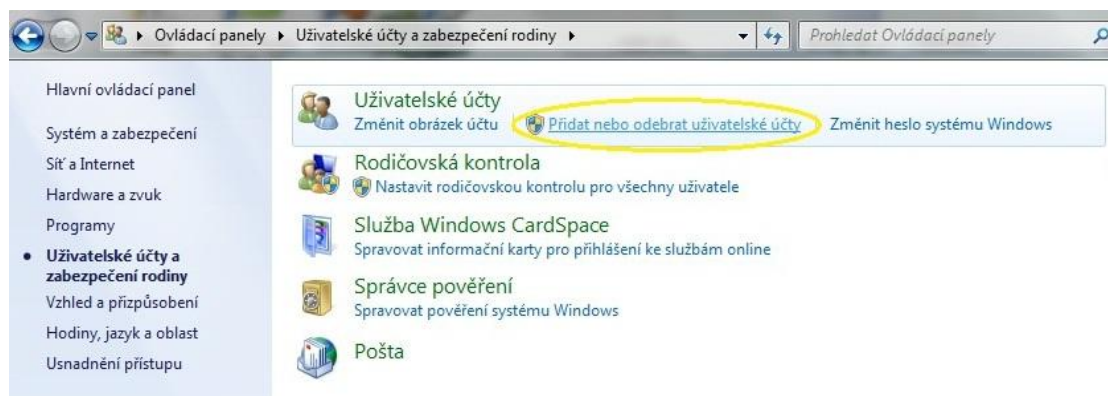
Obr. 31. Uživatelský účet – krok č. 1.

2. Po kliknutí na Ovládací panely se otevře okno s nabídkou. Nyní je třeba kliknout na „Uživatelské účty a zabezpečení rodiny“. Viz Obr. 32.



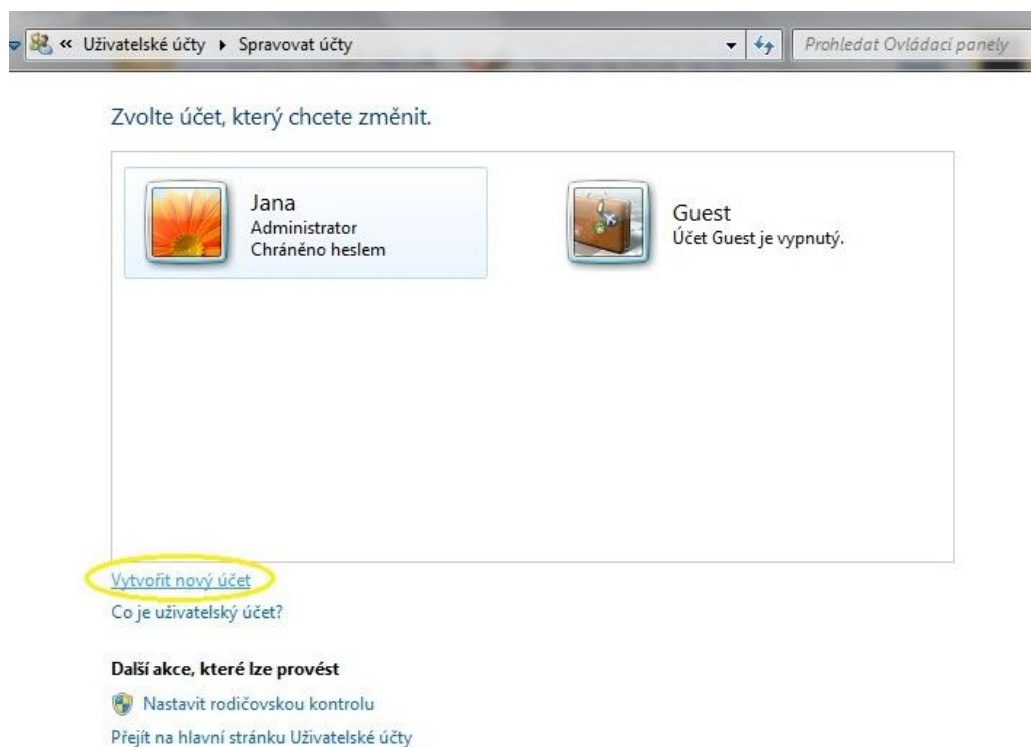
Obr. 32. Uživatelský účet – krok č. 2.

3. Zobrazí se další okno, ve kterém se potvrdí nabídka „*Přidat nebo odebrat uživatelské účty*“. Viz Obr. 33.



Obr. 33. Uživatelský účet – krok č. 3.

4. Pro vytvoření uživatelského účtu se klikne na nabídku „*Vytvořit nový účet*“, viz. Obr. 34.



Obr. 34. Uživatelský účet – krok č. 4.

5. Po kliknutí se otevře další okno, ve kterém je zadáván typ účtu a napsán název účtu, viz Obr. 35. Potvrzením tlačítka „Vytvořit účet“ vznikne nový uživatelský účet, viz Obr. 36.

The screenshot shows the 'Uživatelské účty' (User Accounts) window with the 'Vytvořit nový účet' (Create new account) option selected. The breadcrumb trail is '<< Uživatelské účty >> Spravovat účty >> Vytvořit nový účet'. A link 'Prohlédat Ovládací panely' is visible. The main heading is 'Zadat název účtu a zvolit typ účtu' (Enter account name and choose account type). Below it, a note states: 'Tento název se zobrazí na úvodní obrazovce a v nabídce Start.' (This name will be displayed on the desktop and in the Start menu). A text input field contains the name 'Aninka'. Two radio buttons are present: 'Standardní uživatel' (Standard user) is selected, and 'Správce' (Administrator) is unselected. Descriptions for each type are provided. A recommendation to use a strong password is shown at the bottom, along with a link 'Proč se doporučuje standardní účet?' (Why is a standard account recommended?). At the bottom right are 'Vytvořit účet' (Create account) and 'Storno' (Cancel) buttons.

Obr. 35. Uživatelský účet – krok č. 5.

The screenshot shows the 'Uživatelské účty' (User Accounts) window with the 'Spravovat účty' (Manage accounts) option selected. The breadcrumb trail is '<< Uživatelské účty >> Spravovat účty'. A link 'Prohlédat Ovládací panely' is visible. The main heading is 'Zvolte účet, který chcete změnit.' (Choose an account you want to change). Below this, three account tiles are displayed: 'Jana Administrator Chráněno heslem' (Jana Administrator Protected by a password), 'Aninka Standardní uživatel' (Aninka Standard user), and 'Guest Účet Guest je vypnutý.' (Guest Guest account is disabled). At the bottom left are links 'Vytvořit nový účet' (Create new account) and 'Co je uživatelský účet?' (What is a user account?). At the bottom, under the heading 'Další akce, které lze provést' (Other actions you can take), are links for 'Nastavit rodičovskou kontrolu' (Set parental controls) and 'Přejít na hlavní stránku Uživatelské účty' (Go to the main User Accounts page).

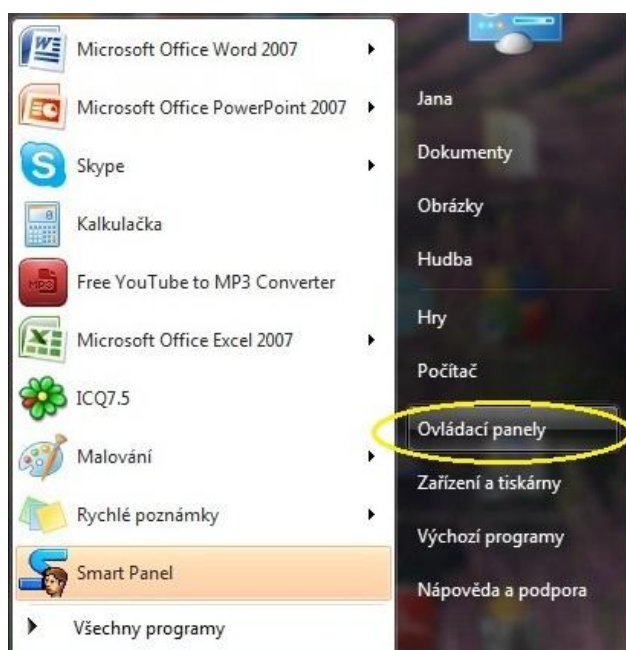
Obr. 36. Nový uživatelský účet.

3.2.2 Firewall

Firewall (FW) je bezpečnostní brána, která zabezpečuje provoz mezi sítěmi a dává jim pravidla pro komunikaci. PC je tak chráněn proti nepovoleným průnikům i proti odesílání dat ven.

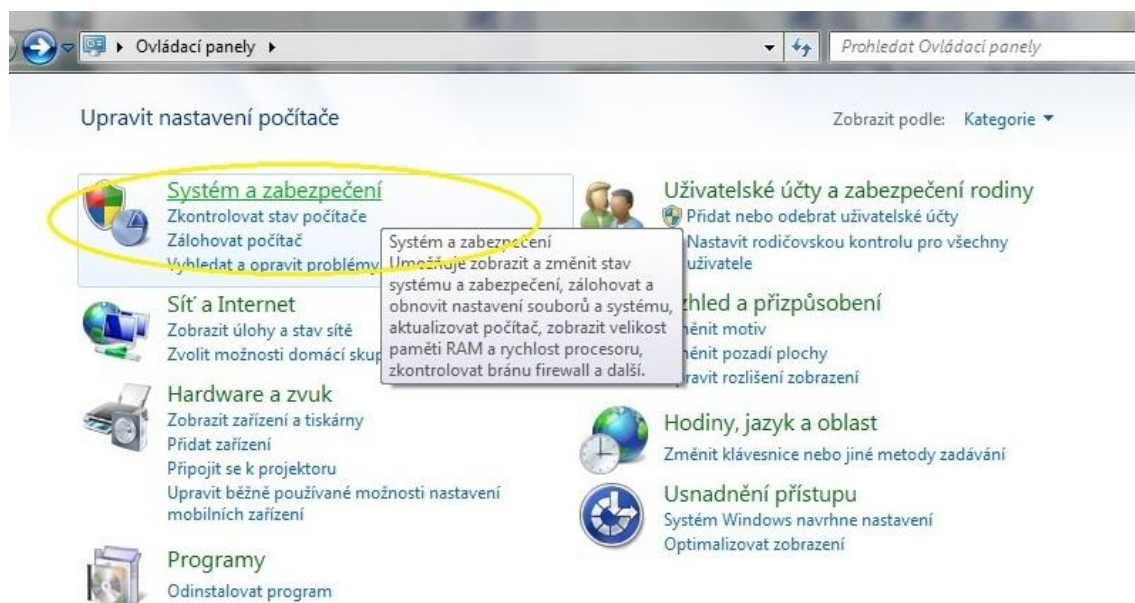
Postup nastavení FW:

1. Pro nastavení brány FW je třeba nejprve kliknout na tlačítko „Start“, při kterém je zobrazeno hlavní menu. Poté kliknout na složku „Ovládací panely“. Viz Obr. 37.



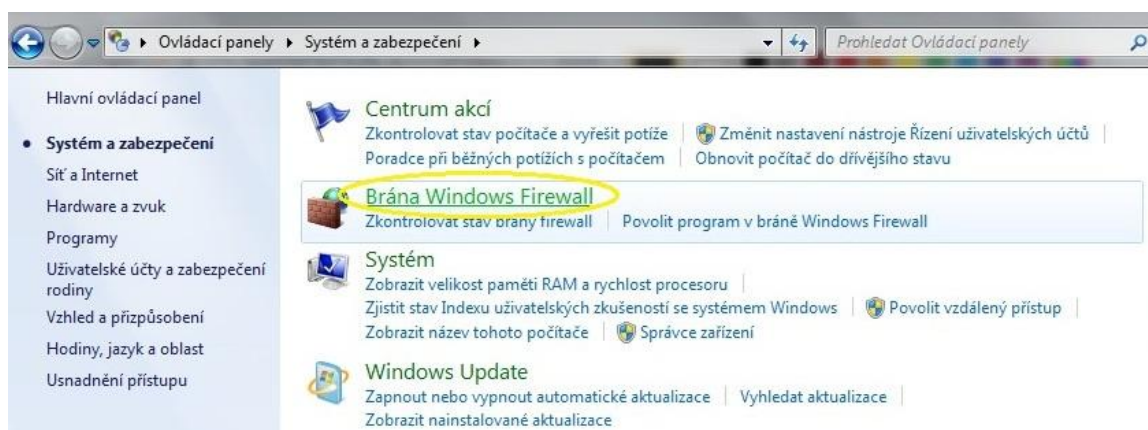
Obr. 37. Firewall – krok č. 1.

2. Nyní je zobrazeno okno, ve kterém je nutno kliknout na ikonu „Systém a zabezpečení“, viz Obr. 38.



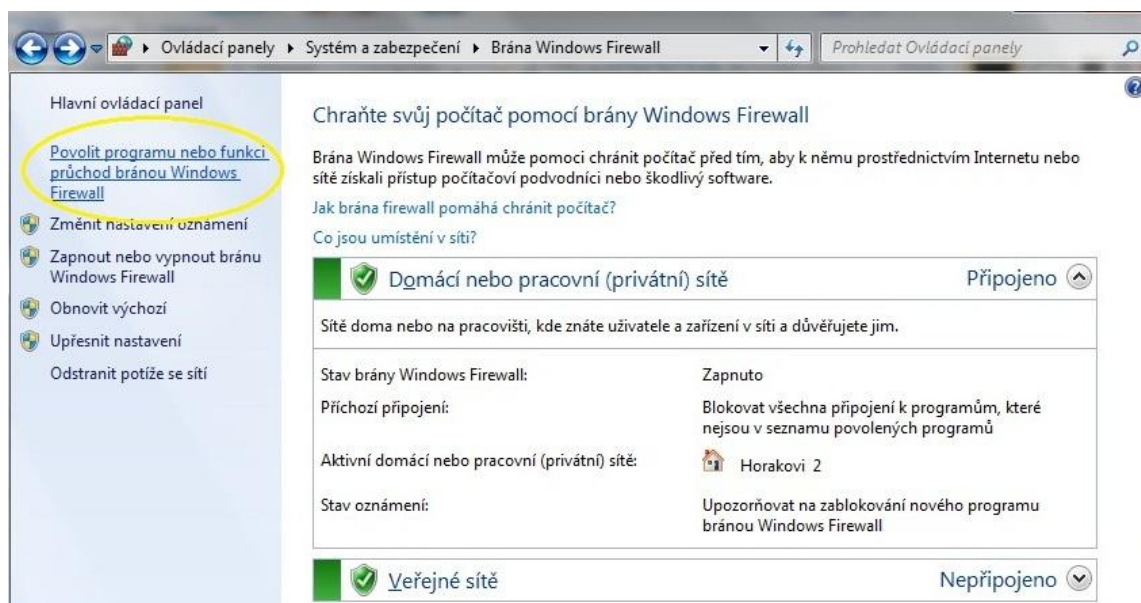
Obr. 38. Firewall – krok č. 2.

3. Po kliknutí na ikonu „Systém a zabezpečení“ se otevře okno, ve kterém je třeba kliknout na nabídku „Brána Windows Firewall“, viz Obr. 39.

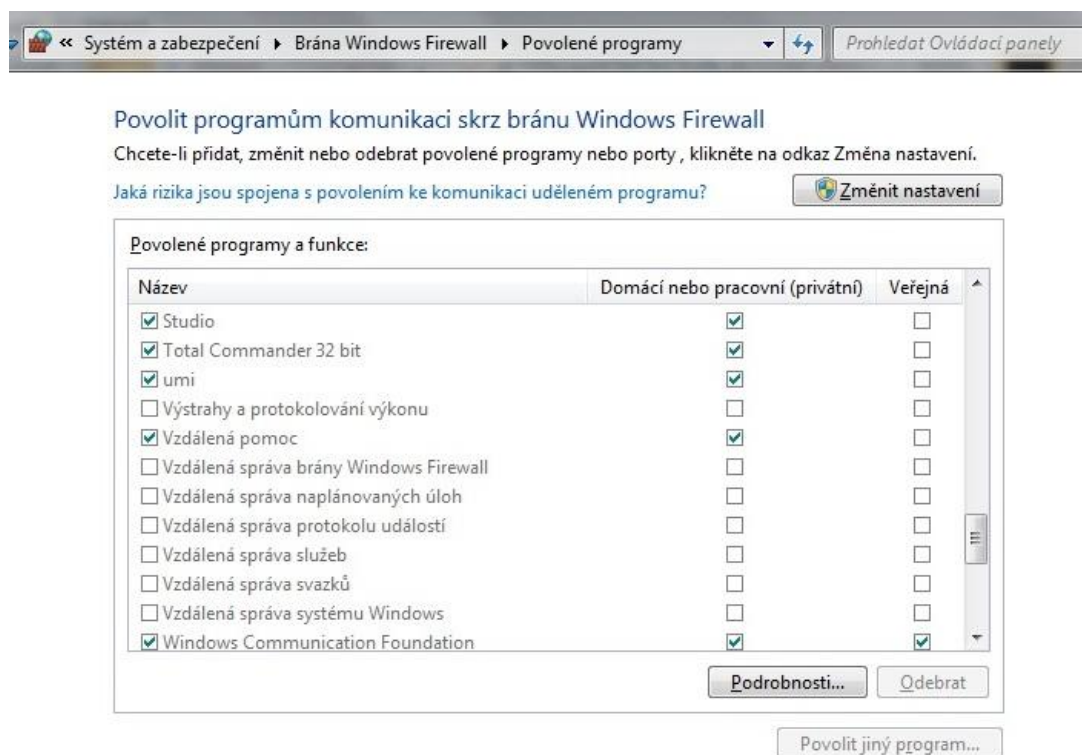


Obr. 39. Firewall – krok č. 3.

4. Poté je nutno kliknout na nabídku zobrazenou v levém panelu – „Povolit programu nebo funkci průchod bránou Windows Firewall“, jehož pomocí lze jednotlivým programům nastavit povolení komunikace skrz bránu Windows Firewall. Viz Obr. 40 a Obr. 41.



Obr. 40. Firewall – krok č. 4.



Obr. 41. Firewall – krok č. 5.

3.2.3 Centrum akcí

Pomocí centra akcí lze spravovat nastavení zabezpečení systému Windows. Pro lepší zabezpečení PC, by měly základní prvky zabezpečení obsahovat nastavení „Zapnuto“.

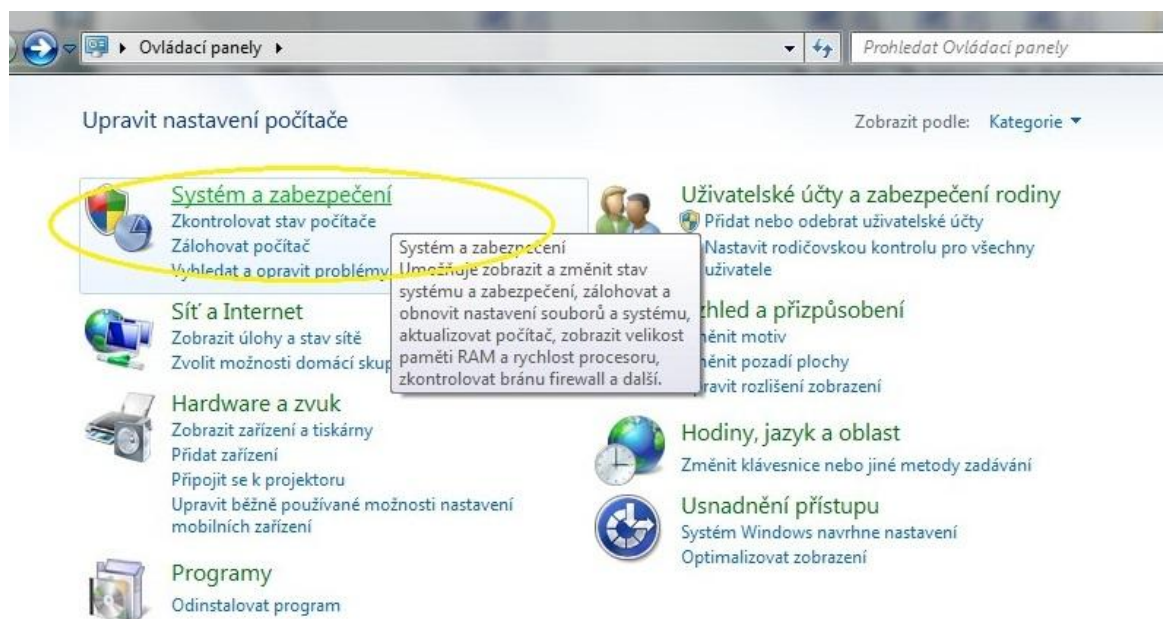
Postup pro správu nastavení zabezpečení:

1. Nejprve je nutno kliknout na „Start“, poté na „Ovládací panely“, viz Obr. 42.

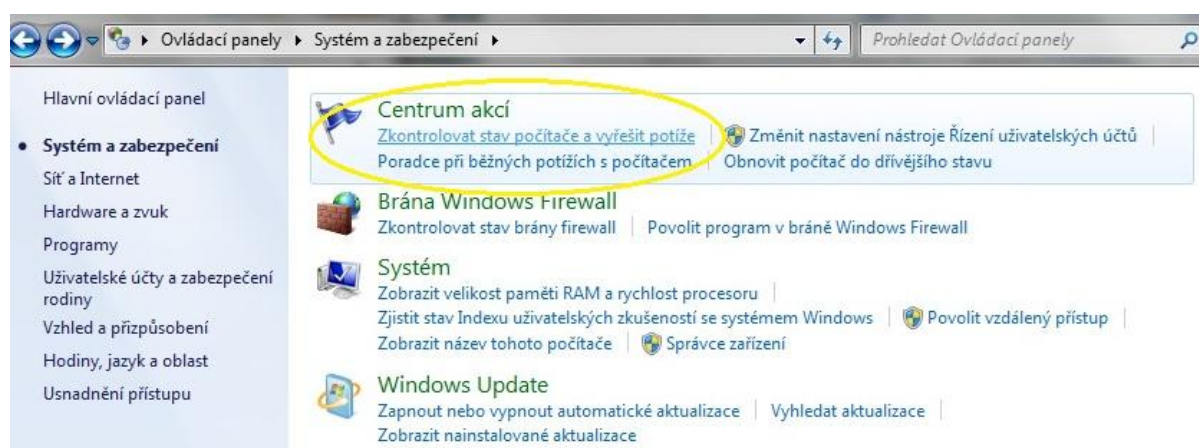


Obr. 42. Centrum akcí – krok č. 1.

2. Zobrazí se okno, v němž je označena nabídka „Systém a zabezpečení“, viz Obr. 43.
3. Po tomto kroku je zobrazeno další okno, ve kterém je třeba kliknout na „Zkontrolovat stav počítače a vyřešit potíže“ stojícím pod ikonkou „Centrum akcí“, viz Obr. 44.

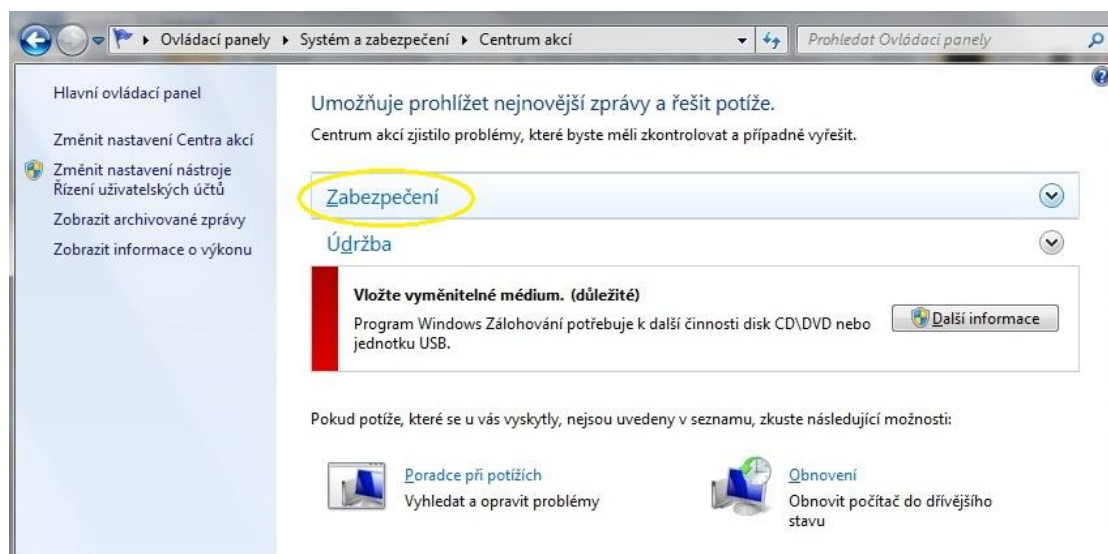


Obr. 43. Centrum akcí – krok č. 2.

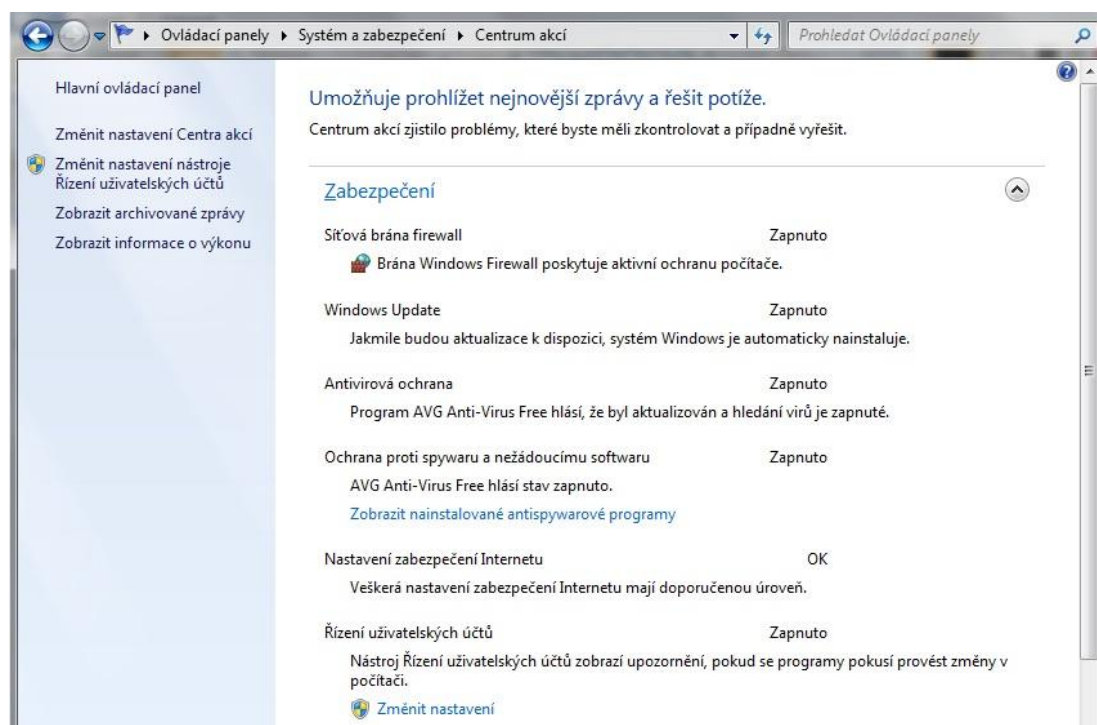


Obr. 44. Centrum akcí – krok č. 3.

4. Nyní je zobrazeno další okno. Pro podrobnější výpis základních prvků je potřeba kliknout na nabídku „Zabezpečení“. Zde lze vidět, že jsou základní prvky nastaveny na „Zapnuto“, viz Obr. 45 a Obr. 46.



Obr. 45. Centrum akcí – krok č. 4.



Obr. 46. Centrum akcí – krok č. 5.

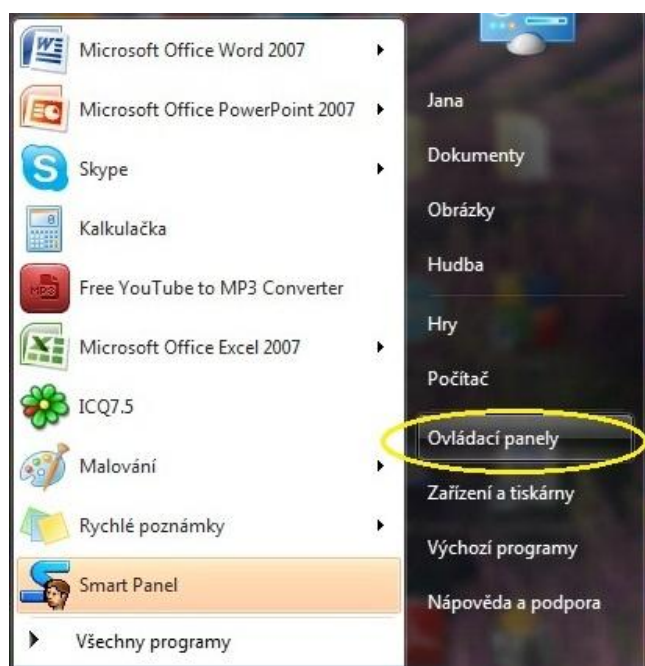
3.2.4 Zabezpečení internetu

Na internetu číhá několik hrozeb, negativních internetových stránek a chatů, které by dítě mohly ohrozit. Aby se těmto hrozbám pokud možno předešlo, jsou následně zobrazeny postupy nastavení webového prohlížeče.

Mezi nejznámější webové prohlížeče v českém prostředí patří Internet Explorer, Mozilla Firefox, Opera, Google Chrome atd.

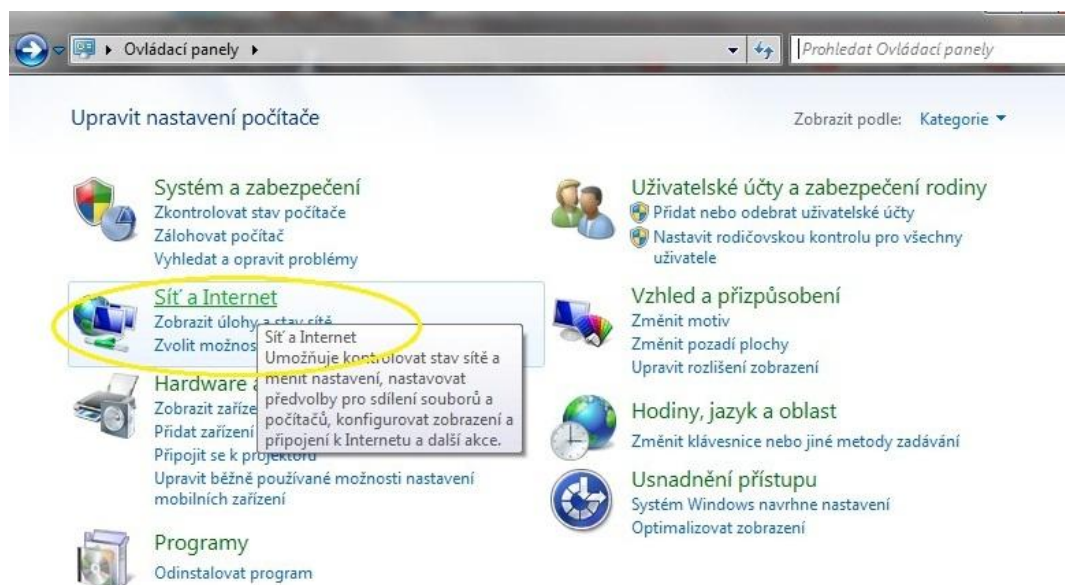
Postup pro nastavení prohlížeče:

1. Pro nastavení webového prohlížeče je třeba kliknout na tlačítko „Start“ a pak na „Ovládací panely“, po kterém se objeví okno s několika ikonami aplikací, viz obrázky Obr. 47 a Obr. 48.

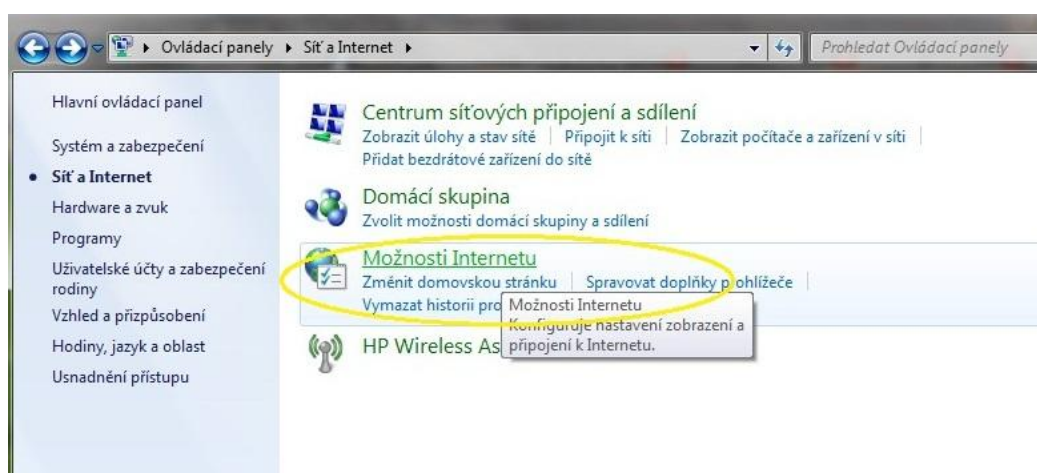


Obr. 47. Zabezpečení internetu – krok č. 1.

2. Nyní je potřeba kliknout na ikonku „Síť a Internet“. Zobrazí další okno. Obr. 48.
3. V nově zobrazeném okně je nutno kliknout na „Možnosti Internetu“. Obr. 49.

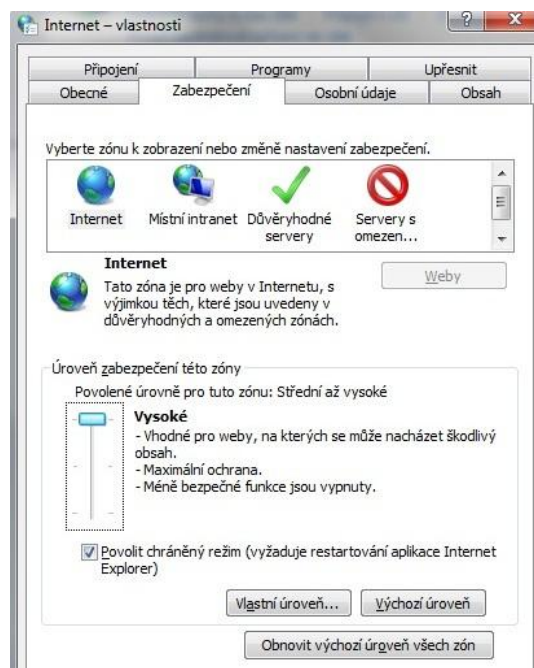


Obr. 48. Zabezpečení internetu – krok č. 2.



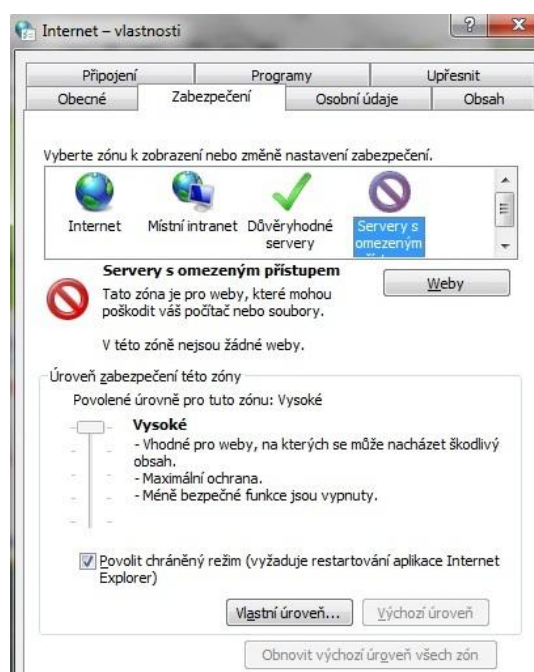
Obr. 49. Zabezpečení internetu – krok č. 3.

4. Po kliknutí na „Možnosti Internetu“ je zobrazeno okno s několika panely, viz Obr. 50. V liště „Zabezpečení“ by úroveň zabezpečení této zóny měla být nastavena na „Vysoké“.



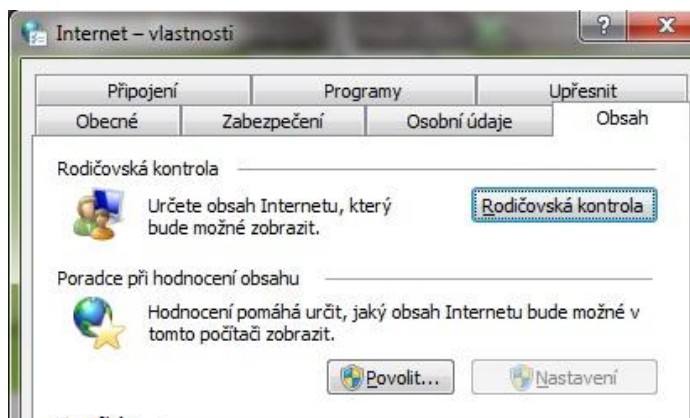
Obr. 50. Zabezpečení internetu – krok č. 4.

5. V nabídce „Zabezpečení“ je třeba kliknout na ikonku „Servery s omezeným přístupem“ a nastavit jeho úroveň na „Vysoké“. Viz Obr. 51.



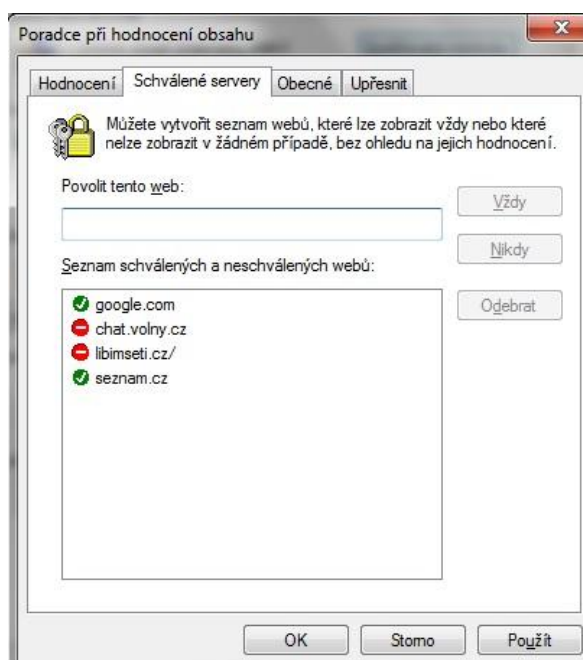
Obr. 51. Zabezpečení internetu – krok č. 5.

6. Dále je nutno kliknout na lištu „Obsah“, ve které lze nastavit rodičovská kontrola. Je potřeba kliknout na tlačítko „Rodičovská kontrola“. Obr. 52.



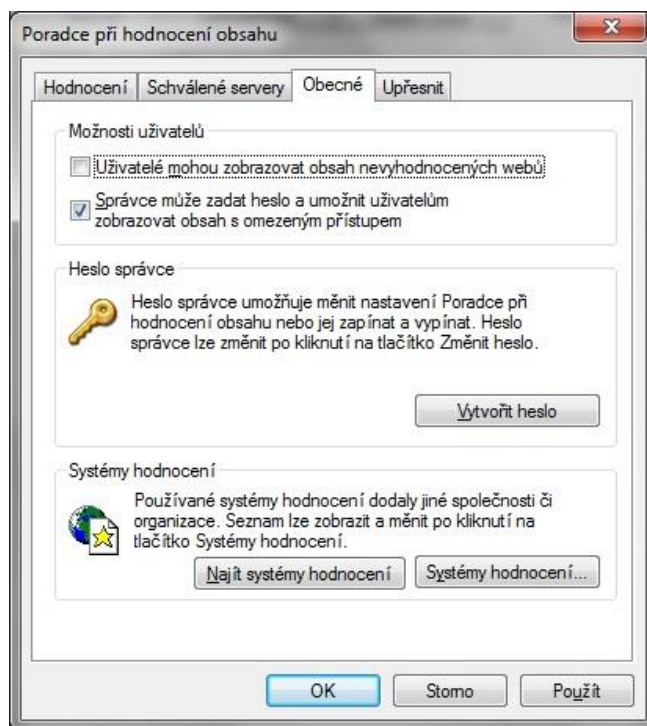
Obr. 52. Zabezpečení internetu – krok č. 6.

7. Po potvrzení je zobrazeno okno „Poradce při hodnocení obsahu“, ve kterém je nutno označit „Schválené servery“. Zde se do seznamu zadají všechny schválené a neschválené weby, které správce určí. Obr. 53.

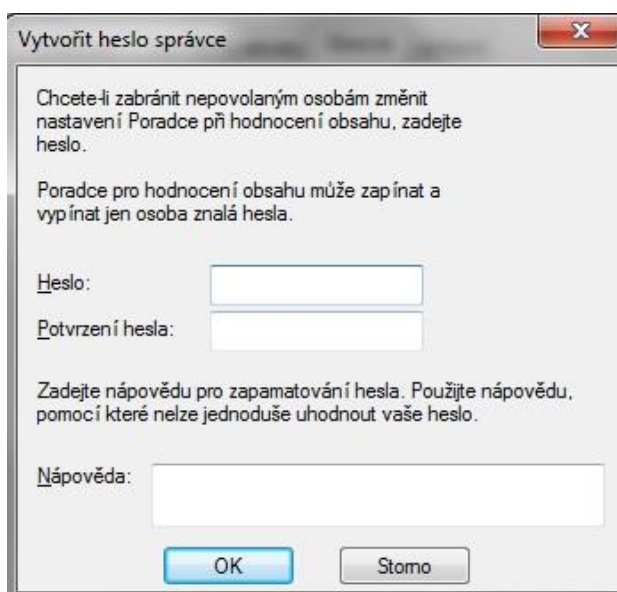


Obr. 53. Zabezpečení internetu – krok č. 7.

8. Heslo správce bude před každým spuštěním webu vyzývat uživatele k povolení zobrazení a zadání hesla správce. Lze jej vytvořit kliknutím na lištu „Obecné“, kde lze nastavit možnosti uživatele a vytvořit heslo správce, viz Obr. 54 a Obr. 55.



Obr. 54. Zabezpečení internetu – krok č. 8.



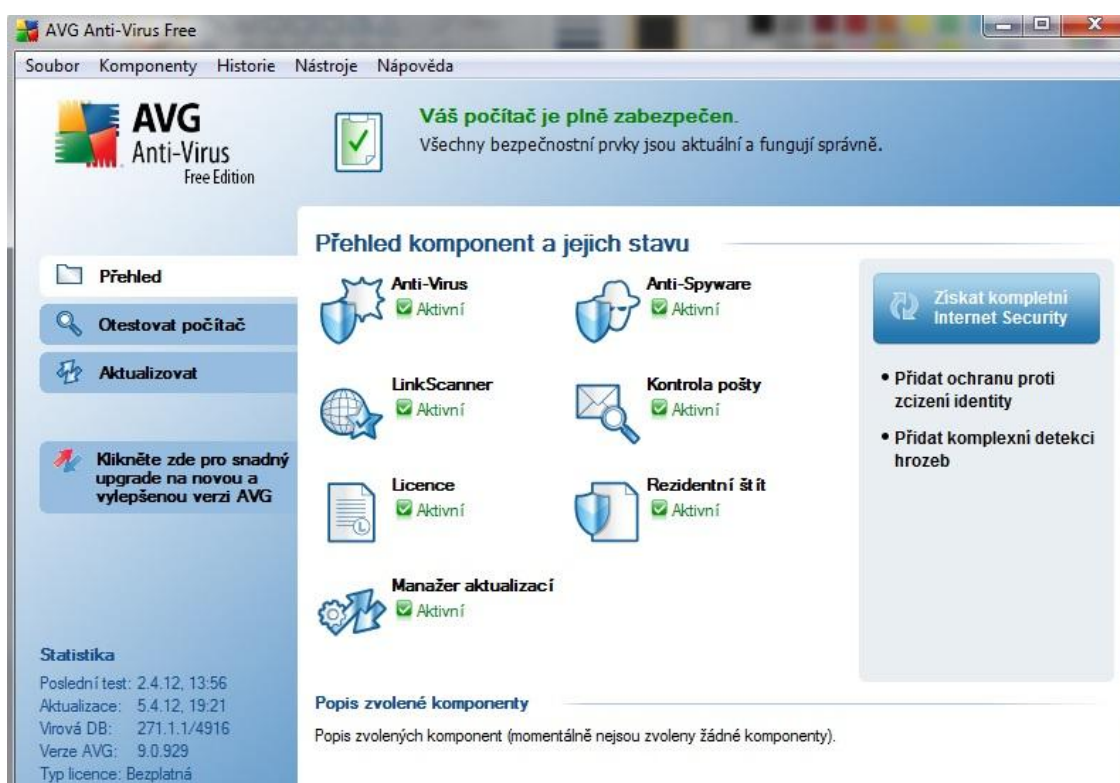
Obr. 55. Zabezpečení internetu – krok č. 9.

3.2.5 Antiviry

Důležitým pomocníkem je i antivirový program, který by měl být nainstalován v každém PC nebo notebooku. Je to SW, který identifikuje a odstraňuje viry a škodlivý SW (malware).

Postupy antiviru:

1. Antivirový program po výskytu viru soubor je schopen vyléčit nebo opravit soubor tím, že z něj odstraní vir.
2. Aby se virus nemohl rozšířit, umístí soubor do karantény.
3. Antivirus smaže infikovaný soubor s virem.



Obr. 56. Český antivirus AVG.

3.2.6 Uzamčení složek

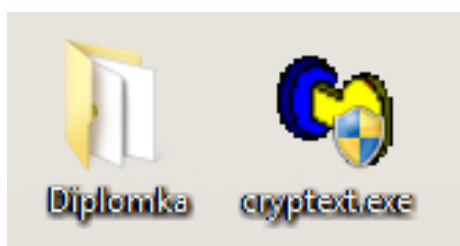
Složky s citlivými daty lze v PC skrýt, ale zvědavější nebo starší děti můžou složky najít. Mnohem lepší a snadnější způsob uchování složky a její utajení před případnými kyberútoky je složku uzamknout, čili zaheslovat ji.

Existuje několik druhů programů pro zaheslování a odheslování složek, např. Cryptext 3.4, ABI-CODER 3.6.1, TrueCrypt 4.2 aj.

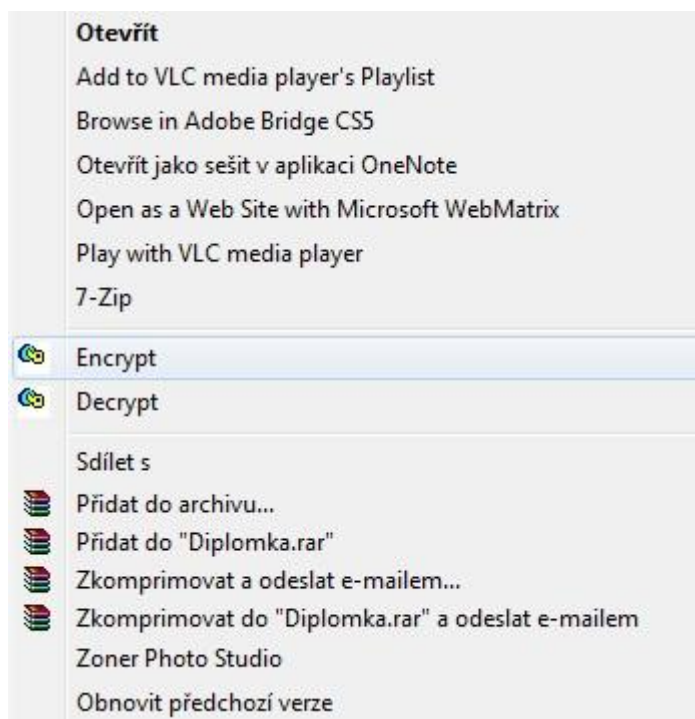
Pro ukázkou uzamčení a odemčení složky byl použit program Cryptext 3.4, jenž je možno zdarma stáhnout z webových stránek slunecnice.cz.

Postup pro uzamčení složky:

1. Na vybranou složku je nutno kliknout sekundárním (pravým) tlačítkem myši. Objeví se okno s nabídkou, ve které se vybere „Encrypt“, viz Obr. 57.
2. Po kliknutí na „Encrypt“ se objeví okno, do nějž se zadá heslo pro uzamčení složky. Obr. 58.
3. Uzamčení složky trvá delší dobu než odemčení. Obr. 59 a Obr. 60.



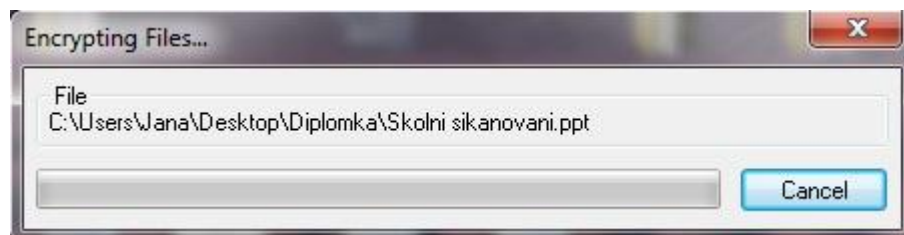
Obr. 57. Složka a ikonka Cryptext.












Obr. 58. Zaheslování složky – krok č. 1.



Obr. 59. Zaheslování složky – krok č. 2.



Obr. 60. Zaheslování složky – krok č. 3.

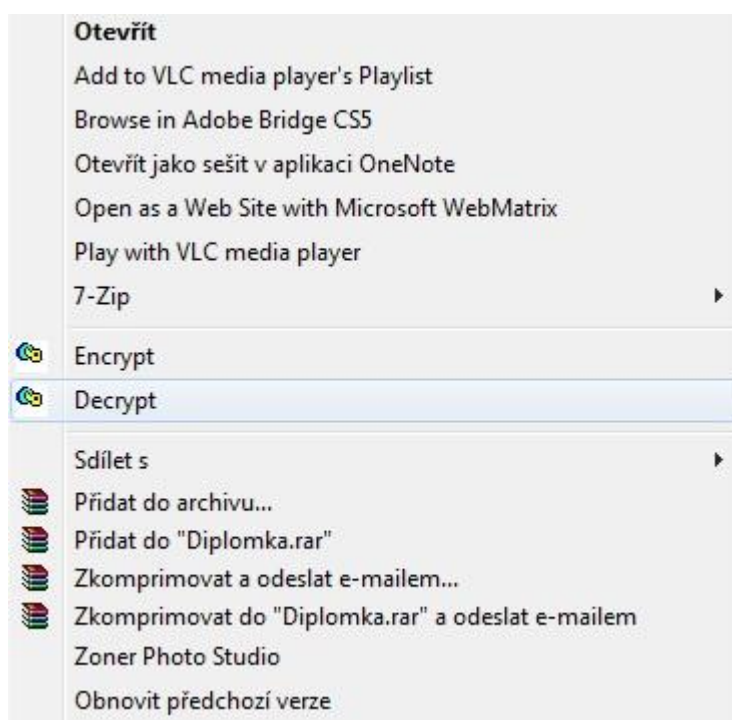
 moderni_psychologie_pro_pravniky-_cirt...	27.3.2012 20:44	Encrypted File	15 854 kB
 osnova DP.docx	21.11.2011 11:05	Encrypted File	13 kB
 PODROBNÁ OSNOVA TEORETICKÉ A PR...	22.1.2012 15:51	Encrypted File	36 kB
 preklad_kyberbulling_1.docx	12.1.2012 16:37	Encrypted File	17 kB
 Skolni sikanovani.ppt	25.1.2012 8:11	Encrypted File	1 531 kB
 slide kybersikanadown_645.pps	21.11.2011 15:58	Encrypted File	926 kB
 Teenageři riskují sexting.docx	11.3.2012 7:14	Encrypted File	14 kB
 Ucnova_Kybersikana_na_ZS_ve_meste_Br...	16.2.2012 19:28	Encrypted File	1 502 kB
 vanaj.ppt	25.1.2012 8:12	Encrypted File	979 kB

Obr. 61. Zaheslovaná data.

Odemčení složky probíhá stejným způsobem jako pro uzamčení složky.

Postup pro odemknutí složky:

1. Na zaheslovanou složku je třeba kliknout sekundárním (pravým) tlačítkem myši. Objeví se okno s nabídkou, ve které se vybere „Decrypt“, viz Obr. 62.
2. Pro odemknutí složky je nutno použít heslo, které se zadalo pro uzamčení, viz Obr. 63.



Obr. 62. Odheslování složky – krok č. 1.



Obr. 63. Odheslování složky – krok č. 2.

	moderni_psychologie_pro_pravniky-_cirt...	27.3.2012 20:44	Adobe Acrobat D...	15 854 kB
	osnova DP.docx	21.11.2011 11:05	Dokument aplikac...	13 kB
	PODROBNÁ OSNOVA TEORETICKÉ A PR...	22.1.2012 15:51	Dokument aplikac...	36 kB
	preklad_kyberbulling_1.docx	12.1.2012 16:37	Dokument aplikac...	17 kB
	Skolni_sikanovani.ppt	25.1.2012 8:11	Prezentace aplikac...	1 530 kB
	slide_kybersikanadown_645.pps	21.11.2011 15:58	Microsoft Office P...	926 kB
	Teenageři_riskují_sexting.docx	11.3.2012 7:14	Dokument aplikac...	14 kB
	Ucnova_Kybersikana_na_ZS_ve_meste_Br...	16.2.2012 19:28	Adobe Acrobat D...	1 502 kB
	vanaj.ppt	25.1.2012 8:12	Prezentace aplikac...	979 kB
	vyzkumna_zprava_2010_v1.pdf	11.3.2012 7:13	Adobe Acrobat D...	930 kB

Obr. 64. Odemčená data.

3.2.7 Programy pro ochranu dětí na internetu

Na internetových stránkách jsou dostupné programy, které chrání děti v prostředí internetu. Dokážou blokovat nevhodné hry, chat či omezit čas, který dítě na internetu tráví, např. uzamknutím klávesnice.

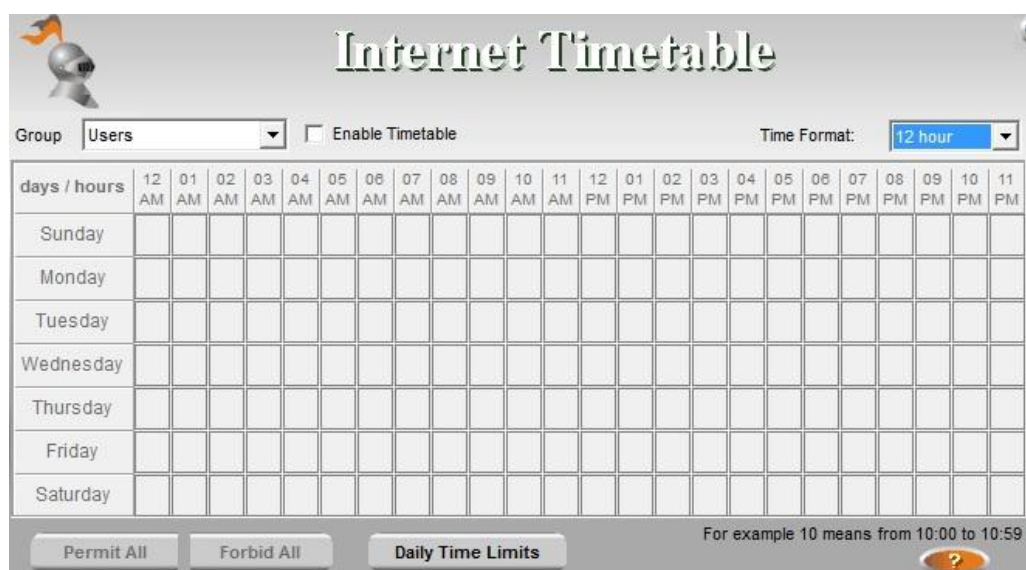
Pro ukázkou byl použit program iProtectYou 8.6.4, jenž byl stáhnut a nainstalován na zkušební dobu.

Pomocí „Internet Timetable“ lze nastavit čas, který smí uživatel nebo skupina uživatelů na internetu trávit. Čas je zadáván jednotlivě na každý den.

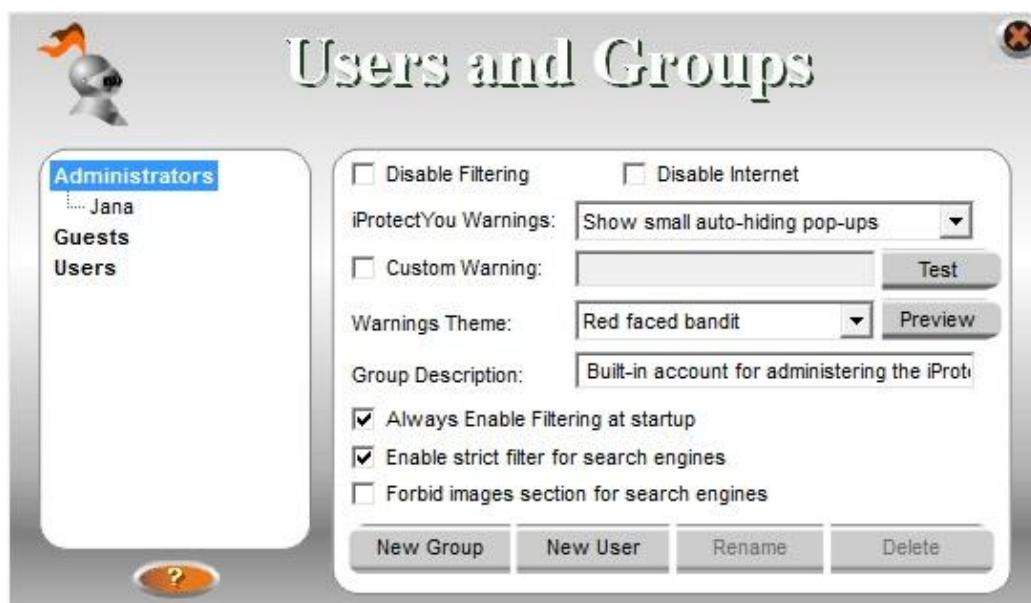
V části „*Users and Groups*“ lze zadat jméno uživatele nebo skupiny, kterou má program chránit při trávení času na internetu. Pomocí funkce „*Logs and Charts*“ je možno sledovat veškerou aktivitu uživatele a pomocí funkce „*Traffic Limits*“ lze nastavit omezení přenosu dat.



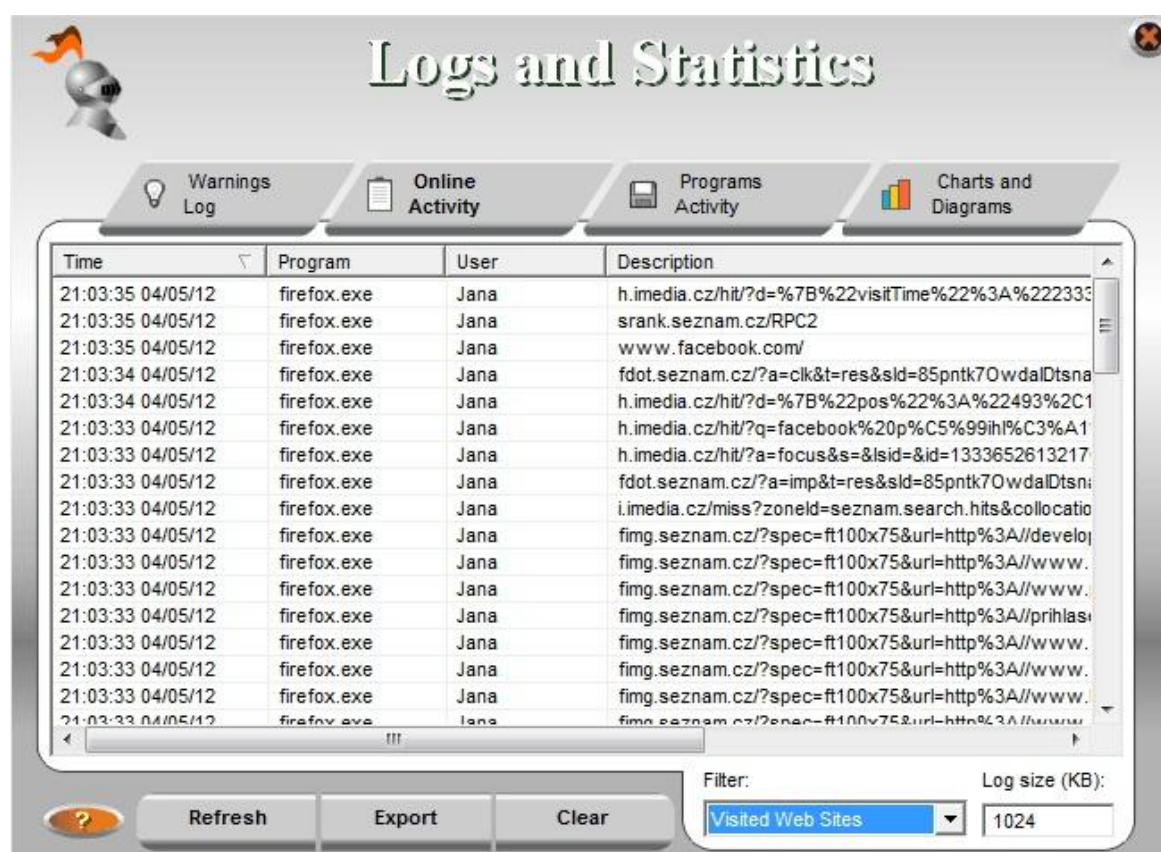
Obr. 65. Program iProtectYou – nabídka funkcí



Obr. 66. Program iProtectYou – nastavení času.



Obr. 67. Program iProtectYou – nastavení uživatele nebo skupiny.



Obr. 68. Program iProtectYou – přehled navštívených stránek.



Obr. 69. Program iProtectYou – nastavení omezení dat.

ZÁVĚR

Cílů, které jsem v úvodu vytýčila, bylo dosaženo, všechny aspekty problematiky jsem popsala. Pomocí prožitků z publikací a odborných článků byly zmapovány a charakterizovány výskyty a projevy kyberšikany na základních a středních školách. Objasnila jsem dopad na školní prostředí a klima třídy a dále definovala organizační opatření.

Na základě hypotéz jsem zhodnotila a vzorně a srozumitelně provedla realizace všech druhů kyberšikany. Předlohou výsledků hypotéz byl průzkum Centra prevence rizikové virtuální komunikace Univerzity Palackého v Olomouci, o kterém jsem se dočetla na internetovém prohlížeči www.novinky.cz. Dále jsem provedla rozhovor s několika výchovnými poradci z okolních základních a středních škol. Díky těmto rozhovorům bylo možno popsat a ilustrovat bezpečnostní opatření na informatické úrovni, jež zamezují výskytu kyberšikany.

Diplomová práce je zpracována na základě hypotéz, které si rodiče a pedagogové neustále kladou. Většina hypotéz podle průzkumu Centra prevence rizikové virtuální komunikace Univerzity Palackého v Olomouci byla na základě výzkumů potvrzena. Naopak některé hypotézy se jevily jako neopodstatněné. Podivuhodné bylo jejich potvrzení hypotézy, že se kyberšikana skutečně na základních a středních školách rozšiřuje a že ji zažilo téměř 60% českých dětí. Toto číslo je vskutku alarmující. Děti se ve velké většině svým rodičům s projevem kyberšikany nesvěří a mnoho rodičů a pedagogů neví, jak rozpoznat výskyt kyberšikany, ani jaké jsou její projevy a jak tomu lze zabránit. Mnoho českých základních a středních škol zamlčuje, že se právě na jejich škole tento problém vyskytl a že jej nedokázali úspěšně vyřešit.

Práce může proto sloužit jako příručka nebo základ zdroje pro čerpání informací o zamezení vzniku kyberšikany mezi dětmi na základních a středních školách. Znázorněné postupy při realizaci a zamezení kyberšikany z praktické části této práce mohou sloužit jako ilustrovaná a zfilmovaná předloha pro pedagogy a rodiče.

Prevence je důležitá pro včasné zamezení kyberšikany. Může to vést k omezení problému v třídním kolektivu, snížení počtu problémových žáků a obecně k příjemné atmosféře a klimatu v třídním kolektivu i v celé škole. Je to důležité právě pro pozitivní výchovu

žáků a dobré hodnocení celé školy žáky, rodiči, okolí, veřejností i pedagogickou obcí. Byť jeden případ kyberšikany s následkem ublížení oběti na zdraví či následkem smrti může vést k negativnímu hodnocení celé školy. Proto je důležité provádět prevenci kyberšikany i šikany obecně.

Tato diplomová práce se především zabývá metodami a projevy kyberšikany prostřednictvím informačních a komunikačních technologií. Teoretická část pojednává o základních, publikovaných zkušenostech z výskytu kyberšikany, jejich projevech a dopadech. Praktická část detailně popisuje a znázorňuje realizaci různých druhů kyberšikany. V praktické části jsou dále popsány postupy pro zamezení výskytu kyberšikany.

Závěrem je nutno podotknout, že rostoucí problém - kyberšikana, je nebezpečná hrozba, neboť způsobuje vážné újmy oběti, v horším případě vede k sebevraždě oběti. Kyberšikana má mimo jiné i negativní vliv na jinak příjemné školní prostředí. Vede ke zhoršení sociálního citění, vztahů mezi žáky a utváření špatné povahy dítěte. Mělo by být pořádáno více přednášek a konferencí týkajících se této problematiky s cílem osvěty a zdokonalování potírání této hrozby.

Ve všech případech, bohužel, kyberšikaně nelze zabránit, i když se o to můžeme v maximální možné míře pokusit.

CONCLUSION

The goals that I set – out in the introduction has been achieved, all aspects of the problem I described. Using the experiences of professional articles and publications have been mapped and characterized by the appearance and symptom of cyberbullying to primary and secondary schools. I explained the impact the school environment and classroom climate and organizational measures defined.

Based on the hypothesis I evaluated and implemented perfectly and comprehensively carry out all kinds of cyberbullying. The model results of the hypotheses was a survey of the risk prevention centers virtual communication Palacký University in Olomouc, which I read on the web browser www.novinky.cz. Next, I conducted an interview with several educational counselors from surrounding primary and secondary schools. Thanks to these talks was possible to describe and illustrate the IT security level to prevent the occurrence of cyberbullying.

The diploma thesis is prepared on the basis of hypotheses that can parents and teachers constantly ask. Most of the hypotheses according to a survey of the risk prevention centers virtual communication Palacký University in Olomouc was confirmed by research. However, certain hypotheses appeared to be unfounded. Amazing was the confirmation of the hypothesis that cyberbullying is indeed the primary and secondary schools to expand and it has experienced nearly 60% of Czech children. This number is indeed alarming. Children are the great majority of their parents entrust a speech cyberbullying and many parents and teachers know how to recognize the incidence of cyberbullying, or what are its symptoms and how it can be prevented. Many Czech elementary and secondary schools conceals that their school was the problem occurred and that it failed to resolve successfully.

The work can thus serve as a guide or basis for resource utilization information on avoidance of cyberbullying among children in elementary and secondary schools. Shown and implement procedures for preventing cyberbullying from the practical part of this work may serve as illustrated and filmed a model for educators and parents.

The prevention is important for early prevention of cyberbullying. This can lead to reduced problem in the class, reducing the number of problem pupils and generally pleasant

atmosphere and climate in the class in the whole school. It is very important for the positive and good upbringing of pupils from schools all pupils, parents, environment, public and an education community. Although one case of cyberbullying victims resulting in harm to health or cause death may lead to a negative evaluation of the whole school. It is therefore important to carry out prevention of cyberbullying and bullying in general.

This diploma thesis mainly deals with methods and symptoms of cyberbullying through information and communication technologies. The theoretical part deals with basic, published experience of the incidence of cyberbullying, its manifestations and implications. The practical part describes and illustrates in detail the implementation of various types of cyberbullying. In the practical part also describes procedures to prevent the occurrence of cyberbullying.

Finally, it should be noted that the growing problem - cyberbullying is a dangerous menace, causing serious damage to the victim, or worse, lead to suicide victims. Cyberbullying among others, has a negative effect on an otherwise pleasant school environment. It leads to the deterioration of social feelings, relationships between pupils and the formation of bad character of the child. It should be more organized lectures and conferences on this issue in order to improve education and fight against this threat.

In all cases, unfortunately, can not prevent cyberbullying, though so we can try as much as possible.

SEZNAM POUŽITÉ LITERATURY

- [1] BOURCET, S., GRAVILLON, I. *Šikana ve škole, na ulici, doma : jak bránit své dítě--: praktický průvodce pro rodiče, pedagogy a vychovatele*. 1. vyd. Překlad Martina Janošková. Praha: Albatros, 2006, 71 s. Albatros Plus, 83. ISBN 80-000-1552-8.
- [2] ČÍRTKOVÁ, L. *Moderní psychologie pro právníky: [domácí násilí, stalking, predikce násilí]*. Vyd. 1. Praha: Grada, 2008, 150 s. Psyché (Grada). ISBN 978-802-4722-078.
- [3] DEHUE, F., BOLMAN, C., VÖLLINK, T. Cyberbullying: Youngsters' Experiences and Parental Perception. *CyberPsychology*. 2008, roč. 11, č. 2, s. 217-223. ISSN 1094-9313. DOI: 10.1089/cpb.2007.0008. Dostupné z: <http://www.liebertonline.com/doi/abs/10.1089/cpb.2007.0008>.
- [4] KOLÁŘ, M. *Bolest šikanování*. Vyd. 1. Praha: Portál, 2001, 255 s. ISBN 80-717-8513-X.
- [5] KOPECKÝ, K., KREJČÍ, V. *Rizika virtuální komunikace: Příručka pro učitele a rodiče*. 1. vydání. Olomouc: NET UNIVERSITY, s.r.o., 2010, 35 s. ISBN 978-80-254-7866-0.
- [6] KOWALSKI, R., LIMBER S., AGATSTON P. *Cyber bullying: bullying in the digital age*. Malden, MA.: Blackwell Pub., 2008, 218 s. ISBN 9781405159920.
- [7] KREJČÍ, V. *Kyberšikana: Kybernetická šikana*. Olomouc, 2010, 72 s. ISBN 978-80-254-7791-5.
- [8] MCQUADE, S., COLT, J., MEYER, N. *Cyber bullying: protecting kids and adults from online bullies*. Westport, Conn.: Praeger Publishers, 2009, 219 s. ISBN 03-133-5193-7.
- [9] PARSONS, L. *Bullied teacher, bullied student: how to recognize the bullying culture in your school and what to do about it*. Markham, ON: Pembroke Publishers, 2005, 95 s. ISBN 15-513-8190-7.
- [10] ROGERS, V. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty*. Vyd. 1. Překlad Ondřej Vágner. Praha: Portál, 2011, 97 s. ISBN 978-807-3679-842.
- [11] ŠLÉGLOVÁ, Veronika. *Kyberšikana očima dospívajících*. Brno, 2011. Dostupné z: http://is.muni.cz/th/157989/fss_b/Bakalarska_prace.txt. Bakalářská práce. MU v Brně.

- [12] Ministerstvo školství, mládeže a tělovýchovy. *Metodický pokyn ministra školství, mládeže a tělovýchovy 28 275/2000-22 k prevenci a řešení šikanování mezi žáky škol a školských zařízení*. 2000, 8 s. Dostupné z: <http://www.msmt.cz/socialni-programy/metodicky-pokyn-k-sikanovani>.
- [13] E-bezpečí. [online]. 2008 [cit. 2012-01-30]. Dostupné z: <http://www.e-bezpeci.cz>.
- [14] Facebook - ponižení. [online]. 2008 [cit. 2012-03-28]. Dostupné z: http://alík.idnes.cz/kybersikana-a-jak-se-s-ni-poprat-d3g-/alík-alikoviny.asp?c=A110923_150234_alík-alikoviny_mrk.
- [15] Happy slapping. [online]. 2011 [cit. 2012-02-30]. Dostupné z: <http://www.kybersikana.eu/2011/05/happy-slapping.html>.
- [16] Hoax – injekční jehly. [online]. 2000 [cit. 2012-02-28]. Dostupné z: <http://www.hoax.cz/hoax/infikovane-jehly-na-sedadlech/>.
- [17] Kybergrooming. [online]. 2008 [cit. 2012-01-30]. Dostupné z: <http://cms.e-bezpeci.cz/content/view/42/6/lang,czech/>.
- [18] Kyberšikana učitele [online]. 2009 [cit. 2012-02-10]. Dostupné z: <http://sip.denik.cz/zpravy/zmlat-ho-tocim-to20090206.html>.
- [19] Netholismus [online]. 2010 [cit. 2012-02-25]. Dostupné z: <http://www.nebudobet.cz/?page=netholismus>.
- [20] Prevence kyberšikany. [online]. 2010 [cit. 2012-03-09]. Dostupné z: <http://www.kybersikana.eu>.
- [21] Prostředky ICT. [online]. 2010 [cit. 2012-03-10]. Dostupné z: <http://lifeinreality.blog.cz/1107/nebezpeci-kyber-sikany>.
- [22] Rady a doporučení proti šikaně [online]. 2011 [cit. 2012-03-15]. Dostupné z: <http://www.proti-sikane.cz>.
- [23] Sexting [online]. 2012 [cit. 2012-03-10]. Dostupné z: <http://www.ceskaskola.cz/2012/03/vlastni-sexualni-materialy-zverejnuje.html>.
- [24] Sms spoofing [online]. 2012 [cit. 2012-03-10]. Dostupné z: <http://cms.e-bezpeci.cz/content/view/21/6/lang,czech/>.
- [25] Útočná sms [online]. 2012 [cit. 2012-03-08]. Dostupné z: <http://www.vengle.com/s/kyber%C5%A1ikana.html>.
- [26] Útočníci veselého fackování [online]. 2012 [cit. 2012-03-20]. Dostupné z: <http://www.martialartstraining.tv/jamie-clubb/>.

- [27] Výzkumy [online]. 2012 [cit. 2012-05-05]. Dostupné z:
<http://www.novinky.cz/internet-a-pc/266020-obeti-kybersikany-je-temer-60-procent-ceskych-teenageru.html>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AVG	Antivirus (<i>Anti – Virus Guard</i>).
DNS	Hierarchický systém doménových jmen (<i>Domain Network System</i>).
E-mail	Elektronická zpráva (<i>Electronic Mail</i>).
FW	Firewall.
ICQ	I Seek You – Instant messaging.
ICT	Informační a komunikační technologie (<i>Information and Communication Technologies</i>).
IM	Instant Messaging.
IP	Internetový protokol (<i>Internet Protocol</i>).
MMS	Multimediální zprávy (<i>Multimedia Messaging Service</i>).
MS	Microsoft.
MSN	Microsoft Network.
MŠMT	Ministerstvo školství, mládeže a tělovýchovy.
OS	Operační systém (<i>Operating System</i>).
PC	Počítač (<i>Personal Computer</i>).
PIN	Osobní identifikační číslo (<i>Personal Identification Number</i>).
SMS	Krátká textová zpráva (<i>Short Message Sending</i>).
SW	Software.

SEZNAM POJMŮ

Kyberagresor	Útočník využívající k šikanování informačních technologií.
Kybergroomer	Agresor, jenž psychicky manipuluje pomocí ICT.
Kyberprávníčka	Právníčka zaměřující se na případy z virtuálního světa.
Kyberpronásledování	Pronásledování v kybernetickém prostoru.
Kyberprostor	Prostor ve virtuálním světě.
Kyberšikana	Šikanování pomocí moderních informačních technologií.
Kyberútok	Útok realizovaný v kybernetickém (virtuálním) světě.
Notebook	Přenosný počítač.
Outsider	Člověk stojící stranou, mimo danou skupinu.
Teenager	Mládež ve věku od 13 – 19 let.

SEZNAM OBRÁZKŮ

<i>Obr. 1. Kyberšikana učitele. [18]</i>	15
<i>Obr. 2. Prostředek ICT. [21]</i>	18
<i>Obr. 3. Útočná sms. [25]</i>	25
<i>Obr. 4. Útočníci – veselé fackování. [26]</i>	33
<i>Obr. 5. Sms spoofing. [24]</i>	34
<i>Obr. 6. Hoax – injekční jehly. [16]</i>	35
<i>Obr. 7. Netholismus. [19]</i>	40
<i>Obr. 8. Facebook – ponížení. [14]</i>	42
<i>Obr. 9. Flaming na chatu kecal.cz.</i>	47
<i>Obr. 10. Obtěžování prostřednictvím SMS.</i>	48
<i>Obr. 11. Obtěžování prostřednictvím elektronických zpráv.</i>	48
<i>Obr. 12. Pomlouvání na sociální síti FB.</i>	49
<i>Obr. 13. Chlubení se získáním hesla oběti.</i>	50
<i>Obr. 14. Předstírání prostřednictvím účtu Skype.</i>	50
<i>Obr. 15. Prozrazení intimní informace o oběti.</i>	51
<i>Obr. 16. Prozrazení informace na Facebooku.</i>	51
<i>Obr. 17. Vytvoření soukromé konverzace.</i>	52
<i>Obr. 18. Odhalení podvodu.</i>	52
<i>Obr. 19. Vyloučení oběti.</i>	53
<i>Obr. 20. Poslání poplašné zprávy.</i>	54
<i>Obr. 21. Útok na náhodnou oběť.</i>	55
<i>Obr. 22. Vložení videa do YouTube.</i>	55
<i>Obr. 23. Rozeslání MMS všem kamarádkám.</i>	56
<i>Obr. 24. Žádost o přidání do kontaktů.</i>	57
<i>Obr. 25. Efekt zrcadlení.</i>	57
<i>Obr. 26. Navozování důvěry.</i>	58
<i>Obr. 27. Donucení k osobní schůzce.</i>	58
<i>Obr. 28. Kontaktování přes další osoby.</i>	59
<i>Obr. 29. Kyberpronásledování telefonním hovorem.</i>	59
<i>Obr. 30. Kyberpronásledování pomocí e-mailu.</i>	60
<i>Obr. 31. Uživatelský účet – krok č. 1.</i>	62

<i>Obr. 32. Uživatelský účet – krok č. 2.</i>	62
<i>Obr. 33. Uživatelský účet – krok č. 3.</i>	63
<i>Obr. 34. Uživatelský účet – krok č. 4.</i>	63
<i>Obr. 35. Uživatelský účet – krok č. 5.</i>	64
<i>Obr. 36. Nový uživatelský účet.</i>	64
<i>Obr. 37. Firewall – krok č. 1.</i>	65
<i>Obr. 38. Firewall – krok č. 2.</i>	66
<i>Obr. 39. Firewall – krok č. 3.</i>	66
<i>Obr. 40. Firewall – krok č. 4.</i>	67
<i>Obr. 41. Firewall – krok č. 5.</i>	67
<i>Obr. 42. Centrum akcí – krok č. 1.</i>	68
<i>Obr. 43. Centrum akcí – krok č. 2.</i>	69
<i>Obr. 44. Centrum akcí – krok č. 3.</i>	69
<i>Obr. 45. Centrum akcí – krok č. 4.</i>	70
<i>Obr. 46. Centrum akcí – krok č. 5.</i>	70
<i>Obr. 47. Zabezpečení internetu – krok č. 1.</i>	71
<i>Obr. 48. Zabezpečení internetu – krok č. 2.</i>	72
<i>Obr. 49. Zabezpečení internetu – krok č. 3.</i>	72
<i>Obr. 50. Zabezpečení internetu – krok č. 4.</i>	73
<i>Obr. 51. Zabezpečení internetu – krok č. 5.</i>	73
<i>Obr. 52. Zabezpečení internetu – krok č. 6.</i>	74
<i>Obr. 53. Zabezpečení internetu – krok č. 7.</i>	74
<i>Obr. 54. Zabezpečení internetu – krok č. 8.</i>	75
<i>Obr. 55. Zabezpečení internetu – krok č. 9.</i>	75
<i>Obr. 56. Český antivirus AVG.</i>	76
<i>Obr. 57. Složka a ikonka Cryptext.</i>	77
<i>Obr. 58. Zaheslování složky – krok č. 1.</i>	78
<i>Obr. 59. Zaheslování složky – krok č. 2.</i>	78
<i>Obr. 60. Zaheslování složky – krok č. 3.</i>	78
<i>Obr. 61. Zaheslovaná data.</i>	79
<i>Obr. 62. Odheslování složky – krok č. 1.</i>	79
<i>Obr. 63. Odheslování složky – krok č. 2.</i>	80
<i>Obr. 64. Odemčená data.</i>	80

<i>Obr. 65. Program iProtectYou – nabídka funkcí.....</i>	<i>81</i>
<i>Obr. 66. Program iProtectYou – nastavení času.....</i>	<i>81</i>
<i>Obr. 67. Program iProtectYou – nastavení uživatele nebo skupiny.....</i>	<i>82</i>
<i>Obr. 68. Program iProtectYou – přehled navštívených stránek.....</i>	<i>82</i>
<i>Obr. 69. Program iProtectYou – nastavení omezení dat.....</i>	<i>83</i>

SEZNAM TABULEK

<i>Tab. 1. Vytvořené fiktivní osoby</i>	46
---	----

SEZNAM PŘÍLOH

PRÍLOHA P I: Video – realizace kyberšikany v souboru na DVD