UNIVERZITA PALACKÉHO V OLOMOUCI

PEDAGOGICKÁ FAKULTA

Ústav pedagogiky a sociálních studií

Diplomová práce

Pavel Valchář

Kybergrooming a další nebezpečné aktivity spojené s využíváním moderních komunikačních technologií

Olomouc 2012

vedoucí práce: PhDr. Linda Švrčinová

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a výhradně s použitím citované literatury.

V Olomouci dne 10. března 2012 ……

podpis

PODĚKOVÁNÍ

Na tomto místě bych rád poděkoval své vedoucí diplomové práce PhDr. Lindě Švrčinové za její odborné vedení, cenné rady, ochotu a celkovou podporu. Dále bych rád poděkoval Mgr. Kamilu Kopeckému, Ph.D. za poskytnuté informace a osobní konzultace. V neposlední řadě bych chtěl poděkovat i svým nejbližším za trpělivost a podporu při mém studiu.

OBSAH

ÚVOD 6
TEORETICKÁ ČÁST 8
1 KOMUNIKACE A MODERNÍ KOMUNIKAČNÍ TECHNOLOGIE 8
1.1 Sociální komunikace 9
1.1.1 Verbální a neverbální sociální komunikace 10
1.1.2 Intrapersonální, interpersonální, skupinová a veřejná komunikace 11
1.1.3 Funkce sociální komunikace 12
1.1.4 Elektronická komunikace jako specifická forma sociální komunikace 13
2 NEBEZPEČNÉ KOMUNIKAČNÍ JEVY PÁCHANÉ V PROSTŘEDÍ INTERNETU A MOBILNÍCH SÍTÍ 28
2.1 Kyberšikana 28
2.2 Sexting 33
2.3 Happy slapping 35
2.4 Kyberstalking 36
2.5 Phishing 40
2.6 Hoax 41
3 KYBERGROOMING 44
3.1 Výskyt kybergroomingu a jeho pachatelé 44
3.2 Oběti kybergroomingu 46
3.3 Etapy manipulace dítěte 47
3.4 Popis jednotlivých etap kybergroomingu 48
3.4.1 První etapa – Příprava podmínek pro zahájení kontaktu s obětí 49
3.4.2 Druhá etapa – První kontakt s obětí, navázání a prohlubování vztahu a snaha o její izolaci 51
3.4.3 Třetí etapa – Příprava na osobní setkání 55
3.4.4 Čtvrtá etapa – Osobní setkání kybergroomera s obětí 56
3.5 Případy kybergroomingu 57
3.5.1 V České Republice 57
3.5.2 V zahraničí 64
3.6 Právní rámec kybergroomingu 67
3.7 Ochrana před kybergroomingem 68
3.7.1 Technické metody ochrany 68

3.7.2 Primární prevence 69
4 PROJEKTY NA OCHRANU DĚTÍ 81
4.1 E-Bezpečí 81
4.2 Centrum prevence rizikové virtuální komunikace 83
4.3 E-Nebezpečí 84
4.4 Saferinternet 84
4.4.1 Bezpečně online 85
4.4.2 Pomoc online (Internet Helpline) 86
4.4.3 Horká linka 86
4.4.4 Osvětové centrum (Online Safety Institute) 87
4.5 Preventivně informační centrum Policie České republiky 88
4.6 Seznam se bezpečně 88
4.7 Internet Hotline 89
4.8 Nebuď oběť 90
PRAKTICKÁ ČÁST 92
5 ÚVOD DO VÝZKUMU 92
5.1 Cíl výzkumu 92
5.2 Výzkumné otázky a hypotézy 93
5.3 Výzkumná metodologie 94
5.4 Charakteristika respondentů 96
5.5 Realizace výzkumu 96
6 ZPRACOVÁNÍ DAT 98
6.1 Vyhodnocení odpovědí všech respondentů 98
6.2 Vyhodnocení odpovědí vybraných respondentů 110
7 ANALÝZA DOSAŽENÝCH VÝSLEDKŮ 116
8 SHRNUTÍ PRAKTICKÉ ČÁSTI 119
ZÁVĚR 121
RESUMÉ 123
SEZNAM POUŽITÉ LITERATURY 124
SEZNAM POUŽITÝCH ZKRATEK 132
SEZNAM TABULEK 134
SEZNAM GRAFŮ 135
SEZNAM PŘÍLOH 137

ÚVOD

„Nebezpečí přichází rychleji, když je přehlíženo.“

Syrius Publius

Komunikace a s ní spojené předávání informací provází lidstvo od jeho počátku. Dnes, díky pokroku, kterého bylo dosaženo v oblasti informačních a komunikačních technologií, jsme svědky stále se zdokonalujícího způsobu předávání informací. V současnosti vládnou světu moderní technologie využívající k přenosu informací digitální síť GSM[1] a celosvětovou počítačovou síť Internet. Moderní technologie obohatily klasické metody sloužící k předávání informací o nové možnosti, díky kterým se podstatně zkrátila doba potřebná pro přenos informace a vzdálenost mezi komunikujícími stranami už nehraje žádnou roli. Je úžasné, kam až se lidstvo dostalo, jak hmatatelně jsme už vzdáleni od přenosu informací na dálku kouřovými signály, poštovními holuby, pony expressy, telegrafy, analogovými drátovými telefony či klasickými poštovními službami. Avšak co se definitivně ztrácí, je tzv.[2] „komunikace z očí do očí“ a „možnost ponechat si vlastní tvář“.

Moderní komunikační prostředky se čím dál více stávají běžnou součástí lidského života. Téměř každý dnes ví, co je počítač, internet a mobilní telefon. Obzvláště to ví naše děti, které si jen stěží dokážou představit svůj každodenní život bez těchto výdobytků moderní doby. Bohužel, s jejich používáním je spojeno i mnoho negativních jevů, mezi které můžeme zařadit například kyberšikanu, kyberstalking, happy slapping, sexting a kybergrooming. Mnozí z uživatelů o výše uvedených nebezpečích neví, a tato neznalost je velice často důvodem, proč bezstarostně sdělují na sociálních sítích informace o své osobě a o svých blízkých, nebo proč na Internetu zcela otevřeně komunikují s osobami, které osobně neznají. Nebezpečnost svého chování si většinou uvědomují až ve chvíli, kdy jejich důvěru nebo jimi poskytnuté informace někdo zneužije.

Stále větší množství mediálně zveřejňovaných případů zneužití moderních komunikačních technologií bylo důvodem, proč jsem se o kybergrooming a další nebezpečné komunikační jevy začal zajímat a následně si je zvolil jako téma své diplomové práce. Práce, která takto vznikne, by mohla v budoucnu sloužit jako podpůrný materiál všem, kteří projeví zájem o uvedenou problematiku.

[1] GSM – Global System for Mobile Communication – globální systém mobilních komunikací (dále jen „GSM“).
[2] tzv. – takzvaný (dále jen „tzv.“).

Diplomová práce se skládá z teoretické a praktické části. Teoretická část je rozdělena do 4 kapitol. V první kapitole se zabývám komunikací a komunikačními technologiemi. Druhá kapitola se věnuje popisu a rozboru vybraných nebezpečných aktivit spojených s využíváním moderních komunikačních technologií. Ve třetí kapitole blíže představuji kybergrooming, který je považovaný za jednu z nejnebezpečnějších komunikačních aktivit. Ve čtvrté kapitole jsou uvedeny projekty zabývající se nebezpečnými komunikačními jevy. Hlavním cílem teoretické části diplomové práce je charakterizovat problematiku kybergroomingu a některých dalších nebezpečných aktivit spojených s užíváním moderních komunikačních technologií.

Praktická část diplomové práce je věnována vlastnímu výzkumu. Popisuji v ní charakteristiku respondentů, metody a průběh výzkumného šetření, a vyhodnocuji jeho výsledky. Výzkumné šetření budu realizovat pomocí dotazníků distribuovaných mezi žáky 2. stupně základních škol a jejich následného vyhodnocení. Cílem praktické části mé diplomové práce je zmapovat, jak bezpečně se žáci 2. stupně vybraných základních škol chovají na internetu. Dílčími cíli je zjistit, jestli existují u předem stanovených věkových skupin statisticky významné rozdíly v počtu jedinců ochotných jít na osobní schůzku s člověkem, kterého by znali jen přes internet, a zda jsou mezi předem danými věkovými skupinami statisticky významné rozdíly v počtu jedinců ochotných sdělit tajemství člověku, kterého by znaly jen přes internet.

Jelikož téma kybergroomingu, kyberšikany, kyberstalkingu a některých dalších nebezpečných komunikačních aktivit není v současné době v české literatuře uchopeno v dostatečném rozsahu a hloubce, musel jsem při psaní své diplomové práce ve větší míře využívat internet a na něm zveřejněné informace vztahující se k této problematice. Jako další důležitý zdroj mi posloužily přednášky pořádané na dané téma, konzultace s odborníky a informační, propagační a preventivní materiály zabývající se danou problematikou.

TEORETICKÁ ČÁST

1 KOMUNIKACE A MODERNÍ KOMUNIKAČNÍ TECHNOLOGIE

Původ slova **komunikace** lze nalézt v latině. *„V latině communicare znamená communem reddere – učinit společným. Toto širší pojetí* ***sociální komunikace*** *lze v češtině vyjádřit termínem sdílení (na rozdíl od pouhého sdělování), v užším pojetí hovoříme o výměně informací. K nim řadíme i představy, ideje, nálady, pocity a postoje, které si lidé při komunikaci vyměňují.“*[3]

Během vývoje se slovo komunikace v českém jazyce značně rozšířilo a v praxi nabylo mnoho významů právě s ohledem na to, v jaké oblasti lidské činnosti se tento výraz používá, a tak je možné si pod ním představit například prostor vymezený pro spojení dvou míst, jako jsou chodníky, cesty, silnice, cyklostezky; obecně pak dopravní cesty – železnice, vodní a letecké cesty. Další výraz, se kterým se dá uvedené slovo spojit, je telekomunikace – mezi lidmi velmi rozšířené označení pro všechny metody elektronické komunikace, jako je telefon, telegraf, internet; rozšířený je i pojem masová komunikace, zahrnující televizi, rozhlas, tisk apod.[4]

Jedním z nejdůležitějších významů slova komunikace je dorozumívání čili kontakt dvou nebo více lidí, který se nejčastěji projevuje řečí a písmem. Právě na využití tohoto významu slova komunikace je založeno veškeré lidské bytí, bez ní by člověk nebyl schopen existovat jako druh. Od narození až do konce života mu komunikace pomáhá žít, vzdělávat se, pracovat, spolupracovat s ostatními, chápat přírodní i společenské zákonitosti, pokračovat kupředu k dalšímu rozvoji.[5]

Je ale také nutné si uvědomit, že během komunikace je jednání a následná reakce komunikujících osob ovlivněna nejen tím, co je sděleno, ale i tím, jak si sdělenou informaci daná osoba vyloží. U dvou osob může dojít k úplně odlišnému pochopení stejné sdělené informace, protože žádný člověk není stejný a každý má jiné zkušenosti, znalosti, je v jiném psychickém stavu, v jiné situaci a ovlivňuje ho spousta dalších věcí.

[3] BEDNAŘÍKOVÁ, I. *Sociální komunikace : texty k distančnímu a kombinovanému studiu.* Dotisk 1. vyd. z r. 2006. Olomouc : Univerzita Palackého v Olomouci, 2008. 79 s. ISBN 80-244-1357-4. s. 13.
[4] apod. – a podobně (dále jen „apod.“).
[5] TEGZE, O. *Neverbální komunikace : co vám prozradí lidské chování a jednání, a jak toho využít.* 1. vyd. Praha : Computer Press, 2003, 482 s. ISBN 80-7226-429-X.

Každá komunikace probíhá z nějakého důvodu, očekává nějakou reakci a je nevratná, ať už jde o komunikaci běžnou nebo elektronickou. Pokud je již něco vysloveno nebo napsáno a odesláno, nelze to již vzít zpět a je nutné počítat s reakcí jiné komunikující osoby nebo osob. Této skutečnosti se při nebezpečných internetových aktivitách snaží využít útočník a jeho cílem je takzvaně „vyloudit" na oběti nějaké osobní kompromitující informace, které po jejich získání útočník použije k vydírání dané osoby, případné oběti.

Komunikace je také jedinečná a neopakovatelná, protože každý se mění, jak po stránce psychické, tak i fyzické. Ke komunikaci dochází mezi všemi živými organismy na této planetě. Dodnes odborníci netuší, jak přesně funguje předávání informací mezi rostlinami, ale je fakt, že když například dojde k masovému okusu akácií žirafami v Africe, listy vedlejších stromů stejného druhu se stanou jedovatými, aby alespoň část stromů přežila.[6] Zvířata jsou v boji o přežití a zachování rodu nucena mezi sebou komunikovat a mezi nejznámější formy patří předávání informací pomocí zvuků, doteků tykadel, různých „tanců", soubojů a podobně. I když bylo v předchozí části zmíněno, že hlavními způsoby dorozumívání mezi lidmi jsou řeč a písmo, nelze opomenout ani další formy komunikace, jako jsou doteky, gesta, mimika, rituály, tanec apod., kterými se tak lidský rod řadí mezi ostatní druhy živočišné říše. Proto i v chápání pojmu komunikace jako dorozumívání je třeba rozlišovat komunikaci, která probíhá mezi zvířaty, a komunikaci mezi lidmi.[7]

1.1 Sociální komunikace

Aby se specifická lidská komunikace odlišila od ostatních komunikací, bývá označena jako komunikace sociální. Existuje mnoho různých definic snažících se přesně popsat slovní spojení „sociální komunikace". Sociální komunikaci lze definovat například takto: *„Sociální komunikace je specifickou formou spojení mezi lidmi, a to prostřednictvím předávání a přijímání významů."*[8]

[6] HUGHES, S. Antelope activate the acacia's alarm system. *NewScientist* [online]. 29.9.1990. [cit. 2011-07-12]. Dostupné z WWW: <http://www.newscientist.com/article/mg12717361.200-antelope-activate-the-acacias-alarm-system.html>. ISSN 0262-4079.

[7] TEGZE, O. *Neverbální komunikace : co vám prozradí lidské chování a jednání, a jak toho využít.* 1. vyd. Praha : Computer Press, 2003, 482 s. ISBN 80-7226-429-X.

[8] JANOUŠEK, J. Sociální komunikace. In VÝROST, J.; SLAMĚNÍK, I. *Sociální psychologie. 2. přepracované a rozšířené vydání.* Praha : Grada, 2008. s. 404 . ISBN 978-80-247-1428-8. s. 217.

1.1.1 Verbální a neverbální sociální komunikace

Ve spojitosti s nebezpečnými komunikačními jevy je důležité zaměřit se na oblast verbální a neverbální sociální komunikace. Je zřejmé, že způsob komunikace mezi pachatelem a obětí často značným způsobem ovlivní to, jestli pachatel bude, nebo nebude ve svých aktivitách úspěšný.

Podle komunikačních prostředků, které komunikace využívá, je možné ji podle Vymětala[9] dělit na:

- komunikaci verbální,
- komunikaci neverbální,
- komunikaci realizovanou činy a skutky.

Verbální komunikace se uskutečňuje za pomoci slov a písma. Řeč je základním dorozumívacím prostředkem lidí, který je vydělil z živočišné říše a umožnil člověku nevídaný rozvoj. Řeč vznikla dříve než písmo, a proto lze za základní formu verbální komunikace považovat rozhovor. Protože bylo potřeba předávat informace dalším generacím a také komunikovat i na delší vzdálenosti, vzniklo písmo. Tímto způsobem zaznamenané informace slouží k vyjádření věcného obsahu sdělovaného.

Druhou formou komunikace z tohoto úhlu pohledu je **komunikace neverbální** (mimoslovní), kdy komunikace „beze slov“ probíhá například za pomoci gest, mimiky, haptiky (kontaktu dotekem), proxemiky (fyzický odstup mezi osobami), posturologie (fyzických postojů těla) atd.[10] Proto je také nezřídka označována pojmem „řeč těla“, je autentičtější, hůře se skrývá, vyjadřuje emoce a často odhalí více informací o člověku a důvodech jeho jednání než pouhá řeč.[11]

Formou neverbální komunikace je **komunikace činem a skutkem,** která je často považovaná za nejúčinnější, protože příklad chování a jednání bývá mnohem důležitější než slova. Zvláště markantně vystupuje důležitost uvedené formy komunikace ve vztazích dospělých a dětí. Stokrát lze dítěti říkat, že nemá lhát nebo bít kamaráda, když dítě dospělého vidí, že sám lže nebo ubližuje slabšímu. V daném případě je čin (příklad) skutečně víc než slova. Pod komunikaci skutkem lze zahrnout i komunikaci darem, kdy je obdarovávanému

[9] VYMĚTAL, J. *Průvodce úspěšnou komunikací : efektivní komunikace v praxi*. 1. vyd. Praha : Grada, 2008. 322 s. ISBN 978-80-2472-614-4.
[10] atd. – a tak dále (dále jen „atd.“).
[11] TEGZE, O. *Neverbální komunikace : co vám prozradí lidské chování a jednání, a jak toho využít.* 1. vyd. Praha : Computer Press, 2003, 482 s. ISBN 80-7226-429-X.

typem vybraného dárku naznačeno, co o něm dárce ví nebo co si o něm myslí. Dárce tím zároveň vypovídá i o sobě, o své schopnosti empatie, o míře vkusu, schopnosti potěšit atd.

1.1.2 Intrapersonální, interpersonální, skupinová a veřejná komunikace

Dalším faktorem, který ovlivňuje úspěšnost pachatelů, je bezpochyby množství osob, které mohou oslovit. Se zvyšujícím se počtem osob, které dokáže pachatel oslovit, narůstá úměrně i jeho šance na úspěch.

Existují různé formy mezilidské komunikace, které mimo jiné určují, kolik osob v jednom okamžiku komunikuje. Zmíněné rozdělení určuje počet komunikujících osob od jedné do stovek, tisíců a dokonce i milionů.[12] Podle počtu zúčastěných osob pak je možné komunikaci rozdělit na tyto čtyři formy:

- intrapersonální,
- interpersonální,
- komunikace uvnitř malé skupiny lidí,
- veřejná komunikace.

Počet zúčastněných osob ovlivňuje i to, v jaké rovině organizace (uspořádání) společnosti se komunikace odehrává. Při **intrapersonální komunikaci** komunikuje člověk se sebou samým. Dochází k ní například v situacích, kdy jedinec zvažuje možná rozhodnutí nebo zpracovává nový poznatek. Jestliže dochází ke komunikaci mezi dvěma až třemi osobami, jedná se o **komunikaci interpersonální**. Tito lidé se prezentují jako jednotlivci, setkání je osobní a prezentované názory se neschovávají za anonymitu davu. Jako **skupinová komunikace** se označuje komunikace probíhající uvnitř určité ustanovené skupiny lidí, například rodiny, školní třídy, zájmového kroužku apod., mohou to být také různé konference, sympózia, semináře. Existují tzv. původci informace (vystupující) a příjemci (posluchači), kteří se s informacemi mohou i nemusí ztotožnit, mohou i nemusí k dané problematice vystoupit. Na rozdíl od interpersonální komunikace jde tedy ze strany příjemce informace o jistou anonymitu. Dalším druhem komunikace je **meziskupinová komunikace**, která probíhá mezi ustanovenými skupinami, například mezi sportovními týmy, školními třídami, zájmovými skupinami apod. V případě, že komunikace zahrnuje komunikační

[12] DEVITO, J. A. *Základy mezilidské komunikace*. 1. vyd. Praha : Grada, 2001. 420 s. ISBN 80-7169-988-8.

procesy probíhající například v rámci politických systémů, státních institucí, uvnitř podnikatelského subjektu, mezi podnikatelskými subjekty apod. jedná se o **institucionální/organizační komunikaci**. Komunikační aktivity, kdy jsou komunikační procesy potencionálně dostupné všem příslušníkům určité společnosti, zastupuje **celospolečenská komunikace**. Do celospolečenské komunikace zahrnujeme i mediální komunikaci podmíněnou existencí masových médií. Jde vlastně o specifický typ komunikace, kdy je informace předávána veřejnosti (tedy jakési anonymní skupině) prostřednictvím veřejných sdělovacích prostředků, kdy určitá skupina lidí informuje jinou skupinu lidí, aniž by příjemci informace mohli bezprostředně ovlivnit názory a postoje informátora či téma sdělované informace. Jedná se vlastně o jednostrannou formu komunikace s cílem informovat co největší množství lidí například o aktuální situaci ve společnosti.[13]

S ohledem např.[14] na téma kybergroomingu a na možné ohrožení komunikujících je třeba si v této souvislosti uvědomit, že je velmi pravděpodobné, že se úspěšnost pachatele bude měnit v závislosti na tom, jak bude s potencionální obětí komunikovat a jak velké množství lidí bude moci oslovit.

1.1.3 Funkce sociální komunikace

Sociální komunikace plní mnoho důležitých funkcí, kterými naplňuje rozmanité potřeby člověka. Například funkce **informativní**, zahrnující oblast předávání určitých informací. Funkce **instruktivní**, která je podobná předchozí funkci, ale navíc je zde zpravidla uveden postup, návod, popis, jak něčeho dosáhnout. Dále pak funkce **přesvědčovací**, zahrnující působení na druhého člověka s cílem změnit jeho názory nebo postoje. Funkce **svěřovací**, která slouží ke svěřování důvěrnějších informací blízkým osobám a k odstranění vnitřního napětí. Velmi důležité jsou také další funkce, a to **vzdělávací** a **výchovná**, poznávací, socializační a společensky integrující, které bývají často spojovány pouze se vzdělávacími institucemi, ale své nezastupitelné místo zde má i rodina, firmy a celá společnost. V souvislosti s moderními komunikačními technologiemi zaujímá velice významné místo funkce **zábavná**, která má za úkol pobavit, rozveselit, rozesmát a vytvořit příjemný pocit. Právě zábava je jedním z hlavních důvodů, proč mladá generace ráda využívá

[13] JIRÁK, J.; KÖPPLOVÁ, B. *Média a společnost*. 1. vyd. Praha : Portál, 2003. 207 s. ISBN 80-7178-697-7.
[14] např. – například (dále jen „např.“).

služeb moderních komunikačních technologií. Komunikace probíhá s nějakým záměrem. Jak uvádí Devito[15], tak pro většinu forem komunikace je společných těchto 5 cílů:

- učit se, tj.[16] získávat znalosti o druhých, o světě, o sobě,
- spojovat, tj. vytvářet vztahy s druhými, vzájemně na sebe reagovat,
- pomáhat, tj. naslouchat druhým a nabízet jim řešení,
- ovlivňovat, tj. posilovat nebo měnit postoje nebo chování druhých,
- hrát si, tj. těšit se z okamžitého prožitku.

1.1.4 Elektronická komunikace jako specifická forma sociální komunikace

Elektronická komunikace je zvláštní forma mezilidské (sociální) komunikace, která pro sdělování a vyměňování informací v reálném čase nevyžaduje fyzickou přítomnost komunikujících osob na jednom místě. Jedná se o „odlidštěnou" formu komunikace, kdy se osoby, které spolu komunikují, vlastně vůbec nemusí znát osobně. Výše uvedené může být i jedním ze zdrojů problémů. Právě na problémy spojené s využíváním moderních komunikačních technologií je tato diplomová práce zaměřena.

Za elektronickou komunikaci je možné označit veškerou komunikaci vedenou pomocí moderních prostředků informačních a komunikačních technologií. Díky obrovskému rozvoji ICT[17] došlo v posledních letech k podstatnému zvýšení množství komunikace probíhající v prostředí internetu, intranetu a mobilních sítí.[18] Mezi nejčastější typy elektronické komunikace patří telefonování, posílání e-mailů a chatování.[19]

Elektronickou komunikaci lze rozdělit na **on-line**, která se vyskytuje ve dvou podobách - synchronní a asynchronní, a **off-line**. Za online komunikaci se považuje komunikace, která probíhá pomocí počítačové sítě. *„Je-li tedy někdo on-line, je připojen k počítačové síti a je schopen komunikace."*[20]

U synchronní komunikace probíhá výměna informací okamžitě, tak jako v běžném hovoru. Dá se tedy říci, že se uskutečňuje v reálném čase. Komunikující strany jsou

[15] DEVITO, J. A. *Základy mezilidské komunikace*. 1. vyd. Praha : Grada, 2001. 420 s. ISBN 80-7169-988-8.
[16] tj. – to je (dále jen „tj.").
[17] ICT – Information and Communication Technology - informační a komunikační technologie - zařízení a prostředky výpočetní techniky (dále jen „ICT").
[18] KOPECKÝ, K. *Moderní trendy v e-komunikaci*. 1. vyd. Olomouc : Hanex, 2007. 98 s. ISBN 978-80-8578-378-0.
[19] chatování – „četování" - typ komunikace na internetu v reálném čase.
[20] KOPECKÝ, K. *Moderní trendy v e-komunikaci*. 1. vyd. Olomouc : Hanex, 2007. 98 s. ISBN 978-80-8578-378-0. s. 21.

komunikaci přítomny ve stejném čase, nenacházejí se však až na výjimky na stejném místě. Ovšem i tato komunikace pomocí prostředků ICT může být někdy zpožděna, a to díky rychlosti přenášených dat v komunikačním kanálu, takzvané odezvě, jejíž rychlost je často závislá právě na druhu a kvalitě vytvořeného propojení. Typickými představiteli synchronních komunikačních služeb jsou chaty, ICQ[21], Skype[22], Twitter[23] a další služby, kdy komunikace probíhá v reálném čase.

U asynchronní komunikace naopak dochází ke zpoždění v přenosu informací. Typickým příkladem je elektronická pošta, kdy je příjemce informován až ve chvíli, kdy si aplikaci s elektronickou poštou spustí, zprávu si přečte a rozhodne se, jak s informací naloží, a zda na ni bude reagovat. Takže komunikace probíhá teprve až po uplynutí určitého časového intervalu. K online komunikaci se v některých případech dá přiřadit komunikace mobilními telefony, kdy hovor lze považovat za komunikaci synchronní a zasílání textových zpráv za komunikaci asynchronní.[24] Na druhé straně za offline komunikaci se považuje taková komunikace, která je uskutečňována mimo počítačovou síť. *„Offline komunikace probíhá mimo počítačovou síť (například dopis, pohled). K offline komunikaci řadíme i uměle generované komunikační odezvy – např. u výukových programů, multimediálních encyklopedií apod.“*[25]

Podmínky pro využívání elektronické komunikace

Mezi hlavní prostředky umožňující veřejnosti připojit se do infrastruktury ICT patří mobilní telefony a domácí počítače. Aby společnost mohla tyto prostředky elektronické komunikace úspěšně využívat, je zapotřebí splnit několik podmínek. První podmínkou je **dostupnost těchto prostředků.** Díky rychlému rozvoji informačních technologií a rozšiřující se konkurenci ve výrobě těchto prostředků došlo i k prudkému poklesu cen, takže se mobilní telefony a osobní počítače staly dostupné prakticky každému zájemci. Kdokoli tak má možnost je využívat, a to tím způsobem, že si je buď pořídí, nebo využije veřejně přístupný internet například v internetové kavárně, počítačové učebně, knihovně, atd.

[21] ICQ – “I seek you“ – „Hledám tě“ – název klientského programu pro okamžitou komunikaci (dále jen „ICQ“).
[22] Skype – software pro internetovou telefonii.
[23] Twitter – poskytovatel sociální sítě a mikroblogu, který umožňuje uživatelům posílat a číst příspěvky zaslané jinými uživateli, známé jako tweety.
[24] KOPECKÝ, K. *Moderní trendy v e-komunikaci*. 1. vyd. Olomouc : Hanex, 2007. 98 s. ISBN 978-80-8578-378-0.
[25] KOPECKÝ, K. *Moderní trendy v e-komunikaci*. 1. vyd. Olomouc : Hanex, 2007. 98 s. ISBN 978-80-8578-378-0. s. 21.

Samotná komunikace je ovšem závislá nejen na již výše uvedeném přístupu k mobilním telefonům a osobním počítačům, ale i na dostupnosti infrastruktury umožňující připojení do sítí mobilních operátorů, poskytovatelů internetu a podobně. Druhou podmínkou je tedy **dostupnost připojení do sítě**, v níž elektronická komunikace probíhá. V této oblasti došlo v několika posledních letech k prudkému rozvoji technologií, výstavbě nových vysílačů. Používání optických kabelů a satelitního vysílání umožnilo získat připojení většině lidí i v odlehlých oblastech. Rozšíření možnosti Wi-Fi[26] připojení ve veřejných prostorech zdarma zase zabezpečuje možnost komunikace i těm, kteří si to doma nemohou dovolit.

Další nezbytnou podmínkou k využití e-komunikace je samozřejmě i určitá **úroveň znalostí**, jak s podobnými zařízeními pracovat. V této souvislosti se často mluví o takzvané „počítačové gramotnosti“. Pro mladou generaci je ovládání mobilních telefonů i počítačů samozřejmostí, střední generace zapojená do pracovní činnosti si už také dokázala osvojit potřebné znalosti a pozitivní je i snaha naučit v různých kurzech aktivně využívat tyto prostředky i seniory. Takže také tato podmínka je do značné míry již naplněna.

Pokud komunikující osoby splňují výše uvedené podmínky, potom lze říci, že je elektronická komunikace časově a místně neomezená a umožňuje komunikovat komukoli s kýmkoli, a to kdekoli a kdykoli.[27]

Elektronická komunikace rozšířila portfolio možností nabízejících získávání a výměnu informací o další dimenzi. Tento typ komunikace je v mnoha ohledech odlišný od ostatních, řekněme například klasických poštovních služeb. Vyniká především rychlostí a v současné době i poměrně dobrou dostupností všem, kteří mají přístup k některému z technických zařízení, které umožňuje její využití, jako jsou osobní počítače, notebooky, chytré mobilní telefony, osobní kapesní počítače PDA[28] a podobně. Současný rozvoj v elektronice umožňuje uživatelům mobilních telefonů ve stále větší míře využívat služby dříve dostupné jen uživatelům stolních počítačů.

To, jak se postupně přibližují možnosti uživatelů mobilních telefonů možnostem uživatelů s klasickým počítačem při práci s internetem, znázorňuje uvedený přehled:

[26] Wi-Fi – Wireless Fidelity – bezdrátová síť (dále jen „Wi-Fi“).
[27] KOPECKÝ, K. *Moderní trendy v e-komunikaci*. 1. vyd. Olomouc : Hanex, 2007. 98 s. ISBN 978-80-8578-378-0.
[28] PDA – Personal Digital Assistant – kapesní počítač nebo zápisník – malé přenosné elektronické zařízení (dále jen „PDA“).

<table>
<tr><th>Osobní počítač</th><th>Mobilní telefon</th></tr>
<tr><td>volání do mobilních i pevných sítí</td><td>volání do mobilních i pevných sítí</td></tr>
<tr><td>výměna textových zpráv SMS[29]</td><td>výměna textových zpráv SMS</td></tr>
<tr><td>výměna multimediálních zpráv MMS[30]</td><td>výměna multimediálních zpráv MMS</td></tr>
<tr><td>výměna e-mailových zpráv</td><td rowspan="12">Další funkce jsou závislé na vybavenosti konkrétního mobilního telefonu. Pokud mobilní telefon umožňuje připojení k síti internet, je co do počtu a kvality nabízených služeb téměř srovnatelný s osobním počítačem. To platí zejména při použití tzv. chytrých mobilních telefonů.</td></tr>
<tr><td>vyhledávání informací různého charakteru</td></tr>
<tr><td>účast na e-learningových[31] kurzech</td></tr>
<tr><td>možnost sdílení informací, zvuku i videa</td></tr>
<tr><td>komunikace pomocí sociálních sítí</td></tr>
<tr><td>možnost účasti na různých fórech</td></tr>
<tr><td>přístup k bankovním účtům</td></tr>
<tr><td>členství v on-line herních komunitách</td></tr>
<tr><td>sledování zpráv, televizního vysílání a poslouchání rádií</td></tr>
<tr><td>účast v různých soutěžích a hlasování v nich</td></tr>
<tr><td>komunikace se státní správou, tzv. e-Government[32] přes webová rozhraní</td></tr>
</table>

Tabulka č. 1 - Příklady služeb dostupných prostřednictvím osobního počítače a mobilního telefonu[33]

Rozdíly mezi běžnou a elektronickou komunikací

Je možné říci, že běžná i elektronická komunikace dnes již plní stejné funkce. Přesto lze při srovnání elektronické komunikace s běžnou komunikací nalézt jak shodné znaky, tak rozdíly. V obou se vyskytují stejné typy komunikace, ať už se jedná o komunikaci osobní, mezi dvěma osobami, skupinovou nebo s veřejností. „*Své myšlenky zaměníte na slova pomocí klávesnice a odešlete je prostřednictvím modemu způsobem velmi podobným tomu, kterým postupujete, když svá slova vysíláte vzduchem.*“[34] Pokud bychom hledali rozdíl, tak je to především ten fakt, že účastníci elektronické komunikace nemusí být ve chvíli

[29] SMS – Short Messaging Service – služba krátkých textových zpráv (dále jen „SMS“).
[30] MMS – Multimedia Messaging Service – služba multimediálních zpráv (dále jen „MMS“).
[31] e-learning – vzdělávací aktivity, kdy hlavním komunikačním médiem je počítač.
[32] e-Government – transformace vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií.
[33] Tabulka vytvořená autorem diplomové práce.
[34] DEVITO, J. A. *Základy mezilidské komunikace*. 1. vyd. Praha : Grada, 2001. 420 s. ISBN 80-7169-988-8. s. 20 – 21.

komunikace na stejném místě, ani nemusí komunikovat ve stejném čase a jejich komunikace je zprostředkovaná technikou. Není podstatné, jestli přes počítač, notebook, telefonní linku, mobilní telefon, webovou kameru nebo jiné technické zařízení.[35]

V elektronické komunikaci se navíc díky její částečné otevřenosti a neřízenosti můžeme často setkávat s mnohými komunikačními kódy, které představují například různé akronymy[36], emotikony[37], jazyky, grafické a vizuální symboly apod. Přestože existují určitá pravidla stanovující slušné chování při elektronické komunikaci známá pod názvem „netiketa“, mnozí komunikanti je nedodržují a používají výrazy, oslovení, slova, které by často při jiné komunikaci než elektronické nepoužili. To je obvykle zapříčiněno jejich pocitem anonymity, který získávají například při komunikaci přes internet.[38]

Nespornou výhodou na straně elektronické komunikace je rychlost, jakou se přenáší informace mezi komunikujícími. Níže je uvedeno několik rozdílů mezi běžnou komunikací a e-komunikací.

[35] KOPECKÝ, K. *Moderní trendy v e-komunikaci*. 1. vyd. Olomouc : Hanex, 2007. 98 s. ISBN 978-80-8578-378-0.
[36] akronym – zkratkové slovo složené z počátečních hlásek nebo slabik více slov.
[37] emotikon – „smajlík" - grafický symbol obvykle složený z interpunkčních a speciálních znaků.
[38] KOPECKÝ, K. *Moderní trendy v e-komunikaci*. 1. vyd. Olomouc : Hanex, 2007. 98 s. ISBN 978-80-8578-378-0.

Běžná komunikace	e – komunikace
Základním prostředkem komunikace je mluvený jazyk.	Základním prostředkem komunikace je zejména psaný jazyk, menší množství uživatelů využívá jazyk mluvený (Skype a VoIP[39] technologie).
Uživatelé nejsou anonymní.	Uživatelé mohou být anonymní.
Uživatelé zpravidla navzájem komunikují v omezeném počtu, ve skupinách.	Uživatelé mohou současně komunikovat s velkým počtem komunikantů (chat).
Uživatelé jsou omezeni prostorem a časem.	Uživatelé nejsou omezeni prostorem a časem.
Uživatelé využívají prostředky neverbální komunikace (mimika, gesta, proxemika, haptika aj.[40]	Uživatelé nahrazují neverbální komunikaci zástupnými symboly/ikonami (emotikony, akronymy).
Uživatelé jsou v přímém sociálním kontaktu.	Uživatelé jsou ve zprostředkovaném sociálním kontaktu.
Uživatelé komunikují (v rámci synchronní komunikace) bez předchozí přípravy.	Uživatelé komunikují (v rámci synchronní komunikace) po přípravě.
Uživatelé pro komunikaci nepotřebují žádné specifické zařízení.	Uživatelé pro komunikaci potřebují hardwarové a softwarové vybavení.
Uživatelé mohou ve velmi omezené míře využívat časově náročné (z hlediska doručení informace) asynchronní komunikace (dopisy, hlasové zprávy). Asynchronní informaci je obtížné snadno opravit (opravy v psaném dopise).	Uživatelé mohou velmi snadno využívat asynchronní komunikace bez časového omezení doručení informace (e-mail, ICQ zpráva, Skype chat). Veškeré textové informace lze snadno upravit.

Tabulka č. 2 - Rozdíly mezi běžnou komunikací a e-komunikací[41]

Mobilní telefony a internet jako základní prostředky elektronické komunikace

Mobilní telefon je zařízení fungující jako normální obyčejný telefon, ovšem s tím rozdílem, že pro komunikaci jej lze používat bez nutnosti fyzického (drátového) propojení s telefonní ústřednou. Mobilní telefony využívají pro zprostředkování přenosu hovoru a dat mobilními operátory vybudované sítě vysílačů, které dohromady vytvářejí globální systém pro mobilní komunikaci GSM. Propojení mezi jednotlivými uživateli telefonu není tedy

[39] VoIP – Voice over Internet Protocol – hlasové přenosy po internetu.
[40] aj. – a jiné (dále jen „aj.“).
[41] KOPECKÝ, K. *Moderní trendy v e-komunikaci*. 1. vyd. Olomouc : Hanex, 2007. 98 s. ISBN 978-80-8578-378-0.

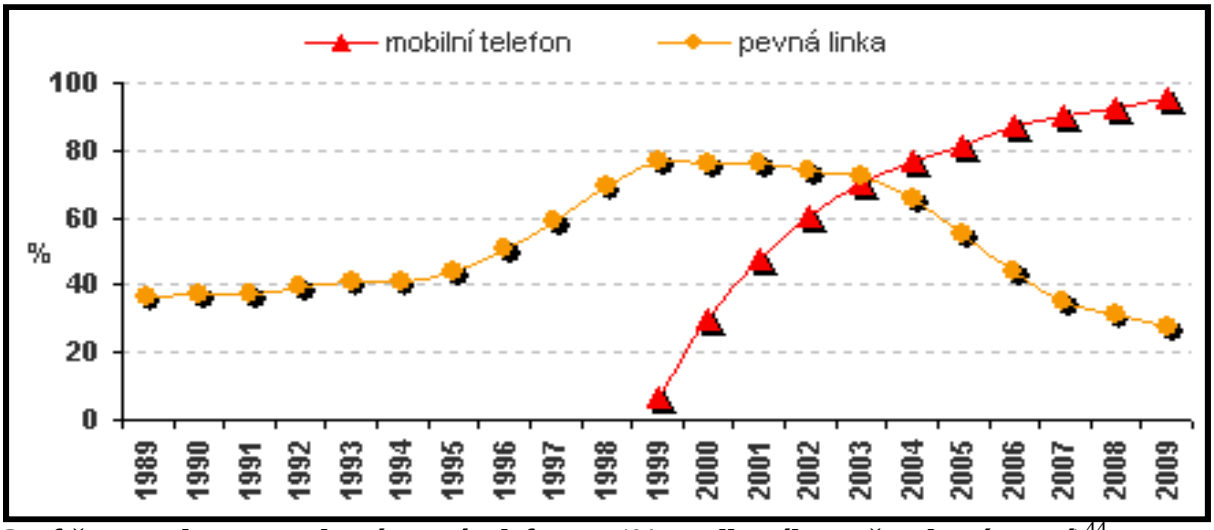
závislé na jejich propojení „drátem“, ale na dostupnosti vysílače (signálu mobilního operátora), který účastníkovi umožní využívat jeho služby.[42]

První mobilní telefon se na světě objevil již v roce 1973 a jmenoval se Motorola DynaTAC 8000X. Důležitým předpokladem pro jeho funkčnost byl vynález pocházející z laboratoře firmy Bell. Tyto laboratoře v roce 1947 zformovaly koncept celulárního (buňkového) systému vysílačů a přijímačů, které pokrývají určitou oblast. Mobilní sítě první generace využívaly pro přenos analogový signál, který byl později vytlačen digitálním signálem sítí druhé generace označované jako 2G. Dnes již mluvíme o sítích třetí generace umožňujících provozování nejnovějších technologií v mobilní komunikaci a tyto sítě třetí generace jsou označovány jako 3G. Vzhledem k tomu, že již od počátku byl o nově vznikající komunikační technologii obrovský zájem, zapojil se do jejího vývoje velký počet firem s vidinou obrovských zisků. Dnes můžeme potvrdit, že se jim tato očekávání vyplnila. Snaha o překonání konkurence vedla k ohromnému pokroku v této oblasti. Jen pro představu, mobilní telefon Siemens z roku 1986 vážil úctyhodných 8,8 kilogramů. To bylo důvodem, proč se první mobilní telefony montovaly hlavně do osobních automobilů, kde jejich váha, rozměry a energetická náročnost příliš nevadily. V průběhu let docházelo k neustálému zmenšování mobilních telefonů až do dnešní podoby. Díky této miniaturizaci můžeme mít telefon neustále u sebe, aniž by nás to nějak omezovalo. S postupující dobou se podařilo do telefonů implementovat různé rozšiřující funkce, např. budíky, fotoaparáty, videokamery, navigace, upomínky a další méně či více užitečné doplňky a aplikace.[43]

Vybavenost domácností pevnou telefonní linkou a mobilním telefonem

Dynamický nárůst počtu majitelů mobilních telefonů od roku 1999 v České republice znázorňuje graf vycházející z dat shromážděných Českým statistickým úřadem.

[42] Chcete vědět, jak funguje mobilní síť? *Mobilmania* [online]. 2001. [cit. 2011-06-20]. Dostupné z WWW: <http://www.mobilmania.cz/clanky/chcete-vedet-jak-funguje-mobilni-sit/sc-3-a-1100650>.
[43] KUBÍK, M. Vývoj mobilních telefonů (1. díl). *Galaxie* [online]. 7.5.2006. [cit. 2011-05-14]. Dostupné z WWW: <http://www.galaxie.name/index.php?clanek=vyvoj-mobilnich-telefonu-1-dil>.



Graf č. 1 - Vybavenost domácností telefonem (% z celkového počtu domácností)[44]

ČSÚ[45] uvádí, že na poli komunikačních technologií je pevná telefonní linka nejdéle sledovanou technologií v českých domácnostech. V roce 1989 disponovalo pevnou linkou 37 % domácností, během dalších deseti let se zvedl podíl o 40 procentních bodů na 77 % vykázaných v roce 1999. Od roku 1999 již ke zvyšování podílu nedocházelo, naopak pozvolný pokles vykazovaný do roku 2003 byl v následujících letech vystřídán prudkým poklesem domácností s pevnou telefonní linkou.

Je zřejmé, že k onomu poklesu docházelo na základě nástupu masivního využívání mobilních telefonů. V roce 1999 vlastnilo mobilní telefon 7 % domácností, o rok později již 30 % domácností a v roce 2001 mobilní telefon vlastnilo 48 % domácností tedy prakticky každá druhá domácnost v ČR[46]. I v dalších letech se vybavenost domácností mobilním telefonem neustále zvyšovala a v roce 2009 využívalo tuto technologii již 96 % domácností.

Ještě v roce 1999 připadlo na sto domácností pouhých 11 mobilních telefonů, jejich počet však v následujících letech prudce stoupal a v roce 2009 již připadalo na sto domácností téměř 200 mobilních telefonů.

V případě využívání mobilních telefonů, vyjádřeném počtem aktivních SIM[47] karet na 100 obyvatel, vykazovala Česká republika v roce 2009 ve srovnání s ostatními zeměmi Evropské unie dokonce vysoce nadprůměrné hodnoty.

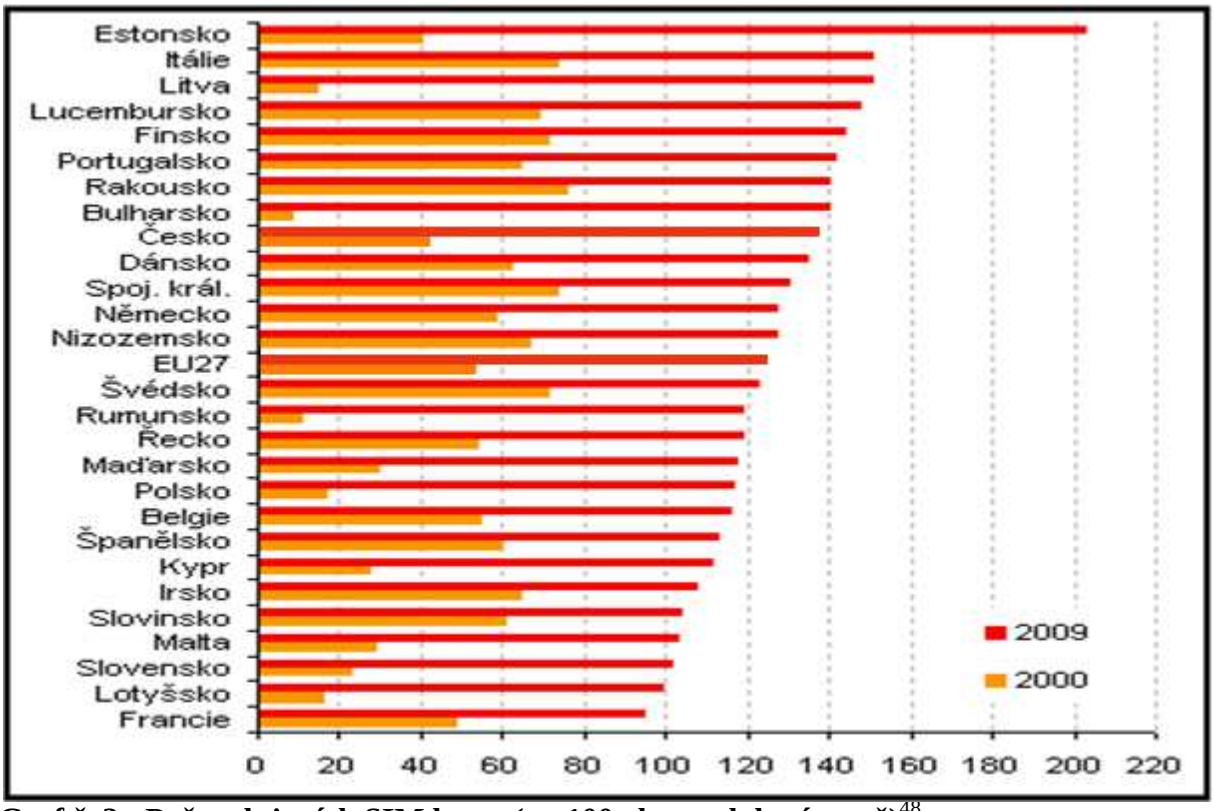
---

[44] Vybavenost domácností pevnou telefonní linkou a mobilním telefonem. *Český statistický úřad* [online]. 2009. [cit. 2011-10-20]. Dostupné z WWW: <http://www.czso.cz/csu/redakce.nsf/i/1_vybavenost_domacnosti_pevnou_telefonni_linkou_a_mobilnim_telefonem>.

[45] ČSÚ – Český statistický úřad (dále jen „ČSÚ“).

[46] ČR – Česká republika.

[47] SIM – Subscriber Identity Module – identifikační karta uživatele v mobilní síti (dále jen „SIM“).



Graf č. 2 - Počet aktivních SIM karet (na 100 obyvatel dané země)[48]

Už v roce 2009 bylo v České republice 138 aktivních SIM karet na 100 obyvatel a Česká republika se tak zařadila na 9. místo mezi zeměmi EU[49] v počtu používaných mobilních telefonů. V té době činil průměr evropské sedmadvacítky 125 aktivních SIM karet na 100 obyvatel. Dle ČSÚ Česká Republika překonala evropský průměr zatím v každém sledovaném roce od roku 2001. Nejlépe mezi zeměmi EU dopadlo v roce 2009 Estonsko, Itálie a Litva, nejhůře pak Slovensko.[50]

Internet a jeho vývoj

Internet představuje globální počítačovou „supersíť" spojující navzájem jednotlivé menší veřejně přístupné počítačové sítě. Jeho název se odvozuje z anglického slova network (síť), podle něhož obvykle končily názvy amerických počítačových sítí příponou „net"

[48] Vybavenost domácností pevnou telefonní linkou a mobilním telefonem. *Český statistický úřad* [online]. 2009. [cit. 2011-10-20]. Dostupné z WWW: <http://www.czso.cz/csu/redakce.nsf/i/1_vybavenost_domacnosti_pevnou_telefonni_linkou_a_mobilnim_telefonem>.

[49] EU – Evropská unie (dále jen „EU").

[50] Vybavenost domácností pevnou telefonní linkou a mobilním telefonem. *Český statistický úřad* [online]. 2009. [cit. 2011-10-20]. Dostupné z WWW: <http://www.czso.cz/csu/redakce.nsf/i/1_vybavenost_domacnosti_pevnou_telefonni_linkou_a_mobilnim_telefonem>.

a předpony „inter“ vycházející z latiny a znamenající „mezi“. Následným spojením této předpony „inter“ s příponou „net“ vznikl dnes známý název „Internet“. V současnosti je internet využíván k mnoha účelům jak v soukromé, tak ve veřejné sféře. Mezi nejznámější služby poskytované díky existenci internetu patří například různé webové stránky, elektronická pošta, chaty, sociální sítě[51] apod.[52]

Základem internetu je tzv. „hypertext“. Jde vlastně o odkaz na jiný dokument či soubor na webu. Služba World Wide Web vznikla v roce 1989 ve výzkumném středisku CERN[53] a odtud se rozšířila po celém světě.[54] Přenos informací v síti Internet probíhá pomocí aplikačních protokolů známých pod označením TCP/IP.[55]

Prvopočátky internetu spadají do poloviny šedesátých let. Tehdy se americká armáda snažila najít způsob, jak zajistit, aby armádní počítače rozmístěné po celém území USA[56] mohly spolu bez problému komunikovat, a to i v případě, že část této sítě bude vyřazena z provozu. Pracovníci RAND[57] Corporation přišli s unikátním řešením - vybudování sítě bez centrálního uzlu. Pokud by došlo ke zničení nebo poškození některé z linek, pak by byla informace ihned vedena k příjemci jinou trasou. Proto byla v USA vládou založena organizace Advanced Research Projects Agency ARPA[58], která byla pověřena speciálním výzkumem. Díky finančním prostředkům z resortu obrany v roce 1969 společnost ARPA vybudovala experimentální síť označovanou jako ARPANET. Tato síť byla určena především pro účely vládních a vojenských organizací. Postupně se k této síti připojovaly další instituce, především univerzity. Síť byla nekomerční záležitostí, na její vybudování přispívala americká armáda a různé vládní agentury. Podnikatelé o ni nestáli, protože v té době nenacházeli žádný komerčně zajímavý způsob jejího využití. Také proto se uvádí, že v roce 1984 bylo k Internetu (jak se začalo rozvíjející se síti říkat) připojeno pouhých 1000 počítačů.[59]

[51] sociální síť – nebo také komunita, je navzájem propojená skupina lidí.
[52] BEDNÁŘ, M. Co je vlastně internet? *Owebu* [online]. 4.7.2007. [cit. 2011-04-12]. Dostupné z WWW: <http://owebu.bloger.cz/Internet/Internet>.
[53] CERN – European Organization for Nuclear Research – Evropské středisko jaderného výzkumu.
[54] Vysvětlete babičce co je to Internet. *Owebu* [online]. 2004. [cit. 2011-03-15]. Dostupné z WWW: <http://owebu.bloger.cz/Internet/Vysvetlete-babicce-co-je-to-Internet>.
[55] TCP/IP – Transmission Control Protocol/Internet Protocol – přenosový kontrolní protokol/síťový protokol.
[56] USA – United States of America – Spojené státy americké.
[57] RAND – Research ANd Development – výzkum a vývoj.
[58] ARPA – Advanced Research Projects Agency – agentura pro výzkum pokročilých obranných projektů.
[59] BEDNÁŘ, M. Historie vzniku internetu. *Owebu* [online]. 9.7.2007. [cit. 2011-05-02]. Dostupné z WWW: <http://owebu.bloger.cz/Internet/Historie-vzniku-internetu>.

Vybavenost české populace osobními počítači a připojením k internetu

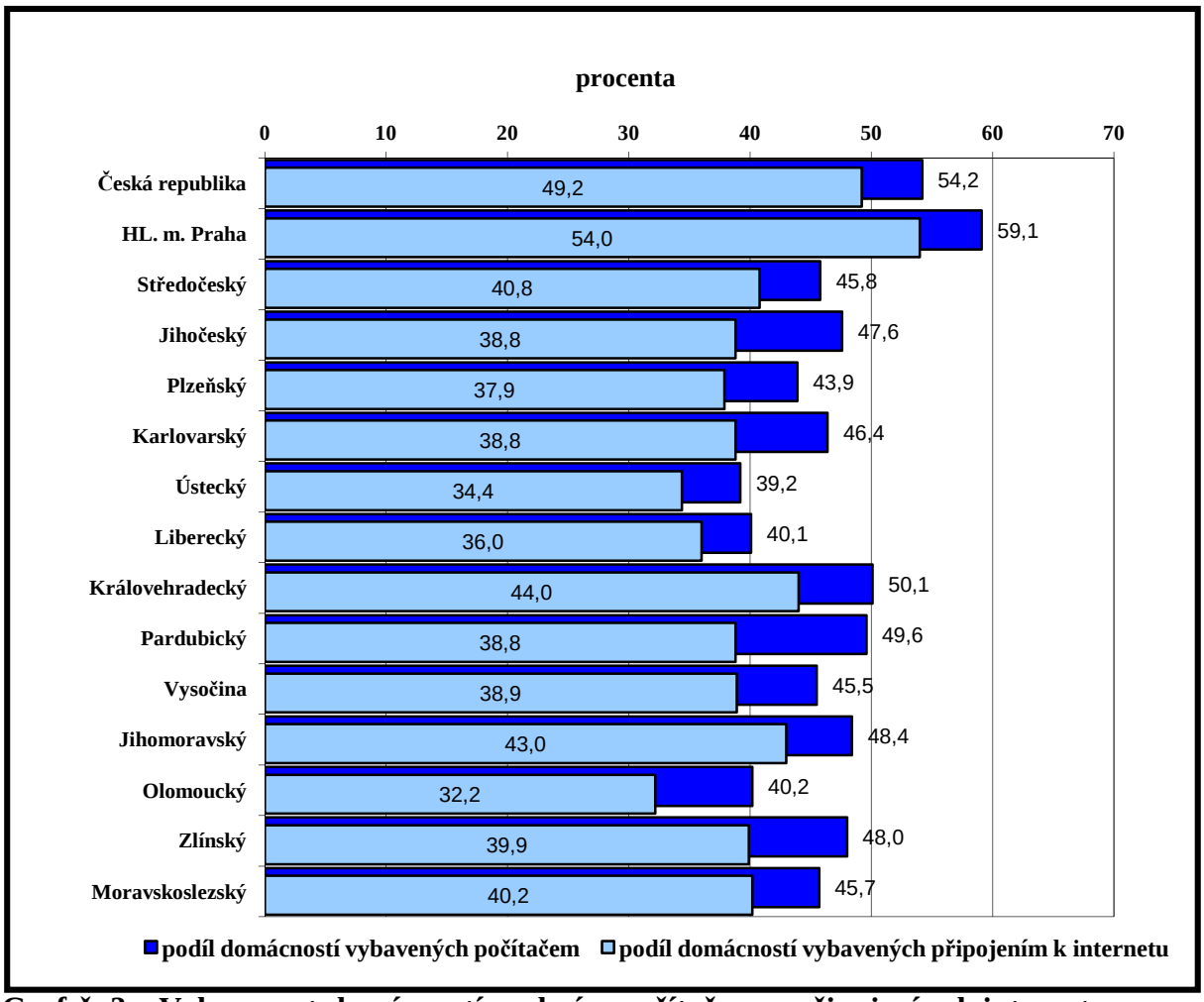
Obdobně jako vybavenost domácností mobilními telefony, narůstala v posledních letech i vybavenost domácností osobními počítači. Je zřejmé, že současně se zvyšujícím se počtem domácích počítačů docházelo také k nárůstu jejich připojení k internetu. Tento fakt podporují výsledky výzkumu, který ve 2. čtvrtletí 2009 uskutečnil ČSÚ. Ten provádí pravidelné šetření o využívání ICT v domácnostech. Údaje jsou vždy zjišťovány jedenkrát ročně. Z důvodu vyšší reprezentativnosti byla data od roku 2009 v regionálním členění publikována pouze za tříleté průměry. Pro představu, hodnota uvedená za rok 2009 je průměrem hodnot zjištěných v šetření ve 2. čtvrtletí roku 2007, 2008 a 2009. Právě na tomto šetření lze prokázat, že neustále dochází ke zvyšování vybavenosti domácností počítačem a zároveň ke zvyšování počtu domácích počítačů připojených k internetu.[60]

	Podíl domácností vybavených osobním počítačem (% z celkového počtu domácností)				Podíl domácností vybavených připojením k internetu (% z celkového počtu domácností)			
	2006	2007	2008	2009	2006	2007	2008	2009
Česká republika	35,7	39,6	47,7	54,2	26,7	32,0	41,7	49,2
HL.m. Praha	39,3	43,4	51,8	59,1	32,1	36,1	46,5	54,0
Středočeský	31,8	34,6	40,4	45,8	24,4	27,7	34,9	40,8
Jihočeský	30,5	33,6	40,7	47,6	19,8	24,2	31,2	38,8
Plzeňský	33,7	35,7	39,3	43,9	21,2	24,5	31,1	37,9
Karlovarský	31,4	34,6	41,5	46,4	20,2	23,6	31,1	38,8
Ústecký	23,6	27,5	32,8	39,2	16,4	20,2	27,0	34,4
Liberecký	27,8	31,8	35,8	40,1	18,8	23,8	29,7	36,0
Královehradecký	32,6	35,9	42,3	50,1	23,2	26,3	35,0	44,0
Pardubický	34,5	38,6	43,7	49,6	21,6	25,8	31,4	38,8
Vysočina	35,0	38,8	40,9	45,5	20,7	25,6	32,0	38,9
Jihomoravský	34,3	36,6	41,6	48,4	22,4	27,9	34,5	43,0
Olomoucký	23,0	25,7	34,1	40,2	16,1	19,1	26,2	32,2
Zlínský	28,8	32,9	39,5	48,0	16,4	21,7	30,0	39,9
Moravskoslezský	31,7	35,4	40,9	45,7	19,6	24,6	32,6	40,2
Období sběru dat: 4.Q 2003, 1.Q 2005, 2.Q 2006, 2.Q 2007 ,2.Q 2008, 2.Q 2009								
Krajské hodnoty jsou průměrem ze tří po sobě následujících let								

Tabulka č. 3 - Vývoj vybavenosti domácností osobním počítačem a připojením k internetu[61]

[60] Počítače v domácnostech. *Český statistický úřad* [online]. 2009. [cit. 2011-05-25]. Dostupné z WWW: <http://www.czso.cz/xb/redakce.nsf/i/pocitace_v_domacnostech>.

[61] Počítače v domácnostech. *Český statistický úřad* [online]. 2009. [cit. 2011-05-25]. Dostupné z WWW: <http://www.czso.cz/xb/redakce.nsf/i/pocitace_v_domacnostech>.



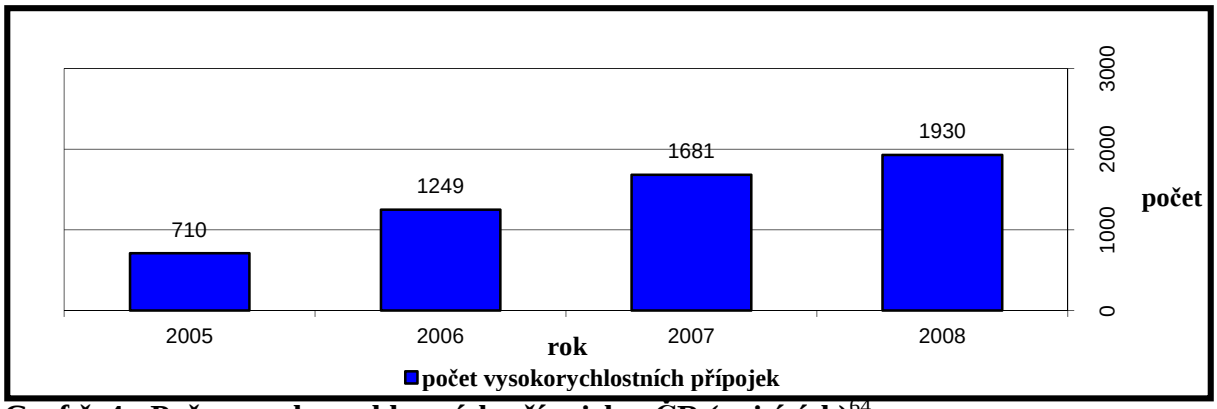
Graf č. 3 - Vybavenost domácností osobním počítačem a připojením k internetu v roce 2009[62]

Na základě zjištěných údajů lze konstatovat, že ve vybavenosti populace osobním počítačem došlo od roku 2006 do roku 2009 k průměrnému nárůstu o 15,13 procentního bodu. A v oblasti připojení populace k internetu došlo od roku 2006 do roku 2009 k průměrnému nárůstu o 15,11 procentního bodu.[63]

Dalším ukazatelem narůstajícího počtu uživatelů moderních komunikačních technologií je také množství vysokorychlostních přípojek. Vysokorychlostní připojení je totiž jednou z důležitých podmínek pro provozování aplikací nabízejících přenos obrazu a zvuku, tedy aplikací náročnou na množství přenesených dat za časovou jednotku. Vysokorychlostní připojení je nezbytné například pro bezproblémový přenos obrazu přes webovou kameru.

[62] Počítače v domácnostech. *Český statistický úřad* [online]. 2009. [cit. 2011-05-25]. Dostupné z WWW: <http://www.czso.cz/xb/redakce.nsf/i/pocitace_v_domacnostech>.
[63] Počítače v domácnostech. *Český statistický úřad* [online]. 2009. [cit. 2011-05-25]. Dostupné z WWW: <http://www.czso.cz/xb/redakce.nsf/i/pocitace_v_domacnostech>.

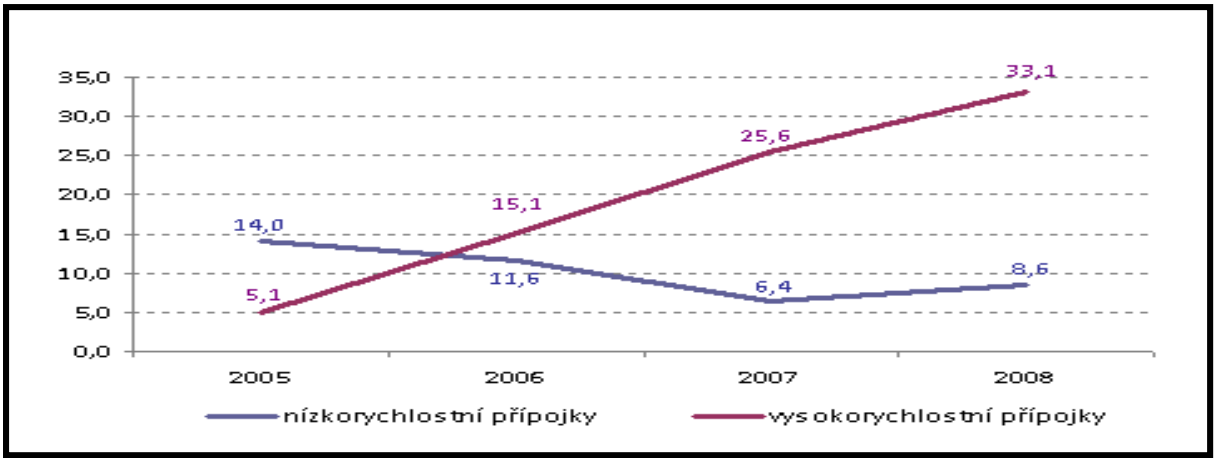
Následující graf ukazuje počet vysokorychlostních internetových přípojek v České republice a jejich vývoj od roku 2005.



Graf č. 4 - Počet vysokorychlostních přípojek v ČR (v tisících)[64]

Na základě údajů z grafu, který znázorňuje dynamický nárůst počtu vysokorychlostních přípojek do konce roku 2008, lze usuzovat, že během roku 2009 a následujících let překročí jejich počet hranici 2 miliónů.[65]

Z dalšího grafu, který znázorňuje zastoupení obou typů připojení v domácnostech, je ihned patrné, že i zde se vývoj ubíral očekávaným směrem. Zatímco počet nízkorychlostních přípojek v domácnostech klesal, počet těch vysokorychlostních zaznamenával postupný nárůst.



Graf č. 5 - Počet domácností s nízkorychlostním a vysokorychlostním připojením k internetu[66]

[64] Internetová infrastruktura. *Český statistický úřad* [online]. 2009. [cit. 2010-01-21]. Dostupné z WWW: <http://czso.cz/csu/redakce.nsf/i/internetova_infrastruktura>.
[65] Internetová infrastruktura. *Český statistický úřad* [online]. 2009. [cit. 2010-01-21]. Dostupné z WWW: <http://czso.cz/csu/redakce.nsf/i/internetova_infrastruktura>.
[66] Internetová infrastruktura. *Český statistický úřad* [online]. 2009. [cit. 2010-01-21]. Dostupné z WWW: <http://czso.cz/csu/redakce.nsf/i/internetova_infrastruktura>.

Využití mobilních telefonů v internetové komunikaci

Ve spojení s internetem lze mobilní telefony využívat k mnoha činnostem. Tento rozsah možného využití mobilních telefonů je přímo svázán zejména s následujícími faktory, technickou vybaveností konkrétního přístroje, schopností uživatele do zařízení implementované technologie využívat a portfoliem služeb nabízených mobilními operátory, popřípadě dalšími společnostmi umožňujícími komunikovat pomocí mobilních telefonů.[67] Mezi základní možnosti využití mobilního telefonu v internetové komunikaci můžeme zařadit:

- procházení (surfování) po internetu,
- čtení e-mailů,
- chatování,
- posílání a umísťování pořízených fotografií a videa na internet,
- stahování videa z internetu,
- sledování videa umístěného na internetu,
- sledování televizních stanic šířících svůj obsah přes internet,
- využívání služeb elektronického bankovnictví.

V dnešní době tzv. „chytré“ mobilní telefony často využívají ke svému provozu mobilní operační systémy. Tyto mobilní operační systémy mohou být modifikovanou verzí operačních systémů instalovaných do osobních počítačů, jako je například operační systém Windows mobile, ale i samostatnými operačními systémy vytvořenými primárně pro využití v mobilních telefonech. Mezi typické představitele systémů vytvořených pro mobilní telefony patří například systém Symbian nebo dnes stále se rozšiřující systém Android. Podstatné je, že obvyklou součástí operačních systémů instalovaných do mobilních telefonů bývají různé internetové prohlížeče.

U operačního systému Windows Mobile je to například internetový prohlížeč Internet Explorer, který se stal součástí operačních systémů řady Windows určených pro osobní počítače. Zejména v poslední době se v mobilních telefonech můžeme ve větší míře setkávat i s prohlížeči takzvaných třetích stran jako je například Opera či Firefox. Na základě využití těchto integrovaných prohlížečů internetových stránek je pak možné pohybovat se pomocí

[67] KOPECKÝ, K. *Moderní trendy v e-komunikaci*. 1. vyd. Olomouc : Hanex, 2007. 98 s. ISBN 978-80-8578-378-0.

mobilního telefonu v síti internet téměř v takovém rozsahu, jako kdyby uživatel seděl u klasického osobního počítače.

Nelze nezmínit možné využití mobilních telefonů jako modemu, tedy jako jakéhosi prostředníka pro spojení osobních počítačů s poskytovatelem internetu, a to zejména tam, kde se nelze připojit k internetu pomocí zařízení Wi-Fi, optického kabelu nebo jiných technologií umožňující připojení k poskytovateli internetu.

Využití mobilních telefonů v internetové komunikaci tedy sahá od prostého hlasového přenosu přes prostředníka a rozhraní sloužící k pořizování různých forem záznamů a jejich následného umísťování na internetu až po mobilní zařízení umožňující plné využití možností nabízených distributory moderních komunikačních technologií. Omezení spočívá opět jen v ceně takového zařízení, dostupnosti technologií na daném území a schopnosti majitele využít potenciál, který v sobě skrývá jeho mobilní telefon.

Z výše uvedených výzkumů, přehledů, grafů, tabulek však lze odvodit i určitá rizika spojená s používáním nových technologií při komunikaci mezi lidmi. Neustále se zvyšující počet mobilních telefonů mezi obyvateli České republiky jen dokazuje dostupnost služeb mobilních operátorů a internetu stále většímu počtu obyvatelstva. Na druhou stranu tato dostupnost s sebou nese riziko ohrožení většího množství obyvatel nebezpečnými komunikačními jevy. Zvláště pak příchod takzvaných „chytrých“ mobilních telefonů, běžně vybavených fotoaparátem nebo minikamerou, rozšířil možnosti jejich zneužití zejména pak k nafocení nebo natočení škodlivého obsahu. Takto pořízené záznamy mohou být dále šířeny prostřednictvím mobilních telefonů a internetu. Zatímco pevné linky neznamenají tak velké riziko zneužití z důvodu menší anonymity jejich uživatelů, tak u mobilních telefonů je ono riziko mnohem větší. Je totiž mnohem snazší zjistit majitele pevné telefonní linky, například z obyčejného telefonního seznamu, než majitele mobilního telefonu, kterému poskytují sítě mobilních operátorů větší anonymitu. Zmiňovanou anonymitu lze snadno získat v podstatě neomezenou možností nákupu takzvaných „přednabitých“ telefonních karet SIM. S každou takovou kartou poté případný útočník získává nové telefonní číslo, za kterým se může poměrně úspěšně skrývat. Ve chvíli, kdy má útočník pocit, že by mohl být odhalen, prostě starou kartu vyhodí a koupí si novou.

2 NEBEZPEČNÉ KOMUNIKAČNÍ JEVY PÁCHANÉ V PROSTŘEDÍ INTERNETU A MOBILNÍCH SÍTÍ

2.1 Kyberšikana

Jedním z nebezpečných komunikačních jevů spojených s využíváním moderních komunikačních technologií je kybernetická šikana (kyberšikana, cyberbullying). Jedná se o specifickou formu psychické šikany, kdy je oběť záměrně vystavována posměškům, nadávkám, vyhrůžkám a jiným druhům psychických útoků přicházejícím z kyberprostoru. Důsledkem kyberšikany jsou pak různá psychická traumata, která mohou oběť negativně ovlivňovat po celý její život a jejichž následkem může být v krajním případě i její smrt. Mezi obvyklé prostředky využívané pro realizaci kyberšikany patří zařízení připojená k internetu a sítím mobilních operátorů, která umožňují komunikaci pomocí chatů, e-mailů, MMS zpráv, SMS zpráv apod.

Kyberšikana má s tradiční šikanou jednu věc společnou, a tou je snaha útočníka své oběti ublížit nebo ubližovat. Další znaky jsou však poměrně odlišné. Jedním z rozdílných znaků je podle Krejčí[68] fakt, že se klasická šikana může projevovat útoky psychickými i fyzickými, zatímco u kyberšikany jde vždy pouze o útoky psychické. Portál E–Bezpečí[69] charakterizuje rozdílnost obou druhů šikany velice výstižně těmito slovy: *„Tak, jako se liší virtuální svět od světa reálného, liší se kyberšikana od tradiční šikany. Ve virtuálním světě mohou být lidé anonymní, mohou komunikovat, aniž by byli zatíženi společenskými rolemi, svými fyzickými nedostatky, psychickými bloky plynoucími z osobního kontaktu s lidmi, mohou vzájemně komunikovat, i když nejsou fyzicky přítomni, a pokud s někým v kontaktu být nechtějí, mohou komunikaci snadno ukončit.“*

Výše uvedená anonymita pachatelů je jedním z dalších specifických znaků, kterými se kyberšikana odlišuje od šikany. Tyto další znaky včetně již zmíněné anonymity pachatelů jsou popsány v následujícím textu.

[68] KREJČÍ, V. Kyberšikana - kybernetická šikana. *Net University* [online]. 2010. 72 s. [cit. 2011-07-23]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=14%3Akybersikana-studie>. ISBN 978-80-254-7791-5.
[69] Co je kyberšikana? *E-Bezpeci* [online]. 22.5.2009. [cit. 2011-07-27]. Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/14/6/lang,czech/>.

Specifické znaky kyberšikany

Anonymita útočníků

Uživatelé se při komunikaci ve virtuálním prostředí mohou na rozdíl od komunikace tváří v tvář schovávat za různé přezdívky, dočasně založené e-mailové účty nebo falešné identity, které si za tímto účelem vytvářejí. Díky zmíněnému faktu nelze jednoduchým způsobem odhalit jejich skutečnou identitu. To je také důvodem, proč při neosobní komunikaci potencionální útočníci získávají klamný pocit anonymity. Často se neoprávněně spoléhají na to, že nemohou být odhaleni, a právě domnělý pocit anonymity a nepolapitelnosti je jedním z důvodů, proč se útočníci kyberšikany bezostyšně dopouštějí, a proč jsou jejich útoky často velice brutální.[70]

Útočníci

Na základě anonymity, kterou poskytuje komunikace probíhající ve virtuálním prostředí, se pachateli kyberšikany stávají i jedinci, kteří by se tradiční šikany v reálném světě nedopustili. Právě anonymita pachatele a nepřítomnost fyzického kontaktu při komunikaci ve virtuálním prostředí totiž stírají rozdíly ve věku, pohlaví, fyzické síle a sociálním postavení, které by v případě tradiční šikany byly pro útočníka jistou překážkou. Pachatelem kyberšikany se tak narozdíl od tradiční šikany může stát v podstatě jakákoliv osoba, která disponuje znalostmi potřebnými pro aktivní využívání moderních ICT. Jak uvádí Kavalír a Rottová[71], *„pro kyberšikanování není zapotřebí fyzická síla, ale zdatnost v komunikačních technologiích, kterou může mít prakticky kdokoli“*.

Oběti

Obětí kyberšikany se může stát kdokoliv, a to bez ohledu na věk, pohlaví, sociální postavení či fyzickou zdatnost. V případě kyberšikany vždy záleží jen na tom, koho si útočník vybere za cíl svého útoku. Může se stejně tak jednat o předem vybraného jedince, jako

[70] BOCÁN, J. Kyberšikana. *Policie České republiky* [online]. [cit. 2011-06-29]. Dostupné z WWW: <http://www.policie.cz/clanek/krajske-reditelstvi-policie-pdk-aktuality-aaa.aspx>.
[71] KAVALÍR, A.; ROTTOVÁ, N. a kol. *Kyberšikana a její prevence – příručka pro učitele.* Plzeň : Dragon Press, 2009. 108 s. ISBN 978-80-86961-78-1. Dostupné z WWW: <http://www.varianty.cz/download/pdf/texts_160.pdf>. s. 17.

o náhodně zvolenou osobu. Mezi dětmi jsou kyberšikanou více ohroženy ty, které jsou závislé na používání mobilních telefonů a internetu.[72]

Čas a místo útoku

U tradiční šikany je možné v některých případech dopředu odhadnout místo a čas útoku. Díky této skutečnosti pak lze riziko potenciálního útoku dopředu omezit například tím, že dojde k zamezení fyzického kontaktu mezi pachatelem a obětí v rizikových časech a lokalitách. Naproti tomu obětí kyberšikany se může jedinec stát vždy, když používá internet, nebo když má u sebe mobilní telefon, a to bez ohledu na denní dobu a místo, kde se právě nachází. K útoku tak může například dojít i v jinak bezpečném prostředí domova.[73]

Chování jedinců ve virtuálním prostředí

Chování jedinců ve virtuálním prostředí je často velice odlišné od jejich chování při komunikaci v prostředí reálném. Jak uvádí Krejčí[74], *„virtuální realitu vnímají jako skvělé místo, kde se mohou bavit, plnit si své sny, kde mohou být takoví, jací chtějí být, kde si mohou vybudovat život podle svých představ. Lidé do virtuálního prostředí a virtuální komunikace vstupují s velkou důvěrou. Nechávají se ukolébat zdánlivou anonymitou prostředí - ta je svádí k tomu, aby se chovali méně opatrně než v reálném světě - jsou odvážnější v komunikaci, probírají citlivá témata (své problémy, sexualitu atd.), komunikují bez zábran.“*

Uživatelé si však obvykle neuvědomují, že jejich anonymitou ovlivněné chování ve virtuálním prostředí do značné míry ovlivňuje i to, jak snadno se mohou stát obětí kyberšikany nebo jiné nebezpečné komunikační aktivity. Na druhou stranu mnoha uživatelům anonymita virtuálního prostředí otevírá možnost, aby si vyzkoušeli aktivitu, které by se v reálném světě nedopustili, například šikanu.

Publikum a sekundární útočníci

Proto, aby pachatel kyberšikany svou oběť zasáhl několikanásobně a ve velkém měřítku, nemusí nutně v útoku pokračovat nebo jej opakovat. Zpravidla postačí, aby pouze

[72] Šikana a kyberšikana. *Protišikaně* [online]. 2011. [cit. 2011-07-28]. Dostupné z WWW: <http://proti-sikane.saferinternet.cz/sikana-a-kybersikana>.
[73] Co je kyberšikana *? E-Bezpeci* [online]. 22.5.2009. [cit. 2011-07-27]. Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/14/6/lang,czech/>.
[74] KREJČÍ, V. Kyberšikana - kybernetická šikana. *Net University* [online]. 2010. 72 s. [cit. 2011-07-23]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=14%3Akybersikana-studie>. ISBN 978-80-254-7791-5. s. 7.

jednou na internetu zveřejnil jakoukoliv hanlivou informaci (fotografii, video, karikaturu, pomluvu) o své oběti a vyčkal, až zmíněnou informaci rozšíří ostatní uživatelé, kteří ji na internetu naleznou. Publikum, které se tímto způsobem dostane ke kompromitujícím materiálům na internetu, lze pak rozdělit na diváky a šiřitele. Rozdíl mezi nimi spočívá v tom, že zatím co diváci pouze zvyšují okruh osob, které se o šikaně dozví, tak šiřitelé navíc ještě informaci o kompromitujícím obsahu poskytnou dalším uživatelům. Inkriminovaným jednáním se však vědomě, nebo i nevědomě do šikany sami zapojují. Z tohoto pohledu se pak šiřitelé stávají sekundárními útočníky, kteří poškozují oběť více než samotný primární aktér šikany. Množství osob, které se v roli diváka s projevy kyberšikany seznámí, tak může v konečném důsledku mnohonásobně převýšit velikost publika, které se obvykle stává svědky tradiční šikany.[75]

Dopady kyberšikany na oběť

Tradiční formu šikany, jakou je například fyzický útok, lze často odhalit díky modřinám a podlitinám na těle oběti. Sama tato skutečnost poskytuje rodičům (učitelům, vychovatelům apod.) možnost začít problém včas řešit. Výše zmíněné platí i v případech, kdy je oběť vystavena zároveň tradiční fyzické šikaně a kyberšikaně. Pokud se ale jedná jen o kyberšikanu, pak je často pro okolí oběti velmi nesnadné hned v počátcích na ni zareagovat, protože je spojená jen s psychickým týráním. Že je nějaká osoba pod psychickým tlakem není zpočátku hned patrné a je obtížně rozpoznatelné, což znesnadňuje možnost problém včas odhalit a řešit. Navíc samotné oběti kyberšikany často o svých problémech s okolím nemluví a nechávají si je jen pro sebe. Důvodem jejich neochoty svěřit se někomu se svou situací může být například stud, strach, nepochopení závažnosti situace nebo pocit, že by jim stejně nikdo nepomohl. Oběti kyberšikany tak na řešení svých problémů často zůstávají sami, což může vést k tomu, že situaci nezvládnou.[76]

[75] KREJČÍ, V. Kyberšikana - kybernetická šikana. *Net University* [online]. 2010. 72 s. [cit. 2011-07-23]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=14%3Akybersikana-studie>. ISBN 978-80-254-7791-5.
[76] Co je kyberšikana ? *E-Bezpeci* [online]. 22.5.2009. [cit. 2011-07-27]. Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/14/6/lang,czech/>.

Případy kyberšikany

Ghyslain Raza - Star Wars Kid

V roce 2002 si Ghyslain Raza, žák střední školy z Quebecu v Kanadě, nahrál na video své pokusy o ztvárnění postavy Darth Maula z Hvězdných válek. Jeho spolužáci nahrávku našli a v roce 2003 ji zveřejnili na internetu. Mělo jít o malý kanadský žertík. Nahrávka se ale stala velice populární a během 14 dnů zaznamenala několik milionů stažení. Posléze byla parodována a mixována s filmy jako je Kill Bill, Matrix, Pán prstenů a další. V roce 2008 byl Raza parodován i v jednom z dílů seriálu South Park. Díky uvedení ve jmenovaném televizním seriálu tak mohli scénku shlédnout i lidé nepřipojení k internetu. Když se Raza dozvěděl o této pro něj negativní popularitě, zhroutil se a musel být dlouhodobě hospitalizován. Chlapcova rodina zažalovala rodiče čtyř Razových spolužáků, kteří nahrávku na internet umístili, a požadovala odškodné ve výši 250 000 kanadských dolarů. Ještě dnes je možné na internetu shlédnout jak originální záznam pořízený samotným Razou, tak i jeho různé parodované mutace.[77]

Anna Halman

Šokující příběh polské dívky Anny Halman (* 21.6.1992- + 21.10.2006) se díky velké medializaci dostal do povědomí mnoha lidí, a široká veřejnost tak měla možnost seznámit se s nebezpečným jevem, jakým je kyberšikana. Její smutný příběh se odehrál v roce 2006 v Polském Gdaňsku. Anna byla podle svých spolužáků i rodičů mimořádně stydlivá dívka. Možná proto se nikomu nesvěřila, že ji ve škole šikanují spolužáci. Jednoho z nich odmítla, když s ní chtěl chodit, a on se jí tímto způsobem začal mstít a jeho kamarádi mu pomáhali. První útoky byly slabé, ale postupně nabíraly na intenzitě. Její kamarádky si na problém stěžovaly a napsaly o něm do školní knihy stížností. Zmíněné výpovědi dívek později vyvrátily tvrzení ředitele školy, že o ničem nevěděl a proto nemohl útokům nijak zabránit. Situace se vyhrotila dne 20.10.2006, kdy učitelka odešla na delší dobu ze třídy. Annini spolužáci využili příležitost a napadli ji. Začali Annu ponižovat, strhávat z ní šaty, osahávat a předstírat, že ji znásilňují. I když je Anna prosila, aby toho nechali a snažila se jim uniknout, útok pokračoval. Ostatní spolužáci na její prosby o pomoc nereagovali a pouze přihlíželi. Spolužačky, které Anně pomoci chtěly, zase neměly tolik sil, aby proti útočníkům zakročily.

[77] FUKA, F. FFFILM: Star Wars Kid. *Novinky* [online]. 30.7.2003. [cit. 2011-09-21]. Dostupné z WWW: <http://www.novinky.cz/kultura/12434-fffilm-star-wars-kid.html>.

Jeden z chlapců zaznamenával průběh útoku na mobilní telefon. Posléze také dívce oznámil, že záznam zveřejní na internetu, aby si jej mohl každý prohlédnout. Dívka po této události utekla domů a nikomu se s uvedeným útokem nesvěřila. Večer za ní přišla spolužačka, ale nic nenasvědčovalo tomu, že by si Anna chtěla vzít život. O několik hodin později 21. října rodiče našli Annu oběšenou. Nikde se nenašel žádný dopis na rozloučenou, ve kterém by zdůvodnila svůj čin. Pátrání policie se postupně zaměřilo na školu, kterou dívka navštěvovala. Od tohoto okamžiku začaly na světlo vystupovat hrozné události, které předcházely zoufalému činu Anny. Vyšetřování vedlo ke zjištění, že i když se ve škole vědělo o posledním útoku na Annu už v pátek 20. října, nebyla učiněna žádná opatření směřující k prošetření incidentu. Nebyly včas zajištěny důkazy, ani potrestáni pachatelé. Na rozdíl od přehlíživého postoje školy policie neváhala a na základě zjištěných informací už ve středu zatkla viníky útoku. Ti byli hned na začátku vyšetřování umístěni do ústavu pro nezletilé, odkud je po několika týdnech na žádost právníků propustili. Jejich propuštění provázela kritika jak ze strany laické, tak i odborné veřejnosti. Protože se pachatelům podařilo videonahrávku útoku smazat, neexistoval o něm důkaz. Obhájci pachatelů se tedy snažili bezostyšně tvrdit, že nešlo o nic hrozného a že pravým důvodem dívčiny sebevraždy byly neutěšené poměry v její rodině. Oproti jejich očekávání se však policejním technikům povedlo smazaný záznam zčásti obnovit, a tak se rekonstruovaná videonahrávka stala velice důležitou pro celý případ. Díky ní měla žalující strana relevantní informace, k čemu v inkriminovaný den skutečně došlo. Dne 20. dubna 2007 soud rozhodl, že případ nebude odložen ani ukončen navržením kurátorského dohledu, ale že provinilci podstoupí řízení, které rozhodne o jejich umístění v nápravných ústavech pro mladistvé. Na smuteční obřad a pohřeb Anny, který se konal 27.10.2006, přišlo okolo jednoho tisíce lidí. Souběžně v tento den na všech školách v Polsku proběhly demonstrace žáků a studentů proti násilí na školách.[78]

2.2 Sexting

Termín sexting vznikl spojením slov sex a textování. Jedná se o elektronické rozesílání textů, obrázků nebo videa se sexuálním obsahem. Rozesílaný citlivý materiál často vzniká v rámci partnerských vztahů, kdy si partneři navzájem vyměňují své intimní erotické fotografie. Problém nastává v okamžiku, kdy je taková citlivá informace zneužita s cílem

[78] Polská studentka se oběsila kvůli sexuální šikaně. *iDNES* [online]. 26.10.2006. [cit. 2011-09-22]. Dostupné z WWW: <http://zpravy.idnes.cz/polska-studentka-se-obesila-kvuli-sexualni-sikane-fsb-/zahranicni.aspx?c=A061026_141456_krimi_rez>.

poškodit zaznamenanou osobu. Jde kupříkladu o situace po ukončení vztahu, kdy se zhrzený partner s rozchodem nesmíří a chce se bývalému partnerovi pomstít a zesměšnit ho. Zveřejní intimní citlivá data o svém protějšku například na internetu nebo je začne šířit prostřednictvím mobilního telefonu. V případech sextingu, kdy jsou šířeny erotické intimní materiály zobrazující osoby mladší 18 let, může být tato činnost považována za šíření dětské pornografie, ohrožování mravní výchovy mládeže apod.[79]

Případ sextingu v České republice

Patnáctiletá dívka z Měřína na Žďársku pořídila svůj erotický snímek, a poslala ho elektronickou poštou chlapci, který se jí líbil. Onen chlapec získanou fotografii dívky následně poskytl dalším spolužákům. Intimní fotografie se postupně šířila mezi dětmi, dostala se až k učitelkám Základní školy v Měříně, a ty případ oznámily kriminalistům. Chlapci, který fotografii obdržel a rozšířil, stejně jako dalším osobám, co se na její distribuci podílely, hrozil trest za šíření dětské pornografie. Celý případ nakonec skončil tím, že u nezletilých spolužáků, kteří se rozšiřování fotografie účastnili, bylo vzhledem k jejich věku trestní stíhání odloženo. U mladistvých spolužáků bylo zahájené trestní stíhání zastaveno poté, co si hříšníci odpykali svůj trest splněním desítek hodin společensky prospěšné činnosti.[80]

Případ sextingu v zahraničí

Studentka z amerického Cincinnati Jessie Loganová poslala svému příteli svoji erotickou fotografii. Dotyčnou fotografii však její zhrzený partner zneužil poté, co se spolu rozešli. Za rozchod chtěl dívku potrestat tím, že zmíněnou fotografii umístil na internetu. Kamarádi, kteří uveřejněnou fotku shlédli, ji začali rozesílat dalším lidem a ti zase dalším. Fotografie se řetězově šířila mezi lidmi. Postupně se tak dívka stala středem nechtěné pozornosti ve škole i na internetu. Vše dospělo do takového stádia, že se Jessie díky zneužité fotografii musela neustále potýkat s různými pošklebky a narážkami, a to i od zcela neznámých lidí. Nevěděla si rady, ani oznámení na policii jí nepomohlo. Nakonec se odhodlala k poslednímu zoufalému kroku, kterým chtěla vše zastavit. Vystoupila v regionální televizi, kde všechny žádala, aby jí neubližovali a nechali ji být. Její žádost však

[79] KOPECKÝ, K.; KREJČÍ, V. Co je vlastně sexting? *Sexting* [online]. 2009. [cit. 2011-09-19]. Dostupné z WWW: <http://www.sexting.cz/>.
[80] KUBÍKOVÁ, L. Děti z Měřína byly potrestány za šíření porna. *Žďárský deník* [online]. 29.10.2009. [cit. 2011-09-19]. Dostupné z WWW: <http://zdarsky.denik.cz/zlociny-a-soudy/deti-z-merina-byly-potrestany-za-sireni-porna.html>.

nebyla vyslyšena a útoky na dívku pokračovaly. Jessie nakonec situaci neunesla a spáchala zoufalý čin, oběsila se.[81]

2.3 Happy slapping

Jednou z mnoha nebezpečných internetových aktivit je i happy slapping volně překládané jako „spokojené fackování“. Jedná se o typ šikany, kdy útočníci záměrně a nečekaně napadají jiné osoby, přičemž si pořizují záznam svého útoku například na videokameru, nebo mobilní telefon. Takto pořízený záznam pak zveřejňují na internetu, nebo šíří prostřednictvím mobilních telefonů, aby mohl sloužit pro pobavení ostatních lidí. Happy slapping se stal velice nebezpečným ve chvíli, kdy se původní zaznamenávání a zveřejňování „neškodných žertů“ zvrhlo v natáčení záměrných brutálních útoků, které nezřídka pro oběť končily těžkým ublížením na zdraví, nebo dokonce i smrtí.

Za kolébku happy slappingu je považována Velká Británie, kde se v roce 2004 začaly objevovat první případy této nebezpečné aktivity. Zde také v roce 2005 vyšel novinový článek, který se danou problematikou zabýval, a ve kterém byl poprvé použitý termín happy slapping. Po značném rozmachu, který v Anglii happy slapping zaznamenal, se tento nebezpečný jev postupně rozšířil i do mnoha dalších zemí celého světa.[82]

Pachateli happy slappingu jsou především mladí lidé, kteří se tímto způsobem snaží zviditelnit, pobavit nebo zahnat nudu. Pro představu, čeho jsou aktéři při happy slappingu schopni, mohou posloužit níže uvedené případy.

Anglická policie v roce 2005 zatkla tři chlapce ve věku 14 let pro podezření ze znásilnění 11 leté dívky. Policejní orgány se o činu dozvěděly na základě oznámení zaměstnance školy, který našel záznam útoku na mobilním telefonu jednoho ze studentů.[83]

Starší muž z Anglie byl v roce 2009 při odchodu z mešity napaden a zbit členy happy slappingového gangu. Tento muž o týden později podlehl následkům zranění, které mu násilníci při brutálním útoku způsobili.[84]

[81] Dívka se oběsila kvůli své nahé fotce na webu. *Aktuálně* [online]. 18.3.2009. [cit. 2011-09-19]. Dostupné z WWW: <http://aktualne.centrum.cz/zpravy/krimi/clanek.phtml?id=632277>.
[82] Happy slapping. *E-Bezpeci* [online]. 15.11.2008. [cit. 2011-06-23]. Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/71/39/lang,czech/>.
[83] TOSIN, S. Girl's rape 'filmed by teenagers on mobile'. *Timesonline* [online]. 18.6.2005. [cit. 2011-08-27]. Dostupné z WWW: <http://www.timesonline.co.uk/tol/news/uk/article534788.ece>.

V roce 2005 byli v České republice zatčeni příslušníci gangu, který se nazýval „Plameňák“. Tato skupina mladých lidí na internetu zveřejňovala svá videa, na kterých členové gangu bezdůvodně napadali náhodně vybrané oběti.[85]

2.4 Kyberstalking

Kyberstalking představuje další nebezpečný komunikační jev, jehož existence je přímo svázána s moderními ICT. Označení kyberstalking se používá v případech, kdy útočník využije moderní ICT pro páchání tzv. stalkingu. Pojem stalking lze přitom do českého jazyka přeložit jako pronásledování, stopování, a původně byl používán v souvislosti s lovnou zvěří. Poté, co se stalkingem začaly v polovině devadesátých let zabývat první klinické studie, zahrnuli jejich autoři pod tento pojem i pronásledování lidí.

Válková[86] na téma stalking uvádí: *„Vycházeli-li bychom z doslovného překladu, pak bychom přeložili stalking nejspíše obratem „pronásledovat, stopovat divokou zvěř“, který vcelku příhodně vystihuje, oč v celé věci jde. Namísto lovné zvěře zde ovšem vystupuje člověk, který je vystaven podobným útokům, ne vzácně dokonce i se stejně fatálním vyústěním, jako je tomu u úspěšného lovu, pokud se totiž lovci podaří svou kořist dostihnout a usmrtit.“*

Díky dostupnosti internetu, počítačů a mobilních telefonů široké veřejnosti mají stalkeři k dispozici další, vcelku jednoduchý a nenáročný způsob, kterým mohou stalking páchat, a tím pronásledovanou oběť systematicky deptat.[87] Stalking i jeho následky popisuje Čírtková[88] následujícím způsobem: *„v kriminologickém smyslu je stalking definován jako úmyslné, zlovolné pronásledování a obtěžování jiné osoby, které snižuje kvalitu života a ohrožuje její bezpečnost. Přímým následkem stalkingu je závažné narušování soukromí, osobní svobody a lidské důstojnosti oběti. V závažných případech poškozuje stalking duševní i tělesné zdraví oběti, či dokonce ohrožuje její život.“*

---

[84] Attorney General to review 'happy-slap' sentence. *BBC News [*online]. 29.6.2009. [cit. 2011-06-24]. Dostupné z WWW: <http://www.bbc.co.uk/news/uk-england-london-10808090>.
[85] FRANZLOVÁ, O. Při napadání lidí se útočníci fotili. *iDNES* [online]. 19.1.2005. [cit. 2011-08-21]. Dostupné z WWW: <http://zpravy.idnes.cz/krimi.aspx?r=krimi&c=A050118_211928_krimi_sas>.
[86] VÁLKOVÁ, H. Česká podoba stalkingu podle § 354 TrZ v širších než jen trestněprávních souvislostech. *iPrávník* [online]. 26.3.2010. [cit. 2011-08-19]. Dostupné z WWW: <http://www.ipravnik.cz/cz/clanky/pd_1/txtexpresion_dlu%C5%BEn%C3%ADku/art_6562/detail.aspx>.
[87] ČÍRTKOVÁ, L. *Moderní psychologie pro právníky : domácí násilí, stalking, predikce násilí.* 1. vyd. Praha : Grada, 2008. 150 s. Psyché (Grada). ISBN 978-80-247-2207-8.
[88] ČÍRTKOVÁ, L. *Moderní psychologie pro právníky : domácí násilí, stalking, predikce násilí.* 1. vyd. Praha : Grada, 2008. 150 s. Psyché (Grada). ISBN 978-80-247-2207-8. s. 53.

Pachatelé stalkingu a kyberstalkingu

Dle Kopeckého[89] nemusí být snadné stalkera rozpoznat a často se to ani nepodaří. Stalker může navenek vypadat jako společensky naprosto normální člověk, o kterém ani jeho nejbližší okolí nemusí tušit, že se dopouští obtěžování například prostřednictvím internetu nebo mobilního telefonu. Každý stalker schopný využívat moderní ICT může být zároveň i kyberstalkerem.

Oběti stalkingu a kyberstalkingu

Obětí stalkingu a kyberstalkingu se může stát kdokoliv, a to bez ohledu na věk, pohlaví, sociální statut, kulturní zázemí, vzhled nebo sexuální orientaci. Pronásledování se vyskytuje stejně tak mezi osobami, které pojí nebo pojily skutečné vztahy, jakož i mezi osobami, které se nikdy osobně nesetkaly.[90] Jak uvádějí Dresssing, Maulk-Backer a Gass[91], tak častějšími oběťmi stalkingu bývají ženy, dále pak také osoby, které jsou osamoceny, a osoby, co ukončily se stalkerem vztah. Nebezpečí stalkingu ve větší míře hrozí taktéž veřejně známým osobnostem, jako jsou herci, politici, a osobám, jež jsou v užším kontaktu s jinými lidmi (učitelé, lékaři, soudci, advokáti, profesoři).

Typické projevy stalkingu a kyberstalkingu

Stalker může svoji činnost provádět několika způsoby, například šířením pomluv, ničením věcí, posíláním dárků, telefonováním apod. Pokud jsou používané způsoby využívány jednotlivě a samostatně, nelze je považovat přímo za stalking. Teprve souhrnné informace o všech aktivitách stalkera podávají celkový obraz případu a je možné stanovit, jestli se jedná o stalking.[92]

Pachatel zpravidla používá následující způsoby pronásledování:

---

[89] KOPECKÝ, K. Stalking a kyberstalking : Nebezpečné pronásledování. *E-Nebezpečí* [online]. Olomouc : Net University, 2010. 14 s. [cit. 2011-07-29]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu>.
ISBN 978-80-254-7737-3.

[90] ČÍRTKOVÁ, L. *Moderní psychologie pro právníky : domácí násilí, stalking, predikce násilí.* 1. vyd. Praha : Grada, 2008. 150 s. Psyché (Grada). ISBN 978-80-247-2207-8.

[91] DRESSSING, H.; MAULK-BACKER, H.; GASS, P. Posuzování stalkingu z kriminalistického hlediska. *iPrávník* [online]. 28.11.2007. [cit. 2011-07-22]. Dostupné z WWW: <http://www.ipravnik.cz/cz/clanky/trestni-pravo/art_5000/posuzovani-stalkingu-z-kriminalistickeho-a-psychiatrickeho-hlediska.aspx>.

[92] ČÍRTKOVÁ, L. *Moderní psychologie pro právníky : domácí násilí, stalking, predikce násilí.* 1. vyd. Praha : Grada, 2008. 150 s. Psyché (Grada). ISBN 978-80-247-2207-8.

- Neustále se opakující pokusy kontaktovat oběť například pomocí dopisů, telefonátů, SMS zpráv, MMS zpráv, e-mailů, prostřednictvím chatu, sociálních sítí nebo zasíláním pozorností a dárků.
- Přímé nebo nepřímé výhrůžky, které u oběti vyvolávají nepříjemné pocity.
- Fyzické pronásledování oběti například při její cestě do zaměstnání, na nákup nebo prostým čekáním na oběť v místě jejího bydliště.
- Záměrné ničení a poškozování majetku pronásledované osoby například poškrábáním laku u vozidla oběti, rozbitím oken u jejího bytu nebo zasíláním zavirovaných e-mailů.
- Zneužívání osobních údajů oběti a ničení její pověsti například tím, že stalker zveřejní osobní údaje oběti na internetu a spolu s nimi uvede nepravdivou, nebo hanlivou informaci.[93]

Právní rámec stalkingu

V lednu 2010 začal v České republice platit nový trestní zákoník č.[94] 40/2009 Sb.[95], ve kterém je nově zařazeno mezi trestné činy nebezpečné pronásledování (stalking) pod ustanovením § 354. Pro oběti stalkingu se tak objevila možnost právní ochrany. Začaly se ale vyskytovat případy, kdy nemohl být trestný čin kvalifikován jako stalking, jelikož nebylo přesně stanoveno časové hledisko, tj. doba, po kterou musí pronásledování trvat, aby bylo možné § 354 uplatnit. Ministerstvo vnitra a ministerstvo spravedlnosti se tedy vzájemně dohodla a minimální doba pro dlouhodobé pronásledování byla stanovena na dobu nejméně 1 měsíce.[96]

Příklady stalkingu a kyberstalkingu v České republice

Drenk versus Sklenkovi

V roce 2007 začalo manželům Sklenkovým přicházet několikrát denně velké množství SMS zpráv a urážlivých e-mailů od Christopha Drenka. Jen e-mailů jim přišlo přes tisíc tři sta za rok. Obsahem těchto obtěžujících zpráv byly velice nevybíravé urážky. Sklenka se proto několikrát obrátil kvůli Drenkově obtěžování na policii, aby mu pomohla, ta ovšem nijak

[93] FRYDECKÁ, L. Nebezpečné pronásledování. *Bílý kruh bezpečí* [online]. [cit. 2011-08-11]. Dostupné z WWW: <http://www.bkb.cz/pomoc-obetem/trestne-ciny/nebezpecne-pronasledovani/>.
[94] č. – číslo (dále jen „č.“).
[95] Sb. – sbírka zákonů (dále jen „Sb.“).
[96] KOPECKÝ, K. Stalking a kyberstalking : Nebezpečné pronásledování. *E-Nebezpečí* [online]. Olomouc : Net University, 2010. 14 s. [cit. 2011-07-29]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu>.
ISBN 978-80-254-7737-3.

nereagovala. Psychologové později označili Drenkovo chování za chování odpovídající profilu stalkera.

Sám Drenk na tohle označení reagoval pouhým úsměvem a později své chování obhajoval oprávněným bojem o svého syna, který zůstal s jeho expartnerkou a kterého ona nyní vychovává se Sklenkou. Obtěžovaní Sklenkovi však shledávali příčinu Drenkova chování v něčem jiném. Hlavní pohnutkou Drenka podle nich byla snaha pomstít se bývalé přítelkyni za to, že jej opustila a založila si novou rodinu.

Cílem Drenkových útoků se stalo také podnikání pana Sklenky, kdy obesílal jeho obchodní partnery dopisy, v nichž podnikatele pomlouval. Jeho záměrem bylo, jak sám uvedl, zničit Sklenkovi mnohamiliónové podnikání v realitách. Jedna z nadnárodních firem spolupracujících s panem Sklenkou se v Německu obrátila na soud se žádostí o vydání předběžného opatření, aby Drenk přestal hanět firmu a znevažovat její spolupráci se Sklenkou. Žádosti soud vyhověl, předběžné opatření vydal, a za jeho porušení hrozila Drenkovi pokuta v přepočtu okolo šesti miliónů korun. Podobný postup chtěl Sklenka uplatnit i v České Republice. Podařilo se mu sice rovněž dosáhnout vydání předběžného opatření, které nařizovalo Drenkovi okamžitě ukončit jednostrannou korespondenci, ale problém byl v tom, že za porušení tohoto opatření Drenkovi nehrozily žádné sankce, takže ten v Česku klidně rozesílal své urážlivé zprávy i nadále.

Drenkovo obtěžování se nakonec zvrhlo až v poškození majetku a zdraví Sklenky. Jednoho dne totiž Drenk při sledování automobilu, v němž jel jeho syn, vjel do vrat hospodářské budovy Sklenkových, a přitom zranil Sklenku stojícího v blízkosti vrat. Případem se začala zabývat policie a začala jej vyšetřovat jako pokus o ublížení na zdraví, poškozování cizí věci a porušování domovní svobody. Soud posléze rozhodl v neprospěch Drenka a odsoudil jej k tříleté podmínce. Drenk se odvolal, ale s odvoláním neuspěl.

Jak uváděl Sklenka, Drenk si z rozsudku nic nedělal. Neustále se ve svých SMS zprávách vysmíval Sklenkovým a také české justici, pro její pomalost a bezzubost. Podle slov Sklenky česká policie a soudy nedokáží obětem stalkingu účinně pomoci. Obdobné případy jsou pro ně nevděčné, zdlouhavě se vyšetřují, špatně dokazují, a pokud stalkeři svou oběť nezraní, pak se počet odsouzených pachatelů rovná nule. Podobné zkušenosti s řešením stalkingu jako rodina Sklenkových mělo více obětí v České Republice. Je otázkou, do jaké míry to bylo zaviněno jen v té době platným Trestním zákonem č.140/1961 Sb.[97]

[97] HLOUŠKOVÁ, L. Stalker aneb Někdo vás chce uštvat. *Reflecta* [online]. 2010. [cit. 2011-09-20]. Dostupné z WWW: < http://www.reflecta.cz/data/dn/000000322_dn.pdf>.

Petr Hanuš

Charakteristice sadistického pronásledovatele přesně odpovídal dvaatřicetiletý Petr Hanuš. Ten byl odsouzen na patnáct let vězení za vraždu o rok starší Michaely Maličké. Oba se znali z ruzyňského letiště, kde pracovali. Hanuš do zaměstnání na letišti nastoupil v roce 2005 a jeho nová kolegyně Maličká se mu snažila pomoci zapojit do kolektivu. Její snahu si ale Hanuš vyložil jako milostné nadbíhání. Po odmítnutí Hanuše Maličkou následoval od pozdějšího vraha její dvouletý teror. Hanuš oběti psal výhrůžné e-maily, SMS zprávy, špehoval ji a fyzicky napadal. Později oběti zničil i osobní automobil. Za tyto útoky dostal u Obvodního soudu v Praze nejdříve 250 hodin veřejně prospěšných prací a poté 125 dní vězení. Maličká opakovaně na agresora upozorňovala policii, žádala ji o pomoc a svůj příběh dokonce zveřejnila, bohužel všechno bylo marné. Hanuš ji nakonec ubil čtyřkilovou větví před vchodem do domu, kde bydlela a její matka byla tou, která ji našla mrtvou. Mimo odpykání si trestu vězení vznikla Hanušovi ještě povinnost zaplatit matce zavražděné Michaely 280 tisíc korun jako odškodnění za smrt její dcery.[98]

2.5 Phishing

Phishing se do českého jazyka překládá jako rybaření, rybolov nebo tzv. „rhybaření“. Útočníci při phishingu „rozhodí“ pomyslnou síť a čekají, kdo se do ní chytí. Nastraženou návnadou se v případech phishingu obvykle stává podvodný e-mail, rozeslaný pomocí internetu. James[99] definuje phishing *„jako činnost, kdy je uživateli zaslán padělaný e-mail, který se klamavým způsobem staví do pozice, že byl odeslán skutečnou finanční institucí ve snaze oklamat příjemce e-mailu tak, aby sdělil své soukromé informace typu čísla platební karty nebo bankovního účtu.“*

Příkladem mohou být podvodné e-maily obsahující text, ve kterém je adresátům sděleno, že si z důvodu zvýšení bezpečnosti musí změnit přihlašovací údaje ke svému bankovnímu účtu. Velice důležitou součástí takových e-mailu je přiložený odkaz, který jim má tuto akci umožnit. Jestliže uživatelé informacím uvedeným v e-mailu uvěří a na nastražený odkaz kliknou, jsou okamžitě přesměrováni na podvrženou stránku, kde je po nich požadováno, aby dosavadní přihlašovací údaje změnili. Vyplněním

[98] HLOUŠKOVÁ, L. Stalker aneb Někdo vás chce uštvat. *Reflecta* [online]. 2010. [cit. 2011-09-20]. Dostupné z WWW: < http://www.reflecta.cz/data/dn/000000322_dn.pdf>.
[99] JAMES, L. *Phishing bez záhad.* 1. vyd. Praha : Grada, 2007. 282 s. ISBN 80-247-1766-2. s. 40.

přihlašovacích údajů na takto podvržených stránkách však oběti nevědomky pachatelům poskytnou informace, které útočníci potřebují k tomu, aby mohli jakkoliv nakládat s jejich bankovními účty.[100]

V případech phishingu se pachatelé spoléhají na to, že „uloví“ jedince, který jejich podvodu uvěří, a z kterého prostřednictvím nastražené pasti vylákají požadované informace. Z této skutečnosti vyplývá, že jednou z účinných možností, jak se těmto útokům ubránit, je vždy pečlivě zvažovat každou situaci, kdy je po uživateli požadováno, aby sdělil jakékoliv citlivé údaje, které mohou být zneužity.

2.6 Hoax

Anglické slovo hoax [:houks:] označuje smyšlenku, falešnou zprávu, mystifikaci, novinářskou kachnu, podvod, poplašnou zprávu, výmysl, žert. V počítačovém světě je slovem hoax nejčastěji označována poplašná zpráva varující před neexistujícím nebezpečným virem. Za hoax je možné rovněž považovat šířenou zprávu obsahující nepřesné, zkreslující informace, účelově upravené polopravdy nebo směs polopravd a lží. Ve většině případů se autor zprávy snaží příjemce přesvědčit, že varování přišlo z důvěryhodných zdrojů. Typickou součástí hoaxu bývá text, ve kterém je adresát z různých důvodů nabádán, aby předal obdržený hoax dalším lidem.[101]

Typy hoaxů

Dle informací zveřejněných na serveru hoax.cz mohou mít klasické typy hoaxů několik možných podob. První z nich je například *varování před smyšlenými viry a různými útoky na počítač.* V tomto případě se jedná o nejčastější typ poplašných e-mailů, ve kterých je zpravidla smyšlené nebezpečí stručně popsáno a někdy může být přiložen i nesmyslný návod, jak se před ním chránit. Dalším typem hoaxu může být *popis jiného nereálného nebezpečí,* kdy jde o zprávy varující před smyšleným nebezpečím hrozícím v reálném světě, a které se dotýkají různých oblastí lidského života, nebo *falešná prosba o pomoc* formou smyšlených příběhů o lidech, kteří potřebují pomoc. Jedná se například o zprávy, kdy je adresát informován o srdcervoucích příbězích lidí, kteří urgentně potřebují kostní dřeň,

[100] JIROVSKÝ, V. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha : Grada, 2007. 288 s. ISBN 978-80-247-1561-2.
[101] Co je to hoax. *Hoax* [online]. 2011. [cit. 2011-09-23]. Dostupné z WWW: < http://www.hoax.cz/hoax/co-je-to-hoax>.

krev nebo něco jiného, co je může zachránit před smrtí. Mezi těmito falešnými prosbami může bohužel zaniknout i prosba skutečná. Jako hoax se objevuje také *fáma o mobilních telefonech*, což jsou nepravdivé informace o vlastnostech mobilních telefonů (například o jejich vysokém vyzařování, pomocí kterého je možné uvařit vejce), a *řetězový dopis štěstí*, který může mít podobu dopisu nebo e-mailu a může příjemce přesvědčovat například o tom, že pouhé tzv. nepřerušení řetězu a přeposlání obdrženého dopisu štěstí dalším lidem jim přinese štěstí, lásku, peníze apod. Kromě uvedených možností může hoax vypadat jako petice, výzva, žertovná zpráva, nabídka snadného výdělku apod.[102]

Škodlivost hoaxů

I když by se mohlo zdát, že hoaxy nejsou příliš nebezpečné, není tomu tak. Podle serveru e-bezpečí.cz se škodlivost hoaxů projevuje například v *obtěžování příjemců* (hoaxy masově šířené pomocí e-mailů mohou uživatelům zaplňovat e-mailové schránky), v *nebezpečných radách* (hoaxy někdy obsahují návody a rady, které mohou vést k poškození zdraví a majetku důvěřivého adresáta), ve *zbytečném zatěžováním linek a serverů* (k nadbytečnému zatěžování může docházet v případech, kdy se hoaxy díky přeposlání od uživatele k uživateli masově šíří internetem, a to ve statisícových kopiích po celém světě), ve *ztrátě důvěryhodnosti odesílatele* (odesílatel může ohrozit nejen svoji důvěryhodnost, ale i důvěryhodnost firmy, ve které pracuje. Obzvláště pokud takové zprávy odesílá z pracovního e-mailu zaměstnanec firmy, která se zabývá výpočetní technikou nebo programováním), v *prozrazení důvěrných informací* (jedná se například o případy, kdy uživatel přepošle hoax na mnoho dalších adres a přitom nechá adresy všech předchozích příjemců v odesílané zprávě), v *přetěžování konkrétní cílové e-mailové schránky* (k přetěžování dochází v případech, kdy autor zprávy použije odkaz na e-mail osoby, kterou chce poškodit. Například tím, že ve zprávě uvede: „Chcete pomoci postižené dívce? Pošlete co nejvíce e-mailů na tento e-mail. Za každý e-mail dostane postižená dívka peněžní částku ve výši 5,- Kč.“ Pokud zpráva vyvolá vlnu solidarity důvěřivých lidí, pak je uvedená e-mailová schránka zahlcována „dárcovskými“ e-maily a stává se pro jejího majitele prakticky nepoužitelnou.) nebo v *poškozování konkrétní instituce* (uváděním nepravdivých

[102] Co je to hoax. *Hoax* [online]. 2011. [cit. 2011-09-23]. Dostupné z WWW: <http://www.hoax.cz/hoax/co-je-to-hoax>.

zpráv o nich. Příkladem může být zveřejnění nepravdivé informace o zdravotní závadnosti výrobku konkrétní společnosti).[103]

Omezení šíření hoaxu

Pokud přijatá zpráva obsahuje výzvu k hromadnému rozesílání na další adresy, může jít o hoax. V takových případech je dobré nejprve se přesvědčit, zda se podobná nebo stejná zpráva nevyskytuje v seznamu hoaxů na některém ze serverů zabývajících se danou problematikou. Na českém internetu lze využít zejména stránky serveru www.hoax.cz, kde se nachází obsáhlý seznam hoaxů včetně komentářů zdůvodňujících proč se v tom kterém případě jedná o hoax. Jestliže obdržená zpráva v seznamu hoaxů figuruje, pak k omezení šíření postačí, když uživatel zprávu smaže bez toho, aby ji rozeslal dále.[104]

Příklad hoaxu

„ Důležitá zpráva, pošli ji dál !!!

Po jaderném výbuchu v neděli a dalších dvou ve Fukushime v Japonsku, musíme být všichni opatrní. Pokud bude dnes nebo v příštích dnech pršet, NEVYCHÁZEJTE DO DEŠTĚ!! Pokud ano, musíte použít deštník nebo pláštěnku, i když jen mrholí. To proto, že nukleární odborníci poukazují na to, že radioaktivní částice mohou vstoupit do atmosféry, a tak se z ozonové vrstvy rozšíří do celého světa deštěm, který může způsobit popáleniny, vypadávání vlasů a dokonce i rakovinu. Prosím, předejte dál tuto informaci! Jaderné varování je už na stupni 6 ze 7 v Japonsku, ve Francii 6 ze 7 kvůli pohybu větrů, Německo a Rusko vyhlásili stupeň 5 ze 7. Nemažte tuto zprávu, je to reálná hrozba, o které se můžete více informovat ve vysílání CNN, NHW, BBC, 24H international či TVE.“

[103] Co je hoax. *E-Bezpeci* [online]. 18.5.2008. [cit. 2011-09-23]. Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/25/40/lang,czech/>.
[104] DOSEDĚL, T. *21 základních pravidel počítačové bezpečnosti*. 1. vyd. Brno : CP Books, 2005. 50 s. ISBN 80-251-0574-1.

3 KYBERGROOMING

Během několika posledních let došlo v oblasti ICT k prudkému rozvoji. S tímto rozvojem bylo spojeno jejich masové šíření do všech oblastí lidského života. Počítače, mobilní telefony, připojení k internetu a další vymoženosti, dříve dostupné jen úzké skupině lidí, se postupně stávaly obvyklou součástí každodenního života široké veřejnosti. Stejně jako dříve, tak i v dnešní době si bohužel málokdo uvědomuje, že používání těchto moderních technických vymožeností s sebou přináší i nová nebezpečí, mezi které můžeme zařadit i kybergrooming.

Slovo **grooming** se do českého jazyka překládá jako krášlení, vábení, vylepšování se. V souvislosti s negativní činností bývá uvedený pojem často spojen s dalším atributem a objevuje se např. jako chat grooming, child grooming, cyber grooming (česky kybergrooming) apod.[105]

Pojem **kybergrooming** označuje jednu z nejnebezpečnějších komunikačních aktivit spojených s využíváním moderních komunikačních technologií. Označuje se tak chování útočníka z kyberprostoru, snažícího se úmyslně vyvolat u vytipované oběti pocit důvěry ve svou osobu a přimět ji k osobnímu setkání. Vysoká nebezpečnost kybergroomingu spočívá právě v tom, že se kontakt kybergroomera s obětí po určité době přesouvá z prostředí virtuálního do prostředí reálného. Během osobního setkání v reálném prostředí pak může být oběť útočníkem například sexuálně zneužita, fyzicky napadena, zneužita k prostituci nebo jakkoliv jinak ohrožena.[106]

Pro kybergrooming je charakteristické, že psychická manipulace oběti kybergroomerem před jejich osobním setkáním trvá obvykle několik měsíců, nezřídka i let. Délka manipulace závisí na způsobu manipulace a na tom, jak moc je oběť důvěřivá.

3.1 Výskyt kybergroomingu a jeho pachatelé

Kybergrooming je negativní jev, jehož existence je přímo svázána se sociální komunikací probíhající v rámci počítačové sítě zvané Internet. Z mnoha celosvětových výzkumů vyplývá, že nejčastějšími místy, kde se děti mohou setkat s útoky kybergroomerů

[105] KOPECKÝ, K. *Moderní trendy v e-komunikaci*. 1. vyd. Olomouc : Hanex, 2007. 98 s. ISBN 978-80-8578-378-0.
[106] KOPECKÝ, K.; KREJČÍ, V. Rizika virtuální komunikace. *Net University* [online]. 2010. [cit. 2011-09-26]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=10%3Abrozura>. ISBN 978-80-254-7866-0.

jsou instant messengery[107], sociální sítě, veřejné chaty a internetové seznamky. Velikou oblibu mezi kybergroomery v poslední době získaly zejména sociální sítě. Díky povaze informací, které na nich děti zveřejňují, je kybergroomeři začali používat jako adresáře svých budoucích obětí.[108]

Kromě výše uvedených lokalit kybergroomeři s oblibou směřují své aktivity i na internetové portály, které dětem „něco zajímavého" nabízí, například možnost uplatnění v reklamě, možnost finančního zisku a další lákavé příležitosti. Nezřídka kybergroomeři útočí i na portálech vytvořených přímo pro nezletilé děti. Jde například o portály zaměřené na hraní dětských on-line her, stahování hudby, sledování filmů a na další volnočasové aktivity dětí.[109]

Nezbytným předpokladem pro páchání kybergroomingu je to, aby útočník uměl komunikovat pomocí moderních komunikačních technologií. V tomto směru lze kybergroomery obvykle považovat za jedince velice zdatné, jejichž schopnosti využívat moderní komunikační technologie nezřídka převyšují schopnosti samotných obětí, jejich rodičů, učitelů a dalších osob, které o děti pečují.[110]

Podle studie Choo[111] kybergroomeři tvoří heterogenní skupinu, ve které je možné nalézt jedince s nízkým i vysokým sociálním statutem. V souvislosti s novými případy kybergroomingu se mezi útočníky zařadili i zástupci profesí považovaných za skutečné pilíře společnosti, protože šlo například o učitele, policisty a právníky. Výsledky uvedené ve jmenované studii zároveň s tímto poukázaly na skutečnost, že v 85 – 95 % případů oběť pachatele znala a byla na něm závislá. V mnoha případech byl za pachatele útoku označen známý rodiny oběti. Dle výzkumů byly pachateli kybergroomingu ve většině případů osoby, které do té doby nebyly trestány, a v menším počtu případů se kybergroomery stávali i ti, kteří již v minulosti byli za sexuální útoky proti dětem a mladistvým odsouzeni, a u kterých

[107] instant messenger – program umožňující komunikaci mezi uživateli po síti v reálném čase, např. ICQ apod.
[108] WOLAK, J.; FINKELHOR, D.; MITCHELL, K. Online "Predators" and Their Victims. *University of New Hampshire* [online]. 2008. 18 s.
[cit. 2011-07-28]. Dostupné z WWW:<http://www.apa.org/pubs/journals/releases/amp-632111.pdf>.
[109] KOPECKÝ, K. Kybergrooming nebezpečí kyberprostoru. *Net Univers*ity [online]. 2010. [cit. 2011-09-26]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie>. ISBN 978-80-254-7573-7.
[110] PUTT, J. Responding to online child sexual grooming : an industry perspective. *Australian Institute of Criminology* [online]. 2009. [cit. 2011-07-29]. Dostupné z WWW:
<http://www.aic.gov.au/en/publications/current%20series/tandi/361-380/tandi379/view%20paper.aspx>.
[111] CHOO, K. R. Online child grooming : a literature review on the misuse of social networking sites for grooming children for sexual offences. *Australian Institute of Criminology* [online]. 2009. [cit. 2011-07-29]. Dostupné z WWW: <http://www.aic.gov.au/documents/3/C/1/%7B3C162CF7-94B1-4203-8C57-79F827168DD8%7Drpp103.pdf>. ISBN 978-1-921532-33-7.

tím pádem došlo k recidivě. U většiny jedinců dopouštějících se kybergroomingu byl prokázán patologický zájem o děti.[112]

3.2 Oběti kybergroomingu

Obětí kybergroomingu se může stát v podstatě jakékoliv dítě, které je schopno samostatně komunikovat s ostatními osobami pomocí počítače připojeného k internetu. Co se týče pohlaví, jsou častějšími oběťmi dívky než chlapci. Mezi dívkami jde zejména o ty ve věku 13 - 17 let.[113]

Jak uvádí Kopecký a Krejčí[114] ve své příručce pro děti a učitele, jsou většímu riziku útoku kybergroomera vystaveni především ti jedinci, kteří tráví velkou část svého volného času na internetu. Zmíněné riziko útoku se pak zvyšuje zejména u těch dětí, které pomocí internetu navazují kontakty s ostatními uživateli například pomocí internetových seznamek, chatů, instant messengerů a podobných komunikačních prostředků. Během několika posledních let se ve stále větší míře objevují případy útoků kybergroomerů, ke kterým došlo na sociálních sítích. Sociální sítě totiž díky propracovanému systému virtuálních sociálních vazeb poskytují ideální podmínky pro jejich aktivity. Kybergroomeři nejčastěji zaměřují své útoky na děti, u kterých předpokládají vyšší míru své úspěšnosti v jejich manipulaci. Zde jsou uvedeny ty nejohroženější skupiny dětí:

- *Děti s nízkou sebeúctou, sebevědomím a nedostatkem sebedůvěry* – děti spadající do této skupiny lze snadněji citově a fyzicky izolovat.
- *Děti s emocionálními problémy, zanedbávané a oběti v nouzi* – děti, které se trápí, často hledají náhradu za své rodiče a potřebují pomocnou ruku.
- *Děti naivní* – tyto děti jsou často ochotnější zapojovat se do online konverzace s neznámými lidmi a obtížně rozpoznávají rizikovou komunikaci.

[112] KOPECKÝ, K. Kybergrooming nebezpečí kyberprostoru. *Net Univers*ity [online]. 2010. [cit. 2011-09-26]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie>. ISBN 978-80-254-7573-7.

[113] CHOO, K. R. Online child grooming : a literature review on the misuse of social networking sites for grooming children for sexual offences. *Australian Institute of Criminology* [online]. 2009. [cit. 2011-07-29]. Dostupné z WWW: <http://www.aic.gov.au/documents/3/C/1/%7B3C162CF7-94B1-4203-8C57-79F827168DD8%7Drpp103.pdf>. ISBN 978-1-921532-33-7.

[114] KOPECKÝ, K.; KREJČÍ, V. Rizika virtuální komunikace. *Net University* [online]. 2010. [cit. 2011-09-26]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=10%3Abrozura>. ISBN 978-80-254-7866-0.

- *Adolescenti/teenageři* – jedince v této věkové skupině obvykle zajímá lidská sexualita a jsou ochotni o ní hovořit.[115]

Výše uvedené charakteristiky nejčastějších obětí ukazují, že obrovskou výhodou kybergroomerů je **dětská sugestibilita**[116]**,** a tedy zejména ta skutečnost, že děti jsou více ovlivnitelné a manipulovatelné než dospělí. Na internetu se děti často chovají naivně a důvěřivě a tato kombinace vlastností následně přispívá k tomu, aby se staly snadnou kořistí útočníka.[117]

3.3 Etapy manipulace dítěte

Celý proces manipulace kybergroomera s obětí probíhá v několika etapách. V různých materiálech zabývajících se kybergroomingem je často uváděn rozdílný počet etap i jejich pojmenování. Tyto rozdíly však vznikají jen díky tomu, že každý autor více či méně podrobně popisuje to, k čemu v jednotlivých etapách kybergroomingu dochází.

Příklady dělení jednotlivých etap kybergroomingu uváděné různými autory:

Například Kopecký[118] uvádí jednotlivé etapy jako:

1. příprava kontaktu
2. kontakt s obětí
3. příprava na osobní schůzku
4. osobní schůzka

[115] CHOO, K. R. Online child grooming : a literature review on the misuse of social networking sites for grooming children for sexual offences. *Australian Institute of Criminology* [online]. 2009. [cit. 2011-07-29]. Dostupné z WWW: <http://www.aic.gov.au/documents/3/C/1/%7B3C162CF7-94B1-4203-8C57-79F827168DD8%7Drpp103.pdf>. ISBN 978-1-921532-33-7.
[116] sugestibilita – ovlivnitelnost.
[117] BERSON, I. Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth. *University of South Florida* [online]. 2002. [cit. 2011-07-29]. Dostupné z WWW: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.104.6160&rep=rep1&type=pdf>.
[118] KOPECKÝ, K. Kybergrooming nebezpečí kyberprostoru. *Net Univers*ity [online]. 2010. [cit. 2011-09-26]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie>. ISBN 978-80-254-7573-7.

Oproti tomu jednotlivé etapy kybergroomingu zveřejněné na stránkách Policie České republiky[119] jsou rozděleny na:

1. Vzbuzení důvěry a snaha izolovat oběť od okolí (osoba mění svoji identitu, je velmi trpělivá)
2. Podplácení dárky či různými službami, budování kamarádského vztahu
3. Vyvolání emoční závislosti oběti na osobě útočníka
4. Osobní setkání
5. Sexuální obtěžování, zneužití dítěte

Na stránkách Nebuď oběť[120] jsou jednotlivé etapy rozdělené takto:

1. Vzbuzení důvěry a snaha izolovat oběť od okolí.
2. Podplácení dárky, penězi, budování přátelského vztahu.
3. Získání nebezpečných materiálů k vydírání.
4. Emocionální závislost na útočníkovi.
5. Osobní schůzka.
6. Zneužití, napadení.

3.4 Popis jednotlivých etap kybergroomingu

Jak již bylo řečeno, kybergrooming je charakteristický tím, že probíhá v několika etapách. Během těchto jednotlivých etap útočník pomocí různých metod a postupů dosahuje dílčích cílů, které mu umožní dosáhnout hlavního cíle, kterým je osobní setkání s obětí. Některé z metod a postupů uplatňovaných během kybergroomingu nemusí být vázány jen na konkrétní etapu, ale mohou být použity i ve více etapách a to opakovaně. Například uplácení oběti může kybergroomer využít pro získávání informací o oběti ve chvíli, kdy si vytváří její profil, i v okamžiku osobního setkání, kdy uplácení využije k tomu, aby u dítěte zvýšil svoji důvěryhodnost. V následujícím textu jsou popsány jednotlivé etapy kybergroomingu.

[119] BURÝŠKOVÁ, L. Víte co je KYBERŠIKANA? *Policie České republiky* [online]. 2009. [cit. 2011-06-18]. Dostupný z WWW: <http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx>.
[120] Co je to kybergrooming? *Nebuď oběť* [online]. 2009. [cit. 2011-07-27]. Dostupné z WWW: <http://www.nebudobet.cz/?page=kybergrooming>.

3.4.1 První etapa – Příprava podmínek pro zahájení kontaktu s obětí

V první etapě se útočník připravuje na provedení útoku a vytváří si podmínky pro realizaci manipulace oběti.

a) Zajištění technických podmínek

Jednou ze základních podmínek, kterou musí kybergroomer splnit k tomu, aby mohl zahájit svůj útok, je zajistit si přístup na internet. Toho může dosáhnout následujícími způsoby. Pořízením vlastního technického vybavení a připojení k internetu, pořízením vlastního technického vybavení a využitím internetového připojení někoho jiného, a to buď legálně, například pomocí veřejně přístupných bezdrátových sítí, nebo nelegálně, například zneužitím mezery v zabezpečení u cizí bezdrátové sítě. Dalším způsobem je využití technického vybavení a internetového připojení veřejných poskytovatelů internetu v internetových kavárnách, veřejných knihovnách apod., nebo zneužitím počítače připojeného k internetu v zaměstnání, a mnohými dalšími způsoby.

Volba toho, odkud a jak se kybergroomer při komunikaci s obětí do sítě internet připojí, může do značné míry ovlivnit i to jak snadné, nebo naopak obtížné bude jeho následné vypátrání a dopadení policií. Například pokud méně zkušený útočník využije na sebe registrované připojení z domova nebo se připojí pomocí svého počítače v zaměstnání, pak bude snadněji dopadnutelný než kybergroomer, který se bude aktivně snažit o znesnadnění své identifikace v síti internet, například tím, že zneužije pro připojení k internetu nezabezpečenou bezdrátovou síť někoho jiného nebo se připojí do internetu pomocí veřejně přístupné bezdrátové sítě, a to pokaždé z jiného místa. Vedoucí Odboru pro potírání informační kriminality Policejního prezidia ČR plukovník Karel Kuchařík v článku Musálkové[121] k tomuto tématu uvádí: *„Někteří pachatelé nejsou vybaveni technickými znalostmi a myslí si, že internet je anonymní prostředí, což ale není pravda. Ty chytíme celkem snadno. Na druhou stranu existuje i velká skupina, která s tím počítá a velice dobře ví, jak za sebou zamést stopy.“*

[121] MUSÁLKOVÁ, Z. Jste na Facebooku? Internetové zločince zajímáte! *Magazín deníku Právo č. 28*. 16.7.2011. [cit. 2011-07-25]. ISSN 1211-2119. s. 10.

b) Vytvoření identity

Dalším velice důležitým krokem v přípravě kybergroomera je vytvoření identity, pod kterou bude při komunikaci s potencionální obětí vystupovat.

Falešná identita slouží útočníkovi k tomu, aby se při komunikaci s obětí vydával za někoho jiného, než kým ve skutečnosti je. Vytváření falešné identity je často pozorovaným postupem, kterým si útočníci snaží usnadnit prvotní navázání a následné rozvíjení kontaktu s vytipovanou obětí. Kybergroomeři při tvorbě falešné identity záměrně pozměňují informace o svém jméně, příjmení, věku a pohlaví. Pravdivost takto pozměněných údajů se často snaží podpořit podvrženou fotografií jedince, který nepravdivě uvedeným údajům odpovídá. Nekonečným zdrojem fotografií sloužících kybergroomerovi k podvržení mohou být například soukromé fotografie vystavené na některé ze sociálních sítí.[122]

Falešná identita se může vyskytovat v následujících dvou formách. *Statická identita* – pro komunikaci si kybergroomer vytvoří jednu identitu, prostřednictvím které oslovuje vybrané oběti. Příkladem statické identity může být uživatelský profil či účet na sociální síti Facebook[123], Twitter apod.[124] *Dynamická identita* - útočník svoji identitu mění a upravuje podle momentální potřeby. Podle nastalé situace pak vystupuje pod různými jmény a přezdívkami. Na základě aktuální potřeby si dodatečně upravuje věk, pohlaví, zájmy, záliby a další údaje, které mu mohou pomoci efektivněji komunikovat s potencionální obětí. Nezřídka útočník s dynamickou identitou komunikuje s více oběťmi najednou, a proto je pro něj velice důležité, aby si pamatoval nebo pečlivě evidoval to, co komu sdělil. To je důvodem, proč je udržení dynamické identity složitější než udržení identity statické. Jestliže si například kybergroomer nechtíc zamění oběť, s kterou právě komunikuje, za jinou ze svých obětí a dotyčná osoba rozpory ve virtuální komunikaci zaznamená (např. útočník opakovaně uvede rozdílný věk, jméno, bydliště nebo jiné údaje), může to pro ni být jasným signálem, že komunikuje s někým, kdo neříká pravdu a kontakt s kybergroomerem ukončí.[125]

---

[122] KOPECKÝ, K. Kybergrooming nebezpečí kyberprostoru. *Net Univers*ity [online]. 2010. [cit. 2011-09-26]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie>. ISBN 978-80-254-7573-7.

[123] Facebook – jedna ze sociálních sítí.

[124] KOPECKÝ, K. Nebezpečí zvané kybergrooming II – metody manipulace. *Metodický portál* [online]. 30.11.2010. [cit. 2011-07-27]. Dostupné z WWW: <http://clanky.rvp.cz/clanek/c/Z/9985/nebezpeci-zvane-kybergrooming-ii-metody-manipulace.html/>.

[125] KOPECKÝ, K. Kybergrooming nebezpečí kyberprostoru. *Net Univers*ity [online]. 2010. [cit. 2011-09-26]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie>. ISBN 978-80-254-7573-7.

Falešná autorita představuje formu falešné identity. V tomto případě však kybergroomeři navenek nevystupují jako fyzické osoby, ale jako představitelé různých fiktivních firem (manažeři, jednatelé, ředitelé), kteří mají přinést vytipovaným obětem (dětem) nějaký užitek. Útočníci tak chtějí pomocí vytvořené falešné autority zvýšit svoji důvěryhodnost u těch, které oslovují.[126]

Využití falešné autority pak může v praxi probíhat například tak, že kybergroomer vydá pod hlavičkou fiktivní firmy (falešné autority) inzerát, který bude určen dětem a bude navenek vypadat jako neškodná anketa s možností výhry. V té osloveným dětem nabídne za pouhé vyplnění banálního dotazníku nebo zodpovězení jednoduchých soutěžních otázek nějakou lákavou odměnu, například mobilní telefon, MP3[127] přehrávač nebo počítač. Nalákanému dítěti pak v rámci ankety předloží registrační formulář, ve kterém ho požádá o vyplnění kontaktních údajů (jména, příjmení, adresy bydliště, e-mailu, čísla mobilního telefonu apod.), u kterých záměrně uvede, že budou sloužit jako pouhý podklad pro doručení slibované odměny. Kybergroomer samozřejmě dítě během vyplňování kontaktních údajů nezapomene zřetelným způsobem upozornit na to, že v případě uvedení neúplných nebo nesprávných údajů mu nebude možné slibovanou odměnu doručit. Tím zpravidla dosáhne toho, že děti vyplní požadované registrační údaje pravdivě, aby slibovanou odměnu dostaly. Uvedeným způsobem tak kybergroomer získá od dětí důvěrné informace, pomocí kterých může pokračovat ve svém útoku.

3.4.2 Druhá etapa – První kontakt s obětí, navázání a prohlubování vztahu a snaha o její izolaci

Během druhé etapy kybergroomer navazuje kontakt s obětí a poté pokračuje v budování a prohlubování takto vytvořeného virtuálního vztahu. V této etapě začíná kybergroomer účelně manipulovat s obětí. Někteří z odborníků na kybergrooming uvádí, že se v procesu manipulace a komunikace s obětí jedná o etapu klíčovou.[128]

[126] KOPECKÝ, K. Kybergrooming nebezpečí kyberprostoru. *Net Univers*ity [online]. 2010. [cit. 2011-09-26]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie>. ISBN 978-80-254-7573-7.
[127] MP3 – formát audio komprese.
[128] KOPECKÝ, K. Nebezpečí zvané kybergrooming II – metody manipulace. *Metodický portál* [online]. 30.11.2010. [cit. 2011-07-27]. Dostupné z WWW: <http://clanky.rvp.cz/clanek/c/Z/9985/nebezpeci-zvane-kybergrooming-ii-metody-manipulace.html/>.

První kontakt s obětí

Při prvním kontaktu s obětí kybergroomeři postupují velice opatrně, aby oslovené dítě nevyplašili. Během něj se snaží u oběti vyvolat pocit důvěry. Toho se pokouší dosáhnout například tím, že hned od prvního navázání komunikace projevují zájem o stejná témata jako jejich oběť. Témata, o kterých budou při prvním kontaktu s obětí hovořit, volí útočníci na základě předem získaných informací o oběti (např. jejím profilováním) nebo podle toho, o čem dítě na internetu „mluví“ ve chvíli, kdy se kybergroomer rozhodne zaútočit.

Využití Mirroringu (zrcadlení) při prvním kontaktu

Často pozorovaným postupem útočníků při prvním kontaktu s obětí je takzvaný mirroring (zrcadlení). Jde o metodu, pomocí které se útočník snaží vytvořit iluzi přátelství a prolomit komunikační bariéry při svém kontaktu s dítětem. Tento postup je charakteristický tím, že útočníci svým chováním vytvářejí pomyslný zrcadlový odraz dítěte. Chování kybergroomera při mirroringu může vypadat například tak, že ve chvíli, kdy dítě kybergroomerovi sdělí, jak se cítí osaměle, kybergroomer na tuto informaci zareaguje odpovědí, že i on se cítí osaměle a následně nabídne dítěti přátelství, aby se oba pocitu osamění zbavili.[129]

Prohlubování vztahu uplácením a získávání informací

Další metodou užívanou k posílení a prohloubení nově navázaného vztahu s obětí je její uplácení. K uplácení obvykle útočník využívá různé dárky, které dítěti posílá. Tyto pozornosti mají většinou formu různě vysokých peněžních částek, kreditů do mobilních telefonů, spotřební elektroniky, značkového oblečení a jiných pro děti zajímavých věcí.

Odesláním uvedených dárků může kybergroomer sledovat ještě další cíle, například jejich pomocí si může ověřovat dříve získané informace o oběti (např. posláním dárků na dítětem uvedenou adresu si může ověřit platnost adresy). Jedním z dalších cílů může být i snaha posilovat svoji důvěryhodnost u oběti, se záměrem využít zvýšenou důvěru k její snazší psychické manipulaci, případně k zisku dalších informací a materiálů využitelných pro dotvoření jejího profilu nebo pro její případné vydírání. Dárky může rovněž využít jako úplatky pro získání dalších intimních materiálů od oběti.

[129] Methods of Predators. *Kids.yahoo* [online]. [cit. 20011-07-27]. Dostupné z WWW: <http://kids.yahoo.com/parents/online-safety/1706/4--Methods+of+Predators>.

Vytváření emoční závislosti dítěte na útočníkovi

Kybergroomer už od navázání prvního kontaktu s dítětem obvykle usiluje o vytvoření jeho emoční závislosti na své osobě. Proto s dítětem vždy ochotně a se zájmem probírá vše, co dítě zajímá nebo trápí. Aktivně dítěti nabízí pomoc hned ve chvíli, kdy mu řekne, že má nějaký problém nebo starost. Řeší s ním i problémy, na které nikdo z okolí dítěte neslyší nebo nemá čas. Tímto postupem se u dítěte snaží dosáhnout stavu, kdy bude na přátelství s kybergroomerem závislé a kybergroomera bude považovat za jediného kamaráda, na kterého se může kdykoliv obrátit, který na něj bude mít vždycky čas a na kterého se může kdykoliv spolehnout. Pokud tohoto stavu kybergroomer docílí, pak dítě zpravidla ztrácí všechny zábrany a začne s útočníkem probírat i své nejdůvěrnější záležitosti a tajemství, o kterých jinak nehovoří s nikým jiným. Díky své sdílnosti tak útočníkovi poskytuje další důvěrné informace.

Izolace oběti od okolí

Spolu se zvyšujícím se počtem důvěrných informací (tajemství), které útočník o oběti získá a zvětšující se mírou závislosti na vztahu, kterou u dítěte vybuduje, vzrůstá i jeho šance izolovat dítě od ostatních a možnost přinutit je, aby některé informace nesdělovalo nikomu jinému a neprozradilo, že s ním komunikuje. Útočník se snaží dítě izolovat především od jeho rodičů, přátel a všech dalších, kteří by mohli nějak narušit jeho plány, tím že jejich vztah odhalí a ukončí.

Jestliže začne mít kybergroomer podezření, že by se dítě mohlo chtít svěřovat i někomu jinému, čímž by ohrozilo vztah s kybergroomerem, začne jej obvykle citově vydírat, aby tomu zamezil.

Citově vydírat může například slovy:

- *„Neříkej to tatínkovi, nenáviděl by tě.“*
- *„Nikomu to neříkej, ostatní by to nepochopili.“*

Díky tomuto citovému vydírání, zůstane kybergroomer i nadále jediným „opravdovým kamarádem“ a dítě se i nadále svěřuje jen jemu.

Zamezení ukončení vztahu

V některých případech se oběť v průběhu komunikace rozhodne, že už v ní nechce nadále pokračovat. Ve chvíli, kdy kybergroomer zjistí, že by dítě chtělo jejich virtuální vztah ukončit, zpravidla zneužije důvěrné informace k vyhrožování a vydírání typu:

- *„Jestli se mi neozveš, tak na tebe řeknu.“*
- *„Jestli to uděláš, zveřejním o Tobě na internetu.“*
- *„Jestli se mnou přestaneš mluvit, řeknu tvým spolužákům.“*

I když si dítě v této situaci uvědomí, že to s ním jeho „kamarád“ nemyslí dobře, často v komunikaci pokračuje jen proto, aby útočník nevyplnil některou ze svých hrozeb. Tímto kybergroomer docílí toho, že může ve svých záměrech pokračovat.[130]

Zařazování sexuálních témat do konverzace

Během druhé etapy kybergroomingu může útočník začít stáčet hovory do oblasti sexu. Obvykle tak, že nejdříve pozvolna otevírá méně závadná témata a postupně v nich přitvrzuje. Například začne řešit běžné partnerské vztahy, posléze přejde k intimnostem v těchto vztazích, pak podle situace dítěti pošle materiály obsahující pornografii, hovoří s ním na toto téma a následně dítěti navrhne, že jej vyfotografuje v sexuálně svůdné poloze. Za tím, proč tak činí, je ukryta jeho snaha zvýšit u dítěte zájem o sexuální tématiku a snížit jeho stud z nahoty.[131]

Takto postupným odstraňováním studu kybergroomer záměrně zvyšuje své šance na úspěch v tom, že mu dítě vyhoví ve chvíli, kdy jej požádá, aby mu poslalo nějakou fotku na které je nahé nebo aby se mu ukázalo nahé přes webkameru.[132]

Zařazování sexuálních témat do konverzace je metodou umožňující kybergroomerovi získat intimní záběry dítěte, které může podle potřeby využít při jeho vydírání.[133]

---

[130] Kybergrooming. *E-Bezpeci* [online]. 13.9.2008. [cit. 2011-07-27]. Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/42/35/lang,czech/>.
[131] BERSON, I. Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth. *University of South Florida* [online]. 2002. [cit. 2011-07-29]. Dostupné z WWW: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.104.6160&rep=rep1&type=pdf>.
[132] webkamera - webová kamera – počítačové vstupní zařízení podobné fotoaparátu nebo kameře.
[133] Kybergrooming. *E-Bezpeci* [online]. 13.9.2008. [cit. 2011-07-27]. Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/42/35/lang,czech/>.

Vytváření profilu oběti

Obvyklou činností kybergroomerů je i to, že si vytvářejí profily svých obětí. Ve zmíněných profilech útočníci postupně shromažďují veškerá data, která o oběti zjistí (jméno, příjmení, věk, bydliště, apod.) a následně je dynamicky upravují na základě nově získaných informací.

Podkladem pro vytváření profilů většinou nejsou jen informace, které o sobě oběti útočníkovi sami sdělily, ale i informace, které kybergroomer bez jejich vědomí nashromáždil sám z internetu. Tyto další informace umístěné na internetu pak může útočník získávat tak, že do internetového vyhledávače (Google, Seznam apod.) zadá nějaký jednoznačný identifikátor oběti například její e-mailovou adresu a počká, jestli mu vyhledávač zobrazí nějaké vazby na další stránky, kde již byla zadaná adresa použita. Pokud vyhledávač takové stránky najde, pak na nich může kybergroomer zjistit další informace, které následně poslouží k doplnění profilu nebo k upřesnění a ověření informací, které již dříve o oběti získal.[134]

3.4.3 Třetí etapa – Příprava na osobní setkání

Jakmile útočník nashromáždí dostatečné množství diskriminujících informací, pomocí kterých je schopen s obětí účelně manipulovat, začne plánovat osobní setkání.

Záměna identity

Během příprav na osobní setkání s obětí musí kybergroomer, pokud tak neučinil již dříve, vyřešit například otázku své falešné identity. Pokud se do této doby vydával za někoho mladšího, musí pro oběť vymyslet logický důvod proč tomu tak není.

Jednou z možností, jak může kybergroomer vyřešit tento problém, je přesvědčit oběť k osobní schůzce a těsně před setkáním jí sdělit následující informaci:

„Ahoj Petře, bohužel jsem se zdržel ve škole, tak tě na domluveném místě vyzvedne autem můj táta, jak pro mě pojede do školy.“ Oním tátou je pak samotný kybergroomer.

[134] KOPECKÝ, K. Kybergrooming nebezpečí kyberprostoru. *Net Univers*ity [online]. 2010. [cit. 2011-09-26]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie>. ISBN 978-80-254-7573-7.

Vydírání oběti

Pokud se pachateli nedaří vylákat oběť na schůzku dobrovolně, nasazuje všechny možné páky k tomu, aby schůzky docílil. Pro kybergroomera nastává pravá chvíle k využití všech choulostivých informací, které během kontaktu s obětí nashromáždil a začne ji vydírat například tím, že o ní tyto důvěrné informace zveřejní ve škole nebo v místě bydliště. Řada dětí se tak pod vidinou zostuzení a hanby spojených se zveřejněním jejich intimních záběrů (fotek, videí) raději podvolí a na osobní setkání přijde.[135]

3.4.4 Čtvrtá etapa – Osobní setkání kybergroomera s obětí

Ve čtvrté etapě se kybergroomer poprvé osobně setkává se svou obětí, což je ostatně hlavním cílem veškerého jeho dosavadního snažení.

Prověřování oběti

Se stále se zvyšujícím povědomím široké veřejnosti o možných nástrahách číhajících na dítě v okolním světě a s tím spojenou zvýšenou ostražitostí museli i kybergroomeři přijmout určitá opatření. Proto často kybergroomer na první schůzce na oběť nezaútočí a využije schůzku jen k tomu, aby si ověřil, že opravdu komunikoval s dítětem (o které má zájem) a že na schůzku nepřišel nikdo jiný, s kým se nechce setkat (rodiče dítěte, policií nasazený agent, apod.).[136] Často svou oběť napřed sleduje z povzdálí, než se přesvědčí, že přišla sama a až pak ji osloví.

Opětovné zvyšování důvěry

V případech, kdy útočník není schopen dítě během schůzky vylákat do míst, kde by na něj mohl beze svědků zaútočit, zúročí zpravidla takové setkání pro posílení důvěry dítěte ve svoji osobu, a to například tím, že ho pozve na zmrzlinu nebo mu koupí nějaký

[135] Seznam se bezpečně. *Seznam se bezpečně* [online]. [cit. 2011-07-27]. Dostupné z WWW: <http://www.seznamsebezpecne.cz/>.
[136] KOPECKÝ, K. Kybergrooming nebezpečí kyberprostoru. *Net Univers*ity [online]. 2010. [cit. 2011-09-26]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie>. ISBN 978-80-254-7573-7.

dárek. Takovým zvyšováním důvěry může na některé z následujících schůzek dosáhnout toho, že dítě vyláká i do míst, kam by dříve nešlo a tam teprve zaútočí.[137]

Útok

Jestliže se útočník dostatečně přesvědčí, že je dítě plně v jeho moci, tedy nikým nehlídané a ochotné jít na jakékoliv místo, které určí, pak při osobním setkání zpravidla dochází k útoku. To, jakým způsobem dítě zneužije, je jen otázkou jeho volby. Může dítě znásilnit, fyzicky napadnout, donutit k nafocení pornografických materiálů, zneužít k páchání trestné činnosti, v krajním případě může být následkem osobního setkání i usmrcení dítěte.

3.5 Případy kybergroomingu

V této kapitole jsou uvedeny nejznámější kauzy kybergroomingu, které se staly v nedávné době v České republice a v zahraničí.

3.5.1 V České Republice

Pavel Hovorka

Mezi nejznámější kauzy uváděné v souvislosti s útokem kybergroomera patří v České republice případ z roku 2009, spojený se jménem Pavel Hovorka. Zmiňovaný Hovorka stanul počátkem února roku 2009 před Pražským Městským soudem pro podezření z údajného zneužití více než dvaceti chlapců.

Své oběti vyhledával přes internet a podle kriminalistů se zaměřoval hlavně na děti ze sociálně slabších rodin a děti pocházející z dětských domovů. Od těchto dětí pak pachatel různými metodami získával fotografie, na kterých byly děti zachyceny nahé. Následně pomocí takto obdržených fotografií děti vydíral a nutil k různým sexuálním aktivitám. Na základě výše jmenovaných skutečností pak žalobci Pavla Hovorku vinili z pohlavního

[137] KOPECKÝ, K. Kybergrooming nebezpečí kyberprostoru. *Net Univers*ity [online]. 2010. [cit. 2011-09-26]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie>. ISBN 978-80-254-7573-7.

zneužívání, vydírání, ohrožování výchovy, svádění k pohlavnímu styku a znásilnění. Za uvedené skutky Hovorkovi v tu chvíli hrozilo až dvanáctileté vězení.[138]

Na základě sdělených obvinění obžalovala státní zástupkyně Hovorku ze spáchání osmadvaceti skutků, kterých se měl dopustit na jednadvaceti chlapcích. Ve skupině poškozených chlapců nebyl nikdo, kdo by překročil věkovou hranici 18 let, několik z nich dokonce spadalo do věkové kategorie pod 15 let.

Co předcházelo obžalobě Hovorky? Z různých zdrojů se postupně doplňoval celkový obraz toho, jak se celá kariéra kybergroomera vyvíjela. Jak už bylo řečeno, Hovorka se nejvíce zaměřoval na děti, které byly z dětských domovů, a mezi těmi následně vyhledával potencionální oběti svých nebezpečných aktivit. Pro usnadnění přístupu k těmto dětem zvolil kybergroomer Hovorka speciální taktiku založenou na tom, že se vydával za majitele prestižní bezpečnostní agentury nazvané VIP. Pod touto identitou následně kontaktoval vybrané dětské domovy a nabízel jim svou sponzorskou podporu.[139]

Tuto svou sponzorskou činnost u soudu později obhajoval argumentem, že chtěl jen pomáhat dětem z dětských domovů, protože i on sám v dětském domově vyrůstal. Otázkou je, nakolik byla jeho argumentace pravdivá. Lze se oprávněně domnívat, že pravým důvodem jeho sponzorské činnosti byl především úmysl dostat se co nejblíže k dětem z dětských domovů a také zajistit si u svých budoucích obětí vyšší důvěryhodnost pomocí takzvané falešné autority. Takto vytvořená falešná autorita mu zřejmě pomohla i v případě zneužití jeho „první“ oběti v roce 2005.

Za první „oficiální“ Hovorkovu oběť je považován chlapec pocházející z dětského domova, kterému Hovorka v roce 2005 namluvil, že se stal výhercem v soutěži nazvané „Dítě VIP“. První cenou v této soutěži měl být dvoutýdenní pobyt v Praze. Chlapec bohužel nemohl tušit, že se ve skutečnosti jedná o podvod a celá zmiňovaná soutěž je pouze Hovorkovou záminkou, jak jej vylákat k osobní schůzce. Pro chlapce se tak zmiňovaná výhra čtrnáctidenního pobytu v Praze změnila na několikadenní znásilňování na rozkládacím lůžku v prostorách vrátnice Libeňské tiskárny, kde v té době Hovorka žil a pracoval jako hlídač.

Poté začal Hovorka vyhledávat další oběti pomocí internetového seznamovacího serveru Lidé.cz. Tady se opět zaměřil na nezletilé chlapce, o kterých si začal zjišťovat, kde bydlí, jaké jsou jejich zájmy, a následně začal vytipované chlapce kontaktovat. Po počátečním

[138] Muž zřejmě zneužil víc jak dvacet chlapců, stojí před soudem. *Česká televize* [online]. 3.2.2009. [cit. 2011-05-02]. Dostupné z WWW: <http://www.ct24.cz/domaci/43695-muz-zrejme-zneuzil-vic-jak-dvacet-chlapcu-stoji-pred-soudem/>.

[139] BARTOSZ, J. Soud potrestal zneužití jednadvaceti chlapců osmi lety vězení. *iDNES* [online]. 5.2.2009. [cit. 2011-06-12]. Dostupné z WWW: <http://zpravy.idnes.cz/soud-potrestal-zneuziti-jednadvaceti-chlapcu-osmi-lety-vezeni-pvv-/krimi.aspx?c=A090205_101224_krimi_jba>.

dopisování a telefonátech, zpravidla ve chvíli kdy už měl pocit, že si u nich získal potřebnou důvěru, je začal pod různými záminkami zvát k sobě do zaměstnání. Pokud se oslovený chlapec na schůzku dostavil, Hovorka jej zpravidla zavedl na vrátnici tiskárny, a tam následně sexuálně zneužil. Během sexuálních aktivit s chlapci si Hovorka často pořizoval fotografický materiál, na kterém byli vylákaní chlapci zachyceni v různých choulostivých sexuálních pozicích. Takto pořízený citlivý materiál pak i nadále používal k vydírání a zastrašování zdokumentovaných obětí, které se většinou pod pohrůžkou zveřejnění pořízených záznamů neodvážili bránit. Hovorka pro chlapce pořízením fotografií vytvořil jakýsi začarovaný kruh, z kterého pro ně nebylo snadné vystoupit.[140]

U dalších obětí dosáhl Hovorka osobního setkání tím, že vytipovaným chlapcům, které kontaktoval přes internet, nabízel různé odměny a dárky za to, že mu pošlou nějakou fotografii, na které jsou zachyceni nazí. Po obdržení takové fotografie nutil na nich uvedeného jedince k osobnímu setkání, opět pod vyhrůžkou zveřejnění kompromitujících materiálů, které mu sama oběť za jeho dárky poslala.[141]

O Hovorkových aktivitách a jeho obětech se Policie České republiky dozvěděla hlavně díky informacím, které obdržela od sociálních pracovnic a zaměstnanců dětských domovů v Praze. Městský soud v Praze na základě obžalování státní žalobkyní nakonec odsoudil Hovorku k osmi letům odnětí svobody. Hovorka byl shledán vinným tím, že se v 7 případech dopustil pohlavního zneužívání a ve 13 případech vydírání. Mimo to byl také uznán vinným z ohrožování výchovy mládeže a svádění k pohlavnímu styku. Velmi zajímavé bylo, že soud v žádném z případů sexuálního zneužití dětí neshledal Hovorku vinného ze spáchání trestného činu znásilnění. Tento trestný čin se mu nepodařilo prokázat, i když obžaloba uvedla, že někteří z chlapců se sexuálnímu styku podvolili jen pod tíhou vyhrůžky ze strany pachatele. Kromě trestu odnětí svobody byla Hovorkovi nařízena také ústavní sexuologická léčba.[142]

Hovorka se proti původnímu rozsudku odvolal a jeho trest byl posléze snížen na šest a půl roku odnětí svobody. Mohlo by se zdát, že tím byl celý případ Hovorka uzavřen, kdyby se ovšem několik dnů po vynesení rozsudku neozvala pětadvacetiletá žena, která uvedla, že se stala Hovorkovou obětí už v roce 1993. Doslova tato žena uvedla: *„Byl to šok, když jsem*

[140] BARTOSZ, J. Soud potrestal zneužití jednadvaceti chlapců osmi lety vězení. *iDNES* [online]. 5.2.2009. [cit. 2011-06-12]. Dostupné z WWW: <http://zpravy.idnes.cz/soud-potrestal-zneuziti-jednadvaceti-chlapcu-osmi-lety-vezeni-pvv-/krimi.aspx?c=A090205_101224_krimi_jba>.

[141] BUBLANOVÁ, A. Za zneužití dvaceti chlapců půjde Hovorka na osm let do vězení. *Mediafax* [online]. 5.2.2009. [cit. 2011-08-14]. Dostupné z WWW: <http://www.mediafax.cz/krimi/2814724-Za-zneuziti-dvaceti-chlapcu-pujde-Hovorka-na-osm-let-do-vezeni>.

[142] Zneužil přes dvacet chlapců, dostal osm let. *Novinky* [online]. 5.2.2009. [cit. 2011-06-12]. Dostupné z WWW: <http://www.novinky.cz/krimi/160547-zneuzil-pres-dvacet-chlapcu-dostal-osm-let.html>.

ho viděla v televizi. Ten ksicht, to jméno, to nezapomenete!“ Podle ženy, která chtěla zůstat v anonymitě, ji Hovorka sexuálně zneužil, když měla devět let. V té době bylo Hovorkovi dvacet let. Právě on měl být tím, kdo jí způsobil celoživotní trauma, a jako důvěřivé dítě zneužíval, vydíral a trápil. Podle toho, co uvedla postižená, měl Hovorka zneužívat ji a její kamarádku už v roce 1993. Svá tvrzení, že šlo o Hovorku, dokládala tím, že jí onen násilník ukázal svůj občanský průkaz, kde bylo uvedeno jeho jméno. Na dotaz, proč jí pachatel ukázal průkaz své totožnosti, žena odpověděla, že už tehdy Hovorka vypadal dosti vyžile a proto mu nechtěla uvěřit jeho věk. Už tehdy prý vypadal tak na čtyřicátníka, a on jí tak chtěl svůj skutečný věk dokázat.

Celé své trápení žena popsala následujícím způsobem. Když jí bylo devět let navštěvovala základní školu v jednom severočeském městě. Právě před touto školou se jednoho dne objevil neznámý člověk, který se k dětem choval moc hezky a mile. Tento člověk si postupně získával důvěru dětí, se kterými se setkával. Ve chvíli kdy měl pocit, že mu některé z dětí dostatečně důvěřuje, donutil ho k nějakým sexuálním praktikám. Pak už následovalo jen další vydírání a zneužívání tohoto dítěte. Žena uvedla, že i ona byla v té době malé, naivní a důvěřivé dítě a podlehla tomu, co jí pachatel řekl. Podle ní právě Hovorka jí, stejně jako všem postiženým dětem, řekl, že když mu nebudou po vůli, tak poví jejich rodičům, co spolu dělali a děti že pak půjdou do pasťáku a rodiče do vězení. Své tehdejší pocity popsala takto: *„Nechcete k němu jít, nelíbí se vám co dělá, ale musíte, protože se bojíte.“*

Pachatel zkrátka držel své oběti v šachu. Během těch tří měsíců co k němu musela chodit, prý zažila sexuální hrátky, které nejsou běžné ani v normálních milostných vztazích. Z okolí školy zmizel až ve chvíli, když se na něj začali ptát učitelé.

Žena uvedla, že podobně postižených dětí bylo víc, ale všechny se bály jeho výhrůžek, a proto při dotazu na onoho podivného pána vyskytujícího se v okolí školy, vše popřely. To bylo také důvodem, proč se nic nevyšetřovalo. Žena tehdy ještě navíc přičítala vinu za prožitá muka sama sobě, brala to jako své selhání, rodiče ji přece častokrát varovali před cizími lidmi a říkali jí, aby od neznámých pánů nebrala bonbony a ona si ten pomyslný bonbon přesto vzala.

O svém zážitku se prý žena svěřila svým rodičům až po sedmi letech, když jí bylo šestnáct let. Chtěli okamžitě jít na policii, ale ona je uprosila, aby to nedělali. Bylo

to ze strachu, že bude hrůznou vzpomínkou opět traumatizována. Rodiče jí tak vyhověli a už se na toto téma raději nikdy nebavili.[143]

Žena se tak rozhodla veřejně promluvit o svém hrůzném zážitku až na základě informací, které o případu Hovorka proběhly v médiích. Nechtělo se jí věřit, že by Hovorka od roku 1993 zůstal nečinný a ve svých aktivitách pokračoval až v roce 2005. Vyčítá si, že už dřív s rodiči celý případ nenahlásila na Policii. Domnívá se, že tak mohlo být pachateli zabráněno v pokračování jeho činnosti.[144]

Otázkou tedy nadále zůstává, kolik dětských obětí má ve skutečnosti kybergroomer Hovorka na svědomí a kdo a kdy byl jeho skutečně první obětí.

Jiří Kadrnožka

Dalším případem kybergroomingu v České Republice je kauza Jiřího Kadrnožky. Velice se odlišuje od ostatních zejména způsobem, jakým došlo k odhalení pachatele. Celý příběh se začal psát v redakci MF DNES v roce 2006. Redaktoři Jana Blažková a Jakub Blažek se rozhodli otestovat, nakolik jsou malé děti při komunikaci na internetu ohroženy různými nebezpečími spojenými s komunikací s neznámými lidmi. Za tímto účelem si vytvořili svou falešnou identitu a začali se vydávat za jedenáctiletou dívku Terezku. Pouhé dva dny potom, co začali pod touto identitou navštěvovat různé internetové seznamky a další internetové stránky, narazili na serveru xchat.cz na velice vulgární dotaz.

"Je tu mladá holka z Prahy nebo Nymburka, která mi ho ...?“

Tento dotaz redaktory nezarazil jen svou vulgaritou ale hlavně i tím, že se objevil v diskusním fóru určeném pro děti ve věkové kategorii od devíti do třinácti let. Na druhou stranu však zároveň šlo o impuls k zahájení komunikace, na který redaktoři celou dobu čekali. Rozhodli se tedy na zmíněný dotaz reagovat a začali s jeho autorem, který se označil jako Jirzin, chatovat.

[143] NEJEZCHLEBOVÁ, L. Ozvěte se, vzkazují vyšetřovatelé obětem sexuálních deviantů. *iDNES* [online]. 18.2.2009. [cit. 2011-06-14]. Dostupné z WWW: <http://zpravy.idnes.cz/ozvete-se-vzkazuji-vysetrovatele-obetem-sexualnich-deviantu-p6t-/krimi.aspx?c=A090218_011257_krimi_nel>.

[144] NEJEZCHLEBOVÁ, L. I mě zneužil deviant Hovorka. Ten ksicht nezapomenu, vzpomíná žena. *iDNES* [online]. 16.2.2009. [cit. 2011-07-21]. Dostupné z WWW: <http://zpravy.idnes.cz/i-me-zneuzil-deviant-hovorka-ten-ksicht-nezapomenu-vzpomina-zena-pyv-/krimi.aspx?c=A090213_154133_domaci_nel>.

Následuje doslovný přepis komunikace redaktorů serveru MF DNES (Terezky) s Jirzinem, autorem vulgárního dotazu. Součástí uvedeného rozhovoru jsou i komentáře redaktorů MF DNES.

Terezka: Jak to myslíš?

Jirzin: Tak, jak to píšu, prostě...

Terezka: Kolik ti je? Mně je 11.

Jirzin: Je mi 27, odkud jsi?

Terezka: Z Prahy.

Jirzin opáčí, že je také z Prahy, a vyptává se dál. Loudí Terezčinu adresu. Dívka odepíše, že bydlí v ulici Na Březince na Smíchově a on jí na oplátku prozradí, že pracuje na sídlišti Jižní Město v pojišťovně jako počítačový odborník.

"*Pošli mi fotku*," pokračuje Jirzin ve svých požadavcích. Redaktor MF DNES mu posílá podomácku pořízenou fotografii tmavovlasé teprve desetileté dívky s culíky a brýlemi. Ani dětsky vyhlížející obrázek však mladého muže nezastaví.

Terezka: Tak už jsem ti fotku poslala. Pošleš mi teď svou?

Jirzin: Moment, jdu se nejdřív podívat.

Jirzin: Koukni se na stránky www.lide.cz/j.k.

Na uvedené adrese v tom okamžiku skutečně byly údaje o jeho osobě. Muž má iniciály J. K., uvádí, že je mu 27 let a má tam vystavené i své tři fotografie. Na všech vypadá pohledně, upraveně a jako sportovec. Na jedné z fotografií dokonce sedí ve sportovním voze se stahovací střechou. To vše může podle sexuologů na malou dívku příznivě zapůsobit. "Dívky kolem deseti let si už uvědomují svou sexuální identitu a jsou zvídavé. Takže některým ani ty jeho otázky nebudou vadit a probudí jejich zájem. I kdyby to byla jen dvě děvčata z deseti, která se na to chytí, je ten člověk nebezpečný," míní dětský psychiatr Vladimír Hort. Fotografie "zabírají" i na fiktivní Terezku.

Terezka: Ty máš auto bez střechy?

Jirzin: Bylo vypůjčený. Už jsi viděla nahatýho kluka někdy?

Terezka: Já bych taky chtěla mít takový auto. Viděla jsem staršího bráchu. Proč?

Jirzin: No jestli budu první.

Terezka: Jak to myslíš?

Jirzin: No chtěla si mi .... pindíka, ne?

Terezka: Já nevím, jak se to dělá.

Jirzin jí v té chvíli podrobně popíše požadovanou sexuální praktiku. Terezka mu vypráví o svých školních problémech. Chodí do páté třídy a ráda by se dostala na gymnázium. Jenže tím ho nezaujme.

Jirzin: Nemáš fotku celý postavy? Máš už nějaký menší prsa?

Terezka: Takovou fotku nemám. Ale už mi rostou, ale jsou malý. Kamarádka má větší.

Jirzin: A co chloupky?

Terezka: Jako myslíš tam dole?

Jirzin: Hmmm...

Terezka: Jé. Mám trochu. Proč?

Jirzin: Začínám být vzrušenej.

Terezka pak odvádí řeč na sport a "bedbington", který ráda hraje. Domlouvají se, že by se mohli sejít.

Jirzin: Není u tebe nějaký místo, kde by nás nikdo neviděl?

Terezka: To není. Máma je furt doma. Nechceš jít radši ven?

Jirzin: Myslím jako venku, kde by nás nikdo neviděl. Zítra bych mohl od 17.40 hodin.

Terezka: Tak prima, nejlepší to bude asi u gymplu Zatlanka, to mám kousek. V šest? Jsi sportovec? Hraješ bedbington?

Jirzin: To by šlo, ale neznám to tam. A tam nikdo není? A nepřijde?

Muž pak od dívky vymámí číslo mobilního telefonu. Terezka nakonec podlehne a číslo vydá. Výměnou získává mužův mobil. Jirzin se ještě vyptává, co bude mít Terezka za oblečení a poradí, aby si vzala sukni. Následně se rozloučí s tím, že se sejdou zítra.[145]

Na základě uvedené komunikace se redaktoři MF DNES rozhodli, že na smluvenou schůzku opravdu půjdou, aby zjistili kdo se pod identitou Jirzin skrývá. Druhý den se Jirzin nečekaně přes internet ozval Terezce znovu, tentokráte se jen chtěl ujistit, zda o jejich domluvené schůzce někomu neřekla. Redaktor jej samozřejmě pod dívčinou identitou ujistil, že ne.

Muž, kterého redaktoři znali jen z fotografie, na smluvenou schůzku ve čtvrtek v podvečer skutečně přišel, dokonce s patnáctiminutovým předstihem. Místo, kde ho měla později čekat fiktivní Terezka, jen nedbale přehlédl, a rovnou vyrazil do parku v kopci, odtud byl dobrý výhled na domluvené místo a schovaný za křovím ho pozorně sledoval.

[145] BLAŽKOVÁ, J.; BLAŽEK, J. Je tu mladá holka, která mi ho…? *iDNES* [online]. 7.10.2006. [cit. 2011-08-23]. Dostupné z WWW: <http://zpravy.idnes.cz/je-tu-mlada-holka-ktera-mi-ho-dpr-/krimi.aspx?c=A061007_094833_domaci_jan>.

Kadrnožka byl velice zaskočen, když ho tady po čtvrthodině oslovili redaktoři s dotazem, jestli čeká na Terezku. Zpočátku se bránil, že o ničem neví. Po chvíli se na základě důkazu - fotografie, kterou měli redaktoři a kterou uvedl na internetu při komunikaci s Terezkou, přiznal, že je tím, kdo s ní komunikoval. Uvedl, že vše dělal jen z hlouposti a zvědavosti, že už má svou dívku a Terezce chtěl jen říci, že už nebude ve svých návrzích pokračovat. Poté požádal redaktory, aby smazali všechny důkazy, že už to nikdy neudělá. Ovšem když zjistil, že si redaktoři zaznamenávají i průběh tohoto rozhovoru, raději utekl.[146]

Redaktoři poté uvedené materiály poskytli Policii ČR, která na jejich základě Jirzina, tedy Kadrnožku zatkla. Před soudem se už Kadrnožka nehájil svou hloupostí, ale jeho advokáti naopak obvinili MF DNES, že vše na Kadrnožku předem připravila ve snaze zvýšit si svou publicitu a prodej. Když na to soudkyně nereflektovala, přišli advokáti s další verzí, ve které uváděli, že Kadrnožka s dívkou komunikoval z nudy a předpokládal, že mu o svém věku neříká pravdu, což je na internetu běžné. Ale ani to mu nepomohlo.

Pět měsíců poté, co Kadrnožku kontaktovali redaktoři MF Dnes, nad ním Městský soud v Praze 5 vynesl verdikt odnětí svobody na dva roky se čtyřletou podmínkou s odůvodněním, že se Kadrnožka dopustil přípravy trestného činu pohlavního zneužívání. Dále mu byla uložena povinnost podrobit se ústavní sexuální léčbě.[147]

Později se v Kadrnožkově případu objevily ještě nějaké nejasnosti ohledně typu deviace, kterou ve skutečnosti trpí. To už ovšem nemá žádný vliv na to, čeho se stihl dopustit.

Za nejdůležitější v této kauze můžeme označit tu skutečnost, že díky zájmu redaktorů MF Dnes o nebezpečí hrozící dětem při navazováním kontaktů s cizími osobami pomocí internetu bylo zabráněno možnému útoku na dítě, které by se s Kadrnožkou pravděpodobně seznámilo, kdyby jej „nepředběhla“ fiktivně vytvořená Terezka.

3.5.2 V zahraničí

Peter Chapman

Mezi velice známé případy kybergroomingu ze zahraničí patří kauza z roku 2009 spojená se jmény Peter Chapman a Ashleigh Hallová. Ashleigh Michelle Hallová byla mladá

[146] BLAŽKOVÁ, J.; BLAŽEK, J. Je tu mladá holka, která mi ho…? *iDNES* [online]. 7.10.2006. [cit. 2011-08-23]. Dostupné z WWW: <http://zpravy.idnes.cz/je-tu-mlada-holka-ktera-mi-ho-dpr-/krimi.aspx?c=A061007_094833_domaci_jan>.

[147] KUBÍK, J. Pozor na znuděné devianty. *iDNES* [online]. 7.4.2007. [cit. 2011-06-30]. Dostupné z WWW: <http://zpravy.idnes.cz/pozor-na-znudene-devianty-09w-/domaci.aspx?c=A070406_212057_nazory_mia>.

sedmnáctiletá dívka, která žila se svou matkou a třemi sestrami v anglickém Darlingtonu. Ashleigh byla mezi přáteli oblíbená, ráda se bavila a seznamovala s novými lidmi. Ke komunikaci s přáteli často používala různé sociální sítě. Svými zájmy se nijak nelišila od ostatních vrstevníků. Stejně jako u dalších mladých lidí, tak i u ní byl mobilní telefon a internet běžnou součástí každodenního života. Ashleigh studovala poslední ročník ošetřovatelství a po ukončení studia chtěla pracovat jako dětská sestra. Se svou matkou i sourozenci měla velice hezký vztah. Její matka uvedla, že Ashleigh pro ni nebyla jenom dcera, ale i nejlepší kamarádka jakou kdy měla, mohla se na ni kdykoliv spolehnout, byla její oporou. Ashleigh jí jako nejstarší dcera pomáhala vychovávat své mladší sestry Olivii, Elli a Evi, které ji měly za druhou mámu. Velice ji milovaly a stejně tak ona milovala je. Ashleigh nebyla nějakým nevyrovnaným jedincem, ale rozumně uvažující mladou dívkou. Snad jen její malé sebevědomí bylo důvodem, proč si nedokázala ve svých 17-ti letech najít chlapce. To se později zřejmě stalo i příčinou toho, proč byla ochotná jít na schůzku s člověkem, se kterým se znala pouze přes internet.[148]

Tím, kdo ji pomocí sítě Facebook kontaktoval, měl být devatenáctiletý pohledný chlapec vystupující pod jménem Peter Cartwright. Ve skutečnosti však Ashleigh nevědomky komunikovala s někým úplně jiným, než si podle informací uvedených v profilu Cartwrighta představovala. Ashleigh pomocí sociální sítě Facebook navázala kontakt se svým budoucím vrahem Peterem Chapmanem.

Peter Chapman alias Peter Cartwright se narodil v roce 1977 a v době, kdy s Ashleigh navázal virtuální vztah, mu nebylo 19 ale 32 let. Další z věcí, kterou Ashleigh netušila, bylo to, že Chapman měl téměř celý život problémy se zákonem.

Jeho kariéra v tomto směru byla opravdu pestrá. Už ve věku 15-ti let byl vyšetřován v souvislosti se sexuálním napadením. O čtyři roky později byl obviněn za znásilnění dívky, ale jeho obvinění bylo později staženo. V roce 1996 byl Chapman opět obviněn, tentokrát z útoku na dvě mladé prostitutky, které ohrožoval nožem a znásilnil. Za zmíněné skutky byl odsouzen k sedmi letům vězení a zároveň nad ním byl stanoven policejní dohled, protože jej označili za mimořádně nebezpečného sexuálního násilníka. Chapman byl z vězení propuštěn už v roce 2001. Již zanedlouho, v roce 2002, byl znovu zatčen a vzat do vazby za únos a znásilnění další prostitutky, ale tento případ byl opět odložen. Podobného činu se dopustil znovu v roce 2003 v Liverpoolu, kde unesl a znásilnil prostitutku, kterou vlákal do svého

[148] STOKES, P. Ashleigh Hall: 'one mistake' cost teenager her life. *Telegraph* [online]. 8.3.2010. [cit. 2011-06-08]. Dostupné z WWW: <http://www.telegraph.co.uk/news/uknews/crime/7398085/Ashleigh-Hall-one-mistake-cost-teenager-her-life.html>.

auta. Byl zatčen, ale i tento případ byl odložen. Jeho oběť tehdy během vyšetřování uvedla, že se choval velmi slušně a příjemně a proto v něm neshledala někoho, kdo by na ni mohl později zaútočit. Zástupce policie o Chapmanovi však již tehdy prohlásil, že je to nebezpečný a nevyzpytatelný jedinec, který může být zodpovědný za další podobné trestné činy.[149]

Chapmanovo chování v následujících letech potvrdilo slova policisty. V roce 2007 se Chapman seznámil pomocí sociální sítě s 25 letou svobodnou matkou Dianou Littlerovou, která žila sama s tehdy čtyřměsíčním dítětem. Ke zmíněné ženě se záhy nastěhoval, po šesti měsících ji požádal o ruku, a žena souhlasila. V té době vůbec netušila, že byl dříve Chapman odsouzen za znásilnění prostitutek. K jejich sňatku nakonec nedošlo jen díky tomu, že ji na Chapmanovu minulost upozornili policisté, když se na něj jako na odsouzeného sexuálního delikventa pod dozorem přišli zeptat do jejího bytu. Diana na základě sdělených informací vztah s Chapmanem okamžitě ukončila. Po jejich rozchodu jí Chapman začal vyhrožovat tím, že jí podpálí dům a zabije dítě. Diana se vyděsila a raději se odstěhovala k matce.

V roce 2009 se Chapman seznámil s další ženou, ke které se opět také nastěhoval. Jejich vztah ovšem skončil brzy poté, co se Chapman neshodl s jejím sousedem, a kterému pak zanedlouho nato vyhořel dům. Chapman zmizel krátce po požáru i s notebookem, který ženě ukradl.[150]

Poté si Chapman pořídil dodávku, ve které cestoval a bydlel, a z které také navazoval pomocí internetových seznamek a sociálních sítí kontakty s dalšími ženami. Do jeho dodávky nastoupila Ashleigh v den, kdy se měla konečně setkat se svým přítelem z internetu Peterem Cartwrightem. Nejprve ji zarazilo, že místo pohledného chlapce přišel na schůzku někdo jiný, ale Chapman ji přesvědčil, že je otcem Petera Cartwrighta a že ji za ním odveze. To, že ji na návštěvu ke „kamarádce“ odveze její otec autem, napsala Ashleigh své matce jako svou poslední SMS-ku. Chapman ji místo toho zavezl na opuštěné místo a tam ji znásilnil. K tomu, aby se mu nebránila a aby nekřičela použil lepící pásku, kterou jí spoutal ruce a přelepil ústa. Poté, co ji znásilnil, použil opět lepící pásku, aby ji ještě pevněji znehybnil, přičemž jí ještě několikrát přelepil ústa i nos. Dívka se tak pomalu udusila. Chapman následně pohodil její bezvládné tělo na skládku.

Hned následující den po vraždě byl Chapman náhodně zadržen policií při dopravní kontrole. Zadržení proběhlo v době, kdy ještě policisté nevěděli, že Chapman někoho zabil

[149] Ashleigh Hall's killer had history of sexual violence. *BBC News* [online]. 8.3.2010. [cit. 2011-05-04]. Dostupné z WWW: <http://news.bbc.co.uk/2/hi/uk_news/england/wear/8555844.stm>.
[150] Ashleigh Hall's killer had history of sexual violence. *BBC News* [online]. 8.3.2010. [cit. 2011-05-04]. Dostupné z WWW: <http://news.bbc.co.uk/2/hi/uk_news/england/wear/8555844.stm>.

a že je Ashleigh pohřešovaná. To však Chapman nevěděl. Myslel si, že jej policisté zadrželi právě v souvislosti s Ashleigh, a tak je sám nechtěně přivedl na stopu svým prohlášením, že jeho auto mohou klidně rozřezat na kusy a stejně nic nenajdou. Chapmanovo sdělení se zdálo policistům divné, a proto se na něj při výslechu zaměřili. Chapman se nakonec k vraždě dívky přiznal. Tvrdil, že ji nechtěl zabít a že šlo jen o nešťastnou náhodu.[151]

Za svůj čin byl Chapman v roce 2010 odsouzen k trestu odnětí svobody na doživotí.

3.6 Právní rámec kybergroomingu

Od 1. 1. 2010 v České Republice nabyl účinnosti nový trestní zákoník č. 40/2009 Sb., který nahradil do té doby platný trestní zákon č. 140/1961 Sb. Tato právní norma sice zařadila mezi trestné činy nebezpečné pronásledování (stalking), ale kybergrooming v ní jako samostatný trestný čin zahrnut není. To však neznamená, že by nebylo možné pachatele takového jednání účinně postihovat. Nebezpečné aktivity kybergroomera je možné postihovat v případech, kdy naplní skutkovou podstatu jiných trestných činů v Trestním zákoníku uvedených. Mezi trestné činy, kterých se kybergroomeři při svých aktivitách mohou dopustit, lze zařadit například tyto:

Trestný čin	Paragraf	Trest odnětí svobody
Obchodování s lidmi	§ 168	na 2 léta až 10 let
Omezování osobní svobody	§ 171	až na 2 léta
Vydírání	§ 175	na 6 měsíců až 4 léta
Znásilnění	§ 185	na 6 měsíců až 5 let
Pohlavní zneužití	§ 187	na 1 rok až 8 let
Výroba a jiné nakládání s dětskou pornografií	§ 192	až na 2 roky
Zneužití dítěte k výrobě pornografie	§ 193	na 1 rok až 5 let
Ohrožování výchovy dítěte	§ 201	až na 2 léta
Svádění k pohlavnímu styku	§ 202	až na 2 léta
Podvod	§ 209	až na 2 léta
Nebezpečné vyhrožování	§ 353	až na 1 rok
Nebezpečné pronásledování	§ 354	až na 1 rok

Tabulka č. 4 - Příklady trestných činů kybergroomerů[152]

[151] ŠVAMBERK, A. Sedmnáctiletou oběť si našel na Facebooku, znásilnil ji a zavraždil. *Novinky* [online]. 9.3.2010. [cit. 2011-06-22]. Dostupné z WWW: <http://www.novinky.cz/zahranicni/evropa/194196-sedmnactiletou-obet-si-nasel-na-facebooku-znasilnil-ji-a-zavrazdil.html>.

[152] VLACHOVÁ, M. Trestná činnost spojená s internetovou kriminalitou. *E-Bezpečí* [online]. 20.11.2009. [cit. 2011-06-12]. Dostupné z WWW: <http://www.e-bezpeci.cz/index.php/temata/dali-rizika/148-226>.

3.7 Ochrana před kybergroomingem

Nejvyšší možnou úroveň ochrany dětí před útoky kybergroomerů je možné zajistit kombinací prevence (děti budou včas vybaveny potřebnými informacemi o nebezpečích souvisejících s komunikací přes internet) a technických metod. Jak uvádí Musil[153], *„vždy je však důležité, aby všechna opatření, nehledě na jejich úroveň, úzce na sebe navazovala a logicky se vzájemně doplňovala“*. V praxi je ovšem téměř nemožné takového ideálního stavu dosáhnout, nicméně by bylo dobré, pokusit se tomuto stavu alespoň co nejvíce přiblížit.

3.7.1 Technické metody ochrany

Technické prostředky sloužící ke snížení rizika útoku kybergroomera mívají podobu různých softwarových nebo hardwarových řešení. Dle Musila[154] *„technické prostředky prevence jsou obecně buď softwarové nebo hardwarové“*.

Jedním z příkladů takových technických řešení jsou proxy servery. Mívají podobu speciálního hardwaru, ale i softwaru spuštěného na běžném počítači. Pracují na principu aktivní regulace možnosti připojení do sítě Internet u počítačů, které spadají pod jeho správu. Uvedená regulace funguje tak, že operátor na proxy serveru dopředu nastaví, na který internetový portál se konkrétní počítač spravovaný tímto serverem dostane a na který ne. Pokud tedy operátor dopředu nastaví jen přístup ke konkrétním bezpečným stránkám, nehrozí následně, že by se uživatel z takto kontrolovaného počítače připojil na jiné stránky než na ty povolené. Pomocí proxy serverů tedy lze zvýšit ochranu dítěte před útoky z kyberprostoru tím, že se mu z jeho počítače zabrání přístupu na internetové stránky, kde hrozí zvýšené riziko kontaktu s kybergroomerem (sociální sítě, internetové seznamky, chat, instant messengery, apod.). V souvislosti s nasazováním technických řešení, které fungují na principu restrikcí, je ale nutné počítat s tím, že pokud se dítěti zakáže přístup na konkrétní internetové stránky, například na sociální sítě, začne hrozit riziko, že to v něm vzbudí zvědavost a podle rčení „zakázané ovoce chutná nejvíce“, se dítě začne o to více snažit zakázanou stránku navštívit.

Jak už bylo řečeno, kromě možnosti využít proxy servery existuje nejen v případě počítačů mnoho dalších technických metod umožňujících snížit riziko útoku kybergroomera. Jistou nevýhodou těchto metod je ale ta skutečnost, že všechna řešení jsou vždy aplikována

[153] MUSIL, S. *Počítačová kriminalita : nástin problematiky : kompendium názorů specialistů.* 1. vyd. Praha : Institut pro kriminologii a sociální prevenci, 2000. 281 s. ISBN 80-86008-80-0. s. 88.
[154] MUSIL, S. *Počítačová kriminalita : nástin problematiky : kompendium názorů specialistů.* 1. vyd. Praha : Institut pro kriminologii a sociální prevenci, 2000. 281 s. ISBN 80-86008-80-0. s. 71.

na předem určený počítač a žádný ze způsobů zabezpečení aplikovaný na konkrétní počítač tak nemůže zamezit tomu, aby se dítě na internet připojilo z jiného počítače nebo zařízení (PDA, „chytrý“ mobilní telefon), které zabezpečené nebude.

Za další velkou nevýhodu u technických řešení zabezpečení ochrany proti útoku z kyberprostoru můžeme považovat to, že o jejich existenci mnozí rodiče nevědí, a v případech kdy o nich ví, tak v drtivé většině netuší jak je zprovoznit, nainstalovat a nastavit tak, aby skutečně fungovala a bezezbytku plnila svůj účel. Právě jejich často vysoká náročnost na znalosti při jejich implementaci způsobuje, že nejsou ve větší míře využívána v běžných domácnostech, ale především tam, kde jejich správu mohou svěřit do rukou odborníků vzdělaných v oblasti ICT (firmy, státní instituce, atd.).

Uvedené nevýhody technických řešení zabezpečení a jejich častá nepřítomnost na domácích počítačích a dalších zařízeních, ze kterých se děti připojují k internetu, jen podtrhují důležitost druhé roviny, pomocí které můžeme dosáhnout zvýšení ochrany proti útoku z kyberprostoru, spočívající ve včasné a dostatečné informovanosti dětí o těchto hrozících nebezpečích.

3.7.2 Primární prevence

Informace jako ochrana proti útoku z kyberprostoru

Informace, kterými je dítě připraveno na život, představují jedno z nejcennějších bohatství, které jim rodiče mohou předat. To platí i v případě informací týkajících se nebezpečí hrozících z kyberprostoru. Pokud jsou dítěti poskytnuty relevantní informace o těchto nebezpečích včas, kvalitně a v potřebném rozsahu, pak už se nemusí rodiče spoléhat jen na to, že dítě bude při komunikaci přes internet chráněno pouze ve chvíli, kdy se k němu připojí z dokonale zabezpečeného zařízení. Informace, kterými své děti na možná rizika upozorní a připraví, tak mohou představovat mnohem důležitější rovinu v jejich ochraně než technická opatření, protože si je děti na rozdíl od dokonale zabezpečeného zařízení „ponesou“ stále s sebou.

Dostatečné množství kvalitních informací o nebezpečích hrozících z kyberprostoru, které jsou dítěti sděleny a které si dítě osvojí, pak může následně do značné míry ovlivnit i to, jak se bude při práci s internetem chovat. Nakolik bude ochotné sdělovat své kontaktní údaje a citlivá data. Jak brzy v případě ohrožení kybergroomerem zjistí, že na něj útočí. Jak rychle,

dostatečně správně a razantně na tento útok zareaguje. A co je v případě kybergroomingu nejdůležitější, jak bude reagovat ve chvíli, kdy jej neznámá osoba z internetu vyzve k osobnímu setkání.

Lze předpokládat, že dítě kvalitně informované a poučené bude schopné v ideálním případě komunikaci s kybergroomerem přerušit už ve chvíli, kdy díky získaným informacím rozpozná první známky nebezpečné komunikační aktivity. Oproti tomu u dítěte neinformovaného může naopak dojít k řešení problémů spojených s kybergroomingem až ve chvíli, kdy bude vydíráno, zneužíváno nebo jinak ohrožováno. Tedy poměrně pozdě. Proto je nutné v rámci primární prevence[155] poskytnout dítěti včas důležité informace o nebezpečích hrozících z kyberprostoru, aby mu umožnily rozpoznat útok z kyberprostoru a pomohly na tento útok adekvátně zareagovat. Tyto cenné informace může dítě získat z několika zdrojů, vždy však záleží na tom, jak kvalitní budou a v jaké míře je dítě v budoucím životě dokáže ke své obraně využít. Je nutné brát v úvahu, že *„na prevenci by se měly podílet všechny složky, které se podílí na výchově dítěte, tedy rodina, škola i celá společnost. Tak jako připravujeme své děti na to, aby zvládly nástrahy skutečného světa, musíme je naučit překonávat i problémy, se kterými se mohou setkat ve světě virtuálním.“*[156]

Zvyšování informovanosti v rámci školy

Významnou roli ve zvyšování informovanosti dětí o nebezpečích spojených s využíváním moderních ICT sehrávají školy a školská zařízení. Mnozí rodiče, kteří o těchto nebezpečích vědí, dokonce spoléhají na to, že jejich potomky potřebnými informacemi v rámci prevence vybaví právě školy, které jejich děti v průběhu studia navštěvují.

Díky stále většímu výskytu případů, kdy bylo dítě vystaveno útoku z kyberprostoru a jejich medializaci, začaly i školy postupně věnovat zvýšenou pozornost těmto problémům. Každá škola má pro daný stupeň vzdělání stanovené závazné rámcové vzdělávací programy, na základě kterých si jednotlivé školy vytvoří své školní vzdělávacími programy a do výuky tak mohou zahrnout i témata spojená s nebezpečími hrozícími z kyberprostoru.

Například učitelé základních škol často zařazují zmiňovaná témata do vzdělávací oblasti nazvané Informační a komunikační technologie (předmět informatika), která je přímo

[155] primární prevence – zahrnuje veškeré aktivity realizované s cílem předejít problémům spojeným s výskytem sociálně patologických jevů.
[156] KREJČÍ, V. Kyberšikana - kybernetická šikana. *Net University* [online]. 2010. 72 s. [cit. 2011-07-23]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=14%3Akybersikana-studie>. ISBN 978-80-254-7791-5. s. 47.

součástí rámcového vzdělávacího programu pro základní vzdělání. Obdobnou možnost zařazení prevence do výuky na některých školách představuje například i průřezové téma nazvané Mediální výchova.

Protože internet mezi média rozhodně patří a *„hlavním cílem Mediální výchovy jak pro základní, tak gymnaziální vzdělávání by mělo být rozvinutí mediální gramotnosti do takové úrovně, aby využívání médií byla činnost, kterou má jedinec co nejvíc pod vlastní kontrolou a již si dokáže řídit tak, aby mohl mediální nabídky co nejvíce využít“*.[157]

Ve většině škol o nebezpečích spojených s využíváním moderních ICT informují žáky kromě proškolených pedagogů i školní metodici prevence a výchovní poradci, kteří preventivní činnost provádí převážně na základě pokynů a informací zveřejňovaných na internetových stránkách Ministerstva školství, mládeže a tělovýchovy. Zmíněné podklady, z kterých jmenovaní pracovníci čerpají, jsou dostupné i všem ostatním zájemcům na webových stránkách www.msmt.cz v sekci nazvané Prevence rizikového chování.

Minimální preventivní program

Velice dobrou možnost, jak obeznámit žáky s nebezpečími hrozícími z kyberprostoru, přináší Minimální preventivní program. MPP[158] školy povinně vypracovávají na podkladě Metodického pokynu k primární prevenci sociálně patologických jevů u dětí, žáků a studentů ve školách a školských zařízeních vydaného v roce 2007 MŠMT[159] pod číslem jednacím 20 006/2007-51, který vychází ze Školní preventivní strategie. MPP představuje základní nástroj prevence v resortu MŠMT. *„Je komplexním systémovým prvkem v realizaci preventivních aktivit v základních školách, středních školách a speciálních školách, ve školských zařízeních pro výchovu mimo vyučování a školských zařízeních pro výkon ústavní a ochranné výchovy a preventivně výchovné péče.“*[160]

MPP zpracovává školní metodik prevence vždy na jeden školní rok a při jeho tvorbě úzce spolupracuje s ostatními pedagogickými pracovníky. Realizovaný program je následně

[157] JIRÁK, J. Mediální výchova - inspirace k realizaci. *Metodický portál RVP* [online]. 2004. [cit. 2011-07-29]. Dostupné z WWW: <http://clanky.rvp.cz/clanek/s/Z/87/MEDIALNI-VYCHOVA-%E2%80%93-INSPIRACE-K-REALIZACI.html/>.
[158] MPP – Minimální preventivní program (dále jen „MPP“).
[159] MŠMT – Ministerstvo školství, mládeže a tělovýchovy (dále jen „MŠMT“).
[160] MŠMT ČR. *Metodický pokyn ministra školství, mládeže a tělovýchovy k prevenci sociálně patologických jevů u dětí a mládeže, Čj.: 14514/2000 – 51*. [online]. Praha : MŠMT, 2000. 12 s. [cit. 2011-08-01] Dostupné z WWW: <http://www.msmt.cz/file/7253_1_1/download/>. s. 2.

průběžně vyhodnocován a písemné vyhodnocení jeho účinnosti za školní rok se stává součástí výroční zprávy o činnosti školy.[161]

Školní metodik prevence při jeho tvorbě vychází z toho, že primární prevence sociálně patologických jevů u žáků v působnosti MŠMT je zaměřena především na:

„a) předcházení následujícím rizikovým jevům v chování žáků:

- záškoláctví,

- šikana, rasismus, xenofobie, vandalismus,

- kriminalita, delikvence,

- užívání návykových látek (tabák, alkohol, omamné a psychotropní látky – dále jen „OPL[162]“) a onemocnění HIV/AIDS a dalšími infekčními nemocemi souvisejícími s užíváním návykových látek,

- závislost na politickém a náboženském extremismu,

- netolismus (virtuální drogy) a patologické hráčství (gambling)

b) rozpoznání a zajištění včasné intervence v případech:

- domácího násilí,

- týrání a zneužívání dětí, včetně komerčního sexuálního zneužívání,

- ohrožování mravní výchovy mládeže,

- poruch příjmu potravy (mentální bulimie, mentální anorexie).“[163]

A i když mezi rizikovými jevy v chování žáků nejsou přímo jmenovány takové nebezpečné aktivity jako kybergrooming a kyberšikana, nic nestojí v cestě tomu, aby se při tvorbě MPP stávaly jeho běžnou součástí, protože představují sociálně patologické jevy, se kterými se žáci mohou ve škole při práci s počítačem setkat. V poslední době jsme svědky toho, že některé ze škol již tuto možnost využily a kyberšikanu i s kybergroomingem do svých MPP zařadily. Jednou z takových škol je například Základní škola Karla IV.

[161] MŠMT ČR, *Metodický pokyn k primární prevenci sociálně patologických jevů u dětí, žáků a studentů ve školách a školských zařízeních, Čj.: 20006/2007 – 51.* [online]. Praha : MŠMT, 2007. 18 s. [cit. 2011-08-02]. Dostupné z WWW: <http://www.msmt.cz/file/7344_1_1/download/>.

[162] OPL – omamné a psychotropní látky.

[163] MŠMT ČR, *Metodický pokyn k primární prevenci sociálně patologických jevů u dětí, žáků a studentů ve školách a školských zařízeních, Čj.: 20006/2007 – 51.* [online]. Praha : MŠMT, 2007. 18 s. [cit. 2011-08-02]. Dostupné z WWW: <http://www.msmt.cz/file/7344_1_1/download/>. s. 1.

z Nového Bydžova, která se ve školním roce 2010/2011 ve svém MPP na kyberšikanu a kybergrooming přímo zaměřila.[164]

Jak uvádí některé ze škol na svých webových stránkách, tak cílem MPP je ve spolupráci s rodiči formovat takovou osobnost žáka, která je s ohledem na svůj věk schopná se v dané problematice orientovat, která si bude vážit svého zdraví, bude umět správně nakládat se svým volným časem a bude zvládat základní sociální dovednosti.

Dlouhodobě trvající zájem o preventivní působení v oblasti rizikových komunikačních aktivit spojených s využíváním moderních komunikačních technologií v resortu MŠMT dokazuje i to, že v souvislosti s nebezpečími hrozícími na internetu již v roce 2004 MŠMT pod číslem jednacím 11 691/2004-24 vydalo příručku nazvanou „Pravidla pro rodiče a děti k bezpečnějšímu užívání internetu“. Podkladem pro vytvoření uvedené příručky byl stejně nazvaný materiál distribuovaný v roce 2001 na II. Světovém kongresu proti komerčnímu sexuálnímu zneužívání dětí, pořádaném v Jokohamě. Příručkou ministerstvo reagovalo na problémy spojené s využíváním internetu, mezi něž zařadilo například:

- nebezpečí šíření virů,
- nebezpečí zneužití osobních dat,
- možnost kontaktu s nežádoucím jedincem nebo nevhodnými informacemi,
- nebezpečí vzniku závislosti na počítači,
- ohrožení pachateli pedofilních forem sexuálního a komerčního zneužívání,
- sledování pornografie a další.

Vydáním příručky tak upozornilo na potřebu *„směřovat preventivní opatření ve smyslu upozornění na nebezpečí, které může hrozit při komunikaci cestou internetu k dětem, k rodičům i širší veřejnosti“*.[165]

Zároveň MŠMT v tomto dokumentu uvedlo své rozhodnutí realizovat seznámení rodičů a široké veřejnosti pomocí „Pravidel pro děti k bezpečnějšímu užívání internetu“ a „Pravidel pro rodiče k bezpečnějšímu užívání internetu jejich dětmi“. Tímto rozhodnutím MŠMT chtělo přispět ke snížení rizik a ke zvýšení povědomí o těchto nebezpečích nejen u dětí, pedagogů a rodičů, ale i u celé veřejnosti. Níže jsou uvedena základní pravidla, která by děti a rodiče při práci s internetem měli vždy dodržovat.

---

[164] *Minimální preventivní program školní rok 2010/2011- ZŠ Karla IV.* [online]. 2010/2011. [cit. 2011-08-03]. Dostupné z WWW: <http://www.karlovka.cz/karlovka/skolni-poradenske-pracoviste/preventivni-program/>.

[165] PILAŘ, J. *Pravidla pro rodiče a děti k bezpečnějšímu užívání internetu, Čj.: 11691/2004 – 24.* [online]. Praha : MŠMT, 2004. 5 s. [cit. 2011-08-02]. Dostupné z WWW: <http://www.msmt.cz/file/7349_1_1/download/>. s. 2.

„PRAVIDLA PRO DĚTI K BEZPEČNĚJŠÍMU UŽÍVÁNÍ INTERNETU

1) *Nikdy nesděluj adresu svého bydliště, telefonní číslo domů nebo adresu školy, kam chodíš, jména a adresy rodičů a rodinných příslušníků i jejich telefonní čísla do práce, někomu, s kým jsi se seznámil/a prostřednictvím internetu, jestliže Ti to rodiče (nebo lidé, kteří se o Tebe starají) přímo nedovolí.*
2) *Pokud se neporadíš s rodiči, neposílej nikomu po internetu fotografii, číslo kreditní karty nebo podrobnosti o bankovním účtu a vůbec žádné osobní údaje.*
3) *Nikdy nikomu, ani nejlepšímu příteli, neprozraď heslo nebo přihlašovací jméno své internetové stránky nebo počítače.*
4) *Nikdy si bez svolení rodičů nedomlouvej osobní schůzku s někým, s kým jsi se seznámil/a prostřednictvím internetu. Doma musí bezpodmínečně vědět, kam jdeš a proč. I když Ti rodiče (nebo lidé, kteří se o Tebe starají) dovolí se s takovým člověkem sejít, nechoď na schůzku sám/sama a sejděte se na bezpečném veřejném místě.*
5) *Nikdy nepokračuj v chatování, když se Ti bude zdát, že se tam probírají věci, které Tě budou přivádět do rozpaků nebo Tě vyděsí. Vždy o takovém zážitku řekni rodičům (nebo lidem, kteří se o Tebe starají).*
6) *Nikdy neodpovídej na zlé, urážlivé, nevkusné nebo hrubé e-maily. Není Tvoje vina, že jsi tyto zprávy dostal/a. Když se Ti to stane, oznam to rodičům.*
7) *Nikdy neotvírej soubory přiložené k elektronickým zprávám (e-mailům), pokud přijdou od lidí nebo z míst, které neznáš. Mohou obsahovat viry nebo jiné programy, které by mohly zničit důležité informace a významně poškodit software počítače.*
8) *Vždy řekni rodičům (nebo lidem, kteří se o Tebe starají) o všech případech nepříjemných, vulgárních výrazů na internetu, totéž platí pro obrázky s vulgární tematikou.*
9) *Vždy buď sám/sama sebou a nezkoušej si hrát na někoho, kým nejsi (na staršího, na osobu jiného pohlaví apod.).*
10) *Vždy pamatuj na následující pravidlo a chovej se podle něho: jestliže některá webová stránka bude obsahovat upozornění, že je určena jen pro dospělé nebo jen pro lidi od určitého věku, musí se to respektovat a ti, kteří nevyhovují kritériím, nemají takovou stránku otevírat.*
11) *Domluv se s rodiči na pravidlech používání internetu a poctivě je dodržuj. Především se domluv, kdy můžeš internet používat a jak dlouho.*
12) *Provždy si zapamatuj další pravidlo: když Ti někdo na internetu bude nabízet něco, co zní tak lákavě, že se to nepodobá pravdě, nevěř mu – není to pravda.*

13) *Jestliže na internetu najdeš něco, o čem jsi přesvědčen, že je to nelegální, oznam to rodičům.“*[166]

V souvislosti s těmito pravidly byla v dokumentu uvedena informace o tom, že „*Pravidla pro děti k bezpečnějšímu užívání internetu lze využít v předmětech informatika, pracovní činnosti, rodinná výchova, občanská výchova a dalších naukových předmětech*“.[167] Šlo tedy o návod, jak seznámení s pravidly realizovat přímo ve výuce.

„PRAVIDLA PRO RODIČE K BEZPEČNĚJŠÍMU UŽÍVÁNÍ INTERNETU JEJICH DĚTMI

1) *Nechte se dítětem poučit o službách, které používá, a ujistěte se o jejich obsahu. Tím zlepšete svou znalost internetu.*
2) *Nikdy svému dítěti nedovolte setkání o samotě s někým, s kým se seznámilo na internetu, bez Vaší přítomnosti. Pokud k setkání svolíte, své dítě doprovoďte.*
3) *Zajímejte se o internetové kamarády svých dětí stejně, jako se zajímáte o jejich kamarády ve škole.*
4) *Základem při komunikaci rodiče s dítětem je otevřenost. Při nepříjemných zkušenostech dítěte s děsivým obsahem nebo nepříjemným člověkem není řešením trestat dítě nebo mu dokonce bránit používat internet, ale poradit mu, jak se v budoucnu nepříjemným zkušenostem vyhnout. Jak se rodič při podobné situaci zachová, určuje, zda se mu dítě svěří i v budoucnu.*
5) *Na místo s nevhodným obsahem se může dítě dostat zcela náhodou. Pro tyto případy neexistuje stoprocentní ochrana a vyplatí se spíše vychovávat dítě tak, aby si podobné skutečnosti interpretovalo způsobem odpovídajícím jeho věku, protože s dítětem nemůžete trávit všechen volný čas.*
6) *Riziko vstupu na stránku s nevhodným obsahem lze snížit jednak prostřednictvím možností zabudovaných přímo do internetového prohlížeče, jednak prostřednictvím speciálních programů obsahujících nepřetržitě aktualizovaný seznam stránek pro děti nevhodných. Tyto programy bývají k dispozici zdarma.*

[166] PILAŘ, J. *Pravidla pro rodiče a děti k bezpečnějšímu užívání internetu, Čj.: 11691/2004 – 24.* [online]. Praha : MŠMT, 2004. 5 s. [cit. 2011-08-02]. Dostupné z WWW: <http://www.msmt.cz/file/7349_1_1/download/>. s. 3.
[167] PILAŘ, J. *Pravidla pro rodiče a děti k bezpečnějšímu užívání internetu, Čj.: 11691/2004 – 24.* [online]. Praha : MŠMT, 2004. 5 s. [cit. 2011-08-02]. Dostupné z WWW: <http://www.msmt.cz/file/7349_1_1/download/>. s. 3.

7) *Uvažujte o společné e-mailové schránce se svými dětmi.*
8) *Dávejte si pozor na soubory, které dítě z internetu stahuje a ukládá je na disk.*
9) *Sledujte, kolik času dítě u počítače stráví. Nepohybuje se ve světě virtuálních her častěji než na hřišti? Nepohybuje se víc na chatu a nekomunikuje s anonymními osobami (skrytými za chatovými přezdívkami) častěji než se svými kamarády Nepozorujete u něj projevy připomínající závislost na chatování či počítačových hrách? Nedovolte, aby virtuální realita dítě příliš pohltila!*
10) *O radu při výchově dětí ke správnému užívání internetu můžete požádat pedagoga, psychologa či pracovníky internetových firem.“*[168]

Kvalita a kvantita informací poskytovaných v rámci prevence před rizikovými komunikačními jevy se však může na různých školách lišit a proto je důležité, aby rodiče nespoléhali pouze na vzdělávací soustavu, ale aby se sami aktivně snažili své děti na tato rizika upozornit a připravit.

Zvyšování informovanosti v rámci rodiny

Z hlediska tolik potřebné informovanosti dětí o nebezpečích číhající na internetu je nezbytné věnovat se uvedenému tématu nejen ve škole, ale především v rodině. „*Rodina je považována za nejdůležitější sociální skupinu, ve které člověk žije. V rodině dochází k uspokojování jeho potřeb, rodina poskytuje zázemí potřebné ke společenské seberealizaci, je zdrojem zkušeností a vzorců chování, které nemůže získat v jiném prostředí. Každá rodina je zdrojem specifického systému hodnot a jejich preference, ty ovlivňují chování členů rodiny v interakci se společenským okolím. Rodina formuje jedince v průběhu jeho vývoje, je významným nositelem jeho budoucích společenských rolí a identity obecně.“*[169]

Děti internet nejčastěji používají právě doma, a každý zodpovědný rodič si musí uvědomit, že na internetu není všechno jen dobré, a že pokud je dítě doma, zavřené ve svém pokoji u počítače, neznamená to, že je v bezpečí. Potřebné informace je dnes pro rodiče velmi snadné získat, a záleží tedy jen na nich, jak se k dané problematice postaví, a co pro bezpečí svého dítěte udělají.

[168] PILAŘ, J. *Pravidla pro rodiče a děti k bezpečnějšímu užívání internetu, Čj.: 11691/2004 – 24,* [online]. Praha : MŠMT, 2004. 5 s. [cit. 2011-08-02] Dostupné z WWW: <http://www.msmt.cz/file/7349_1_1/download/>. s. 3-5.
[169] FISCHER, S.; ŠKODA, J. *Speciální pedagogika : Edukace a rozvoj osob se somatickým, psychickým a sociálním znevýhodněním*. 1. vyd. Praha : Triton, 2008. 205 s. ISBN 978-80-7387-014-0. s. 187.

Jak uvádí Elliottová[170], *„neočekáváme, že by snad děti měly převzít odpovědnost za své bezpečí zcela do svých rukou. Odpovědnost spočívá především na nás – rodičích a vychovatelích. Avšak jejich je právo na bezpečí, a jsou to právě metody prevence, jež snižují jejich zranitelnost a pěstují v dětech více sebedůvěry.“* Zájmem každého rodiče by mělo být zajištění bezpečnosti jeho dítěte a podporování názoru, že není možné nechat děti v naprosté nevědomosti a napospas těmto internetovým nebezpečím. Komunikace rodičů s dětmi o rizicích spojených s využíváním internetu by tak pro děti měla být jedním z hlavních zdrojů informací o nebezpečích číhajících na internetu.

Ne všichni rodiče však ví, jaká nebezpečí jejich dětem při práci s internetem hrozí, a proto je nutné zvýšit jejich informovanost například prostřednictvím informací ze škol, kde už proběhlo školení dětí nebo učitelů na zmíněné téma. Existuje rovněž mnoho jiných informačních zdrojů, v současné době hlavně na různých internetových portálech, kde mohou rodiče potřebné informace získat. Další možnost jak získat informace nabízí také letáky distribuované mezi veřejnost, které varují před nebezpečími spojenými s používáním moderních komunikačních prostředků např. v rámci projektu E-Bezpečí s podporou MŠMT (viz přílohy č. 2 až 6). *„Ve veřejnosti dodnes přetrvává názor, že pachatelem sexuálního násilí je zpravidla sociálně izolovaný, nepřirozeně se chovající mužský jedinec, který dítěti v parku nabízí bonbony a láká ho do křoví. Toto nebezpečí je taky bohužel často jediné, před kterým je rodiči varováno a o kterém je v souvislosti s možností zneužití i poučeno.“*[171]

Rodiče by měli dítě nejen informovat, ale navodit s ním i pocit vzájemné důvěry, aby dítě mělo jistotu, že pokud bude potřebovat pomoc, může se bez obav rodičům svěřit, a najde u nich pomocnou ruku. *„Předpokladem toho, aby se nám dítě s týráním nebo zneužitím svěřilo, je vytvoření vzájemného důvěrného vztahu. Jedná se o vztah, v jehož rámci se dítě může bez obav svěřit se vším, co ho trápí, ale i s čímkoliv, co ho těší.“*[172]

Zásady pro rodiče

Díky skutečnosti, že se problematika nebezpečí číhajících při komunikaci přes internet stala velmi aktuální, začaly vznikat nejrůznější projekty, které se snaží těmto nebezpečím předcházet nebo je pomáhat řešit. V rámci projektů byly informace vztahující se k dané problematice zpracovány a shrnuty do několika užitečných rad, jak se chovat při komunikaci

[170] ELLIOTT, M. *Jak ochránit své dítě*. 1. vyd. Praha : Portál, 1995. 173 s. Rádci pro rodiče a vychovatele. ISBN 80-7178-034-0. s. 17.
[171] PÖTHE, P. *Dítě v ohrožení*. 2. rozšířené vydání. Praha : G plus G, 1999. 186 s. ISBN 80-8610-321-8. s. 53.
[172] PÖTHE, P. *Dítě v ohrožení*. 2. rozšířené vydání. Praha : G plus G, 1999. 186 s. ISBN 80-8610-321-8. s. 67.

na internetu, a jsou každému zájemci volně dostupné na internetu. Rady, co by pro snížení ohrožení svých dětí nebezpečími přicházejícími z prostředí kyberprostoru měli udělat rodiče, byly shrnuty do tzv. desatera pro rodiče, které je uvedeno níže.

„Desatero pro rodiče

1. *Převezměte zodpovědnost. Dítě od vás čeká zajištění bezpečí, proto je nutné mu jej poskytnout.*
2. *Vzdělávejte se. Vyhledávejte zdroje informací, zkoušejte nové věci, snažte se pochopit fungování počítačových programů.*
3. *Komunikujte s dětmi. Informujte se navzájem o výhodách používání počítače stejně jako o nebezpečích, která tato činnost s sebou nese.*
4. *Nastavte pravidla. Nadefinujte jasná pravidla, která je třeba za každých okolností dodržovat. Např. nesdělovat osobní informace či adresu.*
5. *Zajistěte dodržování pravidel. Každé pravidlo je účinné pouze v případě, že se dodržuje.*
6. *Mějte počítač ve společné místnosti. Neposkytujte dětem možnost porušovat pravidla tím, že jim dáte počítač k neomezenému fyzickému i časovému přístupu.*
7. *Využijte technologické nástroje. V mnoha počítačových programech můžete najít – pokud budete hledat – užitečné pomocníky. Třeba filtry nevyžádané pošty (spamu), kontrolu přístupu (k internetu) apod.*
8. *Mějte věci pod kontrolou. Máte-li mít zodpovědnost, mějte i pravomoci. Mějte administrátorský přístup k počítači, rozhodujte o to, jaké programy se budou či nebudou instalovat apod.*
9. *Nenechte děti volně se setkávat s internetovými přáteli. Každé podobné setkání v sobě nese velké riziko – klidně jej umožněte, ale přijměte odpovídající opatření.*
10. *Kontrolujte historii navštívených stránek na internetu. Stejně tak kontrolujte různé další výpisy: s kým dítě komunikuje, kdo mu posílá e-maily apod.“*[173]

[173] Desatero pro rodiče. *Internethotline* [online]. 10.7.2008. [cit. 2011-08-23]. Dostupné z WWW: <http://www.internethotline.cz/informace-pro-rodice/128-3.htm>.

Zásady pro děti

Byly stanoveny nejen výše uvedené zásady pro rodiče, ale také základní zásady, které by děti měly dodržovat při komunikaci s cizími lidmi přes internet. Všichni zájemci, a tedy nejen děti, ale i rodiče, je již mohou najít na mnoha internetových portálech, v informačních letácích a dalších zdrojích zabývajících se nebezpečnými internetovými aktivitami. Dodržování uvedených zásad komunikace by u dětí mělo vést k podstatnému snížení rizika toho, že se stanou například obětí útoku kybergroomera. To, co by měl mít jedinec při komunikaci přes internet vždy na paměti, je shrnuto v následujících bodech:

1. Je důležité nenechat se oklamat virtuálními útočníky, kteří mohou slibovat například porozumění, lásku, dárky, peníze a podobné lákavé věci. Online přátelé nemusí být ve skutečnosti těmi, za koho se vydávají. Úmysly virtuálních přátel nemusí být vždy dobré a mohou o nich záměrně lhát.
2. Vždy si ukládat kopie svých rozhovorů a znovu číst staré rozhovory, aby bylo možné rozpoznat jakékoliv nesrovnalosti v příběhu. Vždy je důležité důkladně přemýšlet o tom, co o sobě řekl neznámý člověk, se kterým se komunikuje přes internet. Pozorně sledovat a srovnávat to, co o sobě uvedl dříve, s tím, co uvádí později. Nepodceňovat případné nesrovnalosti v informacích, které o sobě uvádí, například ohledně jeho věku, toho kde bydlí a jaké má zájmy.
3. Zvažovat, proč někdo chce udržet vztah v tajnosti, nebo proč se ten na druhé straně ptá na otázky mimořádně osobního charakteru. Proč nechce, aby o něm věděl někdo další, nebo proč chce vědět intimní informace.
4. Držet se zpátky, když se v konverzaci vyskytnou otázky sexuální povahy a odmítat kybersex. Dopředu si stanovit hranici, do jaké míry bude přes internet rozebírat téma sexu a partnerských vztahů. Nikdy nepřijímat ani neposílat materiály se sexuální tématikou.
5. Neposkytovat osobní informace lidem, které jste právě potkali v online prostředí, na chatu, při užívání ICQ, Skype apod. Vždy si chránit své osobní údaje a nesdělovat je nikomu, kdo je může jakkoli zneužít. Neposkytovat nikdy osobní fotografie.
6. V žádném případě nechodit s kýmkoliv na osobní schůzku, o které by nevěděli rodiče.

7. Vždy pečlivě zvažovat co o sobě uživatel ostatním na internetu sděluje, s vědomím toho, že se některé informace mohou stát velice nebezpečnou zbraní v rukách útočníka, vůči dané osobě.[174]

Rodiče mohou zajištění bezpečnosti svých dětí proti útoku z kyberprostoru významným způsobem ovlivnit nejen využitím zmíněných užitečných rad, ale také tím, do jaké míry dítěti umožní pracovat s internetem, jaké podmínky dítěti pro práci s internetem vytvoří, a jak moc se budou o danou problematiku sami zajímat. Je naprosto přirozené, pokud rodiče mají obavy o bezpečí svých dětí a hledají možnosti, jak své děti ochránit. Dle Elliottové[175] je jednou z možností, jak rodiče mohou pomoci nejen sobě, ale i dětem od strachu z potenciálního nebezpečí, naučit své děti, jak se mají chovat v nebezpečných situacích.

[174] Kybergrooming. *E-Nebezpečí* [online]. 2010. [cit. 2011-08-24]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=11%3Aprehledovy-list-kybergrooming>.
[175] ELLIOTT, M. *Jak ochránit své dítě*. 1. vyd. Praha : Portál, 1995. 173 s. Rádci pro rodiče a vychovatele. ISBN 80-7178-034-0.

4 PROJEKTY NA OCHRANU DĚTÍ

V poslední době sehrávají důležitou roli v ochraně dětí před útoky kybergroomera mnohé projekty, které se zaměřují právě na oblast nebezpečných komunikačních jevů spojených s využíváním moderních komunikačních technologií. Vzniklé projekty ve většině případů prezentují a provádějí svoji činnost zejména prostřednictvím vlastních internetových portálů. Mimo to však existují i projekty, které směřují své aktivity i mimo internetové prostředí a rozšiřují svoji činnost například tím, že v jejich rámci se pořádají různá školení, přednášky, výzkumná šetření a další akce zaměřené na prevenci, osvětu a výzkum v dané oblasti. Vytvořené portály a informační materiály jednotlivých projektů se tak pro veřejnost stávají zdrojem mnoha důležitých informací. Nezřídka tyto projekty fungují i jako prostředníci pro kontakt s dalšími subjekty, které se zaměřují na stejnou problematiku, tj. na prevenci a na pomoc obětem útoků z kyberprostoru nebo na orgány zabývající se odhalováním pachatelů těchto nebezpečných aktivit. V následujícím textu jsou popsány některé z nich.

4.1 E-Bezpečí

E-Bezpečí je projekt zaměřený na nebezpečné komunikační jevy (hlavně na kyberšikanu, kybergrooming, sexting, hoax, spam, metody sociálního inženýrství, problematiku sdílení osobních údajů prostřednictvím sociálních sítí a další nebezpečné komunikační techniky), se kterými se mohou setkat uživatelé mobilních sítí a internetu. Je určen pro děti a mládež, rodiče, policisty, vychovatele a další osoby, které by se v rámci výkonu svého povolání mohly s uvedenou problematikou setkat. Vznikl v roce 2008 na Univerzitě Palackého v Olomouci. Spadá pod Centrum prevence rizikové virtuální komunikace PdF UP[176] (PRVoK[177]) a představuje jeden z klíčových projektů Pedagogické fakulty UP[178] v Olomouci. Je podporován různými účelovými dotacemi a granty (např. Statutárního města Olomouce, Olomouckého kraje, Ministerstva vnitra ČR, MŠMT, Fondu rozvoje vysokých škol, firmy Vodafone a dalších menších subjektů). Stěžejní činností projektového týmu jsou terénní práce, preventivní vzdělávací akce, různé formy přednášek,

[176] PdF UP – Pedagogická fakulta Univerzity Palackého.
[177] PRVoK – Centrum prevence rizikové virtuální komunikace.
[178] UP – Univerzita Palackého.

besedy, tvorba a distribuce informačních materiálů a provoz bezplatného online poradenského centra.

Velice důležitou činností projektového týmu je pořádání besed, na kterých jsou proškolováni žáci základních škol (již od 1. stupně ZŠ[179]), studenti středních škol a jejich učitelé. Besedy probíhají přímo ve školách, a jsou připraveny na základě modelových situací a skutečných případů online kriminality. Účastníci se dozvědí o konkrétních nebezpečných komunikačních praktikách, seznámí se s postupy, jak se těmto nebezpečným praktikám bránit a s informacemi, kam se v případě nouze obrátit s žádostí o pomoc. Velký zájem škol o přednášky lektorů projektu E-Bezpečí dokazuje počet jimi proškolených žáků. V červnu roku 2011 bylo lektory proškoleno už 10 472 žáků z různých škol v rámci celé České Republiky.

Mimo žáků a jejich učitelů jsou týmem lektorů projektu proškolováni i policisté a zástupci dalších profesí, u kterých lze předpokládat, že se na ně někdo, třeba dítě nebo rodiče, obrátí s žádostí o radu nebo pomoc v souvislosti s nebezpečnými komunikačními aktivitami. Na zmiňovaných přednáškách jsou proto účastníci informováni tak, aby získali potřebné vědomosti a celkový přehled v uvedené problematice. Vysoký zájem mezi zástupci uvedených profesí opět dokazuje počet proškolených účastníků. Ke konci června 2011 bylo proškoleno 642 učitelů a 552 policistů.

Další činností projektu E-Bezpečí je realizace pravidelných celorepublikových výzkumných šetření zaměřených na problematiku rizikové komunikace uživatelů internetu a mobilních telefonů. Výsledky výzkumů jsou zveřejňovány na webových stránkách projektu, kde se s nimi může seznámit široká veřejnost.

Jak autoři projektu uvádí na svých internetových stránkách, úkolem projektu není zakazovat či hlídat činnost dětí při práci s internetem nebo mobilem, ale podporovat zdravou a zodpovědnou práci s těmito komunikačními prostředky.

V současnosti je projekt E-Bezpečí velice dobře fungujícím preventivním projektem, díky kterému má velké množství uživatelů nových komunikačních prostředků možnost dozvědět se, že existují nebezpečné jevy v online prostředí, jak se proti nim bránit, a pokud se již někdo obětí stal, najde zde pomoc.

Informace projektu jsou na stránkách www.e-bezpeci.cz a na www.napisnam.cz.

[179] ZŠ – základní škola.

Adresa a kontakty projektu:

Projekt E-Bezpečí – Centrum prevence rizikové virtuální komunikace

Pedagogická fakulta Univerzity Palackého v Olomouci, Žižkovo nám. 5, 771 40 Olomouc

Kontakt:

Mgr. Kamil Kopecký, Ph.D. (Management projektu)

Mobil: +420 773 470 997, E-mail: info@e-bezpeci.cz

4.2 Centrum prevence rizikové virtuální komunikace

Centrum prevence rizikové virtuální komunikace (PRVoK) vzniklo v roce 2009 a navazuje na činnosti projektu E-Bezpečí. Je provozováno Katedrou českého jazyka a literatury ve spolupráci s dalšími katedrami a ústavy Pedagogické fakulty Univerzity Palackého v Olomouci. Spolupracuje s Ministerstvem vnitra ČR a MŠMT. Hlavní činností centra je preventivní působení v oblasti rizikového chování při využívání ICT. Centrum se zaměřuje hlavně na kybergrooming, kyberstalking, kyberšikanu, hoax, spam, sexting, metody sociálního inženýrství, problematiku sdílení osobních údajů prostřednictvím sociálních sítí a další nebezpečné komunikační techniky.

Prostřednictvím Centra je uskutečňována primární, viktimní[180] a situační prevence.[181] V rámci primární prevence realizuje vzdělávací programy pro školy, veřejnost, studenty, učitele, policisty a pracovníky orgánů sociálně právní ochrany. Dále realizuje preventivní programy pro školy, zabývá se intervencí a provádí výzkumná šetření zaměřená na analýzu přítomnosti nebezpečných jevů na konkrétních školách.

Pedagogická fakulta projekt zajišťuje ve spolupráci s dalšími specializovanými institucemi, například s Preventivně-informační skupinou Policie ČR Olomouc a Odborem prevence kriminality Ministerstva vnitra ČR. Hlavním komerčním partnerem Centra je firma Vodafone Czech, a.s.[182] Regionálním mediálním partnerem je Český rozhlas Olomouc.

Centrum rovněž provozuje online poradnu, má vlastní rozhlasový pořad o rizicích internetu a podílí se na desítkách dalších aktivit pro různé instituce.

[180] viktimní prevence – zaměřuje se na to, jak se nestát obětí trestného činu.

[181] situační prevence – zaměřuje se na odstraňování příležitostí, podmínek a situací, které vedou pachatele k protiprávnímu jednání.

[182] a.s. – akciová společnost (dále jen „a.s.“).

Kontakt:
Centrum prevence rizikové virtuální komunikace
Pedagogická fakulta Univerzity Palackého v Olomouci, Žižkovo nám. 5, 771 40 Olomouc
Webové stránky: www.prvok.upol.cz
Vedoucí centra: Mgr. Kamil Kopecký, Ph.D.
E-mail: kamil.kopecky@upol.cz, Telefon: +420 585 635 601, Mobil: +420 773 470 997

4.3 E-Nebezpečí

Vzdělávací projekt E-Nebezpeci.cz je určen učitelům všech typů škol. Zaměřuje se zejména na nebezpečné jevy, jako je kyberšikana, sexting, kybergrooming, kyberstalking, stalking, zneužití osobních údajů v rámci Internetu, problematika zneužití sociálních sítí a na prevenci kriminality u dětí a mládeže. Úkolem projektu je seznamovat učitele s rizikovým chováním a nebezpečími na internetu, vzdělávat je a pomáhat jim získávat zkušenosti v oblasti problematiky nebezpečných jevů spojených s používáním ICT, tak aby tyto informace mohli následně využít při práci s dětmi. Tým realizátorů projektu tvoří experti na danou problematiku, členové projektu E-Bezpečí a pracovníci Preventivně informační skupiny Policie ČR Olomouc. V rámci projektu jsou realizované akreditované vzdělávací akce, během kterých jsou účastníkům kromě informací a rad poskytovány i nejrůznější informační materiály například právní rozbory, přehledové listy, brožury a pracovní materiály. Projekt realizuje Univerzita Palackého v Olomouci. Webové stránky projektu jsou dostupné na www.e-nebezpeci.cz.

4.4 Saferinternet

Jedním z dalších projektů zabývajícím se nebezpečnými jevy na internetu je projekt Saferinternet, který zahájil svoji činnost v roce 2005. Počátkem roku 2007 byl přejmenován na CZESICON (CZEch Safer Internet COmbined Node – Osvětové centrum pro bezpečnější internet v České republice). Realizuje jej Národní centrum bezpečnějšího internetu, které je členem celoevropské sítě národních osvětových center bezpečnějšího internetu INSAFE a mezinárodní sítě horkých linek INHOPE.

Úkolem projektu je bojovat proti šíření ilegálního a škodlivého (např. pornografického, extremistického) obsahu na internetu, upozorňovat na tyto jevy, zvyšovat povědomí uživatelů o bezpečném užívání internetu, podporovat vzdělávání, výzkum a prevenci v této oblasti. Cílem projektu je podporovat a propagovat zodpovědné chování uživatele na internetu a provádět osvětovou činnost v oblasti bezpečnějšího internetu. Ve spolupráci s partnery (neziskové organizace Sdružení Linka bezpečí a Online Safety Institute) jsou pořádány přednášky, školení, semináře a konference se zaměřením na prevenci internetové kriminality a na bezpečné užívání internetu. Projekt se také snaží sledovat nové trendy v oblasti online technologií a informovat o rizicích s nimi spojenými.

Projektový tým tvoří 4 organizace. *CZI, s.r.o.*[183] (jako koordinátor), *Nadace Naše dítě* (Internet Hotline), *Sdružení Linka bezpečí* (Internet Helpline) a *Software602* (osvětové centrum). Projekt CSESICON spolupracuje se stejně zaměřenými evropskými sítěmi INSAFE a INHOPE.

Komerčním partnerem projektu je například Google Česká republika, Microsoft Česká republika, Telefónica O2 Czech republic a.s., Poštovní spořitelna, T-Mobile Czech republic a.s., Vodafone Czech republic a.s. Odborným partnerem je Ústav pro informace ve vzdělávání.

Kontakt:
Saferinternet.cz -Národní centrum bezpečnějšího internetu
Svornosti 30, 150 00 Praha 5
Ing. Pavel Vichtera (koordinátor projektu)
Tel: +420 734 709 025, Fax: +420 257 328 684, E-mail: vichtera@saferinternet.cz
Webové stránky projektu: www.saferinternet.cz

Na projektu se podílí tyto 4 subjekty: Bezpečně online, Linka pomoci, Horká linka, Online Safety Institute.

4.4.1 Bezpečně online

Jedná se o výchovně - vzdělávací stránky určené pro mládež ve věku 12-17 let, jejich rodiče a učitele, které byly spuštěny v únoru 2010. Jejich cílem je poskytnout uživatelům internetu informace v oblasti bezpečného používání bankovních online služeb, aktivní

[183] s.r.o. – společnost s ručením omezeným (dále jen „s.r.o.“).

ochrany soukromých informací před zneužitím a efektivního využívání možností IT.[184] Návštěvníci stránek se mohou zúčastnit různých kvízů a soutěží, zapojit se do diskuze prostřednictvím diskusního fóra, využít zde nabízených poradenských služeb. Učitelé a další zájemci na stránkách naleznou výukové materiály, slovník pojmů, prezentace ze seminářů, brožury, videa a další materiály související s danou problematikou. Stránky jsou dostupné na adrese www.bezpecne-online.cz.

4.4.2 Pomoc online (Internet Helpline)

Uvedené krizové centrum zahájilo svoji činnost počátkem roku 2007 v rámci akreditované sociální služby TKI[185] (telefonické krizové intervence) a má za úkol pomáhat především dětským a dospívajícím obětem internetové kriminality a v rámci prevence realizovat kampaně zaměřené na děti a jejich rodiče, s cílem seznamovat a upozorňovat je na potenciální rizika internetové komunikace. Na bezplatnou nonstop krizovou linku pomoci se mohou obracet také děti, které se cítí znepokojené nebo ohrožené při využívání internetu, např. při chatování, hraní her, prohlížení stránek, nebo jsou obtěžovány prostřednictvím internetu nebo mobilu. Linku bezpečí je možné kontaktovat telefonicky, pomocí chatu nebo e-mailu. Informace o Lince bezpečí a jejích aktivitách jsou dostupné na internetových stránkách www.pomoconline.cz.

Kontakt:
Telefon: 116 111, E-mail: pomoc@linkabezpeci.cz
Chat: xchat.centrum.cz/lb/

4.4.3 Horká linka

Jedná se o kontaktní centrum, kam mohou uživatelé internetu nahlásit stránky se závadným a škodlivým obsahem. Hlavním cílem je bránit rozšiřování obrazového materiálu se zneužívanými dětmi a dalšího nezákonného a nevhodného obsahu na internetu. Horkou linku realizuje Národní centrum bezpečnějšího internetu. Provozuje ji CZI, s.r.o. a koordinátorem projektu je Ing. Pavel Vichtera. Hlášení je možné podat pomocí formuláře,

[184] Information Technologies – informační technologie.
[185] TKI – telefonická krizová intervence.

e-mailu nebo tzv. Červeného tlačítka, což je projekt, který vytvořilo České centrum bezpečnějšího internetu. **Červené tlačítko** představuje volně dostupnou a volně šiřitelnou aplikaci, která integruje do internetového prohlížeče tlačítko, jehož jediným stiskem může uživatel na horkou linku zaslat hlášení o stránce se závadným obsahem. Cílem Červeného tlačítka je zjednodušit proces nahlášení závadného obsahu. Po nahlášení uživatelem je závažnost stránky posouzena a vyhodnocena odborníky. Podle míry závažnosti se pak tito vyškolení odborníci následně rozhodnou, jak s takovou informací dále naloží, zda ji předají mobilnímu operátorovi, provozovateli internetových služeb nebo ji sdělí přímo Policii ČR. V případě, že se jedná o stránky ze zahraničí, předají informace příslušné zahraniční horké lince, nebo Interpolu. Horká linka usiluje nejen o to, aby se o závadných stránkách na internetu vědělo, ale hlavně aby bylo zajištěno jejich odstranění.

Projekt Červené tlačítko je spolufinancován Evropskou unií. Mezi partnery projektu patří Saferinternet, Policie České republiky a Výbor pro práva dítěte Rady vlády ČR. Horká linka je od roku 2010 členem INHOPE, což je mezinárodní organizace, sdružující horké linky z celého světa. Další informace o projektu Červené tlačítko jsou umístěné na internetové adrese www.cervenetlacitko.saferinternet.cz.

Kontakt:
E-mail: ohlaste@horkalinka.cz
Webové stránky projektu: www.horka-linka.saferinternet.cz; www.horka-linka.cz;

4.4.4 Osvětové centrum (Online Safety Institute)

Osvětové centrum bylo založeno v prosinci 2006, je neziskovým subjektem a je odpovědné za provoz portálu Saferinternet.cz. Jeho hlavním úkolem je zvyšovat informovanost o přednostech, ale i o možných nebezpečích internetu, podpořit studium problematiky bezpečnějšího internetu a online bezpečnosti, vytvořit dokumentační středisko osvědčených postupů, bojovat proti internetové kriminalitě, šíření dětské pornografie, rasismu, xenofobii, extremismu a proti kybernetické šikaně. Hlavním jeho cílem je zformovat jednotné koordinační centrum, které se bude věnovat otázkám bezpečnějšího internetu, studiu internetu a jeho popularizaci. Ve spolupráci s různými partnery organizuje přednášky, semináře, výchovně-vzdělávací soutěže, školení a konference zaměřené na sociální a psychologická rizika internetu a na prevenci internetové kriminality. Centrum podporuje

a vytváří podmínky pro vzájemnou spolupráci veřejné správy, podnikatelské sféry, škol, veřejných knihoven, nevládních organizací a neziskového sektoru. Stránky Online Safety Institute jsou dostupné na adrese www.osi.cz.

4.5 Preventivně informační centrum Policie České republiky

Preventivně informační centrum Policie České republiky provozuje od 4.2.2011 Preventivně informační skupina Hradec Králové v prostorách budovy Policie ČR v Hradci Králové. Centrum pořádá ve svém sídle přednášky pro různé skupiny veřejnosti (předškolní děti, žáky, mládež, rodiče, cyklisty, seniory, chataře, atd.). Tématem přednášek jsou různé rizikové jevy ohrožující uvedené skupiny obyvatelstva (bezpečnost v silničním provozu, ochrana zdraví a majetku, šikana, chování v rizikových situacích a další témata). Pro žáky základních a středních škol pořádá centrum přednášky speciálně zaměřené na nebezpečí virtuální komunikace, jakým je například kyberšikana a kybergrooming. Přednášky jsou doplněny multimediálními prezentacemi a účastníci se při nich mohou seznámit i s konkrétními případy z praxe. Za velmi přínosné lze považovat nejen to, že se centrum snaží nenásilnou a zajímavou formou preventivně působit na veřejnost, ale i to, že přednášky a veškeré informační materiály jsou všem zájemcům poskytovány zdarma.

Kontakt:
Policie České republiky - Preventivně informační skupina Hradec Králové
Mrštíkova 541, 500 09 Hradec Králové
nprap. Jan Čížkovský (vrchní inspektor)
Tel: 974 526 209, E-mail: tiskhk@mvcr.cz;
Webové stránky projektu: www.policie.cz

4.6 Seznam se bezpečně

Seznam se bezpečně je projektem serveru Seznam.cz. Jedná se o třicetiminutový film věnovaný problematice internetových nebezpečí. Jeho vzniku předcházela velice úspěšná konference učitelů, kterou v Praze koncem roku 2008 pořádal server Seznam.cz. Na této konferenci se snažil účastníkům přiblížit rizika, která dětem hrozí na internetu. Na základě velmi kladného ohlasu a zájmu učitelů o uvedenou problematiku se organizátoři rozhodli

natočit film na téma nebezpečné komunikace na internetu. Film byl natočený ve spolupráci s Nadací Naše dítě, Linkou bezpečí a Policejním prezidiem. Je určený pro děti ve věku 12 - 16 roků, jejich rodiče a učitele. Filmem provází Mirek Vaňura, známý z pořadu 112. Pomocí třech příběhů natočených podle skutečných událostí se snaží přiblížit divákům rizika spojená s komunikací na internetu a zároveň jim nabízí informace, jak se v případě ohrožení zachovat a jak takovou situaci řešit, včetně kontaktů na Linku bezpečí a Policii ČR. Film je zdarma distribuován do všech základních škol v ČR.

Informace o projektu a video je možné nalézt na stránkách www.seznamsebezpecne.cz. Na těchto stránkách je zveřejněno desatero bezpečného internetu, které představuje rady, jak jednoduchým, ale účinným způsobem snížit rizika přicházející z kyberprostoru. Jsou zde rovněž uvedeny důležité odkazy, pomocí kterých mohou uživatelé zareagovat na stránky se závadným obsahem. Tyto odkazy jim umožňují obsah oznámit přímo na policii, nebo stránky pouze nahlásit. Je zde i třetí možnost, kterou mohou zvolit ti uživatelé, kteří jsou znepokojeni nebo rozrušeni obsahem takových stránek, a chtějí požádat o radu a pomoc.

Kontakt:
E-mail: seznamsebezpecne@firma.seznam.cz
Webové stránky projektu: www.seznamsebezpecne.cz

4.7 Internet Hotline

Internet Hotline vznikla jako první česká internetová horká linka. Její zkušební provoz zahájila Nadace Naše dítě v roce 2007 v rámci projektu CSESICON za podpory grantu poskytnutého z fondu Evropské komise. Na stránkách Internet Hotline je možné pomocí jednoduchého formuláře anonymně nahlásit závadný nebo nevhodný obsah umístěný na internetu. Tato přijatá oznámení jsou na Internet Hotline zařazována do databáze a následně vyhodnocována proškolenými odborníky. V případě, že posuzovatelé dojdou k závěru, že obsah nahlášených internetových stránek může porušovat právní předpisy České republiky, předávají toto oznámení Policii ČR, vedeni snahou dosáhnout odstranění takového závadného obsahu z internetu.

Stránky kromě možnosti nahlašovat závadný obsah na internetu obsahují také rady pro děti, mládež, rodiče a pedagogy, a to včetně nejrůznějších informačních a vzdělávacích

materiálů vztahujících se k problematice související s využíváním internetu (informace o síti INHOPE, tiskové zprávy, informace pro novináře, statistiky, plakáty, letáky). Na stránkách jsou rovněž uváděny příklady kauz spojených se zneužíváním internetu.

Od roku 2009 linku Internet Hotline financuje Nadace Naše dítě a provozuje ji ve spolupráci s Policií České republiky. Internet Hotline spolupracuje s horkými linkami v zahraničí, vzájemně si s nimi předává informace o závadném obsahu na internetu a podniká kroky k odstranění těchto stránek. V současné době je členem mezinárodní sítě horkých linek INHOPE. Stránky Internet Hotline jsou dostupné na www.internethotline.cz.

Kontakt:
Internet Hotline Nadace Naše dítě
E-mail: info@internethotline.cz., Telefon: +420 266 727 999, Fax: + 420 266 727 911

4.8 Nebuď oběť

Nebuď oběť je zkrácený název, který používá občanské sdružení Rizika internetu a komunikačních technologií. Věnuje se primární prevenci dětí, rodičů a pedagogů v oblasti bezpečného používání moderních komunikačních technologií. Sdružení se zaměřuje na nebezpečné jevy, jakými jsou například kyberšikana, kybergrooming, sexting, stalking, happy slapping nebo netolismus.[186] Pro veřejnost pořádá semináře s názvem Bezpečný internet, během kterých se účastníci seznámí s novými druhy nebezpečí souvisejícími s používáním internetu a komunikačních technologií, a zároveň jsou informováni, jak se těmto nebezpečím bránit.

Od září 2010 sdružení organizuje putovní výstavu po ostravských školách. Výstava má název Nebuď oběť a jejím ústředním tématem je bezpečné chování žáků při práci s internetem. V rámci výstavy je ve školách umístěno 5 samostatně stojících informačních panelů, které mohou učitelé využít ve výuce, při seznamování žáků s uvedenou problematikou. Na výstavu na dané škole ještě navazuje seminář nazvaný Rizika internetu a komunikačních technologií, pořádaný organizátory výstavy. V rámci semináře žáci vyplňují dotazníky, na základě kterých může škola získat přehled o tom, jakou měrou jsou její žáci ohroženi nebezpečnými jevy.

[186] netolismus – závislost na tzv. virtuálních drogách, mezi které patří internet, počítačové hry, televize, videa apod.

Uvedenou problematiku se sdružení snaží mladým uživatelům přiblížit zábavným způsobem, například formou komiksů. Věnuje se také natáčení videoklipů na téma jednotlivých druhů nebezpečí a na téma sdělování osobních dat na internetu a jejich následného zneužití. Na stránkách sdružení funguje poradna, kam mohou uživatelé vznést svůj dotaz a zároveň vyhledat odpovědi na otázky již dříve řešené. Součástí stránek jsou i odkazy na různé články nebo portály, věnující se podobným problémům. Sdružení podporuje Statutární město Ostrava, Národní agentura pro vzdělávací programy, Knihovna města Ostravy a společnost Alvit – inovace a vzdělání s.r.o. Stránky sdružení jsou k dispozici na www.nebudobet.cz.

Kontakt:
Předseda o. s. Nebuď oběť
Martin Pokorný
E-mail: martin.pokorny@alvit.cz

PRAKTICKÁ ČÁST

5 ÚVOD DO VÝZKUMU

Problematika nebezpečných jevů na internetu je v současné době velmi aktuální. Na jedné straně jsou stále častěji v médiích zveřejňovány případy, kdy se někdo stal obětí kybergroomingu nebo jiné nebezpečné aktivity spojené s využíváním moderních komunikačních technologií, a na straně druhé o sobě stále více dávají vědět nejrůznější projekty zabývající se těmito jevy, ať už z hlediska prevence nebo i z hlediska řešení problémů vzniklých v souvislosti s novými komunikačními prostředky. Přitom stále existují lidé, kteří ani netuší, že jim hrozí nějaké nebezpečí při komunikaci s neznámým člověkem na internetu. Bezstarostně poskytují na internetu své osobní údaje, komunikují s neznámými osobami a nechávají se informacemi od těchto osob z internetu ovlivňovat. Nejjednodušší způsob, jak může každý zmenšit riziko napadení na internetu, je snažit se nebezpečím předcházet, to znamená být obezřetný, nesdělovat osobní informace neznámým lidem, nenechat se vydírat a ovlivňovat, a v případě sebemenšího pocitu nebezpečí nebo pocitu nedůvěry během komunikace ihned rizikovou komunikaci ukončit. Problémem, na který se výzkumné šetření v diplomové práci zaměřuje, je bezpečnost chování dětí na internetu.

5.1 Cíl výzkumu

Cílem praktické části diplomové práce je zmapovat, jak bezpečně se žáci 2. stupně základní školy chovají na internetu. Dílčími cíli je zjistit, jestli existují u předem stanovených věkových skupin statisticky významné rozdíly v počtu jedinců ochotných jít na osobní schůzku s člověkem, kterého by znali jen přes internet, a zda jsou mezi předem danými věkovými skupinami statisticky významné rozdíly v počtu jedinců ochotných sdělit tajemství člověku, kterého by znali jen přes internet.

5.2 Výzkumné otázky a hypotézy

Na základě výzkumného problému a stanoveného cíle jsme formulovali následující výzkumné otázky a hypotézy.

Otázka 1:
Existují u předem stanovených věkových skupin statisticky významné rozdíly v počtu jedinců ochotných jít na osobní schůzku s člověkem, kterého by znali jen přes internet?

Předpoklad
Podíl osob ochotných jít na schůzku s člověkem, kterého by znaly jen přes internet, je u věkových skupin různý.

$H1_0$ - Mezi věkovými skupinami nejsou statisticky významné rozdíly co do podílu osob ochotných jít na osobní schůzku s člověkem, kterého by znaly jen přes internet.

$H1_A$ - Podíl osob ochotných jít na osobní schůzku s člověkem, kterého by znaly jen přes internet, je u uvedených věkových skupin různý.

Otázka 2:
Jsou mezi předem danými věkovými skupinami statisticky významné rozdíly v počtu jedinců ochotných sdělit tajemství člověku, kterého by znali jen přes internet?

Předpoklad
Mezi věkovými skupinami nejsou statisticky významné rozdíly co do podílu osob ochotných sdělit tajemství člověku, kterého by znaly jen přes internet.

$H2_0$ - Mezi věkovými skupinami nejsou statisticky významné rozdíly co do podílu osob ochotných sdělit tajemství člověku, kterého by znaly jen přes internet.

$H2_A$ - Podíl osob ochotných sdělit tajemství člověku, kterého by znaly jen přes internet, je u uvedených věkových skupin různý.

Stanovené hypotézy budou ověřovány statistickým testem dobré shody chí-kvadrát, jelikož pomocí statistických testů významnosti se ověřuje, jestli se četnosti, které byly získány měřením v pedagogické realitě, významně odlišují od teoretických četností, které odpovídají

dané nulové hypotéze. Pokud je výsledek výzkumu statisticky významný, pak můžeme říci, že je velmi nepravděpodobné, že by byl způsoben pouhou náhodou. *„Jinak řečeno, statisticky významný výsledek již nelze připsat pouze na vrub náhody.“*[187] Test dobré shody chí-kvadrát stejně jako ostatní testy významnosti začíná formulováním nulové a alternativní hypotézy. *Nulová hypotéza* označovaná jako H_0 je předpoklad, že mezi sledovanými jevy není vztah (rozdíl, souvislost). *Alternativní hypotéza* označovaná jako H_A, nebo H_1 je naopak předpoklad, že mezi sledovanými jevy je vztah (rozdíl, souvislost). O přijetí, nebo odmítnutí stanovených hypotéz rozhodneme na základě testování nulové hypotézy. K uvedenému účelu se zpravidla vypočítá tzv. *testové kritérium* χ^2, což je určitá číselná charakteristika odvozená ze zjištěných dat, která je ukazatelem rozdílu mezi pozorovanou a očekávanou četností. Jak uvádí Chráska[188], *„při rozhodování o platnosti nulové hypotézy zpravidla postupujeme tak, že vypočítanou hodnotu testového kritéria srovnáváme s tzv. kritickou hodnotou“*.

Kritickou hodnotu stanovujeme pro zvolenou hladinu významnosti a stupeň volnosti přičemž *hladina významnosti* představuje pravděpodobnost, že neoprávněně (nesprávně) odmítneme nulovou hypotézu. Ve většině pedagogických výzkumů se pracuje na hladině významnosti 0,05 (5 %), nebo 0,01 (1 %). Počet *stupňů volnosti* je pak stanoven na základě počtu řádků v tabulce, z níž bylo kritérium chí-kvadrát vypočítáno.

Vzorec pro výpočet testového kritéria χ^2

$$\chi^2 = \sum \frac{(P-O)^2}{O}$$

χ^2	-	testové kritérium chí-kvadrát
P	-	pozorovaná četnost
O	-	očekávaná četnost

5.3 Výzkumná metodologie

Jako výzkumný způsob jsme zvolili kvantitativní výzkum formou anonymního dotazníku. V pedagogickém výzkumu je dotazník velmi často používanou metodou k získání

[187] CHRÁSKA, M. *Úvod do výzkumu v pedagogice*. 2. vyd. Olomouc : Univerzita Palackého v Olomouci, 2006. 200 s. ISBN 80-244-1367-1. s. 82.
[188] CHRÁSKA, M. *Metody pedagogického výzkumu : základy kvantitativního výzkumu : vědecký výzkum a analyzování, statistické metody, výhody a nevýhody kvantitativního přístupu, měření v pedagogickém výzkumu, metody zpracování výsledků, sběr dat.* 1. vyd. Praha : Grada, 2007. 265 s. ISBN 978-80-247-1369-4. s. 72.

dat od respondentů. Dle Chrásky[189] se v případě dotazníku jedná o soustavu *„předem připravených a pečlivě formulovaných otázek, které jsou promyšleně seřazeny a na které dotazovaná osoba (respondent) odpovídá písemně“*. Za nespornou výhodu dotazníku můžeme považovat tu skutečnost, že jeho prostřednictvím lze nashromáždit velké množství dat, a to za krátkou dobu s nízkými vstupními náklady. Distribuci dotazníků lze provést poštou, osobně nebo zprostředkovaně přes jiné osoby. Z hlediska návratnosti se jako nejvýhodnější jeví osobní předání dotazníku respondentovi a po vyplnění jeho opětovné vyzvednutí. Při takovém způsobu distribuce se návratnost dotazníků blíží 100 %. Při zasílání dotazníků poštou je velkou nevýhodou jejich malá návratnost, která se pohybuje mezi 30-60 %. Další nevýhodou je, že respondenti nemusí vždy představovat reprezentativní vzorek, jaký je potřebný u daného výzkumu. Aby byli respondenti ochotni v dotaznících odpovídat pravdivě, musí mít jistotu, že zjištěné údaje nebudou nějakým způsobem zneužity. V tomto směru se jako nejlepší jeví dotazník anonymní. Na druhou stranu je však nutné poznamenat, že v některých případech právě anonymita dotazníku svádí respondenty k odpovědím scestným nebo recesním.[190]

Před vlastní tvorbou autorského dotazníku jsme provedli pilotáž, v jejímž rámci jsme ústně oslovili několik žáků 2. stupně základních škol, abychom dopředu zmapovali, do jaké míry je jim znám pojem „kybergrooming“. Během rozhovoru s těmito oslovenými žáky jsme zjistili, že někteří z nich tento pojem sice znali, ale téměř nikdo nevěděl, co přesně označuje. Z toho důvodu jsme se rozhodli v dotazníku nezmiňovat přímo pojem „kybergrooming“, ale zaměřit se na ty oblasti, které s kybergroomingem nějakým způsobem souvisí. Ze strany kybergroomerů jsou to zejména pokusy o manipulaci s vyhlédnutou obětí a ze strany potenciální oběti například ochota sdělovat osobní informace neznámým lidem na internetu nebo ochota sejít se s osobou známou pouze prostřednictvím internetu.

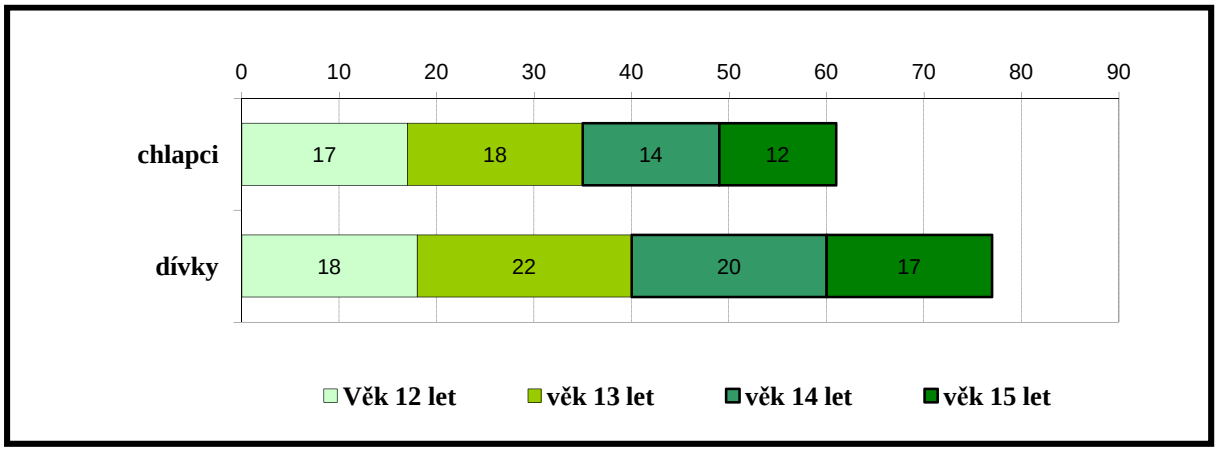
S vědomím všech výše uvedených skutečností jsme vytvořili autorský dotazník. Dotazník byl sestaven ze 17 otázek, jejichž znění jsme konzultovali s vedoucí diplomové práce, PhDr. Lindou Švrčinovou, a odborníkem na problematiku nebezpečných komunikačních jevů, Mgr. Kamilem Kopeckým Ph.D. Na základě jejich odborných informací a připomínek byl dotazník upraven a připraven k použití pro provedení kvantitativního šetření.

[189] CHRÁSKA, M. *Metody pedagogického výzkumu : základy kvantitativního výzkumu : vědecký výzkum a analyzování, statistické metody, výhody a nevýhody kvantitativního přístupu, měření v pedagogickém výzkumu, metody zpracování výsledků, sběr dat.* 1. vyd. Praha : Grada, 2007. 265 s. ISBN 978-80-247-1369-4. s. 163.
[190] CHRÁSKA, M. *Metody pedagogického výzkumu : základy kvantitativního výzkumu : vědecký výzkum a analyzování, statistické metody, výhody a nevýhody kvantitativního přístupu, měření v pedagogickém výzkumu, metody zpracování výsledků, sběr dat.* 1. vyd. Praha : Grada, 2007. 265 s. ISBN 978-80-247-1369-4.

V úvodu dotazníku zjišťujeme od respondentů základní údaje, mezi které patří věk, pohlaví a třída, kterou respondent navštěvuje. Dalšími položkami v dotazníku jsou otázky již přímo zaměřené do oblasti nebezpečných komunikačních aktivit. Dotazník obsahuje otázky uzavřené a otázky polouzavřené. Použitý dotazník je přiložen v přílohách této diplomové práce (viz příloha č. 1).

5.4 Charakteristika respondentů

Zkoumaný vzorek tvořilo 138 žáků 2. stupně dvou vybraných základních škol. Jednalo se tedy o žáky navštěvující 6., 7., 8. a 9. třídu. Věková skladba respondentů byla 12, 13, 14 a 15 let. Jak znázorňuje graf č. 6, z celkového počtu 138 respondentů bylo 61 chlapců a 77 dívek. Graf zobrazuje také věkové rozvrstvení respondentů podle pohlaví.



Graf č. 6 - Věkové rozvrstvení respondentů podle pohlaví.

5.5 Realizace výzkumu

Před finální distribucí dotazníku byl proveden předvýzkum na vzorku 30 respondentů. Pomocí něj jsme zejména ověřovali vytvořený autorský dotazník, přičemž jsme se zaměřili na to, zda neobsahuje případné nedostatky spočívající například v zadání otázek nebo v možnostech jednotlivých odpovědí. Díky provedenému předvýzkumu a na základě poznámek zúčastněných respondentů tak byly odstraněny drobné nejasnosti, které se vyskytly v zadání otázek. Upravený dotazník byl distribuován žákům vybraných základních škol. Distribuce probíhala formou zprostředkovaného rozdání a sběru vyplněných dotazníků. Uvedené předání dotazníků bylo zvoleno z důvodu zajištění jejich větší návratnosti.

Samotný sběr dat proběhl v měsíci červnu 2011 na 2. stupni Fakultní základní školy Tererova a na 2. stupni Fakultní základní školy Helsinská v Olomouci. Předání dotazníků žákům a jejich vyplnění bylo zajištěno přes zástupce ředitele školy. Oslovený zástupce ředitele školy vždy předal třídním učitelům dotazníky v množství odpovídajícím počtu žáků dané třídy. Třídní učitelé dotazníky žákům rozdali, po vyplnění posbírali a předali zpět zástupci školy. Zde uložené dotazníky jsme následně v předem domluvený den vyzvedli. Návratnost byla vysoká, ze 164 respondentům rozdaných dotazníků se nám jich vrátilo 162, což je 98,78 %. Vyzvednuté vyplněné dotazníky jsme prověřili na úplnost údajů. Po provedené kontrole úplnosti jsme museli 24 dotazníků vyřadit z konečného zpracování. Důvodem k jejich vyřazení bylo to, že část dotazníků (7) neobsahovala všechny námi požadované údaje o respondentovi, v některých dotaznících nebyly zodpovězeny všechny kladené otázky (14) a u třech dotazníků došlo ke kombinaci těchto nedostatků. Zbývajících 138 kompletně vyplněných dotazníků bylo roztříděno a data z nich převedena do předem vytvořené tabulky, z které jsme poté vycházeli při dalším zpracování získaných dat.

6 ZPRACOVÁNÍ DAT

Při vyhodnocení jednotlivých otázek používáme pojem „kamarád z internetu“, což je kamarád (osoba), kterého respondent zná jen přes internet. Otázky č. 1, 2, 4, 7, 8, 9, 12, 13, 15, 17 jsme zpracovali podle odpovědí všech 138 dotázaných osob, 61 chlapců a 77 dívek.

Oproti tomu při vyhodnocení otázek 3, 5, 6, 10, 11, 14, 16 jsme brali zřetel jen na odpovědi těch respondentů, kteří u otázky 2. odpověděli ano, tj. že mají kamaráda, kterého znají pouze přes internet. Jednalo se celkem o 72 respondentů, přičemž v uvedené skupině bylo 24 chlapců a 48 dívek. Zbývajících 66 respondentů z celkového počtu 138 nemělo kamaráda, kterého by znali jen přes internet.

6.1 Vyhodnocení odpovědí všech respondentů

Následující otázky č. 1, 2, 4, 7, 8, 9, 12, 13, 15, 17 jsou vyhodnocené podle odpovědí všech 138 dotázaných osob.

Využívání internetu

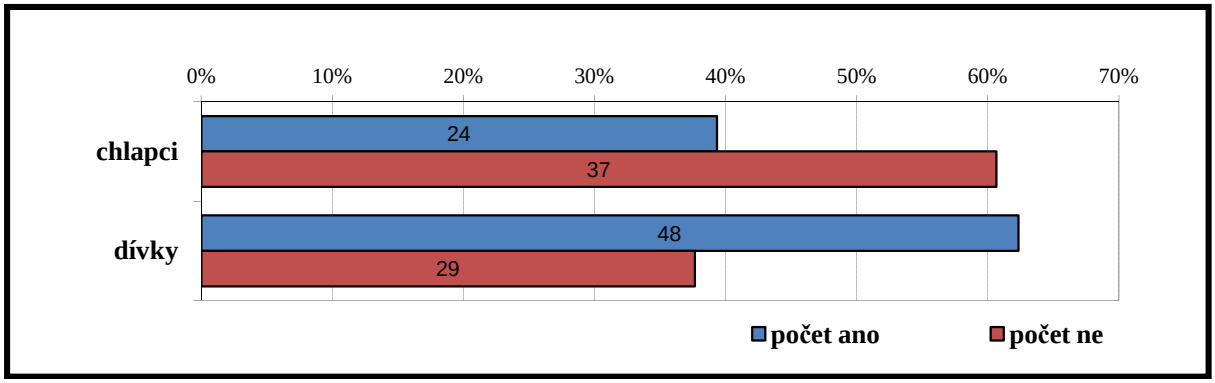
U otázky č. 1 zvolilo odpověď ano, tedy že používá internet, celých 100 % respondentů. Odpověď respondentů nebyla nijak překvapivá, neboť v dnešní době lze konstatovat, že se používání internetu řadí mezi oblíbenou činnost zejména u mladé generace, jelikož nabízí rychlý a pohodlný způsob vzájemné komunikace, je zdrojem informací z různých oblastí života a v neposlední řadě také zdrojem zábavy. V teoretické části práce (v oddílu 1.1.4) uvádíme informace o neustále se zvyšujícím množství domácností připojených k internetu. Díky tomu se internet stává více dostupným i dětem a umožňuje jim tak využívat komunikaci přes internet ve stále větší míře. Námi zjištěné údaje tomu odpovídají.

Komunikace s „kamarádem“, kterého zná žák jen přes internet

V kvantitativním šetření jsme se zaměřili mimo jiné i na to, jestli se děti setkávají s projevy typickými pro kybergrooming. Tomu, aby se dítě stalo potenciální obětí útočníka na internetu, mnohdy napomáhají samotné děti svým chováním na internetu. V některých následujících otázkách se věnujeme problematice chování dětí, kterým mohou nevědomky napomáhat pachatelům kybergroomingu.

Jako problematická se jeví už samotná komunikace s neznámou osobou. Otázku č. 2 jsme položili se záměrem dozvědět se, jaké množství z dotázaných má kamaráda, kterého zná jen z internetu. Podle počtu odpovědí jsme zjistili, že ze 138 dotázaných osob jich má takového kamaráda na internetu 72 (tj. 52,17 %), z čehož bylo 24 (tj. 33,33 %) chlapců a 48 (tj. 66,67 %) dívek. Více přátel známých jen z internetu tedy měly dívky.

Z osob, které mají kamaráda na internetu si jich 11 (3 chlapci a 8 dívek) myslí, že navazování nových známostí přes internet nemůže být nebezpečné, a z těchto by 6 respondentů (2 chlapci a 4 dívky) šlo na schůzku s kamarádem z internetu. Jako pozitivní se jeví skutečnost, že by předem o schůzce někomu řekli.



Graf č. 7 - Máš nějakého kamaráda (člověka), se kterým ses seznámil/a na internetu a kterého neznáš z osobního setkání?

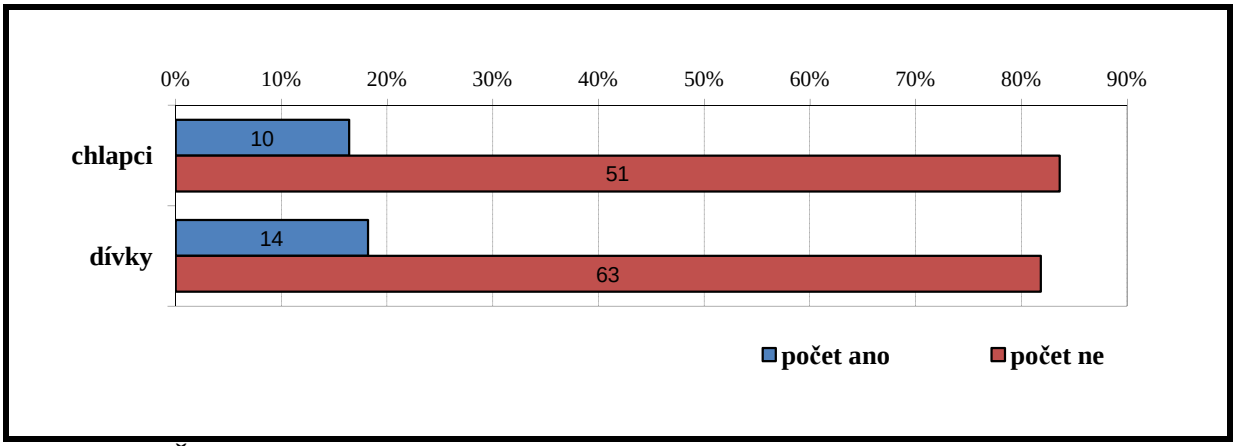
Ochota jít na schůzku s neznámou osobou

Jak uvádíme v teoretické části diplomové práce (v oddílu 3.4.3), je pro kybergrooming typické, že se kybergroomer po určité době vzájemné komunikace s obětí pokusí o to, aby se s ním setkala osobně. Kybergroomer se tak snaží přenést virtuální vztah do prostředí reálného. V otázce č. 4 jsme se proto zaměřili na ochotu respondentů sejít se s osobně

neznámou osobou. Celkem 114 (tj. 82,61 %) dotázaných by na takovou schůzku nešlo, z čehož bylo 51 (tj. 44,74 %) chlapců a 63 (tj. 55,26 %) dívek.

Z výsledných odpovědí dále vyplynulo, že na schůzku s neznámou osobou by šlo 24 (tj. 17,39 %) respondentů, z čehož bylo 10 (tj. 41,67 %) chlapců a 14 (tj. 58,33 %) dívek. Podle odpovědí těchto respondentů u otázky č. 7 se ukázalo, že všichni respondenti, kteří by byli ochotní jít na takovou schůzku, by se někomu svěřili, že na schůzku jdou. Celkem 14 z těchto respondentů (4 chlapci a 10 dívek) si myslí, že taková schůzka může být nebezpečná, 2 chlapci a 3 dívky si myslí, že schůzka nebezpečná není a 5 respondentů (4 chlapci a 1 dívka) zvolilo odpověď, že neví.

Mezi respondenty, kteří by na schůzku s kamarádem z internetu šli, bylo 6 dívek, které se setkaly s nabídkou nějakého úplatku za schůzku s „kamarádem z internetu“.



Graf č. 8 - Šel/šla bys na schůzku s kamarádem (člověkem), kterého bys znal /a pouze přes internet?

U této otázky ověřujeme první hypotézu a statistickým testem dobré shody chí-kvadrát zjišťujeme, zda je mezi danými věkovými skupinami statisticky významný rozdíl co do podílu jedinců ochotných jít na schůzku s osobou, kterou by znali jen přes internet.

Stanovení nulové a alternativní hypotézy.

$H1_0$ - Mezi věkovými skupinami nejsou statisticky významné rozdíly co do podílu osob ochotných jít na osobní schůzku s člověkem, kterého by znaly jen přes internet.

$H1_A$ - Podíl osob ochotných jít na osobní schůzku s člověkem, kterého by znaly jen přes internet, je u uvedených věkových skupin různý.

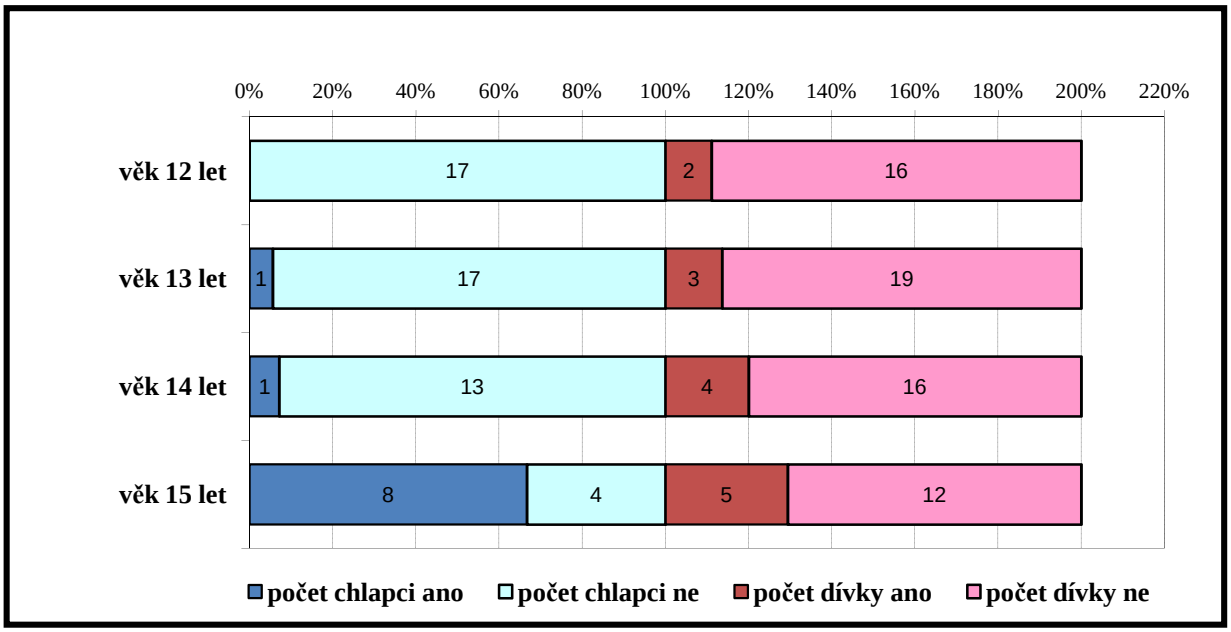
Předpokládáme, že podíl osob ochotných jít na schůzku s člověkem, kterého by znaly jen přes internet, je u věkových skupin různý. Očekáváme, že největší ochotu jít na schůzku projeví jedinci ve věkové skupině 15 let, jelikož mají ve větší míře zájem o moderní technologie a jejich používání, jsou odvážnější, mají více kontaktů, rádi objevují nové věci, chtějí být „in“. Období okolo 15 roku je obdobím puberty, kdy se mladí lidé snaží najít své místo, začlenit se do určité skupiny, jde vlastně o období tzv. „hledání sebe sama“.[191]

Věk	Počet žáků ve věkové kategorii	Pozorovaná četnost **P**	Očekávaná četnost **O**	**P - O**	**$(P - O)^2$**	**$\frac{(P - O)^2}{O}$**
12 let	35	2	6,087	-4,087	16,703	2,744
13 let	40	4	6,957	-2,957	8,741	1,257
14 let	34	5	5,913	-0,913	0,834	0,141
15 let	29	13	5,043	7,957	63,306	12,552
	Σ 138	**Σ** 24	**Σ** 24			**X^2 16,694**

Tabulka č. 5 - Výpočet testového kritéria

Z výše uvedené tabulky vyplývá, že bylo vypočítáno testové kritérium $X^2 = 16,694$. Testové kritérium X^2 jsme posléze srovnali s kritickou hodnotou nalezenou pro zvolenou hladinu významnosti a stupeň volnosti. V našem případě je počet stupňů volnosti 3. Kritická hodnota na hladině významnosti 0,05 je tedy podle statistických tabulek = 7,815. Vzhledem k tomu, že vypočítaná hodnota X^2 je větší než hodnota kritická, odmítáme nulovou hypotézu a přijímáme hypotézu alternativní. Podíl osob ochotných jít na osobní schůzku s člověkem, kterého znají jen přes internet, je u uvedených věkových skupin různý. Na základě výpočtu provedeného ze zjištěných relativních četností potvrzujeme očekávání, že ve věkové skupině 15 let je nejvyšší podíl jedinců ochotných jít na osobní schůzku s člověkem, kterého by znali jen přes internet, celkem se jedná o (44,8 %) z těchto patnáctiletých chlapců a dívek. Ze srovnání věkových skupin chlapců a děvčat jednoznačně vyplývá, že největší podíl jedinců ochotných jít na osobní schůzku je ve věkové skupině patnáctiletých chlapců celkem (66,7 %), což je jasně rozeznatelné z následujícího grafu.

[191] ERIKSON, E. H. *Dětství a společnost*, 1. vyd. Praha : Argo, 2002. 387 s. ISBN 80-7203-380-8.



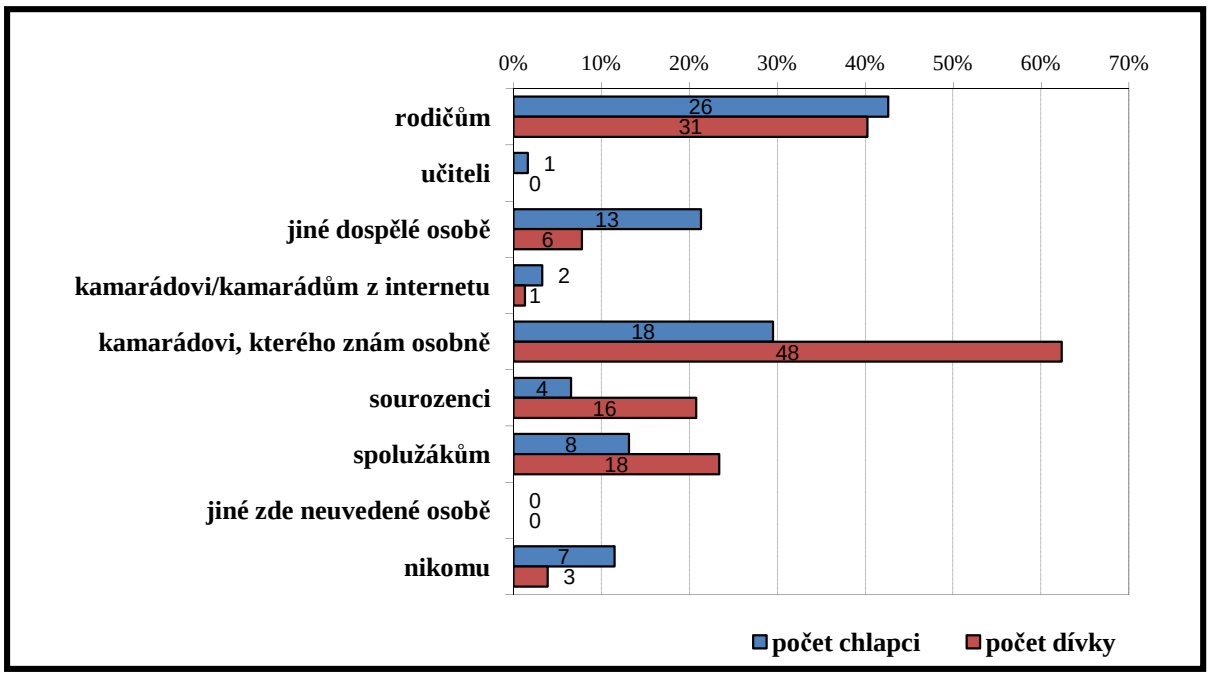
Graf č. 9 - Grafické znázornění odpovědí na otázku týkající se ochoty jít na osobní schůzku s neznámou osobou u jednotlivých věkových kategorií chlapců a dívek.

Ochota dětí svěřit se někomu s tím, že jdou na schůzku s neznámým člověkem

Schůzka s neznámou osobou je již sama o sobě velmi rizikovou záležitostí. Vzhledem k tomu je žádoucí, aby děti, pokud se už rozhodnou na takovou schůzku jít, informovaly o tomto svém rozhodnutí někoho, kdo dokáže zodpovědně posoudit, zda je bezpečné, nebo naopak nebezpečné osobní setkání uskutečnit. Otázka č. 7 se zaměřuje na zjištění, komu by se děti svěřily, že jdou na schůzku s „kamarádem z internetu“. U této otázky jsme zaznamenali celkem 202 odpovědí, jelikož někteří respondenti očekávaně zvolili více z možných odpovědí. Chlapci nejčastěji volili odpověď, že by se svěřili rodičům, a dívky jinému kamarádovi známému osobně.

Ze všech respondentů si pouze jeden chlapec vybral odpověď, že by se svěřil učiteli. Z dívek by se učiteli nesvěřila žádná. Za pozitivní zjištění můžeme považovat skutečnost, že 43 respondentů (11 chlapců a 32 dívek) by se s rozhodnutím jít na schůzku svěřilo hned několika osobám.

Oproti tomu je velmi zneklidňující zjištění, že mezi respondenty bylo 10 (tj. 7,25 %) dětí, které by se s rozhodnutím jít na schůzku nesvěřily nikomu. Důležité je, že všechny tyto děti zároveň v otázce č. 4 odpověděly, že by na takovou schůzku nešly, i když si 2 z těchto respondentů (chlapci) myslí, že taková schůzka není nebezpečná.

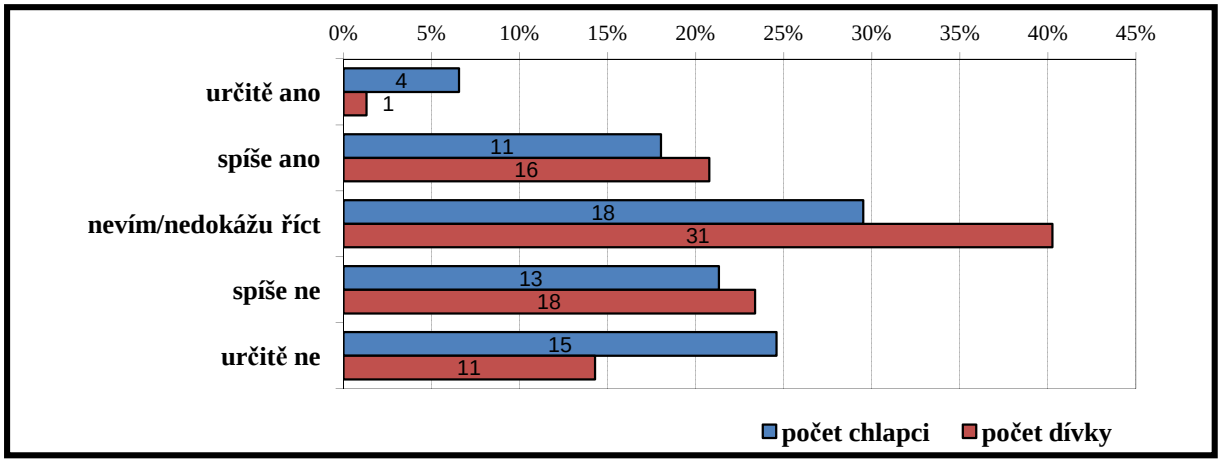


Graf č. 10 - Komu bys řekl/a (by ses svěřil/a) v případě, že bys šel/a na schůzku s kamarádem (člověkem), kterého bys neznal/a osobně, ale jen přes internet?

Ochota věřit informacím sdělovaným při komunikaci přes internet

Při komunikaci přes internet uživatelé sdělují různé informace, a to včetně osobních údajů. Skutečnost, jestli by takové informace včetně těch osobních sdělili osobě známé jen přes internet, závisí i na jejich důvěřivosti. Na zmíněný problém jsme se zaměřili v otázce č. 8 a zjišťovali jsme, do jaké míry jsou respondenti ochotni věřit tomu, co by jim o sobě tvrdil člověk, kterého by znali pouze z internetu. Ze všech 138 respondentů odpověď nevím/nedokážu říct volilo 49 (tj. 35,51 %) osob, z čehož bylo 18 (tj. 36,73 %) chlapců a 31 (tj. 63,27 %) dívek. Jednalo se o nejfrekventovanější odpověď.

Z odpovědí na otázku č. 8 dále vyplynulo, že si 32 respondentů (15 chlapců a 17 dívek) myslí, že se dá věřit tomu, co o sobě „kamarád z internetu“ tvrdí. Mezi nimi bylo 5 chlapců a 4 dívky, kteří u otázky č. 13 uvedli, že by „kamarádovi z internetu“ řekli tajemství, o kterém by nechtěli, aby je věděl někdo jiný, což opět můžeme považovat za rizikové chování.

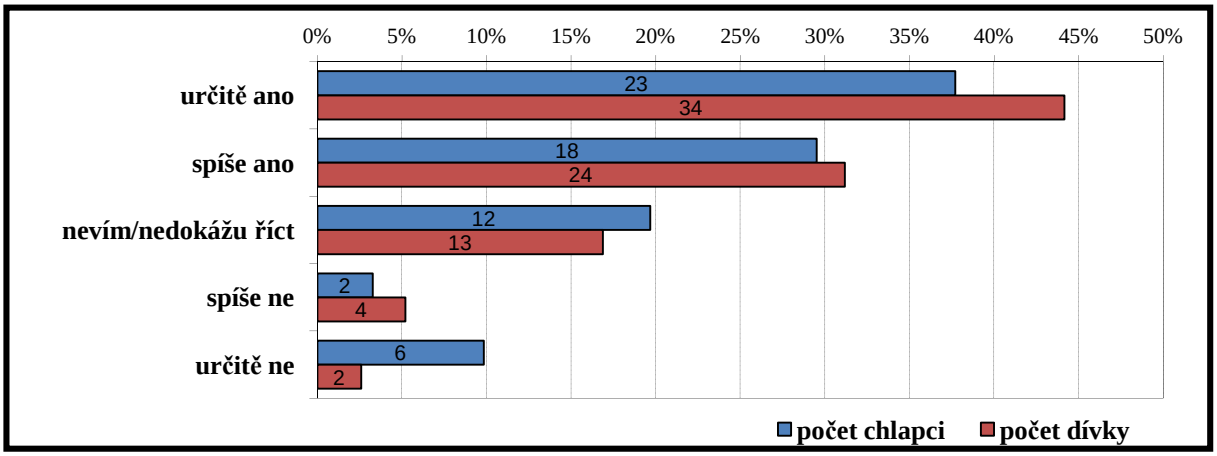


Graf č. 11 - Myslíš si, že by se dalo věřit tomu, co by ti o sobě na internetu tvrdil (říkal), kamarád (člověk), kterého bys neznal/a osobně, ale jen z internetu?

Názor na rizikovost schůzky s neznámou osobou

Schůzka s neznámou osobou z internetu je jedním z největších rizik, která dětem v souvislosti s internetem hrozí. Na dané téma se zaměřila otázka č. 9. Z výsledných odpovědí je patrné, že nejvíce respondentů si je rizika spojeného s takovou schůzkou vědomo.

Celkem 99 respondentů (41 chlapců a 58 dívek) se domnívá, že schůzka je nějakým způsobem nebezpečná. Z celkového počtu 138 respondentů se tedy jedná o 71,74 %. Že schůzka s „kamarádem z internetu“ nemůže být nebezpečná, se domnívá 14 respondentů (8 chlapců a 6 dívek). Z nich by na takovou schůzku šli 2 chlapci a 3 dívky, což můžeme opět považovat za velice rizikové, a to i přesto, že by se každý z nich o schůzce předem někomu svěřil.

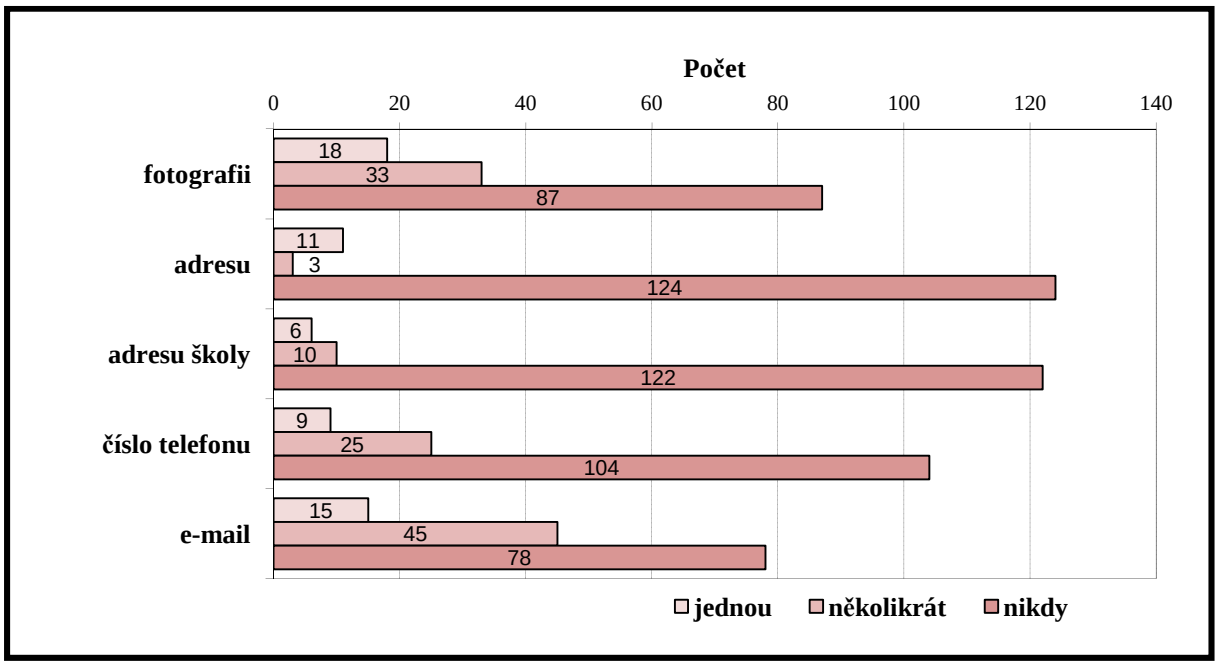


Graf č. 12 - Myslíš si, že může být nebezpečná schůzka s člověkem, se kterým by ses znal/a pouze přes internet?

Ochota poskytovat neznámé osobě osobní informace

Další otázkou zaměřující se na nebezpečné jednání uživatelů byla otázka č. 12. Zde se respondenti vyjadřovali k tomu, zda některou z nabízených informací poskytli neznámé osobě na internetu. Na výběr měli fotografii, adresu bydliště, adresu školy, telefon a e-mail. U jednotlivých odpovědí zároveň uváděli, kolikrát kterou informaci poskytli, zda jednou, několikrát, nebo nikdy.

Nejvíce respondentů volilo variantu, že uvedenou informaci neposkytlo nikdy. To patrně pramení z jejich obavy, jak by se získanými informacemi bylo dále nakládáno, a rovněž z neochoty svěřovat se se soukromými informacemi neznámým lidem.



Graf č. 13 - Jak často jsi na internetu poskytl/a některou z následujících informací?

Druh informace	Pouze jednou		Několikrát		Nikdy		Celkem
	Počet	%	Počet	%	Počet	%	Počet
Fotografie							
Chlapci	8	13,12	8	13,12	45	73,77	61
Dívky	10	12,99	25	32,47	42	54,55	77
Celkem	18	13,04	33	23,91	87	63,05	138
Adresa bydliště							
Chlapci	2	3,28	2	3,28	57	93,44	61
Dívky	9	11,69	1	1,30	67	87,01	77
Celkem	11	7,97	3	2,17	124	89,86	138
Adresa školy							
Chlapci	2	3,28	4	6,56	55	90,16	61
Dívky	4	5,20	6	7,79	67	87,01	77
Celkem	6	4,35	10	7,25	122	88,41	138
Číslo telefonu							
Chlapci	2	3,28	6	9,84	53	86,89	61
Dívky	7	9,09	19	24,68	51	66,23	77
Celkem	9	6,52	25	18,12	104	75,36	138
E-mail							
Chlapci	6	9,84	10	16,39	45	73,77	61
Dívky	9	11,69	35	45,46	33	42,86	77
Celkem	15	10,87	45	32,61	78	56,52	138

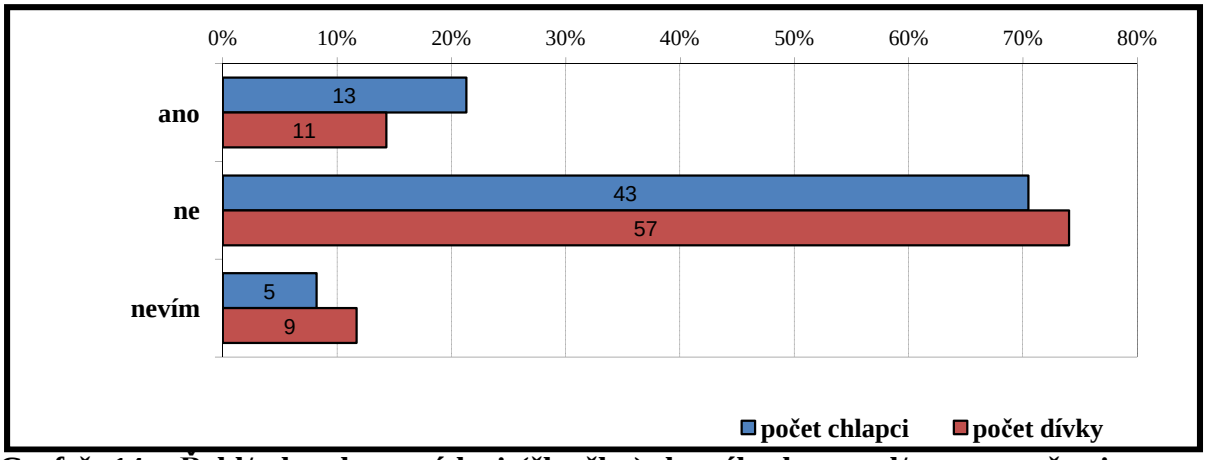
Tabulka č. 6 - Rozdělení odpovědí respondentů, jak často poskytli jednotlivé druhy informací

Ochota sdělovat důvěrné informace „tajemství“ neznámé osobě

Další otázkou týkající se míry rizikového chování dětí, byla otázka č. 13. Zaměřili jsme se v ní na ochotu dětí svěřovat „kamarádovi z internetu“ svá „tajemství“. Ze zjištěných výsledků vyplynulo, že 100 (tj. 72,46 %) respondentů, z čehož bylo 43 (tj. 43,00 %) chlapců a 57 (tj. 57,00 %) dívek, by se s tajemstvím takové osobě nesvěřilo.

Z kvantitativního šetření dále vyplynulo, že 24 (tj. 17,39 %) dětí by se neznámé osobě s tajemstvím svěřilo, a to 13 (tj. 54,17 %) chlapců a 11 dívek (tj. 45,83 %). Můžeme je označit za velice ohroženou skupinu dětí. Jak uvádíme v teoretické části diplomové práce (v oddílu 3.4.3) tak v případech, kdy útočník od oběti získá důvěrné informace a „tajemství“, dostává tím zároveň k dispozici velice mocnou zbraň, jak oběť donutit například vydíráním a vyhrožováním k věcem, které by v jiném případě nebyla ochotna udělat.

Je zneklidňující, že 8 respondentů (4 chlapci a 4 dívky), kteří by se s tajemstvím svěřili, zároveň u otázky č. 4 vybralo odpověď, že by šli na schůzku s „kamarádem z internetu“. Každý z nich by se dopředu o této schůzce někomu svěřil.



Graf č. 14 - Řekl/a bys kamarádovi (člověku), kterého bys znal/a pouze přes internet tajemství, o kterém bys nechtěl/a, aby věděl někdo jiný?

U otázky č. 13 ověřujeme druhou hypotézu, přičemž statistickým testem dobré shody chí-kvadrát zjišťujeme, zda jsou mezi danými věkovými skupinami statisticky významné rozdíly v podílu jedinců ochotných sdělit tajemství člověku, kterého by znali jen přes internet.

Stanovení nulové a alternativní hypotézy.

$H2_0$ - Mezi věkovými skupinami nejsou statisticky významné rozdíly co do podílu osob ochotných sdělit tajemství člověku, kterého by znaly jen přes internet.

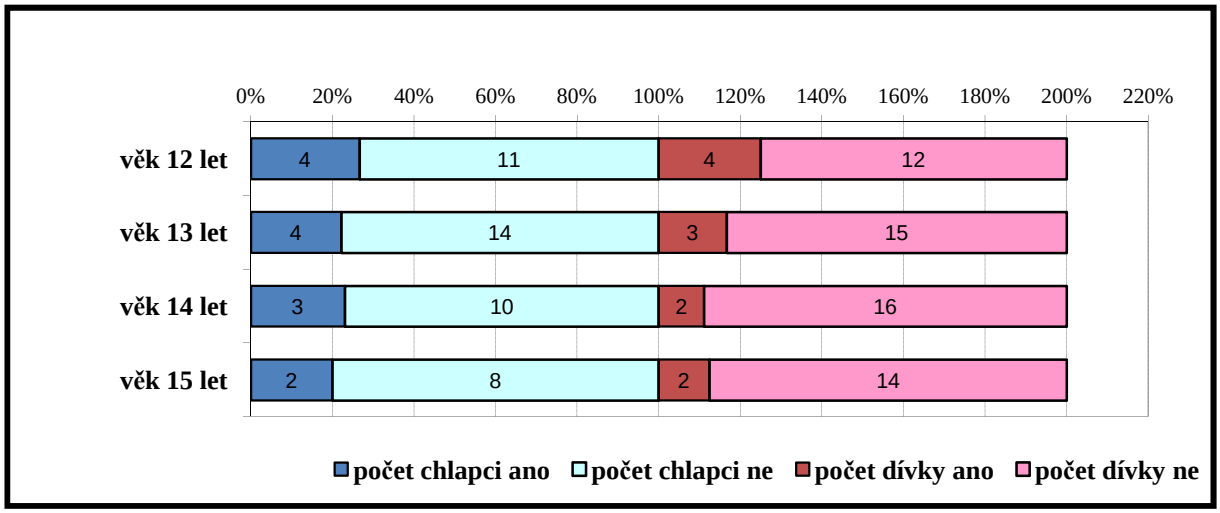
$H2_A$ - Podíl osob ochotných sdělit tajemství člověku, kterého by znaly jen přes internet, je u uvedených věkových skupin různý.

Předpokládáme, že mezi věkovými skupinami nejsou statisticky významné rozdíly co do podílu osob ochotných sdělit tajemství člověku, kterého by znaly jen přes internet.

Otázka č. 13	počet žáků ve věkové kategorii	Pozorovaná četnost **P**	Očekávaná četnost **O**	**P - O**	**$(P - O)^2$**	**$\frac{(P - O)^2}{O}$**
věk 12 let	31	8	6,000	2,000	4,000	0,667
věk 13 let	36	7	6,968	0,032	0,001	0,000
věk 14 let	31	5	6,000	-1,000	1,000	0,167
věk 15 let	26	4	5,032	-1,032	1,066	0,212
	Σ 124	**Σ** 24	**Σ** 24			**X^2 1,045**

Tabulka č. 7 - Výpočet testového kritéria

Z výše uvedené tabulky vyplývá, že bylo vypočítáno testové kritérium x^2 = 1,045. Testové kritérium x^2 jsme posléze srovnali s kritickou hodnotou nalezenou pro zvolenou hladinu významnosti a stupeň volnosti. V našem případě je počet stupňů volnosti 3. Kritická hodnota na hladině významnosti 0,05 je tedy podle statistických tabulek = 7,815. Vzhledem k tomu, že vypočítaná hodnota x^2 je menší než hodnota kritická, přijímáme nulovou hypotézu a odmítáme hypotézu alternativní. Mezi věkovými skupinami nejsou statisticky významné rozdíly co do podílu osob ochotných sdělit tajemství člověku, kterého by znaly jen přes internet.

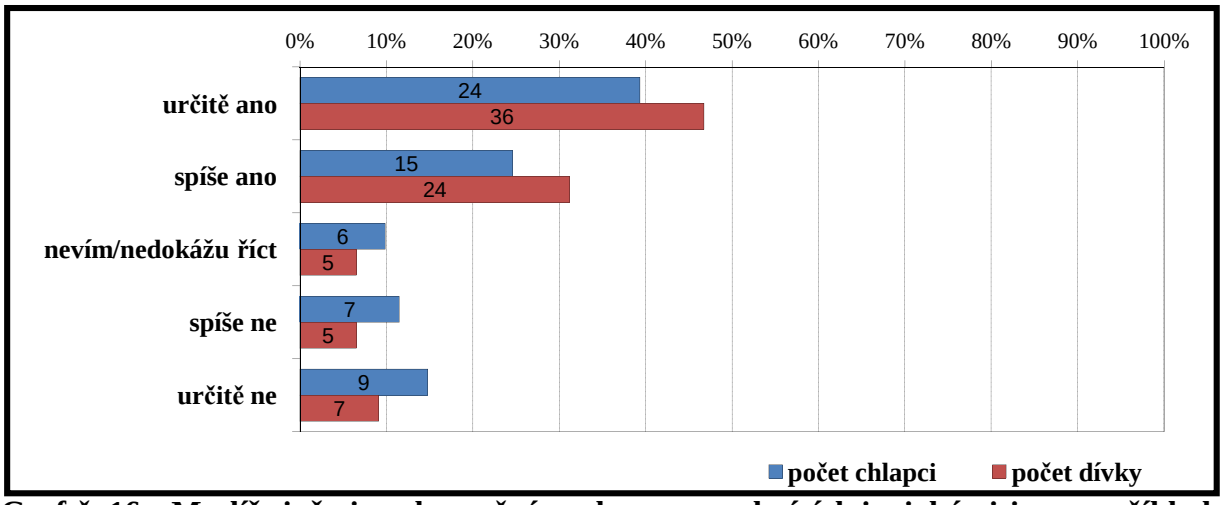


Graf č. 15 - Grafické znázornění odpovědí na otázku týkající se ochoty sdělit tajemství člověku, kterého by znaly jen přes internet u jednotlivých věkových kategorií chlapců a dívek.

Názor na rizikovost poskytování osobních údajů neznámé osobě

Názor na rizikovost poskytování osobních údajů neznámé osobě je velmi důležitý, protože i od něj se odvíjí ochota osobní údaje poskytovat. Zmíněné poskytování osobních údajů v prostředí internetu je v současnosti považováno za jedno z největších bezpečnostních rizik. Danému tématu se proto věnovala otázka č. 15. Celkem 99 (tj. 71,74 %) respondentů uvedlo, že si myslí, že je nebezpečné poskytovat osobní údaje, jakými jsou například jméno, datum narození, adresa bydliště, telefonní číslo, e-mail apod. Jednotlivé odpovědi u dalších variant otázky č. 15 přibližuje níže uvedený graf.

Z 28 respondentů (16 chlapců a 12 dívek), kteří si myslí, že poskytování osobních údajů není nebezpečné, by 5 chlapců a 3 dívky řekli „kamarádovi z internetu“ tajemství, o kterém by nechtěli, aby je věděl někdo jiný. Mezi nimi byli 2 chlapci a 3 dívky, kteří zároveň uvedli, že by šli na schůzku s „kamarádem z internetu“. O schůzce by dopředu někoho informovali.



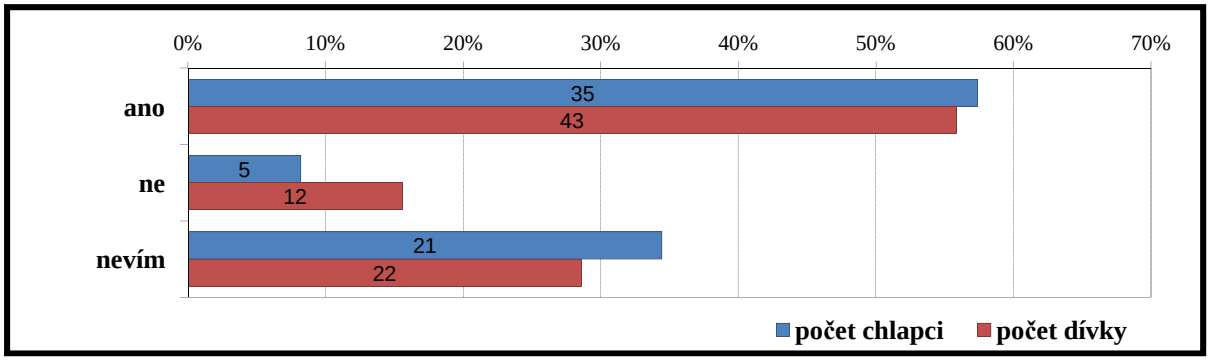
Graf č. 16 - Myslíš si, že je nebezpečné poskytovat osobní údaje, jakými jsou například jméno, datum narození, adresa bydliště, telefonní číslo, e-mail apod. lidem, které bys znal/a jen z internetu?

Názor na rizikovost navazování nových známostí přes internet

Otázka č. 17 mapovala, co si děti myslí o navazování nových známostí na internetu. Z výsledků dotazníkového šetření vyplynulo, že navazování nových známostí na internetu považuje za nebezpečné 78 (tj. 56,52 %) respondentů, z čehož bylo 35 (tj. 44,87 %) chlapců a 43 (tj. 55,13 %) dívek.

Celkem 17 respondentů (5 chlapců a 12 dívek) si myslí, že navazování nových známostí přes internet nemůže být nebezpečné. Z těchto respondentů jich má 11 (3 chlapci a 8 dívek) kamaráda na internetu. Z výše uvedených 11 respondentů se jich 6 (2 chlapci a 4 dívky) domnívá, že se dá věřit tomu, co o sobě tvrdí „kamarád z internetu“, a z nich by 1 chlapec a 4 dívky šli na schůzku s „kamarádem z internetu“. O schůzce by všichni předem někomu řekli.

Ze 17 respondentů, kteří zvolili odpověď, že navazování nových známostí přes internet nemůže být nebezpečné, jich 5 (2 chlapci a 3 dívky) zastává názor, že není nebezpečné poskytovat osobní údaje lidem známým jen přes internet.



Graf č. 17 - Myslíš, že může být nebezpečné navazování nových známostí přes internet?

6.2 Vyhodnocení odpovědí vybraných respondentů

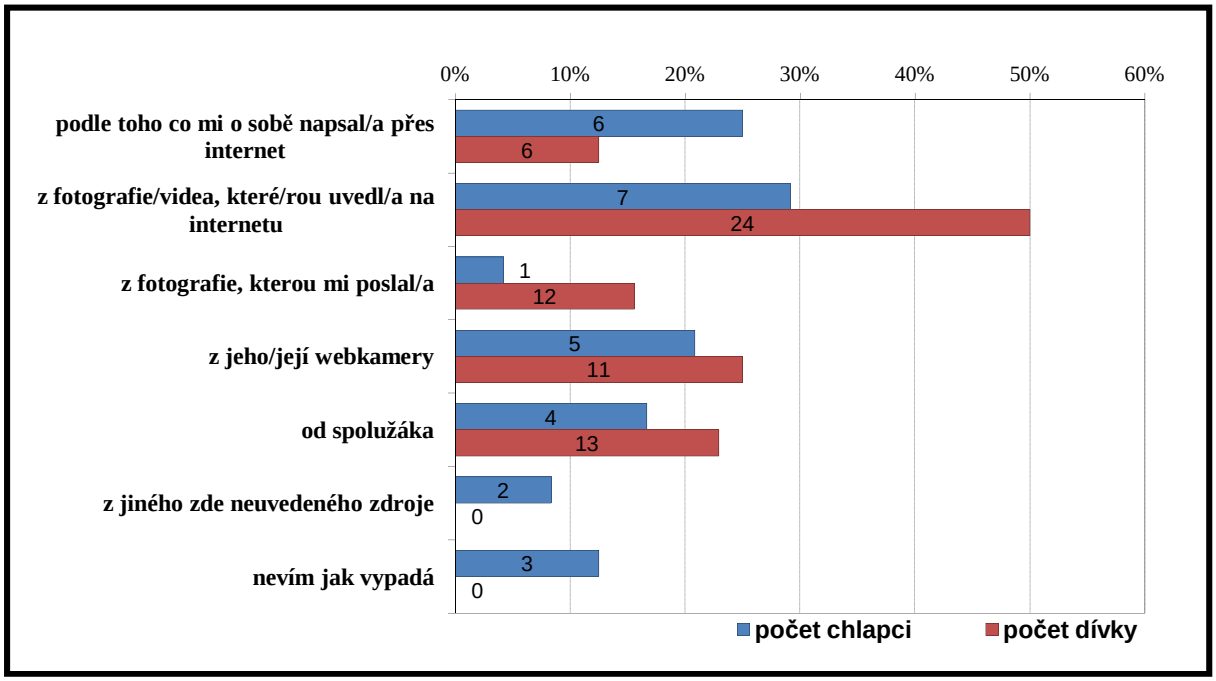
U následujících otázek 3, 5, 6, 10, 11, 14, 16 jsme brali zřetel jen na odpovědi těch respondentů, kteří u otázky 2. odpověděli ano, tj. že mají kamaráda, kterého znají pouze přes internet. Jednalo se celkem o 72 respondentů, přičemž v uvedené skupině bylo 24 chlapců a 48 dívek.

Odkud respondent ví, jak kamarád z internetu vypadá

V otázce č. 3 jsme zjišťovali, zda respondenti vědí, jak „vypadá“ jejich internetový kamarád a z jakého zdroje uvedenou informaci získali. U této otázky mohli dotázaní kombinovat více odpovědí týkajících se zdrojů informace. Ze všech respondentů, kteří mají kamaráda na internetu, jich 69 (21 chlapců a 48 dívek) uvedlo nějaký zdroj, ze kterého ví, jak „kamarád z internetu“ vypadá. Z výsledků vyplynulo, že chlapci i dívky nejčastěji uváděli jako zdroj informací fotografii nebo video, které o sobě kamarád (člověk) uveřejnil na internetu. Tuto odpověď zvolilo 31 (tj. 43,06 %) respondentů, z čehož bylo 7 (tj. 22,58 %) chlapců a 24 (tj. 77,42 %) dívek.

Z respondentů, kteří z nějakého zdroje vědí, jak vypadá jejich „kamarád z internetu“, zvolilo 34 odpověď, že zdrojem informací byla fotografie nebo to, co o sobě „kamarád z internetu“ napsal. Jak uvádíme v teoretické části diplomové práce (v oddílu 3.4.1), v souvislosti s kybergroomingem si útočník vytváří falešnou identitu, která mu při komunikaci s obětí umožňuje vydávat se za někoho jiného, než kým ve skutečnosti je. Falešné identity dociluje např. podvrženými fotografiemi nebo uváděním nepravdivých informací

o sobě. Vzhledem k tomu lze považovat oba zdroje informací u výše zmíněných 34 respondentů za ne příliš důvěryhodné.

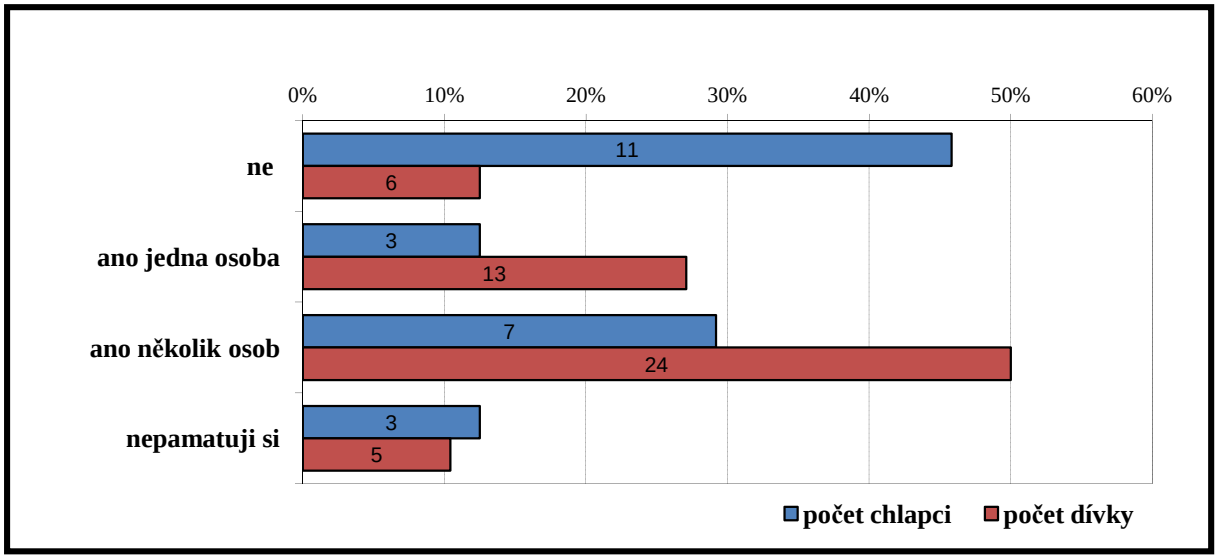


Graf č. 18 - Odkud víš, jak vypadá tvůj kamarád (člověk), kterého znáš pouze přes internet a ne osobně?

Pozvání na schůzku osobně neznámou osobou

Pomocí otázky č. 5 jsme zjišťovali, jestli se respondenti setkali s pozváním na schůzku od osoby, kterou by znali jen z internetu. Z odpovědí vyplynulo, že se s pozváním setkalo 47 (tj. 65,28 %) respondentů, 10 (tj. 21,28 %) chlapců a 37 (tj. 78,72 %) dívek.

Z respondentů, kteří se setkali s pozváním na schůzku, 3 chlapci a 13 dívek současně odpovědělo, že by na schůzku s „kamarádem z internetu“ šli. Zároveň s tím však uvedli, že by se s takovou schůzkou dopředu svěřili. Mezi uvedenými šestnácti respondenty byl 1 chlapec a 10 dívek, kteří si myslí, že schůzka s takovou osobou může být nebezpečná. Další 2 chlapci a 1 dívka zvolili odpověď nevím a zbývající 2 dívky se domnívají, že schůzka nebezpečná není.

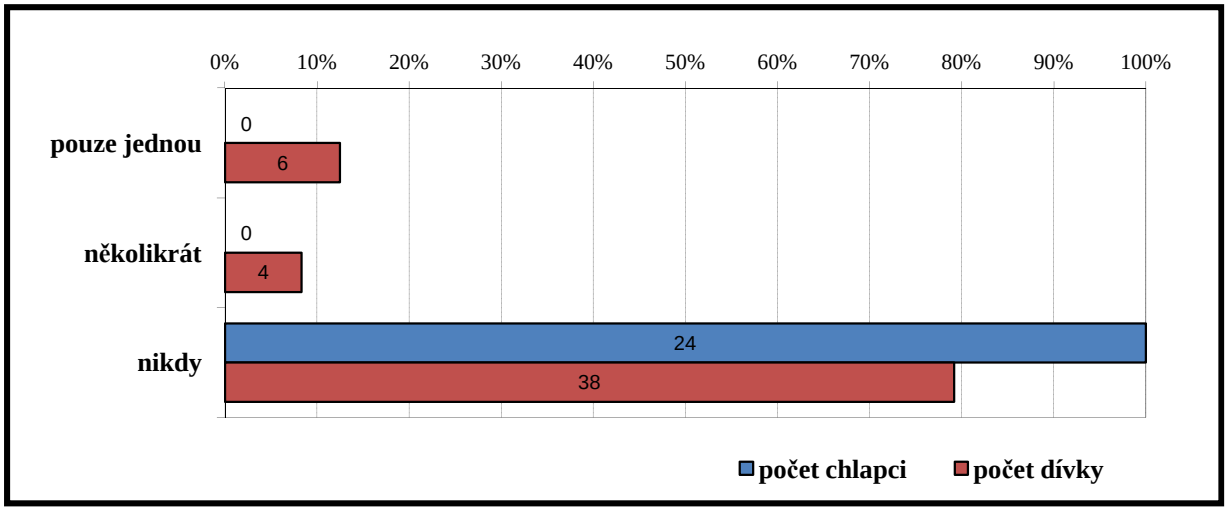


Graf č. 19 - Chtěl se s tebou osobně sejít někdo, koho znáš jen přes internet?

Nabídka úplatku za příslib osobního setkání

Při hodnocení odpovědí u otázky č. 6 se ukázalo, že se s nabídkou úplatku za osobní schůzku nesetkal žádný z chlapců, který u otázky č. 2 uvedl, že má kamaráda známého pouze z internetu. Stejně tak odpovědělo u obou otázek i 38 (tj. 61,29 %) dívek.

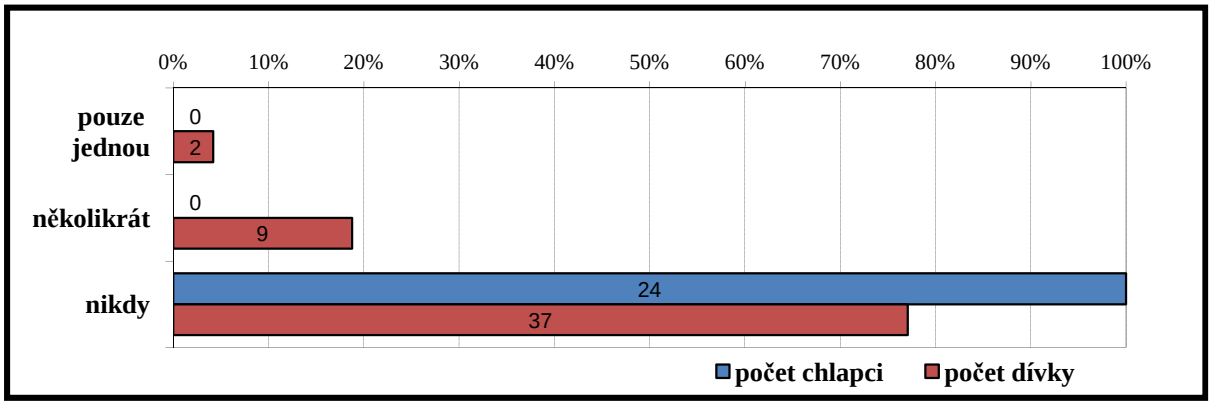
S nabídkou úplatku za osobní setkání se setkalo 10 dívek. Šest z nich zároveň projevilo ochotu jít na schůzku s „kamarádem z internetu“. Všechny by dopředu o této schůzce někomu řekly.



Graf č. 20 - Nabízel ti kamarád (člověk), kterého znáš pouze z internetu například peníze, mobilní telefon, telefonní kredit nebo nějaký jiný úplatek za to, že se s ním sejdeš?

Zkušenost s posíláním dárku od neznámé osoby z internetu

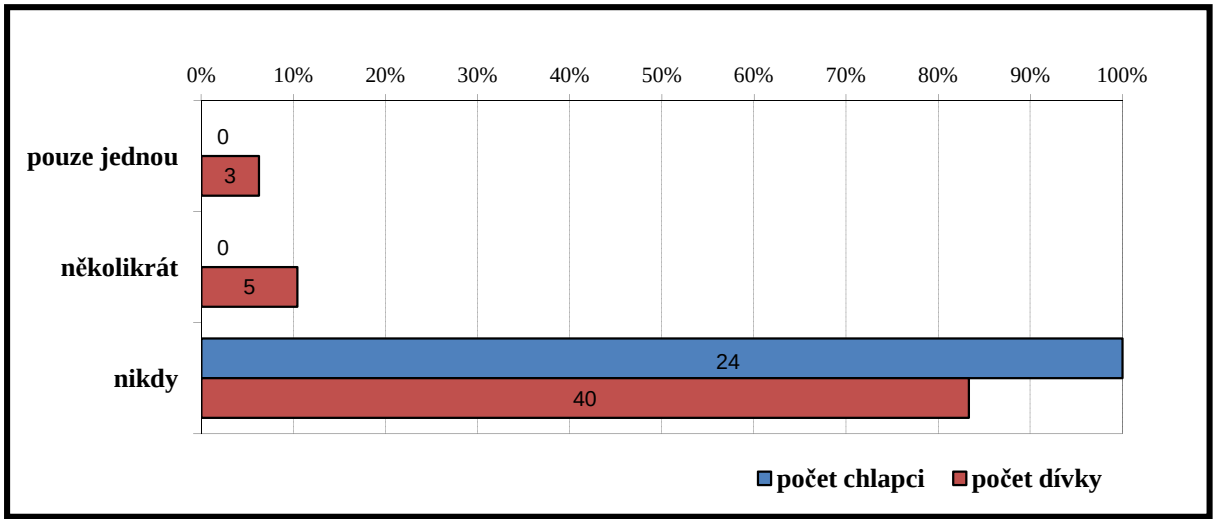
Otázka č. 10 mapovala, jestli se respondenti setkali s tím, že by jim „kamarád z internetu“ poslal nějaké dárky, například peníze, mobilní telefon, kredit do mobilního telefonu nebo něco podobného. Odpověď, že se s uvedenou nabídkou nesetkali, zvolilo 61 (tj. 84,72 %) respondentů, 24 (tj. 39,34 %) chlapců a 37 (tj. 60,66 %) dívek. Se zmíněným posíláním dárků mělo zkušenost pouze 11 dívek. Z dívek, kterým „kamarád z internetu“ poslal dárek, se jich 5 setkalo se žádostí, aby za zaslané dárky poslaly například fotografii nebo jinou informaci o sobě.



Graf č. 21 - Poslal ti kamarád (člověk), kterého znáš pouze z internetu, nějaké dárky? Například peníze, mobilní telefon, kredit nebo něco podobného?

Zkušenost s žádostí o zaslání osobních informací neznámé osobě výměnou za dárek

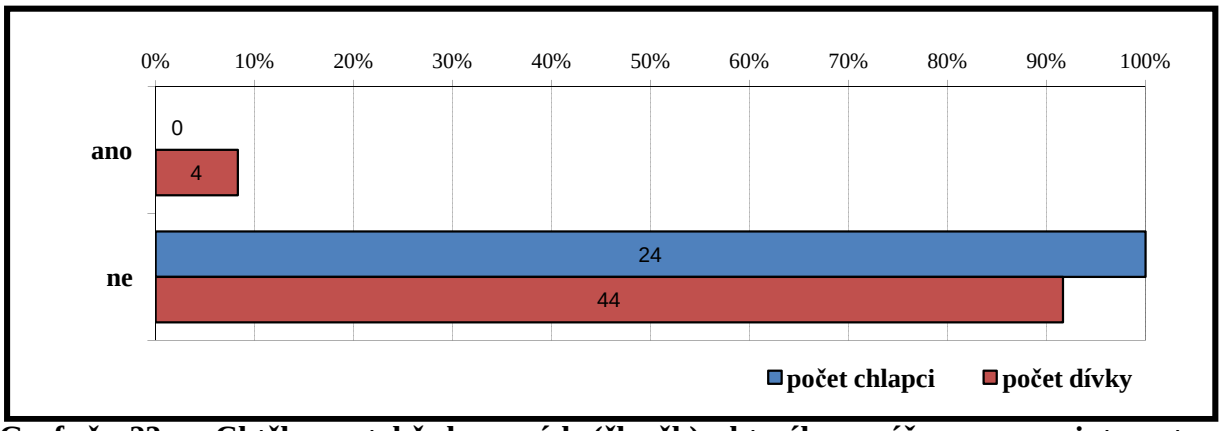
Při komunikaci na internetu na uživatele číhají mnohá rizika. Jedním z nich je nebezpečí zneužití osobních nebo důvěrných informací sdělených neopatrným uživatelem neznámé osobě. Následující otázka č. 11 se zaměřovala na uvedenou problematiku, konkrétně na zkušenosti respondentů s žádostí o sdělení osobních informací za úplatu. Výsledkem kvantitativního šetření u této otázky bylo zjištění, že se zmíněnou žádostí o informaci se již setkalo 8 (tj. 11,11 %) dívek. Současně si 7 z nich myslí, že je nebezpečné poskytovat osobní informace osobám známým jen z internetu a jedna dívka zastává názor, že poskytování osobních údajů nebezpečné není.



Graf č. 22 - Chtěl/a od tebe kamarád (člověk), kterého znáš pouze z internetu, abys mu za dárky co ti dal, na oplátku poslal/a například svoji fotografii, číslo mobilního telefonu nebo sdělil/a nějaké důvěrné, intimní informace o sobě?

Žádost o udržení komunikace s neznámou osobou v tajnosti

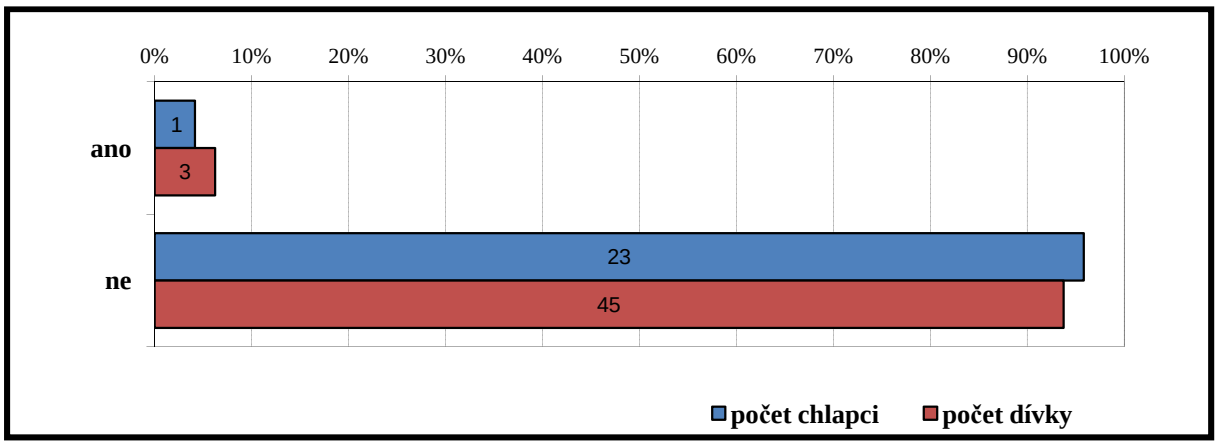
Otázka č. 14 se dotýkala jednoho z typických znaků kybergroomingu, a tím je snaha o udržení komunikace v tajnosti. S výše uvedenou žádostí se nesetkal žádný z chlapců. Z odpovědí dále vyplynulo, že se s žádostí o udržení komunikace v tajnosti před rodiči setkaly 4 (tj. 5,56 %) dívky. Třem z těchto dívek byl nabídnut úplatek za schůzku od kamaráda známého pouze z internetu. Za velice nebezpečné by se dalo považovat, kdyby žádost o utajení a nabídka osobního setkání za úplatek přišla od téže osoby.



Graf č. 23 - Chtěl po tobě kamarád (člověk), kterého znáš pouze z internetu, aby o vašem přátelství nevěděli rodiče?

Setkání s vydíráním

Mezi nebezpečné aktivity kybergroomerů lze zařadit vydírání oběti ve snaze donutit ji k osobní schůzce. Nezřídka se prostředkem pro vydírání stávají informace, které o sobě oběti sami nezodpovědně uvedly, například na internetu. Podle výsledků odpovědí u otázky č. 16, se se situací, kdy „kamarád z internetu“ hrozil prozrazením tajemství, které na respondenta ví, pokud se s ním respondent nesejde, setkali celkem 4 (tj. 5,56 %) respondenti, 1 (tj. 25,00 %) chlapec a 3 (tj. 75,00 %) dívky. Všichni 4 na internetu poskytli některou z osobních informací (fotografii, adresu bydliště, adresu školy kam chodí, číslo mobilního telefonu nebo e-mail). Je zarážející, že 2 dívky ve věku 12 a 13 let, které se setkaly s vydíráním, u otázky č. 13 uvedly, že jsou ochotné sdělit „kamarádovi z internetu“ tajemství, o kterém by nechtěly, aby je věděl někdo jiný.



Graf č. 24 - Vyhrožoval ti (vydíral tě, nutil tě) kamarád (člověk), se kterým se znáš pouze z internetu, že když se s ním nesejdeš, tak na tebe prozradí tajemství, které na tebe ví?

7 ANALÝZA DOSAŽENÝCH VÝSLEDKŮ

Po vyhodnocení jednotlivých otázek dotazníku použitého při výzkumném šetření je možné problematiku bezpečného chování žáků 2. stupně základních škol zhodnotit následujícími zjištěními:

- 100 % respondentů ve věku 12-16 let používá internet.
- Ze 138 dotázaných osob má kamaráda, kterého zná pouze z internetu 72 dětí tedy celých (52,17%) z dotazovaných.
- S aktivitami, které by nasvědčovaly tomu, že se stali cílem útoku kybergroomera, se žáci setkali.
- S pozváním na schůzku od „kamaráda z internetu“ má zkušenost 47 respondentů, 10 chlapců a 37 dívek.
- S nabídkou úplatku za osobní setkání s „kamarádem z internetu“ se setkalo 10 dívek. Žádný z dotazovaných chlapců takovou nabídku nedostal.
- S posíláním dárků od osoby známé jen přes internet se setkalo 11 dívek. Chlapci takovou zkušenost nemají.
- Po 4 dívkách chtěl „kamarád z internetu“, aby o jejich přátelství nevěděli rodiče. Chlapci se s touto žádostí nesetkali.
- Ze zúčastněných respondentů se 8 dívek setkalo se situací, kdy po nich chtěl „kamarád z internetu“, aby mu za dárky, co jim dal, na oplátku poslaly například svoji fotografii, číslo mobilního telefonu nebo sdělily nějaké důvěrné, intimní informace o sobě. Se zmíněnou žádostí se nesetkal žádný z chlapců.
- Někteří žáci svým chováním usnadňují kybergroomerovi útok.
- Z vyhodnocení vyplývá, že 24 respondentů by šlo na schůzku s „kamarádem z internetu“. Podíl osob ochotných jít na osobní schůzku s člověkem, kterého znají jen přes internet, je u zvolených věkových skupin (12, 13, 14 a 15 let) různý. Ve věkové skupině 15 let je nejvyšší podíl jedinců ochotných jít na osobní schůzku s člověkem, kterého by znali jen přes internet, celkem se jedná o (44,8 %) z těchto patnáctiletých

chlapců a dívek. Při srovnání mezi chlapci a dívkami se ukázalo, že podíl jedinců ochotných jít na osobní schůzku je nejvyšší ve věkové skupině patnáctiletých chlapců, celkem (66,7 %).

- Neznámé osobě z internetu by se s tajemstvím svěřilo 24 (tj. 17,39 %) dětí, a to 13 (tj. 54,17 %) chlapců a 11 dívek (tj. 45,83 %). Díky své ochotě by se mohli stát potenciální obětí útočníka. Jako pozitivní se jeví, že 70,49 % chlapců a 74,03 % dívek by neřeklo „kamarádovi z internetu“ tajemství, o kterém by nechtěli, aby je věděl někdo jiný. Mezi věkovými skupinami (12, 13, 14 a 15 let) nejsou statisticky významné rozdíly co do podílu osob ochotných sdělit tajemství člověku, kterého by znaly jen přes internet.

- Celkem 17 respondentů (5 chlapců a 12 dívek) si myslí, že navazování nových známostí přes internet nemůže být nebezpečné.

- Že schůzka s „kamarádem z internetu“ nemůže být nebezpečná, se domnívá 14 respondentů (8 chlapců a 6 dívek).

- Všichni respondenti, kteří odpověděli, že by šli na schůzku s „kamarádem z internetu“, by dopředu o schůzce řekli nějaké jiné osobě, které důvěřují. Největší ochotu jít na tuto schůzku prokázali chlapci ve věku 15 let. Nejméně ochotní byli v tomto směru chlapci ve věku 12 let.

- Překvapivý je výsledek, že učiteli by se ze všech respondentů svěřil jen 1 chlapec.

- Na dotaz, jestli se dá věřit tomu, co o sobě jiní uživatelé uvádí na internetu, odpovědělo nejvíce respondentů „nevím“. Tuto variantu volily hlavně dívky.

- 28 respondentů (16 chlapců a 12 dívek) se domnívá, že není nebezpečné poskytovat osobní údaje (jako je např. jméno, datum narození, adresa bydliště, e-mail, telefonní číslo apod.) lidem, které by znali jen přes internet.

- Nejvíce respondentů zvolilo odpověď, že osobní informace nezveřejňuje. U varianty „jednou“ vychází podle množství odpovědí u jednotlivých druhů informací jako nejčastěji zveřejňovaná fotografie, pak následuje e-mail, nejméně to je telefonní číslo a adresa školy. U varianty „zveřejněno několikrát“ respondenti nejčastěji volili možnost e-mail, pak následuje fotografie, nejméně je to adresa školy a adresa bydliště.

- S vyhrožováním, že „kamarád z internetu“ prozradí tajemství, co ví na respondenta, pokud se s ním respondent nesejde, se setkal 1 chlapec a 3 dívky, což je 5,56% respondentů. Se zmíněným vyhrožováním se nesetkalo 94,44% respondentů.

8 SHRNUTÍ PRAKTICKÉ ČÁSTI

V praktické části diplomové práce jsme se snažili zmapovat, jak bezpečně se žáci 2. stupně základní školy chovají na internetu. Rovněž jsme se pokusili srovnat, jestli jsou mezi předem stanovenými věkovými skupinami žáků 2. stupně základních škol rozdíly v ochotě jít na osobní schůzku s neznámým člověkem a také zjistit, zda jsou mezi předem stanovenými věkovými skupinami žáků 2. stupně základních škol rozdíly v ochotě sdělovat důvěrné informace neznámé osobě na internetu.

Výzkumné šetření v diplomové práci přineslo souhrnné informace o uvedené problematice ve vybraných 2 základních školách. Objevuje se zde několik paradoxů, kdy například na jedné straně si žáci myslí, že navazování známostí na internetu může být nebezpečné, a na druhé straně více než polovina z nich má kamaráda na internetu nebo sdělují na internetu osobně neznámému člověku své soukromé informace.

Další zjištěnou skutečností je, že se někteří z respondentů již setkali s projevy typickými pro kybergrooming. Z uvedeného důvodu se jeví jako nezbytné i nadále zvyšovat informovanost dětí o existenci nebezpečí číhajících na internetu, a to nejen z toho důvodu, aby byly schopny rozpoznat nebezpečí a uměly se mu včas ubránit, ale především proto, aby zmenšovaly riziko případného útoku tím, že se budou při komunikaci přes internet chovat opatrně a zodpovědně. V tom jim mohou radou a informacemi pomoci nejen rodiče a učitelé, ale také nejrůznější projekty, které se zabývají problematikou nebezpečných jevů spojených s využíváním moderních komunikačních prostředků. Velmi účinná by v tomto směru mohla být pokračující spolupráce tvůrců preventivních programů především se školami. Informace, které o uvedené problematice děti získají v rámci školy, pak mohou doma poskytnout i svým rodičům a tím v mnoha případech vědomosti rodičů rozšířit, což by bylo přínosné nejen pro rodiče, kteří jsou již s uvedenou problematikou seznámeni, ale především pro ty, kteří o nebezpečích číhajících na internetu neví. Kromě školy je rovněž nutné se danému tématu věnovat hlavně v rodině, kde děti internet rovněž využívají. Je zřejmé, že k tomu, aby se dítě nedostalo do nebezpečí, může primární prevence výrazně přispět. A pokud se už dítě do nebezpečí přece jen dostane, musí děti i jejich rodiče vědět, že existují různá kontaktní místa, kam se mohou obrátit s žádostí o radu nebo o pomoc.

Pokud by výzkum proběhl celorepublikově, nebo alespoň ve větším množství škol, mohl by daným školám a potažmo celé společnosti podat podrobnější přehled o chování žáků při práci s internetem. Podle výsledků výzkumu realizovaném na dané škole by se následně tato škola mohla soustředit na oblasti, které je potřebné žákům více přiblížit a tak zvýšit jejich

informovanost. Pomocí statistických metod by bylo rovněž možné ověřit, zda mezi věkovými skupinami žáků existují statisticky významné rozdíly v podílu jedinců, kteří se svým chováním při práci s internetem vystavují zvýšenému riziku ohrožení nebezpečnými komunikačními jevy a na tyto se pak přednostně zaměřit.

ZÁVĚR

Většina příslušníků mladé generace si už nedovede představit svůj život bez moderního komunikačního prostředku, jakým je například mobilní telefon nebo počítač. Potřebují být „on line“, komunikovat s kamarády, vyhledávat na internetu nejrůznější informace a mít k dispozici další možnosti nabízené těmito komunikačními prostředky. Jejich používání se postupně stává životním standardem. Ale stále si ne všichni uživatelé dostatečně uvědomují, že technický rozvoj s sebou vždy přináší určitá rizika. Je tomu tak i v případě rozvoje komunikačních technologií a prostředků, kdy se na jedné straně uživatelům otevírá neskutečná možnost, jak poměrně jednoduchým způsobem přímo z domova komunikovat s kýmkoliv na celém světě, ale na druhé straně díky anonymitě, kterou internet poskytuje, se postupně objevují nové druhy nebezpečí, na které je potřeba se připravit, a během komunikace s nimi počítat. V médiích se sice stále častěji objevují případy, kdy se díky svému „naivnímu“ chování na internetu uživatelé dostali do nebezpečí, ovšem ke snížení rizika nestačí jen konstatování uvedené skutečnosti a zveřejňování případů. Je třeba neustále o těchto nebezpečích informovat, hlavně děti, a to i jinými způsoby než jejich pouhou medializací. Je nutné pomocí všech prostředků a metod, jak technických tak i netechnických, dosáhnout toho, aby si děti bezpečné chování na internetu osvojily a považovaly je za standard a za nedílnou součást komunikace.

Hlavním cílem mé diplomové práce bylo charakterizovat a popsat problematiku kybergroomingu a některých dalších nebezpečných aktivit spojených s užíváním moderních komunikačních technologií. Jedním z důvodů, proč jsem si zvolil toto téma, byla snaha připravit souhrnný materiál, který by umožnil zájemci dozvědět se o uvedené problematice více informací. V diplomové práci se nejprve věnuji vysvětlení samotné komunikace a moderním komunikačním technologiím, dále charakterizuji vybrané nebezpečné komunikační jevy páchané v prostředí internetu a mobilních sítí, včetně popisu hlavních rysů jednoho z nejnebezpečnějších jevů, kybergroomingu. Uvádím zde také možnosti obrany proti těmto jevům, a to nejen z hlediska primární prevence v rodině a ve škole, ale i přehled projektů zabývajících se pomocí ohroženým uživatelům, včetně kontaktů na školené odborníky. Cíl diplomové práce byl splněn, z čehož mám dobrý pocit, jelikož se domnívám, že díky vytvořenému materiálu čtenář získá potřebný přehled o dané problematice. Výsledky mé diplomové práce jsou využitelné nejen pro rodiče, aby díky ní získali ucelené informace, které by měl každý rodič mít, pokud chce co nejvíce eliminovat nebezpečí hrozící jeho dítěti ze strany moderních komunikačních prostředků a technologií, ale i pro ostatní, kteří o danou

problematiku projeví zájem. Diplomovou práci mohou využít například i učitelé, aby mohli zde uvedené informace předat svým žákům, a ti si pak osvojili bezpečné chování při zmíněné komunikaci. Výsledky praktické části výzkumného šetření mohou využít především pedagogičtí pracovníci základních škol, na kterých výzkumné šetření probíhalo, jelikož jim poskytuje ucelený přehled, jak bezpečně se na internetu chovají žáci jejich škol, a mohou se tak při práci s dětmi zaměřit na problematické oblasti a věkové skupiny žáků. Stejně tak mohou dotazník použitý v kvantitativním šetření využít i pedagogičtí pracovníci jiných škol k tomu, aby obdobným způsobem zmapovali situaci na škole, kde působí.

Při získávání podkladů k diplomové práci jsem měl možnost seznámit se s do té doby mně neznámými informacemi týkajícími se nebezpečí hrozícími při komunikaci přes internet, a to nejen při práci se zdroji využívanými při psaní diplomové práce, ale i díky své účasti na konferenci projektu E-Bezpečí konané v roce 2010, na které vystoupilo mnoho odborníků zabývajících se problematikou nebezpečných jevů spojených s využíváním moderních komunikačních prostředků a technologií. Dozvěděl jsem se tak mnoho zajímavých a podnětných informací, které využiji i ve svém osobním životě.

Je třeba si uvědomit, že jen uživatel informovaný a včas předem připravený na možná nebezpečí může rizika svého ohrožení minimalizovat. V souvislosti s pokračujícím rozvojem nových komunikačních technologií a stále se zvyšujícím počtem nově vznikajících nebezpečných aktivit se musíme připravit na nevyhnutelnou skutečnost, že i nadále budou vznikat různá nová doposud nám neznámá nebezpečí, a proto bude nutné i nadále se tématem nebezpečných komunikačních aktivit zabývat.

RESUMÉ

Diplomová práce se zabývá problematikou kybergroomingu a dalších nebezpečných aktivit spojených s využíváním moderních komunikačních technologií. Ve své práci seznamuji čtenáře s pojmem komunikace, upozorňuji na nebezpečné aktivity páchané v prostředí internetu a mobilních sítí, charakterizuji téma kybergrooming a předkládám návod, jak uvedeným nebezpečným jevům předcházet a jak minimalizovat jejich následky. Podávám také přehled preventivních programů zabývajících se ochranou dětí v souvislosti s využíváním moderních komunikačních prostředků a technologií. Výzkumné šetření, které jsem provedl pomocí dotazníkového šetření, zmapovalo, jak bezpečně se žáci 2. stupně základních škol chovají na internetu, jestli se setkávají s projevy typickými pro kybergrooming. Pomocí statistického testu dobré shody chí-kvadrát bylo rovněž ověřeno, že mezi předem danými věkovými skupinami respondentů existuje statisticky významný rozdíl co do podílu jedinců ochotných jít na schůzku s osobou, kterou by znali jen přes internet. Stejně tak bylo ověřeno, že mezi předem danými věkovými skupinami neexistuje statisticky významný rozdíl v podílu jedinců ochotných sdělit důvěrné informace (tajemství) člověku, kterého znají jen přes internet.

SEZNAM POUŽITÉ LITERATURY

Monografie:

BEDNAŘÍKOVÁ, I. *Sociální komunikace : texty k distančnímu a kombinovanému studiu.* Dotisk 1. vyd. z r. 2006. Olomouc : Univerzita Palackého v Olomouci, 2008. 79 s. ISBN 80-244-1357-4.

ČÍRTKOVÁ, L. *Moderní psychologie pro právníky : domácí násilí, stalking, predikce násilí.* 1. vyd. Praha : Grada, 2008. 150 s. Psyché (Grada). ISBN 978-80-247-2207-8.

DEVITO, J. A. *Základy mezilidské komunikace*. 1. vyd. Praha : Grada, 2001. 420 s. ISBN 80-7169-988-8.

DOSEDĚL, T. *21 základních pravidel počítačové bezpečnosti*. 1. vyd. Brno : CP Books, 2005. 50 s. ISBN 80-251-0574-1.

ELLIOTT, M. *Jak ochránit své dítě.* 1. vyd. Praha : Portál, 1995. 173 s. Rádci pro rodiče a vychovatele. ISBN 80-7178-034-0.

ERIKSON, E. H. *Dětství a společnost*, 1. vyd. Praha : Argo, 2002. 387 s. ISBN 80-7203-380-8.

FISCHER, S.; ŠKODA, J. *Speciální pedagogika : Edukace a rozvoj osob se somatickým, psychickým a sociálním znevýhodněním*. 1. vyd. Praha : Triton, 2008. 205 s. ISBN 978-80-7387-014-0.

CHRÁSKA, M. *Úvod do výzkumu v pedagogice*. 2. vyd. Olomouc : Univerzita Palackého v Olomouci, 2006. 200 s. ISBN 80-244-1367-1.

CHRÁSKA, M. *Metody pedagogického výzkumu : základy kvantitativního výzkumu : vědecký výzkum a analyzování, statistické metody, výhody a nevýhody kvantitativního přístupu, měření v pedagogickém výzkumu, metody zpracování výsledků, sběr dat.* 1. vyd. Praha : Grada, 2007. 265 s. ISBN 978-80-247-1369-4.

JAMES, L. *Phishing bez záhad.* 1. vyd. Praha : Grada, 2007. 282 s. ISBN 80-247-1766-2.

JANOUŠEK, J. Sociální komunikace. In VÝROST, J.; SLAMĚNÍK, I. *Sociální psychologie. 2. přepracované a rozšířené vydání.* Praha : Grada, 2008. s. 404 . ISBN 978-80-247-1428-8.

JIRÁK, J.; KÖPPLOVÁ, B. *Média a společnost*. 1. vyd. Praha : Portál, 2003. 207 s. ISBN 80-7178-697-7.

JIROVSKÝ, V. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha : Grada, 2007. 288 s. ISBN 978-80-247-1561-2.

KAVALÍR, A.; ROTTOVÁ, N. a kol. *Kyberšikana a její prevence – příručka pro učitele.* Plzeň : Dragon Press, 2009. 108 s. ISBN 978-80-86961-78-1. Dostupné z WWW: <http://www.varianty.cz/download/pdf/texts_160.pdf>.

KOPECKÝ, K. *Moderní trendy v e-komunikaci*. 1. vyd. Olomouc : Hanex, 2007. 98 s. ISBN 978-80-8578-378-0.

MUSIL, S. *Počítačová kriminalita : nástin problematiky : kompendium názorů specialistů.* 1. vyd. Praha : Institut pro kriminologii a sociální prevenci, 2000. 281 s. ISBN 80-86008-80-0.

PÖTHE, P. *Dítě v ohrožení*. 2. rozšířené vydání. Praha : G plus G, 1999. 186 s. ISBN 80-8610-321-8.

TEGZE, O. *Neverbální komunikace : co vám prozradí lidské chování a jednání, a jak toho využít.* 1. vyd. Praha : Computer Press, 2003, 482 s. ISBN 80-7226-429-X.

VITOVSKÝ, A. *Anglicko – český a česko – anglický výkladový slovník Internetu.* 1. vyd. Praha : Antonín Vitovský - AV software, 2004, 300 s. ISBN 80-901428-7-7.

VYMĚTAL, J. *Průvodce úspěšnou komunikací : efektivní komunikace v praxi*. 1. vyd. Praha : Grada, 2008. 322 s. ISBN 978-80-2472-614-4.

Články:

MUSÁLKOVÁ, Z. Jste na Facebooku? Internetové zločince zajímáte! *Magazín deníku Právo č. 28*. 16.7.2011. [cit. 2011-07-20]. ISSN 1211-2119.

Internetové zdroje:

Ashleigh Hall's killer had history of sexual violence. *BBC News* [online]. 8.3.2010. [cit. 2011-05-04] Dostupné z WWW: <http://news.bbc.co.uk/2/hi/uk_news/england/wear/8555844.stm>.

Attorney General to review 'happy-slap' sentence. *BBC News* [online]. 29.6.2009. [cit. 2011-06-24]. Dostupné z WWW: <http://www.bbc.co.uk/news/uk-england-london-10808090>.

BARTOSZ, J. Soud potrestal zneužití jednadvaceti chlapců osmi lety vězení. *iDNES* [online]. 5.2.2009. [cit. 2011-06-12]. Dostupné z WWW: <http://zpravy.idnes.cz/soud-potrestal-zneuziti-jednadvaceti-chlapcu-osmi-lety-vezeni-pvv-/krimi.aspx?c=A090205_101224_krimi_jba>.

BEDNÁŘ, M. Co je vlastně internet? *Owebu* [online]. 4.7.2007. [cit. 2011-04-12]. Dostupné z WWW: <http://owebu.bloger.cz/Internet/Internet>.

BEDNÁŘ, M. Historie vzniku internetu. *Owebu* [online]. 9.7.2007. [cit. 2011-05-02]. Dostupné z WWW: <http://owebu.bloger.cz/Internet/Historie-vzniku-internetu>.

BERSON, I. Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth. *University of South Florida* [online]. 2002. [cit. 2011-07-29]. Dostupné z WWW: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.104.6160&rep=rep1&type=pdf>.

BLAŽKOVÁ, J.; BLAŽEK, J. Je tu mladá holka, která mi ho…? *iDNES* [online]. 7.10.2006. [cit. 2011-08-23]. Dostupné z WWW: <http://zpravy.idnes.cz/je-tu-mlada-holka-ktera-mi-ho-dpr-/krimi.aspx?c=A061007_094833_domaci_jan>.

BOCÁN, J. Kyberšikana. *Policie České republiky* [online]. 2010. [cit. 2011-06-29]. Dostupné z www: <http://www.policie.cz/clanek/krajske-reditelstvi-policie-pdk-aktuality-aaa.aspx>.

BUBLANOVÁ, A. Za zneužití dvaceti chlapců půjde Hovorka na osm let do vězení. *Mediafax* [online]. 5.2.2009. [cit. 2011-08-14]. Dostupné z WWW: <http://www.mediafax.cz/krimi/2814724-Za-zneuziti-dvaceti-chlapcu-pujde-Hovorka-na-osm-let-do-vezeni>.

BURÝŠKOVÁ, L. Víte co je KYBERŠIKANA? *Policie České republiky* [online]. 11.12.2009. [cit. 2011-06-18]. Dostupné z WWW: <http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx>.

Co je hoax. *E-Bezpeci* [online]. 18.5.2008. [cit. 2011-09-23]. Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/25/40/lang,czech/>.

Co je to hoax. *Hoax* [online]. 2011. [cit. 2011-09-23]. Dostupné z WWW: <http://www.hoax.cz/hoax/co-je-to-hoax>.

Co je kyberšikana? *E-Bezpeci* [online]. 22.5.2009. [cit. 2011-07-27]. Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/14/6/lang,czech/>.

Co je to kybergrooming? *Nebuď oběť* [online]. 2010. [cit. 2011-07-27]. Dostupné z WWW: <http://www.nebudobet.cz/?page=kybergrooming>.

Desatero pro rodiče. *Internethotline* [online]. 10.7.2008. [cit. 2011-08-23]. Dostupné z WWW: <http://www.internethotline.cz/informace-pro-rodice/128-3.htm>.

Dívka se oběsila kvůli své nahé fotce na webu. *Aktuálně* [online]. 18.3.2009. [cit. 2011-09-19]. Dostupné z WWW: <http://aktualne.centrum.cz/zpravy/krimi/clanek.phtml?id=632277>.

DRESSSING, H.; MAULK-BACKER, H.; GASS, P. Posuzování stalkingu z kriminalistického hlediska. *iPrávník* [online]. 28.11.2007. [cit. 2011-07-22]. Dostupné

z WWW: <http://www.ipravnik.cz/cz/clanky/trestni-pravo/art_5000/posuzovani-stalkingu-z-kriminalistickeho-a-psychiatrickeho-hlediska.aspx>.

FRANZLOVÁ, O. Při napadání lidí se útočníci fotili. *iDNES* [online]. 19.1.2005. [cit. 2011-08-21]. Dostupné z WWW: <http://zpravy.idnes.cz/krimi.aspx?r=krimi&c=A050118_211928_krimi_sas>.

FRYDECKÁ, L. Nebezpečné pronásledování. *Bílý kruh bezpečí* [online]. [cit. 2011-08-11]. Dostupné z WWW: <http://www.bkb.cz/pomoc-obetem/trestne-ciny/nebezpecne-pronasledovani/>.

FUKA, F. FFFILM: Star Wars Kid. *Novinky* [online]. 30.7.2003. [cit. 2011-09-21] Dostupné z WWW: <http://www.novinky.cz/kultura/12434-fffilm-star-wars-kid.html>.

Happy slapping. *E-Bezpeci* [online]. 15.11.2008. [cit. 2011-06-23]. Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/71/39/lang,czech/>.

HLOUŠKOVÁ, L. Stalker aneb Někdo vás chce uštvat. *Reflecta* [online]. 2010. [cit. 2011-09-20]. Dostupné z WWW: < http://www.reflecta.cz/data/dn/000000322_dn.pdf>.

HUGHES, S. Antelope activate the acacia's alarm system. *NewScientist* [online]. 29.9.1990. [cit. 2011-07-12]. Dostupné z WWW: <http://www.newscientist.com/article/mg12717361.200-antelope-activate-the-acacias-alarm-system.html>. ISSN 0262-4079.

Chcete vědět, jak funguje mobilní síť? *Mobilmania* [online]. 11.8.2001. [cit. 2011-06-20]. Dostupné z WWW: <http://www.mobilmania.cz/clanky/chcete-vedet-jak-funguje-mobilni-sit/sc-3-a-1100650>.

CHOO, K. R. Online child grooming : a literature review on the misuse of social networking sites for grooming children for sexual offences. *Australian Institute of Criminology* [online]. 2009. [cit. 2011-07-29]. Dostupné z WWW: <http://www.aic.gov.au/documents/3/C/1/%7B3C162CF7-94B1-4203-8C57-79F827168DD8%7Drpp103.pdf>. ISBN 978-1-921532-33-7.

Internetová infrastruktura. *Český statistický úřad* [online]. 2009. [cit. 2010-01-21]. Dostupné z WWW: <http://czso.cz/csu/redakce.nsf/i/internetova_infrastruktura>.

JIRÁK, J. Mediální výchova - inspirace k realizaci. *Metodický portál RVP* [online]. 2004. [cit. 2011-07-29]. Dostupné z WWW: <http://clanky.rvp.cz/clanek/s/Z/87/MEDIALNI-VYCHOVA-%E2%80%93-INSPIRACE-K-REALIZACI.html/>.

KOPECKÝ, K. Leták bezpečný internet. *E-Bezpečí* [online]. 25.4.2009. [cit. 2012-01-17]. Dostupné z WWW: <http://cms.e-bezpeci.cz/component/option,com_docman/task,doc_details/gid,15/Itemid,2/lang,czech/>.

KOPECKÝ, K. Přehledový list Kyberšikana 1 a 2. *E-Bezpečí* [online]. 29.8.2009. [cit. 2012-01-17]. Dostupné z WWW: <http://cms.e-bezpeci.cz/component/option,com_docman/task,doc_details/gid,20/Itemid,2/lang,czech/>.

KOPECKÝ, K. Přehledový list Hoax. *E-Bezpečí* [online]. 25.11.2009. [cit. 2012-01-17]. Dostupné z WWW: <http://cms.e-bezpeci.cz/component/option,com_docman/task,doc_details/gid,29/Itemid,2/lang,czech/>.

KOPECKÝ, K. Přehledový list Kybergrooming. *E-Bezpečí* [online]. 25.11.2009. [cit. 2012-01-17]. Dostupné z WWW: <http://cms.e-bezpeci.cz/component/option,com_docman/task,doc_details/gid,30/Itemid,2/lang,czech/>.

KOPECKÝ, K. Přehledový list Stalking a kyberstalking. *E-Bezpečí* [online]. 25.11.2009. [cit. 2012-01-17]. Dostupné z WWW: <http://cms.e-bezpeci.cz/component/option,com_docman/task,doc_details/gid,31/Itemid,2/lang,czech/>.

KOPECKÝ, K. Kybergrooming nebezpečí kyberprostoru. *Net Univers*ity [online]. 2010. [cit. 2011-09-26]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5%3Akybergrooming-studie>.
ISBN 978-80-254-7573-7.

KOPECKÝ, K. Nebezpečí zvané kybergrooming II – metody manipulace. *Metodický portál* [online]. 30.11.2010. [cit. 2011-07-27]. Dostupné z WWW: <http://clanky.rvp.cz/clanek/c/Z/9985/nebezpeci-zvane-kybergrooming-ii-metody-manipulace.html/>.

KOPECKÝ, K. Stalking a kyberstalking : Nebezpečné pronásledování. *E-Nebezpečí* [online]. Olomouc : Net University, 2010. 14 s. [cit. 2011-07-29]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu>. ISBN 978-80-254-7737-3.

KOPECKÝ, K.; KREJČÍ, V. Co je vlastně sexting? *Sexting* [online]. 2010. [cit. 2011-09-19]. Dostupné z WWW: <http://www.sexting.cz/>.

KOPECKÝ, K.; KREJČÍ, V. Rizika virtuální komunikace. *Net University* [online]. 2010. [cit. 2011-09-26]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=10%3Abrozura>.
ISBN 978-80-254-7866-0.

KREJČÍ, V. Kyberšikana - kybernetická šikana. *Net University* [online]. 2010. 72 s. [cit. 2011-07-23]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=14%3Akybersikana-studie>.
ISBN 978-80-254-7791-5.

KUBÍK, J. Pozor na znuděné devianty. *iDNES* [online]. 7.4.2007. [cit. 2011-06-30]. Dostupné z WWW: <http://zpravy.idnes.cz/pozor-na-znudene-devianty-09w-/domaci.aspx?c=A070406_212057_nazory_mia>.

KUBÍK, M. Vývoj mobilních telefonů (1. díl). *Galaxie* [online]. 7.5.2006. [cit. 2011-05-14]. Dostupné z WWW: <http://www.galaxie.name/index.php?clanek=vyvoj-mobilnich-telefonu-1-dil>.

KUBÍKOVÁ, L. Děti z Měřína byly potrestány za šíření porna. *Žďárský deník* [online]. 29.10. 2009. [cit. 2011-09-19]. Dostupné z WWW: < http://zdarsky.denik.cz/zlociny-a-soudy/deti-z-merina-byly-potrestany-za-sireni-porna.html>.

Kybergrooming. *E-Bezpeci* [online]. 13.9.2008. [cit. 2011-07-27]. Dostupné z WWW: <http://cms.e-bezpeci.cz/content/view/42/35/lang,czech/>.

Kybergrooming. *E-Nebezpečí* [online]. 2010. [cit. 2011-08-24]. Dostupné z WWW: <http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=11%3Aprehledovy-list-kybergrooming>.

Methods of Predators. *Kids.yahoo* [online]. [cit. 20011-07-27]. Dostupné z WWW: <http://kids.yahoo.com/parents/online-safety/1706/4--Methods+of+Predators>.

Minimální preventivní program školní rok 2010/201 1- ZŠ Karla IV. [online]. 2010/2011. [cit. 2011-08-03]. Dostupné z WWW: <http://www.karlovka.cz/karlovka/skolni-poradenske-pracoviste/preventivni-program/>.

MŠMT ČR, *Metodický pokyn k primární prevenci sociálně patologických jevů u dětí, žáků a studentů ve školách a školských zařízeních, Čj.: 20006/2007 – 51*. [online]. Praha : MŠMT, 2007. 18 s. [cit. 2011-08-02]. Dostupné z www:<http://www.msmt.cz/file/7344_1_1/download/>.

MŠMT ČR. *Metodický pokyn ministra školství, mládeže a tělovýchovy k prevenci sociálně patologických jevů u dětí a mládeže, Čj.: 14514/2000 – 51*. [online]. Praha : MŠMT, 2000. 12 s. [cit. 2011-08-01]. Dostupné z WWW: <http://www.msmt.cz/file/7253_1_1/download/>.

Muž zřejmě zneužil víc jak dvacet chlapců, stojí před soudem. *Česká televize* [online]. 3.2.2009. [cit. 2011-05-02]. Dostupné z WWW: <http://www.ct24.cz/domaci/43695-muz-zrejme-zneuzil-vic-jak-dvacet-chlapcu-stoji-pred-soudem/>.

NEJEZCHLEBOVÁ, L. I mě zneužil deviant Hovorka. Ten ksicht nezapomenu, vzpomíná žena. *iDNES* [online]. 16.2.2009. [cit. 2011-07-21]. Dostupné z WWW: <http://zpravy.idnes.cz/i-me-zneuzil-deviant-hovorka-ten-ksicht-nezapomenu-vzpomina-zena-pyv-/krimi.aspx?c=A090213_154133_domaci_nel>.

NEJEZCHLEBOVÁ, L. Ozvěte se, vzkazují vyšetřovatelé obětem sexuálních deviantů. *iDNES* [online]. 18.2.2009. [cit. 2011-06-14]. Dostupné z WWW: <http://zpravy.idnes.cz/ozvete-se-vzkazuji-vysetrovatele-obetem-sexualnich-deviantu-p6t-/krimi.aspx?c=A090218_011257_krimi_nel>.

PILAŘ, J. *Pravidla pro rodiče a děti k bezpečnějšímu užívání internetu, Čj.: 11691/2004 – 24.* [online]. Praha : MŠMT, 2004. 5 s. [cit. 2011-08-02]. Dostupné z WWW: <http://www.msmt.cz/file/7349_1_1/download/>.

Počítače v domácnostech. *Český statistický úřad* [online]. 2009. [cit. 2011-05-25]. Dostupné z WWW: <http://www.czso.cz/xb/redakce.nsf/i/pocitace_v_domacnostech>.

Polská studentka se oběsila kvůli sexuální šikaně. *iDNES* [online]. 26.10.2006. [cit. 2011-09-22]. Dostupné z WWW: <http://zpravy.idnes.cz/polska-studentka-se-obesila-kvuli-sexualni-sikane-fsb-/zahranicni.aspx?c=A061026_141456_krimi_rez>.

PUTT, J. Responding to online child sexual grooming : an industry perspective. *Australian Institute of Criminology* [online]. 6.7.2009. [cit. 2011-07-29]. Dostupné z WWW: <http://www.aic.gov.au/en/publications/current%20series/tandi/361-380/tandi379/view%20paper.aspx>.

Seznam se bezpečně. *Seznam se bezpečně* [online]. 2011. [cit. 2011-07-27]. Dostupné z WWW: <http://www.seznamsebezpecne.cz/>.

STOKES, P. Ashleigh Hall: 'one mistake' cost teenager her life. *Telegraph* [online]. 8.3.2010. [cit. 2011-06-08]. Dostupné z WWW: <http://www.telegraph.co.uk/news/uknews/crime/7398085/Ashleigh-Hall-one-mistake-cost-teenager-her-life.html>.

Šikana a kyberšikana. *Protišikaně* [online]. 2011. [cit. 2011-07-28]. Dostupné z WWW: <http://proti-sikane.saferinternet.cz/sikana-a-kybersikana>.

ŠVAMBERK, A. Sedmnáctiletou oběť si našel na Facebooku, znásilnil ji a zavraždil. *Novinky* [online]. 9.3.2010. [cit. 2011-06-22]. Dostupné z WWW: <http://www.novinky.cz/zahranicni/evropa/194196-sedmnactiletou-obet-si-nasel-na-facebooku-znasilnil-ji-a-zavrazdil.html>.

TOSIN, S. Girl's rape 'filmed by teenagers on mobile'. *Timesonline* [online]. 18.6.2005. [cit. 2011-08-27]. Dostupné z WWW: <http://www.timesonline.co.uk/tol/news/uk/article534788.ece>.

VÁLKOVÁ, H. Česká podoba stalkingu podle § 354 TrZ v širších než jen trestněprávních souvislostech. *iPrávník* [online]. 26.3.2010. [cit. 2011-08-19]. Dostupné z WWW:

<http://www.ipravnik.cz/cz/clanky/pd_1/txtexpresion_dlu%C5%BEn%C3%ADku/art_6562/detail.aspx>.

VLACHOVÁ, M. Trestná činnost spojená s internetovou kriminalitou. *E-Bezpečí* [online]. 20.11.2009. [cit. 2011-06-12]. Dostupné z WWW: <http://www.e-bezpeci.cz/index.php/temata/dali-rizika/148-226>.

Vybavenost domácností pevnou telefonní linkou a mobilním telefonem. *Český statistický úřad* [online]. 2009. [cit. 2011-10-20]. Dostupné z WWW: <http://www.czso.cz/csu/redakce.nsf/i/1_vybavenost_domacnosti_pevnou_telefonni_linkou_a_mobilnim_telefonem>.

Vysvětlete babičce co je to Internet. *Owebu* [online]. 2004. [cit. 2011-03-15]. Dostupné z WWW: <http://owebu.bloger.cz/Internet/Vysvetlete-babicce-co-je-to-Internet>.

WOLAK, J.; FINKELHOR, D.; MITCHELL, K. Online "Predators" and Their Victims. *University of New Hampshire* [online]. 2008. 18 s. [cit. 2011-07-28]. Dostupné z WWW: <http://www.apa.org/pubs/journals/releases/amp-632111.pdf>.

Zneužil přes dvacet chlapců, dostal osm let. *Novinky* [online]. 5.2.2009. [cit. 2011-06-12]. Dostupné z WWW: <http://www.novinky.cz/krimi/160547-zneuzil-pres-dvacet-chlapcu-dostal-osm-let.html>.

SEZNAM POUŽITÝCH ZKRATEK

aj.	-	a jiné
apod.	-	a podobně
atd.	-	a tak dále
a.s.	-	akciová společnost
č.	-	číslo
ARPA	-	Advanced Research Projects Agency – agentura pro výzkum pokročilých obranných projektů
CERN	-	European Organization for Nuclear Research – Evropské středisko jaderného výzkumu
ČR	-	Česká republika
ČSÚ	-	Český statistický úřad
EU	-	Evropská unie
GSM	-	Global System for Mobile Communication – globální systém mobilních komunikací
ICQ	-	"I seek you" – „Hledám tě" – název klientského programu pro okamžitou komunikaci
ICT	-	Information and Communication Technology – informační a komunikační technologie – zařízení a prostředky výpočetní techniky
IT	-	Information Technologies – informační technologie
MS	-	Multimedia Messaging Service – služba multimediálních zpráv
MP3	-	formát audio komprese
MPP	-	Minimální preventivní program
MŠMT	-	Ministerstvo školství, mládeže a tělovýchovy
např.	-	například
OPL	-	Omamné a psychotropní látky
PDA	-	Personal Digital Assistant – kapesní počítač nebo zápisník, malé přenosné elektronické zařízení
PdF UP	-	Pedagogická fakulta Univerzity Palackého
PRVoK	-	Centrum prevence rizikové virtuální komunikace
RAND	-	Research ANd Development – výzkum a vývoj
Sb.	-	Sbírka zákonů

SIM	-	Subscriber Identity Module – identifikační karta uživatele v mobilní síti
SMS	-	Short Messaging Service – služba krátkých textových zpráv
s.	-	strana
s.r.o.	-	společnost s ručením omezeným
TCP/IP	-	Transmission Control Protocol/Internet Protocol – přenosový kontrolní protokol/síťový protokol
tj.	-	to je
TKI	-	telefonická krizová intervence
tzv.	-	takzvaný
UP	-	Univerzita Palackého
USA	-	United States of America – Spojené státy americké
VoIP	-	Voice over Internet Protocol – hlasové přenosy po internetu
webkamera	-	webová kamera – počítačové vstupní zařízení podobné fotoaparátu nebo kameře
Wi-Fi	-	Wireless Fidelity – bezdrátová síť
ZŠ	-	základní škola[192]

[192] Pro objasnění některých zkratek bylo využito: VITOVSKÝ, A. *Anglicko – český a česko – anglický výkladový slovník Internetu.* 1. vyd. Praha : Antonín Vitovský - AV software, 2004, 300 s. ISBN 80-901428-7-7.

SEZNAM TABULEK

Tabulka č. 1 - Příklady služeb dostupných prostřednictvím osobního počítače a mobilního telefonu 16
Tabulka č. 2 - Rozdíly mezi běžnou komunikací a e-komunikací 18
Tabulka č. 3 - Vývoj vybavenosti domácností osobním počítačem a připojením k internetu . 23
Tabulka č. 4 - Příklady trestných činů kybergroomerů 67
Tabulka č. 5 - Výpočet testového kritéria..... 101
Tabulka č. 6 - Rozdělení odpovědí respondentů, jak často poskytli jednotlivé druhy informací 106
Tabulka č. 7 - Výpočet testového kritéria..... 107

SEZNAM GRAFŮ

Graf č. 1 - Vybavenost domácností telefonem (% z celkového počtu domácností).....20
Graf č. 2 - Počet aktivních SIM karet (na 100 obyvatel dané země).....21
Graf č. 3 - Vybavenost domácností osobním počítačem a připojením k internetu v roce 2009 24
Graf č. 4 - Počet vysokorychlostních přípojek v ČR (v tisících).....25
Graf č. 5 - Počet domácností s nízkorychlostním a vysokorychlostním připojením k internetu 25
Graf č. 6 - Věkové rozvrstvení respondentů podle pohlaví.....96
Graf č. 7 - Máš nějakého kamaráda (člověka), se kterým ses seznámil/a na internetu a kterého neznáš z osobního setkání?.....99
Graf č. 8 - Šel/šla bys na schůzku s kamarádem (člověkem), kterého bys znal /a pouze přes internet?.....100
Graf č. 9 - Grafické znázornění odpovědí na otázku týkající se ochoty jít na osobní schůzku s neznámou osobou u jednotlivých věkových kategorií chlapců a dívek.....102
Graf č. 10 - Komu bys řekl/a (by ses svěřil/a) v případě, že bys šel/a na schůzku s kamarádem (člověkem), kterého bys neznal/a osobně, ale jen přes internet?.....103
Graf č. 11 - Myslíš si, že by se dalo věřit tomu, co by ti o sobě na internetu tvrdil (říkal), kamarád (člověk), kterého bys neznal/a osobně, ale jen z internetu?.....104
Graf č. 12 - Myslíš si, že může být nebezpečná schůzka s člověkem, se kterým by ses znal/a pouze přes internet?.....104
Graf č. 13 - Jak často jsi na internetu poskytl/a některou z následujících informací?.....105
Graf č. 14 - Řekl/a bys kamarádovi (člověku), kterého bys znal/a pouze přes internet tajemství, o kterém bys nechtěl/a, aby věděl někdo jiný? 107
Graf č. 15 - Grafické znázornění odpovědí na otázku týkající se ochoty sdělit tajemství člověku, kterého by znaly jen přes internet u jednotlivých věkových kategorií chlapců a dívek. 108
Graf č. 16 - Myslíš si, že je nebezpečné poskytovat osobní údaje, jakými jsou například jméno, datum narození, adresa bydliště, telefonní číslo, e-mail apod. lidem, které bys znal/a jen z internetu? 109
Graf č. 17 - Myslíš, že může být nebezpečné navazování nových známostí přes internet?...110

Graf č. 18 - Odkud víš, jak vypadá tvůj kamarád (člověk), kterého znáš pouze přes internet a ne osobně?.....111
Graf č. 19 - Chtěl se s tebou osobně sejít někdo, koho znáš jen přes internet?.....112
Graf č. 20 - Nabízel ti kamarád (člověk), kterého znáš pouze z internetu například peníze, mobilní telefon, telefonní kredit nebo nějaký jiný úplatek za to, že se s ním sejdeš?112
Graf č. 21 - Poslal ti kamarád (člověk), kterého znáš pouze z internetu, nějaké dárky? Například peníze, mobilní telefon, kredit nebo něco podobného?.....113
Graf č. 22 - Chtěl/a od tebe kamarád (člověk), kterého znáš pouze z internetu, abys mu za dárky co ti dal, na oplátku poslal/a například svoji fotografii, číslo mobilního telefonu nebo sdělil/a nějaké důvěrné, intimní informace o sobě?.....114
Graf č. 23 - Chtěl po tobě kamarád (člověk), kterého znáš pouze z internetu, aby o vašem přátelství nevěděli rodiče?.....114
Graf č. 24 - Vyhrožoval ti (vydíral tě, nutil tě) kamarád (člověk), se kterým se znáš pouze z internetu, že když se s ním nesejdeš, tak na tebe prozradí tajemství, které na tebe ví?.....115

SEZNAM PŘÍLOH

Příloha č. 1 - Dotazník – v textu strana č. 96
Příloha č. 2 - Přehledový list Kybergrooming – v textu strana č. 77
Příloha č. 3 - Přehledový list Kyberšikana 1 a 2 – v textu strana č. 77
Příloha č. 4 - Přehledový list Stalking a kyberstalking – v textu strana č. 77
Příloha č. 5 - Přehledový list Hoax – v textu strana č. …….. 77
Příloha č. 6 - Leták bezpečný internet – v textu strana č. 77

Příloha č. 1 - Dotazník – v textu strana č. 96

Věk: 11, 12, 13, 14, 15, 16, 17, ….. **Třída, do které chodíš:** 6., 7., 8., 9.
Pohlaví: chlapec / dívka

1. Využíváš internet?

a) Ano b) Ne

2. Máš nějakého kamaráda (člověka), se kterým ses seznámil/a na internetu a kterého neznáš z osobního setkání?

a) Ano b) Ne

Pokud na tuto otázku odpovíte volbou **b) Ne**, pak u otázek č. **3**, **5**, **6**, **10**, **11, 14 a 16** zvolte vždy odpověď - **nesplňuji podmínky v zadání otázky.**

3. Odkud víš, jak vypadá tvůj kamarád (člověk), kterého znáš pouze přes internet a ne osobně?

a) podle toho, co mi o sobě napsal/a přes internet
b) z jeho/její fotografie/videa, které/rou uvedl/a na internetu
c) z fotografie, kterou mi poslal/a
d) z jeho/její webkamery
e) od spolužáka
f) z jiného zde neuvedeného zdroje …….
g) nevím jak vypadá
h) nesplňuji podmínky v zadání otázky

4. Šel/šla bys na schůzku s kamarádem (člověkem), kterého bys znal/a pouze přes internet?

a) Ano b) Ne

5. Chtěl se s tebou osobně sejít někdo, koho znáš jen přes internet?

a) ne
b) ano, jedna osoba
c) ano, několik osob
d) nepamatuji si
e) nesplňuji podmínky v zadání otázky

6. Nabízel ti kamarád (člověk), kterého znáš pouze z internetu, například peníze, mobilní telefon, telefonní kredit nebo nějaký jiný úplatek za to, že se s ním sejdeš?

a) pouze jednou b) několikrát c) nikdy d) nesplňuji podmínky v zadání otázky

7. Komu bys řekl/a (by ses svěřil/a) v případě, že bys šel/šla na schůzku s kamarádem (člověkem), kterého bys neznal/a osobně, ale jen přes internet?

a) rodičům
b) učiteli
c) jiné dospělé osobě
d) jinému kamarádovi/kamarádům z internetu
e) jinému kamarádovi/kamarádům kterého/které znám osobně
f) sourozenci

g) spolužákům
h) jiné zde neuvedené osobě …….
i) nikomu

8. Myslíš si, že by se dalo věřit tomu, co by Ti o sobě na internetu tvrdil (říkal), kamarád (člověk), kterého bys neznal/a osobně, ale jen z internetu?

a) určitě ano
b) spíše ano
c) nevím/nedokážu říct
d) spíše ne
e) určitě ne

9. Myslíš si, že může být nebezpečná schůzka s člověkem, se kterým by ses znal/a pouze přes internet?

a) určitě ano
b) spíše ano
c) nevím/nedokážu říct
d) spíše ne
e) určitě ne

10. Poslal ti kamarád (člověk), kterého znáš pouze z internetu nějaké dárky? Například peníze, mobilní telefon, kredit nebo něco podobného?

a) pouze jednou b) několikrát c) nikdy d) nesplňuji podmínky v zadání otázky

11. Chtěl/a od tebe kamarád (člověk), kterého znáš pouze z internetu, abys mu za dárky co ti dal, na oplátku poslal/a například svoji fotografii, číslo mobilního telefonu nebo sdělil/la nějaké důvěrné, intimní informace o sobě?

a) pouze jednou b) několikrát c) nikdy d) nesplňuji podmínky v zadání otázky

12. Jak často jsi někomu na internetu poskytl/a některou z následujících informací?

Vlastní fotografii	a) pouze jednou	b) několikrát	c) nikdy
Adresu, kde bydlíš	a) pouze jednou	b) několikrát	c) nikdy
Adresu školy, do které chodíš	a) pouze jednou	b) několikrát	c) nikdy
Číslo tvého mobilního telefonu	a) pouze jednou	b) několikrát	c) nikdy
Tvůj e-mail	a) pouze jednou	b) několikrát	c) nikdy

13. Řekl/a bys kamarádovi (člověku), kterého bys znal/a pouze přes internet tajemství, o kterém bys nechtěl/a, aby věděl někdo jiný?

a) Ano b) Ne c) Nevím

14. Chtěl po tobě kamarád (člověk), kterého znáš pouze z internetu, aby o vašem přátelství nevěděli rodiče?

a) Ano b) Ne c) nesplňuji podmínky v zadání otázky

15. Myslíš si, že je nebezpečné poskytovat osobní údaje, jakými jsou například jméno, datum narození, adresa bydliště, telefonní číslo, e-mail apod. lidem, které bys znal/a jen z internetu?

a) určitě ano b) spíše ano c) nevím/nedokážu říct d) spíše ne e) určitě ne

16. Vyhrožoval ti (vydíral tě, nutil tě) kamarád (člověk), se kterým se znáš pouze z internetu, že když se s ním nesejdeš, tak na tebe prozradí tajemství, které na tebe ví?

a) Ano b) Ne c) nesplňuji podmínky v zadání otázky

17. Myslíš, že může být nebezpečné navazování nových známostí přes internet?

a) Ano b) Ne c) Nevím

Příloha č. 2 - Přehledový list Kybergrooming – v textu strana č. 77[193]

KYBERGROOMING

Co je kybergrooming?

Kybergrooming je označení pro jednání osoby, která se snaží zmanipulovat vyhlédnutou oběť a donutit ji k osobní schůzce. Útočník s obětí komunikuje zejména prostřednictvím chatu, SMS zpráv, ICQ a Skypu.

Jak vypadá manipulace

1. Ukázky získávání informací o oběti

- *Máš počítač ve svém pokojíku, nebo v obýváku? Já v pokojíčku.* (Zjišťuje, jestli někdo jiný může sledovat komunikaci.)
- *Bydlíš v Praze? Já jsem z Brna.* (Zjišťuje, zda má smysl zaměřit se na lokalitu, např. kvůli potenciálnímu vloupání.)
- *Jaké máš zájmy? Já mám rád počítačové hry a U2.* (Zjišťuje zájmy oběti, aby věděl, na co se zaměřit v případě uplácení dítěte dárkem.)
- *Kolik je ti let? Mně je 16.* (Děti svůj věk prozrazují podstatně později než na začátku komunikace. V této oblasti jsou opatrnější.)
- *Pošli mi fotku, já ti pošlu svoji.* (Získává kompromitující materiály, které může využít k vydírání oběti.)
- *Chci ti poslat suprovou MMSku, napiš mi své číslo.* (Získává telefonní číslo oběti.)
- *Máš kluka/holku?* (Zjišťuje, zda má oběť někoho, komu se může svěřit.)
- *V kolik chodí vaši do práce? Jsem doma od 6 do 8 samsama.* (Zjišťuje, kdy je byt prázdný kvůli možnému vloupání.)

2. Ukázky izolování oběti od okolí

- *Rodiče ti nerozumí, já ano, mně se můžeš svěřit se svými problémy.*
- *Neříkej o tom ostatním dětem, žárlily by.*
- *Neříkej o tom mamince. Nenáviděla by tě.*
- *Dospělí to nepochopí, já ano.*
- *Mně se můžeš svěřit, můžeme mít tajemství.*
- *Jsem na tom podobně, svěř se, zůstane to mezi námi.*

3. Ukázky vydírání

- *Potřebuji s tebou nutně mluvit osobně. Jsi moje láska a nemůžu bez tebe žít.*
- *Jestli se se mnou nesejdeš, zabiju se.*
- *Jestli mi neřekneš své právě jméno, zveřejním tvoji fotku a napíšu o tobě, že jsi lesba!!!*
- *Jestli ke mně nepřijdeš, všem pošlu tvou upravenou fotku s nápisem: JSEM DĚVKA!*
- *Jestli to neuděláš, napíšu tvé matce, že se mnou chrápeš!*

Jak kybergroomer postupuje?

Etapy kybergroomingu

1. Vzbuzení důvěry a snaha izolovat oběť

Kybergroomer se staví v komunikaci do pozice osoby, která dítěti rozumí, která chápe jeho problémy, která má stejné problémy a pomůže je dítěti vyřešit. Často s dětmi řeší citlivá témata, jako jsou např. manželské problémy, sexuální život dospělých apod.

Zároveň se snaží izolovat dítě od okolí, např. rodičů nebo kamarádů.

V této etapě kybergroomer obvykle získá e-mail dítěte, telefonní číslo na mobil, jeho adresu nebo adresu školy, kterou navštěvuje. V mnohých případech pak dítěti ukazuje nebo zasílá pornografické materiály.

2. Poplácení dárky nebo různými službami, budování kamarádského vztahu

Získaný vztah kybergroomer posiluje dárky (penize, mobilní telefon, drahé hračky a občerstvení) nebo službami (návštěva kina). Tyto dárky dává dítěti bez konkrétní příčiny nebo za ně požaduje např. fotografie apod.

3. Vyvolání emoční závislosti oběti na útočníkovi

Kybergroomer zná nejtajnější tajemství dítěte. Dítě netuší, jak mocnou zbraň tím útočníkovi poskytlo. Kybergroomer se pro něj stává jediným důvěrným přítelem. Naopak rodičům se se svými problémy odmítá svěřovat a často jim také lže o tom, jak a s kým tráví svůj volný čas.

4. Osobní setkání

Oblíbeným programem osobního setkání je procházka v parku, návštěva ZOO nebo kina, diskotéky či klubu, případně přímo návštěva bytu kybergroomera.

5. Sexuální obtěžování, zneužití nebo manipulace

Poslední etapou je obvykle sexuální obtěžování a zneužití dítěte, může jít ale také o fyzické mučení nebo různé formy manipulace (např. nucení k terorismu).

Realizováno v rámci projektu Prevence nebezpečných komunikačních praktik spojených s elektronickou komunikací pro pedagogy a nepedagogy.

[193] KOPECKÝ, K. Přehledový list Kybergrooming. *E-Bezpečí* [online]. 25.11.2009. [cit. 2012-01-17]. Dostupné z WWW: <http://cms.e-bezpeci.cz/component/option,com_docman/task,doc_details/gid,30/Itemid,2/lang,czech/>.

KYBERGROOMING

Případy kybergroomingu

37 % čtrnáctiletých dětí komunikuje přes internet s cizími lidmi a 14 % dětí se s takovými lidmi dokonce osobně schází. Více než třetina dětí ve věku od 14 do 15 let cizím lidem přes internet předává své osobní a kontaktní údaje.

Usvědčený deviant Pavel H. (vrátný v tiskárnách) využíval k seznamování se s oběťmi např. diskuzní fóra, chat či inzeráty. **Předstíral, že vybírá děti z dětských domovů do soutěže Dítě VIP** apod. Osobní informace a fotografie, které od dětí získal, pak použil k vydírání. **Kombinací vydírání a uplácení přiměl některé děti k osobní schůzce.**

Důsledky:
Znásilňování a zneužívání 20 chlapců. Byl uvězněn na 8 let.

Britský pedofil Michael Wheeler používal k seznamování se s dívkami veřejný chat. S jednou ze zneužitých dívek se seznámil, když jí bylo 11 let. **Postupně ji manipuloval, až se na něm stala citově závislá. Krátce po jejích 13. narozeninách ji začal sexuálně obtěžovat. Kontaktoval a obtěžoval také její kamarádky.**

Důsledky:
11 sexuálních útoků, zneužití 2 dívek (13 let). Byl uvězněn na 3 roky.

Bývalý pošťák Douglas Lindsell **získával sympatie dívek např. tvrzením, že má rakovinu.** Vedl si databázi dívek, se kterými se seznámil online, plánoval si s nimi osobní setkání a znásilnění, **některým posílal své nahé fotografie nebo je nutil např. k obnažování.** Dvě dívky (13 a 14 let) dokonce přiměl k osobní schůzce. **Jednu z nich se snažil nalákat do svého auta a znásilnit.**

Důsledky:
Sexuální obtěžování několika dívek, pokus o znásilnění. Byl uvězněn na 5 let.

Zfalšované zprávy jako nástroj k manipulaci

Kybergroomeři se někdy snaží získat informace od oběti pomocí zfalšovaných zpráv o výhře. Když oběť splní jednoduché podmínky, získá např. nový počítač, telefon apod. Tyto zprávy využívají kombinace tlaku (např. časové omezení nabídky, limitované množství výrobků) a uvolnění (za tlakem následuje nějaká méně důležitá informace - např. vyber si barvu přístroje, který ti pošleme).

Ahoj, vyhrál jsi v soutěži „Dítě chatu VIP" hlavní cenu! Tou je skvělá večeře v centru Prahy v luxusním prostředí firmy Max. Akce pouze pro děti do 15 let!
Odpověz na tento e-mail a získej bližší podrobnosti!

Milí žáci, máte jedinečnou možnost získat ZDARMA nový luxusní počítač se 4 procesory – ideální pro hraní počítačových her a surfování. Stačí nám napsat na e-mailovou adresu vaše jméno, příjmení a adresu, kam máme počítač doručit. Posledních 30 kusů! Akce pouze pro žáky základních škol!

Ahoj, tvoje e-mailová adresa byla náhodně vybrána s dalšími 20 adresami ze 4 milionů dětí v České republice. Vyhráváš nový mobilní telefon Apple iPhone 4G. Odpověz na tento e-mail, připoj své jméno, příjmení a adresu, kam máme telefon poslat. Nezapomeň připojit barvu iPhone, o který máš zájem (černá nebo bílá). Vše zdarma! Odpověz do 5 dnů!

Jak se chránit?

Nejlepší ochranou před kybergroomingem je prevence. Ta spočívá zejména v dobré komunikaci rodičů s dětmi. Rodiče by měli dětem věnovat dostatek času, aby si mohli vytvořit důvěrný vztah. Děti musí vědět, že se mohou rodičům svěřit s jakýmikoliv problémy. Zároveň je nutné, aby byly děti informovány o nebezpečí, které jim hrozí, a o tom, jak se mu vyhnout.

- **Nenechte se oklamat sliby na získání láskyplného vztahu.**
- **Přemýšlejte o „online přátelstvích", všímejte si nesrovnalostí v tom, co vám „online přítel" tvrdí.**
- **Zvažte, proč někdo chce, abyste drželi váš vztah v tajnosti, nebo proč se ptá na velmi osobní témata.**
- **Vytyčte si své osobní hranice s ohledem na rozhovory o sexu. Nebojte se říct NE kybersexu.**
- **Nikomu nesdělujte své osobní údaje.**
- **Nikdy nechoďte na osobní schůzku, aniž byste o ní řekli rodičům.**
- **Online přátelé by měli zůstat online přáteli.**

Příloha č. 3 - Přehledový list Kyberšikana 1 a 2 – v textu strana č. 77[194]

KYBERŠIKANA

Co je kyberšikana?

Kyberšikana je šikanování jiné osoby (ubližování, ztrapňování, obtěžování, ohrožování, zastrašování) s využitím internetu, mobilních telefonů či jiných informačních technologií.

Projevy kyberšikany

1. **Pomlouvání, zastrašování, urážení, zesměšňování nebo jiné ztrapňování** (prostřednictvím e-mailu, SMS zpráv, v chatu nebo v diskuzi).
2. **Pořizování zvukových záznamů, videí či fotografií, jejich upravování a následné zveřejňování s cílem poškodit zachycenou osobu.**
3. **Vytváření internetových stránek, které urážejí, pomlouvají či ponižují konkrétní osobu.**
4. **Zneužívání cizího účtu** (e-mailového, diskuzního apod.).
5. **Vydírání pomocí mobilu nebo internetu.**
6. **Obtěžování a pronásledování voláním, psaním zpráv nebo prozváněním.**

Kyberšikana a tradiční šikana

Kyberšikana a tradiční šikana mají jednu věc společnou - jejich cílem je někomu ublížit nebo ubližovat, ať fyzicky či psychicky. Kyberšikana může být spojena s tradiční šikanou (např. nahrávání fyzického týrání spolužáka). Moderní technologie (internet, mobilní telefony) nám umožňují pohybovat se ve virtuálním světě, který se liší od reálného světa. Tak, jako se liší virtuální svět od světa reálného, liší se kyberšikana od tradiční šikany. Ve virtuálním světě mohou být lidé anonymní, mohou vzájemně komunikovat, i když nejsou fyzicky přítomni, a pokud s někým v kontaktu být nechtějí, mohou komunikaci snadno ukončit.

Znaky kyberšikany

A. Anonymita útočníků

Útočníci většinou vystupují ve virtuálním prostředí pod přezdívkou (nickem), používají pro oběť neznámou e-mailovou adresu, telefonní číslo atd., proto oběť jen zřídka přijde na to, kdo na ni útočí.
Anonymita může být často zdánlivá, protože totožnost útočníků lze s využitím vhodné technologie odhalit.

B. Kde a kdy se s kyberšikanou setkáme

Zatímco u tradiční šikany lze předpokládat, kdy a kde k útoku dojde (např. ve škole, na hřišti), s kyberšikanou se můžeme setkat kdykoliv a kdekoliv. Oběti kyberšikany se můžeme stát vždy, když budeme připojeni k internetu nebo když budeme mít u sebe svůj mobilní telefon.
V takovém případě se před kyberútokem nemáme kam schovat. Útočník si nás může najít i v „bezpečí domova" a klidně to může být i o půlnoci.

C. Kdo jsou útočníci a oběti

Ve virtuálním světě nezáleží na věku, pohlaví, síle, postavení v sociální skupině (partě) ani úspěšnosti útočníka nebo oběti ve společnosti.
Původcem kyberšikany může být každý, kdo má potřebné znalosti informačních a komunikačních technologií, tedy i fyzicky slabý jedinec. Původce kyberšikany bývá někdy také sám její oběti. Oběti kyberútoku se často stávají děti, které tráví více času ve virtuálním světě a jsou na internetu nebo mobilním telefonu závislé. Na internetu také navazují vztahy, zatímco ve skutečném světě nemají příliš mnoho kamarádů.

D. Jak se chovají lidé ve virtuálním prostředí

Ve virtuálním prostředí se lidé chovají jinak než v reálném světě. Mohou udávat jiný věk, jiné pohlaví, jiné povolání, a záměrně tak manipulovat s těmi, se kterými komunikují. Ve virtuálním světě se někteří lidé chovají méně opatrně než v reálném světě (jsou odvážnější v komunikaci, probírají citlivá témata, komunikují často bez zábran apod.). Někdy zkoušejí to, co by se v reálném světě báli udělat (např. útočit na jiné osoby, vyhrožovat jim nebo je vydírat), protože je menší šance na jejich odhalení, a nevidí, jaký dopad má jejich chování na oběti.

E. Při šíření kyberšikany pomáhá útočníkovi publikum

Prostředky kyberšikany (zprávy a pořízené záznamy) se dají jednoduše rozesílat dál, proto může mít kyberšikana velmi početné „publikum". Útočník nemusí oběť napadat opakovaně, stačí, když citlivé zprávy nebo nahrávky publikuje na internetu a o jejich šíření se pak postarají jiní.
Toto publikum zvyšuje intenzitu útoku, a tím zhoršuje jeho dopad na oběť.

F. Oběť kyberšikany není snadné rozpoznat

Kyberšikana je většinou spojena s psychickým týráním oběti, které není snadné poznat (na rozdíl od modřin, jež mohou doprovázet fyzickou šikanu). Oběti kyberšikany jsou často uzavřené do sebe a nekomunikují o problémech s okolím (rodiči). Důvodů pro takové chování může být více (strach, stud, rodiče nerozumí počítačům, dítě nepozná, že jde o projevy psychického šikanování apod.).

G. Kyberšikana může být způsobena i neúmyslně

Kyberšikana může být výsledkem toho, že špatně odhadneme situaci nebo reakci daného člověka (náš žert může způsobit bolest).

Realizováno v rámci projektu Pravidla nebezpečných komunikačních praktik spojených s elektronickou komunikací pro pedagogy a nepedagogy.

bezpečí vodafone GAČR

[194] KOPECKÝ, K. Přehledový list Kyberšikana 1 a 2. *E-Bezpečí* [online]. 29.8.2009. [cit. 2012-01-17]. Dostupné z WWW: <http://cms.e-bezpeci.cz/component/option,com_docman/task,doc_details/gid,20/Itemid,2/lang,czech/>.

KYBERŠIKANA

Případy kyberšikany

První zveřejněný závažný případ kyberšikany:
Oběť: Ghyslain Raza (14 let, Kanada), známý jako Star Wars Kid

Student střední školy Ghyslain Raza natočil **sám sebe při předvádění bojové scény** z Hvězdných válek. Snažil se napodobit postavu Dartha Maula. **Spolužáci mu nahrávku ukradli a pro pobavení ostatních ji zveřejnili na internetu.** Během několika týdnů nahrávka obletěla celý svět, byla mnohokrát upravována, vzniklo množství webů a blogů, na kterých byl chlapec zesměšňován. Ghyslainovi fanoušci napsali petici tvůrcům Hvězdných válek, aby byl obsazen do některé z epizod. Byl parodován dokonce v seriálech (např. South Park, American Dad, Veronica Mars).

Důsledky:
Ghyslain se psychicky zhroutil a musel se dlouhodobě léčit.

Jeden z prvních a zároveň nejtragičtějších evropských případů:
Oběť: Anna Halman (14 let, Polsko)

Pět spolužáků podrobilo Annu před celou třídou sexuální šikaně (strhali z ní šaty a předstírali, že ji znásilňují). **Celou scénu nahráli na mobil a vyhrožovali dívce, že nahrávku zveřejní na internetu.** To také později udělali, video umístili na stránku YouTube. Pro Annu to měla být pomsta za to, že s jedním z chlapců nechtěla chodit.

Důsledky:
Anna spáchala sebevraždu.

Oběť: Patrick Ryan Halligan (13 let, USA)

Patrick byl oběti fyzické šikany. Aby se mohl bránit, začal se učit kickbox. **Útočníkům se postavil, ale prohrál.** Za jeho „drzost" se mu chtěli pomstít. **Využili k tomu spolužačku, která pak na internetu předstírala, že má o Patricka zájem. Jejím úkolem bylo získat o Patrickovi co nejvíce osobních informací. Ty poté zveřejnila na školním webu a označila Patricka za gaye.** Na chatu si z něj dělali legraci i další spolužáci. Dokonce vytvořili www stránku, na niž vyhlásili soutěž o jeho co nejvíce zesměšňující fotografii. Stránka měla velký „úspěch" – postupně na ni začali přispívat žáci celé školy.

Důsledky:
Patrick se oběsil.

Oběť: Jessica Logan (18 let, USA)

Po rozchodu zveřejnil Jessičin bývalý přítel její intimní fotografie, které mu poslala v době, když spolu ještě chodili. Od té doby **byla vystavena neustálému posměchu ze strany spolužáků.** Útoky nepřestaly ani poté, co Jessica vystoupila v televizi a požádala spolužáky, aby ji nechali na pokoji.

Důsledky:
Jessica spáchala sebevraždu.

Oběť: Megan Meier (13 let, USA)

Megan měla komplexy ze svého vzhledu. **Na stránkách MySpace se seznámila s 16letým chlapcem Joshem Evansem. Několik týdnů spolu prožívali virtuální lásku,** aniž by se někdy osobně setkali. **Pak ji Josh začal psát zprávy plné nenávisti, jak je odporná a jak by byl svět bez ní lepší.**

Důsledky:
Megan se oběsila.

Při vyšetřování se zjistilo, že **za chlapce se vydávala 50letá Lori Drew, matka Meganiny bývalé kamarádky.** Tímto způsobem se Megan chtěla pomstít za to, že už nechce kamarádit s její dcerou. Lori pro kyberšikanu využila i kolegy z práce. Po smrti Megan neprojevila Lori žádné výčitky a celou záležitost vnímala jako nevinný žert.

Jak se chránit?

- **Vždy respektujte ostatní uživatele.**
- **Dobře si rozmyslete, co odesíláte a komu.**
- **Nakládejte se svým heslem jako s vlastním životem.**
- **Nikdy nikomu neznámému nesdělujte své osobní údaje (vystupujte pod obecnou přezdívkou, nikde neuvádějte své jméno a příjmení, adresu atd.), podle nichž by vás mohl útočník vystopovat.**
- **Nikomu nedávejte své fotografie nebo fotografie své rodiny.**
- **Seznamte se s pravidly dané služby, ať víte, co je zakázáno dělat.**

KYBERŠIKANA

Projevy kyberšikany s příklady

Obtěžování a pronásledování oběti spojené s kyberšikanou

Jedná se o tzv. **kyberstalking**. Kyberstalking spojuje více praktik kyberšikany, jako jsou intenzivní obtěžování (volání, prozvánění, psaní zpráv) a ponižování, vyhrožování nebo zastrašování oběti. Může vést i k fyzické šikaně a v krajních případech může být zakončeno i smrtí oběti. Útočník se chová jako lovec a oběť je pro něj kořist.

Gábina chodila s Petrem. Když se s ním rozešla, Petr se s rozchodem nemohl smířit a začal ji doslova bombardovat různými zprávami. Prosil, ať se k němu vrátí, vyhrožoval jí, urážel ji, pomlouval před jejími známými, vyhrožoval, že sobě i jí fyzicky ublíží, obtěžoval i její rodiče a známé. Často také Gábině telefonoval.

Krádež identity, zneužití cizí identity ke kyberšikaně

Útočník získá přístup k cizímu účtu (e-mailu, chatu apod.). Pod cizím jménem rozesílá nevhodné zprávy nebo jiné materiály. Snaží se tím dostat majitele účtu do problémů, ohrozit ho nebo poškodit jeho pověst a vztahy. Útočník může také manipulovat s účtem uživatele (mazat zprávy, měnit osobní informace o majiteli účtu, mazat a měnit kontakty, fotografii majitele účtu apod.). Informace, které z účtu získá, se může snažit dále zneužít.

Tereza tajně pozorovala Kláru, když se přihlašovala ke svému e-mailovému účtu. Viděla její heslo. Pak se přihlásila na Klářin účet a začala z něj posílat hrubé zprávy jejím známým. Kláře pak dalo velkou práci vysvětlit známým, že zprávy nepsala ona.

Co je sexting?

Slovo sexting je složeninou slov sex a textování.

Sexting je elektronické rozesílání textových zpráv, fotografií nebo videa se sexuálním obsahem.

Tyto záznamy poté mohou být zveřejněny na internetu, zejména dojde-li k ukončení vztahu mezi dotyčnými osobami. Mohou být také použity k vydírání apod.

Jak se bránit?

- **UKONČETE** - Nekomunikujte s útočníkem, nemstěte se.
- **BLOKUJTE** - Zamezte útočníkovi přístup (kontaktujte poskytovatele služby, zablokujte si přijímání útočníkových zpráv nebo hovorů), změňte svou virtuální identitu.
- **OZNAMTE** - Oznamte útok dospělým, schovejte si důkazy pro vyšetřování (např. zprávy, videozáznamy, odkazy na weby, blogy).
- Pokud víte o kyberšikaně, **nebuďte nevšímaví.**
- **Podpořte oběti**, poraďte jim, co mají dělat, pomozte jim kyberšikanu nahlásit.

KYBERŠIKANA

Projevy kyberšikany s příklady

Kyberšikana se může projevovat různým způsobem. Kyberútoky mohou být realizovány dlouhodobě i krátkodobě, s rozdílnou intenzitou a s využitím velkého množství nástrojů. Útočník při napadání ostatních velmi často kombinuje více typů útoků.

Fyzické napadení oběti spojené s natáčením videozáznamu

U uvedeného typu útoku dojde k fyzickému násilí na oběti, které si původci kyberšikany pro své pobavení zaznamenají pomocí mobilního telefonu a nahrávku dále šíří (např. prostřednictvím serveru YouTube, pomocí MMS zpráv apod.). Jde tedy o spojení kyberšikany s tradiční šikanou. Toto jednání patří mezi nejtypičtější formy kyberšikany.
Variantu tohoto jevu představuje nečekané fyzické napadení osob spojené s nahráváním na mobilní telefon nebo kameru. Jedná se o tzv. **happy slapping**. Útočník se baví reakcí oběti (překvapení, strach, údiv, zděšení). Získané video poté publikuje na internetu. Happy slapping může končit i smrtí oběti.

Dvojice mladíků si vyhlédla hocha čekajícího na autobusové zastávce. Jeden z nich k němu přiběhl a „vrazil" mu facku. Druhý mladík celou situaci, včetně překvapené reakce hocha, nahrával na svůj mobilní telefon. Nahrávku poté zveřejnili na stránkách YouTube.

Vyvedení oběti z rovnováhy spojené s natáčením videozáznamu

Útočník se snaží vyprovokovat oběť k reakci, kterou pak nahraje. Nahrávku může zneužít např. k vydírání oběti nebo ji pro pobavení sebe a svého okolí může umístit na internet. Oběťmi podobných útoků jsou často učitelé.

Dva žáci 9. třídy Marek a Libor se snažili během hodiny vyprovokovat učitelku češtiny Marii K. (pokřikovali na ni, narušovali hodinu, nadávali jí apod.). Když učitelka situaci nezvládla, tajně ji natočili mobilním telefonem a záznam umístili na YouTube. Nahrávku zhlédlo přes 70 000 uživatelů. Učitelka se o její existenci dozvěděla, až když se na ni přišli zeptat rozčílení rodiče.

Provokování a napadání uživatelů v diskuzních fórech

Jedná se o tzv. **flaming** a **trolling**. Jsou to online útoky pomocí elektronických zpráv s urážlivým a vulgárním obsahem, které mají za úkol oběť provokovat a vtáhnout ji do podobného způsobu komunikace, nebo ji z komunikace vyštvat. Někteří uživatelé (trollové) také tzv. „tapetují" diskuzní fóra (donekonečna vkládají do diskuze stejný text).

Petr se nudil a brouzdal internetem, až narazil na diskuzi zaměřenou na počítačové hry. Pro pobavení začal do diskuzního fóra psát urážlivé zprávy o ostatních diskutujících, popichoval je proti sobě, útočil na ně. Nezajímalo ho téma diskuze, chtěl se jen pobavit na úkor ostatních, proto zaplavil diskuzní fórum nesmysly a nadávkami.

Pomlouvání s využitím internetu a mobilních telefonů

Útočník se snaží poškodit pověst oběti a narušit její vztahy s přáteli/rodiči tím, že o ní zveřejňuje nepravdivé informace (pomluvy).

Robert vytvořil internetové stránky s názvem „Nesnášíme Tomáše Černého". Na stránky umisťoval jeho karikatury, pomluvy, výmysly a vtipy o Tomášovi. Na existenci stránek upozornil většinu svých kamarádů.

Odhalování cizích tajemství

Útočník zná intimní či ztrapňující informace o oběti (intimní fotografie, důvěrné informace apod.), které může zveřejnit prostřednictvím internetu nebo mobilního telefonu. Odhalování může být spojeno s vydíráním oběti. Útočník také může svou oběť zmanipulovat, pod záminkou z ní vylákat její tajemství a ta potom zveřejnit.

Jana a Honza se spolu rozešli. V době, kdy spolu chodili, poslala Jana Honzovi na mobil svou intimní fotografii. Po rozchodu se Honza chtěl Janě pomstit, a proto zveřejnil její intimní fotografii na internetu.

Vydírání s pomocí informačních a komunikačních technologií

Útočník využívá mobilní telefon nebo počítač s připojením k internetu k vydírání oběti, čímž se snaží dosáhnout svých záměrů (např. v rámci SMS, diskuzních fór, chatu, pomocí e-mailu).

Zbyněk chodil s Katkou. Danovi se ale Katka také líbila, a tak začal Zbyňkovi posílat výhružné SMSky a e-maily. Hrozil, že pokud se s Katkou nerozejde, vyřídí si to s ním ručně.

Realizováno v rámci projektu Prevence nebezpečných komunikačních praktik spojených s elektronickou komunikací pro pedagogy a nepedagogy.

Příloha č. 4 - Přehledový list Stalking a kyberstalking – v textu strana č. 77[195]

KYBERSTALKING

Co je kyberstalking?

Kyberstalking je zneužívání internetu, mobilních telefonů nebo jiných informačních a komunikačních technologií ke stalkingu.

Co je stalking?

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

Projevy stalkingu

1. **Opakované dlouhodobé pokusy kontaktovat oběť** (pomocí dopisů, e-mailů, telefonátů, SMS zpráv, zasíláním vzkazů na ICQ, Skype, v chatu, zasíláním různých zásilek s dárky apod.).
2. **Demonstrování moci a síly stalkera** (výhrůžky).
3. **Ničení majetku oběti** (např. rozbíjení oken, aut, ubližování domácím zvířatům, zasílání počítačových virů apod.).
4. **Stalker označuje sám sebe za oběť.**
5. **Poškozování pověsti oběti.**

Oběť a totožnost stalkera

A. Oběť stalkera osobně zná a ví, že ji pronásleduje.
B. Oběť stalkera osobně zná, ale neví, že ji pronásleduje.
C. Oběť stalkera osobně nezná (vyhlédl si ji např. na internetu).

Kdo jsou stalkeři?

Rozpoznat stalkera nemusí být vůbec snadné a často se to ani nepodaří. Může se jevit jako společensky naprosto normální člověk, o kterém ani jeho nejbližší okolí nemusí vědět, že pronásleduje jinou osobu. Stalkeři bývají podle statistik častěji muži. Problematičtějšími útočníky ale bývají ženy – zejména pro svou cílevědomost a systematičnost.

Typologie stalkerů

A. Uctivač

Snaží se navázat kontakt se zbožňovanou osobou. Jakákoli reakce oběti ho proto povzbuzuje a motivuje k dalšímu jednání. Předpokládá, že vyhlédnutý cíl bude jeho city opětovat. Věří, že mu oběť dluží opětování jeho „lásky", když do ni tolik investuje. Žárlí, pokud má oběť vztah s jinou osobou. Tento typ má zvýšené citové nároky. Je-li oběti odmítnut, mění se jeho chování (začne oběti vyhrožovat, snaží se ji poškodit, někdy užívá také násilí).
Do této skupiny patří i **stalkeři celebrit**.

B. Poblouznění milovník

Žije v iluzi, že ho oběť miluje. Vysvětluje si tak veškeré její chování. Přitom je přesvědčen, že se jeho vysněná romance stane pevným vztahem. Může trpět akutní paranoiou. Obvykle si vybírá oběť s vysokým sociálním statutem. Zpravidla nereaguje na jakékoli právní řešení (policie, soud). Pokud se nedostane do péče psychologa nebo psychiatra, pokračuje ve stalkingu dál.

C. Bývalý partner

Bývá to člověk, který nezvládl ukončení vztahu (může jít o vztah pracovní, obchodní nebo např. terapeutický). Jeho chování je následkem touhy obnovit vztah nebo je odplatou za odmítnutí. Pociťuje ztráty v kombinaci s frustrací, hněvem, žárlivostí (zejména pokud si oběť nalezne jiného partnera), pomstychtivostí a zármutkem.

D. Neobratný milovník

Přestože touží po romantickém nebo intimním vztahu, nedokáže ho díky svým slabým sociálním a komunikativním dovednostem navázat. Pokouší se o fyzický kontakt s obětí (držet oběť za ruku, políbit ji), zpravidla se však neuchyluje k hrozbám ani k fyzickému násilí. Tento typ není tak vytrvalý jako jiné typy stalkerů. Pokud oběť využije právní a policejní pomoci, stalker většinou pronásledování zanechá.

E. Sexuální útočník

Snaží se o sexuální útok (často je to sexuální deviant). Tento typ stalkera používá také voyerství, exhibicionismus, obscénní telefonní hovory, sadismus, masochismus apod.

F. Ublížený pronásledovatel

Chce se pomstít za skutečné nebo domnělé zranění, jež mu oběť způsobila. Většinou se omezuje na slovní útoky (vyhrožuje, zastrašuje, podává na oběť žaloby), pravděpodobnost fyzického útoku na oběť je minimální. Mstí se na domácích mazlíčcích oběti (krádež či zabití), vloupává se do domu či bytu oběti apod. Obtěžování mu přináší uspokojení, má pocit, že má nad obětí moc a kontrolu. Bývá velmi vytrvalý.

G. Kyberstalker

Využívá informační a komunikační technologie (internet, mobilní telefony). Svou oběť může kontaktovat pod falešnou identitou např. na diskuzním fóru, to mu také může sloužit k získávání informací o oběti od jiných uživatelů, popř. může ke stejnému účelu použít různé spywarové programy. Pravý kyberstalker se nikdy neuchýlí k fyzickému útoku a své pronásledování realizuje výhradně prostřednictvím elektronických médií.
Kyberstalking můžeme nalézt u všech výše uvedených typů. **Každý stalker tedy může být zároveň i kyberstalkerem.**

Realizováno v rámci projektu Prevence nebezpečných komunikačních praktik spojených s elektronickou komunikací pro pedagogy a nepedagogy.

[195] KOPECKÝ, K. Přehledový list Stalking a kyberstalking. *E-Bezpečí* [online]. 25.11.2009. [cit. 2012-01-17]. Dostupné z WWW: <http://cms.e-bezpeci.cz/component/option,com_docman/task,doc_details/gid,31/Itemid,2/lang,czech/>.

KYBERSTALKING

Případy kyberstalkingu a stalkingu

V ČR se se stalkingem setkalo asi 10 % populace. Nejčastějšími obětmi jsou expartneři, celebrity, politici, lidé zhrzení v lásce apod. 2 % případů končí smrtí. V trestním zákoníku platném od 1. 1. 2010 je stalking nově zařazen jako trestný čin nebezpečné pronásledování.

Sadistický stalker Petr H. více než 2 roky pronásledoval svou kolegyni z Ruzyňského letiště. Psal jí **výhružné e-maily, SMS, špehoval ji, fyzicky ji napadal, zničil ji automobil.** Za to byl odsouzen k 250 hodinám veřejně prospěšných prací. Pro jejich nesplnění mu byl trest změněn na 125 dnů vězení. Nástup trestu si Petr H. odložil kvůli špatnému psychickému stavu. Oběť na agresora opakovaně upozorňovala policii, příběh zveřejnila Marně.

Důsledky:
Ubil ji před jejím domem čtyřkilovou větví. Za to byl odsouzen na 15 let vězení.

50letý stalker Štefan Z. obtěžoval o 20 let mladší ženu. **Vulgárně ji urážel, špehoval ji a nahánět autem, bombardoval ji SMS zprávami, nechtěnými pozornostmi**, nakonec i **výhrůžkami** (likvidace ženy i jejího partnera). Za 7 měsíců ji telefonicky kontaktoval nejméně ve 498 zjištěných případech.

„Podívej se, ty špinavá coura, ještě jednou uvidím měšťáky u svého auta, tak se tvůj dozví o tvých úchylárnách. To, co bylo doteď, byl jen pionýrský tábor, teď zažijes peklo. Zničím tě, ode dneška tě bude sledovat chlap, i kdyby mě to mělo stát sto tisíc. Nebudu šetřit nikoho, ani bratra, ani rodiče, zničím tě."

Důsledky:
Byl odsouzen ke 2 letům odnětí svobody do věznice s dozorem za vydírání a násilí proti skupině obyvatel a proti jednotlivci.

Studenta Tomáše K. z Mostu několik let pronásledovala jeho obdivovatelka Barbora K. a její matka. Ta se rozhodla, že udělá vše pro to, aby dceři „ulovila" vyhlédnutého partnera. Barbora mu psala **desítky SMS zpráv denně, zahlcovala ho e-maily, nechávala před jeho dveřmi dárky**. Ať šel student kamkoli, následovala ho. **Na ulici se s ním snažila srovnat krok**, aby to alespoň vzdáleně vypadalo, že k sobě patří. Neustále mu opakovala, že ho miluje, nebo že ho nenávidí.

„Podívej se, s kým tady dneska je. Jestli to není příbuzná, tak je to teda pěkná šereda. Teda Tomáši, za takovouhle štětku jsi vyměnil moji Báru? To je hrůza. Vždyť se podívej, jakou má zlatou kabelku, jako nějaká štětka z E55."

Důsledky:
Tomáš se nemůže nijak bránit, protože stalkerky ho fyzicky nenapadly, nevydíraly nebo vůči němu nespáchaly jiný trestný čin, který by popisoval český trestní zákoník.

Stalkeři celebrit

Karel Gott | Uma Thurman | Mel Gibson | Steven Spielberg | Britney Spears | Madonna

Jak se chránit?

- Dejte stalkerovi najevo, že o jeho zájem nestojíte.
- Neodpovídejte stalkerovi na vzkazy, nechoďte s ním na schůzky.
- Změňte své návyky (choďte či jezděte jinými cestami, nakupujte jinde apod.).
- Uschovejte si důkazy (výhružné SMS a e-maily) a informujte policii.
- Mluvte otevřeně s okolím o tom, co se děje (s rodinou, s dětmi, s obchodními partnery atd.).
- Znáte-li jméno agresora, nebojte se na něj přímo ukázat.
- Chraňte se.

Příloha č. 5 - Přehledový list Hoax – v textu strana č. 77[196]

HOAX

Co je hoax?

Anglické slovo hoax můžeme přeložit jako:

- poplašná zpráva,
- smyšlená zpráva,
- mystifikace,
- výmysl,
- novinářská kachna,
- podvod,
- žert nebo kanadský žertík

apod.

Čím hoax škodí

- Vyvolává paniku a strach.
- Nabízí nebezpečné rady.
- Poškozuje důvěryhodnost šiřitele.
- Poškozuje konkrétní firmy (např. Coca Cola, Microsoft, Nestlé, Mentos apod.).
- Obtěžuje příjemce, zaplavuje e-mailové schránky, zatěžuje linky a servery.
- Vyzrazuje důvěrné informace.
- Umožňuje podvodně získávat peníze (v některých případech).

Co pomáhá šíření hoaxu

- Nekritický příjem informací.
- Věrohodnost opřená o „vědecká fakta" nebo podpořená fotografiemi.
- Výhrůžky a sliby obsažené v hoaxu.
- Dobrý úmysl (soucit, snaha pomoct či chránit apod.).
- Mateřský jazyk.

Hoax se šíří především prostřednictvím e-mailu a ICQ.

Druhy hoaxu

A. Poplašné zprávy

Zpráva manipuluje s informacemi a snaží se uživatele přimět hlavně k dalšímu šíření (např. *„Pozor ICQ vir, pošlete to všem."*) nebo dokonce k nějakému destruktivnímu zásahu (např. *„Smažte win.exe z instalace Windows, je to virus."*).
Do této kategorie spadají také hoaxy informující např. o vážné nemoci, úmrtí nebo uvěznění nějaké známé osobnosti.

B. Zábavné hoaxy, kanadské žertíky

Smyslem těchto hoaxů je především pobavit adresáta, protože informace, které přinášejí, jsou jen těžko ověřitelné. Součástí mohou být také různé obrázky, u nichž je na první pohled jasné, že se jedná o koláže.

C. Smyšlené petice a výzvy

Například: *„Od 1.1. 2009 bude ICQ placené. Pokud jej chcete dále využívat zdarma, pošlete tuto zprávu dalším 15 lidem z vašeho seznamu kontaktů do jedné hodiny od obdržení této zprávy."*

D. Prosby o pomoc

Tyto hoaxy většinou působí na city. Prosí o pomoc (např. darování krve, hledání ztracené osoby) nebo přímo žádají o peníze. Obvykle jsou doprovázeny velmi emotivními fotografiemi.
Některé z těchto zpráv původně opravdu rozeslali lidé ve svízelné životní situaci. Zprávy jsou ale šířeny dál, i když výzvy v nich již nejsou aktuální.

E. Řetězové dopisy štěstí

Dříve se šířily jen klasickou poštou, dnes se přesunuly na internet. Využívají uživatelovy touhy být vtipný nebo jeho pověrčivosti. Často nutí k dalšímu rozesílání různými výhrůžkami (*„Nepřepošles-li, budeš mít smůlu."*). Naopak poslušnému uživateli slibují všechno možné.

F. Nigerijské dopisy a jiné „lákavé nabídky"

Například: *„Chceme převést několik miliónů z revoluci zasažené rozvojové země (zpravidla peníze z diamantů nebo ze zkonfiskované královské pokladnice) a potřebujeme k tomu Váš účet. Odměna v řádu procent až desítek procent. V čem je potíž? Na výdaje spojené s převodem potřebujeme příspěvek od Vás."* Máte před sebou vidinu snadno vydělaných desítek až stovek tisíc, tak zaplatíte. Pak se však vyskytnou komplikace, takže opět zaplatíte. Ale potíže se objeví znovu a vy platíte a platíte... Tak dlouho, dokud jste ochotni nechat se okradat.
Na podobném principu fungují i e-maily s odkazy na e-shopy s lákavými cenami zboží např. z Asie.

G. Pyramidové hry

Princip pyramidové hry: Na špičce pyramidy je člověk, který má pod sebou lidi, a ti na něj vydělávají. Ti mají pod sebou další lidi, kteří na ně vydělávají, ti mají pod sebou zase další lidi, kteří vydělávají na ty, co jsou nad nimi atd. Je jen otázka času, kdy dojdou lidé a pyramida se zhroutí. Ale to už jsou osoby ze špičky pyramidy finančně zajištěny na celý život. Např.: *„Pošli 100 korun na 5 adres, které jsou uvedeny na začátku dopisu. Přepiš dopis, na první místo napiš sebe, poslední adresu vynech. Pošli svým 5 přátelům. Brzo obdržíš obálky, ve kterých bude (pokud nikdo řetěz nepřeruší) 500+2500+12500+62500+312500 = 390 500,- Kč. Proto nepřerušuj řetěz."*
Když dopis pošlete, zapojíte do hry 3 905 lidí, a to jen na své vlákno! To, že za chvíli dostanete znovu tento dopis vy nebo někdo jiný z už dříve zapojených lidí a řetěz se začne přerušovat, je jasné. A tak důvěřivci ztratí své peníze a vrchol pyramidy se utěšeně „napakuje".

Realizováno v rámci projektu Prevence nebezpečných komunikačních praktik spojených s elektronickou komunikací pro pedagogy a nepedagogy.

bezpečí

[196] KOPECKÝ, K. Přehledový list Hoax. *E-Bezpečí* [online]. 25.11.2009. [cit. 2012-01-17]. Dostupné z WWW: <http://cms.e-bezpeci.cz/component/option,com_docman/task,doc_details/gid,29/Itemid,2/lang,czech/>.

HOAX

Příklady hoaxu

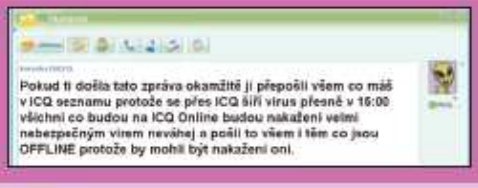
Vajíčko uvařené mobilem

„Umísti syrové vajíčko do porcelánového stojánku. Na jeho protější strany dej dva mobilní telefony. Zavolej z jednoho telefonu na druhý a zůstaň na lince. Během prvních 15 minut se nic neděje. Po 25 minutách je skořápka vajíčka horká. Po 40 minutách se bílek uvaří, je pevný. Po 65 minutách je i žloutek plně uvařen."

Nevěřte účtenkám z Lidlu

„Nakupil som si nakup 9 výrobkov. Kupodivu, ani na jednom nebola vyznačená iná cena, akú uctovala pokladňa. Celková suma sa však nezodpoveda súčtu jednotlivých položiek. Bola to veľká náhoda, že som si prepočítal súčet. Predpokladám, že to nikto bežne nerobí, zvlášť pri nákupoch 20-30 a viac-položkových. Prekvapujúco som zistil rozdiel 66 Sk, čo je 12 % z ceny, ktorú som mal zaplatiť."

ICQ virus



Obří smrtící pavouci

„Tohle jsou pavouci, které nacházejí denně vojáci v Iráku.
Běhají rychlostí 16 km/h, doskočí 92 cm. Jsou to noční pavouci, takže vycházejí ven jen v noci nebo pokud jsou ve stínu. Když vás kousnou, dostáváte dávku novocainu, takže okamžitě ztuhnete. Ani nevíte, když vás kousne ve spaní, pak se jen probudíte s chybějící částí nohy nebo ruky, protože vám ji ohlodával celou noc. Když při chůzi narazíte na něco ve stínu a slunce vám najednou ukáže, s čím jste se potkali, je lepší utíkat. Okamžitě totiž vyrazí za vaším stínem."

Šokující nálezy kostér

„Porovnáte-li jeho hlavu a vedle pracujícího človíčka, musíte opravdu užasnout, o jaké monstrum se jedná."
Tuto zprávu vypustil do světa časopis National Geographic. Jednalo se o pouhý žert. Některé deníky ji ale považovaly za pravdivou a šířily ji dál.

Kostra obra | Netopýří chlapec | Kostra obra

Pozor na injekční jehly

Pozor na injekční jehly!

ČR (vir) - Dávejte pozor, na co si sednete! Jde o zdraví i o život! Takové varování putuje po internetu. V textu jsou pak popsány případy, kdy se například návštěvníci kina při usednutí píchli o nastražené injekční stříkačky. Na jehle byl papír se vzkazem: »Právě jsi byl nakažen virem HIV!« Tyto případy se údajně staly v zahraničí i v Praze! Písatelé v e-mailu tvrdí, že testované jehly opravdu obsahovaly virus HIV nebo žloutenky.

Bill Gates se rozhodl podělit o své bohatství

„Ahoj všichni, prosím Vás, neberte to na lehkou váhu. Bill Gates se rozhodl podělit se o své bohatství. Pokud tohle budete ignorovat, později Vás to může mrzet. Microsoft a AOL jsou teď největší internetové společnosti a aby se ujistili, že Internet Explorer zůstává nejrozšířenějším programem, rozeběhli e-mailový beta test. Jestli přeposlete tento mail svým přátelům, Microsoft to zjistí (pokud jste uživatelé Microsoft Windows) do dvou týdnů. Za každého člověka, kterému tento mail přeposlete, Vám Microsoft zaplatí $ 245, za každého člověka, kterému to pošlete a on také, Vám Microsoft zaplatí dalších $ 243, a za každého třetího člověka, který tuto zprávu obdrží, Vám zaplatí $ 241. Do dvou týdnů se Vás Microsoft bude kontaktovat, aby obdržel Vaši adresu a pak Vám pošle šek.
S pozdravem Chinu!
Myslel jsem si, že je to bibost, ale po dvou týdnech, co jsem tento mail obdržel a přeposlal dále, mi Microsoft kontaktoval kvůli adrese a během pár dnů mi přišel šek na $ 24 800. Musíte odpovědět dříve, než tato akce skončí. Jestli si tohle může někdo dovolit, pak je to Bill Gates. Pro něj jsou to výdaje na marketing. Prosím přeposlete to co nejvíce lidem. Dostanete minimálně US$ 10 000."

Jak se chránit?

- **Nikdy nevěřte všem informacím, které vám z neznámého zdroje přijdou na e-mail.**
- **Nikdy nesdělujte své osobní informace (PIN, rodné číslo apod.).**
- **Nikdy nedůvěřujte zprávám, které vám posílá e-mailem vaše bankovní instituce (bankovní instituce s klienty v případě důležitého sdělení tímto způsobem zpravidla nekomunikují).**
- **Všechny informace si vždy ověřujte.**

Příloha č. 6 - Leták bezpečný internet – v textu strana č. 77[197]

[197] KOPECKÝ, K. Leták bezpečný internet. *E-Bezpečí* [online]. 25.4.2009. [cit. 2012-01-17]. Dostupné z WWW: <http://cms.e-bezpeci.cz/component/option,com_docman/task,doc_details/gid,15/Itemid,2/lang,czech/>.

ANOTACE

Jméno a příjmení:	Pavel Valchář
Katedra:	Ústav pedagogiky a sociálních studií
Vedoucí práce:	PhDr. Linda Švrčinová
Rok obhajoby:	2012

Název práce:	Kybergrooming a další nebezpečné aktivity spojené a využíváním moderních komunikačních technologií.
Název v angličtině:	Cyber Grooming and Other Dangerous Activities Connected with Usage of Modern Communication Technologies.
Anotace práce:	Teoretická část diplomové práce vysvětluje pojem komunikace, popisuje vybrané nebezpečné aktivity spojené s využíváním moderních komunikačních technologií a zaměřuje se na jednu z nejnebezpečnějších komunikačních aktivit – kybergrooming. Přibližuje rovněž různé projekty zaměřené na ochranu dětí. Praktická část se věnuje kvantitativnímu výzkumnému šetření zabývajícímu se problematikou chování dětí při komunikaci na internetu. Jedná se o dotazníkové šetření, jehož hlavním cílem bylo zjistit, jak bezpečně se žáci 2. stupně vybraných základních škol pohybují na internetu a do jaké míry se tito žáci setkávají s aktivitami, které by mohly nasvědčovat útoku kybergroomera a nakolik svým chováním kybergroomerovi usnadňují útok.
Klíčová slova:	Komunikace, internet, mobilní telefon, nebezpečné komunikační aktivity, kybergrooming, manipulace dítěte, prevence, projekty na ochranu dětí
Anotace v angličtině:	Theoretical part of the diploma project explains the term of communication, describes selected dangerous activities connected with usage of modern communication technologies and focuses on one of the most hazardous communication activities – cyber grooming. It also describes various projects focused on protection of children. The practical part focuses on quantitative research dealing with the issue of children's behaviour when communicating on the Internet. It is a questionnaire research, its main aim is to find out how safely pupils at the second stage of selected primary schools move on the Internet and to which extent they face activities, which could indicate attack of a cyber groomer and to what extent they make the attack easier for a cyber groomer.
Klíčová slova v angličtině:	Communication, Internet, mobile telephone, dangerous communication activities, cyber grooming, manipulation of a child, prevention, projects for protection of children
Přílohy vázané v práci:	Příloha č. 1 - Dotazník Příloha č. 2 - Přehledový list Kybergrooming Příloha č. 3 - Přehledový list Kyberšikana 1 a 2 Příloha č. 4 - Přehledový list Stalking a kyberstalking Příloha č. 5 - Přehledový list Hoax Příloha č. 6 - Leták bezpečný internet
Rozsah práce:	137 s. + přílohy
Jazyk práce:	Český jazyk