UNIVERZITA PALACKÉHO V OLOMOUCI
Centrum prevence rizikové virtuální komunikace

NEBEZPEČÍ ELEKTRONICKÉ KOMUNIKACE 2

ZPRÁVA Z VÝZKUMNÉHO ŠETŘENÍ
REALIZOVANÉHO V RÁMCI PROJEKTU
E-BEZPEČÍ – NEBEZPEČÍ ELEKTRONICKÉ KOMUNIKACE PRO ŽÁKY I UČITELE

Mgr. Veronika Krejčí,
Mgr. Kamil Kopecký, Ph.D.

Olomouc 2010-2011

Obsah

1. Úvod

Výzkumné šetření Nebezpečí elektronické komunikace 2 navazuje na výzkumná šetření realizovaná týmem Centra prevence rizikové virtuální komunikace Pedagogická fakulty Univerzity Palackého v Olomouci od roku 2008. Aktuální výzkumné šetření bylo provedeno v rámci projektu *E-Bezpečí – nebezpečí elektronické komunikace pro žáky i učitele*[1], jehož realizátorem je Centrum prevence rizikové virtuální komunikace Univerzity Palackého v Olomouci (www.prvok.upol.cz). Výzkum proběhl s použitím dotazníkového systému portálu E-Bezpečí (www.e-bezpeci.cz). Do výzkumného šetření se od 1. listopadu 2010 do 31. prosince 2010, kdy byl dotazník přístupný, zapojilo 12 533 respondentů ze základních a středních škol z celé České republiky, včetně škol zapojených do Partnerského programu projektu E-Bezpečí.

2. Výzkumný záměr

Cílem výzkumného šetření Nebezpečí internetové komunikace 2 (realizovaného v listopadu-prosinci roku 2010) bylo zjistit následující data:

A. Zkušenosti respondentů s kyberšikanou z pohledu obětí i útočníků a jejich zájem zapojit do řešení těchto problémů další osoby (rodiče a učitele).

B. Ochota respondentů komunikovat s neznámými osobami, jež je kontaktují v rámci služeb internetu, a jejich zkušenosti ze setkávání se s těmito lidmi v reálném světě (kybergrooming).

C. Sdílení osobních údajů respondentů v rámci služeb internetu (zveřejňování osobních volně na internetu, sdělování osobních údajů neznámým osobám na internetu), včetně zkušeností respondentů se sextingem.

C. Zkušenosti respondentů se sociálními sítěmi, webovými úložišti dat nebo portály zaměřenými na dětské uživatele (potenciální prostředí pro získávání osobních dat k jejich možnému zneužití a pro šíření kyberšikany, pro kybergrooming, stalking a další nebezpečné praktiky).

[1] Projekt byl podpořen Ministerstvem školství, mládeže a tělovýchovy v rámci programu prevence rizikového chování.

3. Metodologie

Výzkum Nebezpečí internetové komunikace 2 je svou povahou především deskriptivní, získaná data jsou převážně kvantitativní. Jako základní výzkumná metoda bylo zvoleno online dotazníkové šetření. Online šetření bylo monitorováno dotazníkovým systémem projektu E-Bezpečí a systémem Google Analytics.

Dotazník obsahoval 67 otázek různého typu (dichotomické, polytomické, typ part, typ multipart, otevřené textové apod.).

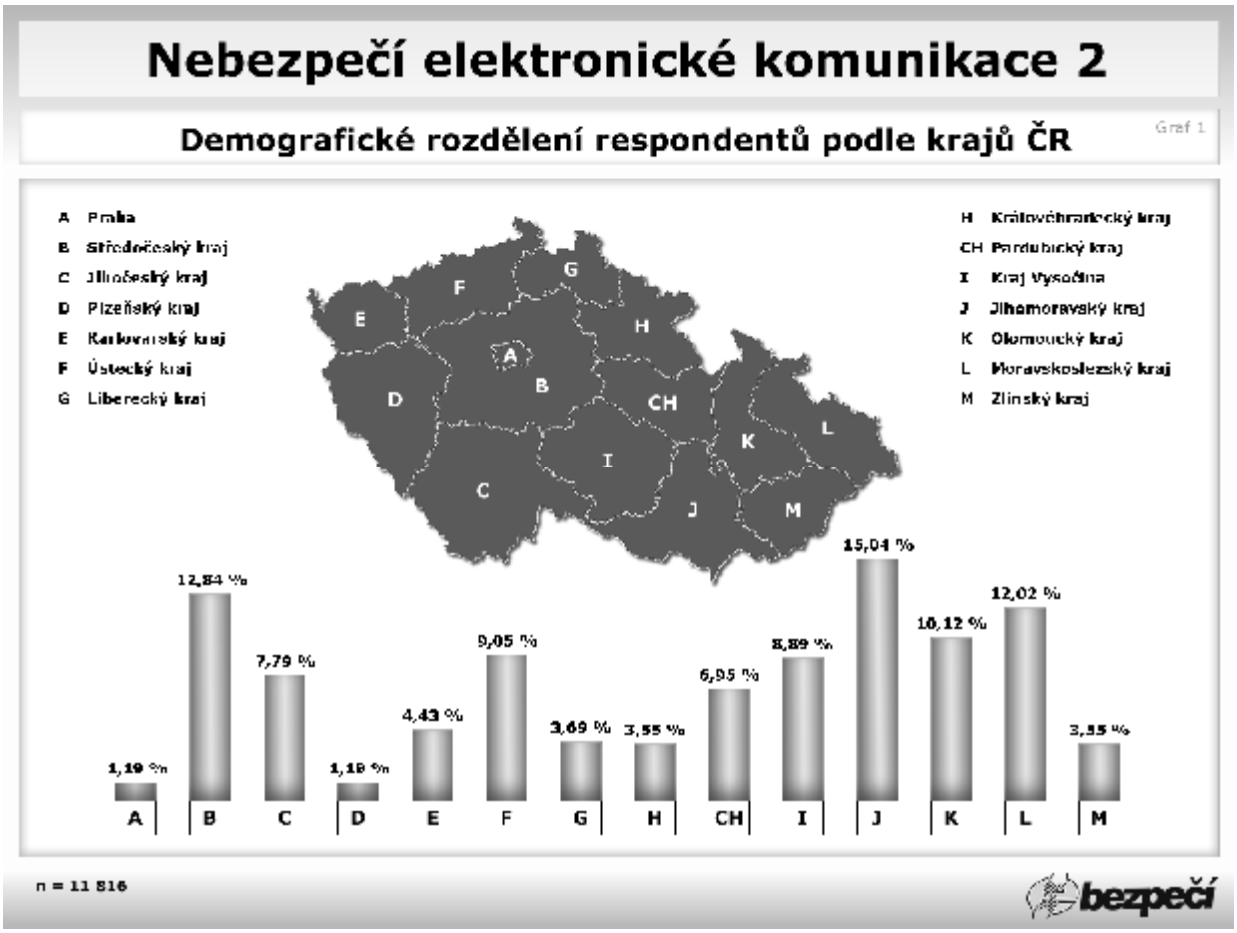
Úsilí respondentů bylo motivováno možností zapojit se do losování o zajímavé ceny, které jsme jim nabídli jako motivační odměnu (trička, reklamní předměty, samolepky apod.). Zájemci o ceny se v dotazníku identifikovali kontaktním e-mailem.

Respondenti výzkumného šetření vyplňovali dotazník anonymně.

4. Výzkumný vzorek

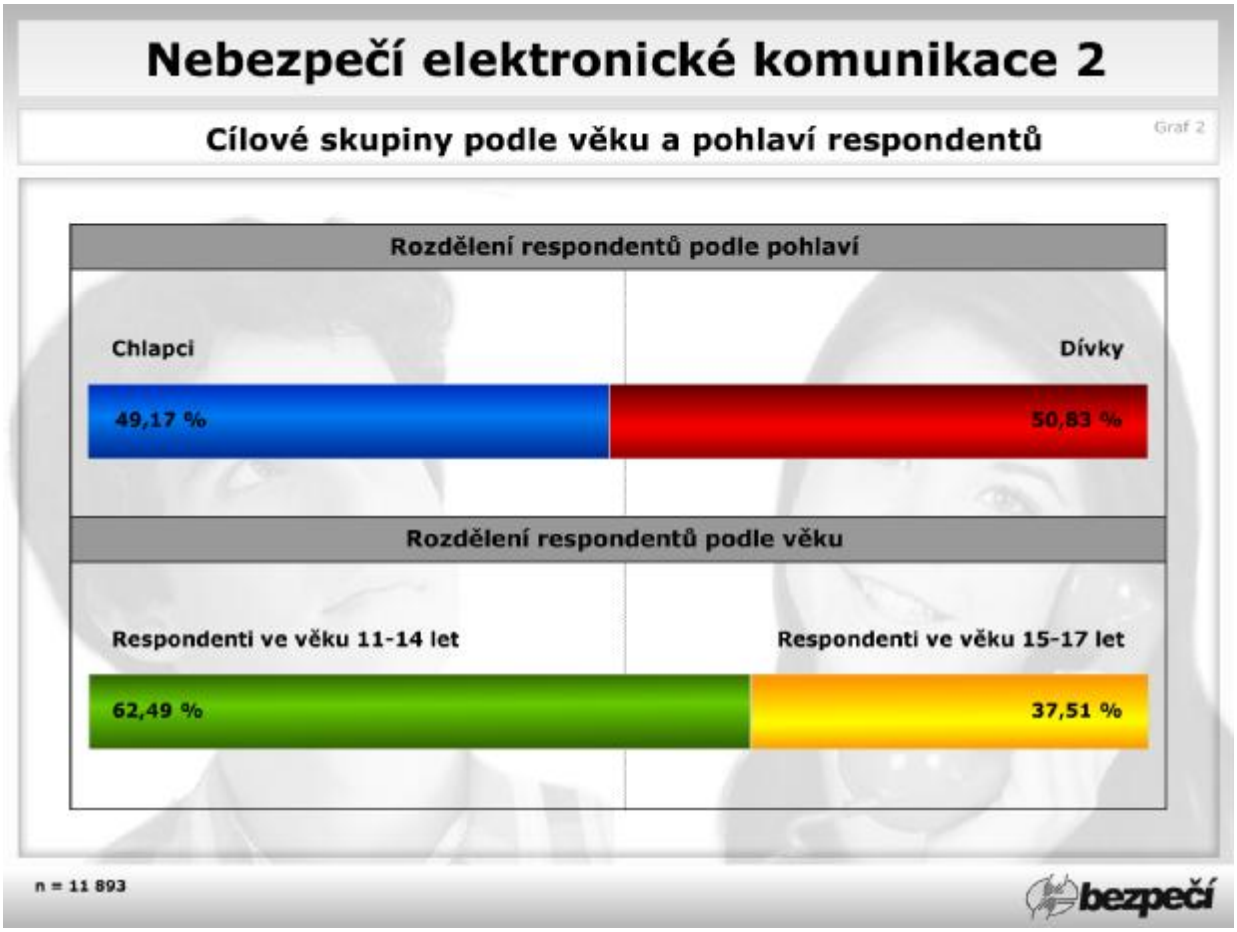
S možností zapojit se do výzkumného šetření bylo osloveno přes 4 000 škol (ZŠ a SŠ) z celého území ČR. Maximální vzorek tvořili 12 533 respondenti. Největší zastoupení měli žáci z Olomouckého kraje (15,04 %), následováni žáky ze Středočeského (12,84 %) a Moravskoslezského (12,02 %) kraje. Naopak nejméně respondentů bylo z Prahy a Plzeňského kraje (shodně 1,19 %). (*Graf 1*)

Graf 1 – Demografické rozdělení respondentů podle krajů ČR



Vzorek byl tvořen ze 49,17 % chlapci a 50,83 % dívkami. Věkově byl vzorek rozdělen do 2 věkových kategorií, které odpovídají 2. a 3. stupni škol. Nejvíce respondentů tvořili žáci ve věku 11-14 let (62,49 %). (*Graf 2*)

Graf 2 – Cílové skupiny podle věku a pohlaví respondentů



5. Výsledky výzkumu

5. 1 Kyberšikana[2]

Kyberšikana je závažný problém, se kterým se žáci potýkají poměrně často, proto jí bylo věnováno nejvíce prostoru také ve výzkumném šetření. V rámci výzkumu bylo sledováno několik projevů kyberšikany:

- ponižování, urážení, zesměšňování nebo jiné verbální ztrapňování,
- publikování ponižujících záznamů (fotografií, videozáznamů a audiozáznamů),
- vyhrožování a zastrašování,
- vydírání,
- prolomení elektronického účtu a jeho případné zneužití (tzv. krádež identity),
- obtěžování (např. telefonováním, prozváněním, spamováním).

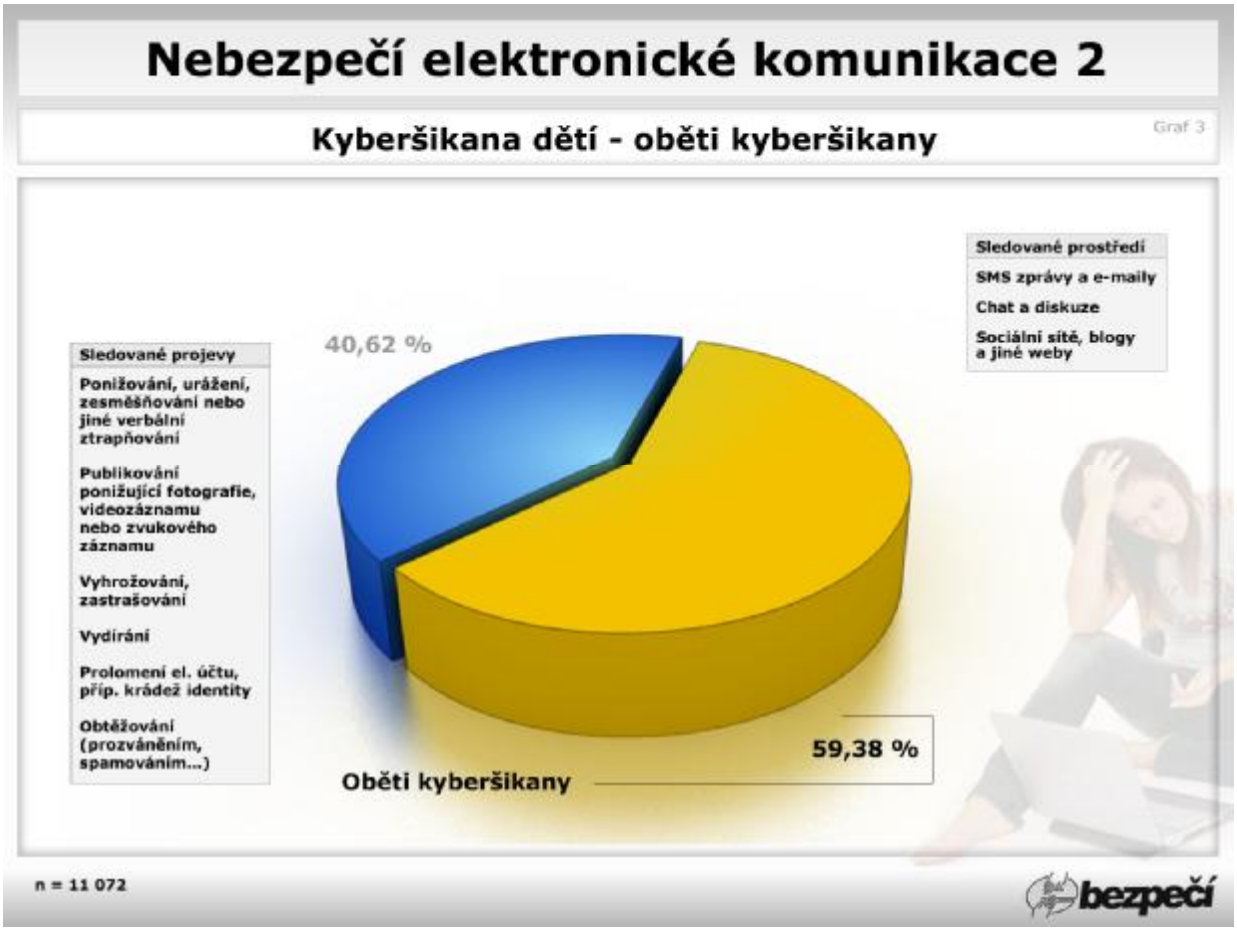
[2] Kyberšikana nebo také kybernetická šikana je druh psychické šikany, při které útočník využívá informační a komunikační technologie (např. mobilní telefony, internet nebo pagery). Pod pojmem kyberšikana se skrývá celá řada projevů (dle Krejčí, V., 2009).

Kyberšikana dětí (oběti kyberšikany)

Z výzkumného šetření vyplynulo, že více než polovina dětí (59,38 %) se setkala s kyberšikanou v pozici oběti. (*Graf 3*) Sledované projevy se však mohou lišit svou intenzitou a délkou.

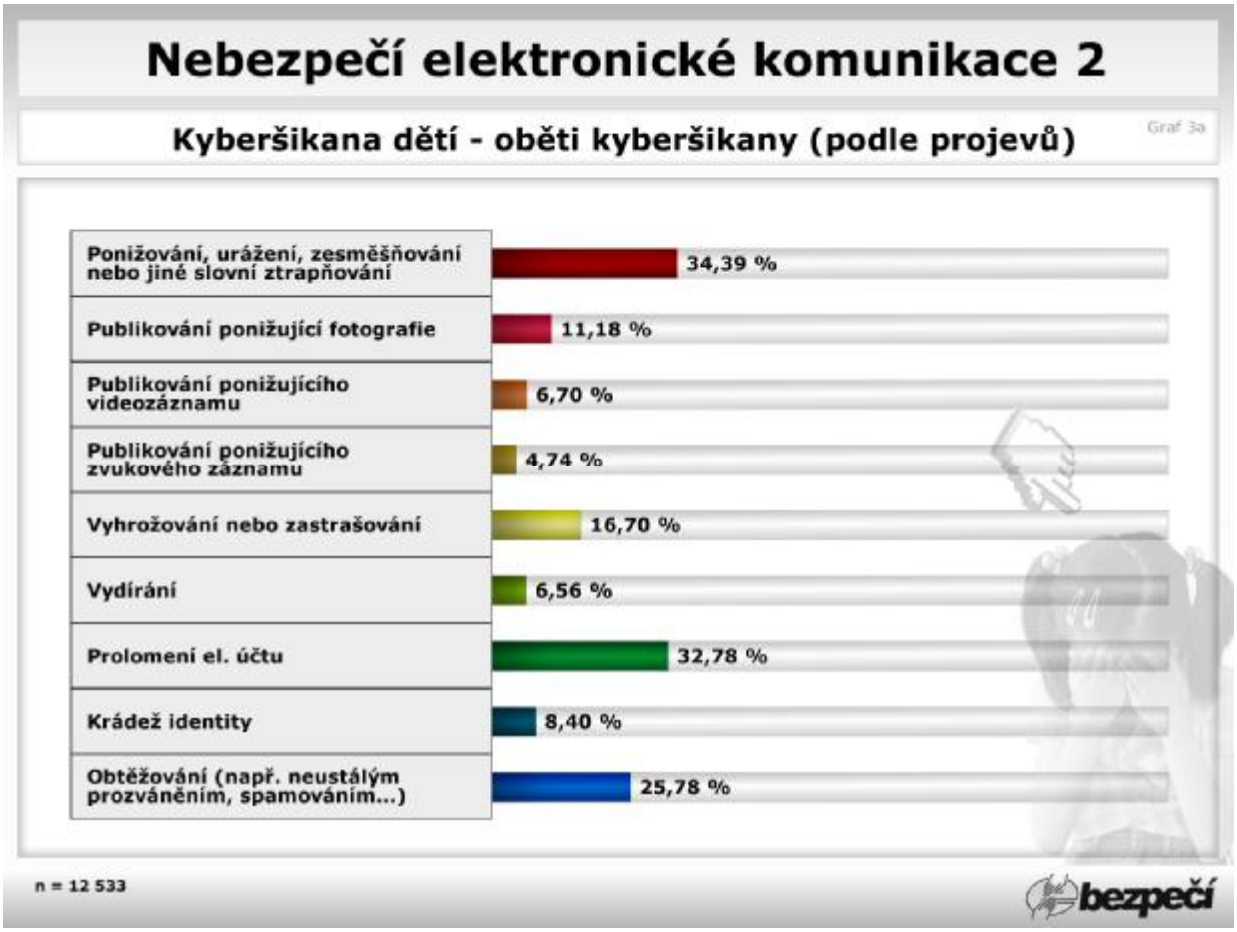
V dotazníku nebylo zohledněno, zda byly útoky na oběť jednorázové nebo se opakovaly, nebylo také sledováno, zda byla oběť podrobena několika útokům (z pohledu různých spolu nesouvisejících útočníků) ani to zda byly útoky na oběť kombinací různých projevů kyberšikany.

Graf 3 - Kyberšikana dětí – oběti kyberšikany



Z pohledu sledovaných projevů kyberšikany je pro žáky nejčastějším problémem verbální ponižování, urážení, zesměšňování nebo jiné ztrapňování (34,39 %) a prolomení elektronického účtu (32,78 %). 25,78 % respondentů se cítí poškozováno obtěžováním, jež má podobu neustálého prozvánění, spamování apod. 16,70 % dětí se setkalo s vyhrožováním nebo zastrašováním, ke kterému bylo využito ICT. (*Graf 3a*)

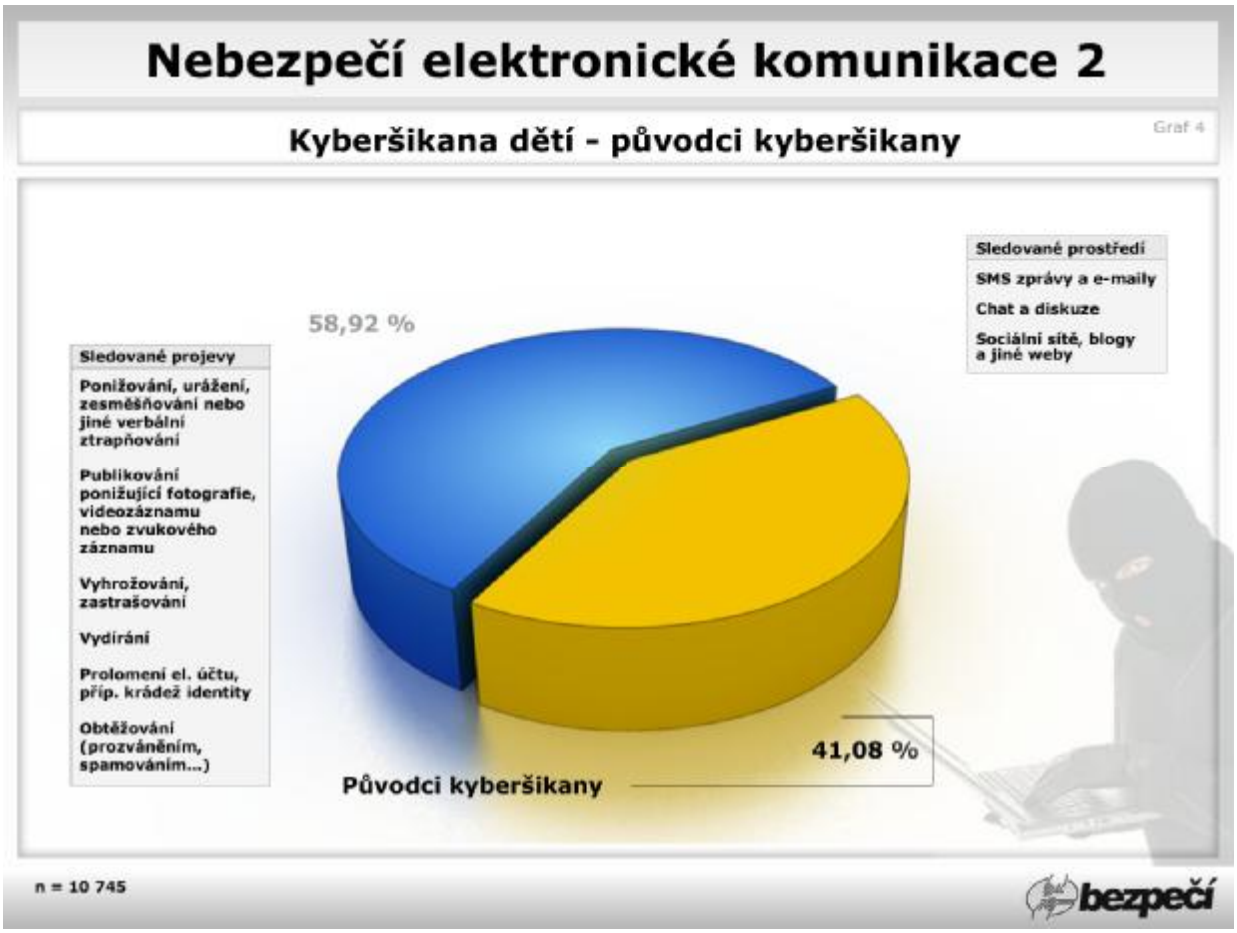
Graf 3a - Kyberšikana dětí – oběti kyberšikany (podle projevů)



Kyberšikana dětí (původci kyberšikany)

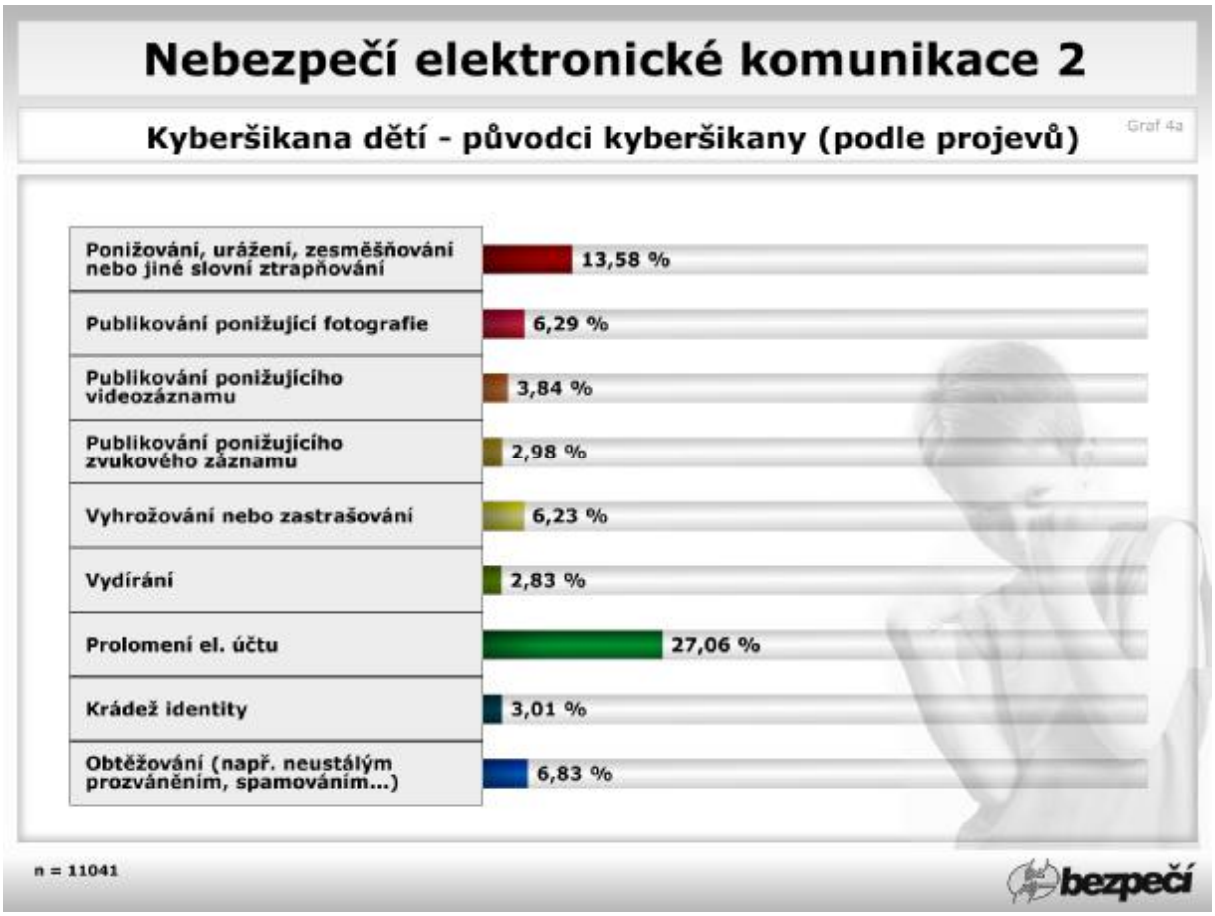
41,08 % respondentů přiznalo, že vyzkoušelo některý ze sledovaných projevů kyberšikany. (*Graf 4*)

Graf 4 - Kyberšikana dětí – původci kyberšikany



K nejčastějším útokům patří prolomení ochrany cizího elektronického účtu (27,06 %) a verbální ponižování, urážení, zesměšňování nebo jiné ztrapňování (13,58 %). (*Graf 4a*)

Graf 4a – Kyberšikana dětí – původci kyberšikany (podle projevů)



Kyberšikana dětí (zapojení dalších osob do řešení kyberšikany)

15,87 % respondentů by s rodiči neřešilo žádný ze sledovaných projevů kyberšikany. Na učitele by se s prosbou o pomoc při řešení některého ze sledovaných problémů neobrátila asi třetina respondentů (26,70 %). Je tedy vidět, že většina dětí by se v konkrétní problémové situaci obrátila o pomoc na rodiče nebo na své učitele. (*Graf 5*)

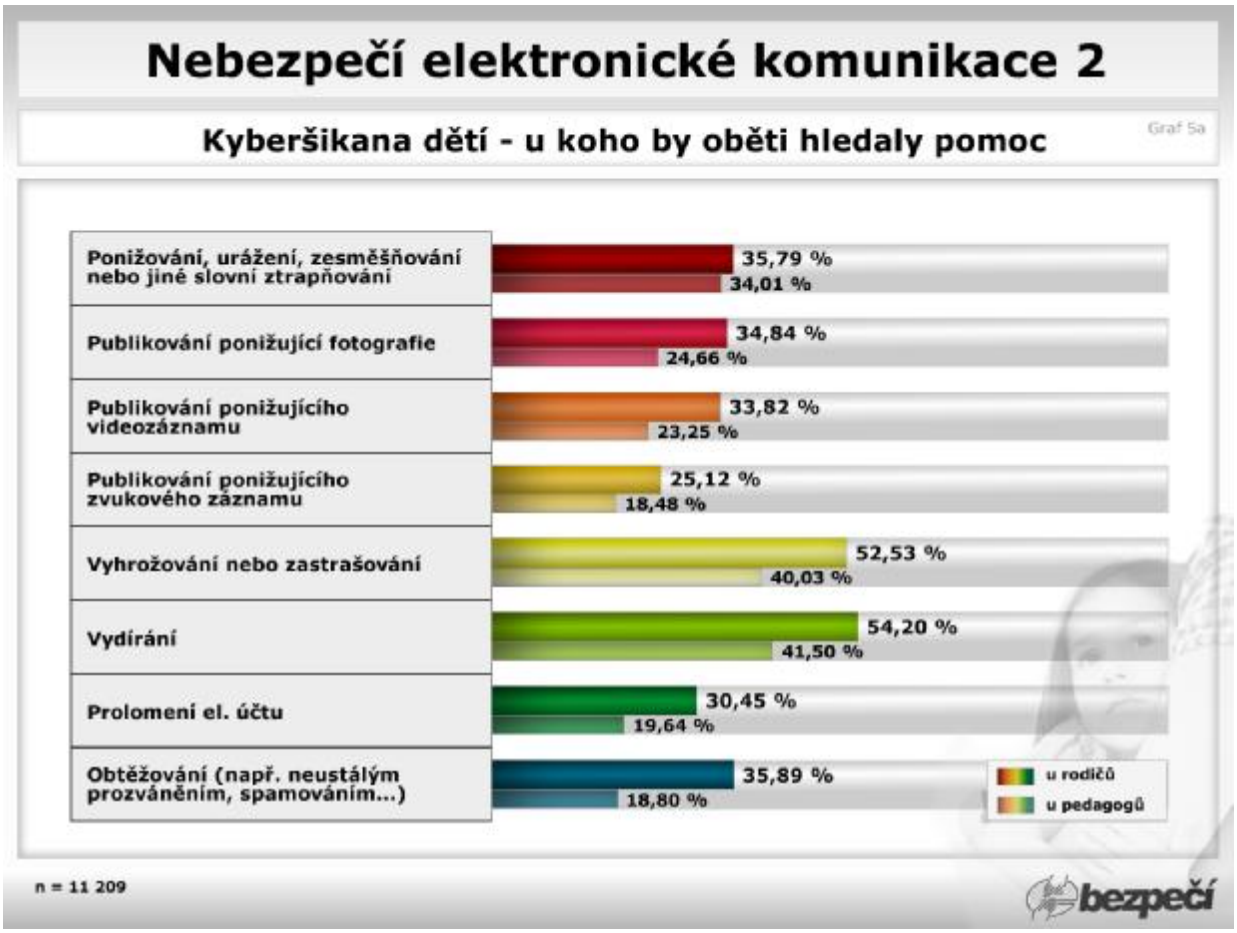
Graf 5 – Kyberšikana dětí – respondenti, kteří by žádný ze sledovaných problémů neoznámili rodičům / učitelům

Jak tato situace vypadá u jednotlivých projevů kyberšikany zachycuje následující graf. *(Graf 5a)*

Děti by se nejčastěji svěřily jiné osobě, pokud by se staly obětí vydírání (54,20 % rodičům, 41,50 % učitelům) a vyhrožování nebo zastrašování (52,53 % rodičům, 40,03 % učitelům). Ostatní problémy by rodičům oznámila asi třetina dětí (hodnoty se pohybují v rozmezí 25,12 % - 35,89 %). 34,01 % by se svěřila učitelům s verbálním ponižováním, urážením, zesměšňováním nebo jiným ztrapňováním, zatímco další projevy by řešila čtvrtina až pětina respondentů (hodnoty se pohybují v rozmezí 18,48 % - 24,66 %).

Ze zachycených hodnot vyplynulo, že na rodiče by se s jednotlivými problémy obracelo průměrně o 10,28 % více respondentů než na učitele.

Graf 5a – Kyberšikana dětí – u koho by oběti hledaly pomoc (podle projevů)

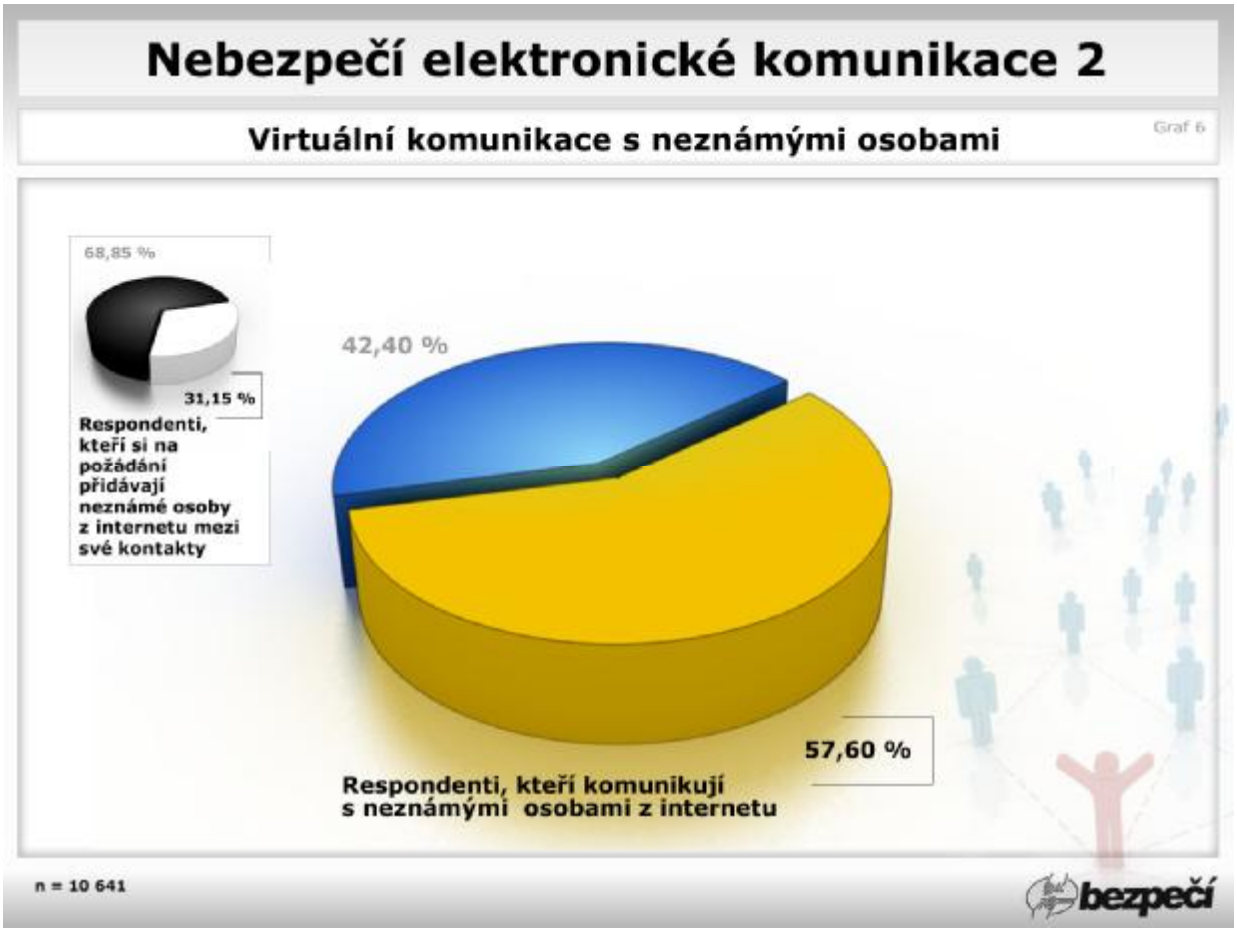


5.2 Virtuální komunikace s neznámými osobami

Komunikace s neznámými osobami na internetu patří také mezi potenciálně rizikové jednání, neboť při ní dítě může být vystaveno nejrůznějším manipulacím. Případem nebezpečných manipulací je např. kybergrooming[3].

V rámci výzkumu bylo zjištěno, že výše vymezenou komunikaci vyhledává 57,60 % dotazovaných dětí. 31,15 % respondentů je ochotno přidávat si na vyžádání neznámé osoby mezi své kontakty / kamarády apod. *(Graf 6)*

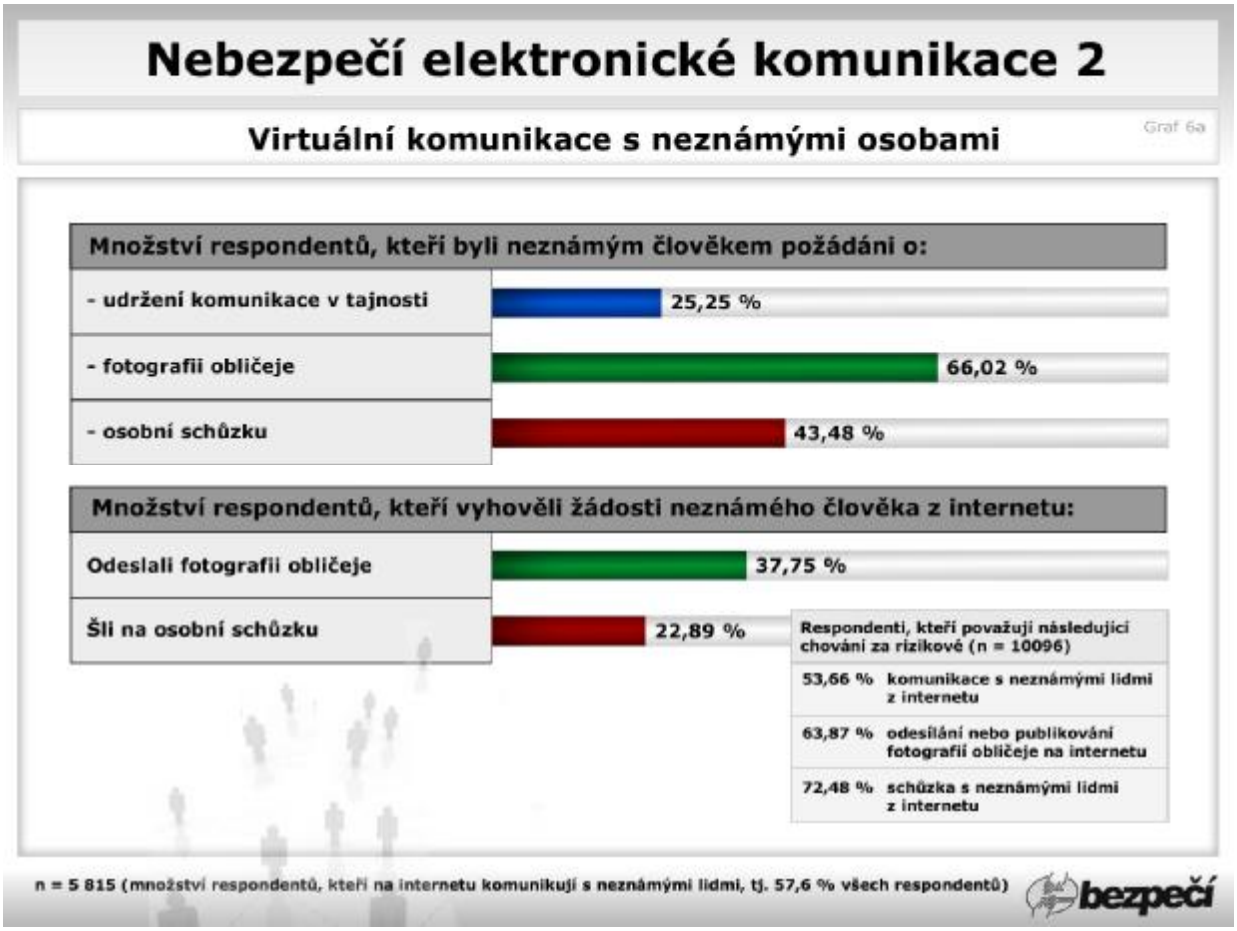
Graf 6 – Virtuální komunikace s neznámými osobami



[3] Kybergrooming označuje manipulativní chování uživatelů internetu, které má v oběti vyvolat důvěru a připravit ji na schůzku. Na osobní schůzce pak může dojít k sexuálnímu obtěžování, pohlavnímu zneužití, týrání nebo manipulaci oběti (např. nucení ke krádežím, terorismu aj.) (dle Kopecký, K., 2008-2010).

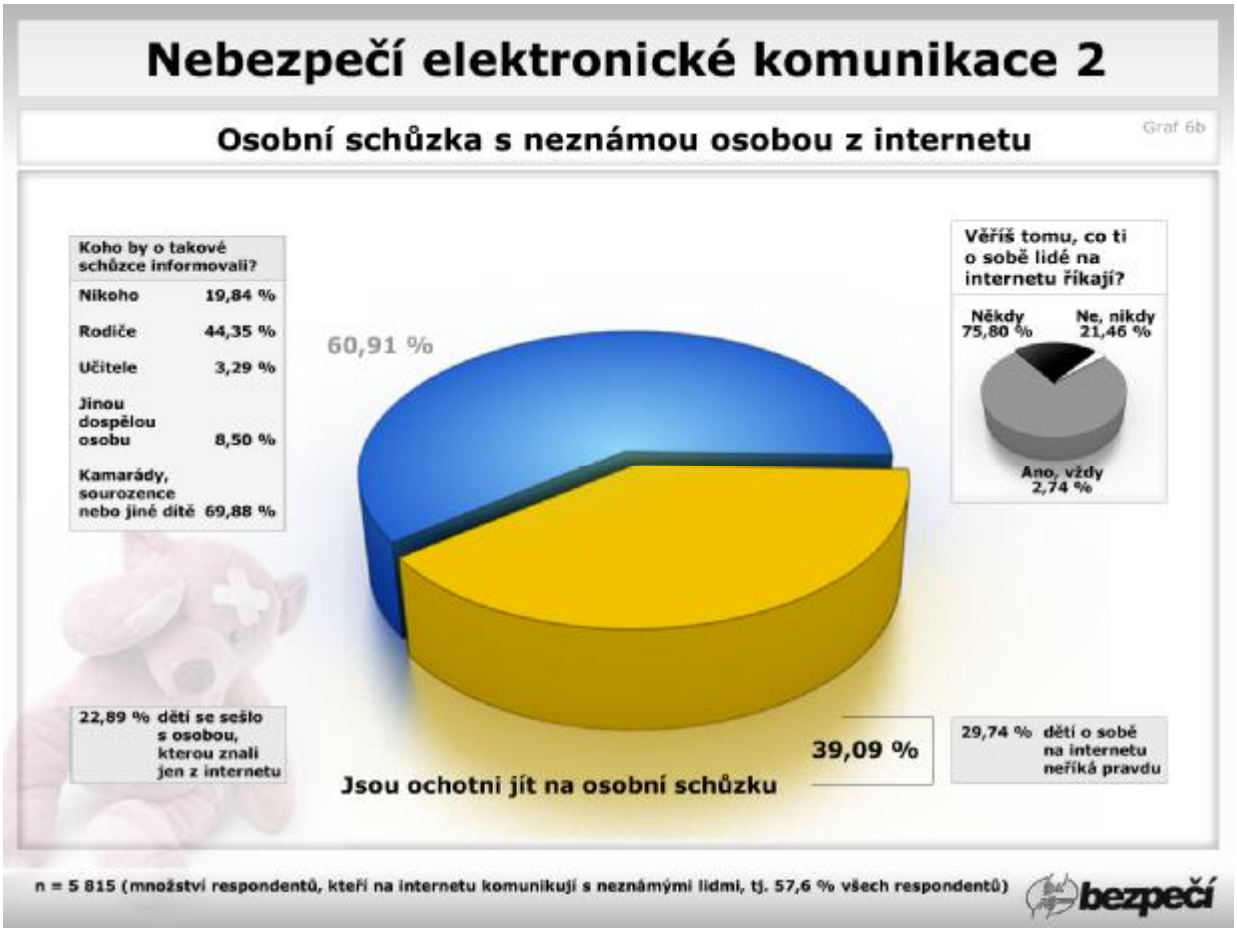
V rámci takové komunikace byla řada dotazovaných vyzvána k jednání, kterým by je mohlo vystavit určitému riziku. Např. 25,25 % dětí komunikujících s neznámými lidmi na internetu bylo požádáno o to, aby nikomu nesdělovaly, že komunikují s konkrétním člověkem na internetu nebo jaký je obsah vedené konverzace. To lze považovat za jeden ze alarmujících signálů, naznačujících, že v komunikaci dochází k něčemu závadnému. Děti komunikující s neznámými osobami jsou také velmi často žádány, aby dané osobě poslali fotografii obličeje (66,02 % respondentů). 37,75 % pak takovou fotografii skutečně odeslalo. 43,48 % dětí bylo neznámou osobou z internetu požádáno o osobní setkání, 22,89 % dětí již takovou schůzku uskutečnilo. *(Graf 6a)*

Graf 6a – Virtuální komunikace s neznámými osobami



Ochotu jít na osobní schůzku, pokud by je o ni internetový známý požádal, projevilo 39,09 % dotazovaných. O svém plánu uskutečnit osobní schůzku s neznámou osobou by přitom respondenti informovali především své kamarády, sourozence, případně jinou nezletilou osobu (69,88 % respondentů). Rodičům by se svěřilo 44,35 % dětí. 19,84 % dotazovaných by přitom neinformovalo vůbec nikoho. *(Graf 6b)*

Graf 6b – Osobní schůzka s neznámou osobou z internetu



5.3 Sdílení osobních údajů v rámci služeb internetu

Sdílení osobních údajů patří k rizikovým prvkům virtuální komunikace, neboť tyto citlivé údaje mohou být velmi snadno zneužity k různým patologickým komunikačním praktikám, jako je např. kyberšikana (zejména pak ve formě vydírání), kybergrooming nebo kyberstalking, ale také k patologickému, či dokonce kriminálnímu jednání (příkladem je využívání těchto údajů zloději- tzv. bytaři).

Respondenti byli dotazováni na tyto konkrétní osobní údaje:

- jméno spolu s příjmením,
- fotografii obličeje,
- adresu bydliště,
- adresu školy,
- telefonní číslo,
- e-mailovou adresu,
- kontaktní údaje VoIP[4] (např. Skype) nebo IM[5] (např. ICQ),
- heslo k e-mailovému účtu,
- rodné číslo,
- PIN kód kreditní karty.

V rámci výzkumného šetření byly sledovány dvě podoby sdílení osobních údajů:

1. Zda respondenti své osobní údaje zveřejňují volně na internetu *(dále jen zveřejňují)*.
2. Zda tyto údaje sdělují neznámým osobám v rámci virtuální komunikace *(dále jen sdělují)*. Ke sdělení osobního údaje mohlo dojít po delší komunikaci s neznámou osobou, za úplatu atd.

[4] Voice over Internet Protocol (zkratka VoIP) je technologie umožňující přenos digitalizovaného hlasu prostřednictvím počítačové sítě nebo jiného média prostupného pro protokol IP. Využívá se pro telefonování prostřednictvím internetu, intranetu nebo jakéhokoliv jiného datového spojení.

[5] Instant messenger (zkratka IM) je internetová služba umožňující svým uživatelům sledovat, kteří jejich přátelé jsou právě připojeni, a dle potřeby jim posílat zprávy, chatovat, přeposílat soubory mezi uživateli atd. Hlavní výhodou oproti používání např. e-mailu spočívá v principu odesílání a přijímání zpráv v reálném čase (zpráva je doručena ve velmi krátké době, většinou v rámci stovek milisekund).

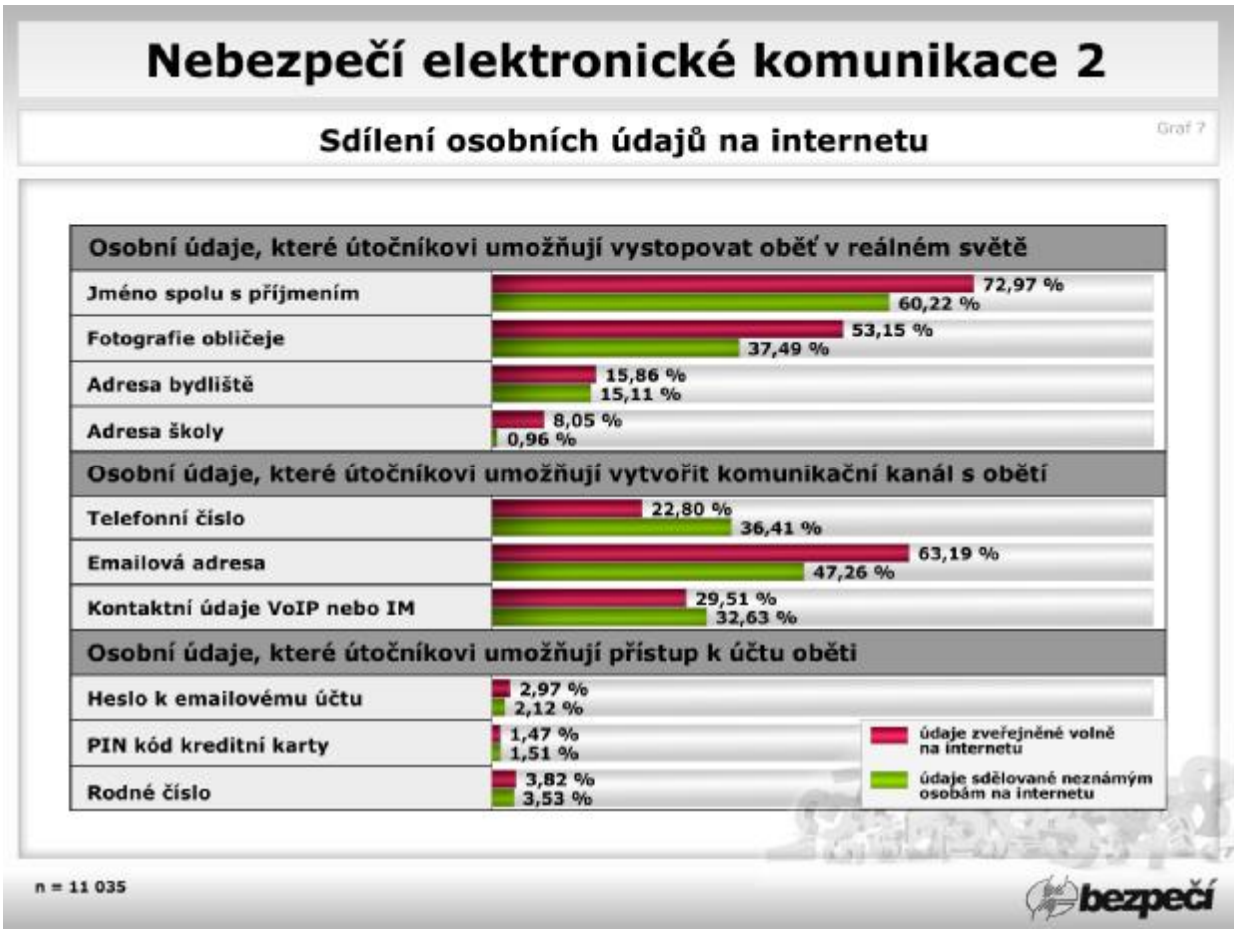
Z výzkumu vyplynulo, že respondenti mají řadu rizikových osobních údajů volně zveřejněných na internetu, což v praxi znamená, že si tyto údaje může prohlédnout v podstatě kdokoli. U většiny sledovaných údajů pak procentuelní hodnota volně zveřejňovaných údajů převyšuje procentuelní hodnotu údajů sdělovaných neznámým osobám v rámci virtuální komunikace. Výjimku tvoří pouze častější sdělování telefonního čísla, kontaktních údajů VoIP nebo IM a PIN kódu kreditní karty. *(Graf 6)*

Při hodnocení jednotlivých osobních údajů je však nutné zvážit rozdílnou rizikovost sdílení těchto údajů a s ní související nebezpečí, které pro respondenta představuje jejich vyzrazení. Mezi rizikové osobní údaje zahrnujeme např.:

- údaje, na základě kterých může být dítě vysledováno v reálném životě (např. jméno spolu s příjmením zveřejňuje 72,97 % a sděluje 60,22 % respondentů, adresu bydliště zveřejňuje 15,86 % a sděluje 15,11 % dotazovaných),
- údaje, které vytvoří mezi dítětem a útočníkem komunikační kanál (např. e-mailovou adresu zveřejňuje 63,19 % a sděluje 47,26 % dětí, kontaktní údaje VoIP nebo IM zveřejňuje 29,51 % a sděluje 32,63 % dotazovaných, telefonní číslo zveřejňuje 22,80 % a sděluje 36,41 % respondentů),
- údaje, které útočníkovi umožňují přístup k cizímu účtu zveřejňuje nebo sděluje oproti předešlým hodnotám výrazně menší počet respondentů (u sledovaných údajů je to 1,47 % a 3,82 % respondentů). (*Graf 7*)

Zvláštní pozornost bychom měli věnovat sdílení fotografií. Kazuistika ukazuje, že právě fotografie obličeje dětí bývá pádným nástrojem např. k vydírání směřujícímu k sexuálnímu násilí na dětech atd. Z výzkumného šetření vyplynulo, že fotografii obličeje má na internetu volně zveřejněnu 53,15 % a 37,49 % je ochotno sdílet ji s neznámou osobou na internetu. *(Graf 7)*

Graf 7 – Sdílení osobních údajů



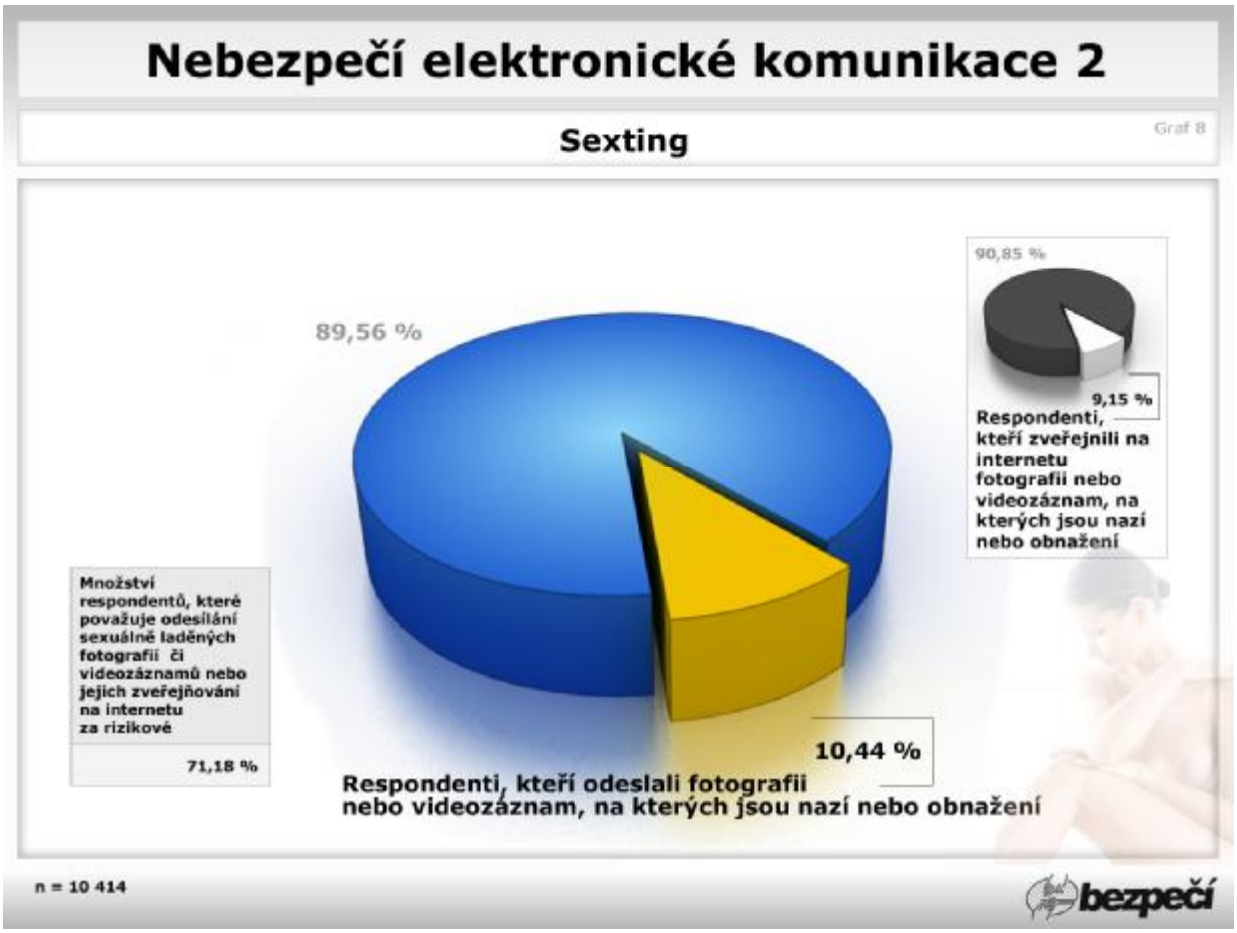
Sexting[6]

V rámci sdílení osobních údajů bylo sledováno také to, zda jsou respondenti ochotni zveřejnit či odeslat další osobě (ať už mobilním telefonem nebo pomocí některé ze služeb internetu) sexuálně laděnou fotografii nebo videozáznam. Konkrétně se jednalo o takový záznam, který zachycuje nahé nebo částečně obnažené tělo dotazovaných. Jedná se o tzv. sexting. Ten patří k dalším rizikovým činnostem souvisejícím s virtuální komunikací, neboť tyto materiály mohou opět sloužit např. jako nástroj vydírání, ponižování nebo diskreditování oběti.

Z odpovědí vyplynulo, že 10,44 % dětí alespoň jednou odeslalo další osobě sexuálně laděnou fotografii nebo videozáznam. 9,15 % pak má takové vyobrazení zveřejněno volně na internetu. Zajímali jsme se také o to, zda děti považují toto jednání za rizikové – to potvrdilo 71, 18 % dotazovaných. (*Graf 8*)

[6] Termíny sexting nebo sextování označuje odesílání sexuálně laděných zpráv, fotografií či videozáznamů, jehož cílem je nejčastěji navázání partnerského vztahu mezi odesilatelem a příjemcem nebo jeho zpestření.

Graf 8 – Sexting



5.4 Potenciálně riziková virtuální prostředí

V rámci výzkumného šetření byla naše pozornost zaměřena také na virtuální prostředí, která jsou dle kazuistiky zneužívána jako nástroj pro realizaci nebezpečných komunikačních praktik nebo jinak souvisí s rizikovou virtuální komunikací.

Na základě této analýzy byly vybrány 3 formy potenciálně rizikových prostředí, k nimž pak byly přiřazeny v českém prostředí nejznámější a nejužívanější příklady konkrétních portálů. Jednalo se o:

- sociální sítě,
- webová úložiště dat,
- portály zaměřené na dětské uživatele.

Sociální sítě[7]

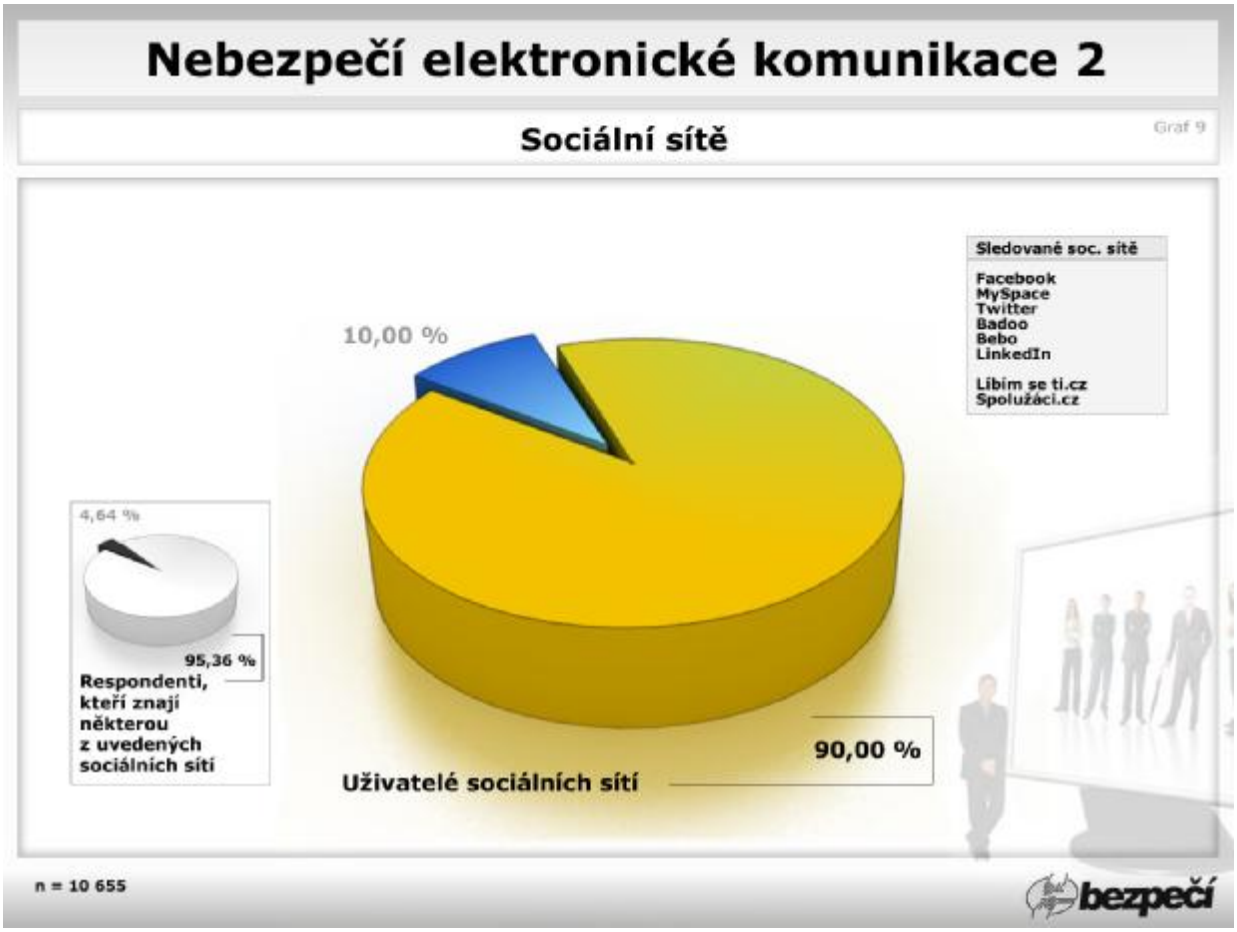
Sociální sítě jsou několik let na velkém vzestupu, po celém světě si našly řadu příznivců. Kromě výhod však pro své uživatele představují určitá rizika plynoucí především ze sdílení osobních údajů, osobních fotografií nebo videí, snadné přístupnosti a anonymity uživatelů. Sociální sítě poskytují velký prostor pro sociální inženýrství[8] a nebezpečné komunikační praktiky, jako jsou např. kyberšikana, sexting, kybergrooming, kyberstalking atd.

[7] Sociální sítě je označení pro informační sítě poskytované internetovými portály, které umožňují vytvářet virtuální společenství. Sociální sítě nabízejí prostor pro prezentaci lidí, komunikaci, navazování sociálních vztahů, vzdělávání, komerci (reklama, marketing, sociotechnika) nebo jakoukoli jinou lidskou činnost, kterou lze virtuálně realizovat.

[8] Sociální inženýrství nebo sociotechnika je způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace. Termín je běžně používán ve významu nezákonného podvodu nebo podvodného jednání za účelem získání utajených informací organizace nebo přístup do informačního systému firmy.

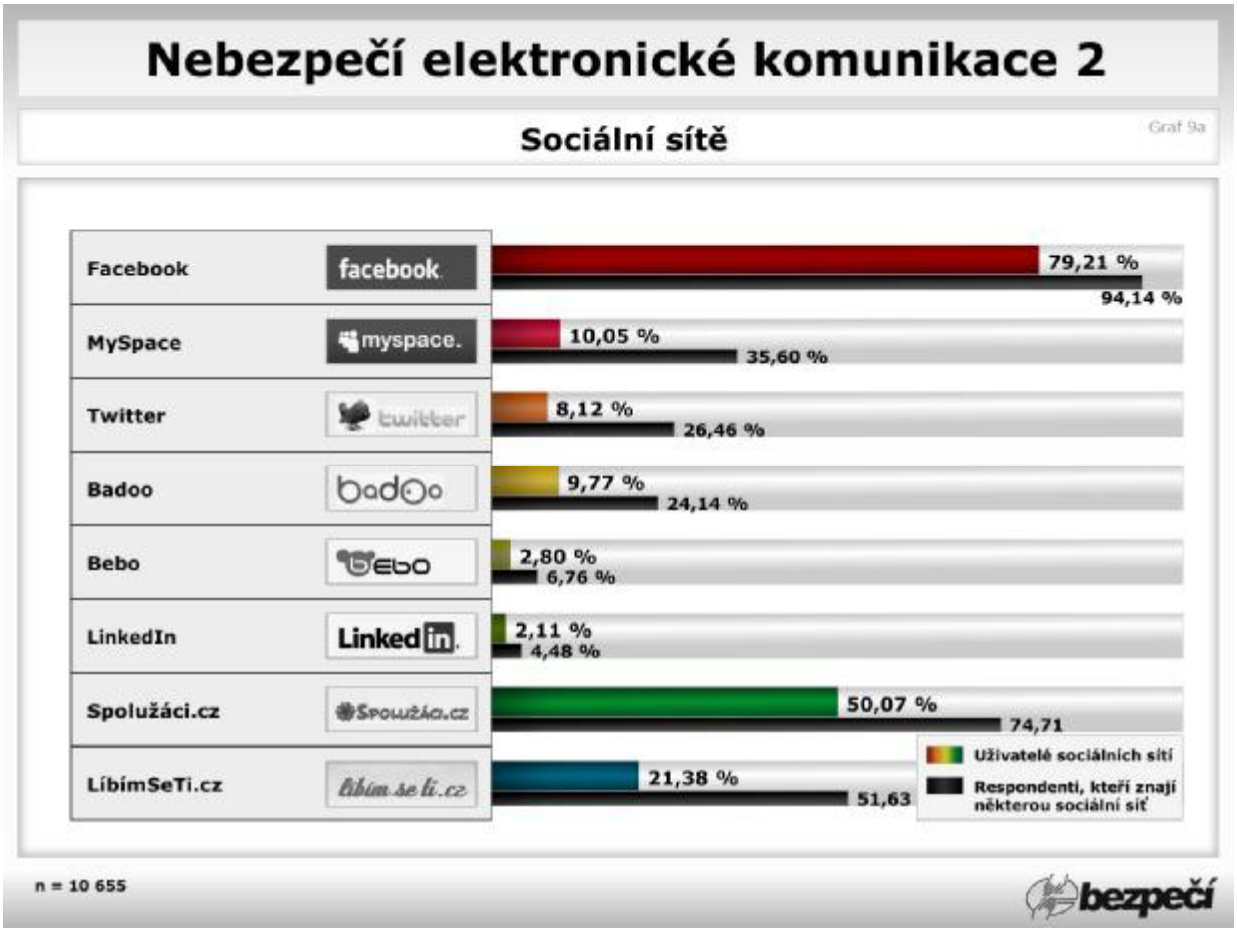
95,36 % oslovených respondentů uvedlo, že zná alespoň jednu z uvedených sociálních sítí. V rámci výzkumu byly sledovány tyto sociální sítě: Facebook, MySpace, Twitter, Badoo, Bebo, LinkedIn, Líbím se ti.cz a Spolužáci.cz. 90,00 % dětí má na některé ze zmíněných sociálních sítí svůj účet. *(Graf 9)*

Graf 9 – Sociální sítě



Nejznámější a uživatelsky nejrozšířenější sociální sítě je americká síť Facebook (94,14 % respondentů uvedlo, že ji zná, 79,21 % na ní má svůj účet). Z českých sociálních sítí je nejznámější i nejužívanější sociální síť Spolužáci.cz (74,71 % ji zná a 50,07 využívá), která v celkovém přehledu skončila na druhém místě, a sociální síť Líbímseti.cz, která se umístila na místě třetím (51,63 % dětí ji zná a 21,38 % používá). *(Graf 9a)*

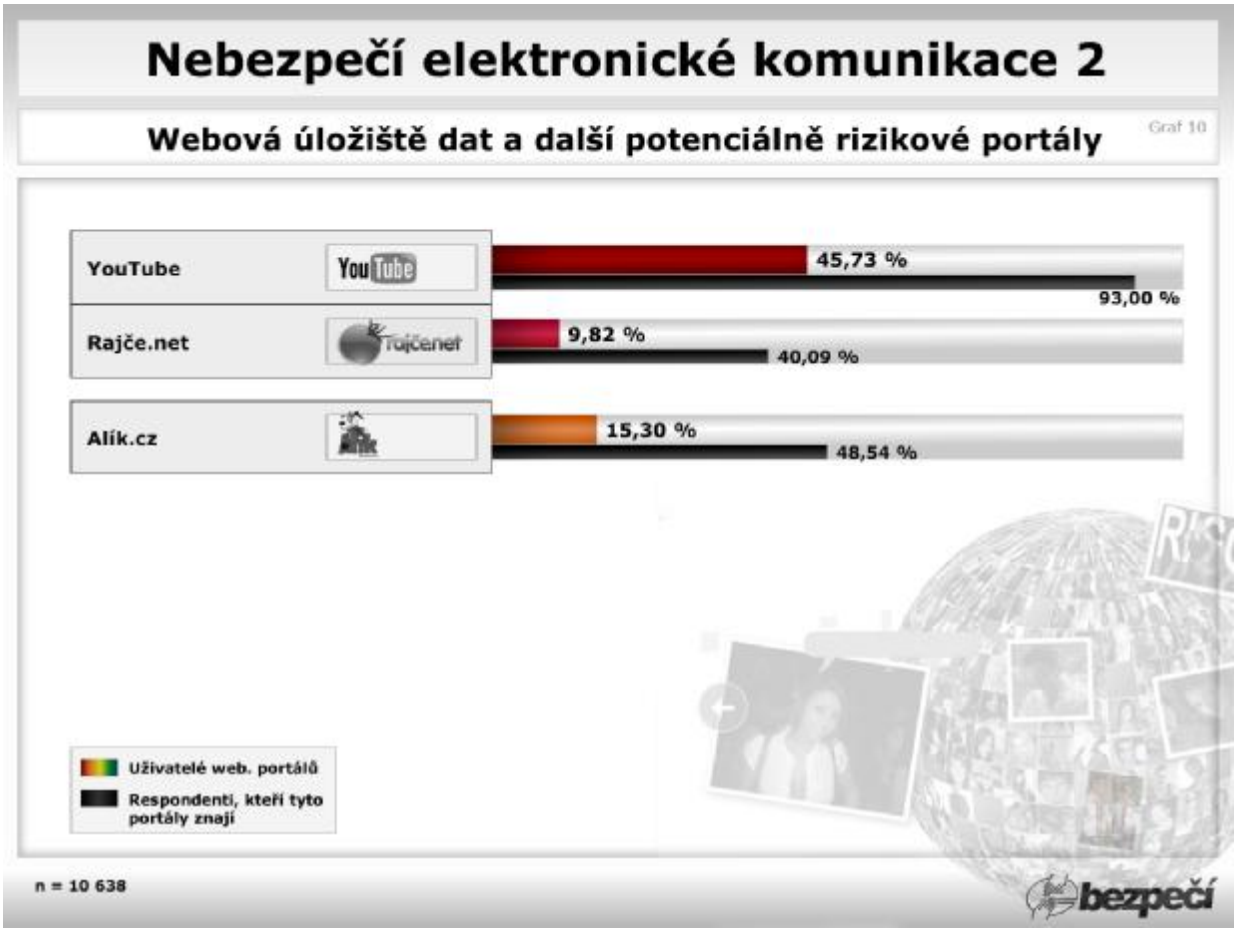
Graf 9a – Sociální sítě (přehled)



Webová úložiště dat a další potenciálně rizikové portály

Z dalších rizikových portálů byla dále sledována webová úložiště videí (konkrétně YouTube) a fotografií (Rajče.net) a portály zaměřené na dětské uživatele (Alík.cz). Tyto konkrétní portály byly v minulosti spojovány např. s projevy kyberšikany, vydíráním a dalšími manipulacemi ze strany sexuálních útočníků. *(Graf 10)*

Graf 10 – Webová úložiště dat a další potenciálně rizikové portály



6. Shrnutí

U řady sledovaných skutečností došlo ve srovnání s výzkumným šetřením Nebezpečí elektronické komunikace (realizace rok 2009-2010)[9], k určitému posunu. Znatelný je např. nárůst původců kyberšikany z 27,8 % na 41,08 %. Počet obětí se oproti předešlému výzkumu zvýšil asi o 6 % (z 53,2 % na 59,38 %). Naopak za pozitivní lze považovat změny hodnot u odpovědí týkajících se hledání pomoci při řešení kyberšikany. U všech sledovaných projevů se zájem respondentů obrátit se o pomoc na dospělou osobu (rodiče / učitele) zvýšil průměrně na dvojnásobek.

Zatímco počet dětí, které jsou ochotny jít na osobní schůzku s neznámou osobou z internetu, zůstal oproti předešlému výzkumnému šetření téměř na stejných hodnotách (z 39,2 % mírně klesl na 39,09 %), vzrostl počet dětí, které by o konání takové schůzky nikoho neinformovalo (z 8,7 % na 19,84 %).

Aktuální výzkumné šetření ukázalo na větší opatrnost respondentů při nakládání s osobními údaji v rámci internetu. U všech sledovaných osobních údajů byl zaznamenán pokles hodnot zachycujících volné zveřejňování těchto údajů na internetu či při jejich vyžádaného sdílení (u řady údajů se jednalo o pokles o 10 i více procent). Co se týká zveřejňování nebo odesílání sexuálně laděných fotografií či videozáznamů, jsou hodnoty srovnatelné s hodnotami získanými z minulého výzkumného šetření (z 10,1 % se počet zvýšil na 10,44 %).

Podobně jsou na tom respondenti také s povědomím o sociálních sítích a jejich užíváním , kde jsou hodnoty prakticky totožné jako v předešlém výzkumném šetření.

[9] Rizika elektronické komunikace 2009-2010 (výzkumná zpráva) online on: http://prvok.upol.cz/index.php/ke-staeni/doc_download/5-nebezpei-internetove-komunikace-e-bezpei-prvok-2009-2010

7. Kontakt

Realizátoři

Mgr. Veronika Krejčí

Centrum prevence rizikové virtuální komunikace

Pedagogická fakulta Univerzity Palackého v Olomouci

veronika.krejci@upol.cz

+420 777 588 382

Mgr. Kamil Kopecký, Ph.D.

Centrum prevence rizikové virtuální komunikace

Pedagogická fakulta Univerzity Palackého v Olomouci

kamil.kopecky@upol.cz

+420 773 470 997

Kontaktní adresa

Centrum prevence rizikové virtuální komunikace

Pedagogická fakulta Univerzity Palackého v Olomouci

Žižkovo nám. 5

771 40 Olomouc

www.prvok.upol.cz

Informace o dalších výzkumech realizovaných v rámci projektu E-Bezpečí naleznete na stránkách projektu www.e-bezpeci.cz a www.prvok.upol.cz .