NEBEZPEČÍ ELEKTRONICKÉ KOMUNIKACE

ZPRÁVA Z VÝZKUMNÉHO ŠETŘENÍ REALIZOVANÉHO V RÁMCI PROJEKTU PREVENCE NEBEZPEČNÝCH KOMUNIKAČNÍCH PRAKTIK SPOJENÝCH S ELEKTRONICKOU KOMUNIKACÍ PRO PEDAGOGY A NEPEDAGOGY

(406/08/P106)

Mgr. Veronika Krejčí

Mgr. Kamil Kopecký, Ph.D.

Olomouc 2009-2010

Obsah

1. Úvod

Výzkumné šetření bylo realizováno jako součást projektu *Prevence nebezpečných komunikačních praktik spojených s elektronickou komunikací pro pedagogy a nepedagogy* (2008-2009), který je řešen s podporou Grantové agentury České republiky. Výzkum proběhl v rámci dotazníkového systému portálu E-Bezpečí (www.e-bezpeci.cz). Do výzkumného šetření se zapojilo téměř 2 000 respondentů ze základních a středních škol z celé České republiky, včetně škol zapojených do Partnerského programu projektu E-Bezpečí.

2. Metodologie

Základním prostředkem získávání dat bylo prostředí online dotazníkového systému E-Bezpečí, které bylo vytvořeno speciálně pro výzkumná šetření tohoto typu. Online dotazník byl volně přístupný na stránkách portálu E-Bezpečí od 1. září do 30. listopadu 2009.

Souběžně s online šetřením probíhala terénní výzkumná šetření s využitím klasických „papírových" dotazníků. Takto získaná data byla poté připojena k datům z online výzkumu.

Do dotazníku byly zařazeny otázky různého typu - s jednou možností, s více možnostmi, s možností otevřené odpovědi apod. Úsilí respondentů bylo motivováno možností zapojit se do losování o zajímavé ceny, které jsme jim nabídli jako motivační odměnu (trička, reklamní předměty, samolepky, plakáty apod.). Zájemci o ceny se v dotazníku identifikovali svým e-mailem.

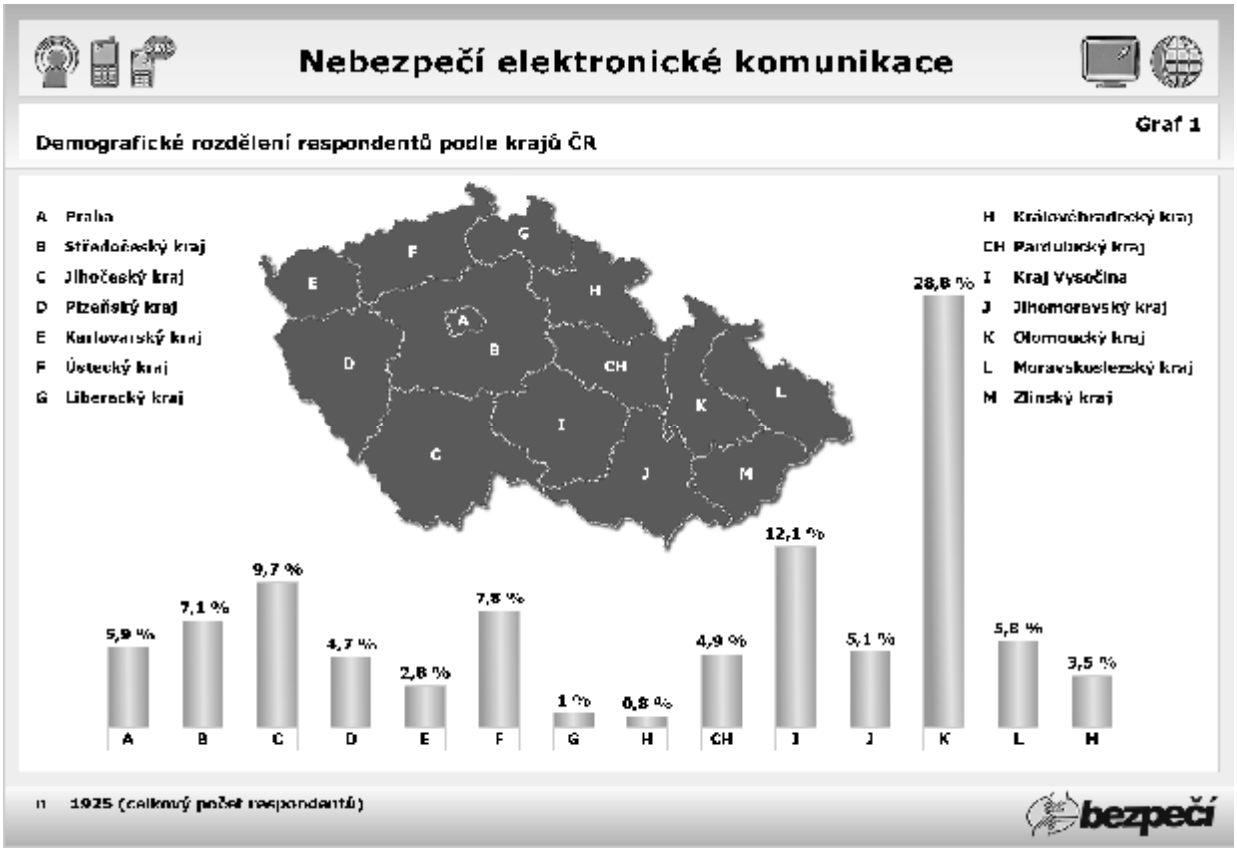
Respondenti výzkumného šetření vyplňovali dotazník anonymně.

Cílem šetření bylo zjistit:

- Zkušenosti respondentů s kyberšikanou z pohledu obětí i útočníků (včetně kyberšikany učitelů) a jejich zájem zapojit do řešení těchto problémů další osoby.
- Zkušenosti respondentů se sextingem.
- Povědomí respondentů o webových stránkách s možností publikování videozáznamu (potenciální prostředí pro šíření kyberšikany).
- Povědomí respondentů o sociálních sítích a jejich zkušenosti s nimi (potenciální prostředí pro získávání osobních dat k jejich možnému zneužití a pro šíření kyberšikany, pro kybergrooming, stalking a další nebezpečné praktiky).
- Ochota respondentů setkávat se s osobami, se kterými se seznámili na internetu, a podmínky takových schůzek (kybergrooming).
- Zkušenosti respondentů se stalkingem a kyberstalkingem z pohledu obětí a pozorovatelů.

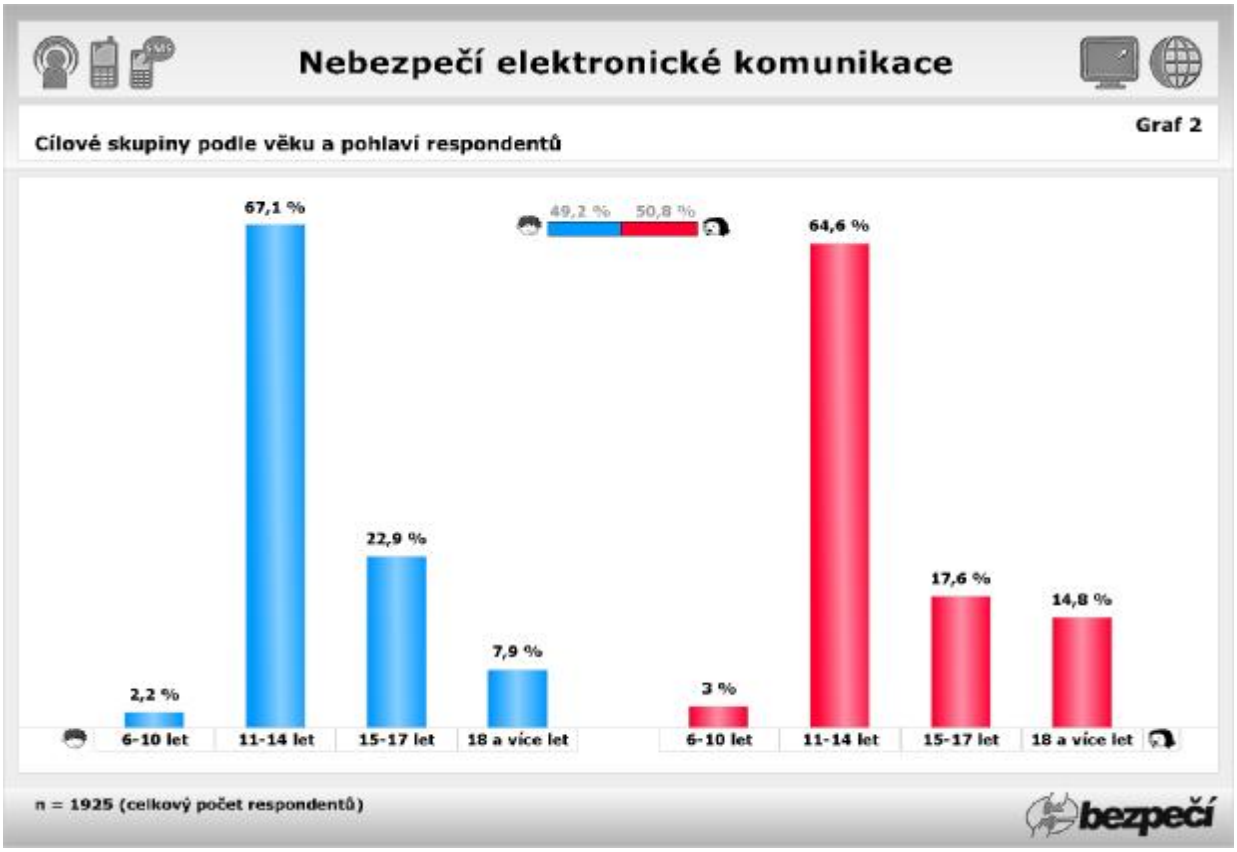
3. Výzkumný vzorek

Výzkumné šetření pracovalo se vzorkem **1 925** respondentů tvořeným zejména žáky základních a středních škol ze všech krajů České republiky. Největší zastoupení měli respondenti z Olomouckého kraje (28,8 %) , naopak nejméně respondentů bylo z Královéhradeckého kraje (0,8 %). (***Graf 1***)



Vzorek byl tvořen ze 49,2 % chlapci a 50,8 % dívkami. Věkově byl vzorek rozdělen do 4 skupin[1]. Nejvíce respondentů tvořili žáci ve věku 11-14 let (65,8 %). (***Graf 2***)

[1] *Při sestavování skupin bylo přihlédnuto jak k příslušnému stupni školy (1. a 2. stupeň ZŠ a 3. stupeň SŠ), tak k hraničnímu věku trestní odpovědnosti (od 15 let) a plnoletosti (od 18 let).*


Nebezpečí elektronické komunikace
Graf 2
Cílové skupiny podle věku a pohlaví respondentů
67,1 %
2,2 %
22,9 %
7,9 %
49,2 %
50,8 %
64,6 %
3 %
17,6 %
14,8 %
6-10 let
11-14 let
15-17 let
18 a více let
6-10 let
11-14 let
15-17 let
18 a více let
n = 1925 (celkový počet respondentů)

4. Výsledky výzkumu

Kyberšikana[2]

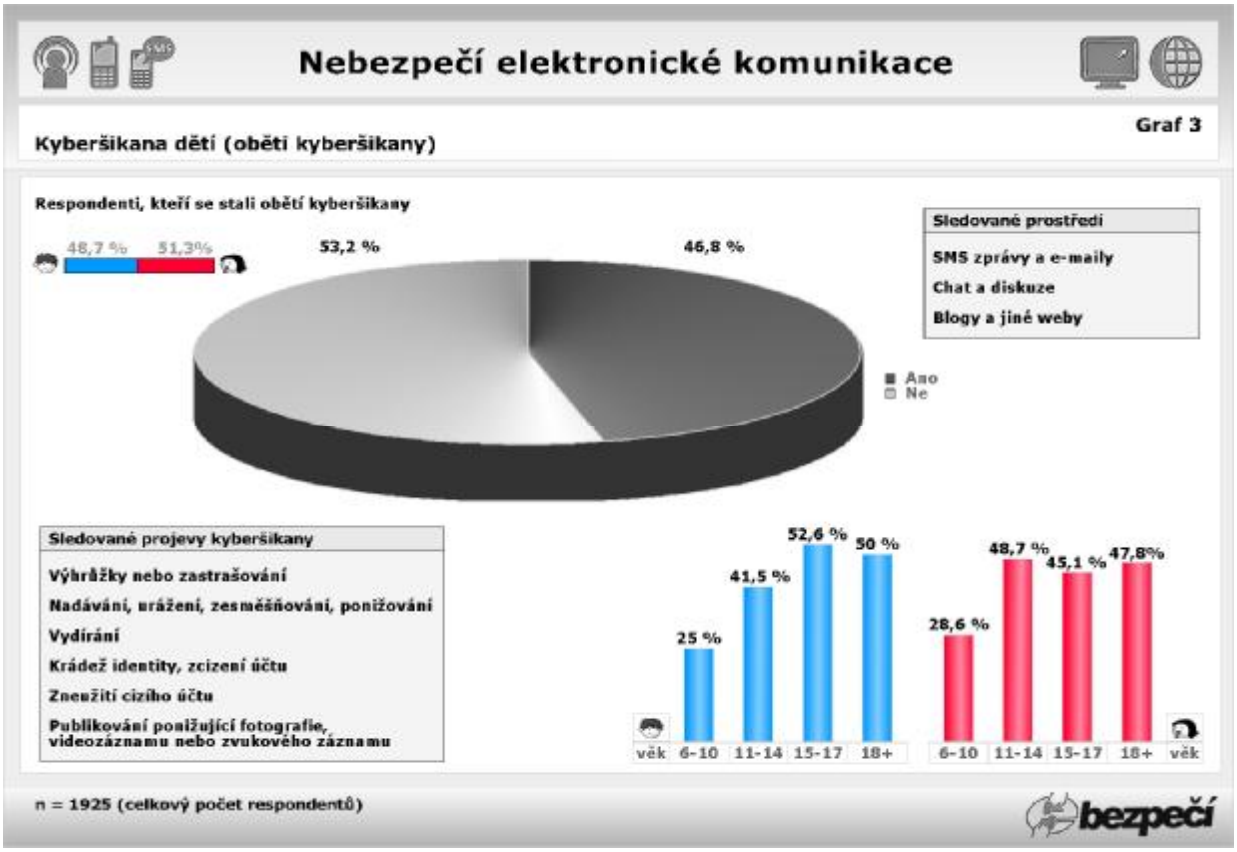
Kyberšikana je závažný problém, se kterým se žáci potýkají poměrně často, proto jí bylo věnováno nejvíce prostoru také ve výzkumném šetření. V rámci výzkumu bylo sledováno několik projevů kyberšikany:

- vyhrožování a zastrašování,
- nadávání, urážení, zesměšňování a ponižování,
- vydírání,
- krádež identity a zneužití cizího účtu ke kyberšikaně,
- publikování ponižující fotografie, videozáznamu nebo zvukového záznamu.

[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.

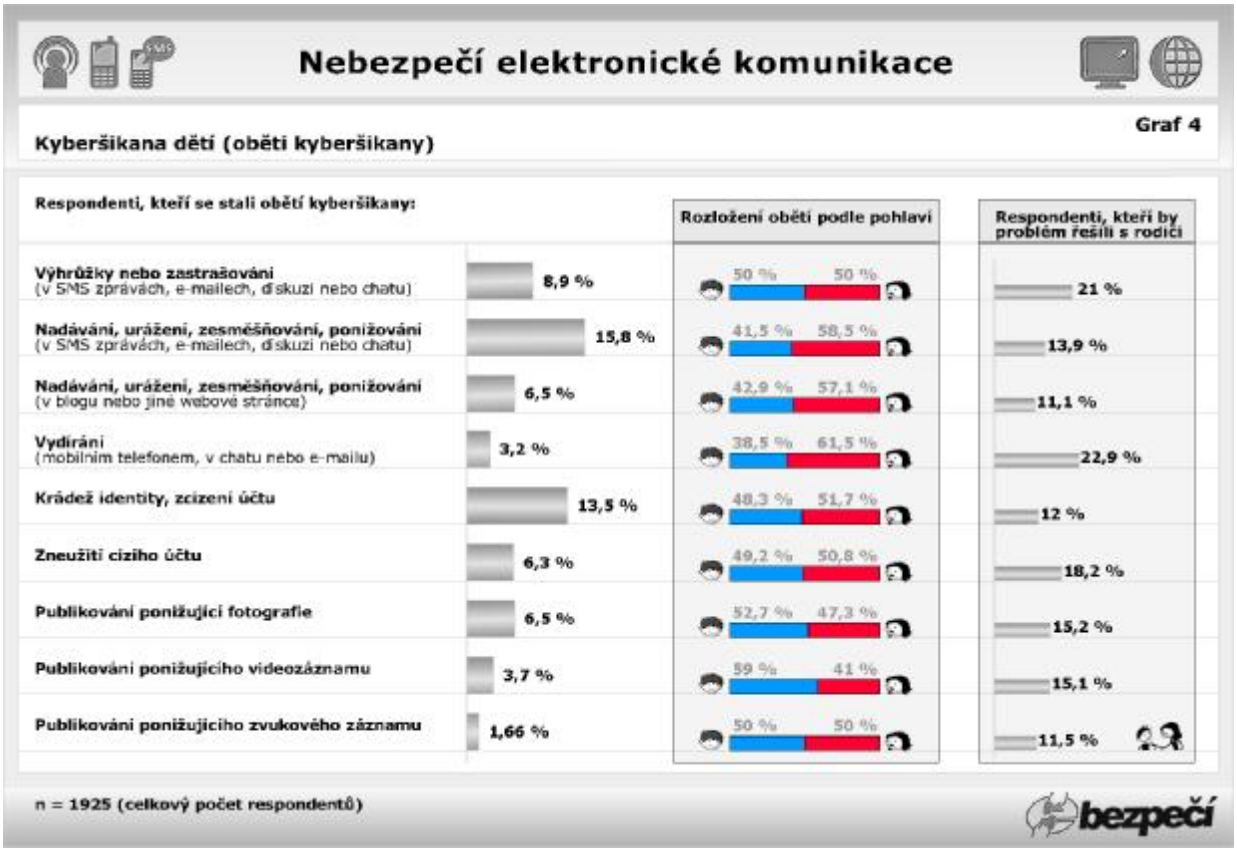
Kyberšikana dětí (oběti kyberšikany, zapojení rodičů do řešení kyberšikany)

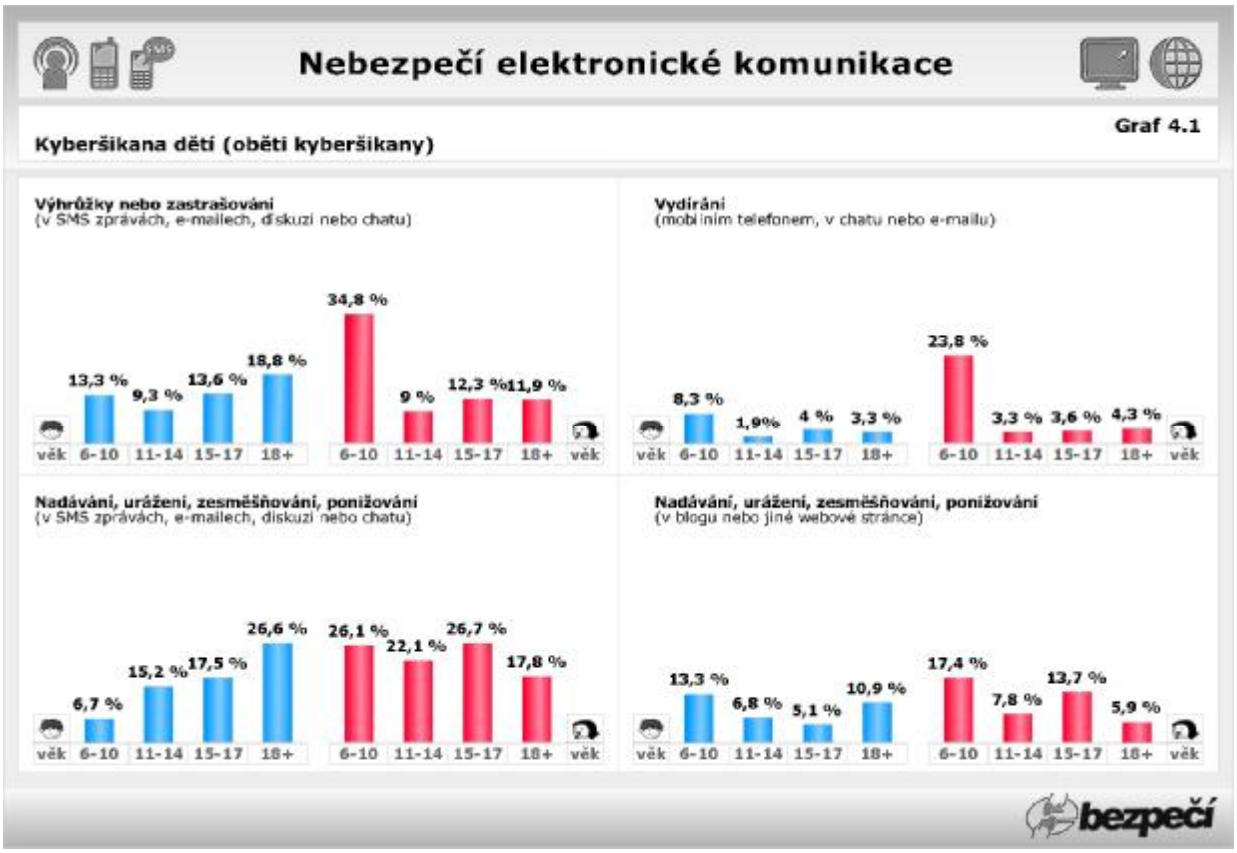
Z výzkumného šetření vyplynulo, že téměř polovina dětí (46,8 %) měla problémy s kyberšikanou. Obětí kyberšikany byly častěji dívky (51,3 %). Graf znázorňující rozložení respondentů podle věku a pohlaví ukazuje, že žáci ve věku 6-10 let jsou vystaveni o téměř polovinu méně útokům (25 % chlapci a 28,6 % dívky) než žáci starší, kde se procento útoků pohybuje v rozmezí 41,5-50 %. (***Graf 3***)



Z pohledu sledovaných projevů kyberšikany je pro žáky nejčastějším problémem nadávání, urážení, zesměšňování a ponižování realizované prostřednictvím SMS zpráv, e-mailů, v chatu nebo v diskuzi. Tuto skutečnost uvedlo 15,8 % všech respondentů. 13,5 % respondentů muselo řešit prolomení ochrany svého elektronického účtu (e-mailového, diskuzního, účtu k vzdělávacímu prostředí atd.). Třetí nejčastější problém představuje vyhrožování nebo zastrašování v SMS zprávách, e-mailech, v diskuzi nebo chatu (8,9 %). (***Graf 4***, ***4.1***, ***4.2***, ***4.3***)

Z výzkumu vyplynulo, že oběti kyberšikany se se svými problémy většinou nesvěřují rodičům. Tuto skutečnost uvedlo 77,1 % dotazovaných. S rodiči by respondenti nejčastěji řešili vydírání (22,9 %). (***Graf 4***)


Nebezpečí elektronické komunikace
Graf 4
Kyberšikana dětí (oběti kyberšikany)
Respondenti, kteří se stali obětí kyberšikany:
Rozložení obětí podle pohlaví
Respondenti, kteří by problém řešili s rodiči
Výhrůžky nebo zastrašování (v SMS zprávách, e-mailech, diskuzi nebo chatu) 8,9 % 50 % 50 % 21 %
Nadávání, urážení, zesměšňování, ponižování (v SMS zprávách, e-mailech, diskuzi nebo chatu) 15,8 % 41,5 % 58,5 % 13,9 %
Nadávání, urážení, zesměšňování, ponižování (v blogu nebo jiné webové stránce) 6,5 % 42,9 % 57,1 % 11,1 %
Vydírání (mobilním telefonem, v chatu nebo e-mailu) 3,2 % 38,5 % 61,5 % 22,9 %
Krádež identity, zcizení účtu 13,5 % 48,3 % 51,7 % 12 %
Zneužití cizího účtu 6,3 % 49,2 % 50,8 % 18,2 %
Publikování ponižující fotografie 6,5 % 52,7 % 47,3 % 15,2 %
Publikování ponižujícího videozáznamu 3,7 % 59 % 41 % 15,1 %
Publikování ponižujícího zvukového záznamu 1,66 % 50 % 50 % 11,5 %
n = 1925 (celkový počet respondentů)


Nebezpečí elektronické komunikace
Graf 4.1
Kyberšikana dětí (oběti kyberšikany)
Výhrůžky nebo zastrašování (v SMS zprávách, e-mailech, diskuzi nebo chatu)
věk 6-10 11-14 15-17 18+ 13,3 % 9,3 % 13,6 % 18,8 %
6-10 11-14 15-17 18+ věk 34,8 % 9 % 12,3 % 11,9 %
Vydírání (mobilním telefonem, v chatu nebo e-mailu)
věk 6-10 11-14 15-17 18+ 8,3 % 1,9% 4 % 3,3 %
6-10 11-14 15-17 18+ věk 23,8 % 3,3 % 3,6 % 4,3 %
Nadávání, urážení, zesměšňování, ponižování (v SMS zprávách, e-mailech, diskuzi nebo chatu)
věk 6-10 11-14 15-17 18+ 6,7 % 15,2 % 17,5 % 26,6 %
6-10 11-14 15-17 18+ věk 26,1 % 22,1 % 26,7 % 17,8 %
Nadávání, urážení, zesměšňování, ponižování (v blogu nebo jiné webové stránce)
věk 6-10 11-14 15-17 18+ 13,3 % 6,8 % 5,1 % 10,9 %
6-10 11-14 15-17 18+ věk 17,4 % 7,8 % 13,7 % 5,9 %

Nebezpečí elektronické komunikace

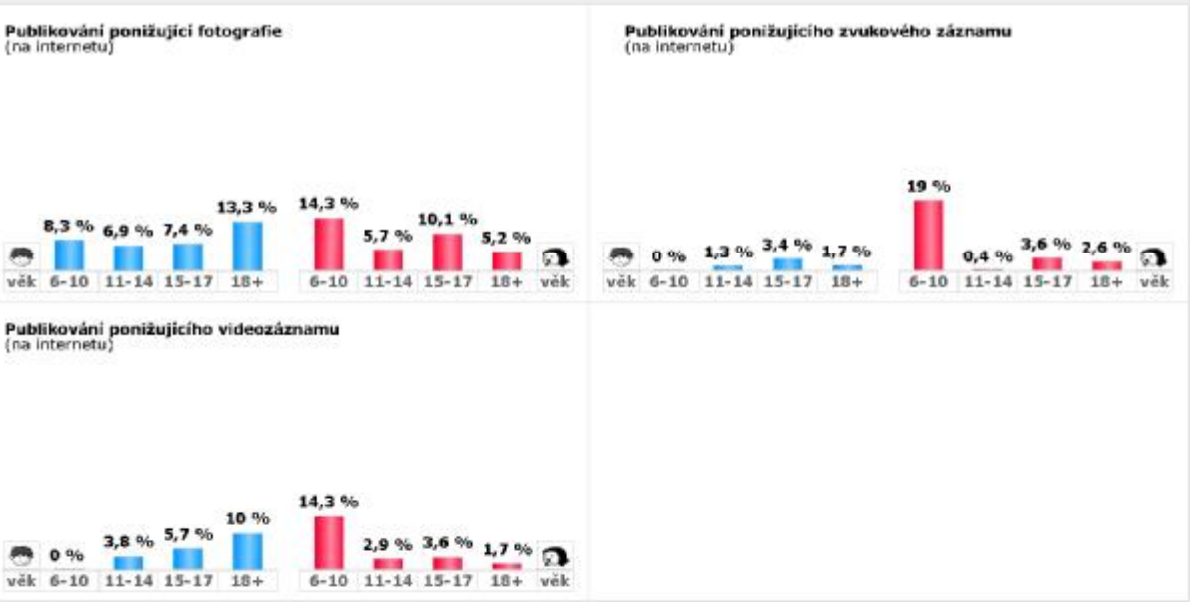
Graf 4.2

Kyberšikana dětí (oběti kyberšikany)

Nebezpečí elektronické komunikace

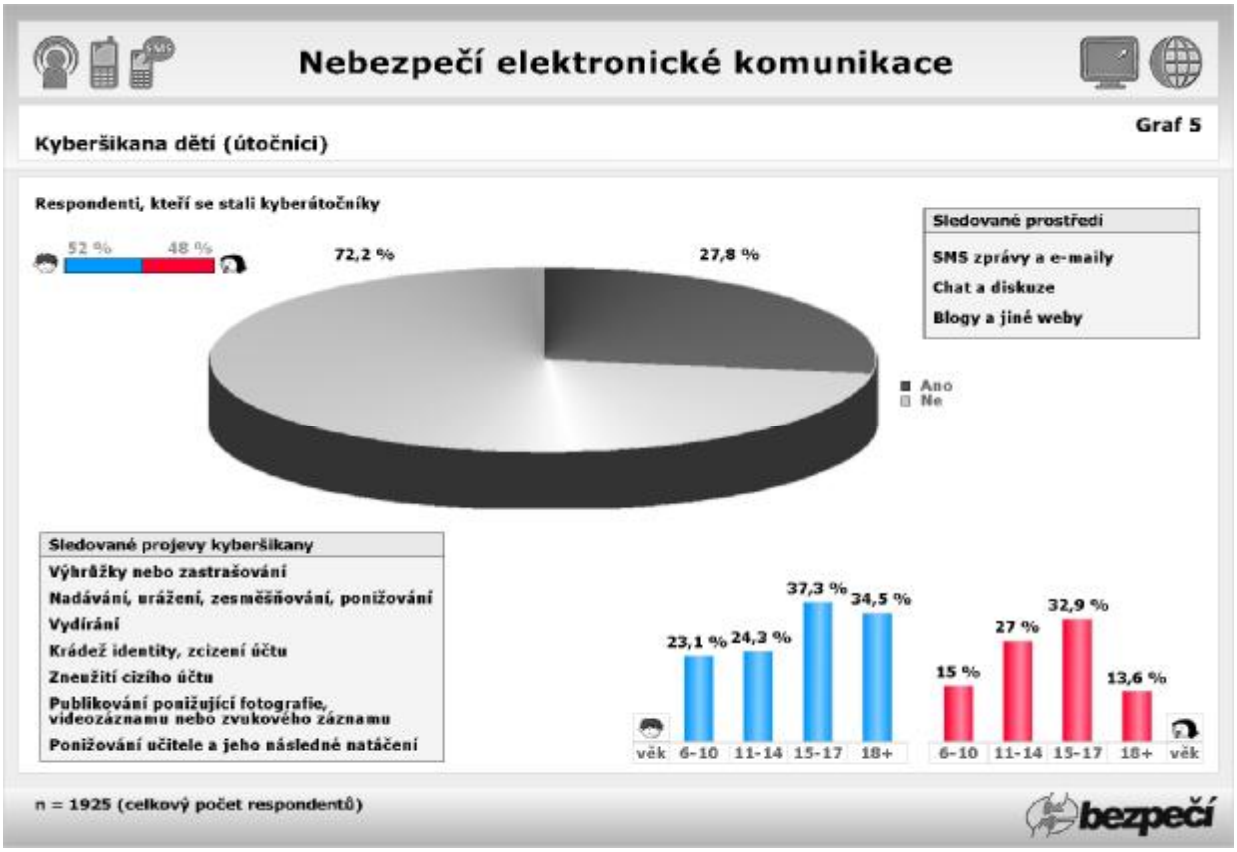
Graf 4.3

Kyberšikana dětí (oběti kyberšikany)

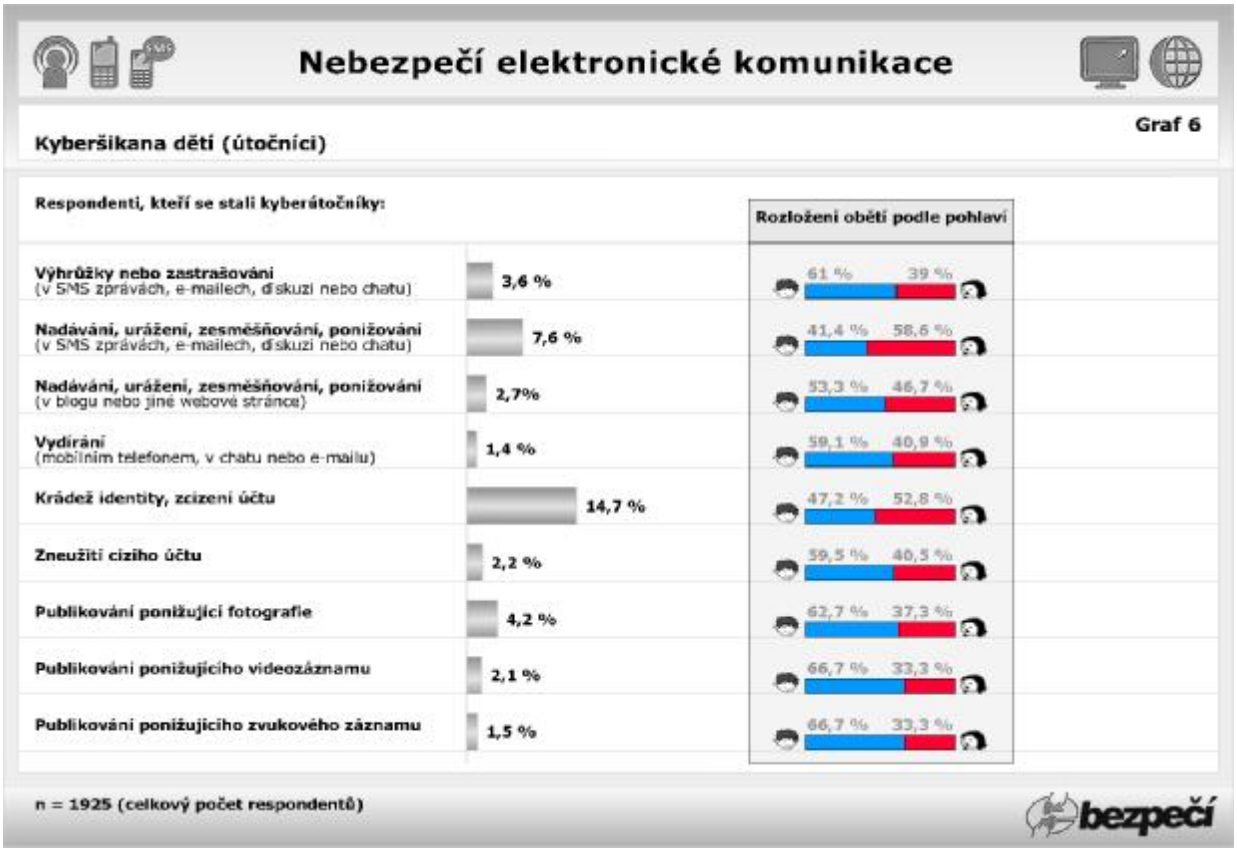


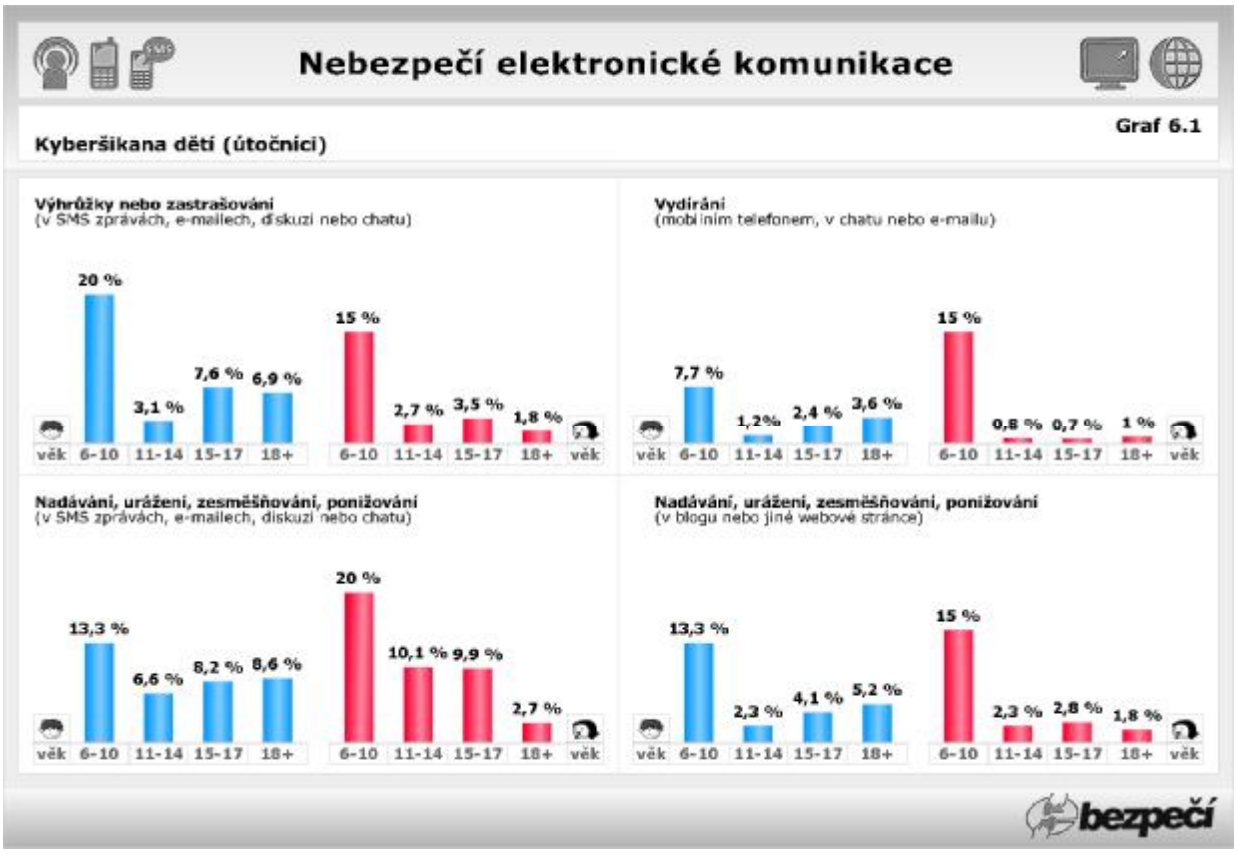
Kyberšikana dětí (útočníci)

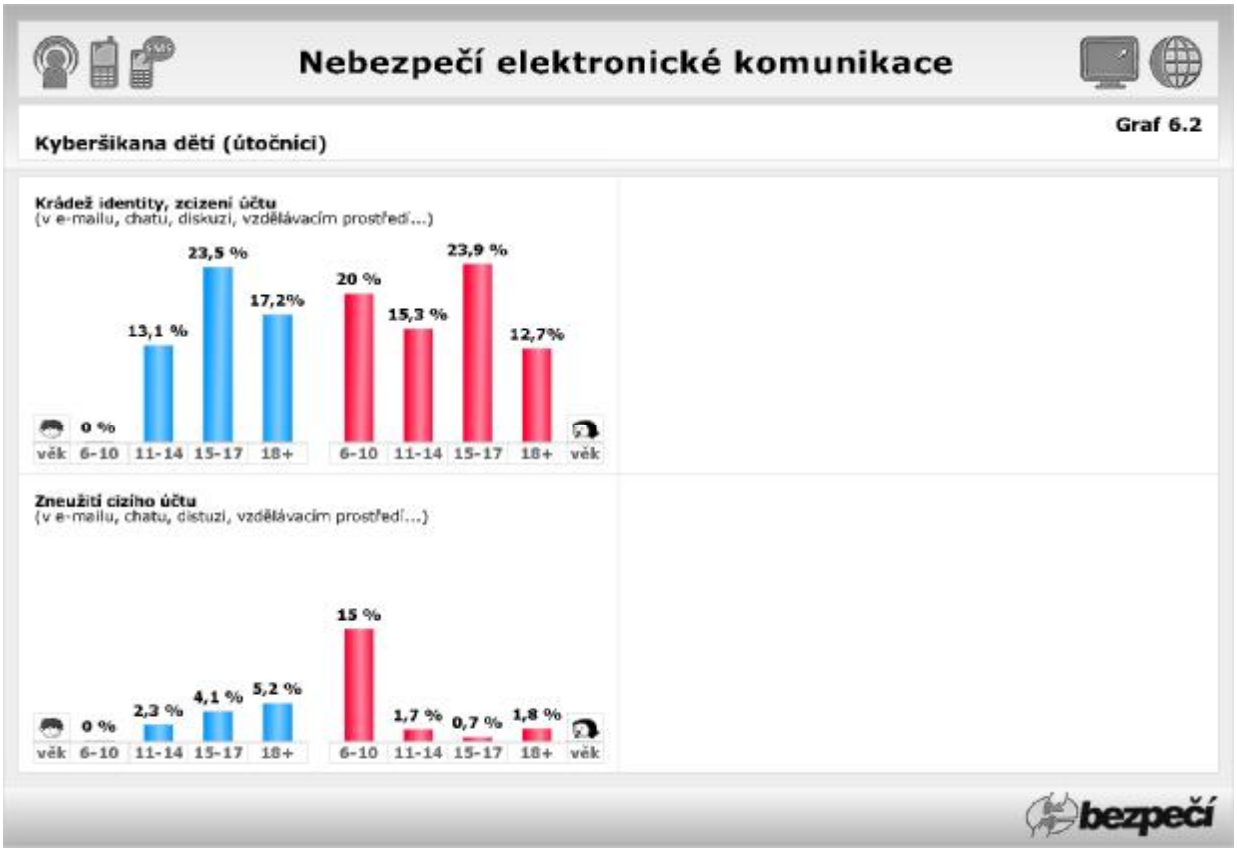
Každý třetí respondent uvedl, že sám vyzkoušel některý ze sledovaných projevů kyberšikany (27,8 %). Útočníky byli častěji chlapci (52 %) než dívky. Ve sledovaném vzorku byli nejčastěji útočníky chlapci ve věku 15-17 let (37,3 %), dále chlapci ve skupině 18+ (34,5 %) a dívky ve věku 15-17 let (32,9 %). (***Graf 5***)

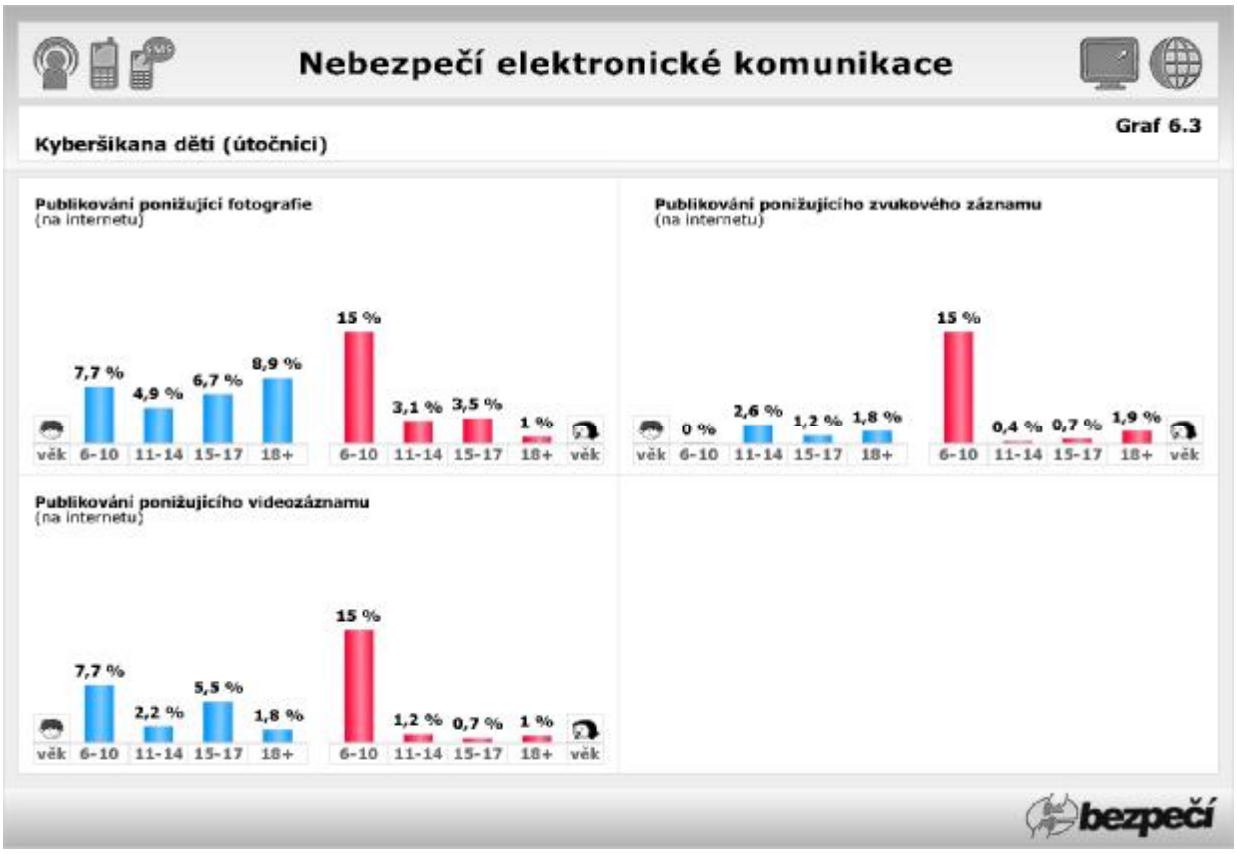


K nejčastějším útokům patří přihlášení se k cizímu účtu (14,7 %). 7,6 % respondentů uvedlo, že nadává, uráží, zesměšňuje nebo ponižuje ostatní SMS zprávami, e-maily, v chatu nebo v diskuzi a 4,2 % ponižuje pomocí zesměšňujících fotografií, jež zveřejňují na internetu. (***Graf 6***, ***6.1***, ***6.2***, ***6.3***)


Nebezpečí elektronické komunikace
Graf 6
Kyberšikana dětí (útočníci)
Respondenti, kteří se stali kyberátočníky:
Rozložení obětí podle pohlaví
Výhrůžky nebo zastrašování (v SMS zprávách, e-mailech, diskuzi nebo chatu) 3,6 % 61 % 39 %
Nadávání, urážení, zesměšňování, ponižování (v SMS zprávách, e-mailech, diskuzi nebo chatu) 7,6 % 41,4 % 58,6 %
Nadávání, urážení, zesměšňování, ponižování (v blogu nebo jiné webové stránce) 2,7% 53,3 % 46,7 %
Vydírání (mobilním telefonem, v chatu nebo e-mailu) 1,4 % 59,1 % 40,9 %
Krádež identity, zcizení účtu 14,7 % 47,2 % 52,8 %
Zneužití cizího účtu 2,2 % 59,5 % 40,5 %
Publikování ponižující fotografie 4,2 % 62,7 % 37,3 %
Publikování ponižujícího videozáznamu 2,1 % 66,7 % 33,3 %
Publikování ponižujícího zvukového záznamu 1,5 % 66,7 % 33,3 %
n = 1925 (celkový počet respondentů)


Nebezpečí elektronické komunikace
Graf 6.1
Kyberšikana dětí (útočníci)
Výhrůžky nebo zastrašování (v SMS zprávách, e-mailech, diskuzi nebo chatu)
20 % 3,1 % 7,6 % 6,9 % 15 % 2,7 % 3,5 % 1,8 %
Vydírání (mobilním telefonem, v chatu nebo e-mailu)
7,7 % 1,2% 2,4 % 3,6 % 15 % 0,8 % 0,7 % 1 %
Nadávání, urážení, zesměšňování, ponižování (v SMS zprávách, e-mailech, diskuzi nebo chatu)
13,3 % 6,6 % 8,2 % 8,6 % 20 % 10,1 % 9,9 % 2,7 %
Nadávání, urážení, zesměšňování, ponižování (v blogu nebo jiné webové stránce)
13,3 % 2,3 % 4,1 % 5,2 % 15 % 2,3 % 2,8 % 1,8 %
věk 6-10 11-14 15-17 18+

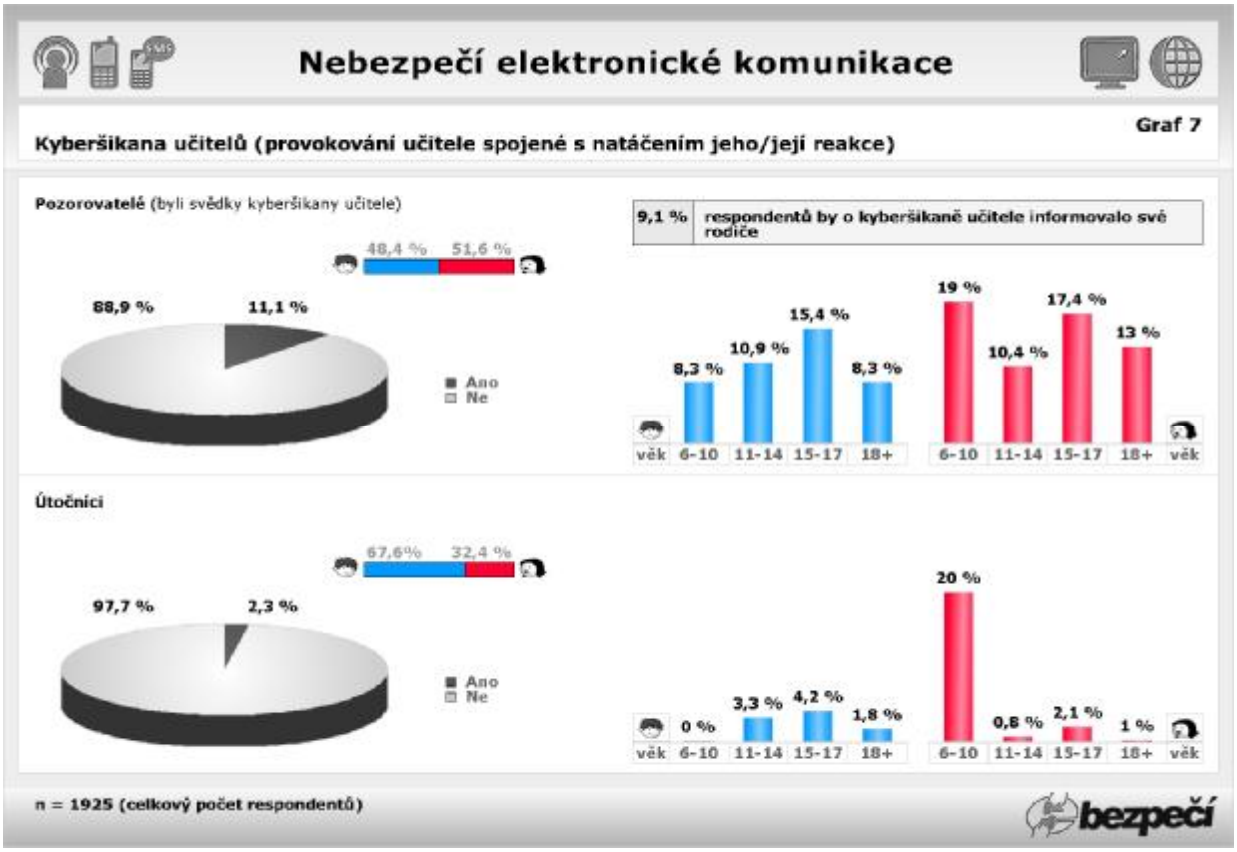

Nebezpečí elektronické komunikace
Graf 6.2
Kyberšikana děti (útočníci)
Krádež identity, zcizení účtu
(v e-mailu, chatu, diskuzi, vzdělávacím prostředí...)
0 %
13,1 %
23,5 %
17,2%
20 %
15,3 %
23,9 %
12,7%
věk 6-10 11-14 15-17 18+ 6-10 11-14 15-17 18+ věk
Zneužití cizího účtu
(v e-mailu, chatu, distuzi, vzdělávacím prostředí...)
0 %
2,3 %
4,1 %
5,2 %
15 %
1,7 %
0,7 %
1,8 %
věk 6-10 11-14 15-17 18+ 6-10 11-14 15-17 18+ věk
bezpečí


Nebezpečí elektronické komunikace
Graf 6.3
Kyberšikana děti (útočníci)
Publikování ponižující fotografie
(na internetu)
7,7 %
4,9 %
6,7 %
8,9 %
15 %
3,1 %
3,5 %
1 %
věk 6-10 11-14 15-17 18+ 6-10 11-14 15-17 18+ věk
Publikování ponižujícího zvukového záznamu
(na internetu)
0 %
2,6 %
1,2 %
1,8 %
15 %
0,4 %
0,7 %
1,9 %
věk 6-10 11-14 15-17 18+ 6-10 11-14 15-17 18+ věk
Publikování ponižujícího videozáznamu
(na internetu)
7,7 %
2,2 %
5,5 %
1,8 %
15 %
1,2 %
0,7 %
1 %
věk 6-10 11-14 15-17 18+ 6-10 11-14 15-17 18+ věk
bezpečí

Kyberšikana učitelů (útočníci a pozorovatelé)

Výzkumné šetření dále sledovalo, zda se žáci aktivně zapojují do kyberšikany učitelů, popř. zda byli svědky takového chování. Sledovaný projev kyberšikany měl podobu provokování učitele a následného nahrání vyhrocené situace.

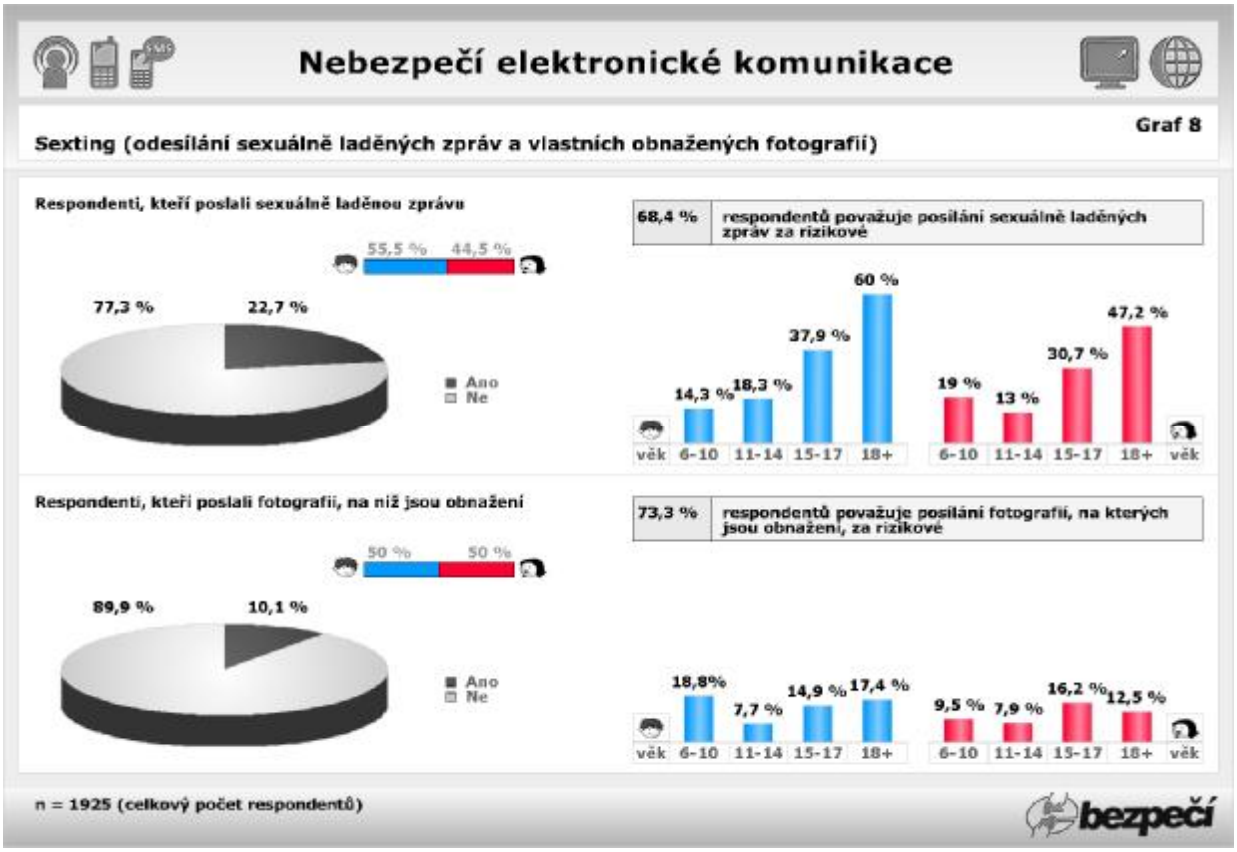
K útoku na učitele se přiznaly 2,3 % respondentů, přičemž téměř 2/3 útočníků byli chlapci (67,6 %). 11,1 % odpovídajících uvedlo, že bylo takovému chování přítomno. Pouze 9,1 % respondentů by o kyberšikaně učitele informovalo rodiče. Tuto skutečnost by s rodiči řešily především dívky (62,3 %). (***Graf 7***)



Sexting[3]

Sexting souvisí velmi úzce s kyberšikanou, neboť toto chování může být ke kyberšikaně zneužito. Výzkumné šetření se zaměřilo především na rozesílání sexuálně laděných SMS zpráv a fotografií. Sleduje, zda respondenti tyto typy elektronických zpráv rozesílají, a také zda takové chování považují za rizikové.

Z odpovědí vyplynulo, že respondenti posílají častěji textové zprávy (22,7 %) než fotografie (10,1 %). To odpovídá také jejich představě o potenciální nebezpečnosti takového chování – posílání sexuálně laděných SMS zpráv uvádí jako rizikové 68,4 % respondentů, zatímco posílání obnažených fotografií považuje za nebezpečné 73,3 % respondentů. (***Graf 8***)



[3] **Sexting** nebo **sextování** lze definovat jako odesílání sexuálně laděných zpráv, obnažených fotografií, videí apod. Tento termín vznikl spojení slov sex a textování.

Sdělování osobních údajů osobám, které respondenti znají pouze z internetu

Sdělování osobních údajů neznámým lidem je velmi rizikové, protože tyto citlivé údaje mohou být velmi snadno zneužitelné k různým patologickým komunikačním praktikám jako je např. kyberšikana (především vydírání), kybergrooming nebo kyberstalking.

Respondenti byli dotazováni na tyto konkrétní osobní údaje:

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

V rámci výzkumného šetření bylo také sledováno, zda se ochota sdělit osobní údaje neznámé osobě na internetu mění v závislosti na různých podmínkách (např. délka komunikace s neznámou osobou či sdělení osobního údaje za úplatu), neboť tyto skutečnosti žáky velmi ovlivňují v jejich rozhodování[6].

Respondenti nejčastěji sdělují křestní jméno (77,5 %), e-mailovou adresu (67,5 %) a kontaktní údaje IM nebo VoIP (66,6 %).

Při hodnocení jednotlivých osobních údajů je nutné zvážit jejich rozdílnou rizikovost 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. adresa bydliště – sděluje 23,5 % respondentů, adresa školy – 56,9 % respondentů),

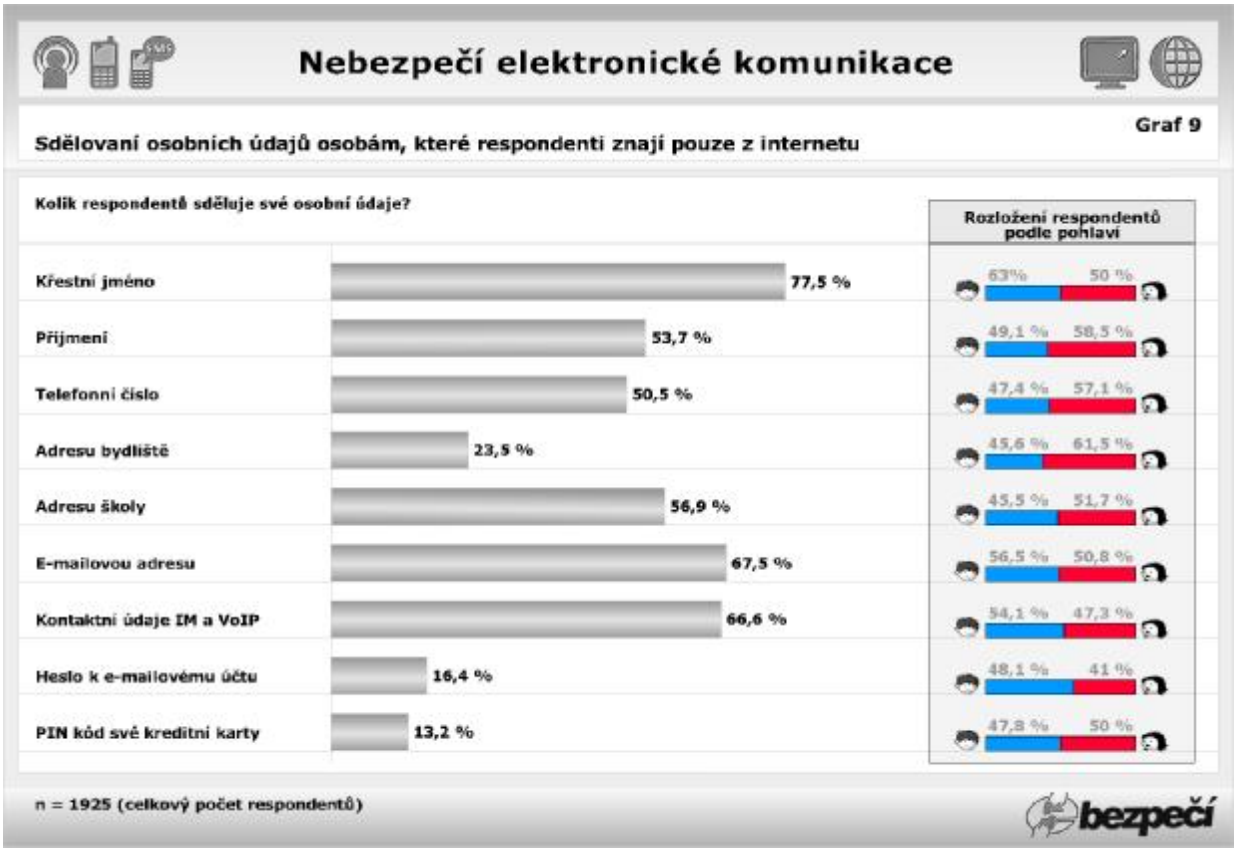
---

[4] **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).

[5] **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.

[6] *Výsledná procentuelní hodnota představuje nejvyšší naměřenou hodnotu pro konkrétní osobní údaj napříč všemi sledovanými podmínkami.*

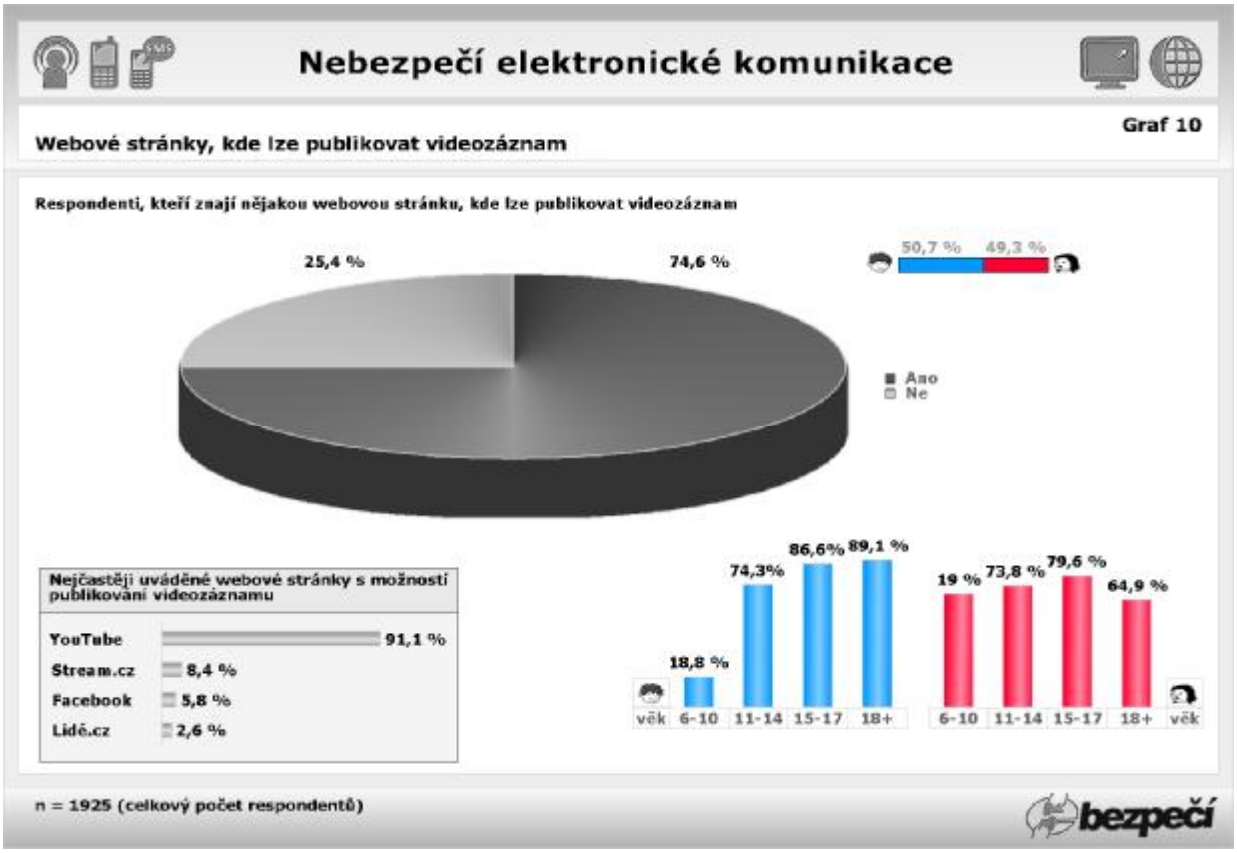
- údaje, které vytvoří mezi dítětem a útočníkem komunikační kanál (např. telefonní číslo – sděluje 50,5 % respondentů, e-mailová adresa – 67,5 %, adresa IM nebo VoIP – 66,6 %),
- údaje, které útočníkovi umožňují přístup k cizímu účtu (heslo k e-mailovému účtu – sděluje 16,4 %, PIN kód kreditní karty – 13,2 %). (***Graf 9***)



Webové stránky, kde lze publikovat videozáznam

Respondenti se měli vyjádřit také k tomu, zda znají webové stránky s možností publikování videozáznamu. Tuto skutečnost jsme zjišťovali především proto, že publikování zesměšňujících videozáznamů je jedním z projevů kyberšikany.

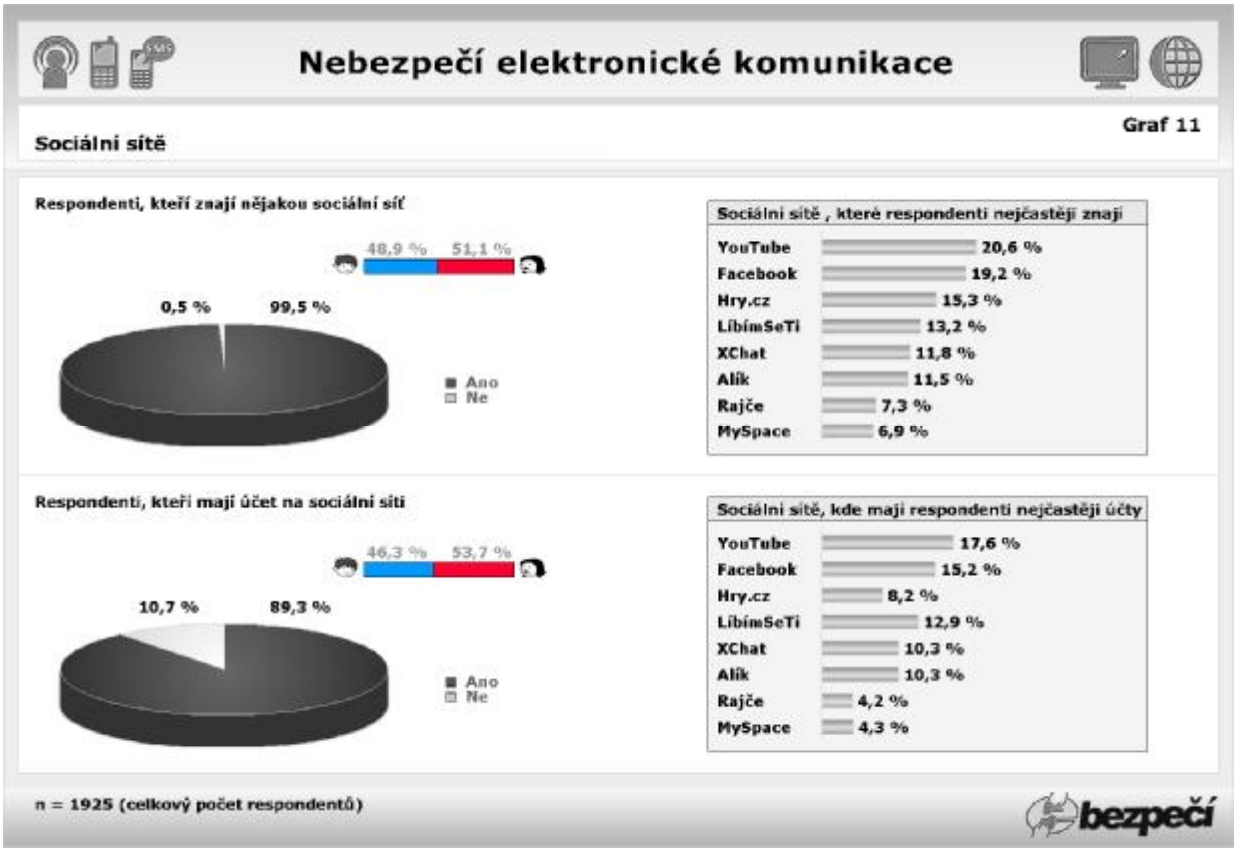
Téměř 3/4 (74,6 %) všech respondentů uvedlo, že takové webové stránky znají. Kromě osobních webových stránek (např. blog) jmenovali především portály YouTube (91,1 %), Stream.cz (8,4 %) nebo Facebook (5,8 %). (***Graf 10***)



Sociální sítě[7]

Sociální sítě v Evropě v současnosti využívá téměř 50 milionů uživatelů. Do roku 2012 se předpokládá, že počet uživatelů vzroste na 108 milionů. Kromě výhod ale sociální sítě pro uživatele představují četná 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 aj.

99,5 % oslovených respondentů uvedlo, že zná alespoň jednu sociální síť. K nejčastěji jmenovaným sociálním sítím patří např. YouTube (20,6 %), Facebook (19,2 %) nebo Hry.cz (15,3 %). 89,3 % respondentů má na některé ze sociálních sítí také svůj účet. I z tohoto pohledu byly nejčastěji zmiňovány portály YouTube (17,6 %) a Facebook (15,2 %). (***Graf 11***)

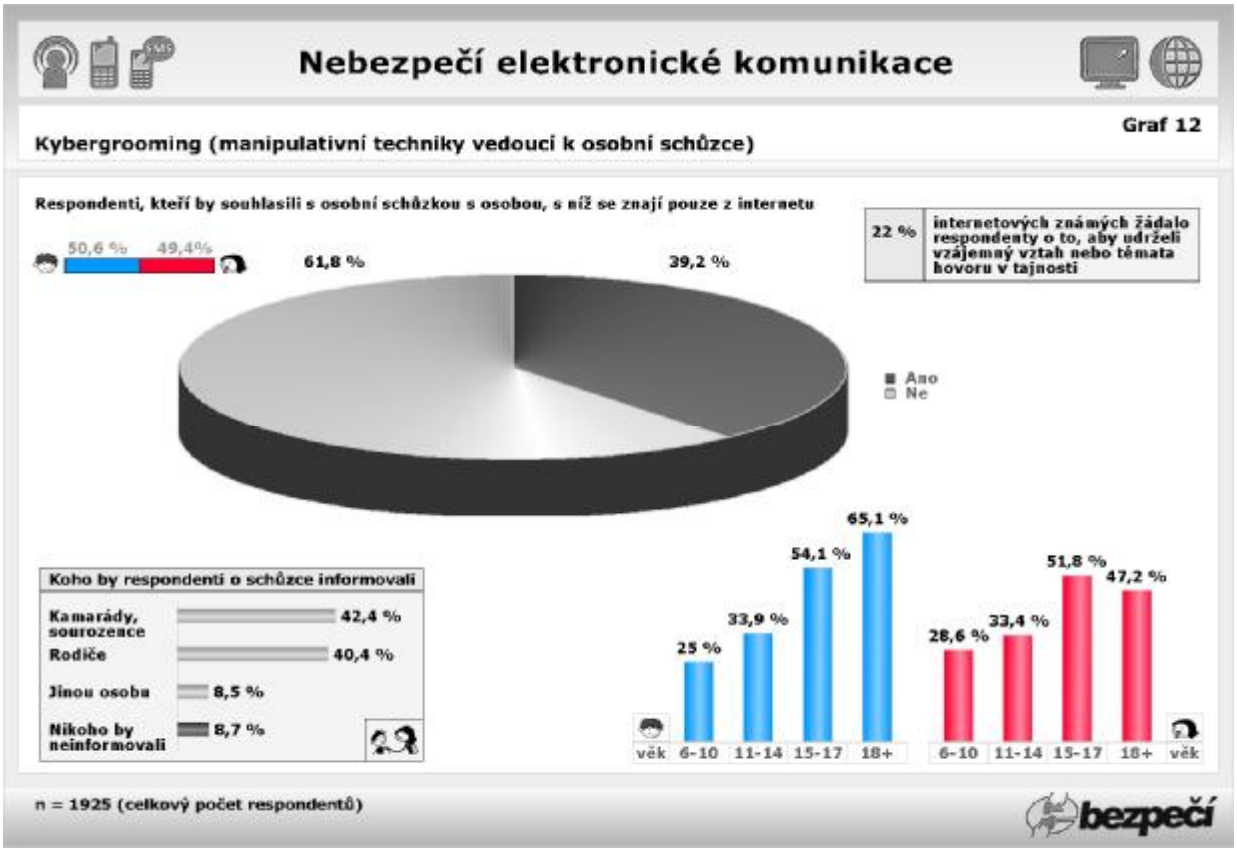


[7] **Sociální sítě** je označení pro informační sítě poskytované internetovými portály, které umožňují vytvářet virtuální společenství. Sociální sítě nabízejí prostor pro prezentaci lidí, komunikaci, navazování sociálních vztahů, vzdělávání, komerci (reklama, marketing, sociotechnika) nebo jakoukoli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

Kybergrooming[9]

39,2 % všech respondentů by souhlasilo s osobní schůzkou s osobou, se kterou se seznámili na internetu. O tom, že plánují schůzku s internetovým známým, by nejčastěji informovali své kamarády nebo sourozence (42,4 %). Rodičům by konání schůzky oznámilo pouze 40,4 % respondentů. 8,7 % dotazovaných by tuto skutečnost nesdělilo vůbec nikomu. Jedním ze signálů, který naznačuje, že se může jednat o rizikovou virtuální komunikaci, je snaha udržet takto navázaný vztah nebo témata hovoru v tajnosti. O splnění této podmínky byl svým internetovým známým požádán více než každý pátý respondent (22%). (***Graf 12***)



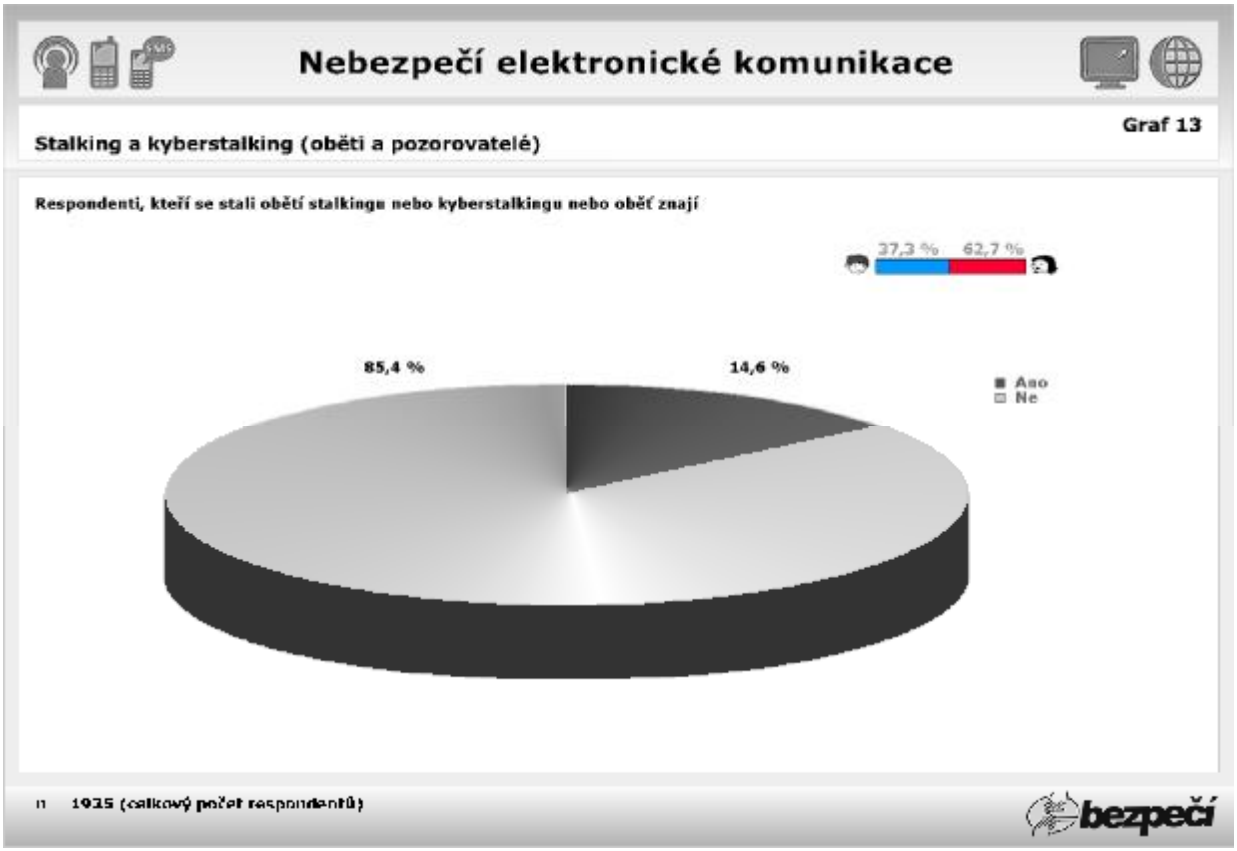
[9] **Kybergrooming** označuje manipulativní chování uživatelů internetu, které má v oběti vyvolat falešnou důvěru a připravit ji na schůzku, na které může dojít k sexuálnímu obtěžování, pohlavnímu zneužití, týrání nebo manipulaci oběti (např. nucení ke krádežím, terorismu aj.).

Stalking[10] a kyberstalking[11] (oběti a pozorovatelé)

V této části výzkumného šetření se měli respondenti vyjádřit k tomu, zde se oni sami nebo někdo z jejich známých ocitl v podobné situaci jako dívka z následujícího příkladu:

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

Podobnou zkušenost uvedlo 14,6 % respondentů. Na tomto výsledku se z více než 2/3 podílely dívky (62,7 % ze všech kladných odpovědí). (***Graf 13***)



[10] **Stalking** definujeme jako pronásledování, opakované stupňované obtěžování, které může mít různou podobu a intenzitu (např. snaha o kontakt, slídění, vyhrožování, vydírání, fyzické napadání apod.). V některých případech může dojít i k zavraždění oběti.

[11] **Kyberstalking** je druh stalkingu. Agresor ke svým útokům využívá především informační a komunikační technologie (mobilní telefony, internet atd.).

5. Shrnutí

Téměř polovina českých žáků je vystavena kyberšikaně (46,8 %). Čelí především dehonestujícím útokům, které mají podobu nadávání, urážení nebo ponižování realizované SMS zprávami, e-maily, v chatu nebo diskuzi (15,8 %). Přestože žáci se s kyberšikanou setkávají poměrně často, při řešení těchto problémů jen málo spoléhají na pomoc rodičů. Rodičům by se svěřila necelá 1/4 respondentů (22,9 %). S rodiči by žáci řešili hlavně vydírání.

Téměř každý třetí respondent přiznal, že si kyberšikanu vyzkoušel (27,8 %). Útoky byly nejčastěji realizovány přihlášením se k cizímu účtu (14,7 %).

2,3 % respondentů se aktivně zapojuje do kyberšikany učitele (konkrétně se jedná o provokování učitele a následného natočení vyhrocené situace). Tito útočníci jsou tvořeni ze 2/3 chlapci. Přibližně každý desátý žák (11,1 %) byl u kyberšikany učitele sám přítomen.

Z výzkumu vyplynulo, že asi 1/3 respondentů se věnuje sextingu. 22,7 % žáků odeslalo sexuálně laděnou zprávu a 10,1 % svou obnaženou fotografii. Přesto většina žáků považuje toto chování za rizikové. V případě sexuálně laděných zpráv to uvedlo 68,4 % respondentů a v případě fotografií 73,3 % respondentů.

Více než 2/3 dotazovaných (67,5 %) se vystavují rizikovému chování jaké představuje sdílení osobních údajů. 67,5 % sděluje e-mailovou adresu, 66,6 % kontaktní údaje IM nebo VoIP, 56,9 % adresu školy a 50,5 % telefonní číslo.

Téměř 3/4 všech respondentů (74,6 %) znají webové stránky umožňující publikovat videozáznam. Z nichž 91,1 % jmenovalo jako příklad stránky YouTube.

99,5 % žáků zná některou ze sociálních sítí. Mezi nejčastěji uváděnými se objevily portály YouTube (20,6 %), Facebook (19,2 %) a Hry.cz (15,3 %). **89,3 % respondentů má na některé ze sociálních sítí také svůj účet** (17,6 % na stránce YouTube, 15,2 % na Facebook)**.**

39,2 % dotazovaných žáků by souhlasila s osobní schůzkou s člověkem, s nímž se seznámila na internetu. O svém úmyslu na takovou schůzku jít by rodiče informovalo pouze 40,4 % respondentů. Častěji by se se svými plány svěřili kamarádům nebo spolužákům (42,4 %). 8,7 % by o schůzce neřeklo nikomu. Přitom více než každý pátý respondent (22 %) byl svým internetovým známým požádán o to, aby držel jejich vzájemný vztah nebo témata rozhovoru v tajnosti, což lze považovat za jeden z alarmujících signálů doprovázejících kybergrooming.

14,6 % žáků (z toho více než 2/3 dívek) má zkušenosti se stalkingem nebo kyberstalkingem z pozice oběti nebo známého oběti.

6. Kontakt

Realizátoři

Mgr. Veronika Krejčí

Projekt E-Bezpečí a Centrum PRVOK PdF Univerzity Palackého Olomouc

redakce@e-bezpeci.cz

+420 723 188 432

Mgr. Kamil Kopecký, Ph.D.

Projekt E-Bezpečí a Centrum PRVOK PdF Univerzity Palackého Olomouc

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

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