Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Ve spolupráci se Safer internet sociální sítě, bezpečnost dětí

Renáta Smutná

Vedoucí: RNDr. Dagmar Brechlerová, Ph.D.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Smutná Renáta

Hospodářská a kulturní studia

Název práce

Ve spolupráci se Safer internet sociální sítě, bezpečnost dětí

Anglický název

Social networks, collaboration with Safer Internet, security of children

---

Cíle práce

Bakalářská práce je zaměřená na problematiku v současné době velmi rozšířených sociálních sítí. Práce se zabývá především nebezpečím a hrozbami, které jsou s tímto fenoménem spojeny, a které si uživatelé často v plné míře neuvědomují. Zvláště se zaměřuje na dětské uživatele. Cílem práce je seznámit čtenáře s těmito riziky a ukázat možnosti prevence sociálně patologických jevů spojených s užíváním nových online technologií, které mohou vážně ohrozit zdravý psychický a sociální vývoj a bezpečnost dětí a mládeže.

Metodika

Teoretická část bakalářské práce vychází ze studia a analýzy dostupné odborné literatury, knižní i elektronické. Praktická část je založena na provedení a vyhodnocení dotazníkového šetření na vybraných základních školách.

Harmonogram zpracování

Studium odborných informačních zdrojů, stanovení dílčích cílů a postupu řešení: 06/2012
Zpracování přehledu řešené problematiky: 07/2012 – 08/2012
Vypracování vlastního řešení, diskuse, doporučení a závěry: 09/2012 - 02/2013
Tvorba finálního dokumentu práce: 02/2013 – 03/2013
Odevzdání práce a tezí: 03/2013

Rozsah textové části

40-50 stránek

Klíčová slova

Sociální síť, facebook, internet, děti, hrozby, kyberšikana, prevence, ochrana

Doporučené zdroje informací

KOLÁŘ, Michal. Nová cesta k léčbě šikany. 1. vyd. Praha : Portál, 2011. 332 s. ISBN 978-80-7367-871-5.

ROGERS, Vanessa. Kyberšikana. Portál, 2011. ISBN 978-80-7367-984-2.

WILLARD, Nancy E. Cyber Savvy. Sage Publications Inc, 2012. ISBN 9781412996211.

PATCHIN, J. W. & HINDUJA, S. (2012). Cyberbullying Prevention and Response: Expert Perspectives. New York: Routledge (ISBN: 978-0415892377).

PATCHIN, J. W. & HINDUJA, S. (2009). Bullying beyond the Schoolyard: Preventing and Responding to Cyberbullying. Thousand Oaks, CA: Sage Publications (ISBN: 978141296689).

NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. Brožura ke kampani Praha bezpečně online. Saferinternet.cz., 2011.

Metodické materiály Národního centra bezpečnějšího internetu

http://www.bezpecne-online.cz/

http://www.saferinternet.cz/

Studie EU Kids Online: Digitální gramotnost dětí

Vedoucí práce

Brechlerová Dagmar, RNDr., Ph.D.

Termín odevzdání

březen 2013

doc. Ing. Zdeněk Havlíček, CSc.
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

prof. Ing. Jan Hron, DrSc., dr.h.c.
Děkan fakulty

V Praze dne 15.1.2013

Čestné prohlášení

Tímto čestně prohlašuji, že jsem bakalářskou práci na téma „Ve spolupráci se Safer internet sociální sítě, bezpečnost dětí“ zpracovávala samostatně, pouze s použitím uvedené literatury, metod a zdrojů.

V Praze, dne 15. 03. 2013 ……

podpis

Poděkování

Ráda bych touto cestou poděkovala panu Ing. Jiřímu Palyzovi (řediteli Národního centra bezpečnějšího internetu) a RNDr. Dagmar Brechlerové Ph.D. za jejich cenné rady, důležité informace, pomoc a vedení, které mi pomohly při vypracování této bakalářské práce, dále Mgr. Janě Neudertové (ředitelce ZŠ Ratibořická) a Ing. Aleně Fremuntové (zástupkyni ředitelky školy a výchovné poradkyni) za umožnění a spolupráci při provedení průzkumné ankety a všem jejím respondentům.

Ve spolupráci se Safer internet sociální sítě, bezpečnost dětí

Social networks, collaboration with Safer internet, security of children

Souhrn

Bakalářská práce se zabývá sociálními sítěmi a nebezpečím, které na nich hrozí zejména dětským uživatelům. V teoretické části je definován pojem sociální síť a u vybraného zástupce (Facebook) je charakterizován vznik, původ, funkce a zabezpečení. Dále jsou přiblíženy základní cíle dětských uživatelů sociálních sítí a popsána rizika a hrozby (zneužití údajů, pornografie, násilí, kyberkriminalita apod.), se kterými uživatelé mohou přijít do styku. Práce také poukazuje na možnosti prevence a ochrany před těmito škodlivými vlivy. Praktická část potom zkoumá formou dotazníkového šetření aktuální situaci na českých základních školách.

Summary

The Bachelor´s thesis deals with social networks and risks threatening primarily to users among children. The theoretical part defines the concept of social network; one example (Facebook) is described in details – its formation, origin, function and security. Next, the basic objectives of child users of social networks are outlined and the risks and threats (abuse of data, pornography, violence, cybercrime, etc.) are described, which the users may face. The thesis deals with potential prevention and protection against detrimental effects of the networks. The practical part analyzes the current situation at Czech basic schools through a questionnaire survey.

Klíčová slova

Sociální sítě, Facebook, internet, děti, hrozby, kyberšikana, prevence, ochrana, bezpečnost

Keywords

Social networks, Facebook, internet, children, threats, cyberbullying, prevention, protection, safety

Obsah

Seznam obrázků a grafů

1. Úvod

Internet už se v dnešní době stal běžnou až nepostradatelnou součástí lidských životů. S jeho rozvojem vzniklo obrovské množství nových možností. Výrazným fenoménem současnosti se stávají Sociální sítě – ať už české (Lide.cz, Libimseti.cz či Spoluzaci.cz) nebo celosvětové (Facebook, Twitter, MySpace). Používají je až miliony, v případě Facebooku dokonce více než miliarda uživatelů a denně přibývají další. Díky nim už se geografická vzdálenost nepočítá za bariéru komunikace, naopak se otevírá cesta pro snadné navazování nových vztahů a přátelství. Tyto sítě usnadňují lidem život, přinášejí mnoho nových možností a přispívají ke sbližování a propojování světa. Co si však lidé uvědomují méně je, že s sebou přinášejí také velké množství různých rizik a nebezpečí. Málokterý účastník virtuálního světa (tím spíše dítě) si je vědom toho, že se nachází v neustálém ohrožení. Lidé jsou o těchto hrozbách všeobecně málo informovaní.

Podle Českého statistického úřadu[1] používá v České republice Facebook přibližně 3,5 milionů lidí, z toho asi 17 % tvoří uživatelé mladší 18 let. Tento údaj je ovšem značně spekulativní, protože prakticky neexistuje způsob, jak ověřit věk, který uživatel při registraci zadá. Studie EU Kids Online[2] z roku 2011 došla k závěru, že profil na Facebooku nebo na některé z dalších sociálních sítí má 52 % českých dětí ve věku od 9 do 12 let a ve věku od 13 do 16 let už dokonce 90 %. Při tom přibližně 66 % dětí smí tyto sítě využívat úplně bez omezení a bez dozoru a jen okolo 20 % je má od rodičů zakázané.

V první kapitole teoretické části je přiblíženo, co vlastně jsou sociální sítě. Jako zástupce byl vybrán Facebook, kterému podle již zmíněné studie EU Kids Online dává přednost 91 % českých dětí. Práce se proto na tento server zaměřuje detailněji než na ostatní a uvádí i jeho základní funkce a možnosti nastavení soukromí. Druhá kapitola se zabývá tím, proč jsou sociální sítě pro děti tolik atraktivní. V následující části jsou potom popsána různá nebezpečí, která zde dětským uživatelům hrozí a poslední kapitola je věnována tomu, jak děti účinně chránit a kde hledat potřebné informace.

[1] Zdroj: www.czso.cz (údaj z ledna 2012)
[2] Studii EU Kids Online pro Evropskou komisi vypracovala London School of Economics na vzorku 25 000 dětí a mladistvých v 25 zemích Evropské unie. (Z každé země bylo vybráno 1 000 respondentů.)

2. Cíl práce a metodika

2.1. Cíl práce

Bakalářská práce je zaměřena na problematiku v současné době velmi rozšířených sociálních sítí. Práce se zabývá především nebezpečím a hrozbami, které jsou s tímto fenoménem spojeny, a které si uživatelé často v plné míře neuvědomují. Zvláště se zaměřuje na dětské uživatele. Cílem práce je seznámit čtenáře s těmito riziky a ukázat možnosti prevence sociálně patologických jevů spojených s užíváním nových online technologií, které mohou vážně ohrozit zdravý psychický vývoj a bezpečnost dětí a mládeže.

2.2. Metodika

Teoretická část bakalářské práce vychází ze studia a analýzy dostupné odborné literatury, knižní i elektronické. Všechny zdroje jsou uváděny v jejich důsledné citaci v seznamu použité literatury na konci práce. Samotné zpracování teoretické části je doplněno o poznámky autora práce.

Praktická část je založena na provedení a vyhodnocení dotazníkového šetření na vybrané základní škole. Byl použit strukturovaný dotazník skládající se z 19 uzavřených nebo polootevřených otázek, který je v kompletním znění uveden v příloze. Výsledky byly zpracovány pomocí webového portálu Vyplň to.cz.

3. Co je sociální síť

Social networking, social network service – to jsou synonymní názvy pro pojem sociálních sítí. Podle slovníku internetových výrazů jsou sociální sítě definovány jako služby určené pro komunity lidí, kteří navzájem sdílí svá data ve virtuální síti. Tyto služby nabízejí různé možnosti interakce[3] mezi uživateli – například chaty[4], zprávy, e-maily, komentáře, diskusní skupiny apod. Obecným principem těchto sítí je možnost vytvoření vlastního profilu. Jednotliví uživatelé si přidávají ostatní uživatele mezi přátele a poté spolu komunikují.[1]

Původně byly sociální sítě určeny k setkávání lidí, diskusím a chatování. Později s rozvojem moderních technologií se začaly používat také ke sdílení multimédií. Sociální sítě se staly prostředkem k používání jiných služeb a staly se významným nástrojem k seznámení a udržování vzájemných vazeb.

Existuje mnoho typů sociálních sítí. Některé vznikají na základě rodinných vazeb, kamarádů, témat, jiné se zaměřují na seznámení.

Mezi významné české sociální sítě patří **Lide.cz** - síť, která je jasně profilována jako rychlá a anonymní seznamka a **Spoluzaci.cz**, která udržuje vazby se současnými i minulými spolužáky. Ze zahraničních sítí tvoří významnou roli **Facebook**, **Twitter** nebo **MySpace**. Používání více sociálních sítí se nevylučuje, naopak je v poslední době aktuálním trendem. [2]

3.1. Facebook

Facebook je v dnešní době jedním z nejznámějších a nejpoužívanějších společenských webových systémů na světě. Je plně přeložen do 68 jazyků. Slouží ke

[3] Interakce je vzájemné působení dvou nebo více činitelů. (Zdroj: ABZ.cz: slovník cizích slov: Interakce. [online]. [cit. 2013-01-29]. Dostupné z: http://slovnik-cizich-slov.abz.cz/web.php/hledat?typ_hledani=prefix&cizi_slovo=interakce)

[4] Chat je komunikace dvou nebo více lidí najednou prostřednictvím komunikační sítě. (Zdroj: ABZ.cz: slovník cizích slov: Chat. [online]. [cit. 2013-01-29]. Dostupné z: http://slovnik-cizich-slov.abz.cz/web.php/hledat?typ_hledani=prefix&cizi_slovo=chat)

komunikaci mezi uživateli, sdílení multimediálních dat, udržování vztahů a k zábavě. Umožňuje udržovat kontakt s přáteli i na velkou vzdálenost a seznámit se s novými lidmi z celého světa, sdílet fotografie, videa či jiné zajímavé články. [3]

Facebook byl založen v roce 2004 Markem Zuckerbergem a sloužil původně pouze pro studenty Harwardovy univerzity. Později se postupně rozšířil i na některé další univerzity patřící do tzv. Ivy League[5]. Nakonec byl přístup otevřen pro všechny uživatele s univerzitní e-mailovou adresou a pro některé schválené zahraniční univerzity (v České republice byla první Masarykova univerzita). Od února 2006 se začaly do systému připojovat i některé nadnárodní společnosti a od srpna téhož roku se může podle licence používání připojit kdokoliv starší 13 let. [4]

V současné době má Facebook více než miliardu uživatelů[6] a z nich 584 milionů[7] je denně aktivních. [5]

3.1.1. Funkce Facebooku

Každý uživatel si musí nejprve založit svůj profil se základními údaji. Registrace je bezplatná a většinou vázaná na e-mailovou adresu. Po přihlášení je možné vyhledat přátele například podle jména nebo e-mailové adresy.

Uživatelé mají v profilu tzv. **Zeď** – anglicky **Wall** (viz obrázek 1), na kterou vkládají statusy[8], ostatní uživatelé sem mohou psát vzkazy a zobrazují se zde v podstatě všechny děje v sociální síti. Na Zeď se dá vkládat i další multimediální obsah, nahrávat fotografie nebo odkazovat na zajímavý web a ten sdílet s ostatními přáteli. U každého příspěvku na zdi je možné nastavit, komu se bude zobrazovat. Ostatní uživatelé mohou

[5] Ivy League (česky Břečťanová liga) je název pro sportovní sdružení osmi nejprestižnějších soukromých univerzit na severovýchodě USA. Patří sem Brownova univerzita, Kolumbijská univerzita, Cornellova univerzita, Dartmouth, Harward, Pensylvánská univerzita, Princeton a Yale. (Zdroj: College admissions: Ivy League Schools. [online]. [cit. 2013-01-29]. Dostupné z: http://collegeapps.about.com/od/choosingacollege/tp/ivy-league-schools.htm)
[6] Údaj z října 2012
[7] Údaj ze září 2012
[8] Status (nebo stavová zpráva) je informace o aktuálním stavu, náladě, názorech nebo novinkách, kterou uživatel vkládá na svou Zeď.

příspěvek ohodnotit tlačítkem **„Líbí se mi“** (anglicky **„Like“**), a tím dát autorovi najevo, že s ním souhlasí nebo, že se jim daná fotografie či video líbí.

Obrázek 1: Zeď (wall)

Zdroj: www.facebook.com

Další z funkcí Facebooku jsou **Události**, sloužící jako prostředek k domluvení schůzky, srazu, oslavy narozenin nebo oznámení jakékoliv jiné události. V rámci události lze nastavit její předmět, místo a čas konání, bližší popis akce, přidat fotky, odkazy či videa, pozvat přátele a sledovat, kolik z nich se události zúčastní a kdo se z akce předem omluvil. Tím pádem není potřeba posílat zvlášť každému z přátel pozvánku nebo všem volat. Když se termín akce přiblíží, systém dokonce pozvaným uživatelům událost na hlavní stránce připomíná. [6]

Jednou z předností Facebooku je **pokročilé sdílení fotografií**. Uživatelé mohou neomezeně nahrávat fotografie, které lze jednoduše třídit ve fotoalbech. Ostatní uživatelé, kteří mají fotografie zpřístupněné, je mohou komentovat. Oblíbenou funkcí Facebooku je označování (tagging) přátel na snímcích, kdy je nejen snadno rozpoznatelné, kde a kdo se na obrázku nachází, ale zároveň se takto označeným uživatelům přidá fotografie do jejich profilu.

Výhodou je také **jednotný a čistý vzhled**. Služby jako Lide.cz nebo MySpace umožnily svým uživatelům částečně měnit vzhled svých profilů, čímž v některých

případech vznikají značně nepřehledné a kýčovité výtvory. Zachování jednotného designu webu zaručuje přehlednost, jednoduchou a efektivnější orientaci na jednotlivých stránkách.

Facebook je propojen s dalšími významnými internetovými službami, jako jsou například YouTube[9], Last.fm[10] nebo Flickr[11]. Tím se stává praktickým centrem informací z více zdrojů.

K profilu lze přistupovat také z mobilních zařízení – telefonů, smartphonů či tabletů pomocí optimalizované webové stránky m.facebook.com, případně pohodlněji ze specializovaných aplikací pro jednotlivé mobilní platformy. To může rodičům ještě více znesnadnit kontrolu nad aktivitami dětí na této síti. V současnosti patří Facebook mezi nejvyužívanější mobilní služby na světě. [7]

Facebook nabízí uživatelům také velké množství her a aplikací.

3.1.2. Nastavení soukromí

Jednou z výhod Facebooku v jeho současné podobě je oproti ostatním sítím možnost **ochrany soukromí**. Každý uživatel si může volitelně upravovat, kolik informací o sobě zveřejní. Do uživatelského profilu může nahlédnout jen ten, komu to majitel profilu dovolil - tj. zařadil si ho mezi své přátele. Navíc přátele lze rozdělit do skupin a jednotlivým skupinám je možné přiřadit (omezit) práva na přístup ke konkrétním údajům nebo souborům - např. lidé z práce nemusí vidět fotky z posledního večírku. [7]

Ne každý uživatel ovšem tuto možnost využívá, buď z důvodu, že o ní ani neví nebo si neuvědomuje závažnost této problematiky. Zvláště u profilů dětských uživatelů by mělo být za pomoci jejich rodičů soukromí pečlivě nastaveno a chráněno.

Sdílení na Facebooku je základním nastavením uživatelského soukromí. Slouží konkrétně k nastavení zobrazení informací a obsahu, který je uveřejněn pro ostatní

[9] YouTube je internetový server pro sdílení video souborů.
[10] Last.fm je internetový server zaměřený na hudbu.
[11] Flickr je komunitní web pro sdílení fotografií.

uživatele, a také zobrazení kontaktních a osobních údajů uživatele. Sdílení má několik předdefinovaných možností nastavení nebo lze upravit přesně podle požadavků konkrétní osoby.

Přednastavené možnosti jsou:

- **Veřejný** - informace se zobrazí všem uživatelům Facebooku
- **Pouze přátelé** - informace se zobrazí pouze uživatelům Facebooku, které má osoba v seznamu přátel
- **Přátelé přátel** - informace se zobrazí pouze uživatelům Facebooku, které má osoba v seznamu přátel a uživatelům, kteří jsou přáteli přátel této osoby
- **Pouze já** – informace nevidí nikdo jiný než sám uživatel

Pokud uživatel zvolí **vlastní nastavení**, může u každého příspěvku nastavit konkrétně, pro které uživatele nebo seznamy uživatelů[12] má být obsah viditelný, a pro které uživatele nebo seznamy uživatelů má zůstat skryt. [6]

Nastavení soukromí se netýká pouze vloženého obsahu a osobních údajů. Uživatel může podobným způsobem (jak je zřetelně vidět na obrázku 2) rozhodnout také o tom, kdo je oprávněn jej vyhledat, požádat o přátelství, posílat mu zprávy nebo vkládat komentáře na jeho zeď.

Obrázek 2: Nastavení soukromí

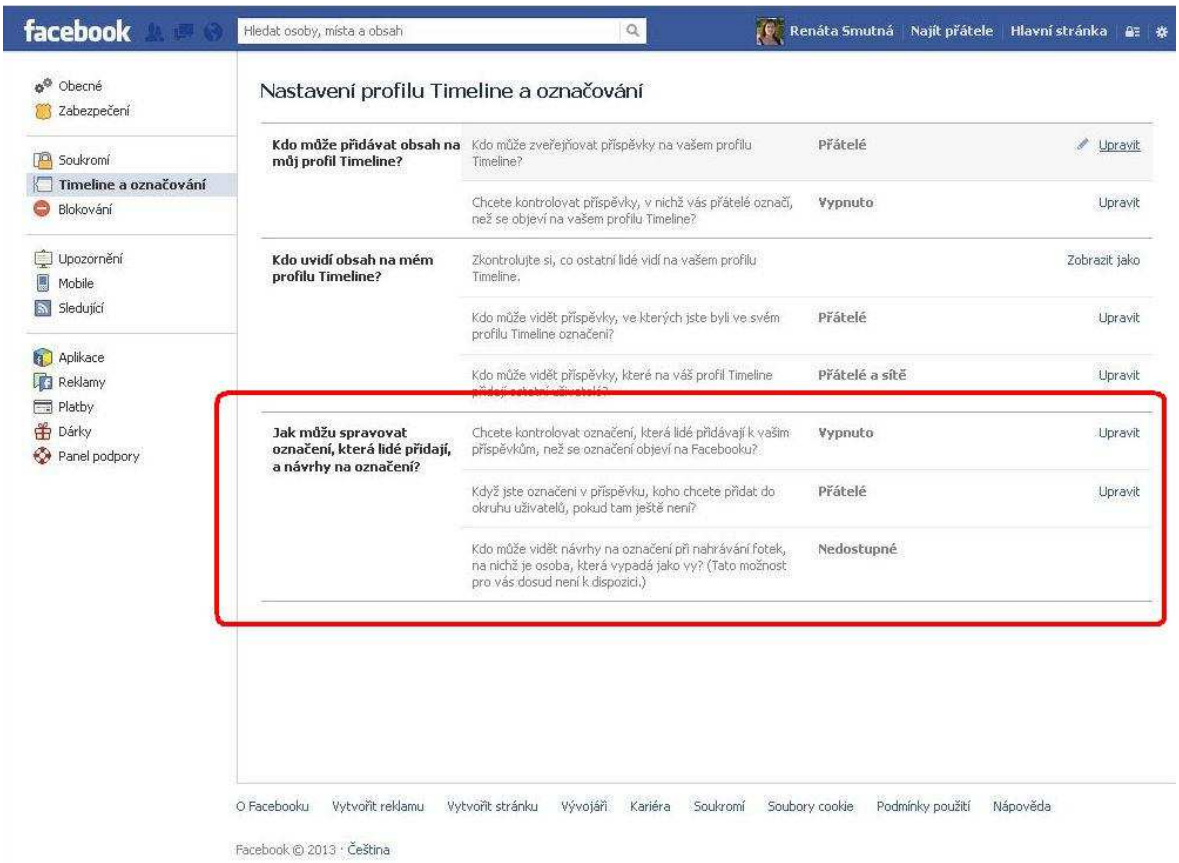
Zdroj: www.facebook.com

[12] Seznam uživatelů je další z funkcí Facebooku. Umožňuje rozdělit přátele do skupin podle libovolných kritérií (například rodina, blízcí přátelé, známí, spolužáci ze školy, přátelé, kteří bydlí ve stejném městě jako já apod.).

3.1.3. Označování (štítkování, tagging)

Uživatelé mohou na fotografiích, které do systému nahrají, ve stavových zprávách a komentářích označovat ostatní uživatele jmény, aniž by je museli žádat o souhlas. Z hlediska soukromí jde o druh informací, které jsou snadno zneužitelné, ať už za účelem žertu nebo přímo poškození osoby například kompromitujícími fotografiemi. Nicméně i toto lze v rámci nastavení soukromí změnit. Nelze kompletně zamezit jakémukoliv označování, ale lze v nastavení profilu zapnout funkci, díky níž bude každé označení muset být nejprve schváleno uživatelem a až poté se na jeho profilu zobrazí. Toto nastavení je názorně vidět na obrázku 3.

Obrázek 3: Nastavení označování



Zdroj: www.facebook.com

4. Proč jsou sociální sítě pro děti atraktivní

Nejatraktivnější vlastností sociálních sítí je především obrovské množství možností, které nabízí. Facebook dokáže usnadnit život, ušetřit čas a postarat se o zábavu na celé hodiny. Ale tak jako každá mince má dvě strany i používání facebooku má své stinné stránky, a co začalo z ryze praktických důvodů za účelem snadné a rychlé komunikace, se může proměnit v závislost a likvidátor veškerého volného času.

4.1. Komunikace

Hlavní náplní sociálních sítí je vzájemná komunikace mezi uživateli. Mohou spolu komunikovat i na velkou vzdálenost, aniž by se museli fyzicky sejít. Pro mnoho dětí (a samozřejmě nejen dětí, ale často i dospělých lidí) je kontakt s ostatními lidmi na Facebooku snazší a pohodlnější než v reálném životě. Zatímco například ve škole by se chlapec možná styděl oslovit nějakou dívku, na Facebooku snadno naváže rozhovor například tím, že okomentuje nějaký její příspěvek. Navíc pohodlí domova, vzdálenost a delší čas na reakci dokáže podstatně zmírnit trapný pocit z případného odmítnutí. Eventuelně může vyjadřovat své názory a pocity anonymně nebo pod cizím jménem, tudíž nemůže být s nimi později osobně konfrontován.

4.2. Přátelství

Sociální sítě podstatně usnadňují nalézání nových přátelství a jejich následné udržování. Dítě může být v kontaktu se svými kamarády i v době, kdy nemá dovoleno nebo z nějakého důvodu nemůže jít ven a skutečně s nimi trávit čas. Pomocí Facebooku je stále v obraze o tom, co kamarádi dělají a co je u nich nového, i když některé z nich už delší dobu nevidělo. Člověk získá během okamžiku pouhým pohledem na něčí profil o dané osobě množství informací, které může libovolně využít (či zneužít).

Hledání nových přátel na sociálních sítích je však velmi rizikové. Nikdy nemáme jistotu o tom, zda člověka, kterého považujeme za přítele, skutečně známe a nakolik je k nám upřímný. Navíc význam slova přátelství se s věkem člověka mění. Malé děti jím

nechápou totéž, co starší děti či dospělí lidé. Děti lehce někoho prohlásí za svého kamaráda a stejně snadno na něj zapomenou. Pro malé dítě je kamarádem každý, kdo je ochotný se s ním podělit o hračku. Pro školní děti je kritériem, kdo si s nimi příjemně popovídá - proto mohou mít „kamarádů“ celé stovky. Zacházejí se slovem kamarád stejně volně jako například angličtina, která slovo „friend“ používá ve smyslu přítel i známý. Ale jen zlomek z nich doopravdy dobře znají. Naopak některé z nich ve skutečnosti nemusejí znát vůbec tak dobře, jak si myslí. Teprve postupem času se přátelství začíná podobně jako manželství chápat jako pevnější svazek, který trvá delší dobu a je schopen překonat i nějaké neshody a překážky. [8]

4.3. Hry a Aplikace

Dalším poměrně atraktivním lákadlem Facebooku je nepřeberné množství aplikací a her. Většina her je navržena tak, že vyžadují spolupráci s ostatními uživateli. V opačném případě buď úplně postrádají smysl, nebo jsou některé jejich funkce značně omezené. Hráč může průběžně zobrazovat na svém profilu své pokroky a úspěchy a soutěžit s přáteli v tom, kdo dosáhne lepšího výsledku. Výběr dostupných her je skutečně rozmanitý. Jsou zde hry různých kategorií – logické, strategické, karetní, postřehové. Nejčastějším typem her jsou tzv. simulační hry. Jejich smyslem je spravovat například virtuální farmu, akvárium, ostrov, cukrárnu či psí útulek nebo pečovat o nějaké zvířátko, které si uživatel na začátku sám vytvoří.

Jedním z principů většiny her jsou dvojí platidla. První druh peněz (nazývaný většinou coin, dolary, apod.) si hráč klasicky vydělává plněním zadaných úkolů a postupem ve hře a poté za ně nakupuje běžné zboží a služby. Druhý druh peněz (nazývaný cash nebo například zlaťáky), za které se dá pořídit různé luxusní a nadstandardní zboží a některé speciální funkce, však lze většinou získat pouze nákupem za skutečné peníze. Hráč většinou na začátku hry malý obnos těchto (například) zlaťáků automaticky obdrží, aby si mohl vyzkoušet výhody s nimi spojené a byl více motivován pořídit si další. Děti tudíž naprosto nesmyslně utrácejí své kapesné a kredit z mobilního telefonu za lepší skóre v bezduchých počítačových hrách.

Za pravidelné přihlašování se během více po sobě jdoucích dní získává hráč bonusy, čímž se tvůrci her snaží uživatele podnítit ke každodenní aktivitě.

5. Rizika a Hrozby

Internet je nepochybně síť obrovských možností a příležitostí. Je to ale také síť hrozeb a nebezpečí. Na uživatele internetu číhají mnohá různá nebezpečí. V případě dětí se tato rizika ještě znásobují a nabírají mnohem větších rozměrů. Především proto, že děti jsou zranitelnější, citlivější, důvěřivější a snadněji manipulovatelné a většinou nedokážou riziko včas rozpoznat.

Nelze s přesností vytvořit žebříček závažnosti těchto hrozeb, ta je u konkrétních osob značně individuální. Potenciální nebezpečí hrozící uživatelům jsou pro všechny stejná, rozdíl však spočívá v tom, nakolik si konkrétní uživatel riziko uvědomuje a jak je schopný se s ním vyrovnat.

5.1. Neověřitelnost údajů

Ve světě sociálních sítí (stejně jako obecně na internetu) není žádný způsob ověření pravdivosti údajů. Anonymita, kterou internet poskytuje, vyloženě svádí k tomu, uvádět nepravdivé údaje. Důvod může být různý. Někteří lidé se takto snaží chránit své soukromí, jiní se chtějí udělat jen o něco lepšími a další za účelem někoho oklamat. Každý se může vydávat, za koho chce a neexistuje žádný naprosto spolehlivý způsob, jak nám předkládané údaje ověřit.

Pokud se bude padesátiletý muž vydávat za patnáctiletou dívku, průměrně inteligentní a zdravě podezíravý dospělý člověk má reálnou šanci, ať už hned nebo po určitém čase, stráveném komunikací s takovou osobou, podvod odhalit. U dítěte se ovšem tato šance rapidně snižuje. Snadno tak narazí na nebezpečného pedofila, který ho může sexuálně zneužívat. I takovým lidem přináší internet nové možnosti. Dnes už pedofil nemusí nutně na dítě čekat u školy nebo v parku, číhá na něj na Facebooku, kde je nesmírně snadné navázat kontakt. Poté, co získá důvěru dítěte, začne mu posílat sexuálně laděné zprávy a požadovat lechtivé, často až pornografické fotografie nebo svlékání před webovou kamerou. Vyhrožováním a zastrašováním jej nutí zacházet dál a dál a zároveň vše udržovat před rodiči a okolím v tajnosti. Pravděpodobně nejhorším možným scénářem

je, když se ho (třeba i pomocí falešné fotografie sympatické dívky) pokusí nalákat na osobní setkání. Pokud dítě ke schůzce svolí, ocitá se v životním nebezpečí. Zneužívání dítěte způsobuje vážné, někdy i trvalé a nenávratné následky na jeho psychickém vývoji, které mohou vést až k sebepoškozování nebo dokonce sebevraždě.

Část viny potom nesou také rodiče, kteří své dítě většinou poučí o možných rizikách, než jej pustí samotné ven, ale o tom, že naprosto stejné nebezpečí hrozí i na Facebooku, už méně často. Nezřídka kdy proto, že o tom sami nemají ani tušení, protože sociální sítě nepoužívají a neznají. Mnozí rodiče si myslí, že dokud je jejich potomek zavřený doma ve svém pokoji, žádné nebezpečí mu nehrozí. To snad možná platilo kdysi, před vznikem internetu, ale dnes už rozhodně ne.

Internetový server facemag.cz prohlašuje, že Facebook disponuje poměrně sofistikovanou technologií, která umožňuje proskenovat miliony zpráv a detekovat mezi nimi ty, které jsou nějakým způsobem podezřelé. Ty pak nahlásí týmu, který má na starost bezpečnost sociálních sítí. Pokud pracovníci vyhodnotí zprávy jako nevhodné a nebezpečné, nahlásí je na policii. Zůstává však otázka, nakolik je tato technologie spolehlivá a nakolik jsou pak soukromé zprávy soukromé. [9]

5.2. Citlivost údajů

Dalším velkým problémem sociálních sítí je vkládání velkého množství citlivých údajů. Sociální sítě jsou vhodným prostorem pro sběr osobních údajů, se kterými mohou útočníci nadále pracovat, jak sami uznají za vhodné. Osobní údaje představují cennou hodnotu, a proto by si je měl každý člověk pečlivě chránit. Tím spíše v současné době, kdy se internet rozšířil do běžných domácností a stal se téměř neoddělitelnou součástí lidských životů. Je nutné, aby si každý jedinec uvědomil, že většině zneužití se dá předejít tím, že bude s informacemi nakládat opatrněji a nebude je bez rozmyslu šířit do svého okolí. Je důležité, aby lidé sebe i své děti vzdělávali v problematice bezpečnosti na internetu. [10]

Je nutné nejprve vysvětlit, co pojem osobní údaj přesně znamená. § 4 zákona o ochraně osobních údajů č. 101/2000 Sb. jej definuje jako: „jakoukoliv informaci týkající se

určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“ Jedná se tedy o každý údaj, který je ve vztahu s nějakou fyzickou osobou a platí, že může-li být osoba z těchto údajů přímo nebo nepřímo identifikována, jedná se o osobní údaj. Patří sem údaje identifikační (například jméno a příjmení, adresa, datum narození a rodné číslo), údaje kontaktní (telefonní číslo nebo e-mailová adresa) a údaje popisné (například počet dětí, výška a váha, národnost, rasová příslušnost, vlastnictví vybraných movitých i nemovitých věcí nebo bankovní spojení). [11]

V reálném světě jsou lidé zdrženlivější a opatrnější. Cizím lidem na potkání neprozrazují své osobní informace. Ve virtuálním světě tato přirozená nedůvěra, která člověka ochraňuje, často mizí. Člověk je na internetu o svém skutečném životě ochoten prozradit mnohem více, než by prozradil cizímu člověku tváří v tvář a neuvědomuje si, že to sděluje obrovskému počtu cizích lidí najednou. [10]

Pro děti to platí tím spíše. Děti si na svém profilu bez rozmyslu kompletně vyplní veškeré identifikační a kontaktní údaje a pravidelně ve svých příspěvcích přidávají další a další zneužitelné osobní údaje. Vkládají fotografie (někdy až poměrně odvážné), které mohou skončit v rukou nebezpečných pedofilů. Vyzrazují své koníčky, probírají rodinné záležitosti, pomlouvají učitele, aniž by pomyslely na to, že se může stát, že si daný pedagog inkriminovaný příspěvek přečte a vyvodí z něj patřičné důsledky. Jen málokdo by si na dveře svého domu či bytu pověsil ceduli říkající: „Všichni jsme odjeli na dva týdny k moři, doma nikdo není.“, na Facebooku se však s odjezdem na prázdniny do zahraničí pochlubí mnozí. Pro potenciálního lupiče je výsledný obsah takového sdělení srovnatelný s cedulí na dveřích, zvlášť pokud adresu jednoduše najde v profilu uživatele, už mu nic nestojí v cestě.

Děti (a často i dospělí lidé) také vůbec neberou na vědomí, že starší příspěvky na síti zůstávají, a i když oni už je na svém profilu dávno nevidí, ve skutečnosti se nemažou ani neztrácejí. Tím se ze sociálních sítí stává obrovské shromaždiště osobních informací.

Jediným možným východiskem z této situace je pečlivější dohled rodičů. Rodiče by se měli lépe informovat a více zajímat o to, jaké nebezpečí jejich dětem na internetu hrozí, a poté na základě zvážení zralosti dítěte rozhodnout, zda je vhodné mu sociální sítě dovolit používat. V případě vytrvalého odmítání ovšem stoupá riziko, že si dítě profil stejně založí, a to tajně za jejich zády. Pokud rodič svému potomkovi souhlas udělí, měl by dítě náležitě poučit, pomoct s registrací a dohlédnout na všechny vkládané údaje a nastavení soukromí. Také by se obě strany měly dohodnout na pravidelných kontrolách vkládaného a sdíleného obsahu, případně také historie zpráv a na naprosté upřímnosti ze strany dítěte.

5.3. Nevhodný obsah

Na sociálních sítích (a na internetu vůbec) se děti nezřídka kdy setkají s materiálem, který je pro ně nevhodný. Snadno přijdou do styku s internetovými stránkami zahrnujícími pornografii, násilí, rasismus, extrémistický obsah, drogy nebo například tzv. „Pro-ana“ a „Pro-mia“ blogy, podporující chorobné hubnutí (anorexie[13], bulimie[14]).

Z průzkumu[15], který si ve 14 zemích světa zadala softwarová firma Symantec, vyplývá, že se téměř dvě třetiny dětí setkaly na internetu s něčím negativním. Šlo o vstup na stránky s nevhodným obsahem, pokus cizího člověka kontaktovat je pomocí sociální sítě, nebo dokonce pozvání na setkání s cizincem v reálném světě. Z průzkumu dále vyplývá, že jen asi polovina rodičů přikládá dostatečnou váhu internetovým zkušenostem svých dětí. Zajímavým zjištěním uvedeného výzkumu je fakt, že děti chtějí, aby se rodiče více zapojili do jejich online aktivit. [12]

[13] Mentální anorexie je nemoc, která spočívá v poruše přijímání potravy. Vyznačuje se odmítáním jídla a touhou po co nejštíhlejším těle.
[14] Bulimie je nemoc, která spočívá v poruše přijímání potravy. Vyznačuje se záchvatovitým přejídáním a následným úmyslným zvracením, někdy také vyvoláváním průjmů.
[15] Výzkum zpracovala pro Symantec mezinárodní společnost StrategyOne v únoru 2010. Dotazovány byly téměř 3000 dětí a více než 7000 dospělých ve 14 zemích světa. Česká republika se výzkumu nezúčastnila.

5.3.1. Pornografie

Pornografie je ve vztahu k dětem a mládeži obecně považována za nevhodnou. Už v dětském věku se vytvářejí základy sexuálních pocitů a postojů, které ovlivňují budoucí milostný život každého člověka. Existují různé výzkumné práce, které dokážou vystopovat vznik některých sexuálních deviací až do velmi raného věku. Vznik nových informačních kanálů a zdokonalování informačních technologií přináší výrazné obavy z předčasné erotizace mládeže. Dnešní mládež dostává ve srovnání s předchozí generací mnohem více sexuálních informací, bohužel však také více desinformací.

Obecně prezentace materiálů zobrazujících zdravý sex v míře adekvátní k mentální vyzrálosti dítěte není podle sexuologa MUDr. Radima Uzla, CSc. pro děti ohrožující. Naopak přispívá k vytváření sexuálního zdraví. Jejich bezpodmínečné odmítání a zakazování a tím potlačování normální dětské zvídavosti považuje za nepřirozené a nezdravé. Problém se týká především zobrazování sexu deviantního, sexu obsahujícího násilí apod., který může u dětí způsobit zkreslené představy, emoční trauma nebo dokonce (jak už bylo dříve zmíněno) vznik sexuálních deviací. [13]

5.3.2. Extrémistický a agresivní obsah

Výše uvedená pornografie však není jediným druhem nevhodného obsahu, s nímž se děti na internetu setkávají. Počítačové hry, sociální sítě a v podstatě celý internet, stejně tak jako třeba televize jsou protkány násilím a brutalitou. Na internetu se mohou setkat s různými názorově vyhrocenými weby – kromě politických (jako jsou nacismus a neonacismus, bolševismus nebo anarchismus) také s extrémními náboženskými ideologiemi nebo s hnutím propagujícím anorexii a bulimii. Extrémisté rozšiřují svá stanoviska různými cestami. Kromě klasických webových stránek píší osobní blogy, zakládají diskuse apod. Cílem těchto hnutí není jen propagace názorů, ale též nábor nových členů. Největší problém přichází v období, kdy si mladí lidé začínají hledat svou identitu a vymezují se vůči okolí. V této době se mohou nechat těmito radikálními názory snadno ovlivnit.

Násilného obsahu je na světové síti přehršel a ani se nemusí týkat extrémistických webů, i když s nimi bývá často spojován. Vědci se už dlouho zaobírají otázkou, jestli má agresivní materiál vliv na děti. Nedá se s jistotou říct, že když se dětem ukazuje násilí, že budou ony samy násilnější. Tendence k agresivitě je z části vrozenou záležitostí a mnohem více než násilí v médiích ovlivňuje děti například násilí v rodině. Přesto častým vystavením agresivním scénám může u dítěte dojít k vytvoření necitlivosti vůči násilí a k posunu v emočním vnímání. Jedinec může časem získat pocit, že násilí je normální a postupně ztrácí soucit s jeho oběťmi. Nejnebezpečnější jsou věci, které se může dítě pokusit napodobit. [14]

5.3.3. Nepravdivé a zavádějící informace

Internet nabízí široké možnosti čerpání informací, je ale důležité umět je hledat a nacházet ty správné, což zvláště pro mladé uživatele internetu není vždy jednoduchý úkol. Při získávání informací z internetu totiž často narážejí na různá úskalí. Kvůli nejednoznačnému zadání do vyhledávače se musí uživatel potýkat s obrovským množstvím výsledků vyhledávání, ze kterého se ta pravá informace těžko vybírá. Děti a dospívající mohou do vyhledávače zadávat pro ně běžná a nevinná slova, v řeči dospělých může mít ale slovo jiný význam a děti se tak dostanou k nevhodnému obsahu. Důležitá je také schopnost správně odhadnout důvěryhodnost nalezené informace.

Při vyhledávání informací na internetu je důležité umět rozpoznat, zda je možné se na nalezenou stránku spolehnout. V první řadě je nutné se zaměřit na to, kdo ji provozuje, zda je například známý ve svém oboru, a jaký je jeho motiv pro provozování webových stránek (zda se nejedná pouze o reklamu). Pro utvoření co možná nejobjektivnějšího obrázku je dobré posoudit, do jaké míry je stránka aktuální a obsáhlá, jestli působí profesionálně a také zjistit, zda je zde uveden kontakt na provozovatele, jestli je někým doporučena nebo jde-li například o oficiální web nějakého podniku či instituce. [15]

5.4. Kyberkriminalita

Kybernetický zločin, je druh trestné činnosti, která je páchána s pomocí počítače a internetu nebo proti počítači. Do této kategorie spadá mnoho trestných činů, jako například kyberšikana, kybergrooming, kyberstalking, sexting, krádež identity, rozesílání spamů a hoaxů a také útoky na zabezpečení počítače (různé druhy malwaru – počítačové viry a červi, Trojští koně, phishing apod.).

5.4.1. Kyberšikana

Termínem kyberšikana označujeme nebezpečné komunikační jevy realizované prostřednictvím informačních a komunikačních technologií, jež mají za následek ublížení nebo jiné poškození oběti. Zahrnuje například různé nadávky a výhrůžky, telefonický teror, šíření ponižujících fotografií a soukromých informací, urážky, ponižování a zesměšňování nebo také ignorování ve skupinách a diskusích a podobně. Během kyberútoku nedochází k osobnímu kontaktu útočníka s obětí (útočník svou oběť dokonce ani nemusí znát, může si ji jednoduše vytipovat např. podle přezdívky nebo věku) a dopad jeho vlivu trvá podstatně déle než nadávka či pomluva v reálném světě. Oběti kyberšikany jsou často uzavřené do sebe a nekomunikují o problémech s okolím. Důvodů pro takové chování může být více (strach, stud, obava ze zákazu používání internetu atd.). Proto zůstávají na řešení svých problémů nezřídka kdy samy, což může vést k tomu, že situaci nezvládnou.

Jedná se o druh psychické šikany, která se odehrává ve virtuálním světě. Zatímco u tradiční šikany lze předpokládat, kdy a kde dojde k útoku (např. ve škole, na hřišti), s kyberšikanou se můžeme setkat kdykoliv a kdekoliv. Obětí útoku se může uživatel stát vždy, když bude připojen k internetu nebo mobilní síti. V takovém případě se před kyberútokem nemá kam schovat a je mu vystaven 24 hodin denně. [16]

Nejhorší následky má šikanování bezesporu pro oběti. Závažnost poškození závisí na tom, jaké míry destruktivní síly dosáhlo a zda bylo krátkodobé, nebo dlouhodobé. Důležitá je i míra obranyschopnosti oběti. Následky mohou být velmi závažné, dotýkají se celé osobnosti, jejíž vývoj můžou narušit a mají někdy i celoživotní charakter. Oběti jsou

frustrovány, pociťují strach, pocity bezmoci a nejistoty, které mohou časem přejít v otupělost, vyhaslost, uzavřenost a poruchy sebehodnocení. Mívají tendence ode všeho uniknout, vše vzdát a skrýt se. Často trpí poruchami spánku a depresemi, které v nejhorších případech vedou až k sebedestrukci nebo i sebevraždě. Oběti šikany se mnohdy později stávají samy jejími pachateli na dalších lidech.

Michal Kovář ve své knize Nová cesta k léčbě šikany uvádí, že vždy, když řešil případ kyberšikany v souvislosti se školou, odkryl zároveň také klasickou šikanu ve škole, kterou je možné řešit. Kyberšikanu je velmi obtížné postihnout. [17]

Pachatel kyberšikany je ve většině případů anonymní, skrytý za přezdívkou nebo jiným neurčitým identifikátorem a může jím být naprosto kdokoliv, kdo má potřebné znalosti informačních a komunikačních technologií bez ohledu na věk, pohlaví a fyzické dispozice, na rozdíl od šikany v reálném prostředí. Sekundárními útočníky se pak stávají diváci a šiřitelé. Množství přihlížejících kyberšikany může být nepoměrně větší než u klasické šikany. Může jím být v podstatě každý, kdo má přístup k internetu. Šiřiteli kyberšikany jsou lidé, kteří se vědomě či nevědomě zapojují například tím, že dále rozesílají informace. Obě tyto skupiny mohou zmnohonásobit dopad útoku na oběť a poškodit ji mnohem víc než primární útočník.

Stejně jako je tomu u původců kyberšikany, ani u jejích obětí nezáleží na věku, pohlaví, fyzické síle, postavení v sociální skupině či úspěšnosti ve společnosti.
V elektronické komunikaci jsou výše zmíněné aspekty potlačeny a nemají takový význam jako při komunikaci tváří v tvář. Oběti tradiční šikany se často stávají také oběťmi kybernetické šikany. Také jimi bývají spíše lidé, kteří jsou málo obeznámeni s riziky spojenými s užíváním ICT, a kteří se proto na internetu nechovají dostatečně opatrně. [16]

Nejlepší ochranou před kyberšikanou je její prevence, to znamená chovat se tak, abychom k ní nikomu nezavdávali příčinu, nebýt příliš důvěřivý, nesdělovat citlivé informace a seznámit se s pravidly užívání internetových služeb. Pokud k útoku i přesto dojde, řešením je ukončit komunikaci s útočníkem, nereagovat a neodpovídat, nesnažit se mstít a pokud možno zamezit mu v přístupu k oběti (zablokovat si příjímání zpráv a

hovorů od této osoby, kontaktovat poskytovatele služby nebo změnit svou virtuální identitu). Je-li možno pachatele odhalit, měl by ho uživatel oznámit, schovat si důkazy pro vyšetřování (uchovat e-maily a textové zprávy, sejmout náhled aktuální stránky pomocí klávesy PrintScreen apod.) a obrátit se na odborníky. Pokud je poškozeným dítě, mělo by vše co nejdříve sdělit rodičům.

Kyberšikana stejně jako šikana není v České republice trestným činem. Takovéto chování ale může naplňovat skutkovou podstatu některých trestných činů. V případě kyberšikany může jít například o trestný čin omezování osobní svobody, vydírání, vyhrožování, nebezpečné pronásledování (stalking) nebo útisk. [18]

5.4.2. Kybergrooming

Kybergrooming označuje chování uživatelů internetu, které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce. Výsledkem této schůzky může být sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod. Je to druh psychické manipulace realizovaný nejčastěji na veřejných chatech, internetových seznamkách, na sociálních sítích nebo pomocí ICQ a Skype[16]. Internetoví predátoři využívají také inzertní portály, na kterých nabízejí dětem různé možnosti výdělku či kariéry (např. v oblasti modelingu), často navštěvují portály zaměřené přímo na nezletilé uživatele internetu (dětské portály, portály zaměřené na volnočasové aktivity, herní portály a další internetové stránky).

Oběťmi jsou zpravidla děti (spíše dívky) nejčastěji ve věku 11-17 let. Jedná se zejména o uživatele internetu, kteří tráví velké množství volného času v online komunikačních prostředích (chat, instant messengery, sociální sítě), kde navazují virtuální kontakty s ostatními. Nejčastějšími typy obětí jsou děti s nízkou sebeúctou nebo nedostatkem sebedůvěry, emocionálními problémy, naivní a přehnaně důvěřivé děti nebo adolescenti.

[16] ICQ a Skype jsou programy umožňující provozovat internetovou telefonii, videohovory a instant messaging.

Útočníky většinou bývají lidé, u kterých byl diagnostikován patologický zájem o děti. Kybergroomeři navazují kontakty s dětmi, protože mají strach z navazování vztahů s dospělými. Vztahy s dětmi vnímají jako méně ohrožující a cítí se v nich bezpečněji než ve vztazích s dospělými. Často dokonce vytvářejí sítě, ve kterých spolu vzájemně spolupracují.

Psychická manipulace v rámci kybergroomingu probíhá obvykle delší dobu – nejčastěji od 3 měsíců po dobu několika let. Doba trvání závisí na způsobu manipulace a na důvěřivosti dětí. Proces manipulace sestává z několika fází (příprava kontaktu, kontakt s obětí, příprava na osobní schůzku a osobní schůzka), během kterých útočník využívá velké množství technik a postupů.

Groomeři většinou vystupují pod falešnou identitou, někdy vytváří i více nepravých identit, které podle potřeby střídají a upravují, aby vybranou oběť oslovili co nejefektivněji. Někdy nevystupují jako fyzické osoby, ale jako jednatelé nějaké firmy (např. modelingové agentury nebo firmy zaměřující se na finanční pomoc sociálně slabým dětem). Po úspěšném navázání kontaktu s obětí útočník pracuje na budování a prohlubování virtuálního vztahu, přičemž často používá tzv. efekt zrcadlení – napodobování oběti ve snaze prolomit její zábrany. V této fázi se snaží získat co nejvíce informací a citlivých materiálů o dítěti a také jeho důvěru, aby ho posléze přiměl souhlasit s osobní schůzkou. Pokud setkání odmítne, dochází k nátlaku a vydírání.

Osobní schůzka je ústředním cílem snahy kybergroomera. První setkání útočníka s obětí může být úplně nevinné, nemusí ještě dojít k sexuálnímu či jinému zneužití oběti. Útočník si může pouze ověřit, zda se jedná skutečně o nezletilou osobu a popřípadě s ní prohloubit navázaný vztah například dárkem. Oběť tak nabude dojmu, že dotyčný je neškodný. Útok (sexuální, fyzický,…), ke kterému může dojít někdy až po několika osobních setkáních, má pro oběť nedozírné následky. Jak v oblasti fyzické, tak zejména v oblasti psychické. Pokud má groomer dostatek účinných nástrojů pro manipulaci, může oběť donutit k opakovaným schůzkám, na kterých útoky pokračují.

Nejefektivnější obranou je (podobně jako u kyberšikany) především opatrnost, informovanost, nedůvěra a efektivní komunikace mezi rodičem a dítětem. [16]

5.4.3. Stalking a kyberstalking

Stalking (lov, pronásledování) označuje opakované, dlouhodobé, systematické a stupňované obtěžování, které může mít řadu různých forem a různou intenzitu. Pronásledovatel svou oběť například vytrvale sleduje, bombarduje SMS zprávami, e-maily, telefonáty či nechtěnými pozornostmi (dárky). Obsah zpráv může být příjemný až veselý, ale též urážející, zastrašující s cílem vyvolat u oběti pocit strachu (prostřednictvím vyhrožování, vydírání a vyvolávání pocitu viny). Pokud dosavadní pokusy stalkera selhávají, může dojít k naplnění těchto výhrůžek. Součástí bývá často také fyzické pronásledování oběti nebo snaha poškodit její reputaci.

Ve spojení s využitím ICT u útočníka hovoříme o termínu **kyberstalking**. V tomto případě jde o zasílání různých zpráv pomocí instant messengerů (ICQ, Skype), chatu nebo prostřednictvím sociálních sítí. Kyberstalkeři navštěvují sociální sítě či diskusní fóra, ve kterých se pod falešnou identitou snaží kontaktovat oběť, případně získat informace o oběti od ostatních uživatelů.

Nejčastějšími oběťmi stalkingu jsou známé osobnosti (zpěváci, herci, politici) a ex-partneři, jinak se jimi může stát prakticky jakýkoliv (většinou svobodný) člověk. Pachatelem je potom většinou bývalý partner, který není schopen přijmout ukončení vztahu s nějakou osobou. Chování stalkera je následkem jeho touhy vztah obnovit nebo je odplatou za odmítnutí. Pachatelem stalkingu může být také neobratný nápadník, jemuž jeho slabé sociální a komunikativní dovednosti neumožní navázat skutečný partnerský vztah. Pronásledovatel se pokouší o fyzický kontakt s obětí, o které se domnívá, že ji miluje a žárlí, pokud má oběť vztah s jinou osobou. [16]

5.4.4. Sexting

Sexting je složenina slov sex a texting (= anglicky posílání SMS zpráv). Sexting je tedy nové slovo, které vystihuje nový trend – posílání erotického obsahu prostřednictvím mobilů. Jedná se nejčastěji o pořizování erotických fotek nebo videí a jejich následné posílání pomocí mobilních telefonů přátelům a známým. Tyto obrázky se obvykle posílají nejprve jen v páru nebo nejlepším kamarádům jako důkaz lásky či přátelství nebo jako forma flirtu. Často potom ale skončí jako pomsta vystavené veřejně na internetu, většinou na stránkách sociálních sítí nebo na různých portálech pro zveřejňování fotografií. Někdy se původně důvěrné osobní fotky stanou i prostředkem vydírání. Mohou se znovu vynořit i po letech, protože jak se jednou dostanou do oběhu, neexistuje žádný způsob, jak spolehlivě zastavit jejich šíření a mohou napáchat závažné škody například v kariéře nebo v soukromých vztazích postižené osoby. [19]

5.4.5. Krádež identity

Krádež identity není ve světě zločinu žádnou novinkou, v současné době se změnila jen její podoba. Zatímco dříve se pachatelé fyzicky vydávali za jinou osobu (ať už na základě ukradených listin nebo jen podobností zevnějšku), dnes se odcizuje především její počítačová identita. Děje se tak nejčastěji odcizením elektronických dat (hesla, přístupové údaje,…), a to zpravidla neoprávněným kopírováním dat, lstivým vylákáním údajů (phishing) nebo nedovoleným vniknutím do cizího počítače (hacking). Pachatel poté neoprávněně nabytou identitu zneužije. Cílem bývá hlavně majetkový prospěch – krádeže čísel bankovních účtů a přístupových hesel či kódů, čísel sociálního zabezpečení apod.

Pokud někdo ovládá něčí identitu, může napáchat i další škody kromě těch finančních. Dokáže například osobu poškodit profesně nebo v soukromém životě. [20]

5.5. Závislost

Jedním z rizik spojených s používáním sociálních sítí je v neposlední řadě také nebezpečí vytvoření si silného návyku na ně vedoucího až k závislosti. Děti tráví na Facebooku čím dál větší množství času na úkor svých koníčků, tráví čím dál méně času venku se svými skutečnými přáteli. Místo toho sedí doma připoutané k monitoru počítače. Mnohé si už neumí život bez sociálních sítí ani představit. Připojují se hned poté, co se ráno probudí, aby zkontrolovaly, co je nového a odhlašují se, až než jdou spát. Věnují Facebooku všechen svůj volný čas. Přesouvají svůj život do virtuálního prostoru a ztrácí tak kontakt s reálným světem. Některé dokonce vykazují stavy podobné abstinenčním příznakům, pokud jim po nějakou dobu není umožněn přístup k internetu.

6. Jak děti ochránit před hrozícím nebezpečím

Jak už bylo dříve řečeno, nejlepší možností, jak děti ochránit před nástrahami internetu, je důkladná osvěta především ze strany rodiny, která je za mladistvé uživatele zodpovědná. Děti vnímají internet pouze jako zdroj zábavy a potenciální problémy vůbec nevidí. Rodiče by se měli o danou problematiku zajímat, předně si sami uvědomit možná rizika, patřičně se v tomto oboru vzdělat a získané informace předat svým potomkům. Měli by si rozhodně všímat jejich činnosti na internetu, stanovit předem jasná pravidla a dohlížet na jejich dodržování, pomoci dítěti například s registrací účtu a nastavením jeho bezpečnosti. Prospěšné by jistě bylo také zavést ve školách pravidelnou výuku týkající se bezpečné práce na internetu.

Existují různé vzdělávací programy a webové portály, na kterých mají lidé možnost čerpat potřebné informace včetně užitečných doporučení.

6.1. Národní centrum bezpečnějšího internetu a Saferinternet.cz

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

NCBI pro uskutečnění svých cílů realizuje řadu projektů, z nichž nejdůležitější je **Saferinternet.cz**, který usiluje o zvyšování povědomí o bezpečnějším užívání internetu. Podporuje vzdělávání dětí i rodičů v této oblasti. Poskytuje pomoc, působí proti šíření ilegálního, zejména pedofilního a extremistického obsahu na internetu. Projekt je spolufinancovaný Evropskou komisí. Ve spolupráci se svými partnery (Ministerstvo školství, Ministerstvo vnitra a Policie ČR) pořádá konference, semináře, přednášky a

školení zaměřené na oblast bezpečnějšího užívání internetu a prevenci internetové kriminality. [21]

Součástí projektu jsou stránky:

- **Bezpecneonline.cz** - Výchovně-vzdělávací stránky, jejichž cílem je poskytovat mladým uživatelům ve věku 12 až 17 let, jejich rodičům a pedagogům, užitečné informace, které jim usnadní používat internet bezpečněji. [22]
- **Horkalinka.cz** - Kontaktní centrum, které přijímá hlášení týkající se nezákonného obsahu na internetu. Jejím hlavním cílem je bránit šíření obrazového materiálu se zneužívanými dětmi. [22]
- **Pomoconline.cz** - Krizové centrum, pomáhající dětským obětem internetové kriminality. Linka pomoci pomáhá a průběžně také realizuje tematické preventivní kampaně zaměřené na děti i rodiče s cílem upozorňovat na potenciální rizika internetové komunikace. [22]
- **Protisikane.cz** – Stránka, která se zabývá kyberšikanou a informuje o tom, jak jí předejít a jak se jí bránit. [23]
- **Mobilstory.cz** – Stránka informující o bezpečném používání mobilních telefonů. [24]

6.1.1. Informační centrum pro mládež (ICM)

Součástí Národního centra bezpečnějšího internetu je Informační centrum pro mládež (ICM), které poskytuje všem zájemcům informace především v oblasti vzdělávání, pracovních příležitostí, způsobů trávení volného času, sociálně-patologických jevů, životních situací občanů, mládeže. Specializuje se na oblast bezpečného užívání internetu, informování o potenciálních rizikách, které hrozí v případě neopatrného užívání sociálních sítí a obecné zvýšení povědomí o zodpovědném používání online technologií. Zajišťuje poradenské služby v krizových situacích, poskytuje kontakty na poradenské organizace, pomoc v naléhavé situaci (domácí násilí, šikana, závislost, zdravotní postižení, atp.). Informace poskytuje prostřednictvím internetových stránek ICM, osobně v ICM, telefonicky a také prostřednictvím elektronické pošty. Pořádá vzdělávací kurzy, besedy, konference a sdílí informace s ostatními centry. [25]

6.1.2. Saferinternet Akademie

NCBI nabízí široké spektrum vzdělávacích a osvětových služeb školám a dalším organizacím v oblasti prevence rizikových jevů spojených s užíváním internetu a online komunikací. Poskytuje konzultace, metodické a výukové materiály a pořádá besedy s odborníky. Semináře pro pedagogické pracovníky, žáky i rodiče žáků zajišťuje odborný lektorský tým centra, složený z psychologů, pedagogů, sociálních pracovníků a ICT specialistů. Všichni lektoři prošli specializovaným výcvikem v oblasti prevence elektronického násilí a kriminality. [26]

6.1.3. Konference

Národní centrum bezpečnějšího internetu pravidelně pořádá odborné konference, které se věnují online kriminalitě a prevenci rizik, která při používání nových informačních a komunikačních technologií hrozí především dětem. Setkávají se na nich mediální odborníci, pedagogové, preventisté, zástupci politické reprezentace a širší odborná veřejnost. Cílem konferencí je otevřít odborný dialog nad ožehavou problematikou bezpečného internetu pro děti. [27]

Jako poslední proběhla konference **Praha bezpečně online**, kterou uspořádalo NCBI ve spolupráci s oddělením prevence Magistrátu hlavního města Prahy. Konala se 10. prosince 2012 v prostorách Magistrátu a jejím hlavním tématem byla internetová kriminalita, praktické zkušenosti dětí a jejich názory a ukázky metodiky prevence. [28]

6.1.4. Soutěže

V rámci projektu Saferinternet.cz se NCBI podílí také na pořádání různých soutěží, které jsou stejně jako celý projekt zaměřeny na téma bezpečnější internet se snahou vzbudit v soutěžících zájem a snahu poznávat, případně i pomoci s vytvářením lepšího prostředí na internetu.

Jednou z nich je soutěž s názvem **„Moje soukromí! Nekoukat, nešťourat!“**, kterou organizuje Úřad pro ochranu osobních údajů ve spolupráci se Saferinternet.cz. Například v letošním ročníku soutěže se mají děti podělit o vlastní zkušenosti se sociálními sítěmi, napsat, co se jim na nich líbí a co by se třeba dalo zlepšit, v loňském zase měly dokončit rozehraný příběh. Soutěž pomůže zúčastněným zamyslet se nad otázkou vlastního soukromí a uvědomit si, že je potřeba si jej chránit. Tím nenásilnou a zábavnou formou vede děti k zodpovědnějšímu a bezpečnějšímu chování. [29]

6.2. Bezpečný internet

Dalším internetovým portálem zaměřeným na vzdělávání je Bezpečný internet.cz. Tento projekt vznikl s cílem ukázat mnohá rizika spojená s používáním internetu a také na způsoby, jak se jim účinně bránit. Projekt není vázán na produkty žádných společností a zcela zdarma poskytuje rady, návody i zkušenosti provozovatelů nejnavštěvovanějších internetových služeb a pomáhá vytvářet správné návyky internetové bezpečnosti. Zakládajícími partnery jsou Česká spořitelna, Microsoft a Seznam, mezi další patří také například Policie ČR nebo Hoax.cz.

Nezaměřuje se jen na jednu konkrétní skupinu uživatelů. Je rozdělen podle cílové skupiny pro začínající uživatele, pokročilé uživatele, rodiče, děti a školy. Návštěvník si vybere svou kategorii a pročítá si články vypracované konkrétně pro jeho potřeby. Po přečtení textu si může vyplnit kontrolní test, na základě kterého si ověří, kolik poznatků si odnesl. Část určená dětem je ozvláštněna veselými obrázky, články jsou přiměřeně dlouhé a navíc jsou přidány vzdělávací články ve formě ilustrovaných komiksů, které děti zaujmou více než samotný text. Součástí této stránky je také poradna, kam je možné poslat dotaz nebo si pročítat odpovědi na již zodpovězené otázky. Zároveň jsou zde užitečné tipy, kde hledat pomoc v případě problémů. [30]

6.3. E-Bezpečí

Jedním z projektů fungujících na podobném principu jako dříve zmiňované je také internetový portál E-Bezpečí. Vznikl v roce 2008 a je realizován Centrem prevence

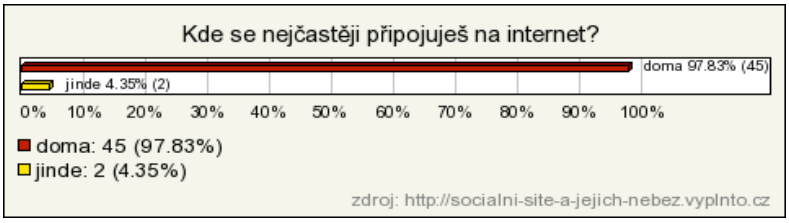
rizikové virtuální komunikace Pedagogické fakulty Palackého ve spolupráci s Ministerstvem vnitra, Ministerstvem školství, mládeže a tělovýchovy, Policií ČR, Olomouckým krajem, firmami Vodafone, Google, Seznam a dalšími. Zaměřuje se na prevenci, vzdělávání, výzkum, intervenci a osvětu spojenou s rizikovým chováním na internetu a souvisejícími fenomény, které ohrožují jak děti, tak i dospělé uživatele internetu. Specializuje se zejména na kyberšikanu a sexting, kybergrooming, kyberstalking a stalking, rizika sociálních sítí, hoax a spam a zneužívaní osobních údajů v prostředí elektronických médií.

Mezi cílové skupiny projektu patří žáci a studenti, učitelé, preventisté sociálně patologických jevů, metodici prevence, policisté (městská policie, Policie ČR), manažeři prevence kriminality, vychovatelé a v neposlední řadě také rodiče. Kromě vzdělávacích akcí realizuje E-Bezpečí také pravidelná celorepubliková výzkumná šetření, zaměřená na rizikovou komunikaci v online prostředích, provozuje online poradnu, vydává řadu zajímavých tiskovin pro žáky/učitele a realizuje řadu dalších aktivit. [31]

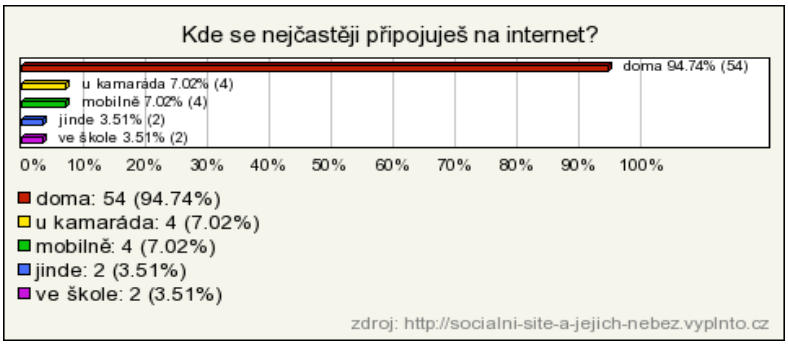
7. Dotazníková anketa

Tématem celé této práce jsou sociální sítě z pohledu bezpečnosti jejich dětských uživatelů. Teoretická část práce ukázala, že sociální sítě jsou mnohostranně užitečnou službou, kterou však lze snadno zneužít. Účelem praktické části práce bylo pomocí dotazníkového šetření zjistit skutečnou situaci u českých dětí. Anketa byla provedena v místě mého bydliště na ZŠ Ratibořická v Horních Počernicích. Po dohodě s vedením školy jsem předala dotazníky tamější výchovné poradkyni Ing. Aleně Fremuntové, která je nechala vyplnit žákům v rámci hodin Občanské a Rodinné výchovy. Můj původní požadavek bylo 100 respondentů, nakonec dotazník vyplnilo celkem 106 dětí ve věku od 9 do 16 let, protože anketa byla vždy zadána celým třídám. Výsledky byly následně zpracovány pomocí webového portálu Vyplň to.cz.

Všechny dotazované děti bez ohledu na věk a pohlaví shodně odpověděly, že internet pravidelně používají. V kategorii mladších dětí (9-12 let) se téměř všichni dotazovaní respondenti (98 %) připojují k internetu nejčastěji z domova, 7 % starších dětí (13-16 let) uvedlo, že se připojuje hlavně přes mobilní zařízení s vlastním datovým tarifem nebo kdekoliv, kde je dostupná wi-fi síť, 7 % používá internet u svých kamarádů a přibližně 4 % ve škole.

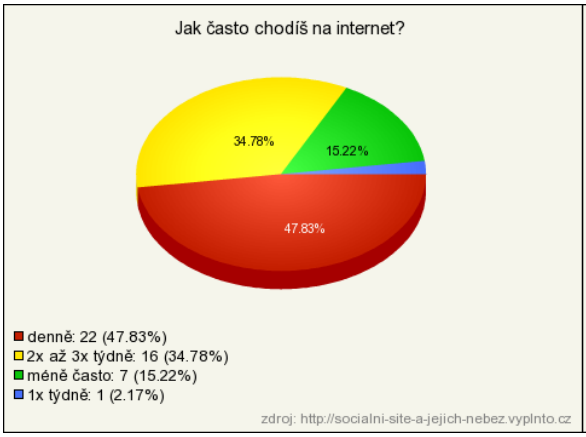


Graf 1a - kategorie 9-12 let

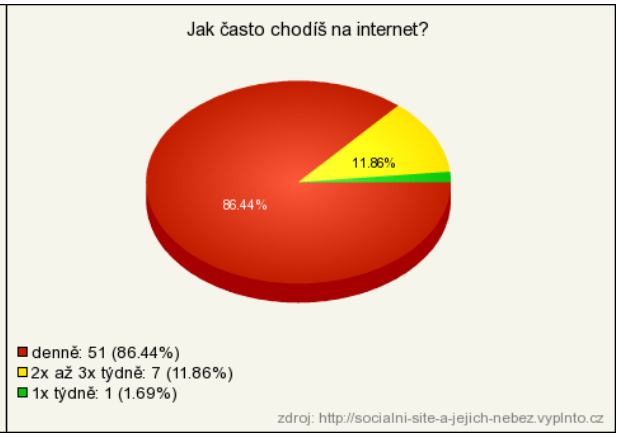


Graf 1b - kategorie 13-16 let

Téměř polovina mladších dětí pracuje s internetem denně, dalších 35 % alespoň dvakrát až třikrát týdně. U starších tvoří každodenní uživatelé více než 86 %.

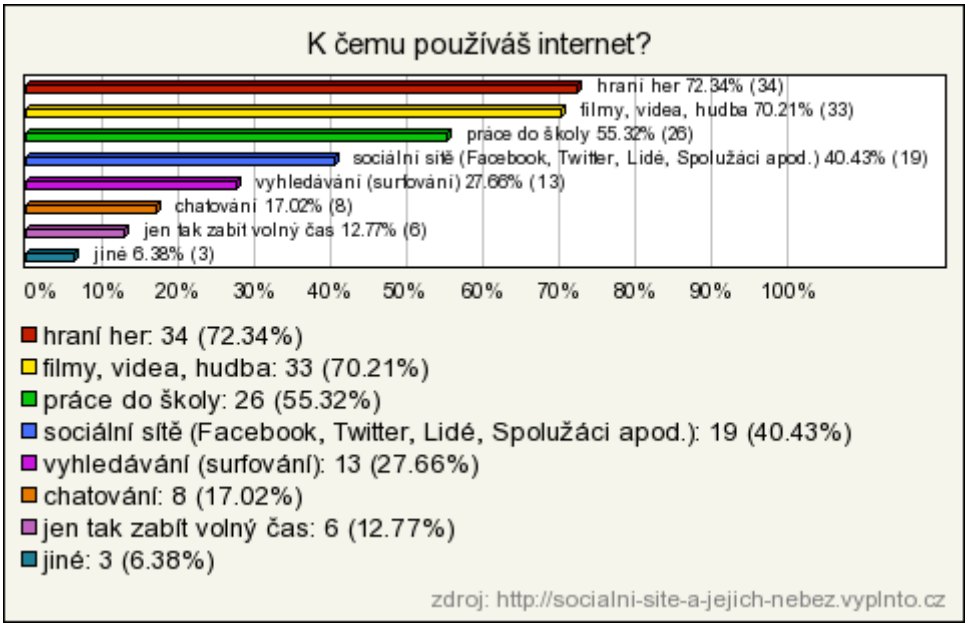


Graf 2a - kategorie 9-12 let

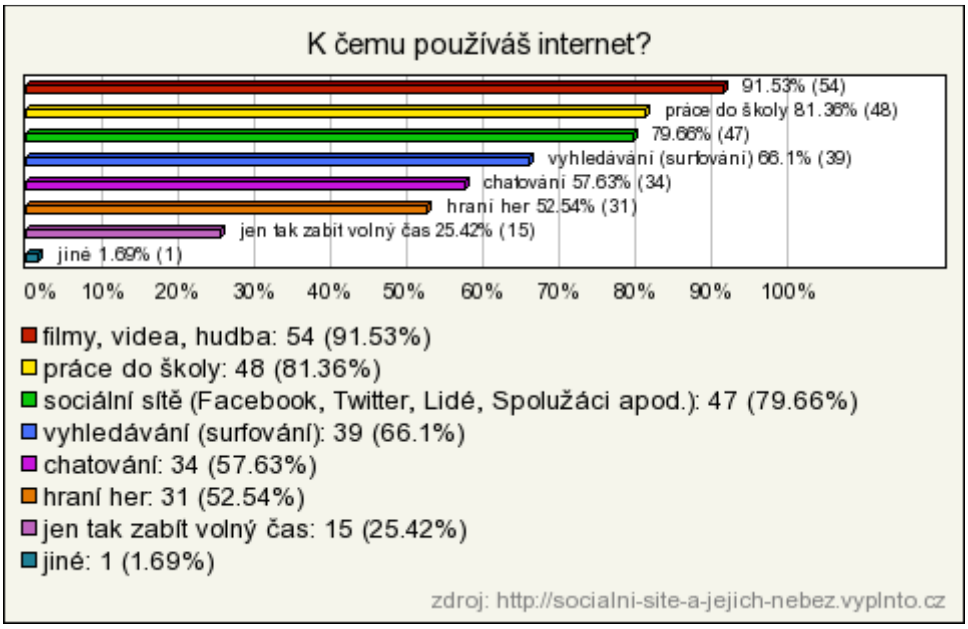


Graf 2b - kategorie 13-16 let

Z následujících dvou grafů vyplývá, že děti shodně v obou věkových kategoriích využívají internet pro stahování filmů, videí a hudby a ke studiu. U mladších však dominuje hraní her. Sociální sítě jsou u mladších na čtvrtém místě a u starších na třetím. Nejvíce oblíbené byly u starších dívek (téměř 97 %).



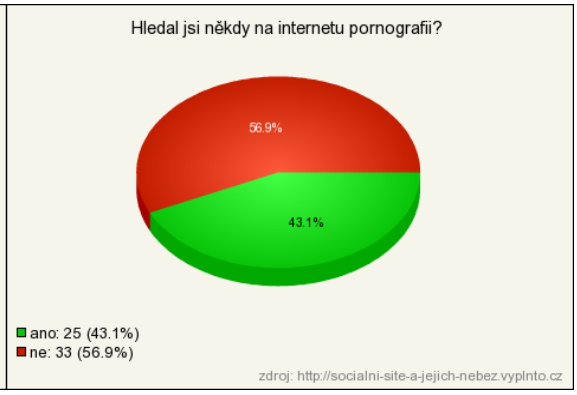
Graf 3a - kategorie 9-12 let



Graf 3b - kategorie 13-16 let

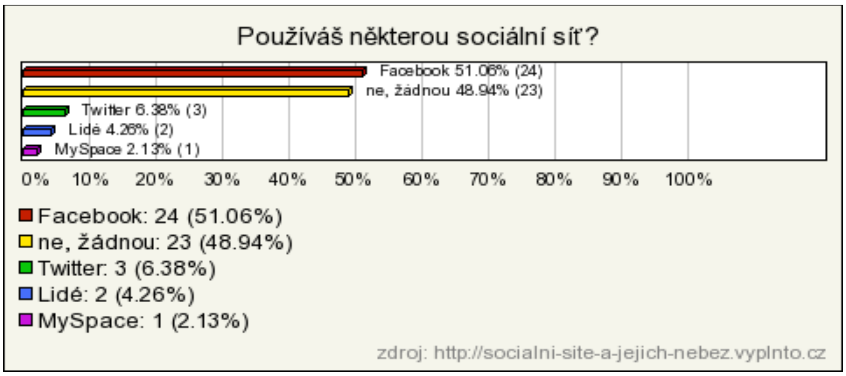
Okolo 43 % starších dětí (častěji chlapců) přiznalo, že někdy samy aktivně vyhledávaly na internetu pornografii, z mladších odpovědělo kladně pouze necelých 7 %.

Graf 4a - kategorie 9-12 let

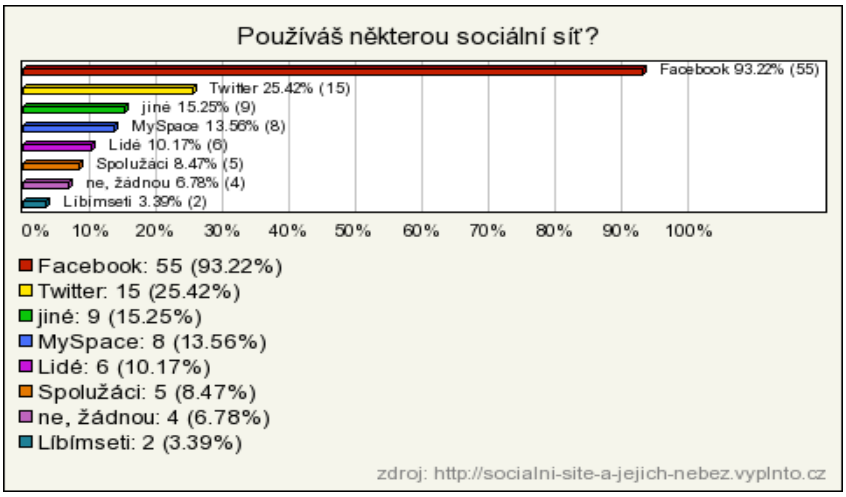


Graf 4b - kategorie 13-16 let

Následující otázkou v dotazníku (viz grafy 5a a 5b) bylo, zda dotazovaní používají některou ze sociálních sítí. Přibližně 51 % mladších dětí uvedlo, že ano a necelých 49 %, že ne. Ve skupině starších je používá už více než 93 % respondentů. Všichni, kteří odpověděli, že sociální sítě využívají, uvedli Facebook, dále se mezi odpověďmi objevovaly Twitter, MySpace, Lide.cz, Spoluzaci.cz a Libimseti.cz.

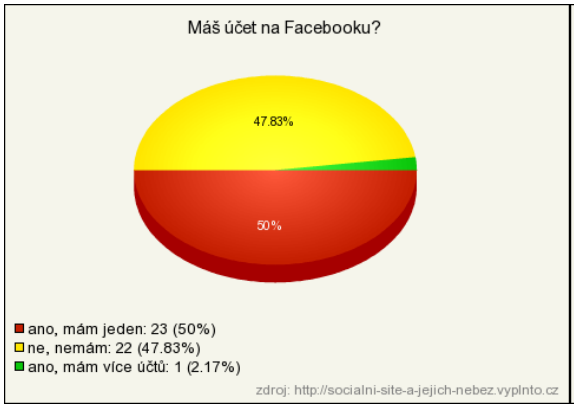


Graf 5a - kategorie 9-12 let

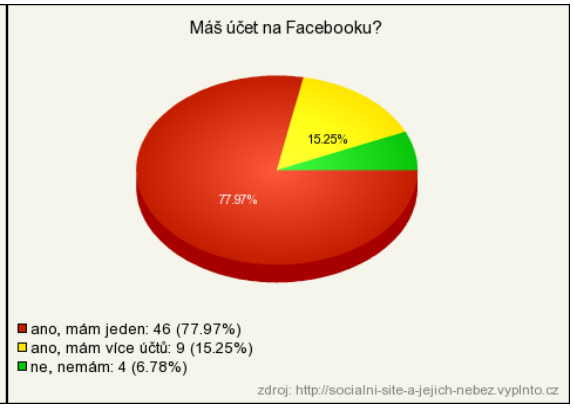


Graf 5b - kategorie 13-16 let

Profil na Facebooku má tedy více než 93 % starších dětí a 52 % dětí ve věku 9-12 let, přestože podle pravidel používání Facebooku si mohou zakládat účty pouze lidé starší 13 let. Přibližně 9 % respondentů také uvedlo, že vlastní více než jeden účet, což je rovněž zakázáno.



Graf 6a - kategorie 9-12 let



Graf 6b - kategorie 13-16 let

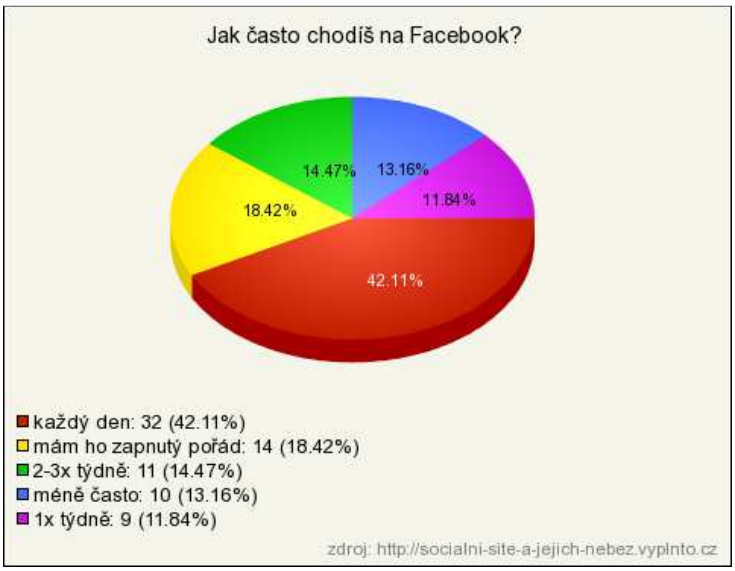
Z následujícího grafu je patrné, že zhruba 79 % rodičů je seznámeno s faktem, že jejich děti používají Facebook, ale pouze přibližně 11 % z nich pravidelně jejich účty kontroluje. Někteří starší respondenti dokonce uvedli, že jejich rodiče vědí o jednom profilu, ale že mají založený ještě další tajný účet, o jehož existenci rodiče netuší.

Graf 7

Jako hlavní důvod pro registraci do sociální sítě dotazovaní nejčastěji uváděli skutečnost, že portál používají jejich přátelé, rodina či známí (70 %), v menší míře také zájem seznámit se s novými lidmi (21,5 %) nebo prostě protože je to v dnešní době moderní (11,5 %).

Graf 8

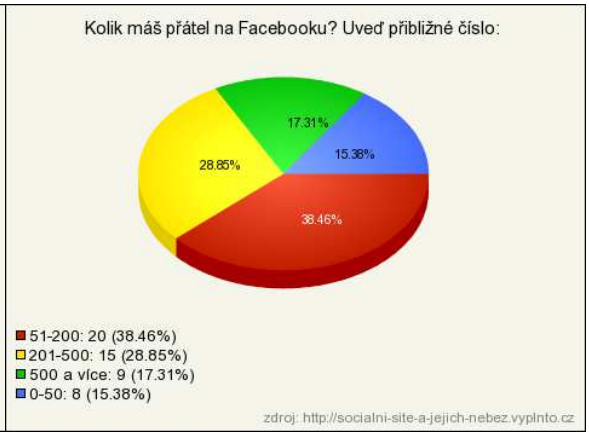
Necelá polovina respondentů (42 %) se na Facebook přihlašuje denně, 18,5 % je dokonce přihlášeno neustále a ostatní se připojují alespoň dvakrát až třikrát týdně (14,5 %) nebo méně často. V těchto bodech se výsledky v obou věkových skupinách příliš nelišily.



Graf 9

Grafy 10a a 10b ukazují, že mladší děti mají průměrně na Facebooku méně přátel. Zatímco děti v kategorii 9-12 let nejčastěji uváděly, že mají pouze 0-50 (62,5 %) nebo 51-200 přátel (21 %), starší děti nejvíce označovaly možnost 51-200 (38,5), poté 201-500 (29 %) a dokonce i 500 a více (17 %) kontaktů.

Graf 10a - kategorie 9-12 let



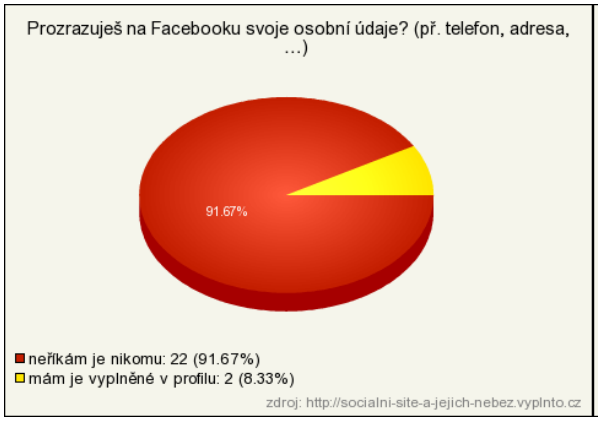
Graf 10b - kategorie 13-16 let

Necelá polovina (44 %) dotazovaných potvrdila, že si mezi přátele čas od času přidává i osoby, které ve skutečnosti nezná, zatímco 53 % přijímá žádosti o přátelství pouze od lidí, které zná osobně. Mladší děti byly v tomto ohledu překvapivě o trochu zodpovědnější.

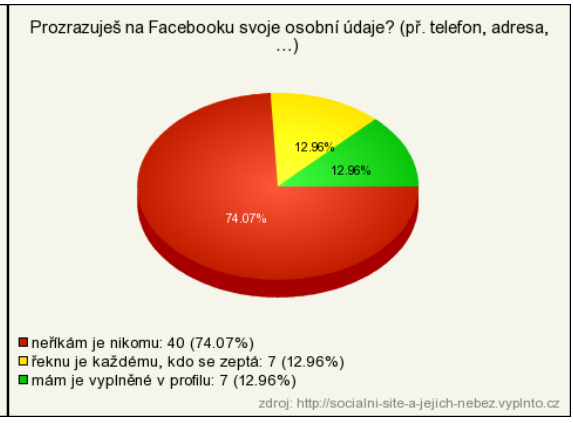
Graf 11

Necelých 5 % dotazovaných přiznalo, že někdy přeměnili své skutečné peníze na platidla do nějaké internetové hry a jeden z respondentů to udělal dokonce opakovaně.

Jako značně opatrnější se mladší děti nečekaně projevily také v otázce ochrany svých osobních údajů. Téměř 92 % z nich uvedlo, že své osobní údaje neprozrazuje nikomu. V druhé skupině respondentů takto odpovědělo jen 75 % dětí, zatímco téměř 13 % starších uživatelů má tyto údaje přímo vyplněné ve svém profilu a dalších 13 % je sděluje každému na požádání.

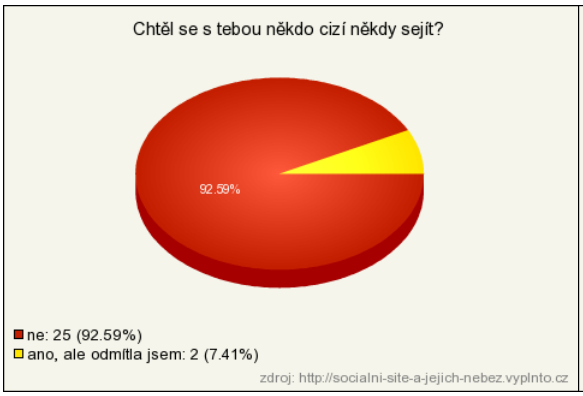


Graf 12a - kategorie 9-12 let

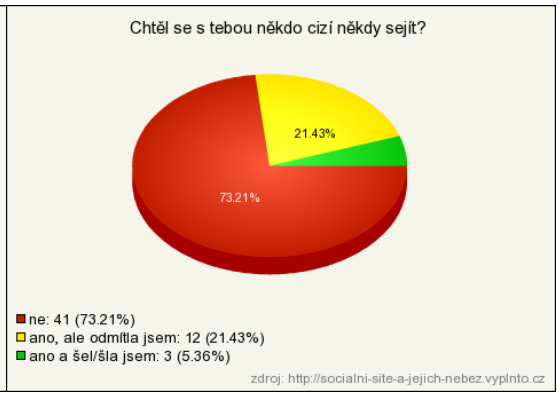


Graf 12b - kategorie 13-16 let

S návrhem osobního setkání od neznámé osoby (grafy 13a a 13b) se 92,5 % mladších dětí zatím nikdy nesetkalo a zbylé nabídku odmítly. Ve skupině starších dětí se však tento problém objevil přibližně u 27 % respondentů, z toho 21,5 % dotazovaných nabídnutou schůzku odmítlo, ale objevili se též tací, kteří se s úplně cizím člověkem dobrovolně sešli (cca 5,5 %).



Graf13a - kategorie 9-12 let

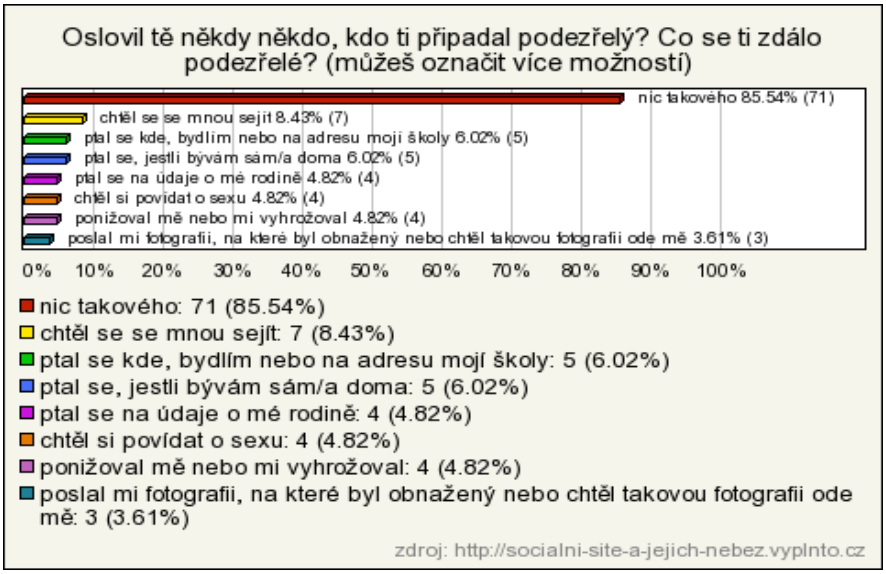


Graf 13b - kategorie 13-16 let

Dotazované děti většinou (téměř 86 %) nepotvrdily, že by se někdy na internetu setkaly s chováním, které by jim připadalo podezřelé či závadné. Otázkou však je, nakolik jsou schopné posoudit, co je závadné a co není. Děti, které v předchozí otázce odpověděly, že se s návrhem schůzky setkaly, však zde tuto možnost neoznačily a místo toho tvrdily, že žádný podezřelý jev nezaznamenaly. Pouze některé (spíše starší děti) uvedly, že se jich někdo ptal na adresu bydliště nebo školy, zda bývají samy doma či údaje o rodině. Mezi další uváděné problémy patřilo zasílání erotických fotografií nebo naopak žádost o poskytnutí takových fotografií, návrh na osobní setkání nebo konverzace na téma sexu. Objevil se i případ ponižování a vyhrožování.

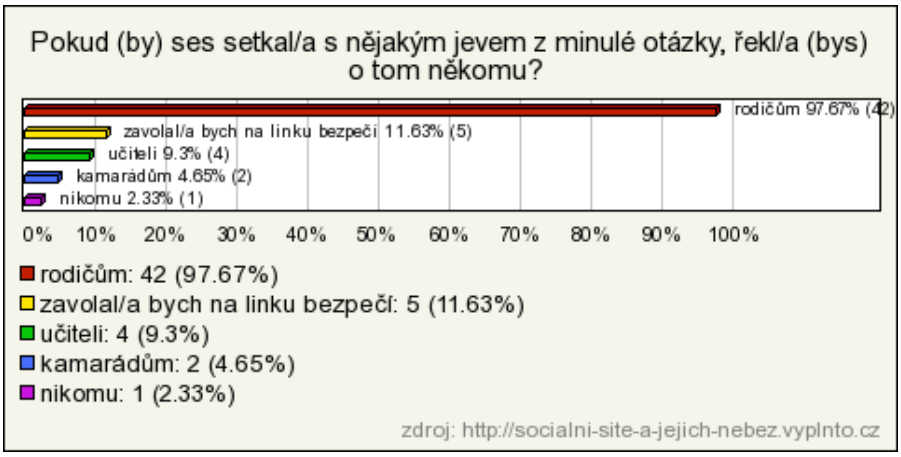
Jedna patnáctiletá dívka v dotazníku popsala případ, kdy ji na Facebooku oslovila cizí osoba, během konverzace se jí ptala na různé soukromé údaje a žádala o zaslání fotografií. Později, když už se o dotyčné dozvěděla mnoho citlivých informací a dostala i kompromitující fotografie, začala ji vydírat a vyhrožovat jí. Nakonec se ukázalo, že pachatelem byla dívčina bývalá kamarádka s falešným uživatelským profilem.

Jiná respondentka se svěřila, že si dokonce kvůli vydírání a vyhrožování svůj účet na Facebooku musela zrušit.

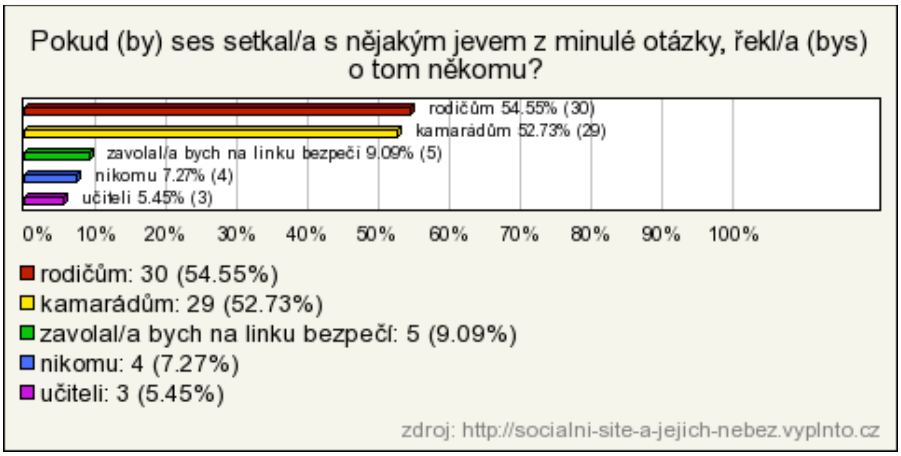


Graf 14

Skoro všechny děti (98 %) ve věku 9 až 12 let uváděly, že pokud by se s některým z jevů, které jsou zachyceny v grafu 14, setkaly, požádaly by o pomoc své rodiče. Z jejich starších spolužáků už ale takto odpověděla pouze přibližně polovina dotazovaných (54,5 %), další by se spíše svěřili svým kamarádům (53 %) nebo nikomu (7 %). Na lince bezpečí by pomoc hledalo jen asi 9 % z nich.

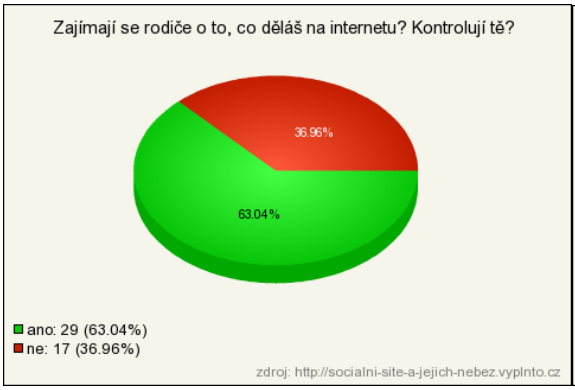


Graf 15a - kategorie 9-12 let

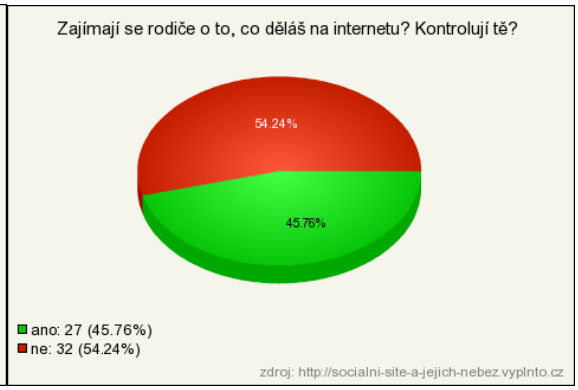


Graf 15b - kategorie 13-16 let

Anketa dále ukázala (viz grafy 16a a16b), že rodiče mladších dětí se o trochu více zajímají o internetové aktivity svých dětí. Zatímco ve skupině mladších dětí více než 63 % rodičů kontroluje, čemu se jejich děti na internetu věnují a jaké stránky navštěvují, podle odpovědí starších se takto chová jen necelých 46 % rodičů.

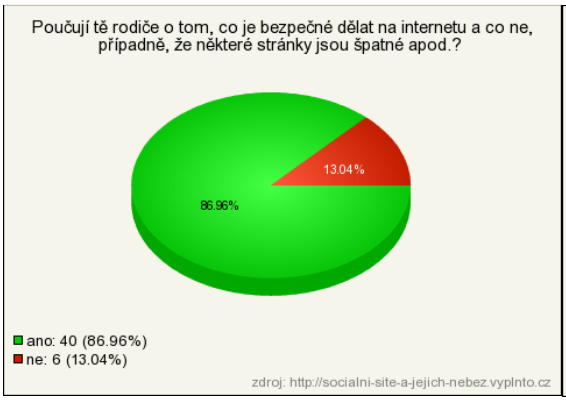


Graf 16a - kategorie 9-12 let

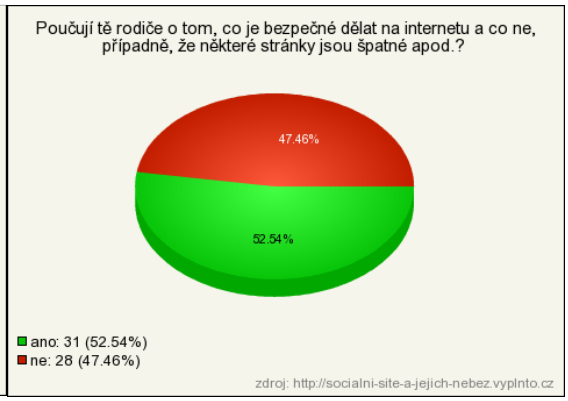


Graf 16b - kategorie 13-16 let

Rodiče mladších žáků také své děti výrazně více informují a poučují je o tom, co je bezpečné dělat na internetu a co ne, o tom které stránky jsou bezpečné a které nevhodné a podobně. Potvrdilo to téměř 87 % menších dětí a 52,5 % starších.



Graf 17a - kategorie 9-12 let



Graf 17b - kategorie 13-16 let

Výsledky této ankety jsou pouze informativního charakteru. Takto malé množství respondentů nemůže jistě přinést přesný obraz celého základního souboru, podává pouze velmi přibližné informace o chování dětí na sociálních sítích.

Považuji za vhodné také zmínit, že výuka dětí na základní škole, kde jsem prováděla tuto anketu, je doplněna přednáškami Policie ČR o kyberšikaně, což mohlo pozitivním směrem ovlivnit výsledky.

Během přednášek zaměřených na kyberšikanu a další nebezpečné jevy spojené s elektronickou komunikací (například kybergrooming apod.) preventisté od Policie ČR vysvětlí dětem, jak se kyberšikana projevuje a jak se takovým situacím vyhnout nebo jak se lze bránit. Beseda bývá doprovázena prezentací, videoukázkami a zajímavými příklady z praxe. V závěru setkání je obvykle nechán prostor pro diskuzi a dotazy ze strany žáků, které mohou být z důvodu zachování anonymity napsány na nepodepsané papíry.
Z přednášek si děti odnášejí kromě ponaučení většinou také různé informační letáčky. Tyto přednášky se však pořádají většinou až pro žáky druhého stupně základní školy, což mě osobně připadá pozdě.

Studenti Gymnázia Chodovická pod vedením PaeDr. Věry Čechákové organizují Projekt Občan, jehož hlavní náplní je pořádání preventivních besed na téma šikana pro žáky čtvrtých až šestých tříd základních škol v této městské části. Od roku 2008 působí i na základní škole Ratibořická. Během besed se proškolení studenti gymnázia snaží formou zábavných her, příběhů a interaktivní diskuze dětem vysvětlit, co je šikana, jak se bránit a

kde hledat účinnou pomoc. Mezi studenty gymnázia a žáky základních škol není velká věková bariéra, což jim značně usnadňuje práci s dětmi. Atmosféra na setkáních bývá kamarádská a uvolněná. Na závěr organizátoři rozdávají dětem letáčky, na kterých jsou shrnuty hlavní informace z besedy. Tisk těchto materiálů financuje ÚMČ Praha 20. Součástí besedy bývá také anonymní dotazníková anketa, jejíž výsledek studenti předávají třídním učitelům.

8. Závěr

Cílem této práce bylo poukázat na bezpečnost dětských uživatelů na sociálních sítích. Snažila jsem se předložit dostupná fakta a informace o rizicích spojených s používáním těchto sítí a o možnostech, jak před nimi sebe i své děti chránit. V praktické části jsem se potom pokusila zjistit, jak se děti na internetu skutečně chovají a jaké mají se sociálními sítěmi zkušenosti.

Je všeobecně známým faktem, že děti v dnešní době používají internet už od velmi útlého věku, což provedená anketa bezvýhradně potvrdila. Současná generace dospělých lidí si život bez internetu již neumí ani představit a v tomto duchu vychovávají i své potomky. Děti dostávají na hraní místo panenek a stavebnic mobilní telefony, tablety a počítače. Jsou tak již od mala vystavené mnohým nebezpečím, která jsou s internetem spojená, aniž by měly dostatek informací a zkušeností k tomu, aby se před těmito riziky ochránily.

Provedená anketa jednoznačně potvrdila šokující, leč obecně známou pravdu o tom, že sociální sítě jsou plné malých dětí. 52 % respondentů mé dotazníkové ankety ve věku 9 až 12 let potvrdilo, že používá Facebook, ačkoliv je to zakázané. Děti, zvláště ty mladší 13 let, oficiálně podle pravidel používání Facebooku nemají v kyberprostoru co dělat. Vzhledem k tomu, že ale neexistuje žádný platný legislativní prostředek (nutnost uvedení data narození splňujícího tento limit za překážku opravdu nepovažuji), který by jim zabránil ve vstupu, toto pravidlo bývá často porušováno. Při rozhodování, zda mladšímu dítěti dovolit si účet založit, stojí na jedné straně vědomí, že jej necháváme podvádět a proti tomu na druhé riziko, že jej ostatní děti, které Facebook používají, vyloučí z kolektivu a také fakt, že si může eventuálně profil stejně založit tajně, pokud mu to zakážeme.

Podle mého názoru by rodiče měli nejprve patřičně zvážit mentální vyspělost svého potomka a dříve, než mu udělí svolení vstoupit do virtuálního světa, jej patřičně vybavit důležitými vědomostmi. Myslím, že zvláště u menších dětí je také na místě pravidelná kontrola jejich internetových aktivit, popřípadě profilů na sociálních sítích a podobně.

Podle výsledků ankety sice většina rodičů ví o skutečnosti, že dítě vlastní účet na Facebooku, ale jen málo z nich jejich profily někdy kontroluje. Respondenti poměrně často vypovídali, že je rodiče sice čas od času o existujících hrozbách poučují, ale jen přibližně polovina z nich se zajímá o to, jakým činnostem se děti na internetu věnují. Vzdělávání by podle mě mělo jít ruku v ruce s kontrolou, aby bylo možné zpětně ověřit jeho účinek. Samozřejmě nepopírám, že důvěra mezi rodiči a dětmi je důležitá, ale nemělo by se na ni bezvýhradně spoléhat.

Poměrně překvapivé pro mne bylo také zjištění (vyplývající z ankety), že mladší děti se v mnoha ohledech chovají na internetu zodpovědněji a opatrněji než ty starší, ať už v otázce kontaktu s cizími lidmi nebo ochrany osobních údajů. Předpokládala jsem spíše, že malé děti jsou více naivní a důvěřivé a budou tedy méně obezřetné. Ale ukázalo se, že zatímco mladší děti si své osobní údaje pečlivě střeží a v případě problémů se svěřují rodičům, ti starší své soukromé informace beze strachu vystaví pro všechny přímo ve svém profilu a se svými problémy se svěřují spíše kamarádům nebo si je nechávají pro sebe. Připadají si neohrožené a schopné se o sebe postarat a často podceňují vážnost situace.

Zodpovědnost za bezpečí dětí mají především rodiče, ale vzhledem k tomu, že mnozí rodiče sami sociální sítě nepoužívají a nechtějí používat, chybí jim praktické zkušenosti, a tudíž nemohou děti efektivně poučit. Proto považuju za vhodné například doplnit školní výuku přednáškami Policie ČR nebo nějakého jiného kompetentního institutu o nejrůznějších formách kyberkriminality, které by mohly vhodně doplnit rodičovskou výchovu. A hlavně zavést do škol výuku, zabývající se touto problematikou už v raném věku, nejlépe ještě před tím než na sociální sítě vstoupí. Samozřejmě je nutné ji aplikovat ve formě adekvátní k jejich věku. Nicméně si myslím, že zavádět takovou výuku až u dětí ve věku, kdy Facebook oficiálně smějí používat je příliš pozdě, vzhledem k tomu, že anketa prokázala, že si účty zakládají už mnohem dříve. Děti by měly být se všemi riziky seznámeny dříve, než budou mít šanci s nimi reálně přijít do kontaktu.

9. Seznam použité literatury

1. Symbio: Slovník internetových výrazů. [online]. [cit. 2013-01-29]. Dostupné z: http://www.symbio.cz/slovnik/social-networking-socialni-site.html

2. Bezpečný internet: Co jsou sociální sítě. [online]. [cit. 2013-01-29]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/socialni-site/co-jsou-socialni-site.aspx

3. Jak na facebook: Co je to facebook?. [online]. [cit. 2013-01-29]. Dostupné z: http://www.jaknafacebook.eu/

4. Facemag - magazín o facebooku: Infografika: Klíčové momenty v historii facebooku. [online]. [cit. 2013-01-29]. Dostupné z: http://www.facemag.cz/infografika-klicove-momenty-v-historii-facebooku-cesky/

5. Facebook: Company info. [online]. [cit. 2013-01-29]. Dostupné z: http://newsroom.fb.com/Key-Facts

6. Jak na facebook: Návody. [online]. [cit. 2013-01-29]. Dostupné z: http://www.jaknafacebook.eu/navody-2

7. HARDYN, Michal. Facebook začíná být také českým fenoménem: Úspěchy Facebooku. *DSL.cz* [online]. 2009, 28. 01. 2009 [cit. 2013-01-31]. Dostupné z: http://www.dsl.cz/clanek/1291-facebook-zacina-byt-take-ceskym-fenomenem

8. KLIMEŠ, Jeroným, PhDr. Mgr. Ph.D. Děti a facebook. *Události a názory* [online]. roč. 2010 [cit. 2013-01-30]. Dostupné z: http://klimes.mysteria.cz/clanky/komentare/facebook2.htm

9. Facemag - magazín o facebooku: Jsou vaše děti na Facebooku v bezpečí?. [online]. 13. 7. 2012 [cit. 2013-02-01]. Dostupné z: http://www.facemag.cz/jsou-vase-deti-na-facebooku-v-bezpeci/

10. MACHÁČKOVÁ, Pavla. *Bezpečnost na sociálních sítích s důrazem na ochranu osobních dat*. Brno: Masarykova univerzita, Filozofická fakulta, Ústav české literatury a knihovnictví, 2011. 121 s. Vedoucí diplomové práce Mgr. Pavla Kovářová.

11. Zákon č. 101/2000 Sb. *Zákony ČR* [online]. c2004-2011 [cit. 2011-05-05]. Dostupné z: http://www.zakonycr.cz/seznamy/101-2000-sb-zakon-o-ochrane-osobnich-udaju-a-o-zmene-nekterychzakonu.html

12. Průzkum: Téměř dvě třetiny dětí měly při surfování po internetu negativní zážitky. ECONOMIA, a.s. *Ihned.cz* [online]. 18. 6. 2010 [cit. 2013-02-01]. Dostupné z: http://tech.ihned.cz/c1-44339960-pruzkum-temer-dve-tretiny-deti-mely-pri-surfovani-po-internetu-negativni-zazitky

13. UZEL, Radim, MUDr. CSc. Vliv pornografie na delikventní chování mládeže. *Společnost pro plánování rodiny a sexuální výchovu* [online]. [cit. 2013-02-01]. Dostupné z: http://www.planovanirodiny.cz/view.php?cisloclanku=2006010916

14. Extrémistický a agresivní obsah na internetu ve vztahu k dětem. INTERNET INFO, s.r.o. *Slunečnice.cz: Bezpečnost dětí* [online]. [cit. 2013-02-01]. Dostupné z: http://www.slunecnice.cz/special/bezpecnost-deti/extremisticky-a-agresivni-obsah-na-internetu/

15. Bezpečnější internet: Informace na netu. NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. *Saferinternet.cz* [online]. 2011 [cit. 2013-02-05]. Dostupné z: http://www.saferinternet.cz/pro-rodice/informace-na-netu

16. KOPECKÝ, Kamil a Veronika KREJČÍ. *Rizika virtuální komunikace: příručka pro učitele a rodiče*. Olomouc: NET UNIVERSITY, 2010. ISBN 978-80-254-7866-O. Dostupné z: http://www.google.cz/url?sa=t&rct=j&q=e%20nebezpe%C4%8D%C3%AD%20rizika%20virtu%C3%A1ln%C3%AD%20komunikace&source=web&cd=1&ved=0CC0QFjAA&url=http%3A%2F%2Fwww.e-nebezpeci.cz%2Findex.php%2Fke-stazeni%2Fmaterialy-pro-studium-studie-atd%3Fdownload%3D10%253Abrozura&ei=0hkRUdzPLOeD4AS9zICwDw&usg=AFQjCNHYULvrAU_hZl2MFGoUFqovg3rl_A&bvm=bv.41867550,bs.1,d.d2k&cad=rja

17. KOLÁŘ, Michal. *Nová cesta k léčbě šikany*. Praha: Portál, 2011. ISBN 978-80-7367 - 871-5.

18. ROGERS, Vanessa. *Kyberšikana: Pracovní materiály pro učitele, žáky i studenty*. Praha: Portál, 2011. ISBN 978-80-7367-984-2.

19. Bezpečnější internet: Sexting & Kybergrooming. NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. *Saferinternet.cz* [online]. 2011 [cit. 2013-02-05]. Dostupné z: http://www.saferinternet.cz/pro-rodice/sexting-kybergrooming

20. Bezpečný internet: Krádež identity a jak se jí bránit. [online]. [cit. 2013-02-06]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx

21. O nás. NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. *Saferinternet.cz.* [online]. 2011 [cit. 2013-02-07]. Dostupné z: http://www.saferinternet.cz/o-nas

22. Aktivity. NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. *Saferinternet.cz.* [online]. 2011 [cit. 2013-02-07]. Dostupné z: http://www.saferinternet.cz/aktivity-projektu

23. Protišikaně.cz. NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. *Saferinternet.cz.* [online]. 2011 [cit. 2013-02-08]. Dostupné z: http://proti-sikane.saferinternet.cz/index.asp

24. Mobilstory.cz. NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. *Saferinternet.cz* [online]. 2011 [cit. 2013-02-08]. Dostupné z: http://mobil-story.saferinternet.cz/

25. ICM. NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. *Saferinternet.cz.* [online]. 2011 [cit. 2013-02-22]. Dostupné z: http://www.saferinternet.cz/icm

26. Saferinternet Akademie. NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. *Saferinternet.cz.* [online]. 2011 [cit. 2013-02-22]. Dostupné z: http://www.saferinternet.cz/si.akademie

27. Aktivity: Konference. NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. *Saferinternet.cz.* [online]. 2011 [cit. 2013-02-22]. Dostupné z: http://www.saferinternet.cz/konference

28. MAŠKOVÁ, A., LUKÁŠOVÁ, K., PACÁK, R., a BRANDEJSOVÁ, J. NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. *Brožura ke kampani Praha bezpečně online*. 2011. Dostupné z: http://www.saferinternet.cz/ke-stazeni/letaky

29. Soutěž "Moje soukromí! Nekoukat, nešťourat!". ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *ÚOOÚ* [online]. [cit. 2013-02-22]. Dostupné z: http://www.uoou.cz/uoou.aspx?menu=287&submenu=333

30. O projektu. *Bezpečný internet.cz* [online]. [cit. 2013-02-09]. Dostupné z: http://www.bezpecnyinternet.cz/o-projektu/default.aspx

31. Informace o projektu. CENTRUM PREVENCE RIZIKOVÉ KOMUNIKACE. *E-Bezpečí* [online]. [cit. 2013-02-06]. Dostupné z: http://www.e-bezpeci.cz/index.php/o-projektu/oprojektu

Příloha

Jako příloha je přiloženo úplné znění otázek z dotazníku, který byl použit pro vypracování praktické části práce.

Kolik je Ti let?..... Jsi **dívka/chlapec**

1. **Chodíš na internet?**
   ano/ne

2. **Kde se <u>nejčastěji</u> připojuješ na internet?**
   a) doma
   b) ve škole
   c) u kamaráda
   d) jinde (kde……)

3. **Jak často chodíš na internet?**
   a) denně
   b) 2x až 3x týdně
   c) 1x týdně
   d) méně často

4. **K čemu používáš internet?** (můžeš označit více možností)
   a) práce do školy
   b) vyhledávání (surfování)
   c) hraní her
   d) filmy, videa, hudba
   e) sociální sítě (Facebook, Twitter, Lide.cz, Spoluzaci.cz apod.)
   f) chatování
   g) jen tak zabít volný čas
   h) jiné ……

5. **Hledal jsi někdy na internetu pornografii?**
   ano/ne

6. **Používáš některou sociální síť? (můžeš označit vice možností)**
   a) ne, žádnou
   b) Facebook
   c) Twitter
   d) MySpace
   e) Lide.cz
   f) Spoluzaci.cz
   g) Libimseti.cz
   h) jiné ……..

7. **Máš účet na Facebooku?**
   a) ne, nemám
   b) ano, mám jeden
   c) ano, mám více účtů

8. **Vědí tvoji rodiče, že máš účet na Facebooku?**
   a) ano, vědí o něm
   b) vědí a pravidelně mi ho kontrolují
   c) vědí o jednom, ale mám ještě další účet, o kterém nevědí
   d) nevědí, protože je to nezajímá
   e) nevědí, protože nechci, aby to věděli

9. **Z jakého důvodu sis založil účet na Facebooku?** (uveď hlavní důvod)
   a) protože ho mají kamarádi/příbuzní/známí
   b) abych mohl/a hrát hry na Facebooku
   c) chtěl/a jsem se seznámit s novými lidmi
   d) protože je to cool a mají ho všichni
   e) jiný důvod ……..

10. **Jak často chodíš na Facebook?**
   a) mám ho zapnutý pořád
   b) každý den
   c) 2-3x týdně
   d) 1x týdně
   e) méně často

11. **Kolik máš přátel na Facebooku?** Uveď přibližné číslo: ……

12. **Přijímáš žádosti o přátelství od cizích lidí?**
   a) ano, beru každého
   b) ne, přidávám si jenom kamarády, které dobře znám
   c) někdy ano, někdy ne

13. **Kupuješ si někdy do nějaké hry na Facebooku herní peníze za skutečné peníze?**
   a) ne
   b) ano, koupil/a jsem jednou
   c) ano, koupil/a jsem je vícekrát

14. **Prozrazuješ na Facebooku svoje osobní údaje? (př. telefon, adresa, …)**
   a) mám je vyplněné v profilu
   b) řeknu je každému, kdo se zeptá
   c) neříkám je nikomu

15. **Chtěl se s tebou někdo cizí někdy sejít?**
   a) ne
   b) ano a šel/šla jsem
   c) ano, ale odmítla jsem

16. Oslovil tě někdy někdo, kdo ti připadal podezřelý? Co se ti zdálo podezřelé?
(můžeš označit více možností)

a) ptal se na údaje o mé rodině
b) ptal se kde, bydlím nebo na adresu mojí školy
c) ptal se, jestli bývám sám/a doma
d) chtěl si povídat o sexu
e) poslal mi fotografii, na které byl obnažený nebo chtěl takovou fotografii ode mě
f) chtěl se se mnou sejít
g) ponižoval mě nebo mi vyhrožoval
h) nic takového
i) něco jiného: ……

17. Pokud (by) ses setkal/a s nějakým jevem z minulé otázky, řekl/a (bys) o tom někomu?

a) nikomu
b) rodičům
c) kamarádům
d) učiteli
e) zavolal/a bych na linku bezpečí

18. Zajímají se rodiče o to, co děláš na internetu? Kontrolují tě?
ano/ne

19. Poučují tě rodiče o tom, co je bezpečné dělat na internetu a co ne, případně, že některé stránky jsou špatné apod.?
ano/ne