

Česká zemědělská univerzita v Praze

Institut vzdělávání a poradenství

Katedra celoživotního vzdělávání a podpory studia



**Česká
zemědělská
univerzita
v Praze**

**Poradenství o bezpečnosti v kybernetickém
prostředí pro dospělé v roli rodičů**

Bakalářská práce

Autor: Hana Janelová

Vedoucí práce: PhDr. Lucie Smékalová, Ph.D. et Ph.D.

2021

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Institut vzdělávání a poradenství

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Hana Janelová

Specializace v pedagogice
Poradenství v odborném vzdělávání

Název práce

Poradenství o bezpečnosti v kybernetickém prostředí pro dospělé v roli rodičů

Název anglicky

Advice on security in the cyber environment for adults in the role of parents

Cíle práce

Cílem práce je popsat rizika v kybernetickém prostředí, zmapovat povědomí dospělých v roli rodičů o bezpečnosti v kybernetickém prostředí a zjistit jejich orientaci v sociálních sítích. Dále poskytnout rady dané cílové skupině o dodržování bezpečnosti v dotčené problematice.

Metodika

1. Studium vybrané problematiky v dostupných informačních zdrojích a průběžné konzultace s vedoucí práce.
2. Vymezení terminologie a deskripce teoretických východisek.
3. Vymezení předmětu: Popis tematiky bezpečnosti v kybernetickém prostředí a na sociálních sítích a zmapovat u cílové skupiny prostřednictvím průzkumného šetření nástrojem dotazníku dle věku dětí rodičů jejich obeznámenost. Vyhodnocení dat a doporučení pro rodiče.
4. Vyvození závěru, soupis literatury, korekce formálních a stylistických náležitostí.

Harmonogram zpracování: Kompletní pracovní verzi práce odevzdat vedoucí práce do konce února 2021 (kombinovaní studenti). Finální verzi práce odevzdat na studijní oddělení do konce března 2021.

Doporučený rozsah práce

Dle pravidel pro psaní bakalářské práce.

Klíčová slova

Sociální sítě, kyberprostor, informovanost rodičů, typy sociálních sítí, rizika, bezpečnost

Doporučené zdroje informací

- Černá, Alena et al. Kyberšikana: průvodce novým fenoménem. Vyd. 1. Praha: Grada, 2013. 150 s. Psyché. ISBN 978-80-210-6374-7.
- Dočekal, Daniel a kol. Dítě v síti: manuál pro rodiče a učitele, kteří chtějí rozumět digitálnímu světu mladé generace. První vydání. Praha: Mladá fronta, 2019. 207 stran. Flowee. ISBN 978-80-204-5145-3.
- Eckertová, Lenka a Dočekal, Daniel. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. 1. vyd. Brno: Computer Press, 2013. 224 s. ISBN 978-80-251-3804-5.
- Hulanová, Lenka. Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality. 1. vyd. Praha: Triton, 2012. 217 s. ISBN 978-80-7387-545-9.
- Ševčíková, Anna a kol. Děti a dospívající online: vybraná rizika používání internetu. Vyd. 1. Praha: Grada, 2014. 183 s. Psyché. ISBN 978-80-210-7527-6.

Předběžný termín obhajoby

2020/21 LS – IVP

Vedoucí práce

PhDr. Lucie Smékalová, Ph.D. et Ph.D.

Garantující pracoviště

Katedra celoživotního vzdělávání a podpory studia

Elektronicky schváleno dne 3. 2. 2021

PhDr. Lucie Smékalová, Ph.D. et Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 2. 2021

Ing. Karel Němejc, Ph.D.

Pověřený ředitel

V Praze dne 14. 03. 2021

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci na téma:

Poradenství o bezpečnosti v kybernetickém prostředí pro dospělé v roli rodičů

vypracovala samostatně a citovala jsem všechny informační zdroje, které jsem v práci použila a které jsem rovněž uvedla na konci práce v seznamu použitých informačních zdrojů.

Jsem si vědoma že, na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

Jsem si vědoma, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to bez ohledu na výsledek její obhajoby.

Svým podpisem rovněž prohlašuji, že elektronická verze práce je totožná s verzí tištěnou a že s údaji uvedenými v práci bylo nakládáno v souvislosti s GDPR.

V Praze dne 17. března 2021

.....

(podpis autora práce)

PODĚKOVÁNÍ

Ráda bych touto cestou poděkovala své vedoucí bakalářské práce, PhDr. Lucii Smékalové, Ph.D. et Ph.D., za odborné vedení a věcné připomínky během zpracování této bakalářské práce. Dále bych chtěla poděkovat svému manželovi za podporu, vstřícnost a péči o syny, bez něžž by bylo dokončení celého studia obtížné.

Abstrakt

Cílem této bakalářské práce bylo zjistit, jaké povědomí o rizicích v kybernetickém prostředí mají dospělí v roli rodičů a na základě vyhodnocení dotazníkového šetření poskytnout doporučení, jak případným rizikům čelit. V teoretické části této práce jsem se věnovala definování základních pojmů souvisejících s kybernetickým prostorem, základnímu rozdělení sociálních sítí a vyjmenování nejčastěji používaných. V neposlední řadě popisují rizika spojená s využíváním sociálních sítí a právní postizitelnost nebezpečného chování. Praktická část je sestavena z vyhodnocení dotazníkového šetření, které probíhalo mezi rodiči žáků 5. - 9. třídy základní školy. Prostřednictvím anonymního online dotazníku byli rodiče dotazováni, jaké sociální sítě používají oni sami a jejich děti, a jakým způsobem se snaží předcházet rizikům spojených s online světem. Také uváděli, jaká rizika kybernetického prostředí znají. Na základě vyhodnocení průzkumu byly sestaveny doporučující body, které působí preventivně. Práce je doplněna tabulkou s výčtem trestných činů, kterých se může pachatel dopustit při svém jednání v kybernetickém prostředí.

Klíčová slova

sociální sítě, kybernetický prostor, informovanost rodičů, rizika, bezpečnost

Abstract

The aim of this bachelor's thesis was to find out what awareness of risks in the cyber environment of adults have in the role of parents and based on the evaluation of the questionnaire survey to provide recommendations on how to deal with potential risks. In the theoretical part of this work, I focused on defining the basic concepts related to cyberspace, the basic division of social networks and listing the most commonly used. Last but not least, I describe the risks associated with the use of social networks and the legal vulnerability of dangerous behavior. The practical part is composed of the evaluation of a questionnaire survey, which took place among the parents of pupils in the 5th - 9th grade of primary school. Through an anonymous online questionnaire, parents were asked what social networks they and their children use, and how they try to prevent the risks associated with the online world. They also mentioned what risks the cyber environment knows. Based on the evaluation of the survey, recommendation points were compiled that have a preventive effect. The work is supplemented by a table with a list of crimes that the offender can commit in his actions in the cyber environment.

Keywords

social networks, cyberspace, parental awareness, risks, security

OBSAH

ÚVOD.....	11
TEORETICKÁ ČÁST	12
1 Cíl a metodika.....	12
2 Internet a sociální sítě.....	13
2.1 Definice internetu.....	13
2.2 Definice kyberprostoru.....	13
2.3 Definice sociální sítě	14
3 Sociální sítě a jejich dělení	15
3.1 Profilové sociální sítě.....	15
3.1.1 Facebook.....	16
3.1.2 LinkedIn	17
3.2 Obsahové sociální sítě.....	17
3.2.1. You Tube	17
3.2.2 Instagram	18
3.2.3 Pinterest	18
3.2.4 Tik Tok	19
3.3 Mikro-blogovací sociální sítě.....	19
3.3.1 Twitter	20
3.4 Komunikační služby.....	20
3.4.1 WhatsApp	20
4 Rizikové chování na sociálních sítích	21
4.1 Kyberšikana.....	22
4.1.1 Definice pojmů	22
4.1.2 Účastníci kyberšikany	23

4.1.3	Projevy kyberšikany	24
4.2	Kybergrooming	24
4.3	Kyberstalking	24
4.4	Sexting.....	25
4.5	Phising.....	25
4.6	Ostrakizace	25
4.7	Hoax	26
4.8	Viry a spamy	26
4.9	Závislost	26
5	Právní úprava v České republice	28
6	Organizace a projekty zabývající se prevencí a vzděláváním	29
6.1	E-bezpečí – www.e-bezpeci.cz	29
6.2	Bezpečný internet – www.bezpecnyinternet.cz	29
6.3	Národní centrála bezpečného internetu – www.NCBI.cz	29
6.4	Dětské krizové centrum – www.ditekrize.cz	30
6.5	Kraje pro bezpečný internet – www.KPBI.cz	30
	PRAKTICKÁ ČÁST	31
7	Dotazníkové šetření	31
7.1	Cíl průzkumného šetření	31
7.2	Charakteristika regionu a respondentů.....	31
7.3	Metoda dotazníku.....	32
7.4	Popis a interpretace dat	32
7.5	Závěr dotazníkového šetření	49
7.6	Doporučení pro rodiče.....	49
7.6.1	Preventivní opatření.....	49

7.6.2 Řešení problému	51
ZÁVĚR	53
SEZNAM POUŽITÝCH ZDROJŮ	55
SEZNAM GRAFŮ A OBRÁZKŮ	59
SEZNAM PŘÍLOH.....	61

ÚVOD

Toto téma jsem si vybrala s ohledem na mou profesi policejního preventisty, kdy tato práce obnáší převážně diskuse se žáky ZŠ a SŠ na různá preventivní témata. V posledních letech je jedním z nich také téma kyberprostor a bezpečné chování v něm. V loňském roce na toto téma byl do kin uveden dokumentární film „V síti“, režisérů Víta Klusáka a Barbory Chalupové, který sklidil nebývalý úspěch. Film se věnuje problematice rizikové online komunikace dětí s ostatními uživateli internetových služeb. Spoustě lidí otevřel oči, co se týče fungování dětí a mladistvých na internetu, sociálních sítích a v kyberprostoru vůbec.

Ve své bakalářské práci bych se ráda zaměřila na povědomí rodičů o rizicích v kyberprostoru. Jsou to v první řadě hlavně rodiče, kdo své dítě chrání a učí ho novým dovednostem. Fungují jako první článek prevence. Proto je důležité, aby oni sami měli dostatečné znalosti o případných rizicích, která mohou jejich děti v kyberprostoru ohrozit. Rodič by měl být připraven poskytnout dítěti dostatečné informace, ale zároveň dítě i pozitivně ovlivňovat ke smysluplnému využívání online prostředí.

Rozvoj informačních technologií je stále rychlejší a převážná většina populace je jejich uživatelem. Nejen rodiče, ale v dnešní době i většina dětí, tráví spoustu svého času na internetu a sociálních sítích. Bohužel ani dospělí, ani děti si často nějaká rizika či nebezpečí nepřipouštějí. Nejohroženější skupinou jsou děti okolo 10 let, které se stávají poprvé uživateli internetu a sociálních sítích. Vzhledem ke svému věku, nemají tyto uživatelé dostatečně vyvinuté rozlišovací schopnosti a psychickou zralost. Proto se stávají snadnou kořistí predátorů, pohybujících se právě v rozlehlých vodách internetu a sociálních sítích. Stejně jako učíme děti opatrnosti např. v dopravním provozu a samotné fungování mimo bezpečí domova, je nutné předat jim co nejvíce informací o možných nástrahách i ve virtuálním světě.

TEORETICKÁ ČÁST

1 Cíl a metodika

Cílem bakalářské práce je popsat rizika v kybernetickém prostředí, kde uživatelé čteně využívají sociální sítě a jsou jimi také do značné míry ovlivňováni. Dále jsem chtěla zmapovat povědomí dospělých v roli rodičů o bezpečnosti v kybernetickém prostředí a zjistit jejich orientaci v sociálních sítích. Rodiče by měli být primárně ti, co své děti upozorní na různá rizika vyskytující se v kybernetickém prostředí. V návaznosti na předešlé informace mě také zajímala otázka preventivních opatření ze stran rodičů směrem k dětem a používání sociálních sítí. V závěrečné části pak uvádím rady pro danou cílovou skupinu týkající se dodržování bezpečnosti v dotčené problematice.

První část bakalářské práce je zaměřena na charakteristiku nejčastěji používaných sociálních sítí a vymezení základních pojmů týkajících se kybernetického prostředí. Dále upozorňuji na rizika spojená s používáním sociálních sítí, např. kyberšikana, kybergrooming a závislost.

Druhá část bakalářské práce obsahuje dotazníkové šetření směřované na zjištění povědomí rodičů o rizicích v kybernetickém prostředí. Součástí dotazníku jsou i rady pro:

- preventivní opatření, jak předcházet rizikům v kybernetickém prostředí;
- případná doporučení na postup při řešení již vzniklého problému.

2 Internet a sociální sítě

Se sociálními sítěmi se setkáváme téměř na každém našem kroku nejen na internetu, ale už i v reálném životě. To, že máme založený profil na nějaké sociální síti, se stává samozřejmostí a v některých kruzích dokonce společenskou povinností.

Pro lepší pochopení je nutné definovat si základní pojmy, související s online prostředím, které pro laiky mohou působit jako totožné. Nicméně jejich význam je různý.

2.1 Definice internetu

„Internet je komplexní, celosvětová počítačová síť (WAN – Wide Area Network – rozlehlá počítačová síť), ve které jsou propojeny jednotlivé počítače a počítačové systémy“ (Schellmann et. al. 2004, s. 284). Samotné slovo internet pocházející z anglických slov „inter“ a „net“, lze přeložit jako vnitřní síť.

2.2 Definice kyberprostoru

Encyklopedie Britannica vysvětluje kyberprostor jako „virtuální svět tvořený propojením počítačů, zařízení s přístupem k internetu, serverů, routerů a jiných komponentů internetové infrastruktury“ (Britannica.com, 2021).

Jako první použil termín kyberprostor autor sci-fi William Gibson v roce 1982 ve své povídce Burning Chrome a později v roce 1984 v knize Neuromancer:

„Kyberprostor. Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky... Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyšlitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města, ustupující...“ (Gibson, 1998, s. 58).

Kyberprostor (angl. cyberplace) je prostředí, které „utváří celosvětové propojení počítačů. Termín zároveň označuje hmotnou infrastrukturu digitální komunikace, nesmírné množství informací v síti, stejně jako osoby, které je užívají, stahují, sdílejí a zásobují“ (Šmahaj, 2014, s. 15).

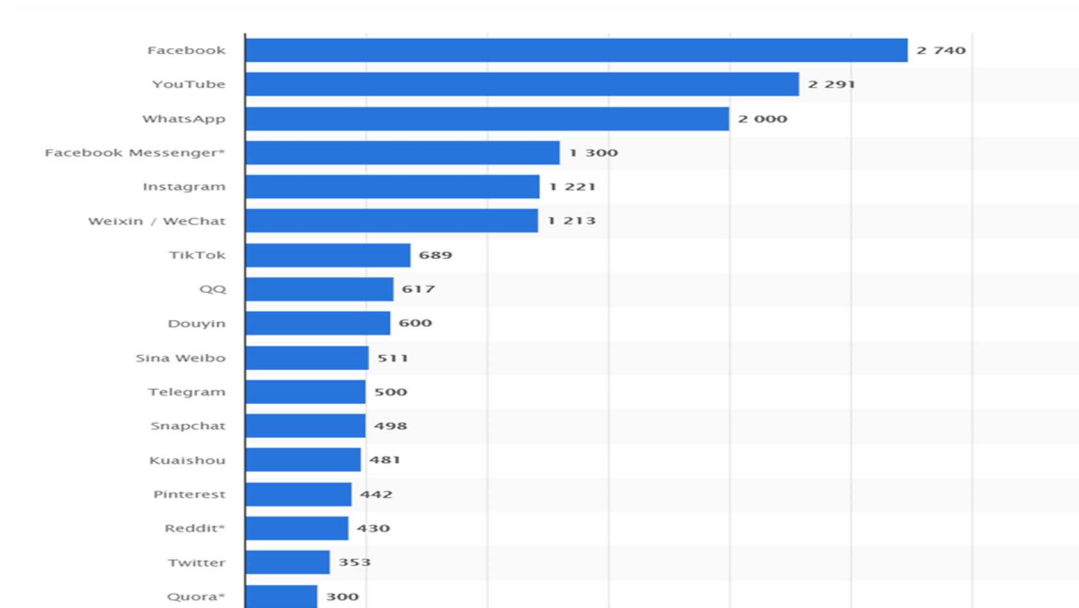
Z výše uvedených definic lze usoudit, že internet je globální síť tvořena fyzickými servery. Naproti tomu kyberprostor je spíše jakýmsi symbolickým vyjádřením onoho nehmotného (nehmatatelného) světa, připomínající nekonečný vesmír.

2.3 Definice sociální sítě

„Specifickým prostředkem komunikace v rámci internetu jsou tzv. sociální sítě (angl. Social Networks). Jak již název „sociální“ napovídá jedná se o společenské propojení. Internetovou sociální sítí tvoří jednotliví uživatelé, které vzájemně spojuje přátelství, příbuzenské vztahy nebo společné zájmy“ (Vašutová, 2010, s. 43). Mezi nejpočetnější patří např. Facebook, Instagram, Twitter, aj.

Sociální síť je místo na Internetu, kde můžeme s ostatními lidmi sdílet informace, fotografie, videa či své pocity. Díky těmto sítím se lidé mohou něčemu přiučit, mohou si navzájem pomoci, mohou se vyslechnout nebo se také seznámit. Jedná se o virtuální prostor, kde spolu komunikují dva nebo více uživatelů Internetu. Každá sociální síť požaduje před použitím založení takzvaného profilu. Jedná se o registraci na určité internetové stránce, na námi vybrané sociální síti. Dle odhadů existuje zhruba 200 sociálních sítí, které využívá až 46 % celosvětové populace.

Graf 1: Nejpoužívanější sociální sítě na světě k lednu 2021, seřazené dle počtu aktivních uživatelů (v milionech)



Zdroj: Statista.com, 2021

3 Sociální sítě a jejich dělení

Pro současnou generaci mladých lidí jsou sociální sítě nezbytnou součástí života. Život bez nich si již nedovedou představit. Hlavní přínos sociálních sítí je v umožnění komunikace, jež nezná hranic. „Tím, že umožňuje komunikaci lidí různých národností, vytváří jakousi on-line komunitu, ve které se každý uživatel internetu může cítit jejím právoplatným členem. Dalo by se říct, že internet boří hranice, a to nejen hranice geografické, ale i hranice související s věkem, pohlavím, sociální třídou, rasou a náboženstvím“ (Hulanová, 2012, s. 24).

Sociální sítě můžeme rozdělit do několika kategorií. Touto problematikou se zabývá několik autorů, kdy každý využívá jiný způsob dělení, např. socializační, osobní, profesní, navigační aj. Já jsem si vybrala dělení uváděná na webu www.chapiteau.cz, a to následující:

- profilově založené – Facebook, LinkedIn,
- obsahově založené – YouTube, Instagram, Snapchat, Pinterest,
- mikro – blogovací – Twitter,
- komunikační služby – Facebook Messenger, WhatsApp, Viber.

3.1 Profilové sociální sítě

Pro přihlášení do konkrétní sociální sítě, si musí každý uživatel založit svůj profil (účet, registrace). Jedná se o virtuální vizitku s osobními údaji, kterými se poté na sociální síti prezentuje a je podle nich dohledatelný a identifikovatelný pro ostatní. Kromě jména to mohou být údaje jako: místo bydliště, fotografie, stručný životopis, informace o dosaženém vzdělání, o rodinném stavu, možnostech kontaktování, vlastních zálibách atd. Onu viditelnost citlivých údajů lze omezit nastavením správné ochrany soukromí, které je nutné věnovat patřičnou pozornost při samotném zakládání profilu na jakékoli sociální síti.

3.1.1 Facebook

Málokdo dnes nemá tušení, co je Facebook. Zřejmě ani Mark Zuckerberg v roce 2004 neměl ponětí, jaké obliby se jeho síti dostane. Na počátku se svým spolužákem Edduardem Severinem naprogramoval síť pro studenty Harvardské univerzity, a časem se přidávaly ostatní americké univerzity, později i zahraniční. První českou univerzitou, jež se připojila, byla Masarykova univerzita v Brně. Od 26.9.2006 se mohl na síť Facebook připojit jakékoli osoba, starší 13 let. Toto je odůvodněno původem sítě. Jedná se o americkou síť. V USA je zákon zakazující používání osobních údajů dětí mladších 13 let ke komerčním účelům. Když pomineme tento zákon, můžeme říct, že do určitého věku dítěte, není dostatečně vyspělé a také většinou nezná zásady bezpečného chování na sociálních sítích.

Dnes je tato síť nejznámější a nejpoužívanější sociální sítí na světě, kdy poskytuje své služby více než 2,5 miliardám registrovaných uživatelů. Facebook je primárně určen ke sdílení informací a dat v okruhu svých přátel nebo fanoušků. Přátele, jež tvoří základ, lze získat vzájemným potvrzením a dále je umožněno sledovat jejich příspěvky. Registrace a následné užívání Facebooku není zpoplatněno. Je tomu proto, že je financován pomocí reklam. Čím je síť významnější, tím více přitahuje inzerenty.

Facebook poskytuje nespočet výhod, namátkou můžeme jmenovat rychlou komunikaci a snadný kontakt s osobami fyzicky vzdálenými. Spojení několika služeb v jedné, např. vyhledávání různých služeb a zboží v mapách, inzerování čehokoli, kalendář s upomínkou na narozeniny přátel, plánování aktivit v návaznosti na konané akce v okolí a dle zájmu uživatele. Velkým přínosem je sdílení informací na Facebooku pro charitativní akce, jež si nemohou dovolit drahou placenou propagaci.

Nicméně můžeme uvést i nevýhody této sociální sítě, do nichž patří např. zanechání digitální stopy, kterou svým pobytem na sítích tvoříme. Další negativní stranou jsou informace o naší poloze, četnosti využívání sociálních sítí, nejčastěji vyhledávaných produktech, službách, druh oblíbené hudby. Tyto informace slouží Facebooku, např. k lepšímu cílení reklamy. Všechny uvedené příklady jsou pro jmenovanou síť cenným artiklem, umožňující rozvoj jejich obchodu.

3.1.2 LinkedIn

Jedná se o propojení lidí, hledající práci nebo komunikující s potenciálními zaměstnavateli po celém světě. Zároveň dovoluje veřejně publikovat uživateli přednosti v profesní sféře a navazovat vztahy s lidmi z vybraného odvětví. Byl založen v roce 2002 a dnes je využíván více jak 280 miliony lidí z celého světa.

Web sitevhrsti.cz objasňuje důvod vzniku sítě takto: „Sociální síť LinkedIn byla vytvořena pro zvýšení šancí na pracovním trhu, díky zviditelnění uživatele. Původně určena pro profesionály a freelancery, dnes však pro širokou skupinu OSVČ i zaměstnanců“ (Sítě v hrsti.cz, 2021).

3.2 Obsahové sociální sítě

Hlavním pilířem těchto sítí je samotný obsah, nikoli sám uživatel. Je to kombinace uměleckého, osobního a profesního obsahu, kterými se uživatel projevuje.

3.2.1. You Tube

Nejpoužívanější a nejznámější sociální síť pro ukládání videozáznamů na internet. Ty lze pak jednoduše umístit na web nebo sdílet dalším uživatelům pomocí jiných sociálních sítí.

Základním principem této sítě je sdílení videa mezi širokým publikem. YouTube tvoří dvě skupiny uživatelů – přispěvatelé a publikum. Pro pasivní publikum není nutná registrace, takže sledující může zcela anonymně sledovat vybraná videa po libovolnou dobu. Registrovanému uživateli je umožněno používat několik jednoduchých funkcí. Má možnost nahrávat vlastní videa, vytvářet playlisty s oblíbenými videi a komentovat videa vlastní, ale i ostatních uživatelů. Stejně jako na Facebooku i na YouTube existuje tlačítko „Líbí se mi“. Na rozdíl od Facebooku je tu i tlačítko „Nelíbí se mi“. Uživatel se přihlašuje k odběrům různých kanálů ať už umělců, televizních pořadů či amatérů a jejich videa se pak uživateli zobrazují na jeho hlavní stránce.

YouTube obsahuje velké množství videí z různých kategorií. Nalezneme zde hudbu, sport, návody, ale také vzdělávací a osvětová videa.

„YouTube díky svému širokému záběru umí být skvělým učitelem a zdrojem mnoha zajímavých informací. Na druhou stranu, ale stejně jako jiné sociální sítě, skrývá mnoho videí, které mohou potenciálně škodit. Jedná se o nevhodná videa např. s násilným či sexuálním motivem. Vzhledem k velkému počtu denně přidaných videí, je těžké včasné odhalení všech nevhodných videí a jejich následné smazání. Pokud se navíc jedná o nějakou „senzaci“ nebo tzv. virál, je pravděpodobné, že ve chvíli, kdy YouTube originál daného videa zakáže, jeho kopie budou dál kolovat internetem. I zde platí pravidlo, že co jednou dáš na internet, zůstane tam navždy“ (Knollová, Křivánková, Šutová, 2019, str. 19).

3.2.2 Instagram

„Instagram je bezplatná aplikace pro sdílení fotek a videí, která je dostupná pro iPhone a zařízení se systémem Android. Lidé mohou na Instagram nahrát fotky a videa a pak se o ně podělit se svými sledujícími nebo s vybranou skupinou přátel“ (Facebook.com, 2021).

Instagram není jen obyčejné sdílení fotek z každodenního života. Základním principem je vyfotit cokoli více či méně zajímavého, použít či nepoužít jeden z předpřipravených grafických filtrů a sdílet. Podstatou je vytvoření téměř uměleckého díla z původní fotky, která zobrazuje běžné činnosti netradičně.

Osoba prezentující se na Instagramu a používající ho jako prostředek k získání peněz z reklamních sdělení, se nazývá influencer. Jde o uživatele internetu, který svým chováním dokáže ovlivnit chování ostatních uživatelů a důvěryhodnou cestou jim nabídnout nějaký produkt. Marketingové kampaně takto fungují prostřednictvím známých osobností, kdy můžeme jmenovat např. Petra Čecha nebo Leoše Mareše.

3.2.3 Pinterest

Jedná se o online nástroj umožňující jeho registrovaným uživatelům vytváření online nástěnek a specifičtěji vyhledávat obsah odpovídající jejich zájmům mezi velkým množstvím obrázků, tzv. pinů. Na jednom místě může uživatel najít spoustu nápadů, objevovat, vyhledávat mezi nimi a vracet se k nim. Pinterest se tak stal alternativou k běžným vyhledávačům.

Samotný obsah Pinterestu se dělí do několika různých kategorií, mezi které patří např. architektura, vzdělávání, móda, cestování, jídlo a pití, výzdoba interiérů a další. Sociální rozměr Pinterestu spočívá ve sledování ostatních uživatelů, tzv. pinnerů. Každý pinner si může zcela nezávazně vybrat, zda bude sledovat všechny nástěnky daného uživatele, nebo jen ty, které opravdu odpovídají jeho zájmům.

3.2.4 Tik Tok

Web www.digitalninomadstvi.cz charakterizuje TikTok jako: „sociální síť pro vytváření a sdílení krátkých, zpravidla, zábavných videí. Jde původem o čínskou sociální síť, jež si získává popularitu na celém světě. Mobilní aplikace umožňuje uživatelům vytvářet krátké videoklipy o délce 3–60 vteřin na téma tancování, karaoke, dovednostní kreace či vtipné skeče“ (Digitální nomádi.cz, 2021).

Pro pouhé sledování videí, není nutné založení účtu. V případě zájmu přidávat videa na TikTok je již registrace a vytvoření vlastního účtu podmínkou. Registrace je povolena uživatelům po dovršení 13 let. Nicméně v praxi jde o odkliknutí daného věku a odsouhlasení podmínek užívání aplikace. K žádné další kontrole věku uživatele již nedochází.

I tato sociální síť má svá bezpečnostní rizika, která si mladí uživatelé neuvědomují. Také rychlý vzestup uvedené sítě zapříčiňuje i neznalost rodičů v tomto prostředí. Aplikaci nelze blokovat rodičovskou kontrolou, tudíž se v tomto prostředí mohou děti pohybovat bez jakéhokoli omezení. Málomocný uživatel si při založení profilu všimne automatického nastavení na veřejný. To umožňuje komukoli sledovat obsah uživatele a psát jim zprávy různého charakteru.

3.3 Mikro-blogovací sociální sítě

Dovolují svému uživateli psát a publikovat krátké zprávy, které jsou limitovány délkou a formou.

3.3.1 Twitter

Jedná se o mikro-blogovací sociální síť, kterou spoluzaložil Jack Dorsey v roce 2006 (Lupa.cz, 2021). V počátcích nabízela svým uživatelům sdělit informaci ve 140 znacích. V roce 2017 se však tento počet navýšil na 280 znaků, známých jako tweety. Na Twitteru se většinou objevují nové informace jako první. Je využíván mnoha médii i známými osobnostmi ke sdílení informací v reálném čase.

Twitter využívá tzv. #hashtagy, které fungují jako klíčová slova, shromažďující nejpodobnější informace pod zadanými hesly. Hashtagy jsou na této síti velmi populární, lze je též vidět i na Instagramu či Facebooku, ale ne v takové míře.

3.4 Komunikační služby

Tyto sítě umožňují rychlé přesuny informací mezi jednotlivými uživateli. K dispozici jsou po datovém připojení.

3.4.1 WhatsApp

WhatsApp Messenger, nebo jednoduše WhatsApp, je americká služba zasílání zpráv, vlastněná společností Facebook, Inc. Umožňuje uživatelům odesílat textové zprávy a hlasové zprávy, uskutečňovat hlasové a videohovory, a sdílet obrázky, dokumenty, umístění uživatelů a další obsah.

Přes 2 miliardy lidí ve více než 180 zemích používají aplikaci WhatsApp ke komunikaci s přáteli a rodinou – kdykoli a kdekoli. WhatsApp je zdarma a nabízí jednoduché, bezpečné a spolehlivé vedení hovorů a posílání zpráv, dostupné na telefonech po celém světě. „Všechny sdílený materiál je chráněn koncovým šifrováním, což zabraňuje, aby skončil v nesprávných rukou“ (WhatsApp.com, 2021).

Posílání zpráv je u WhatsAppu zdarma, pouze je vyžadováno internetové připojení. Tímto způsobem se uživatel může vyhnout poplatkům např. za SMS zprávy.

„Přes WhatsApp je možné komunikovat i ve velkých skupinách, kdy lze sdílet vybraný obsah až s 256 lidmi najednou“ (WhatsApp.com, 2021).

4 Rizikové chování na sociálních sítích

Moderní doba s sebou přináší moderní informační a komunikační technologie a jejich častější využívání v běžném každodenním životě. I zde je nutné mít na paměti, že nás mohou nemile překvapit. Proto je důležité dodržovat určité zásady bezpečného chování na internetu a sociálních sítích, stejně jako dodržujeme pravidla v reálném světě.

Používání informačních technologií je, nejen mezi dětmi, stále rozšířenější. Stále více žáků druhého stupně základní školy má svůj účet na některé ze sociálních sítí a denně se pohybuje v prostředí kyberprostoru. Sociální sítě jsou zdrojem velkého množství informací, které ne každý zvládne patřičně zpracovat. Zároveň nám mimo jiné umožňují komunikovat na nemalé vzdálenosti s lidmi z celého světa. Ne vždy se jedná o naše blízké, se kterými nám není umožněn osobní kontakt. V dnešní době virtuálního světa je kontakt s druhým člověkem neosobní, často nahrazuje tzv. face to face setkání. Nemůžeme si být jisti, kdo se opravdu skrývá za profilem, s nímž komunikujeme. Kdokoliv si může založit profil s falešným jménem, fotografií a údaji a vytvořit si zcela novou identitu.

Nejvíce ohroženou skupinou, která se dostává do nepříjemných situací na sociálních sítích, jsou děti a mladiství. Jde vlastně o tzv. Generaci Z, jejíž příslušníci se narodili v letech 1997-2012. Tato generace žije od samého počátku svého života v online prostředí, jež vnímá jako běžnou součást svého života. Internet se pro mladou generaci stal nezbytnou součástí jejich každodennosti. „Děje v online a offline světě vnímají jako navzájem propojené a vyznačit mezi nimi přesnou hranici by mohlo být obtížné.“ (Ševčíková a kol., 2013, 31). Předchozí generace jejich rodičů, patřící do Generace X nebo Y, moderní technologie do svých životů začleňovali postupně. Znalosti o fungování internetu si předávali vzájemně a případná rizika objevovali víceméně náhodou. Mohou tedy rodiče z uvedených generací být právě málo flexibilní ve vztahu k bezpečnosti na internetu nebo je tomu naopak? Dokážou porozumět a následně využívat rychle se vyvíjející moderní technologie?

Definice pojmu riziko

Ševčíková (2014, str. 9) pojem riziko specifikuje jako „jakákoliv nežádoucí událost, jež může, ale také nemusí nastat“, a dále uvádí, že se může jednat o „ohrožení jedince ať už po psychické, tělesné či materiální stránce.“ Autorka se následně zabývá přímo riziky spojenými s užíváním internetu, kde uvádí klasifikaci online rizik podle Livingstona a Haddona (2009) (v Ševčíková, 2014, str. 9,10). Ty jsou vymezeny čtyřmi typy rizik a to komerční, agresivní, sexuální a hodnotového rázu.

Také Eckertová a Dočekal (2013) vymezují rizika hrozící na internetu, těmi je komunikace s nevhodnými lidmi – kybergrooming (agresivní devianti s pedofilními sklony v internetovém prostředí). Dále kyberšikana, ke které patří Happy Slapping (natáčení reálného fyzického útoku), Kyberstalking (pronásledování a obtěžování za využití internetu) a Sexting (zasílání nebo sdílení vlastních odhalených fotografií, videozáznamů nebo textů), dále jako rizikový označují nevhodný obsah jako je pornografie, extremismus, násilí atd. Také „počítačová havěť“, mezi kterou řadí viry, spamy (nevyžádané zprávy), hoaxy (nepravdivé informace), phishing (získávání přihlašovacích údajů a hesel), dále závislost na internetu a hrách, ovlivňování komercí a reklamou, online nakupování a nakonec nekritické přejímání informací z internetu.

V následující řádcích si přiblížíme nejčastěji uváděná rizika, která mohou mladí uživatelé na sociálních sítích potkat.

4.1 Kyberšikana

Jak již název napovídá, jedná se o šikanu vedenou v kyberprostoru. Mezi kyberšikanou a šikanou je nepatrná hranice, kdy může docházet i k vzájemnému prolínání v reálném a online prostředí. Podobnost je hlavně v projevech a základních rysech. Pro lepší názornost podobnosti si oba pojmy definujeme.

4.1.1 Definice pojmů

Šikana

Dle pedagogického slovníku je šikana definována jako fyzické, psychické či kombinované ponižování až týrání žáků obvykle jinými žáky, vzácněji dospělými (Průcha, Walterová, Mareš, 2011, s. 238).

Kyberšikana

Jednoduchou, ale výstižnou definici kyberšikany uvádí L. Hulanová: „Kyberšikana je specifický druh šikany, který využívá internet, mobilní telefony a další nástroje moderních komunikačních technologií za účelem ublížení či zesměšnění jiné osoby“ (Hulanová, 2012, s. 37).

Matoucí v určení kyberšikany může být to, že „V procesu kyberšikany se nevyskytují přímé znaky šikanování, jako jsou zranění, roztrhané oblečení, ztráta věcí, peněz apod., což znesnadňuje identifikaci oběti jejím okolím“ (Hulanová, 2012, s. 48).

Nejčastějším rozdílem bývá větší skrytí kyberšikany, neboť nekonečný kyberprostor umožňuje agresorovi vystupovat zcela anonymně. Útočník tak ztrácí zábrany a spoléhá na strach oběti se někomu svěřit. Proto agresorovi útoky mohou být časově téměř neomezené.

4.1.2 Účastníci kyberšikany

Oběť

Stejně jako u klasické šikany se obětí stávají jedinci se sníženou schopností se bránit. Oběť se může cítit bezmocná a neschopná, protože se nemůže bránit proti útokům neznámého agresora. Často zůstává na řešení problému sama, neboť se může obávat reakcí okolí, případně se stydět (Hulanová, 2012, s. 48).

Agresor

Útočníkem může být kdokoliv, role účastníků kyberšikany se často vzájemně střídají. Není podmínkou, že jde o silného jedince co do fyzických dispozic. „Agresorem se stává jedinec silný v informačních technologiích – může to být prakticky kdokoli“ (Hulanová, 2012, s. 48).

Přihlízející

U kyberšikany proto častěji hrozí, že přihlízející se svou (i pasivní) reakcí přidají na stranu agresora (mlčení znamená souhlas, což si agresor může vyložit jako podporu svého jednání), přičemž často ani nemusí odhadnout skutečné důsledky svého jednání. (Černá, 2013, s. 74–75).

4.1.3 Projevy kyberšikany

K základním projevům kyberšikany patří zasílání obtěžujících, ponižujících a útočných zpráv pomocí moderních technologií. Lze brát v úvahu i vytváření blogů, které svým obsahem ponižují, zesměšňují daného jedince či skupinu. Dále může jít o fyzické napadání oběti a úmyslné provokování, spojené s natáčením videa, které je dále umístováno na sociální síť (Internetem bezpečně.cz, 2021).

4.2 Kybergrooming

Zjednodušeně můžeme takto nazvat nevhodnou a nebezpečnou komunikaci s neznámými lidmi, která cíhá na uživatele internetu, především na sociálních sítích. Velkým problémem je zveřejňování citlivých informací a následná ochota uživatelů, nejen si psát, ale i potkat se s lidmi, které znají pouze z online prostředí. Jedná se o největší riziko pro náctileté uživatele. Nejčastější obětí bývají dívky ve věku 11-17 let, které mají nízké sebevědomí a cítí se osamělé. Cílem útočníka – groomera, je oběť zmanipulovat, získat si důvěru dítěte, které je následně ochotné plnit pachatelovi požadavky. Důležitou roli hraje pachatelova trpělivost. Ten vydrží i dlouhé měsíce vést s obětí komunikaci, jež vede k osobní schůzce (Internetem bezpečně.cz, 2021).

„Termín kybergrooming označuje chování uživatelů internetu (predátorů, kybergroomerů), 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.“ (Kopecký, Krejčí, 2010, s. 14).

4.3 Kyberstalking

Kyberstalking probíhá v online prostředí za použití elektroniky nebo internetu pro nebezpečné pronásledování, následné vyvolání pocitu strachu o soukromí, zdraví a případně i život. Moderní technologie jsou nezbytnou součástí kyberstalkingu tvořící vhodné anonymní prostředí, umožňující pronásledování vybrané oběti. Pro běžné pronásledování – stalking, byl nutný lidský kontakt s obětí, což u kyberstalkingu chybí. Kyberstalking může oběti značně uškodit po psychické stránce, potažmo i ohrozit život. Od roku 2010 je stalking postižitelný dle českých zákonů po novelizaci

Trestního zákoníku č. 40/2009 Sb. Jedná se o nový trestný čin Nebezpečné pronásledování a je upraven v § 354 (Zákony pro lidi.cz, 2021). Staneme-li se obětí tohoto trestného činu, je nutné obrátit se na Policii České republiky.

4.4 Sexting

„Sexting (česky sextování, slovo vzniklo složeninou slov sex a textování) je elektronické rozesílání textových zpráv, fotografií či videí se sexuálním obsahem. Tyto záznamy (fotografie, video) jsou pak často zveřejněny na internetu“ (Hulanová, 2012, s. 62).

Sexting je dobrovolné sdílení vlastních intimních materiálů (fotografií, videí, případně sexuálně explicitního textu) s jinými osobami (partnerem, přáteli, ale také např. neznámými lidmi). Sexting je potenciálně velmi rizikový jev, protože pokud dojde k úniku intimních materiálů do online prostředí (a tvůrce a příjemce tak nad šířením materiálů ztratí kontrolu), dítě se snadno může stát obětí různých druhů online útoků – např. verbálního dehonostování, vydírání či vyhrožování, které mají na dítě vážný dopad a v extrémních situacích mohou končit až sebevraždou dítěte.

4.5 Phising

Phishing je dalším termínem, který se v této práci objevuje. Dle webu banky.cz jde o: „podvodné vylákání hesel k internetovému bankovníctví, či vylákání hesel, čísel kreditních karet apod. Útočník využívá nevyžádaného e-mailu, nebo SMS, pomocí které vyvolá dojem, že si oslovený musí jít na web zkontrolovat svoje přístupy, nebo aktualizovat heslo. Útočník většinou provozuje falešné stránky, které se tváří jako stránky banky a při údajné aktualizaci hesla jen přepošlou údaje napadeného“ (Banky.cz, 2021).

4.6 Ostrakizace

Jedná se o vyloučení z prostředí moderních technologií, kde je oběť vyloučená z různých skupin, online, her, chatů, událostí apod. Frustrující bývá i to, že to vidí větší skupina lidí, než by bylo možné v offline světě. Přestože je tento způsob kyberagrese

nepřímý, je často pro jeho oběť toto vyloučení bolestné a nepříjemné (Černá, 2013, s. 25–26).

4.7 Hoax

Anglický výraz pro podfuk. Jedná se o falešnou, záměrně vytvořenou zprávu rozesílanou prostřednictvím moderních technologií. Mezi hoaxy lze zařadit poplašné zprávy obsahující smyšlené nebezpečí a obyčejné podvody. Hoaxy obvykle reagují na aktuální dění ve společnosti. V současné době může jít o hoaxy týkající se léčby koronaviru (Avast.com, 2021).

4.8 Viry a spamy

Avast označuje virus jako program nebo část kódu, která se spustí na jakémkoli telekomunikačním zařízení bez vědomí či svolení uživatele. Některé viry pouze znepríjemňují uživateli život. Většina virů je ale navržena tak, aby získala kontrolu nad napadeným systémem a prováděla destruktivní akce (Avast.com, 2021).

V případě spamu jde o nevyžádanou, převážně komerční nabídku, která je rozeslána velkému počtu uživatelů. Nejčastěji se se spamem můžeme setkat v elektronické poště. Může se šířit i prostřednictvím skupinových diskusí a upozorňovat na různé internetové projekty (např. prodejní weby).

4.9 Závislost

Stále rozšiřující se online svět a všudypřítomné propojení virtuálního s reálným světem přináší i svá úskalí. Tato neustálá propojenost může svým uživatelům způsobovat závislost na tzv. virtuálních drogách. Může se jednat o závislost na internetu, sociálních sítích, počítačových hrách, mobilním telefonu, televizi, kterou lze odborně pojmenovat „netolismus“. Eckertová a Dočekal (2013, str. 126) popisují závislost na sociálních sítích jako „nutkání neustále sledovat, co píšou přátelé, kde jsou, co dělají, co vyfotografovali, co si přečetli, co doporučili.“

Současná doba závislosti na různých moderních technologiích jen podporuje. Téměř každý majitel mobilního telefonu má i datové připojení, tedy internet v telefonu. Zvykli jsme si, že potřebné informace získáme v pouhých pár minutách. Pro dnešní

dobu je typická rychlost a neustálá pohotovost. Ne každý dokáže pohotově reagovat na požadavky doby, nedokáže své kompetence praktikovat v reálném životě a své potřeby, tedy řeší únikem z reálného světa do toho online. O závislosti lze tedy hovořit v případě, že čas strávený na internetu se prolíná s reálným životem a komplikuje jej. Abychom mohli hovořit o závislosti, musí být dle anglického psychologa Marka Griffitha (Netolismus.cz, 2021) přítomno šest základních příznaků:

1. VÝZNAČNOST – určitá aktivita se stane nejdůležitější v životě člověka a začíná ovládat jeho myšlení, cítění a chování.
2. ZMĚNY NÁLADY – změny nálady v důsledku zapojení se do určité aktivity, které mohou být vnímány jako vyrovnávací strategie za účelem uklidnění se.
3. TOLERANCE – proces, při kterém je nutno stále více aktivity k dosažení předchozí míry uspokojení. V praxi tedy např. roste délka času trávené online.
4. ODVYKACÍ SYMPTOMY – ukončení či omezení aktivity se projevuje abstinenními symptomy.
5. RELAPS – tendence opakovat dřívější vzorce závislostního chování.
6. KONFLIKT – závislost vyvolává problémy – narušuje např. vztahy v zaměstnání, ovlivňuje prospěch, dochází ke ztrátě kontroly, výčitkám apod.

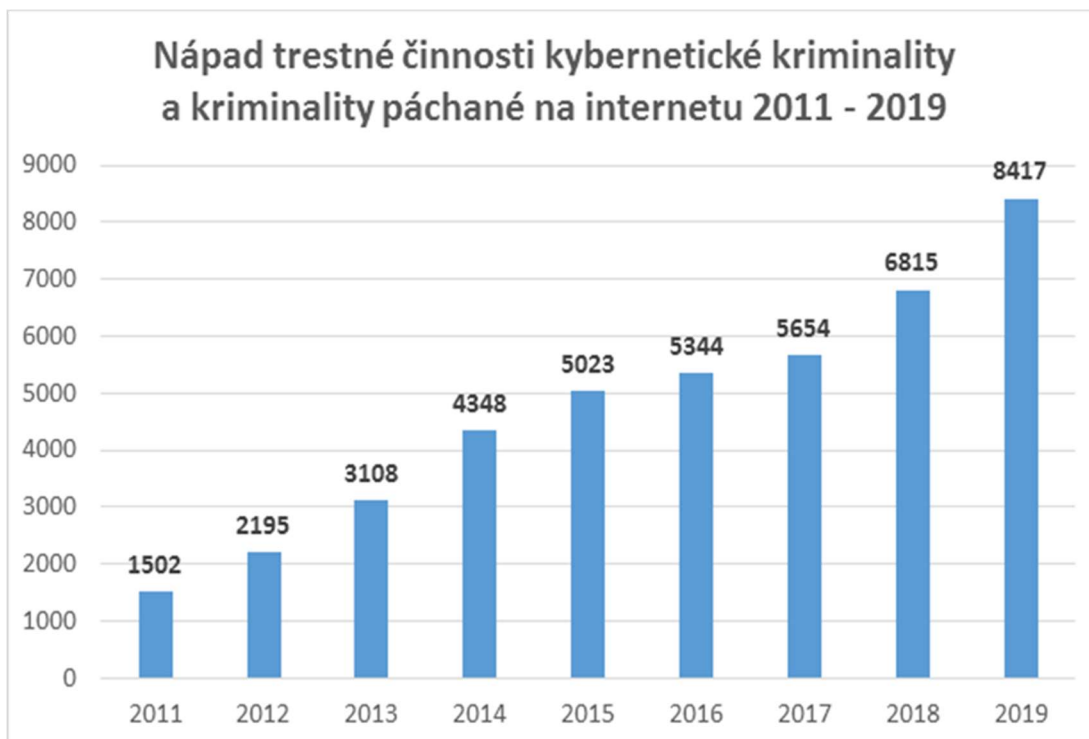
Z uvedených příznaků lze odvodit, že závislost na internetu či sociálních sítích velkou měrou zasahuje do jedincova života a postupem času se stává dominantní nad běžnými denními aktivitami. Vše je ještě doprovázeno změnou nálady a ztrátou volného času.

5 Právní úprava v České republice

Obecně lze říct, že právě sociální sítě jsou fenoménem posledních 20 let ve vztahu k seznamování. Napomáhají ve velké míře dětem k socializaci ve společnosti. Prostřednictvím internetu, resp. sociálních sítí a chatů, se snaží seznámit s dalšími vrstevníky a neuvědomují si veškerá rizika, která jim z této činnosti hrozí. Nejčastější hrozbou je kyberšikana, která ovšem v našem právním řádu není nijak zakotvena, jelikož Trestní zákoník nezná skutkovou podstatu trestného činu Kyberšikana. Při prokázání jednání spadajícího pod kyberšikanu se jedná o přešupek či o jiný správní delikt (např. porušení školního řádu). V některých případech může dojít i ke spáchání trestného činu. Seznam možných trestných činů je uveden v příloze č. 1.

Policie ČR od r. 2011 sleduje počet trestných činů spáchaných v kyberprostoru (zejména v síti Internet). V uvedeném období je zaznamenán trend setrvalého nárůstu evidovaných případů kybernetické kriminality (od 1 502 trestných činů v roce 2011, po 8 417 trestných činů v roce 2019).

Graf 2: Nápad trestné činnosti kybernetické kriminality



Zdroj: Policie ČR

6 Organizace a projekty zabývající se prevencí a vzděláváním

V důsledku narůstajícího počtu rizik spojených s užíváním internetu a sociálních sítí vzniklo několik projektů či organizací, které se věnují prevenci a vzdělávání široké veřejnosti v oblasti kyberkriminality. Nejznámější a nejúspěšnější si uvedeme níže.

6.1 E-bezpečí – www.e-bezpeci.cz

„Projekt E-Bezpečí je celorepublikový certifikovaný projekt zaměřený na prevenci, vzdělávání, výzkum, intervenci a osvětu spojenou rizikovým chováním na internetu a souvisejícími fenomény. V posledních letech se projekt také věnuje pozitivnímu využívání IT ve vzdělávání a běžném životě. Projekt E-Bezpečí je realizován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého ve spolupráci s dalšími organizacemi“ (E-bezpečí.cz, 2021).

6.2 Bezpečný internet – www.bezpecnyinternet.cz

„Projekt Bezpečný internet.cz oslovuje různé cílové skupiny uživatelů a na názorných příkladech pomáhá vytvářet správné návyky internetové bezpečnosti. Projekt není vázán na produkty žádných společností a zcela zdarma poskytuje rady, návody i zkušenosti provozovatelů nejnavštěvovanějších internetových služeb. Počin tohoto projektu je tedy cílený hlavně na rizika virtuálního světa a na způsoby, jak s nimi bojovat“ (Kožíšek, Písecký, 2016, s. 148).

6.3 Národní centrála bezpečného internetu – www.NCBI.cz

NCBI, z. s., provádí osvětu a podporuje bezpečnější užívání online technologií a vzdělávání v této oblasti. K tomu využívá svých zkušeností z realizace řady národních a mezinárodních projektů, z nichž nejdůležitější byl projekt Safer Internet Centre provozovaný a koordinovaný NCBI od roku 2006 do roku 2018 s podporou Evropské komise a dalších partnerů (NCBI.cz, 2021).

6.4 Dětské krizové centrum – www.ditekrize.cz

Celorepublikově působící centrum specializované na odbornou pomoc dětem v nelehkých životních situacích. Též se zaměřuje na vydávání různých preventivních materiálů souvisejících s procesem socializace, sociální integrace, sociálních dovedností a kompetencí (Dítě krize.cz, 2021).

6.5 Kraje pro bezpečný internet – www.KPBI.cz

Projekt Kraje pro bezpečný internet podporovaný Asociací krajů České republiky se zaměřuje na vzdělávání pedagogů, rodičů i žáků ve věcech zodpovědného zacházení s informačními a komunikačními technologiemi a následného chování v kyberprostoru (KPBI.cz, 2021).

PRAKTICKÁ ČÁST

7 Dotazníkové šetření

7.1 Cíl průzkumného šetření

Bakalářská práce se zabývá povědomím rodičů o rizicích v kybernetickém prostoru, a proto jsem se v dotazníkovém šetření zaměřila na otázky v těchto okruzích:

1. Jaké povědomí mají rodiče o rizicích v kybernetickém prostoru?
2. Jaké preventivní kroky, týkající se sociálních sítí a rizik v kybernetickém prostoru, činí rodiče vůči svým dětem?

7.2 Charakteristika regionu a respondentů

Dotazníkové šetření probíhalo v nejmenované základní škole v Městské části Praha 6. Jedná se o školu zaměřenou na rozšířenou výuku jazyků, tělesnou výchovu a výuku informatiky. V současné době vzdělává více než 600 žáků. Škola si nepřeje být jmenována.

Respondenty dotazníkového sběru dat byli rodiče žáků 5. – 9. tříd výše uvedené školy. Prostřednictvím školy byl rodičům rozeslán anonymní online dotazník. Z původního záměru, rozdat tradiční papírové dotazníky při třídních schůzkách, bylo upuštěno vzhledem k epidemické situaci COVID-19, která toto neumožňovala. Na základě domluvy zaslali třídní učitelé rodičům odkaz k vyplnění online dotazníku.

Do dotazníkového šetření se zapojilo 64 respondentů. Dle dotazníkových statistik navštívilo sdílený odkaz na konkrétní dotazník 110 respondentů, ale 46 respondentů vyplnění dotazníku nedokončilo. Z čehož vyplývá pouze 58% návratnost a úplné dokončení dotazníku. Domnívám se, že jako hlavní důvod nízké účasti na dotazníkovém šetření je aktuální epidemické situace COVID-19. V probíhajícím školním roce 2020/2021, kdy většina výuky probíhá distanční formou, jsou ze strany školy prováděny časté průzkumy týkající různých oblastí. Rodiče tedy po obdržení dotazníku prostřednictvím školy nemuseli řešit původ a účel, a do dotazníkového šetření se nezapojili.

7.3 Metoda dotazníku

Jako nástroj sběru dat jsem zvolila anonymní online dotazník tvořený 2 částmi. V první jsem se respondentům představila a objasnila jsem svůj důvod sběru dat. Dále byli respondenti ujištěni, že se jedná o anonymní dotazník a instruováni, jak postupovat při vyplňování dotazníku. Hlavní část – samotný dotazník obsahuje 27 otázek a je pomyslně rozdělen do několika oddílů. Nejprve se jedná o okruh otázek směřující na zjištění, jaké technologie rodiče a děti používají. Následují rizika kyberprostoru a jaký druh preventivního chování v kybernetickém prostoru je respondenty volen ve vztahu k dětem. Dotazník uzavírají všeobecné otázky týkající se pohlaví, věku a vzdělání respondenta.

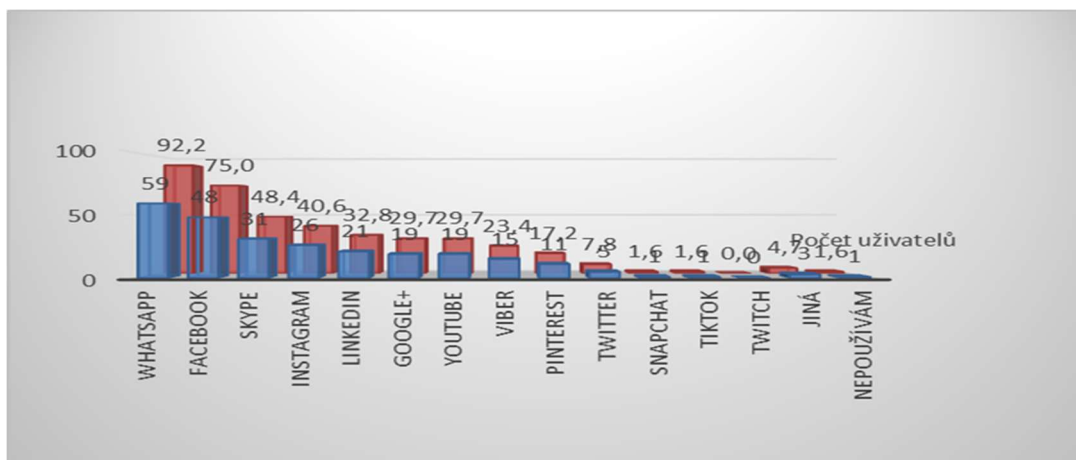
Sběr dat probíhal v měsících leden a únor 2021 a následně byl vyhodnocován. K vytvoření online dotazníku a ke sběru dat byl použit server www.surveio.com. Následně byly výsledky zpracovány v programu Excel. Dotazník je součástí bakalářské práce uvedený v přílohách (příloha č. 2).

7.4 Popis a interpretace dat

Při interpretaci výsledků dotazníkového šetření bylo postupováno podle pořadí otázek v dotazníku. Výsledky jsou zobrazeny v grafech a blíže rozepsány. Do šetření bylo zahrnuto 64 zcela vyplněných dotazníků.

1. Na jaké uvedené sociální síti máte Vy osobně účet?

Graf 3: Sociální síť používané rodiči



Zdroj: vlastní zpracování

Z 64 respondentů uvedlo 92,2 %, že jsou uživateli komunikační sociální sítě WhatsApp. Dále 75 % využívá sociální síť Facebook, která je celosvětově nejpoužívanější. Za zmínku stojí 32,8 % uživatelů sítě LinkedIn, jež zřejmě z velké části využívají z profesních důvodů. Z preventivního hlediska je přínosné, mají-li rodiče přehled i o jiných sociálních sítích, než sami používají. To především z důvodu užívání těchto sítí jejich dětmi a odpovídajícího nastavení soukromí a ochrany před cizími lidmi.

2. V jakém věku máte děti?

Graf 4: Věk dětských uživatelů

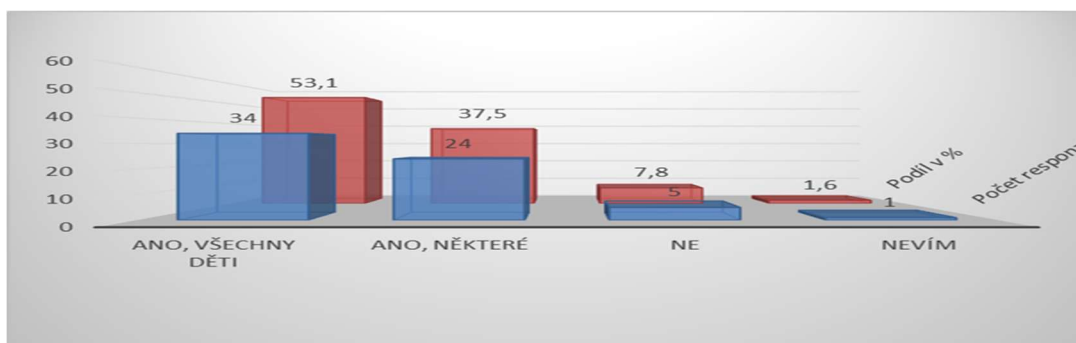


Zdroj: vlastní zpracování

Nejpočetnější skupinou bylo zastoupeno stáří dítěte ve věku 12-13 let a to 53,1 %. Z čehož lze usuzovat i další kroky při vyplňování dotazníku. Neboť, jak je všeobecně známo, většina sociálních sítí dovoluje registraci dětem od 13 let.

3. Je Vaše dítě (děti) uživatelem sociálních sítí?

Graf 5: Dětsí uživatelé sociálních sítí

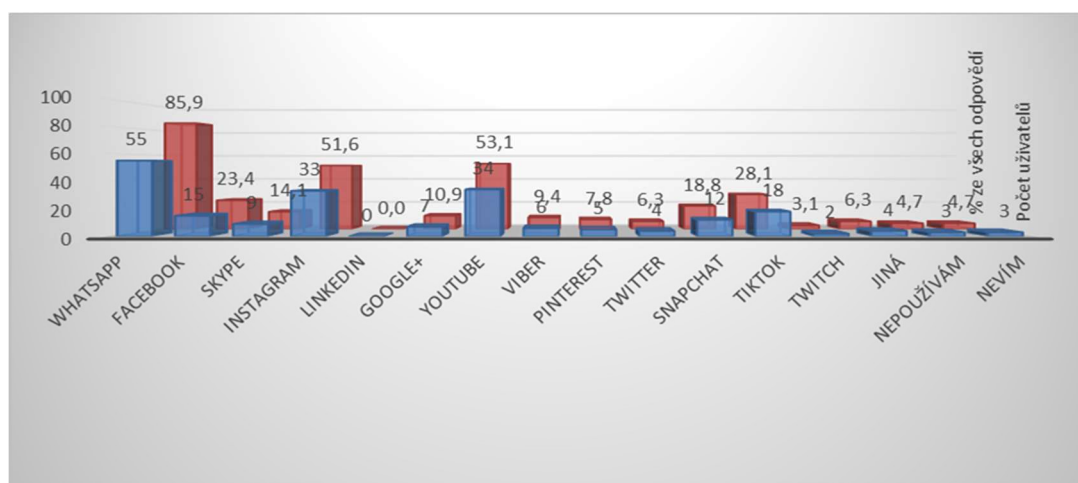


Zdroj: vlastní zpracování

53,1 % rodičů uvádí, že jejich dítě je uživatelem sociálních sítí. Vzhledem k tomu, že věk dětí se pohyboval v rozpětí 6-15 let je patrné, že většina rodičů povoluje svým dětem registraci na sociálních sítích, byť povolená věková hranice je 13 let. K zamyšlení je, zda o této věkové hranici rodiče vědí, a přesto toto nerespektují. Možný důvod spatřuji i v začlenění dítěte do skupiny uživatelů a případného nevytlačení z určité společnosti (třída, kroužek, kamarádi).

4. Jaké sociální sítě Vaše děti používají?

Graf 6: Sociální sítě používané dětmi

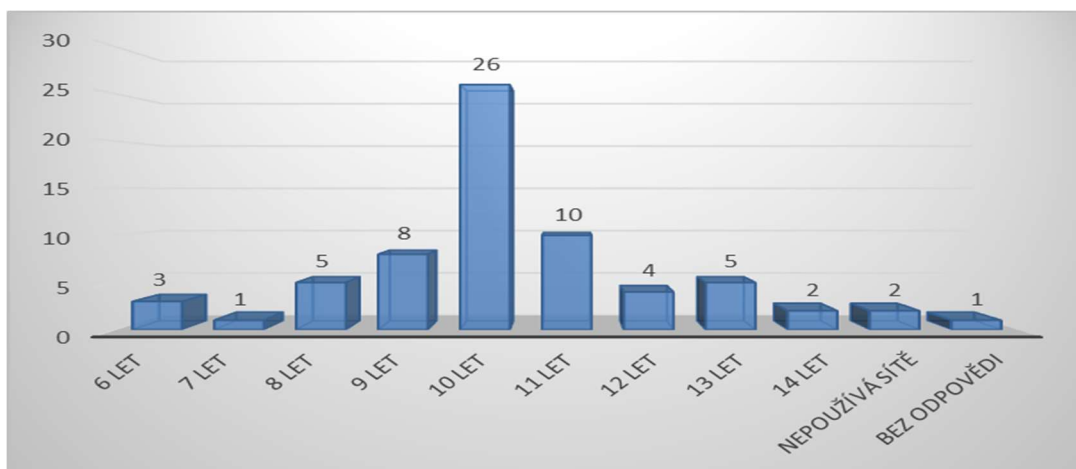


Zdroj: vlastní zpracování

Nejčastěji uváděnou sociální sítí používanou dětmi je WhatsApp a to v 85,9 % odpovědí. Obdobně vysoké procento získala tato komunikační sociální síť i mezi dospělými uživateli, což lze odůvodnit jako nejjednodušší komunikační kanál mezi rodinou. Velké oblíbenosti se také těší kanál YouTube s 53,6 % odpovědí a dále pak například Instagram, který používá 51,6 % dětí dotazovaných respondentů. V grafu lze najít nízké procento používání Facebooku, jež značí všeobecný společenský trend u mladých uživatelů. Důvodem může být i větší soukromí, neboť Instagram je síť spíše pro mladé a rodiče tuto síť využívají zřídka. Zajímavým zjištěním a potvrzením odborných diskusí je obliba aplikace Tik Tok, kdy 28,1 % dětí oslovených respondentů tuto aplikaci používá, ale rodiče se na této síti vyskytují jen v 1,6 % případů mnou oslovených respondentů.

5. Od jakého věku Vaše dítě (děti) sociální sítě využívají?

Graf 7: Od kdy využívají děti sociální sítě

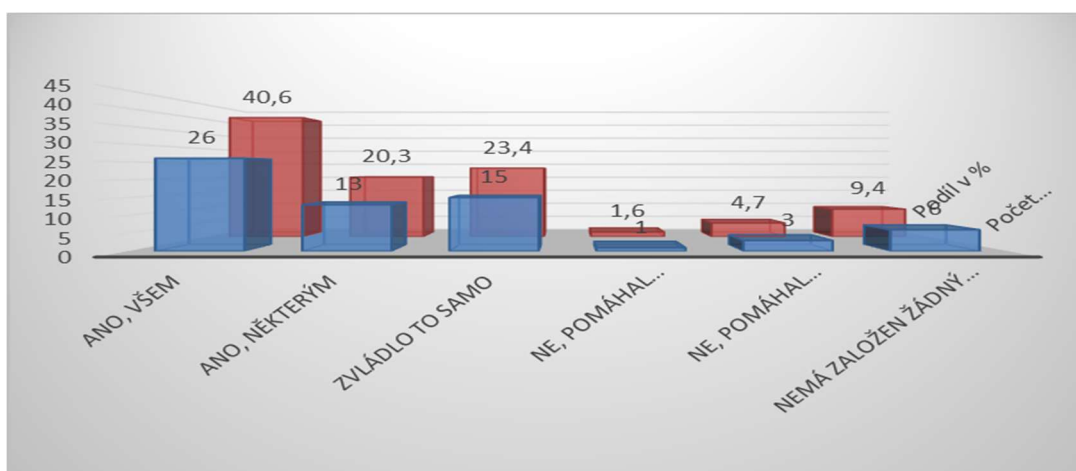


Zdroj: vlastní zpracování

Převážně uváděný věk, pro začátek využívání sociálních sítí, je rodiči uvádět věk 10 let. Jedná se tedy o střední školní věk, kdy dochází k potřebě sdílení společných zážitků s vrstevníky. Ve spojitosti se sociálními sítěmi je i tato aktivita podporována rodiči, například i z důvodů, aby dítě nebylo vyčleňováno z kolektivu.

6. Pomáhali jste svému dítěti (dětem) při zakládání profilu (úctu) na některé sociální síti?

Graf 8: Pomoc při založení profilu



Zdroj: vlastní zpracování

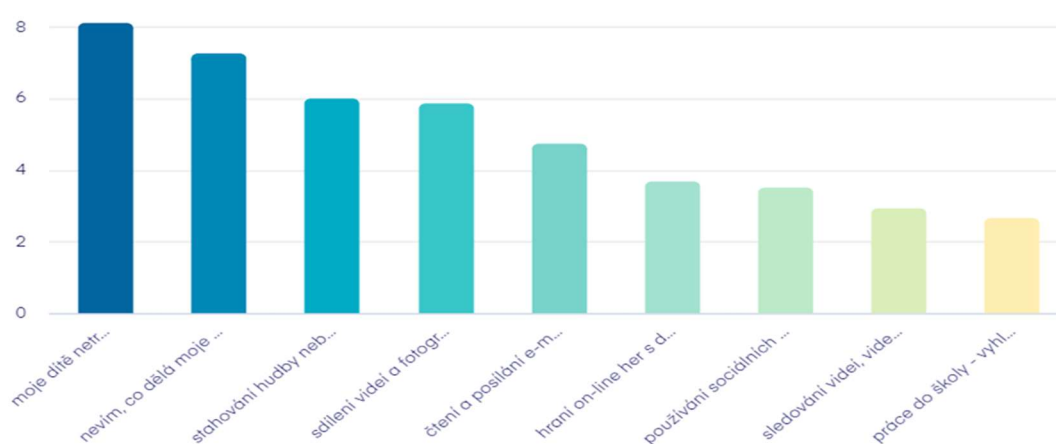
Nadpoloviční většina, přes 60 %, rodičů pomáhala svému dítěti při zakládání profilu. (Berme v potaz, že u odpovědi ano, některým se může jednat o dítě např. předškolního věku). Zajímavé je, že u 23,4 % dětí dotazovaných respondentů si účet zakládalo samo. V takovém případě, by byla vhodnější pomoc rodičů, kdy může dojít k lepšímu nastavení soukromí. A do budoucna, tak zamezit nevhodnému obsahu, či komunikaci s možnými predátory.

7. Za jakým účelem Vaše děti používají internet?

(očíslyte pořadí aktivit od nejčastěji po méně používanou)

- a) NEVÍM, CO MOJE DÍTĚ DĚLÁ NA INTERNETU
- b) POUŽÍVÁNÍ SOCIÁLNÍCH SÍTÍ
- c) ČTENÍ A POSÍLÁNÍ E-MAILŮ
- d) PRÁCE DO ŠKOLY – VYHLEDÁVÁNÍ
- e) HRANÍ ONLINE HER S DALŠÍMI LIDMI
- f) SLEDOVÁNÍ VIDEÍ, VIDEOKLIPŮ (YOUTUBE)
- g) SDÍLENÍ VIDEÍ A FOTOGRAFIÍ (TIK TOK, INSTAGRAM, ...)
- h) MOJE DÍTĚ NETRÁVÍ NA INTERNETU ŽÁDNÝ ČAS
- i) STAHOVÁNÍ HUDBY NEBO FILMŮ
- j) JINÉ

Graf 9: Nejčastější využití internetu dětmi

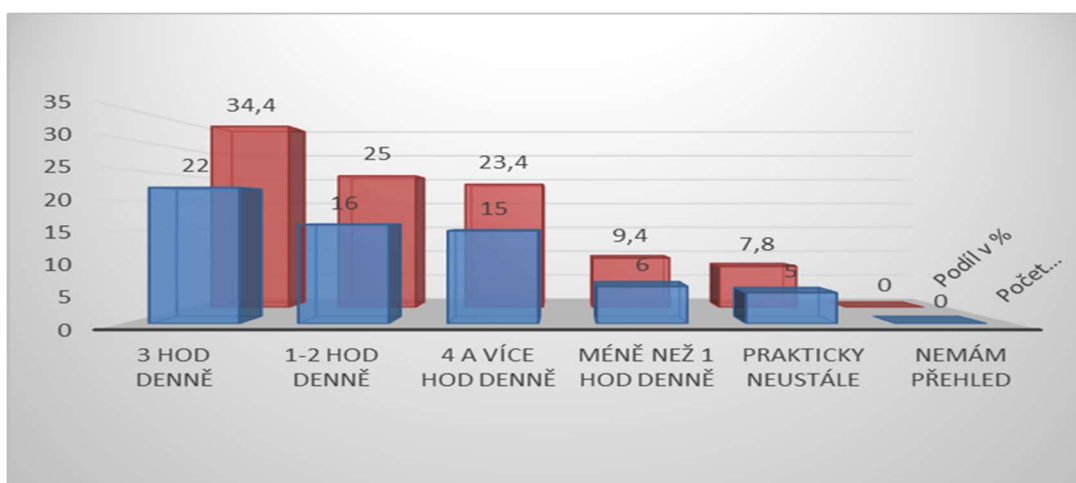


Zdroj: vlastní zpracování

Zde se jedná o otázku, kde se řadí aktivity spojené s internetem od nejpoužívanější po méně používanou. Je překvapivé, že nejčastějšími aktivitami na předních pozicích, byly odpovědi zmiňující „moje dítě netráví na internetu žádný čas“ a „nevím, co dělá moje dítě na internetu“. Nevím, zda si tuto situaci vysvětlovat nezájmem rodičů o činnosti dětí na internetu. Nebo opět pandemickou situací a dlouhodobým pobytem dětí u počítačů všeobecně.

8. Kolik času Vaše děti tráví na internetu (sociálních sítích)?

Graf 10: Čas trávený dětmi na internetu

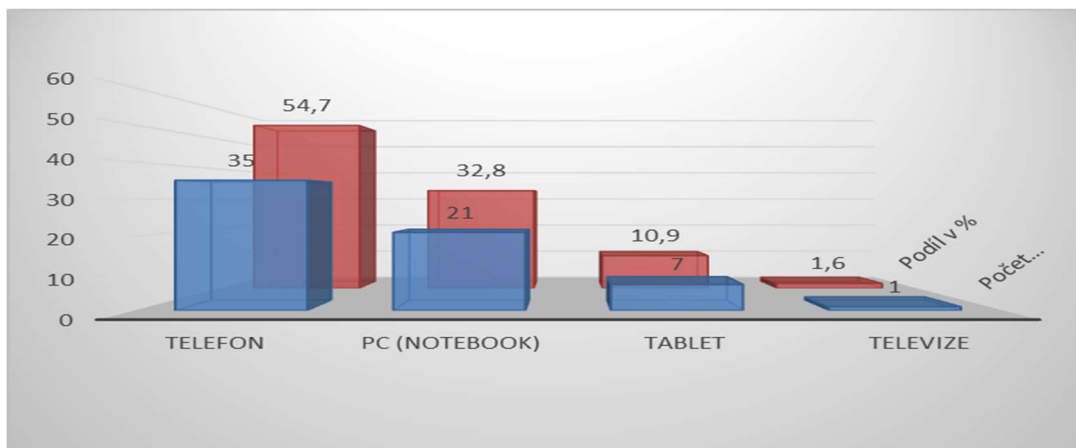


Zdroj: vlastní zpracování

Odborníci se shodují, že čas trávenými dětmi na internetu by se měl měnit na základě jejich věku. V 34,4, % odpovědí rodiče uvedli, že děti tráví na internetu 3 hodiny denně. Jsem si vědoma současné pandemické situace, která může výsledky šetření ovlivnit, neboť žáci od 3. třídy ZŠ mají výuku distanční formou. Tudíž rodiče mohli čas trávený na internetu (sociálních sítích) započítat do celkové doby používání. Ovšem mělo by se brát v potaz, že děti do věku 10 let, jsou nejvíce náchylné k vytvoření závislosti, a proto čas trávený na internetu, by se měl těmto dětem kontrolovat, případně korigovat.

9. Z jakého zařízení se Vaše dítě (děti) nejčastěji připojuje k internetu, sociálním sítím?

Graf 11: Zařízení umožňující dětem připojení k internetu

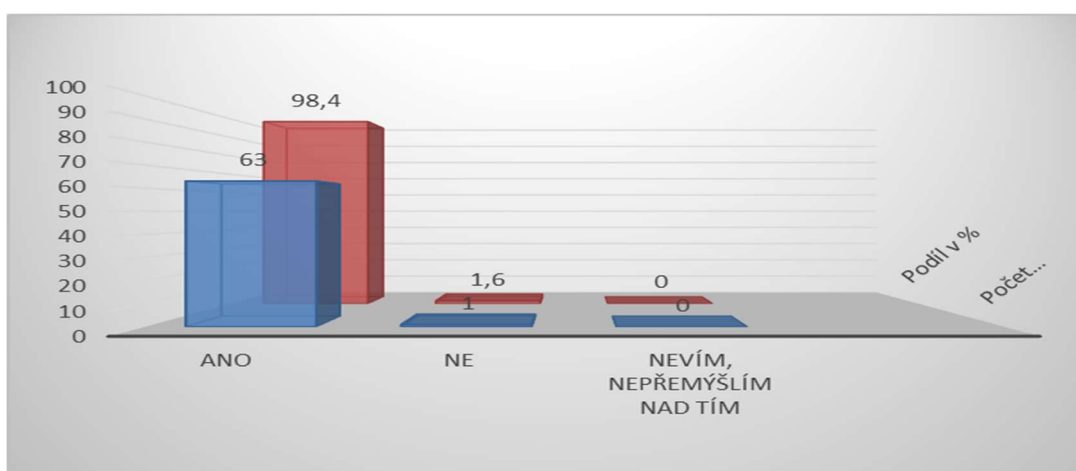


Zdroj: vlastní zpracování

Dotazníkové šetření zmapovalo, že více než polovina – 54,7 % dětí se na internet připojuje přes mobilní telefon. Z tohoto je patrné, že telefon v sobě zahrnuje více možností komunikace, mimo jiné i připojení na internet, a tudíž je nejpoužívanější technologií. Také lze uvést, že původní funkce telefonu – volání a zasílání SMS, již není prioritou.

10. Myslíte si, že internet a sociální sítě mohou být nebezpečné?

Graf 12: Nebezpečnost internetu a sociálních sítí

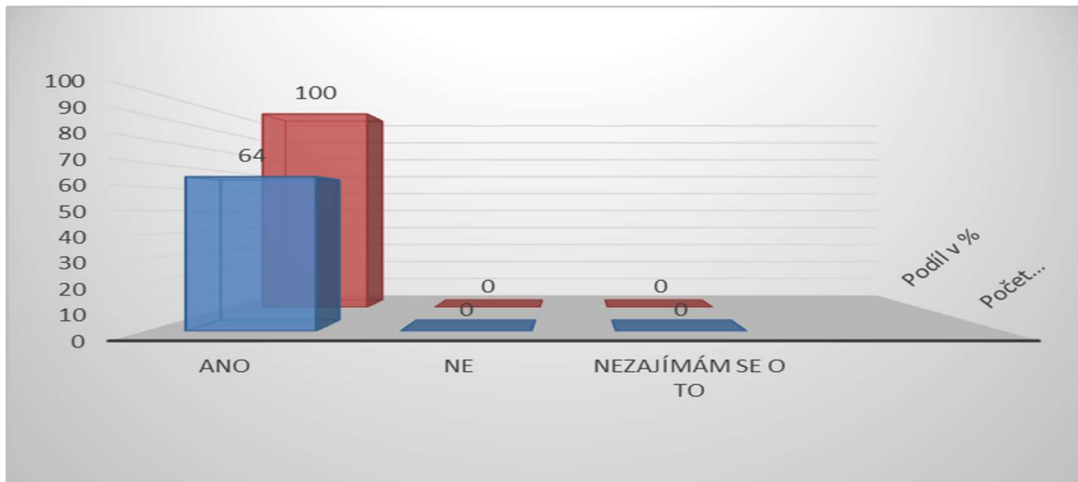


Zdroj: vlastní zpracování

Vzhledem k množství rizik vyskytujících se v internetovém světě, je pozitivní, že si rodiče tato rizika uvědomují a to 98,4 % dotazovaných. Pouze 1,6 % v této oblasti nepřipouští rizika.

11. Víte, jaká jsou rizika sociálních sítí?

Graf 13: Znalost rizik na sociálních sítích



Zdroj: vlastní zpracování

100 % respondentů uvádí, že zná rizika sociálních sítí. Toto lze zdůvodnit i vysokým podílem zastoupení vysokoškolsky vzdělaných respondentů.

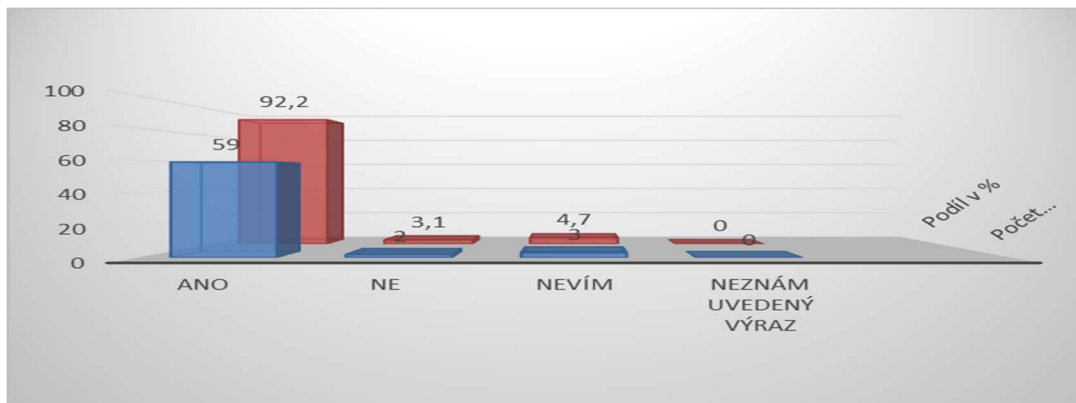
12. Vypište, jaká konkrétní rizika sociálních sítí znáte.

Dotazníkového šetření se zúčastnilo 64 osob, tudíž v tomto případě bylo 64 různých názorů na rizika vyskytující se v kybernetickému prostředí. Nicméně, byť každý respondent uvádí jiná rizika, v součtu se rodiče shodují, neboť 57,8 % uvedlo jako jedno z rizik kyberšikanu. Rodiče sice neuvádí odborníky uznávané názvy rizik, ale dle charakteristik je dokážou vystihnout. Odpovědi, které byly uváděny často jsou např.: závislost (18 %), nevhodný obsah (17 %), zneužití osobních údajů (17 %), kontakt s cizími lidmi vydávající se za kamaráda (20%), sdílení soukromí (15%), stalking (15%), různé druhy podvodů (12%), šíření nepravdivých zpráv (8%).

13. Jedná se podle Vašeho mínění o „kyberšikanu“ v následujícím výroku?

„Spolužáci o mně natočili video, které už viděl každý z naší školy. Už se tam nikdy nevrátím. Jak se jim můžu sám ubránit?“

Graf 14: Pojem "kyberšikana"



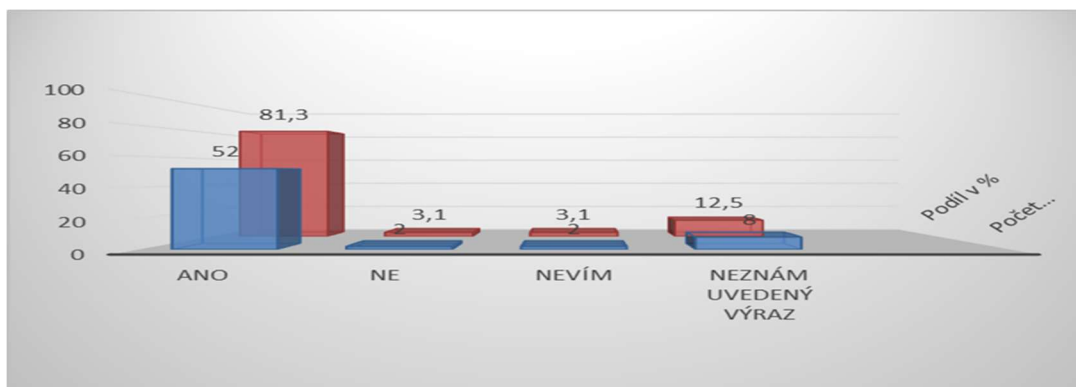
Zdroj: vlastní zpracování

92,2 % dotázaných správně identifikuje uvedený výrok, jako kyberšikanu. Je patrné, že tento pojem je ve společnosti známý, možná i z důvodu časté medializace.

14. Jedná se podle Vašeho mínění o „kybergrooming“ v následujícím výroku?

„Byl na mě tak milý, vůbec jsem si neuvědomila, že se mnou manipuluje. A teď mi začal vyhrožovat, že rozešle mé polonahé fotky mým kamarádům. Nevím jak dál, má mě v hrsti.“

Graf 15: Pojem "kybergrooming"



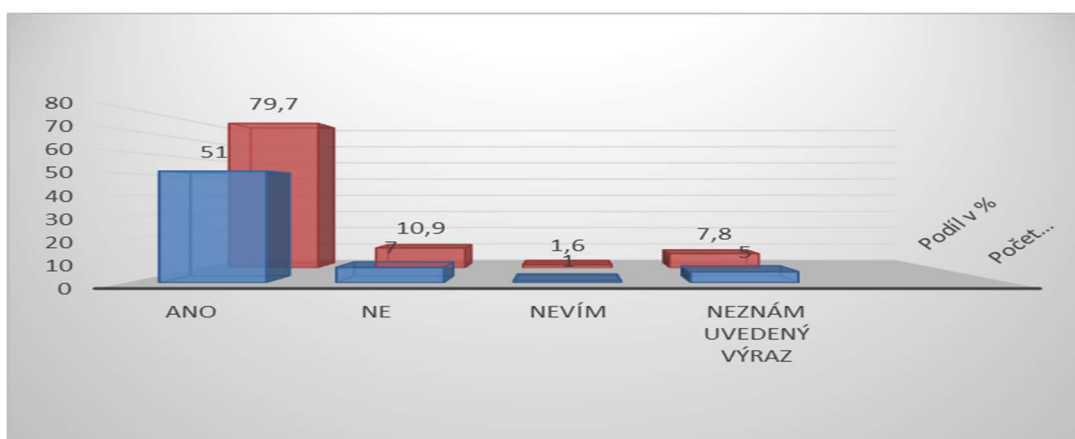
Zdroj: vlastní zpracování

V 81,3 % odpovědí bylo správné tvrzeno, že ve výroku se hovoří o kybergroomingu. Zde je již patrné, že tento výraz není běžně užívaný, neboť 12,5 % respondentů nezná daný výraz. Toto jednání je pro děti a mladé uživatele nejrizikovější, tudíž je vhodné, aby společnost slovo kybergrooming a jeho charakteristické rysy znala.

15. Jedná se podle Vašeho mínění o „sexting“ v následujícím výroku?

„Poslala jsem svému klukovi svoje lechtivé video, jenže on se teď na mě naštvál a vyhrožuje, že ho dá na internet. Jak mi to může udělat, sliboval přece, že je to jen mezi náma!?“

Graf 16. Pojem "sexting"



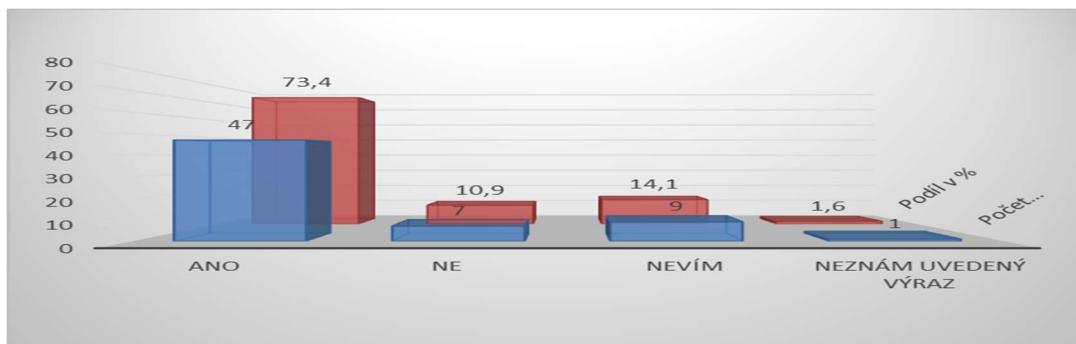
Zdroj: vlastní zpracování

79,7 % respondentů spatřuje v uvedeném výroku sexting, což je správné tvrzení. Naproti tomu 10,9 % se k tomuto názoru nepřidává. Jako odůvodnění bych viděla, že uvedený výraz sexting neznají nebo si pod ním představují něco jiného.

16. Jedná se podle Vašeho mínění o „kyberstalking“ v následujícím výroku?

„Nikdy bych nevěřila, že mi bude v patách na každém mém kroku. Jak se ho mám zbavit?“

Graf 17: Pojem "kyberstalking"

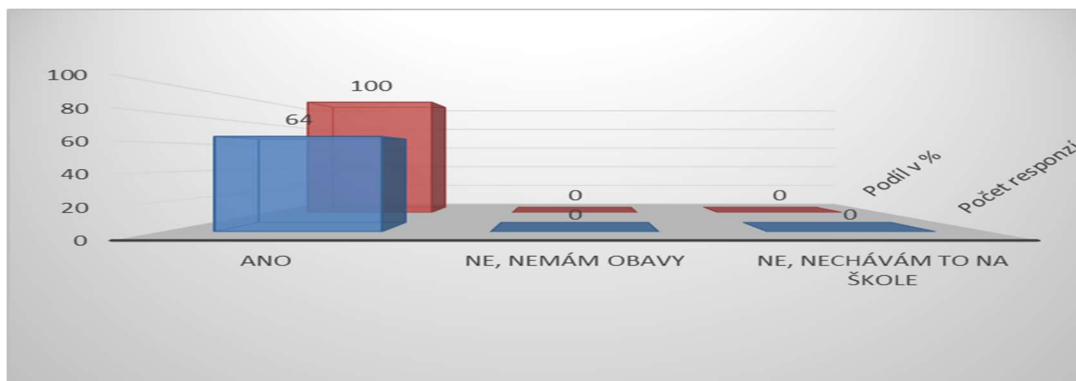


Zdroj: vlastní zpracování

Další z odborně uváděných výrazů je kyberstalking, který je ze všech uváděných rizik nejméně známý. V porovnání s kyberšikanou dokáže uvedený výrok správně určit 73,4 % dotazovaných. Zbylých více jak 25 % respondentů si tímto pojmem není zcela jisto.

17. Bavíte se se svými dětmi o možných rizicích na internetu, sociálních sítích?

Graf 18: Informovanost dětí o rizicích



Zdroj: vlastní zpracování

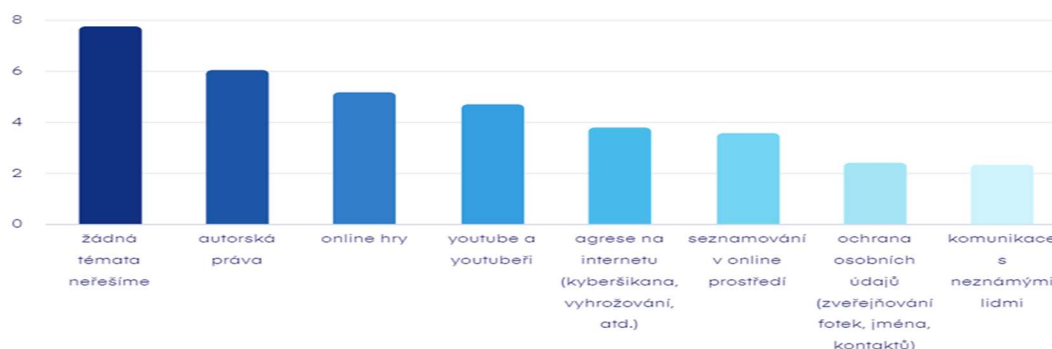
V rámci prevence je pozitivní, že celých 100 % respondentů mluví se svými dětmi o možných rizicích.

18. Jaká témata preventivních aktivit řešíte nejčastěji se svým dítětem (dětmi)?

(očísľujte pořadí aktivit od nejčastěji po méně používanou)

- a) KOMUNIKACE S NEZNÁMÝMI LIDMI
- b) SEZNAMOVÁNÍ V ONLINE PROSTŘEDÍ
- c) AGRESE NA INTERNETU (KYBERŠIKANA, VYHROŽOVÁNÍ, ATD.)
- d) OCHRANA OSOBNÍCH ÚDAJŮ (ZVEŘEJŇOVÁNÍ FOTEK, JMÉNA, KONTAKTY)
- e) AUTORSKÁ PRÁVA
- f) YOUTUBE A YOUTUBEŘI
- g) ONLINE HRY
- h) ŽÁDNÁ TÉMATA NEŘEŠÍME
- i) JINÁ.....

Graf 19: Nejčastější preventivní aktivity konané rodiči

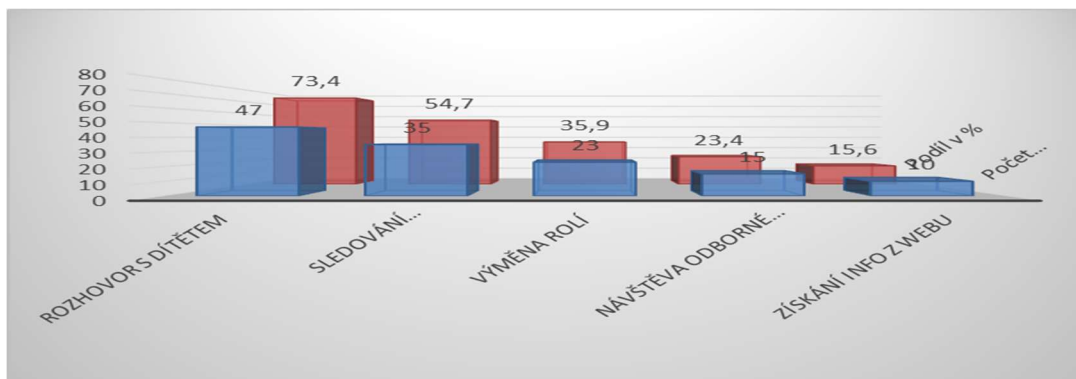


Zdroj: vlastní zpracování

Při řazení řešení preventivních aktivit s dětmi uváděli respondenti nejčastěji na přední příčce odpověď „žádná témata neřešíme“. V návaznosti na předešlou otázku jsou odpovědi přinejmenším zarážející a vzájemně si odporující. Je s podivem, že největší nebezpečí v podobě komunikace s neznámými lidmi, řeší respondenti nejméně často. Přitom toto riziko bylo frekventovanou odpovědí u otázky č. 12, kdy respondenti uváděli rizika hrozící v kybernetickém prostředí, které znají. Pro mě osobně, je tato situace alarmující a jediné vysvětlení mám v podobě špatného přečtení zadání a řazení odpovědí opačným směrem.

19. Jakou metodu byste volili pro lepší přiblížení rizik v kyberprostoru vůči svému dítěti (dětem)?

Graf 20: Metody přiblížení rizik

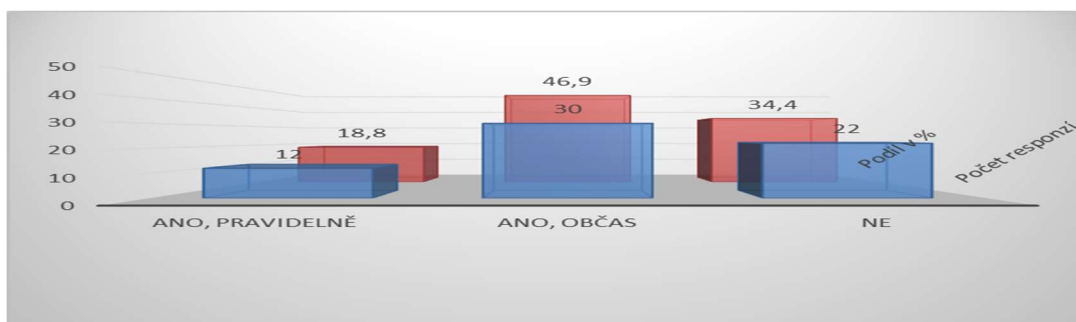


Zdroj: vlastní zpracování

Mezi nejčastější formy preventivních metod rodičů je rozhovor s dítětem. 73,4 % rodičů touto cestou informuje svoje děti. Vysoký podíl odpovědí, 54,7 % respondentů volí metodu sledování preventivního filmu s danou problematikou, což může být zapříčiněno velkým ohlasem kritiků i publika u dokumentárního filmu V síti. Dle své zkušenosti, bych doporučovala přednášky zaměřené na nebezpečí kybernetického prostředí, jež pomůže rodičům lépe si toto představit.

20. Sledujete aktivitu svých dětí na internetu? (např. historie v prohlížeči, Family Link, aj.)

Graf 21: Sledování aktivity dětí na internetu

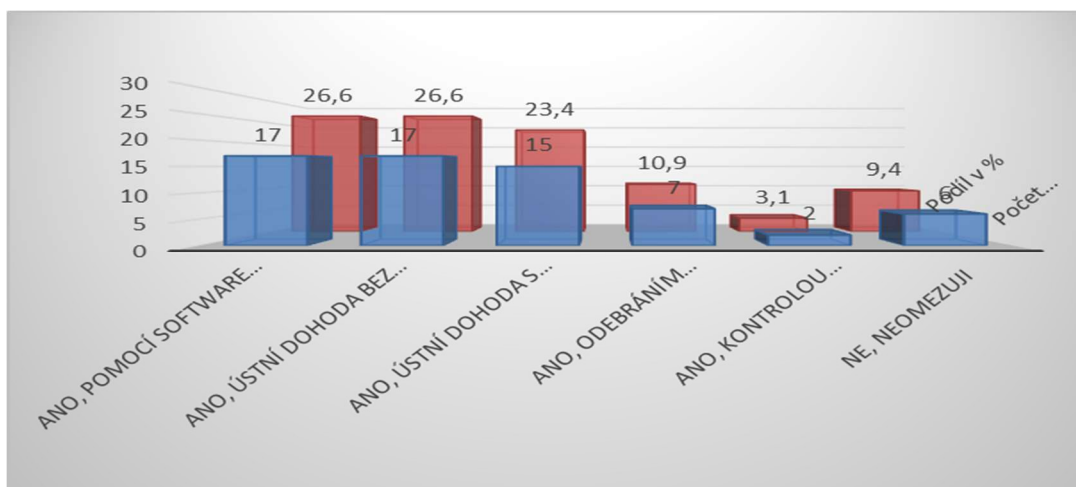


Zdroj: vlastní zpracování

2/3 rodičů považují kontrolu za důležitou a buď ji provádějí pravidelně nebo občas.

21. Omezujete svým dětem přístup na internet?

Graf 22: Omezení přístupu dětí na internet



Zdroj: vlastní zpracování

Jako často používaný způsob omezení pro přístup na internet respondenti uvedli použití rodičovské kontroly nebo aplikace. Stejné hodnoty dosáhla i dohoda, bez další kontroly. Zde se projevuje velká důvěra rodičů vůči svým dětem.

22. Přemýšlí Vaše dítě (děti) nad tím, jaký obsah – příspěvek, foto zveřejňuje?

Graf 23: Zamyšlení dítěte nad zveřejněným obsahem

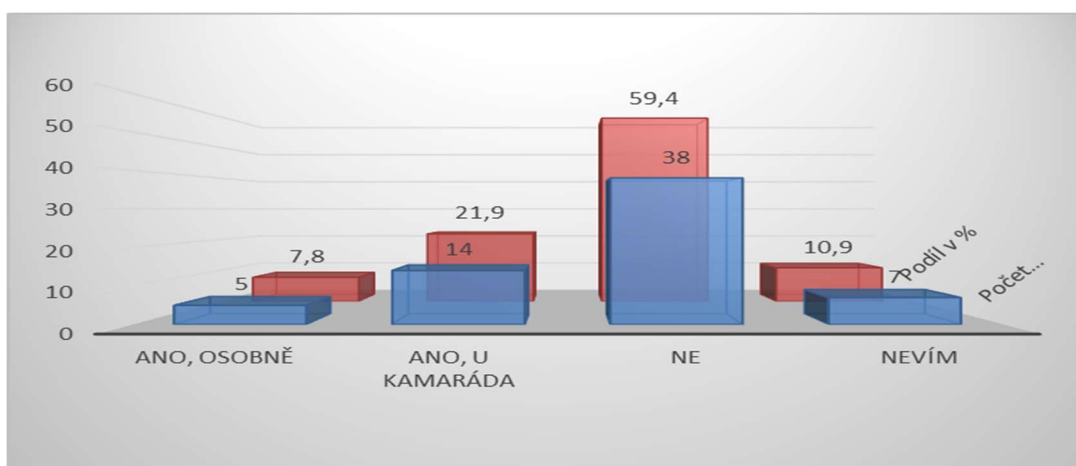


Zdroj: vlastní zpracování

V 32,8 % odpovědí rodiče nevědí, zda jejich dítě přemýšlí nad sdíleným obsahem. Tato část rodičů může mít ke svým dětem důvěru, zřejmě i z důvodu věku dítěte a jeho náležité obeznámenosti o rizicích vyskytujících se na internetu a sociálních sítích.

23. Setkalo se Vaše dítě v kybernetickém prostředí (internet, sociální sítě) s nějakým bezprávím (např. kyberšikana, stalking)?

Graf 24: Setkání dítěte s bezprávím v kybernetickém prostředí

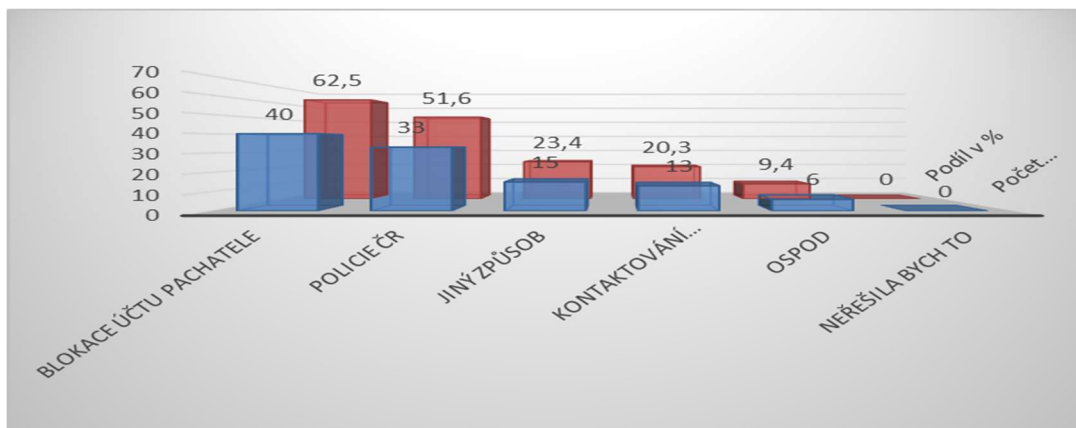


Zdroj: vlastní zpracování

Téměř 30 % dětí respondentů má nějakou, ať už přímou nebo nepřímou, zkušenost s bezprávím v kybernetickém prostředí. Vysoké procento může být důsledkem přesunu běžného života do virtuálního světa.

24. Jak byste reagoval/a, kdyby se Vám dítě svěřilo, že má v internetovém prostředí problémy?

Graf 25: Reakce rodičů na vzniklý problém v internetovém prostředí

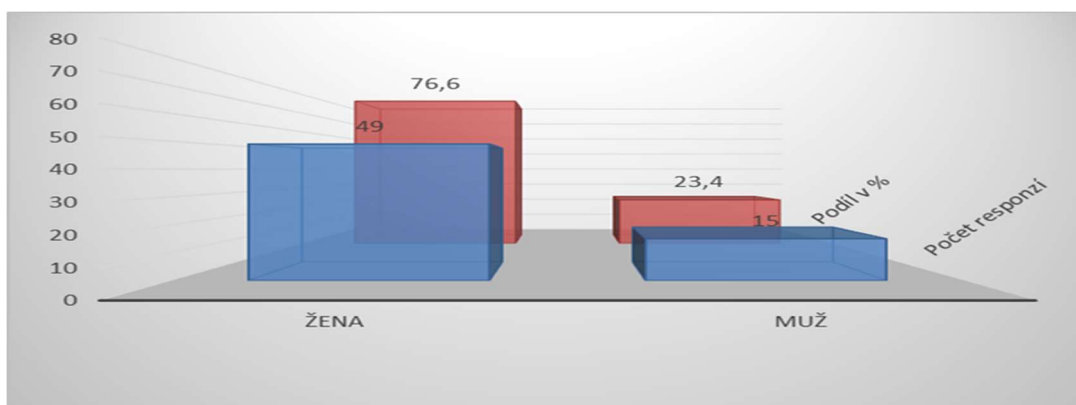


Zdroj: vlastní zpracování

Převážná část rodičů uvedla, že v případě výskytu problému na internetu u jejich dítěte, by volili blokaci účtu pachatele a kontaktovali by Policii ČR. Jsem toho názoru, že tento postup je správný a sama bych ho doporučila.

25. Jakého jste pohlaví?

Graf 26: Pohlaví respondentů

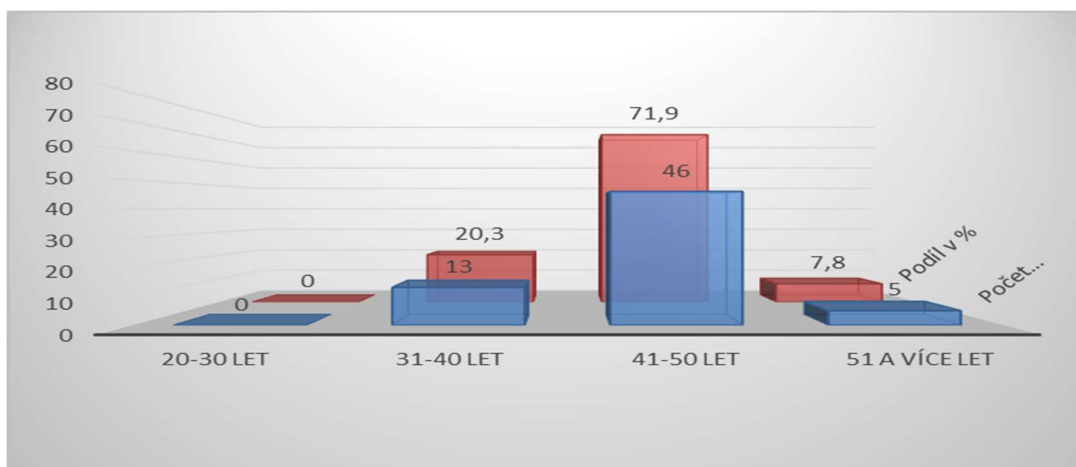


Zdroj: vlastní zpracování

Dotazníkového šetření se zúčastnilo 76,6 % žen a 23,4 % mužů. Stojí za zamyšlení, zda složení respondentů s převažujícím ženským elementem, má vliv na odpovědi. A v případě genderového vyvážení, zda by odpovědi byly diametrálně odlišné.

26. Kolik je Vám let?

Graf 27: Věk respondentů

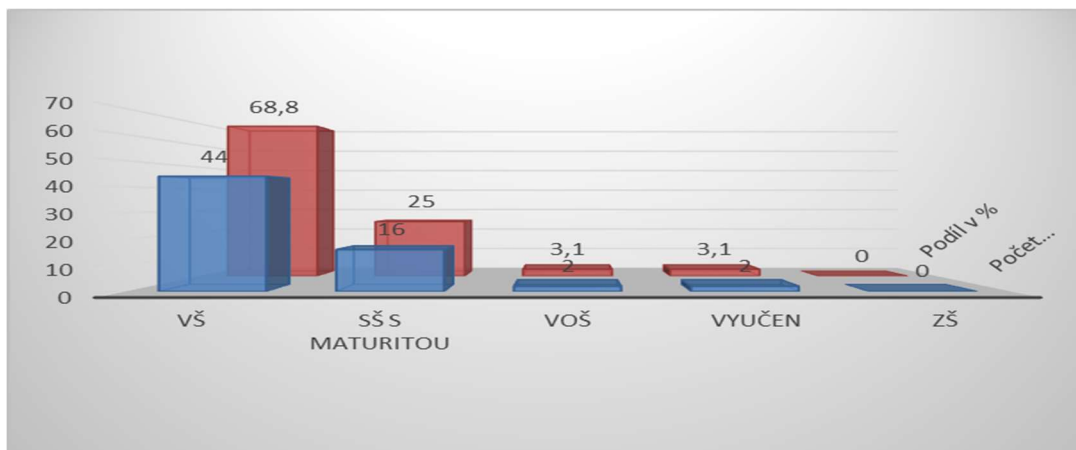


Zdroj: vlastní zpracování

Přes 90 % respondentů náleží do tzv. Generace X a Y. Z jejich odpovědí soudím, že mají přehled o dění ve virtuálním světě a dokážou být svým dětem oporou.

27. Jaké je Vaše nejvyšší dosažené vzdělání?

Graf 28: Vzdělání respondentů



Zdroj: vlastní zpracování

Vysoké procento respondentů má vysokoškolské vzdělání, což může hrát svou roli při skladbě odpovědí.

7.5 Závěr dotazníkového šetření

Na základě dotazníkového šetření bylo zjištěno, že rodiče sice znají a dokážou popsat různá rizika vyskytující se v kyberprostoru, ale odborné výrazy jsou jim ve většině případů cizí.

Co se týče preventivních kroků rodičů vůči svým dětem, mají rodiče dle mého názoru, ještě prostor ke zlepšení. Někteří zřejmě nedokážou domyslet následky špatné informovanosti dětí. Náležitou a včasnou prevencí lze v budoucnu předcházet případným negativním událostem.

7.6 Doporučení pro rodiče

Po vyhodnocení dotazníku bych doporučovala, aby hlavně rodiče, potažmo i škola, fungovali jako prostředníci vzdělávání dětí v oblasti bezpečného užívání informačních technologií. Nesnažili se dětské uživatele odradit, ale náležitě nebezpečí vyskytující se na sociálních sítích přiblížit a upozornit na něj. Neboť dnešní doba, moderní informační technologie bere jako součást každodennosti a je důležitá řádná informovanost o případných rizicích, zejména u mladých uživatelů.

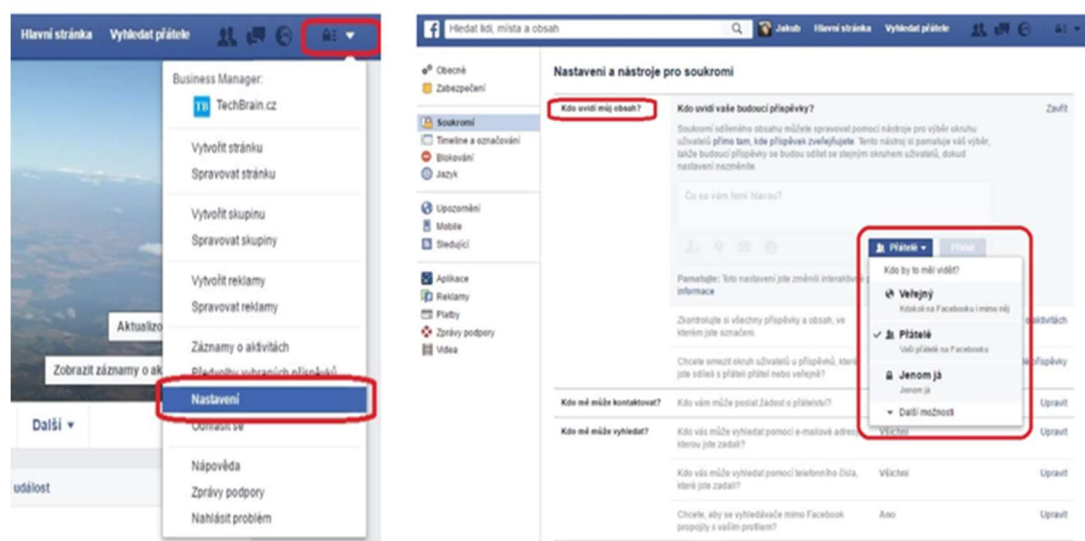
7.6.1 Preventivní opatření

V následujících řádcích nabízím řešení, jak předcházet případnému útoku v kyberprostoru. Jedná se o doporučení dle osobních a profesních zkušeností, ale také o inspiraci po přečtení knihy *Dítě v síti* od Daniela Dočekala.

- Jako rodiče budme seznámeni s případnými riziky, která nejen dětem, hrozí v kyberprostoru. Tím můžeme dítěti poskytnout potřebné informace a máme větší šanci zvládnout případný problém.
- Komunikujme s dětmi. Berme je jako rovnocenné partnery. O fungování online světa často vědí více než rodiče. Nebojme se výměny rolí, kdy dítě předává své znalosti rodiči. Ten nabízí své znalosti z oblasti rizik. Je dobré mít vzájemnou důvěru.
- Stanovujte dětem pravidla adekvátní k jejich věku. Co je účinné pro čerstvé školáky, není již vhodné pro náctileté. Ze svých opatření postupně slevujte, dopřejte dětem pocit zodpovědnosti.

- Při zakládání profilu na jakékoli sociální síti buďte svému dítěti průvodcem, či pomocníkem a dbejte opatrnosti s ohledem na citlivost zveřejňovaných informací. Jako nejvhodnější pro uveřejnění jsou informace o zálibách, přezdívka a foto uživatele.
- Při nastavování statusu většina sociálních sítí umožňuje nastavit veřejný (zobrazit si ho mohou všichni uživatelé, případně i návštěvníci služby) nebo soukromý (zobrazitelný pouze propojeným kontaktům, případně jen určité části z nich). Věnujte těmto základním nastavením náležitou pozornost. Můžete tím předejít v budoucnu nepříjemnostem. Např. u Facebooku není nastavení soukromí přímo nabízeno. Zde záleží na uživateli, zda se o toto bude aktivně zajímat.

Obrázek 1: Nastavení statusu na Facebooku



Zdroj: Techbrain.cz, 2021

- Poučte děti o sdílení vlastního i externího obsahu. Každý uživatel po sobě zanechává digitální stopu v online prostředí. Proto je dobré pamatovat na budoucnost, kdy potenciální zaměstnavatel dohledává informace o uchazečích, mimo jiné i na internetu. To, co by v běžném životě uživatel nesděloval náhodným kolemjdoucím na ulici, necht' nesděluje ani na sociálních sítích.
- Buďme občas s dětmi v jejich online prostředí. Zjistíme, co je na tomto prostředí láká a zároveň můžeme společně najít nevhodné a nebezpečné obsahy.
- Nabízejme dětem i společně strávený čas mimo síť. Např. hrou deskových her či procházkou v přírodě.

Na závěr bych použila slova MUDr. Hnízdila: „*To, co se dědí, totiž nejsou nemoci, ale způsoby chování, rodinné vzorce, které k nemoci vedou. Křik, zabavování počítače a příkazy: „Nesed' pořád u toho mobilu, jdi se proběhnout!“ nikam nevedou. Rodiče by měli mít dostatek informací o tom, jaké možnosti a rizika počítačové technologie přinášejí. Měli by být pro děti vzorem ve způsobu, jak s nimi zacházet. Jestliže rodiče sami pěstují pohyb a společenské vyžití, je to pro jejich děti také samozřejmá realita a nemají potřebu utíkat do té virtuální.*“ (Dočekal a kol. 2019, str. 10).

7.6.2 Řešení problému

Pokud již došlo k jakémukoli útoku v kyberprostoru, mohou pomoci následující kroky uváděné na www.e-bezpeci.cz.

1. Ukončete komunikace

Nekomunikujte s útočníkem, nesnažte se ho žádným způsobem odradit od jeho počínání, nevyhrožujte, nemstěte se. Pokud se vám podaří zvládnout tuto fázi, máte možná vyhráno. Útočník to dřív nebo později vzdá, protože jeho námaha nepřinese prakticky žádnou odezvu (E-bezpečí.cz, 2021).

2. Blokujte útočníka

Zamezte útočníkovi přístup k vašemu účtu nebo telefonnímu číslu (zablokujte si přijímání útočnickových zpráv či hovorů, změňte svou virtuální identitu) a je-li to v dané situaci možné, i k nástroji či službě, pomocí které své útoky realizuje (kontaktujte poskytovatele služby). Vzhledem k tomu, že útočník může své virtuální identity jednoduše měnit, blokování mu nemůže definitivně zabránit v dalších útocích. Jde tedy spíše o to znesnadnit mu jeho počínání (E-bezpečí.cz ,2021).

3. Oznamte útok

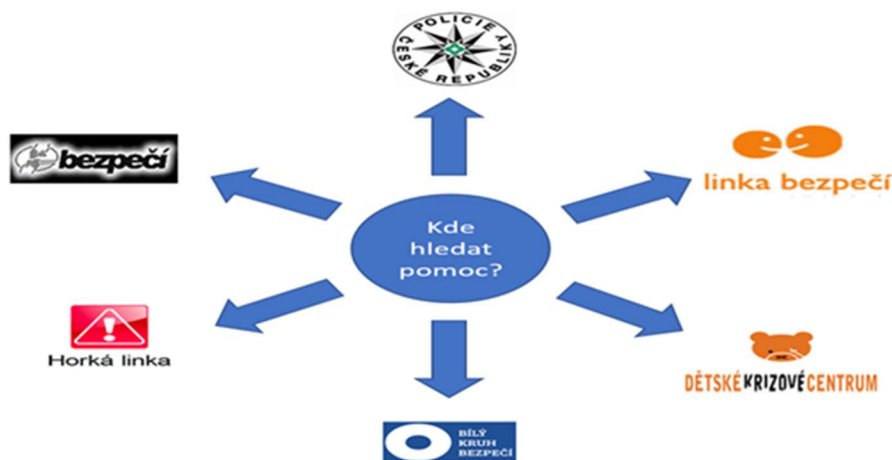
I když se v důsledku útoku můžete cítit poníženi a zranitelní, můžete pociťovat obavy z reakcí okolí apod., nikdy nezůstávejte na řešení problému sami. Svěřte se se svým problémem. Určitě máte ve svém okolí mnoho lidí, kterým na vás záleží a rádi vám pomohou. Navíc vzhledem k tomu, že nebudou osobně zainteresováni, pomohou vám situaci řešit s chladnou hlavou a s určitým odstupem. Možná zjistíte, že i oni se s

podobným problémem někdy dřív setkali a mohou vám tak předat cenné zkušenosti, které při řešení získali. Stane-li se obětí kyberšikany dítě, je velmi důležité, aby o situaci informovalo dospělého člověka – v ideálním případě rodiče, učitele. Dospělí mají mnohem více zkušeností s řešením problémů obecně, proto mohou nabídnout účinnější rady než kamarádi. Dospělí jsou schopni lépe posoudit, kdy je problém natolik závažný, že je pro řešení potřeba zapojit specializované instituce (policii, intervenční služby specializující se na řešení kyberšikany, psychology apod.).

Pro oběť je velmi důležité, aby si uchovávala důkazy kyberšikany (SMS zprávy, e-mailové zprávy, zprávy z chatu, odkazy na webové stránky s problematickým obsahem apod.). Na základě těchto důkazů může být proti útočníkovi či útočníkům zahájeno vyšetřování (E-bezpečí.cz, 2021).

V případě pomoci se lze obrátit na následující organizace:

Obrázek 2: Přehled vybraných organizací poskytujících pomoc obětem napadeným v kyberprostoru



Zdroj: vlastní zpracování

ZÁVĚR

Uživatelé si neuvědomují, že internet je světem, ve kterém se setkávají lidé nejrůznějších zájmů, zaměření a cílů. Stejně jako v reálném, tak i v kybernetickém světě nemusejí být tyto úmysly vždy čisté a pozitivní.

S rozmachem sociálních sítí je tato problematika stále aktuálnější v souvislosti se stoupající popularitou a počtem uživatelů sociálních sítí.

V bakalářské práci bylo mým cílem zjistit jaké povědomí o rizicích v kybernetickém prostředí mají dospělí v roli rodičů a na základě vyhodnocení dotazníkového šetření poskytnout doporučení, jak případným rizikům čelit.

První část byla věnována teorii, kde jsem s pomocí uvedené literatury definovala základní pojmy týkající se kybernetického prostředí a popsala možné dělení sociálních sítí. Další bod teoretické části je věnován rizikovému chování (definice konkrétních rizik a jejich charakteristika) a právní úpravě jednání pachatelů dopouštějících se nebezpečného jednání.

Prostřednictvím dotazníkového šetření jsem v praktické části zjistila, jaké povědomí mají rodiče dětí, které jsou uživateli internetu a sociálních sítí. Dále jsem chtěla zjistit, jaké kroky činí rodiče směrem ke svým dětem v otázce prevence a obeznamenosti konkrétních rizik vyskytujících se na internetu a sociálních sítích. Z výsledku šetření vyplynulo, že nejznámějším rizikem je kyberšikana, kterou spousta rodičů dokáže definovat. Méně známými jsou již pojmy kybergooming, sexting a kyberstalking, ale přesto je rodiče charakterizují správným popisem. Jelikož názvy nejsou ve společnosti tak medializované, nejsou mezi rodiči tolik ukotvené. Z tohoto důvodu by bylo vhodné zvýšit informovanost uživatelů internetu a sociálních sítí.

Vypracování bakalářské práce pro mě bylo velký přínosem a obohacením novými informacemi. Bylo mi touto cestou umožněno provést vlastní dotazníkové šetření, které mě utvrdilo v mých domněnkách, ale zároveň jsem získala nový pohled na celou problematiku rizik v kybernetickém prostředí. Na základě získaných informací je možné v budoucnu provést obdobné dotazníkové šetření, či navázat např. na preventivní přednášky k danému tématu. Je třeba zmínit, že sociální sítě svou otevřeností a rychlým vývojem nabízí prostor pro činnosti a osoby různého charakteru,

proto je nutné dbát zvýšené opatrnosti a celoživotně se v této oblasti vzdělávat. Za připomenutí jistě stojí i závislost na sociálních sítích a internetu vůbec, která je co do počtu nově diagnostikovaných osob, velkým nebezpečím pro další generace.

Jakožto policejní preventista působící na území hlavního města Prahy, bych ráda své poznatky z bakalářské práce předala dále, konkrétně rodičům žáků základních škol. Jednalo by se o preventivní přednášky či besedy na téma Sociální sítě a jejich rizika, které lze realizovat v odpoledních hodinách nebo v rámci třídních schůzek. Přednášky lze nabízet i různým rodičovským sdružením či zájmovým organizacím, kde se rodiče scházejí. Jako hlavní přínos takovýchto preventivních přednášek vidím ve zvýšení informovanosti rodičů k dané problematice a následné preventivní působení rodičů na děti, neboť ti jsou prvotním článkem veškeré prevence.

SEZNAM POUŽITÝCH ZDROJŮ

1. ČERNÁ, Alena et al. Kyberšikana: průvodce novým fenoménem. Vyd. 1. Praha: Grada, 2013. 150 s. Psyché. ISBN 978-80-210-6374-7.
2. DOČEKAL, Daniel a kol. Dítě v síti: manuál pro rodiče a učitele, kteří chtějí rozumět digitálnímu světu mladé generace. První vydání. Praha: Mladá fronta, 2019. 207 stran. Flowee. ISBN 978-80-204-5145-3.
3. ECKERTOVÁ, Lenka a DOČEKAL, Daniel. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. 1. vyd. Brno: Computer Press, 2013. 224 s. ISBN 978-80-251-3804-5.
4. HULANOVÁ, Lenka. Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality. 1. vyd. Praha: Triton, 2012. 217 s. ISBN 978-80-7387-545-9.
5. GIBSON, William. Neuromancer. 2. vyd. Plzeň: Laser-books, 1998. 279 s. Edice SF; sv. 81. ISBN 80-7193-048-2.
6. KOPECKÝ, K., - KREJČÍ, V. Rizika virtuální komunikace (příručka pro učitele a rodiče). 1. vydání. Olomouc: Net University, 2010. 35 s. ISBN 978-80-254-7866-0.
7. KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně n@ internetu: průvodce chováním ve světě online. První vydání. Praha: Grada Publishing, 2016. 175 stran. ISBN 978-80-247-5595-3.
8. PRŮCHA, Jan, MAREŠ, Jiří a WALTEROVÁ, Eliška. Pedagogický slovník. 3., rozš. a aktualiz. vyd. Praha: Portál, 2001. 322 s. ISBN 80-7178-579-2.
9. SCHELLMANN, Bernhard et al. Média: základní pojmy, návrhy, výroba. Vyd. 1. Praha: Europa-Sobotáles, 2004. 482 s. ISBN 80-86706-06-0.
10. ŠEVČÍKOVÁ, Anna a kol. Děti a dospívající online: vybraná rizika používání internetu. Vyd. 1. Praha: Grada, 2014. 183 s. Psyché. ISBN 978-80-210-7527-6.
11. ŠMAHAJ, Jan. Kyberšikana jako společenský problém = Cyberbullying as a social problem. 1. vyd. Olomouc: Univerzita Palackého v Olomouci, 2014. 232 s. Monografie. ISBN 978-80-244-4227-3.

12. VAŠUTOVÁ, Maria a kol. Proměny šikany ve světě nových médií. Vyd. 1. Ostrava: Filozofická fakulta Ostravské univerzity v Ostravě, 2010. 225 s. ISBN 978-80-7368-858-5.

Internetové zdroje:

1. KNOLLOVÁ, J., KŘÍVÁNKOVÁ, K., ŠUTOVÁ, M. Průvodce po sociálních sítích. [online]. [3.3.2021]. Dostupné z:
https://zvolsi.info/app/uploads/2020/01/zvolsi_brozura_digitalni.pdf
2. Cyberspace | communications | Britannica. Encyclopedia Britannica | Britannica [online]. Copyright ©2021 Encyclop [cit. 25.02.2021]. Dostupné z:
<https://www.britannica.com/topic/cyberspace>
3. Most used social media 2020 | Statista. • Statista – The Statistics Portal for Market Data, Market Research and Market Studies [online]. [cit. 03.03.2021]. Copyright © Statista 2021 [cit. 26.02.2021]. Dostupné z:
<https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>
4. Sociální síť. Chapiteau | Reklama a tisk pro umění i podnikání [online]. [cit. 03.03.2021]. Dostupné z: <https://chapiteau.cz/socialni-site-zna-uz-kazde-dite/>
5. Sociální síť LinkedIn: Spojuje lidi napříč profesemi a rozšiřuje pracovní trh. Sociální síť: Rozcestník pro správu a marketing na sociálních sítích [online]. Copyright © 2021. Všechna práva vyhrazena. Icons made by [cit. 25.02.2021]. Dostupné z: <https://sitevhrsti.cz/socialni-site/linkedin/>
6. WhatsApp [online]. [cit. 03.03.2021] Dostupné z: <https://www.whatsapp.com/>
7. Facebook [online]. [cit. 03.03.2021] Dostupné z: <https://cs-cz.facebook.com/>
8. Co je TikTok a jak funguje? Co musí vědět uživatel i marketingový ředitel? Digitální nomádi: Cestuj po světě a pracuj odkudkoli – Jak na to? [online]. Copyright © 2011 [cit. 25.02.2021]. Dostupné z: <https://digitalninomadstvi.cz/tiktok/>
9. Devět let Twitteru: Vše začal památný první tweet z 21. března 2006 - Lupa.cz. Lupa.cz - server o českém Internetu [online]. Copyright © 1998 [cit. 14.03.2021].

Dostupné z: <https://www.lupa.cz/clanky/devet-let-twitteru-pamatny-prvni-tweet-z-21-brezna-2006/>

10. Facebook tipy: jak správně nastavit soukromí na svém profilu? Techbrain | Propojujeme technologie s lidmi [online]. Copyright © 2016 [cit. 26.02.2021]. Dostupné z: <https://techbrain.cz/2016/05/facebook-tipy-jak-spravne-nastavit-soukromi-na-svem-profilu/>

11. Vše o bankách a bankovních produktech: srovnávače, pobočky, bankomaty | Banky.cz [online]. [cit. 03.03.2021]. Dostupné z: <https://www.banky.cz/bankovni-slovník/phishing>

12. Co je to hoax? A proč se posílá? | Buď safe online. [online]. [cit. 03.03.2021]. Dostupné z: <https://www.avast.com/cz/besafeonline/blog/co-je-to-hoax-a-proc-se-posila>

13. Co je počítačový virus? | Nástroj na nalezení a odstranění virů | Avast. [online]. [cit. 03.03.2021] Dostupné z: <https://www.avast.com/cs-cz/c-computer-virus>

14. Netolismus – vše o online závislostech. Netolismus – vše o online závislostech [online]. [cit. 3.3.2021]. Dostupné z: <http://www.netolismus.cz/>

15. Kybergrooming – INTERNETEM BEZPEČNĚ. INTERNETEM BEZPEČNĚ – Užívejme internet bezpečnějším způsobem [online]. Copyright © 2018 INTERNETEM BEZPEČNĚ. Všechna práva vyhrazena. [cit. 14.03.2021]. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/>

16. Kyberkriminalita – Policie České republiky. Úvodní strana – Policie České republiky [online]. Copyright © 2020 Policie ČR, všechna práva vyhrazena [cit. 25.02.2021]. Dostupné z: <https://www.policie.cz/clanek/kyberkriminalita.aspx>

17. 40/2009 Sb. Trestní zákoník. Zákony pro lidi – Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 14.03.2021]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40?text=354>

18. Informace o projektu – E-Bezpečí. Projekt E-bezpečí – E-Bezpečí [online]. [cit. 14.03.2021]. Dostupné z: <https://e-bezpeci.cz/index.php/o-projektu/oprojektu>

19. Bezpečný internet | Rady pro bezpečnost na internetu. Bezpečný internet | Rady pro bezpečnost na internetu [online]. [cit. 14.03.2021]. Dostupné z: <http://www.bezpecnyinternet.cz/>
20. nás. O nás [online]. Copyright © [cit. 25.02.2021]. Dostupné z: <https://www.ncbi.cz/>
21. Dětském krizovém centru – Dětské krizové centrum. Dětské krizové centrum – Odborná pomoc dětem a rodičům [online]. Copyright © Všechna práva vyhrazena, Dětské krizové centrum 2021 [cit. 25.02.2021]. Dostupné z: <https://www.ditekrize.cz/o-detskem-krizovem-centru/>
22. Informace o projektu – KRAJE PRO BEZPEČNÝ INTERNET. KRAJE PRO BEZPEČNÝ INTERNET [online]. Copyright © 2015 [cit. 25.02.2021]. Dostupné z: <https://www.kpbi.cz/o-projektu>

SEZNAM GRAFŮ A OBRÁZKŮ

Seznam obrázků

OBRÁZEK 1: NASTAVENÍ STATUSU NA FACEBOOKU	50
OBRÁZEK 2: PŘEHLED VYBRANÝCH ORGANIZACÍ POSKYTUJÍCÍCH POMOC OBĚTEM NAPADENÝM V KYBERPROSTORU	52

Seznam grafů

GRAF 1: NEJPOUŽÍVANĚJŠÍ SOCIÁLNÍ SÍTĚ NA SVĚTĚ K LEDNU 2021, SEŘAZENÉ DLE POČTU AKTIVNÍCH UŽIVATELŮ (V MILIONECH)	14
GRAF 2: NÁPAD TRESTNÉ ČINNOSTI KYBERNETICKÉ KRIMINALITY	28
GRAF 3: SOCIÁLNÍ SÍTĚ POUŽÍVANÉ RODIČI	32
GRAF 4: VĚK DĚTSKÝCH UŽIVATELŮ	33
GRAF 5: DĚTŠTÍ UŽIVATELÉ SOCIÁLNÍCH SÍTÍ	33
GRAF 6: SOCIÁLNÍ SÍTĚ POUŽÍVANÉ DĚTMI	34
GRAF 7: OD KDY VYUŽÍVAJÍ DĚTI SOCIÁLNÍ SÍTĚ	35
GRAF 8: POMOC PŘI ZALOŽENÍ PROFILU	35
GRAF 9: NEJČASTĚJŠÍ VYUŽITÍ INTERNETU DĚTMI	36
GRAF 10: ČAS TRÁVENÝ DĚTMI NA INTERNETU	37
GRAF 11: ZAŘÍZENÍ UMOŽŇUJÍCÍ DĚTEM PŘIPOJENÍ K INTERNETU	38
GRAF 12: NEBEZPEČNOST INTERNETU A SOCIÁLNÍCH SÍTÍ	38
GRAF 13: ZNALOST RIZIK NA SOCIÁLNÍCH SÍTÍCH	39
GRAF 14: POJEM "KYBERŠIKANA"	40
GRAF 15: POJEM "KYBERGROOMING"	40
GRAF 16. POJEM "SEXTING"	41
GRAF 17: POJEM "KYBERSTALKING"	42
GRAF 18: INFORMOVANOST DĚTÍ O RIZICÍCH	42
GRAF 19: NEJČASTĚJŠÍ PREVENTIVNÍ AKTIVITY KONANÉ RODIČI	43
GRAF 20: METODY PŘIBLÍŽENÍ RIZIK	44

GRAF 21: SLEDOVÁNÍ AKTIVITY DĚTÍ NA INTERNETU	44
GRAF 22: OMEZENÍ PŘÍSTUPU DĚTÍ NA INTERNET	45
GRAF 23: ZAMYŠLENÍ DÍTĚTE NAD ZVEŘEJNĚNÝM OBSAHEM.....	45
GRAF 24: SETKÁNÍ DÍTĚTE S BEZPRÁVÍM V KYBERNETICKÉM PROSTŘEDÍ	46
GRAF 25: REAKCE RODIČŮ NA VZNIKLÝ PROBLÉM V INTERNETOVÉM PROSTŘEDÍ	47
GRAF 26: POHLAVÍ RESPONDENTŮ	47
GRAF 27: VĚK RESPONDENTŮ	48
GRAF 28: VZDĚLÁNÍ RESPONDENTŮ.....	48

SEZNAM PŘÍLOH

PŘÍLOHA Č. 1: VÝČET SKUTKOVÝCH PODSTAT TRESTNÝCH ČINŮ SOUVISEJÍCÍ S RIZIKY V KYBERNETICKÉM PROSTORU.....	62
PŘÍLOHA Č. 2: DOTAZNÍK.....	64

Příloha č. 1: Výčet skutkových podstat trestných činů související s riziky v kybernetickém prostoru

Výčet skutkových podstat trestných činů souvisejících s riziky v kybernetickém prostoru

Některé útoky v kyberprostoru (např. kyberšikana, kybergrooming, sexting) nejsou klasifikovány jako trestné činy nebo přestupky – nemají svou skutkovou podstatu trestného činu. Nutností je klasifikace dle platných ustanovení z. č. 40/2009 Sb., trestního zákoníku.

Paragraf	Název trestného činu	Trestní sazba	Útok v kyberprostoru
§ 140	Vražda	10-20 let	Happy slapping
§ 145	Těžké ublížení na zdraví	3-10 let	Happy slapping
§ 146	Ublížení na zdraví	6 měsíců - 3 roky	Happy slapping
§ 168	Obchodování s lidmi	2-10 let	Kybergrooming
§ 171	Omezování osobní svobody	2-8 let	Kybergrooming, sexting
§ 175	Vydírání	6 měsíců - 4 roky	Kyberšikana, kybergrooming
§ 177	Útisk	až 1 rok	
§ 180	Neoprávněné nakládání s osobními údaji	až 3 roky	Kyberšikana
§ 181	Poškození cizích práv	až 2 roky	Kyberšikana
§ 182	Porušení tajemství dopravovaných zpráv	až 2 roky	Kyberšikana
§ 183	Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí	až 1 rok	Kyberšikana
§ 184	Pomluva	až 1 rok	Kyberšikana
§ 185	Znásilnění	6 měsíců - 5 let	Sexting, kybergrooming
§ 186	Sexuální nátlak	6 měsíců- 4 roky	Sexting, kybergrooming
§ 187	Pohlavní zneužití	1 – 8 let	Sexting, kybergrooming
§ 191	Šíření pornografie	až 1 rok	Kyberšikana, sexting, kybergrooming
§ 192	Výroba a jiné nakládání s dětskou pornografií	až 2 roky	Kyberšikana, sexting, kybergrooming
§ 193	Zneužití dítěte k výrobě pornografie	1-5 let	Kyberšikana, sexting, kybergrooming

§ 193b	Navazování nedovolených kontaktů s dítětem	až 2 roky	Kyberšikana, sexting
§ 201	Ohrožování výchovy dítěte	až 2 roky	Kybergrooming, sexting
§ 202	Svádění k pohlavnímu styku	až 2 roky	Kyberšikana, sexting
§ 205	Krádež	až 2 roky	Kyberšikana
§ 209	Podvod	až 2 roky	Kybergrooming, phishing
§ 228	Poškození cizí věci	až 1 rok	Kyberšikana
§ 230	Neoprávněný přístup k počítačovému systému a nosiči informací	až 8 let	Phising
§ 231	Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	až 5 let	Phising
§ 232	Poškození záznamu v počítačovému systému a na nosiči informací a zásah do vybavení počítače z nedbalosti	až 2 roky	Phising
§ 287	Šíření toxikomanie	až 3 roky	Kyberšikana
§ 352	Násilí proti skupině obyvatelů a proti jednotlivci	až 1 rok	Kyberšikana
§ 353	Nebezpečné vyhrožování	až 1 rok	Kyberšikana, kybergrooming
§ 354	Nebezpečné pronásledování	až 1 rok	Kyberšikana, sexting, kyberstalking, kybergrooming
§ 355	Hanobení národa, rasy, etnické nebo jiné skupiny osob	až 2 roky	Kyberšikana
§ 356	Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod	až 2 roky	Kyberšikana
§ 357	Šíření poplašné zprávy	6 měsíců – 5 let	Hoax
§ 358	Výtržnictví	až 2 roky	Happy slapping

Příloha č. 2: Dotazník

Dobrý den,

ráda bych Vás tímto požádala o vyplnění dotazníku k mé bakalářské práci, která se zabývá zmapováním povědomí rodičů o rizicích v kybernetickém prostředí a orientaci v sociálních sítích.

Jedná se o anonymní dotazník, kdy výsledky budou interpretovány bez spojitosti s osobou respondenta.

Na níže uvedené otázky odpovídejte prosím pravdivě. Vhodnou odpověď zakroužkujte. Není-li u otázky uvedeno jinak, vyberte jednu vhodnou odpověď'.

U otevřených otázek vypište odpověď dle svého uvážení.

Předem děkuji za Váš čas strávený vyplněním dotazníku.

Hana Janelová, ČZU, Institut vzdělávání a poradenství

1. Na jaké uvedené sociální síti máte Vy osobně účet?

(vyberte jednu nebo více odpovědí)

- | | | |
|------------------------|-----------------------------------|-------------|
| a) FACEBOOK | b) TWITTER | c) YOUTUBE |
| d) WHATSAPP | e) INSTAGRAM | f) LINKEDIN |
| g) SNAPCHAT | h) PINTEREST | i) GOOGLE+ |
| j) SKYPE | k) TIK TOK | l) VIBER |
| m) TWITCH | n) NEPOUŽÍVÁM ŽÁDNÉ SOCIÁLNÍ SÍTĚ | |
| o) JINÉ (vypište)..... | | |

2. V jakém věku máte děti?

(vyberte jednu nebo více odpovědí)

- | | | |
|-------------------|--------------|--------------|
| a) PŘEDŠKOLNÍ VĚK | b) 6-7 let | c) 8-9 let |
| d) 10-11 let | e) 12-13 let | f) 14-15 let |
| g) nad 15 let | | |

3. Je Vaše dítě (děti) uživatelem sociálních sítí?

- a) ANO VŠECHNY b) ANO NĚKTERÉ c) NE d) NEVÍM

4. Jaké sociální sítě Vaše děti používají?

(vyberte jednu nebo více odpovědí)

- a) FACEBOOK b) TWITTER c) YOUTUBE
d) WHATSAPP e) INSTAGRAM f) LINKEDIN
g) SNAPCHAT h) PINTEREST i) GOOGLE+
j) SKYPE k) TIK TOK l) VIBER
m) TWITCH n) NEPOUŽÍVAJÍ ŽÁDNÉ SOCIÁLNÍ SÍTĚ
o) NEVÍM p) JINÉ (vypište).....

5. Od jakého věku Vaše dítě (děti) sociální sítě využívají?

.....

6. Pomáhali jste svému dítěti (dětem) při zakládání profilu (úctu) na některé sociální sítě?

- a) ANO, VŠEM b) ANO, NĚKTERÝM
c) NE, POMÁHAL MU SOUROZENEC d) NE, POMÁHAL MU KAMARÁD
e) ZVLÁDLO TO SAMO f) NEMÁ ZALOŽEN ŽÁDNÝ PROFIL

7. Za jakým účelem Vaše děti používají internet?

(očísľujte pořadí aktivit od nejčastěji po méně používanou)

- a) NEVÍM, CO MOJE DÍTĚ DĚLÁ NA INTERNETU
b) POUŽÍVÁNÍ SOCIÁLNÍCH SÍTÍ
c) ČTENÍ A POSÍLÁNÍ E-MAILŮ
d) PRÁCE DO ŠKOLY - VYHLEDÁVÁNÍ
e) HRANÍ ONLINE HER S DALŠÍMI LIDMI
f) SLEDOVÁNÍ VIDEÍ, VIDEOKLIPŮ (YOUTUBE)
g) SDÍLENÍ VIDEÍ A FOTOGRAFIÍ (TIK TOK, INSTAGRAM, APOD.)
h) MOJE DÍTĚ NETRÁVÍ NA INTERNETU ŽÁDNÝ ČAS
i) STAHOVÁNÍ HUDBY NEBO FILMŮ
j) JINÉ

8. Kolik času Vaše děti tráví na internetu (sociálních sítích)?

- a) MÉNĚ NEŽ HODINU DENNĚ b) 1-2 HODINY DENNĚ
c) 3 HODINY DENNĚ d) 4 A VÍCE HODIN DENNĚ
e) PRAKTICKY NEUSTÁLE f) NEMÁM PŘEHLED

9. Z jakého zařízení se Vaše dítě (děti) nejčastěji připojuje k internetu, sociálním sítím?

- a) TELEFON b) PC(NOTEBOOK)
c) TABLET d) TELEVIZE

10. Myslíte si, že internet a sociální sítě mohou být nebezpečné?

- a) ANO b) NE
c) NEVÍM, NEPŘEMÝŠLÍM NAD TÍM

11. Víte, jaká jsou rizika sociálních sítí?

- a) ANO b) NE c) NEZAJÍMÁM SE O TO

12. Vypište jaká konkrétní rizika sociálních sítí znáte.

.....
.....
.....
.....

13. Jedná se podle Vašeho mínění o „kyberšikanu“ v následujícím výroku?

„Spolužáci o mně natočili video, které už viděl každý z naší školy. Už se tam nikdy nevrátím. Jak se jim můžu sám ubránit?“

- a) ANO b) NE
c) NEVÍM d) NEZNÁM UVEDENÝ VÝRAZ

14. Jedná se podle Vašeho mínění o „kybergrooming“ v následujícím výroku?

„Byl na mě tak milý, vůbec jsem si neuvědomila, že se mnou manipuluje. A teď mi začal vyhrožovat, že rozešle mé polonahé fotky mým kamarádům. Nevím, jak dál, má mě v hrsti.“

- a) ANO
- b) NE
- c) NEVÍM
- d) NEZNÁM UVEDENÝ VÝRAZ

15. Jedná se podle Vašeho mínění o „sexting“ v následujícím výroku?

„Poslala jsem svému klukovi svoje lechtivý video, jenže on se teď na mě naštvál a vyhrožuje, že ho dá na internet. Jak mi to může udělat, sliboval přece, že je to jen mezi náma!?“

- a) ANO
- b) NE
- c) NEVÍM
- d) NEZNÁM UVEDENÝ VÝRAZ

16. Jedná se podle Vašeho mínění o „kyberstalking“ v následujícím výroku?

„Nikdy bych nevěřila, že mi bude v patách na každém mém kroku. Jak se ho mám zbavit?“

- a) ANO
- b) NE
- c) NEVÍM
- d) NEZNÁM UVEDENÝ VÝRAZ

17. Bavíte se se svými dětmi o možných rizicích na internetu, sociálních sítích?

- a) ANO
- b) NE, NECHÁVÁM TO NA ŠKOLE
- c) NE, NEMÁM V TOMTO SMĚRU OBAVY

18. Jaká témata preventivních aktivit řešíte nejčastěji se svým dítětem (dětmi)?

(očísľujte pořadí aktivit od nejčastěji po méně používanou)

- a) KOMUNIKACE S NEZNÁMÝMI LIDMI
- b) SEZNAMOVÁNÍ V ONLINE PROSTŘEDÍ
- c) AGRESE NA INTERNETU (KYBERŠIKANA, VYHROŽOVÁNÍ, ATD.)
- d) OCHRANA OSOBNÍCH ÚDAJŮ (ZVEŘEJŇOVÁNÍ FOTEK, JMÉNA, KONTAKTY)
- e) AUTORSKÁ PRÁVA
- f) YOUTUBE A YOUTUBEŘI
- g) ONLINE HRY
- h) ŽÁDNÁ TÉMATA NEŘEŠÍME
- i) JINÁ.....

19. Jakou metodu byste volili pro lepší přiblížení rizik v kyberprostoru vůči svému dítěti (dětem)?

(vyberte jednu nebo více odpovědí)

- a) ROZHOVOR S DÍTĚTEM
- b) VÝMĚNA ROLÍ – RODIČ NASLOUCHÁ A UČÍ SE OD DÍTĚTE
- c) c)SLEDOVÁNÍ PREVENTIVNÍHO FILMU ZAMĚŘENÉHO NA DANOU PROBLEMATIKU
- d) NÁVŠTĚVA ODBORNÉ PŘEDNÁŠKY
- e) ZÍSKÁNÍ INFORMACÍ Z WEBOVÝCH STRÁNEK ZABÝVAJÍCÍCH SE DANOU PROBLEMATIKOU

20. Sledujete aktivitu svých dětí na internetu? (např. historie v prohlížeči, Family Link, aj.)

- a) ANO, PRAVIDELNĚ
- b) ANO, OBČAS
- c) NE

21. Omezujete svým dětem přístup na internet?

- a) NE, NIJAK PŘÍSTUP NEOMEZUJI
- b) ANO, ÚSTNÍ DOHODOU – BEZ KONTROLY
- c) ANO, ÚSTNÍ DOHODOU – S NÁSLEDNOU KONTROLOU
- d) ANO, ODEBRÁNÍM TECHNIKY
- e) ANO, KONTROLOU HISTORIE
- f) ANO, POMOCÍ APLIKACE NEBO PROGRAMU RODIČOVSKÉ KONTROLY, ZÁMKU

22. Přemýšlí Vaše dítě (děti) nad tím, jaký obsah – příspěvek, foto zveřejňuje?

- a) ANO
- b) NE
- c) NEVÍM

23. Setkalo se Vaše dítě v kybernetickém prostředí (internet, sociální sítě) s nějakým bezprávím (např. kyberšikana, stalking)?

- a) ANO, OSOBNĚ
- b) ANO, PROSTŘEDNICTVÍM KAMARÁDA
- c) NE
- d) NEVÍM

24. Jak byste reagoval/a, kdyby se Vám dítě svěřilo, že má v internetovém prostředí problémy?

(vyberte jednu nebo více odpovědí)

- a) NEŘEŠIL/A BYCH TO
- b) KONTAKTOVALA BYCH PŘÍMO KONKRÉTNÍ OSOBU(PACHATELE) NA INTERNETU
- c) OBRÁTIL/A BYCH SE NA POLICII ČR
- d) PROVEDL/A BYCH BLOKACI ÚČTU KONTRÉTNÍ OSOBY (PACHATELE) NA INTERNETU
- e) OBRÁTILA BYCH SE NA OSPOD
- f) ŘEŠIL BYCH TO JINAK (uved'te):

.....

25. Jakého jste pohlaví?

- a) ŽENA
- b) MUŽ

26. Kolik je Vám let?

- a) 20-30 b) 31-40 c) 41-50 d) 51 a více

27. Jaké je Vaše nejvyšší dosažené vzdělání?

- a) ZŠ b) VYUČEN/A c) SŠ S MATURITOU
d) VOŠ e) VŠ