Opatření pro zvýšení bezpečnosti uživatelů sociálních sítí

Tereza Hrachovcová

Bakalářská práce 2020

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tereza Hrachovcová**
Osobní číslo:	**L17437**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Opatření pro zvýšení bezpečnosti uživatelů sociálních sítí**

Zásady pro vypracování

1. Zpracujte rešerši současného stavu předmětné problematiky.
2. Identifikujte hrozby spojené s užíváním sociálních sítí.
3. Navrhněte opatření pro zvýšení bezpečnosti uživatelů na sociálních sítích.
4. Sumarizujte získané výstupy a tyto znázorněte graficky.

Rozsah bakalářské práce:
Rozsah příloh:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. *Děti a dospívající online*. Praha: Grada Publishing,2014. ISBN 978-80-247-5010-1.
2. *Internetová kriminalita páchaná na dětech*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.
3. *Kyberšikana*. Praha: Portál, 2011. ISBN 978-80-7367-984-2.
Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. listopadu 2019**
Termín odevzdání bakalářské práce: **15. května 2020**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2019

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- 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 (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 15. 5. 2020

Jméno a příjmení studenta: Tereza Hrachovcová

.....
podpis studenta

ABSTRAKT

Bakalářská práce se zaměřuje na bezpečnostní opatření spojená s užíváním sociálních sítí. V teoretické části jsou zmíněny důležité pojmy související s touto problematikou a popsány jednotlivé druhy rizik a zavedená opatření. Praktická část obsahuje dotazníkové šetření, ve kterém bylo cílem zjistit popularitu sociálních sítí u dětí. Dále vzhledem k navrhnutým opatřením byla otestována bezpečnostní mobilní aplikaci a počítačový software. V závěru mé práce jsem ilustrovala skryté hrozby sociálních sítí, se kterými se děti mohou setkat a popřípadě jak se takovým hrozbám vyhnout.

Klíčová slova: bezpečnostní opatření, Facebook, internet, kyberšikana, ochrana dětí, rizika sociálních sítí, sociální sítě.

ABSTRACT

The central theme of this bachelor thesis is safety measures connected with social media using. The theoretical part of this study explores important terms related to these issues including particular types of risks posed to children online as well as established measures. The key issue focused on in the practical part was a survey, aimed to examine the popularity of social media among children. Subsequently, considering the suggested measure, the effectiveness of the safety mobile application and computer software were assessed. In conclusion, hidden threats of social media, which can child user be exposed to, and how to avoid these threats were exemplified.

Keywords: child protection, cyberbullying, Facebook, internet, risks of social media, safety measures, social media.

Ráda bych poděkovala vedoucímu mé práce panu Ing. Petru Svobodovi, Ph.D. za odborné vedení a cenné rady při zpracování mé bakalářské práce. Kamarádovi Richardu Moštěkovi, který mi pomohl s ilustracemi obrázkových karet pro děti. A dále děkuji celé mé rodině a všem blízkým za podporu v průběhu studia na této fakultě.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Sociální sítě jsou v dnešní době celosvětovým fenoménem. Jsou populární jak u dospělých, tak především u dětí. Denně sociální sítě navštíví miliony lidí za účelem, aby se pobavili, dozvěděli se nové věci nebo se třeba seznámili. Sociální sítě ale nejsou jen komunikačním nástrojem. Můžete na nich poslouchat třeba hudbu nebo zadarmo propagovat například svůj projekt či podnik. Tyto funkce mohou být velmi atraktivní a výhodné například pro podnikatele. Dále pomocí nich můžete plnit různé úkoly do školy či práce, protože na internetu najdete všechny informace, které potřebujete.

Sociální sítě s sebou nesou kromě výhod také spoustu rizik. Díky modernizaci a velkým nárokům uživatelů jsou sítě a celkově internet čím dál víc usnadňovány na úkor bezpečí. Zjednodušuje se přístup a přihlášení do aplikací a účtů, na internetu hrozí dětem daleko větší nebezpečí v podobě různých pedofilů, kyberšikany a sextingu. Dospělým může hrozit nabourání se do počítače hackery a zneužití různých přihlašovacích údajů a hesel a dalších plno nástrah.

Abychom zabránili případným rizikům, můžeme předejít použitím některých z bezpečnostních opatření. Základní opatření by měl zvládnout a znát každý uživatel sociálních sítí. Instalace některých složitějších opatření v podobě softwaru je již individuální. Záleží však na přístupu. Pokud se člověk cítí ohrožený, udělá maximum pro to, aby se cítil bezpečněji. Spousta lidí se ale nijak nechrání. Myslím, že každý dospělý by měl mít svůj obsah na sociálních sítích pod kontrolou. Pokud ale ne, měl by vykonávat dohled alespoň nad svým dítětem, které ještě nemusí mít dostatečný rozum na to, aby vědělo, co může sdílet a co ne. Už tohle považuji za jedno z velmi důležitých opatření, díky kterému jsem se rozhodla zaměřit mou bakalářskou práci zejména na děti.

Cílem této bakalářské práce je zpracování rešerše současného stavu předmětné oblasti, vymezení důležitých souvisejících pojmů, seznámení se s riziky na sociálních sítích a navržení opatření pro zvýšení bezpečnosti uživatelů sociálních sítí.

I. TEORETICKÁ ČÁST

1 VYMEZENÍ JEDNOTLIVÝCH POJMŮ

Nejprve si vysvětlíme význam velice důležitých pojmů, o kterých celá má bakalářská práce je. Řekneme si, jak vznikl dnešní populární internet a jeho stručnou historii, poté navážeme na dnešní fenomén sociální sítě. Přiblížím druhy sociálních sítí a bezpečnostní opatření. Na závěr popíšu dvě nejpopulárnější sociální sítě, které se vyskytují u nás v České republice, mezi ty se řadí Facebook a Instagram.

1.1 Internet

V dnešní době je internet součástí našeho života. Na internetu můžeme nakupovat prostřednictvím internetových obchodů tzv. e-shopu, můžeme si psát nebo komunikovat s přáteli z druhého konce světa nebo vyhledávat informace různého druhu pomocí klíčových slov, které se zadají do vyhledávače. Zkrátka internet nám usnadňuje nejen čas, ale také peníze, jelikož mnoho věcí je na internetu dostupných zdarma. S výhodami, které nám internet v dnešní době přináší, přichází také řada nevýhod.

1.1.1 Historie internetu

Historii vzniku internetu můžeme spojit s počátkem studené války, kdy tehdejší ARPANET sloužil jako experimentální program Spojených států amerických. Cílem tohoto programu bylo zaručit rychlejší přenos informací mezi armádou národní obrany a univerzitními laboratořemi, aniž by nad tím bylo zapotřebí vykonávat lidský dohled. (Hulanová, 2012) Problémy s internetovou bezpečností se ale začaly řešit až na přelomu osmdesátých a devadesátých let minulého století, kdy poprvé začal kolovat sítí celého světa počítačový virus. V dnešní době viry ale fungují jinak. V podstatě jsou velice těžko odhalitelné. Útočník se snaží získat informace z vašeho počítače, které by následně mohl využít ve svůj prospěch. Tvůrci viru to mají dnes ještě jednodušší díky sociálním sítím, kdy jim stačí vymyslet dostatečně zajímavé téma, zveřejnit ho na sociálních sítích, a pak už to jen nechat na lidech, kteří díky své zvědavosti začnou klikat na příspěvek a vir začnou nevědomě šířit. (Eckertová, Dočekal, 2013)

1.1.2 Žebříček příležitostí

Internet lidem a především dětem přináší také kromě rizik spoustu příležitostí a možností ke kreativitě. Může být využíván ke vzdělávání, tvorbě webových stránek, k práci s různými programy všeho typu a k mnoha dalším užitečným a rozvíjejícím věcem.

Hovoříme tedy o žebříčku příležitostí, to znamená, že čím výše dítě v žebříčku stoupá, tím více využívá příležitostí, které mu internet nabízí. Vědci z organizace EU Kids online vytvořili žebříček následovně.

Na nejnižším stupni jsou všechny děti, které doma internet používají, hrají na něm hry a využívají jej ke vzdělávání. O stupeň výše jsou děti, které internet využívají zejména ke sledování online videí. Internet tak poskytuje dítěti jak informace, tak i zábavu. Dalším krokem je používání internetu ke komunikaci s kamarády. K tomuto se používají z velké části sociální sítě, kde můžete komunikovat online nebo využívat videohovory. Poslední stupeň zahrnuje hraní online her, stahování filmů a hudby. Do této úrovně ale dosahuje 56 % Evropanů a z toho pouze jedna třetina dětí ve věku 9–10 let. (Ševčíková a kolektiv, 2014)

1.1.3 Kybernetické útoky na internetu

O kybernetickém útoku se hovoří tehdy, je-li počítač napaden jedním nebo vícero nebezpečnými či nevyžádanými padouchy. Používají k tomu speciálně zaměřený software, který dokáže napadnout obyčejný počítač připojený k internetu. Útok probíhá tak, že s vaším počítačem někdo začne po sítí komunikovat. Dochází tak k výměně datových paket. Útočník komunikaci spouští opakovaně, tím počítač zcela zahltí. O rozloženém odmítnutí služby neboli Distributed Denial of Server (DDoS) se mluví tehdy, jestliže bylo k útoku použito více počítačů, které tuto akci zintenzivnili. Opatření, která mohou takovému jednání zamezit, jsou zpravidla stejně jednoduchá jako samotný útok. K tomu se používá firewall, který sleduje neustálé spouštění komunikace. Napadený si může v nastavení omezit maximální počet datových spojení za sekundu, a tím tak většině rizik zamezit. (Petrowski, 2014)

1.1.4 Netiketa

Pojem složený ze slova NET (net = zkratka pro slovo internet) a slova ETIKETA (etiketa = pravidla slušného chování), vyjadřuje určitá pravidla, jak by se člověk měl na internetu a zejména sociálních sítích chovat v zájmu slušného chování.

1) Lidé by neměli zapomínat, že na druhé straně počítače jsou také lidé. To znamená, že by se nemělo psát to, co nikdy neřeknete do očí.
2) Nevhodné chování v běžném životě se nehodí ani na internet.
3) Nesmějí se porušovat autorská práva.
4) Nerozesílat spam.
5) Nešířit žádné falešné poplašné zprávy.
6) Respektovat soukromí. Pokud přijde nějaká zpráva, která vám nebyla určena, smažte ji a odesílatele taktně informujte o omylu. Nebo pokud se na vašem zařízení osoba ze svého účtu neodhlásí, neprocházejte si jeho soukromé zprávy. Osobu informujte a následně ji odhlašte.
7) Nešířit lživé informace o ostatních. (Eckertová, Dočekal, 2013)

1.2 Sociální sítě

Sociální sítě mohou být někdy známy pod zkratkou SNS neboli Social Networking Sites. Sociální sítě jsou v dnešní době používány celosvětově. Jsou populární především tím, že mezi sebou mohou komunikovat přátelé, známí či příbuzní z opačných konců světa. (Petrowski, 2014) Lidé tuto internetovou službu využívají především kvůli tomu, že mohou vytvářet veřejné, soukromé ale i firemní profily, prezentace a mohou se účastnit v diskuzních fórech. Oblíbené jsou tematické skupiny, kde si účastníci mohou vyměňovat své zkušenosti a předávat si rady. (Kožíšek, Písecký, 2016) Podle výzkumu z roku 2018 využívalo sociální sítě 50,1 % mužů nad 16 let a 53,1 % žen nad 16 let. Lidé na sociálních sítích mohou také prezentovat své vlastní fotografie, sledovat a komentovat fotky svých přátel nebo si prohlížet fotografie cizích lidí. S takovýmto množstvím aktivit se ale také zvyšuje riziko možných sexuálních útoků, podvodů a zejména hrozí ukradení identity a s tím spojená ztráta soukromí. (Petrowski, 2014) Sociální sítě lákají různé pedofily, dále také může docházet k vydírání, sexuálnímu obtěžování nebo šikaně. Nejčastějšími obětmi se pak stávají zejména děti, které jsou na sociálních sítích zranitelnější. (Hulanová, 2012) To, že jsou sociální sítě čím dál víc populárnější, dokazuje i nárůst uživatelů, který se z roku 2010 a 0,97 miliardy uživatelů zvýšil v roce 2018 na neuvěřitelných 2,5 miliardy uživatelů. Při obývání planety

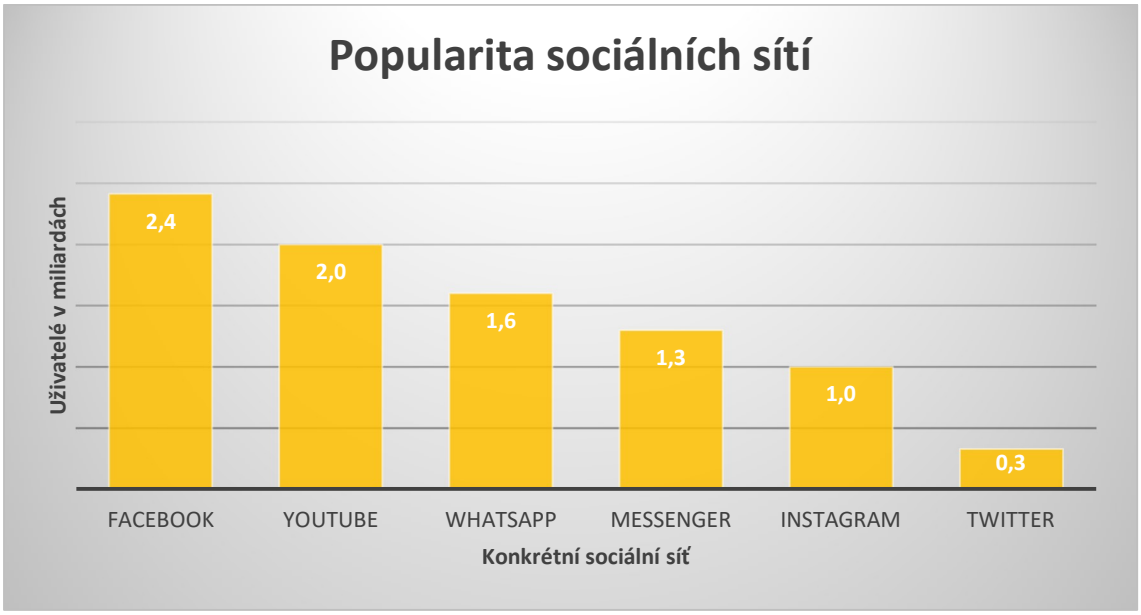
Země 7,2 miliardy lidí se tedy jedná o větší třetinu lidské populace. (Internetem bezpečně, 2018)

- **Celosvětový fenomén Facebook**

Facebook byl založen několika studenty z Harvardské univerzity v čele s Markem Zuckerbergem. Byl vytvořen za účelem pomoci prvním ročníkům se lépe orientovat v novém prostředí a na univerzitě. Již tehdy byl velice populární a je tomu tak i dodnes. (Petrowski, 2014) K listopadu roku 2019 je na Facebooku téměř 2,41 miliardy registrovaných uživatelů. (Internetem bezpečně, 2018) Jedním z důvodů založení a zároveň prvotním rozdílem bylo to, že se na Facebook kromě fotek, videí a profilů, jako tomu bylo u mnoha dalších sociálních sítí, mohl přidávat i tzv. vybraný příspěvek. Lidé si tak mohli zobrazit aktuální informace o svých přátelích. Pokud si představíme popularitu Facebooku mezi studenty, nemůžeme se divit, že i kantoři či bývalí spolužáci chtějí spolu zůstat v kontaktu. Což jim právě tato sociální síť umožňuje. (Petrowski, 2014) Na Facebook se může zaregistrovat jakákoliv osoba starší 13 let. Ve skutečnosti ale víme, že věk se při registraci nijak neověřuje, tudíž není problém se zaregistrovat v mnohem mladším věku. Ve výsledku to vypadá tak, že pro děti na základní škole je používání Facebooku zcela běžné a málokdy se objeví dítě, které nemá vytvořený profil. Velmi často také dochází k tomu, že rodiče nemají ponětí o tom, že dítě Facebook využívá nebo s kým po síti dítě komunikuje a s kým se přátelí. Dalším nebezpečím je například sdělování osobních informací. Děti zde mají pocit soukromí, ale ve skutečnosti tomu tak není. Již při samotném zakládání facebookového účtu se musí uvést jméno, příjmení, datum narození a e-mailová adresa. (Eckertová, Dočekal, 2013) Může se také vyplnit spousta dalších informací tykajících se vzdělání, zaměstnání, rodinných vztahů, informace o koníčcích a zájmech. Dále se zde dají přidávat fotky, ale bohužel většina z nich je často nevhodná. Při vkládání fotografií je třeba zvážit, které na sociální síť umístit a které raději ponechat v soukromí počítače. Právě nevhodné fotografie mohou být využity například pro ještě nevhodnější úpravu a následné vydírání, nebo se mohou objevit v rukou pedofilů či jiných úchylů. Velkým varováním je i fakt, že Facebook si všechny informace, které se do něj zadají, archivuje. Nepomůže nám ani, když si upravíme nastavení nebo smažeme účet. Jelikož tato sociální síť pochází ze Spojených států amerických, ochrana osobních údajů nespadá pod náš zákon č. 101/2000 Sb., o ochraně osobních údajů ale řeší se podle americké legislativy. Proto jsou zásady ochrany osobních údajů služby Facebook dostupné pouze v anglickém jazyce. (Kulhánková, Čamek, 2010)

- **Populární Instagram**

Sociální síť, která je zaměřena zejména na svůj vizuální obsah, má dnes téměř miliardu uživatelů. Poprvé se objevila 6. října roku 2010. Hlavní pointou aplikace je přidávání fotografií a videí s trochou obsahu. Pomocí této aplikace se mohou lehce a hlavně zdarma prezentovat i malé či větší firmy nebo neziskové organizace, zkrátka kdokoliv. (Hošková, 2018) Instagram některé celebrity využívají jako zdroj financí. Probíhá to tak, že dělají reklamu určité firmě, která jim nabídne spolupráci. Poté jen testují, recenzují a sdílí jejich produkty, zboží, oblečení, jídlo, hotely a vše, na co si vzpomenete.



Obr. 1 Graf – popularita sociálních sítí

Zdroj: Sociální sítě, internetembezpecne.cz (vlastní zpracování)

2 JEDNOTLIVÉ DRUHY RIZIK

Internet s sebou přináší nejenom spoustu výhod, ale také mnoho rizik. Kromě toho, že každý počítač, který je připojen k internetu, je vystaven útokům ze stran různého malwaru, anonymita, která internetem koluje, dává uživatelům pocit, že mohou od ostatních cokoliv chtít. Pokud ale srovnáme skutečný svět s tím virtuálním, není ani jeden více či méně nebezpečný. Přináší ale nová rizika, které se musíme naučit vnímat, rozpoznat je a nějak na ně reagovat. Například mnoho rodičů děti varuje, ať se nebaví s cizími lidmi a nikam s nimi nechodí, ale je spíše výjimečné, pokud rodiče varují své děti, aby nechatovali s cizími lidmi. (Eckertová, Dočekal, 2013)

2.1 Kyberšikana

S tímto tématem úzce souvisí pojem kyberprostor nebo anglicky cyberspace. Nejprve se tento pojem začal objevovat ve sci-fi literatuře, později však pronikl také do podvědomí lidí a dnes už se vyskytuje zcela často. Kyberprostorem rozumíme prostor, který je tvořen moderními technologiemi a zpravidla vše se v kyberprostoru děje virtuálně.

Kyberšikana je novější forma šikany, kdy skupina lidí nebo jedinec ohrožuje, vydírá či psychicky týrá druhého. Může jít buď o úmyslnou, nebo neúmyslnou formu šikany. Tuto hranici je velice těžké určit. Spousta dětí právě tohle vnímá často pouze jako vtip, který neměl oběti ublížit, ale bohužel se vymkl kontrole. (Eckertová, Dočekal 2013) Pojem kyberšikana není v České republice posuzována jako trestný čin. Může ale naplnit znaky skutkové podstaty trestného činu, protože v kyberšikaně může docházet k vydírání, vyhrožování či ke stalkingu, které jsou podle trestního zákona trestný čin. Kyberšikana se od šikany liší tím, že agresor je často anonymní, a tím má větší pocit bezpečí a nezjistitelnosti jeho skutku. Toto zdání je ale mylné, jelikož internet v podstatě anonymní není. Vše je dopátratelné i zpětně. Zatímco u obyčejné šikany se agresor s obětí dostává do přímého kontaktu. Dále kyberšikana může probíhat úplně kdekoliv. Jelikož probíhá v kyberprostoru, oběť se tak může vyskytovat ve školní družině, v zájmovém kroužku nebo třeba doma a zároveň může být šikanována prostřednictvím textových zpráv, sociálních sítí nebo přes e-mail. Mezi další rozdíly můžeme zařadit to, že kyberšikana ve své podstatě může trvat 24

hodin denně. Zatímco u šikany, kdy se oběť s agresorem potkají tváří v tvář, může trvat pouhých pár minut nebo hodin. (Rogers, 2011)

Kyberšikana ale není jen záležitostí dětí a dospívajících, ale může se také dotýkat i dospělých. Americká právnička Nancy Willard rozdělila tuto problematiku do sedmi kategorií, které se vztahují jak na děti, tak dospělé.

- Online válka – pachatel posílá oběti nevhodné, vulgární zprávy prostřednictvím online komunikačních prostředků. Cílem je vyvolat hádku.
- Online obtěžování – pachatel posílá nechutné, urážlivé zprávy přes e-mail nebo jiné sítě. Takovéto zprávy oběť obtěžují.
- Kyber pronásledování – pachatel oběť online pronásleduje a vyhrožuje jí.
- Očerňování – útočník o oběti rozesílá nepravdivé informace ostatním uživatelům.
- Přetvařování se za někoho jiného – pachatel se na sociálních sítích vydává za svou oběť. Cílem tohoto útoku je zostudit opravdovou oběť.
- Odhalování intimností – pachatel o oběti zveřejňuje osobní, citlivé informace nebo fotky. Zveřejní je na sociálních sítích anebo přeposílá do soukromých zpráv.
- Vyloučení – pachatel oběť vyloučí z online skupiny

2.1.1 Star Wars Kid

První případ, kdy byla zaznamenána kyberšikana a začala se touto problematikou také zajímat široká veřejnost, pochází z kanadského Quebecu, kdy se obětí stal patnáctiletý chlapec přezdívaný také jako Star Wars Kid. Nechal se natočit svým kamarádem, jak se neúspěšně snaží ztvárnit postavu ze Star Wars. Chlapcův spolužák video umístil na internet, kde po několika hodinách mělo stovky zhlédnutí. Po tom, co se to mladý chlapec dozvěděl, se psychicky zhroutil a musel se dlouho léčit. Video také někteří lidé různě upravovali grafickými či zvukovými efekty, a tak chlapce více zesměšnili. Video se na internetu vyskytuje dodnes. (Hulanová,2012)

2.1.2 Ryan Halligan

Tento mladý americký chlapec trpěl vývojovými obtížemi, kvůli kterým se později stal obětí psychické šikany ze strany svých spolužáků. Rodiče začali navštěvovat terapeuta, díky kterému se jeho motorické a řečnické obtíže výrazně zlepšily, a proto s terapií mohl skončit. Šikana od spolužáků ale neskončila a vše vyvrcholilo o dva roky později. Chlapec ze strachu nechtěl chodit do školy. Informovat vedení školy ale rodičům nedovolil a rozhodl se

spolužákům postavit sám. Naučil se bojové umění a svému trýzniteli se s úspěchem postavil. Spolužák ale Ryana označil za gaye. Proto se Ryan o prázdninách začal online kamarádit s populární a pěknou studentkou na jejich škole. Když se ji ale po čase rozhodl osobně oslovit, dívka mu dala přede všemi jasně najevo, že se celou online komunikací jen bavila a nechce s ním mít nic společného. Celé to bylo promyšlené tak, aby z něho dívka vylákala důvěrné informace, nad kterými se potom všichni bavili. Ryan nátlak neunesl a doma v koupelně se oběsil. Jeho otec se po tomto incidentu rozhodl, že se bude snažit pomoct lidem, kteří se do této situace mohli také dostat a bude zvyšovat povědomí lidí o kyberšikaně a sebevraždách mladistvých. Dále se taky zasadil o přijetí zákona o prevenci šikany. (E-bezpečí, 2019)

2.2 Kybergrooming

Pod tímto pojmem si můžeme představit lákání oběti na schůzku. U tohoto druhu kriminality může jít buď o pachatele, který předstírá, že je někdo jiný, anebo oběť ví, kdo je skutečně osoba, s kterou je v kontaktu. Kybergrooming můžeme popsat tak, že pachatel neboli groomer si vymyslí falešnou identitu na sociální síti, s úmyslem nejprve u oběti získat důvěru a vylákat z ní intimní fotografie. Následně jej nalákat na schůzku, kde zpravidla dojde ke znásilnění. Je to docela snadné, neboť děti tráví spoustu času na sociálních sítích zejména kvůli tomu, aby si zde našly nové kamarády. Proces kybergroomingu může probíhat v následujících etapách.

- Pachatel se nejprve snaží u oběti získat důvěru. Staví se do pozice, kdy je jeho nejlepší a jediný přítel, který mu rozumí. Mají spoustu společných zájmů a stejné problémy, například s rodiči, ve škole, v zájmovém kroužku a s těmito problémy mu může pomoct. Snaží se zjistit o oběti informace jako je adresa, místo bydliště, e-mail, telefonní číslo a další důležité informace. Útočník se také snaží rozdělit oběť od okolí. Právě proto, aby se o jejich kontaktu nikdo nedozvěděl.
- Groomer podporuje vztah tím, že oběti kupuje různé dárky. Ať už to jsou sladkosti, drahé hračky a šperky, snaží se tak oběť nějakým způsobem umlčet a zároveň podpořit svou důvěru.
- Další etapou je emoční závislost na groomerovi. Oběť se nesvěřuje svým rodičům ani kamarádům o svých problémech a často jim lžou o tom, s kým se ve svém volném čase kamarádí. Dítě důvěřuje pouze groomerovi, který o něm ví všechno.

- Dále následuje osobní setkání, pokud k němu nedošlo již dříve. Útočník vyláká oběť například do kina, na procházku do parku, anebo přímo k sobě do bytu.
- Poslední etapou je sexuální obtěžování. V mnoha případech ale dojde i k sexuálnímu zneužití. (Hulanová, 2012)

2.3 Kyberstalking

Pod tímto pojmem si představíme slídila neboli stalkera, který svojí oběti posílá obtěžující e-maily, SMS zprávy nebo zprávy z jiných komunikačních prostředků. Jde o zprávy se sexuálním podtextem či výhružné zprávy o zničení jejího života či ublížení na zdraví. Tyto zprávy jsou často doprovázeny agresivním chováním a oběť je tak vystavována velkému psychickému nátlaku. (Hulanová,2012) Stalkeři pocházejí z různých společenských vrstev a svou oběť si mohou například vybírat dlouhodobě dopředu. Může taky jít o člověka, který pachatele nějakým způsobem zajímá či přitahuje, ale city oběti nejsou opětované. Může ale jít o náhodně vybranou oběť. Sklony k nebezpečnému pronásledování mají ve velké míře expartneři. Jejich chování nesou známky manipulace a vydírání. Stalking neboli nebezpečné pronásledování je uvedeno jako trestný čin v trestním zákoníku, konkrétněji v paragrafu 354.

(1) Kdo jiného dlouhodobě pronásleduje tím, že:
   a) vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým,
   b) vyhledává jeho osobní blízkost nebo jej sleduje,
   c) vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontroluje,
   d) omezuje jej v jeho obvyklém způsobu života, nebo
   e) zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu, a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

(2) Odnětím svobody na šest měsíců až tři roky bude pachatel potrestán, spáchali čin uvedený v odstavci jedna
   a) vůči dítěti nebo těhotné ženě,
   b) se zbraní, nebo
   c) nejméně se dvěma osobami.

Stalking se projevuje docela viditelně. Útočník používá přímé nebo nepřímé výhružky. Často za oběť uvádí sám sebe. Dále se skutečné oběti mstí a snaží se ji očernit nepravdivými informacemi. Pronásleduje ji cestou do práce, do školy nebo třeba na nákup. Může používat i výhružky fyzického napadení. Lidé mají možnost se ale bránit. Jednou z nich je takové jednání nahlásit administrátorovi služeb. Pokud ale k takovýmto napadením dochází na internetové stránce docela často a administrátoři to ignorují a tento problém neřeší, není nic jednoduššího než takovéto stránky nenavštěvovat. Dalším řešením je svěřit se o problému se stalkerem osobě blízké, anebo ihned kontaktovat policii. (Kožíšek, Písecký 2016)

2.4 Sexting

Pod pojmem sexting rozumíme zasílání textových zpráv, videí nebo fotografií se sexuálním podtextem. S tímto problémem souvisí masové používání moderních informačních technologií. Tato problematika může být rozdělena do dvou úrovní. Jedna úroveň probíhá mezi partnery a druhá mezi zcela neznámými lidmi. Obě dvě úrovně jsou velmi rizikové. Zvláště pokud dochází k sextingu mezi partery se na první pohled může zdát bezpečné, neboť v první momentě partnerovi věříte. V mnoha případech ale dochází po rozchodu k vydírání. Někdy je na oběť vyvíjen takový nátlak, že to může skončit sebepoškozováním až sebevraždou. Nejprve, než je lechtivá fotografie partnerovi poslána, je dobré položit si pár základních otázek: Mám tak obrovskou důvěru ve svém partnerovi, že fotografie nikdy nezneužije proti mně? Budu mít v něm tu stejnou důvěru o několik let později? Popřípadě jsou to takové fotografie, za které bych se po zveřejnění mohla stydět? Vyvěsila bych tu samou fotografii na nástěnku v domě či zaměstnání? Pokud u těchto otázek dochází k zaváhání, nic by se nemělo odesílat. Důvodů, proč je sexting nejrizikovější je mnoho. Jedním z nich je například obava, že citlivý materiál, který byl odeslán, se může na internetu nebo jiných místech kdykoliv objevit. Slibu, že partner fotky nikde nezveřejní, nemůžete nikdy stoprocentně věřit. Dalším důvodem, proč je sexting nebezpečný je i důvod možného vydírání. Kdy pachateli jedna zaslaná lechtivá fotografie nestačí a požaduje další. Pokud oběť tak neučiní, dochází k vydírání o zveřejnění na sociální síti. Provozování sextingu s nezletilými je považováno za obzvlášť závažné a je tedy posuzováno jako šíření dětské pornografie či ohrožování mravní výchovy apod. Tento druh „zábavy“ je na internetu velice populární a velmi často vyhledávaný. Více informací zabývající se dětskou pornografií nám poskytuje zákon č. 40/2009 Sb., trestní zákoník, konkrétněji paragraf 192 – výroba a jiné nakládání s dětskou pornografií a paragraf 193 – zneužití dítěte k výrobě pornografie.

Existuje několik rad, jak při tomto problému postupovat a eliminovat následky. V první řadě je velmi důležité dát útočníkovi najevo, že se vám jeho chování nelíbí a okamžitě s ním přestat komunikovat. Zazálohujte si veškerou komunikaci s ním a odeberte si ho z přátel, aby bylo zamezeno kontaktování vašich přátel. Neprodleně poté informovat policii a jako důkazní materiál poskytnout zazálohovanou komunikaci. Tento krok je velice důležitý, neboť pachatel nemusí mít jen jednu oběť. Tím, že tento čin bude nahlášený, můžete pomoci i dalším obětem. Pokud si ale nejste jistí, jak v tomto případě postupovat, můžete kontaktovat i specializované poradny jako je například projekt e-bezpečí, linka bezpečí nebo dětské krizové centrum. Je dobré mít na paměti, že i když jde o velice citlivý materiál, vše se dá řešit anonymně. A pokud pachatel tvrdí, že je nedohledatelný, není to pravda. Každý za sebou zanechává digitální stopy, které se dají vypátrat. (Kožíšek, Písecký 2016)

2.4.1 Roztahovačky

Velmi známý případ související s touto problematikou nese název „roztahovačky“. Při této kauze byla zneužita populární aplikace Snapchat, ze které se nashromáždily vyzývavé fotografie dívek. Konkrétněji došlo k založení facebookové stránky, která nesla název „Pražské roztahovačky“. Tuto stránku tvořily intimní fotografie dívek, které tam přidávali členové skupiny. Fotografie byly odeslány dívkami chlapcům přes sociální sítě, zejména již zmíněný Snapchat. Fotografie byly doplněny informacemi o dívkách, jejich popisem a zda se jedná o amatérku či své služby poskytuje za peníze. Dále se začaly vyskytovat tyto stejnojmenné skupiny i z města Olomouce, Brna či Ostravy a dalších měst. Případem se později začala zajímat jak média, tak policie. Ve většině případů ale věc byla odložena s odůvodněním, že fotografie byly zveřejněny a umístěny na různých internetových stránkách samotnými oznamovatelkami. Samotní pachatelé tak neudělali nic jiného než jen, že fotografie shromáždili na jedno veřejně dostupné místo. (Kožíšek, Písecký 2016)

2.4.2 Jessica Logan

Jessica Logan byla studentka střední školy, která žila se svou rodinou v americkém Ohiu. Osudným se ji stal den, kdy se rozešla se svým přítelem. Ten neváhal a rozeslal její nahou fotku, kterou mu Jessica v minulosti poslala, všem lidem na její škole. Lidé se ji vysmívali a nadávali jí. Jessica ze strachu začala zanedbávat školu. Po pár měsících promluvila i do televize, kde řekla svůj příběh a sdělila, že doufá, že se nikomu podobné věci nebudou opakovat. Po pár měsících od rozhovoru v televizi, konkrétněji v červenci roku 2008, našla Jessičina matka svou dceru oběšenou ve skříni. (PureSight, c2005-2018)

3 PREVENCE

Jednou z možností, jak se vyhnout problémům, je nesdělovat o sobě příliš mnoho osobních údajů jako je například adresa bydliště, telefonní číslo, adresa školy nebo třeba rodné číslo. Jsou to informace, na jejichž základě můžete být identifikováni. (Eckertová, Dočekal 2013) Další z možnosti, jak si zajistit bezpečný účet na sociální síti je vytvořit si silné heslo. V dnešní době máme bohužel tolik elektronických služeb, že potřebujeme více přístupových hesel. A to je problém. Čím více věcí si musí lidé pamatovat, tím mají větší pokušení si je zjednodušovat. Další z nejčastějších chyb, kterých je dopouštěno je ukládání hesla. Nikdy by se hesla neměla ukládat do cizích počítačů, nebo do nezašifrovaného souboru. Další chybou je používání stejných hesel pro všechny účely. Stačí, když hacker přijde na jedno heslo a má přístup na všechny vaše účty. I to nejbezpečnější heslo se dá prolomit. Pro bezpečné heslo je třeba zvolit vhodnou kombinaci. V ideálním případě by heslo dohromady nemělo dávat vůbec žádný smysl. Mělo by být složeno z velkých a malých písmen, mezi nimi by měla být umístěna čísla a mohou být využity i speciální znaky. (Petrowski, 2014)

3.1 Projektové aktivity

V dnešní době máme několik možností, jak můžeme dětem „zpestřit“ nudnou teorii o tom, jak se mají chovat na internetu bezpečně. Jednou z nich jsou projekty, které dětem i rodičům pomohou uvědomit si, jak je důležité vnímat jeden druhého. Cílem těchto projektů je předejít případným internetovým kriminalitám a působit tak pro uživatele preventivně a zároveň zábavnou formou.

3.1.1 NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost je ústřední správní orgán, který vznikl 1. srpna 2017. Jeho účelem je zajistit kybernetickou bezpečnost včetně ochrany utajovaných informací a kryptografické ochrany. (NÚKIB, b. r.) Úřad se snaží vzdělávat a šířit problematiku využívání digitálních technologií na různé cílové skupiny. Zaměřují se především na úředníky a zaměstnance veřejné správy. Dále je pro ně ale velice důležitá skupina žáků mateřských, základních a středních škol. Spolupracují ale i s univerzitami a ostatními vysokými školami. Také pomáhají seniorům a veřejnosti se začleňováním do digitálního světa a orientováním se na internetu. Všem těmto skupinám se snaží pomáhat vzdělávacími aktivitami ať už formou konferencí, přednášek a seminářů nebo na svých webových

stránkách nabízejí elektronickou brožurku, která vysvětluje danou problematiku a je doprovázena video návody. (NÚKIB, b. r.)

3.1.2 E-bezpečí

Projekt zaměřený na prevenci, výzkum, vzdělávání a intervenci je také úzce spojený s rizikovým chováním na internetu. Je realizován zejména díky pedagogické fakultě univerzity Palackého, centrem prevence rizikové virtuální komunikace. Zaměřují se na nejrůznější cílové skupiny, s pozitivním dopadem zejména na žáky základních a středních škol, učitelé, preventisty, policisty a také na rodiče. Problematiku jako jsou například kyberšikana, kyberstalking, hoax, spam a podobná rizika představují v podobě modelových situací a skutečných kauz. Pořádají například besedy pro školy, které jsou doprovázené prezentacemi a videoukázkami. Kromě vzdělávacích akcí se projekt zaměřuje na pravidelná celorepubliková šetření. (E-bezpečí, c2008-2020)

3.1.3 Internetem bezpečně

Tento projekt vznikl za účelem zvýšit povědomí uživatelů sociálních sítí a internetu o jejich rizicích. Ke své tvorbě využívají nové a interaktivní metody. Pořádají různé vzdělávací akce po republice. Nejpopulárnější jsou ale jejich krátká videa, kde ukazují reálné a nebezpečné hrozby na internetu, kterým se někteří lidé sami vystavují, zejména kvůli neopatrnosti nebo neznalosti. (Internetem bezpečně, c2018)

3.1.4 Say No!

Kampaň Evropského policejního úřadu (zk. EUROPOL) vznikla za účelem chránit děti proti online sexuálnímu vydírání. Vyzívá děti, které mají podobnou zkušenost, ať se svěří blízké osobě a nahlásí to na policii. Kampaň ve svém videu promítá reálné situace, které se v dnešním světě dějí. Pachatel, který svou oběť vydírá a chce po ní buď další intimní fotografie, nebo peníze, páchá trestný čin a je zapotřebí, aby byl za tento čin potrestán. Mnoho dětí však tuto situaci vůbec nikomu neoznámí, neboť vůbec netuší, že se stali oběti trestného činu a jsou v rozpacích z materiálu, který pachateli poslali. Dále také na webu varují, jak být v bezpečí, pokud vás někdo pozve na schůzku, jak mít své osobní věci v soukromí a podobné užitečné rady. Se souvisejícími problémy připravila kampaň pro pět cenných rad.

Řekni NE!

1. Pokud vás někdo požádal, abyste mu řekl nebo ukázal věci, které pro vás nejsou příjemné.
2. Pokud vám někdo vyhrožuje sdílením vašich fotek nebo videí, když nepošlete další.
3. Pokud vás někdo požádá, abyste svůj chat udrželi v tajnosti.
4. Pokud někdo reaguje vulgárně, když neděláte to, co on chce.
5. Pokud vás někdo požádá o připojení k vašim soukromým sítím. (Europol, c2020)

3.2 Antivirové ochrany

Jednou z nejvyhledávanějších kontrol, kterou má dnes většina lidí nainstalovanou ve svém počítači je antivirová ochrana. Jejím účelem je sledovat všechny nejdůležitější vstupní i výstupní místa, kterými by mohly viry do počítače proniknout. (Mamchur, 2011)

- **Kaspersky**

Společnost byla založena v roce 1997 v Moskvě. Je v popředí žebříčku s antiviry a dominuje trhu. Výhodou je celkem nízká pořizovací cena a jednoduché ovládání a instalace. Dále dokáže velmi dobře chránit internetové bankovnictví. (Zich, c2020)

- **Avast**

Česká společnost, která byla založena roku 1988. Antiviry této společnosti jsou určeny především pro domácí užití a pro malé a střední podniky. Dostupný je ve více než 40 jazycích včetně češtiny, což je velká výhoda a díky tomu vyrovnává trochu vyšší pořizovací cenu. (Zich, c2020)

II. PRAKTICKÁ ČÁST

4 VÝZKUMNÁ ČÁST

V praktické části jsem se zaměřila na výzkum pomocí dotazníkového šetření, který byl určen jenom dětem. Na začátku výzkumu jsem si stanovila tři cíle. Díky odpovědím v dotazníku jsem mohla navázat na bezpečnostní opatření.

4.1 Dotazníkové šetření

Dotazník byl směřován dětem od 9 let do 18 let. Šetření probíhalo přibližně jeden měsíc, a to takovým způsobem, že 31 respondentů odpovídalo na dotazník v papírově podobě a 85 respondentů bylo osloveno přes internet pomocí webové stránky Survio. Celkem se tedy šetření zúčastnilo 116 dětí.

Dotazník měl celkem 16 otázek. Odpovědi byly uzavřené a polouzavřené. U některých otázek mohlo být i více odpovědí (viz příloha P II).

4.2 Cíle a hypotézy dotazníkového šetření

Cíl č. 1

Prvním cílem bylo zjistit, kolik dětí mladších 13 let má založeno účet na sociální síti.

Cíl č. 2

Zjistit, zda zapojují děti své rodiče do jejich virtuálního světa a pokud ano, kolik dětí by se jim svěřilo, kdyby mělo nějaký problém spojený s vyhrožováním, vydíráním.

Cíl č. 3

Která sociální síť je u dětí nejpopulárnější.

Hypotéza č. 1

Předpokládám, že více jak 90 % tázaných bude mít založený profil na jedné či více sociálních sítích.

Hypotéza č. 2

Domnívám se, že více než 30 % dětí nemluví s rodiči o tom, co dělají na internetu a sociálních sítích.

Hypotéza č. 3

Myslím, že pokud by dítě mělo problém ať už s vydíráním, obtěžováním či vyhrožováním svěřila by se někomu pouze 1/3 dotazovaných dětí.

4.3 Vyhodnocení dotazníkového šetření

1. **Jaké jsi pohlaví?**
2. **Kolik ti je let?**

V prvních dvou otázkách jsem si respondenty rozdělila podle pohlaví a podle věku. Jelikož dotazník byl směřován dětem od 9 do 18 let, rozdělila jsem tázající do dvou věkových skupin.

Tab. 1 Pohlaví respondentů

Odpověď	*Počet*	*Počet v procentech*
Dívky	61	52,6 %
Chlapci	55	47,4 %

Zdroj: [vlastní]

Tab. 2 Věková kategorie respondentů

Odpověď	*Počet*	*Počet v procentech*
9-12	48	41,4 %
13-18	68	58,6 %

Zdroj: [vlastní]

Ze 116 oslovených se šetření účastnilo více dívek než chlapců a většinou odpovídaly děti ve věku od 13 do 18 let.

3. **Máš založený účet na sociální sítí?**

Rozhodující otázkou, jestli dítě bude ve vyplňování dotazníku pokračovat, byla třetí otázka týkající se sociálních sítí. Zda dítě má založený účet na sociální síti nebo ne. Pokud dítě odpovědělo, že nemá založený účet, dotazník tím pro něj skončil, jelikož se ho další otázky už netýkaly a bylo by těžké na otázky najít odpověď.

Tab. 3 Výskyt sociálních sítí

Odpověď	*Počet*	*Počet v procentech*
Ano, mám	114	98,3 %
Ne, nemám	2	1,7 %

Zdroj: [vlastní]

Po této otázce ve vyplňování dotazníku tedy pokračovalo 114 dětí. Pouze dvě dívky ve věku 9-12 let ze 116 tázaných neměly založený profil na sociální síti. Jelikož 98 % dětí má profil na sociálních sítí má hypotéza se potvrdila.

Tato otázka mi také odpověděla na jeden z mých cílů, které jsem si určila při vytváření tohoto dotazníku. První výzkumná otázka zněla, kolik dětí pod 13 let má založený účet? Znamená to tedy, že 46 dětí má nelegálně založenou sociální síť, jelikož jim není více než 13 let. To znamená, že při zakládání účtu skoro 50 % dotazovaných dětí muselo lhát ohledně svého věku.

Pokud si přečtete smluvní podmínky Facebooku, zjistíte, že ho nesmí používat děti mladších 13 let! (Facebook, 2019) Další služby jako je například Instagram či WhatsApp spadají pod stejnou firmu jako je Facebook, tudíž pro něj platí stejné podmínky, jako pro již zmiňovaný Facebook. (Kluska, 2019) Zakládání účtu není nijak složité a stačí si bohužel jenom změnit datum narození, a hned je člověk „způsobilý“ uživatel dané sociální sítě. A pokud máte Facebook, je jednoduché se přihlásit na další sociální síť. Neboť Facebook je s mnoha sítěmi propojený, a tak stačí použít jeho prvotně uložené údaje.

4. **Pokud máš založený účet, tak na jaké sociální síti?**

V další otázce měly děti označit, jaké sociální sítě mají. Na výběr měly Facebook, Messenger a Instagram. Jako další možnost mohli vypsat, jaké další výše nezmiňované sítě mají.

Tab. 4 Popularita konkrétních sociálních sítí

Odpověď	***Počet***	***Počet v procentech***
Facebook	76	66,6 %
Messenger	106	93,0 %
Instagram	91	79,8 %
Jiné:	29	25,4 %

Zdroj: [vlastní]

Největší popularitu u dětí má messenger, díky kterému si děti můžou zadarmo volat či psát. Mezi další sítě, které děti navštěvují, patří mobilní aplikace TikTok, na které děti mohou vytvářet krátká hudební videa. Další populární aplikace, velice podobná Messengeru, je WhatsApp.

5. Proč jsi účet na sociální síti založil?

V návaznosti na předchozí otázku, děti měly určit důvod, pro který si sociální síť založily. Mohly také označit více odpovědí. Nejčastějším důvodem děti uvedly, že chtějí být v kontaktu se svými přáteli. Také třináct dětí ze všech dotázaných přiznaly, že účet mají založený zejména kvůli kamarádům a kvůli tomu, aby tzv. nekazily partu.

Tab. 5 Důvody k založení

Odpověď	*Počet*	*Počet v procentech*
Chci být v kontaktu s přáteli	100	87,7 %
Chci poznat nové lidi	18	15,8 %
Mají to všichni mí kamarádi, tak nechci kazit partu	13	11,4 %
Cítím se sama/sám	2	1,8 %
Mám problémy s navazováním osobního kontaktu	3	2,6 %
Jiné důvody:	14	12,3 %

Zdroj: [vlastní]

Mezi jiné důvody děti zejména uvedly, že je to proto, aby měly větší přehled o okolí, neboť na sociálních sítích jsou lehko dostupné informace o jejich kamarádech. Dále také děti tvrdily, že účet mají založený zejména kvůli škole. Například mají na sociální síti založenou skupinu, do které si mohou lehce posílat úkoly, a také kvůli zájmovému kroužku, kde děti s vedoucím mohou komunikovat a psát si cenné rady.

6. Víš, od kolika let si můžeš vytvořit profil na této sociální síti?

U otázky č.6 jsem se přesvědčila, že mnoho dětí ví, od kolika let si účet můžou na sociální síti založit. U této otázky měly děti na výběr ze dvou možností. Tou první byla odpověď, že

si profil může založit každý, kdo chce, bez ohledu na věk. Tuto odpověď zvolilo 15 respondentů.

Tab. 6 Věková hranice k založení sociální sítě

Odpověď	***Počet***	***Počet v procentech***
Profil si může založit kdo chce. A je jedno kolik má roků.	15	13,2 %
Profil si můžu založit od …… let	99	86,8 %

Zdroj: [vlastní]

Další možností bylo napsat věk, od kterého může dítě legálně užívat sociální sítě. Více než 50 % tázaných odpovědělo, že nejnižší hranice je 13 let.

7. **Ví tvoji rodiče o tom, že máš vytvořený profil na sociální síti?**

Další otázkou, kterou jsem si v dotazníku nemohla odpustit byla, zda ví rodiče o tom, že jejich dítě má založený profil na sociální síti. 98 % dětí tvrdí, že jsou jejich rodiče o této problematice informovány.

Tab. 7 Povědomí rodičů o užívání sociálních sítí

Odpověď	***Počet***	***Počet v procentech***
Ano	112	98,2 %
Ne	2	1,8 %

Zdroj: [vlastní]

Proto je pro mne nepochopitelné, že tak mnoho rodičů, i přesto nechá dítě volně využívat sociální sítě, které jsou limitovány věkem, na které děti nedosahují.

8. **Mluvíš se svými rodiči o tom, co vůbec děláš na internetu, jaké stránky navštěvuješ, s kým se kamarádíš a s kým si píšeš?**

Navazující otázkou byla tedy informovanost rodičů o aktivitách dítěte na internetu. Jestli s nimi v tomto směru děti komunikují. Zda rodič ví, jaké stránky dítě navštěvuje, s kým se

kamarádí a s jakými lidmi si jeho potomek píše na sociálních sítích? Zda se rodič zajímá o virtuální aktivity svého dítěte, když už ho tyto stránky nechá navštěvovat?

Tab. 8 Informovanost rodičů

Odpověď	***Počet***	***Počet v procentech***
Ano	95	83,3 %
Ne	19	16,6 %

Zdroj: [vlastní]

Děti, které odpověděly, že jejich rodiče tyto informace nemají, musely uvést i důvod, proč jim tyto údaje nesdělují. Nejčastěji tak odpovídaly, že by děti přišly o své soukromí, anebo to rodiče nezajímá. Tyto odpovědi mi vyvrátily moji hypotézu, neboť s rodiči nekomunikuje pouze 16,6 %.

9. <u>Myslíš, že se na tvůj profil nikdo cizí nemůže přihlásit?</u>

Další otázka, na kterou museli respondenti odpovědět, se týkala jejich zabezpečení. Skoro 59 % dětí si myslí, že se na jejich profil může přihlásit i někdo cizí, tudíž je jejich účet napadnutelný.

Tab. 9 Napadnutelnost účtu

Odpověď	***Počet***	***Počet v procentech***
Ano, může	67	58,8 %
Ne, nemůže	47	41,2 %

Zdroj: [vlastní]

Myslím, že to muže být hlavně tím, že spousta dětí neví, jak si vytvořit dostatečně silné heslo a co by správné heslo mělo všechno obsahovat.

10. **Máš vytvořené silné heslo, které jen tak někdo nezjistí? To znamená, že v něm používáš háčky, čárky, číslice a další speciální znaky (-,*^%) ?**

Předchozí názor mi ale vyvrátila otázka číslo 10, ve které 68 % dětí tvrdí, že má vytvořené nezjistitelné heslo, ve kterém používají diakritiku, číslice i speciální znaky.

Tab. 10 Dostatečně silné heslo

Odpověď	*Počet*	*Počet v procentech*
Ano	78	68,4 %
Ne	36	31,6 %

Zdroj: [vlastní]

V této otázce si podle mého názoru děti nechtěly připustit pravdu. Spousta lidí, nejen dětí, si hesla opravdu ulehčují a velice často používají jedno stejné heslo pro všechny účty či aplikace.

11. **Přidáváš na svůj profil fotky, a různé aktuálnosti (např.: že jsi na dovolené, že máš nové telefonní číslo, že ses přestěhoval)?**

Otázka č.11 zasahovala do soukromí dětí. Některé děti totiž přidávají příspěvky, fotografie či informace, které obsahují různé detaily, a na první pohled tak nemusí přijít dítěti tyto informace ohrožující. Na otázku, zda takové informace skutečně na internet přidávají, odpověděly následovně.

Tab. 11 Sdílení soukromí

Odpověď	*Počet*	*Počet v procentech*
Ano, přidávám	36	31,6 %
Ne, nepřidávám	78	68,4 %

Zdroj: [vlastní]

Výsledky odpovědí na tuto otázku mě docela zarazily. Na jednu stranu je to dobře, že děti takové informace nesdělují. Z mé vlastní zkušenosti ale vím, že mnoho rodičů sdílí informace za své děti. Tím, že vyfotí děti v plavkách u moře, o sobě prozrazují ne jednu

velice intimní informaci. V prvním případě se tím dává najevo, že se právě nenachází doma a v druhém případě fotografie vašeho dítěte může zneužit například pedofil.

12. Už jsi přes sociální síť poznal nového kamaráda, kterého si ve skutečnosti ještě nikdy neviděl ale jen si s ním píšeš?

V dnešním světě si spousta dětí neuvědomuje, kdo za člověka skutečně sedí na druhé straně počítače. Proto bychom měli být velice opatrní, komu opravdu potvrzujeme přátelství. 36 % dětí se na sociálních sítích seznámily s osobou, kterou ve skutečnosti ještě vůbec neviděly.

Tab. 12 Seznámení přes sociální sítě

Odpověď	*Počet*	*Počet v procentech*
Ano, poznal	41	36,0 %
Ne, nepoznal	73	64,0 %

Zdroj: [vlastní]

Tento druh seznamování mi přijde velice nebezpečný. Nikdy nevíte kdo sedí na druhé straně počítače a co má ve skutečnosti v úmyslu.

13. Potvrdíš přátelství někomu, koho ve skutečnosti vůbec neznáš?

Další otázka byla velice podobná té předchozí, a ptala se v dotazníku na to, zda děti potvrdí přátelství někomu, koho ve skutečnosti vůbec neznají.

Tab. 13 Potvrzení přátelství

Odpověď	*Počet*	*Počet v procentech*
Ano, potvrdím	30	26,3 %
Ne, nepotvrdím	84	73,7 %

Zdroj: [vlastní]

Když porovnám tyto dvě otázky, je jasné, že některé děti v dotazníku bohužel neodpovídaly úplně pravdivě. Pokud se totiž s někým seznámily, znamená to, že ho na počátku tohoto virtuálního kamarádství vůbec neznaly. Tudíž je velice pravděpodobné, že přátelství neznámým lidem potvrdí, jen si to třeba nechtějí připustit.

14. Vyhrožoval ti přes sociální sítě někdo, lákal tě na schůzku, chtěl po tobě někdo tvé intimní fotografie?

Podle odpovědí dětí na tuto otázku se zdá, že většina z nich zatím naštěstí nenarazily na nikoho, kdo by je prostřednictvím sociálních sítí nějakým způsobem obtěžoval.

Tab. 14 Obtěžování na sociálních sítích

Odpověď	*Počet*	*Počet v procentech*
Ano	12	10,5 %
Ne	102	89,5 %

Zdroj: [vlastní]

Pokud děti nelhaly, protože se například některé bály přiznat, je 102 neoslovených děti velice pozitivní odpověď. Může to být tím, že se děti snaží na sebe na sociálních sítí moc neupozorňovat a nesdílí nebo nepřidávají svoje fotografie.

15. Pokud by si měl v budoucnu nějaký výše zmíněný problém, komu by ses svěřil?

Odpověď na otázku, zda by se děti někomu svěřily, kdyby měly problém ať už s šikanou, vydíráním, nebo jakýmkoliv obtěžováním, odpověděly nad moje očekávání. Pouze 8 dětí ze 114 respondentů odpovědělo, že by se nikomu nesvěřilo, což opět vyvrátilo moji hypotézu.

Tab. 15 Svěřování se s problémy

Odpověď	*Počet*	*Počet v procentech*
Nikomu bych se nesvěřila	8	7,0 %
Někomu z rodiny	74	64,9 %
Kamarádovi, kamarádce	54	47,4 %
Někomu jinému:	7	6,1 %

Zdroj: [vlastní]

Nejčastěji by se děti svěřily samozřejmě svým rodičům nebo svým blízkým. Mezi jiné odpovědi patřili zejména učitelé.

16. Cítíš se díky těmto sociálním sítím šťastnější?

Poslední otázkou, kterou jsem dětem položila, jsem se snažila zjistit, zda dětem sociální sítě pomáhají a zda díky nim žijí lepší život. 62 % dětí odpovědělo, že se díky nim cítí šťastnější.

Tab. 16 Závěrečné pocity

Odpověď	*Počet*	*Počet v procentech*
Ano, cítím se šťastnější	71	62,3 %
Ne, necítím	43	37,7 %

Zdroj: [vlastní]

V dnešní době se dá pochopit, že sociální sítě dělají děti šťastnými. Tráví na nich spoustu volného času, hrají online hry, komunikují se svými kamarády a mají na nich spousta soukromých věcí. Proto je ale důležité stále udržovat i osobní kontakt a nevyhýbat se společnosti. Online svět a skutečný svět jsou stále dvě rozdílné věci.

4.4 Důležité závěry dotazníkového šetření

Výsledky dotazníku hodnotím kladně, některé odpovědi jako například fakt, že více než 30% dětí informuje své rodiče o jejich aktivitách na sociálních sítích, mě velice mile překvapily. Naopak to, že 71 dětí ze 114 žije díky sociálním sítím šťastnější život mě docela šokovalo, neboť 62 % je docela vysoké číslo. Myslím, že radost dětem by měly přinášet jiné věci a to například, že jsou zdravé, mohou chodit do školy, a jiné hodnoty, které si děti zatím ještě neuvědomují. Takové věci ale nemůžeme dětem vůbec vyčítat. Může za to dnešní doba a rodiče. Kdyby rodiče místo investice do drahých telefonů věnovali více času dětem a tyto peníze do společných zážitků, všem by to maximálně prospělo. Rodiče by tak zjistili, s jakými problémy bojuje jejich dítě, a tak by předešli tomu, že by se jejich dítě muselo svěřovat někomu online. Bohužel, v dnešní době se veškeré problémy, hádky, rozchody řeší přes internet a málo kdo to umí říct do očí. Kdyby rodiče omezili dětem čas strávený na internetu, dítě by se tak dokázalo naučit si hrát a zabavit se i jinak.

5 SOFTWAROVÁ ZABEZPEČENÍ

V práci jsem se rozhodla otestovat dva různé softwary, které mají ale stejný cíl. A to zajistit bezpečnější internetový a online svět pro děti. V prvním případě jsem otestovala mobilní aplikaci Family Link, která je dostupná jak pro zařízení s Androidem, tak pro iPhony s operačním systémem iOS. Aplikaci jsem otestovala na jedenáctiletém chlapci. Po dobu přibližně čtrnácti dnů jsem mohla mít kontrolu nad jeho aktivitou na mobilním telefonu. V druhém případě jsem prozkoumala počítačový software od společnosti Microsoft.

5.1 Mobilní aplikace FAMILY LINK

Tato mobilní aplikace je volně dostupná ke stáhnutí na Google Play nebo na App Store. Díky aplikaci mohou být nastaveny základní pravidla pro pohyb na internetu jak pro děti, tak pro dospívající. Dalšími výhodami mohou být považovány nastavitelné limity času stráveného na zařízení ve dne i v noci, rodiče mohou povolovat a blokovat libovolné aplikace, a také je díky GPS snadno zjistitelná poloha zařízení dítěte. Za velkou výhodu můžeme považovat i to, že je zcela zdarma i přes to kolik funkcí nabízí. Proto jsem se rozhodla tuto aplikaci nainstalovat mému jedenáctiletému bratranci, kterému jsem po dobu přibližně čtrnácti dnů mohla spravovat a nastavovat aplikace v jeho telefonu.

5.1.1 Instalace aplikace do telefonu rodiče

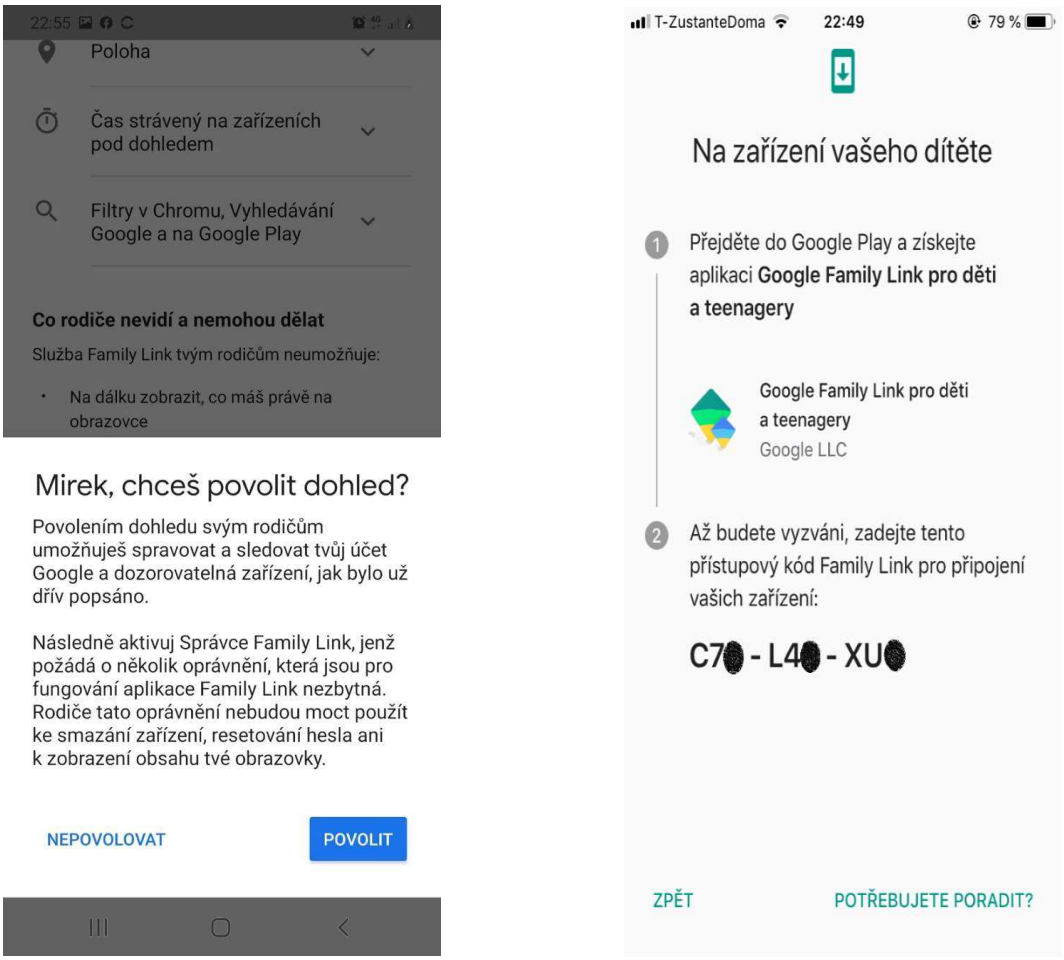
Jako první krok považujeme stáhnutí aplikace do mobilu rodiče. Dále se vás aplikace v úvodních snímcích zeptá na pár otázek týkajících se instalace aplikace do telefonu. Otázky, zda rodič má kompatibilní zařízení Android pro své dítě, jestli jsou rodiče připraveni vytvořit Google účet pro své dítě apod. Pokud všechny tyto kroky rodič potvrdí, může se přejít s instalací aplikace do telefonu dítěte.

5.1.2 Instalace aplikace do telefonu dítěte

Dítěti se musí nejprve nainstalovat aplikace Family Link pro děti a teenagery. Je zapotřebí stáhnout opravdu verzi pro děti a teenagery, aby aplikace fungovala. Testovaný chlapec měl založený účet na Googlu, tudíž instalace byla snadnější. Na můj telefon mi přišel devítimístný přístupový kód, který jsem zadala do telefonu dítěte. Díky tomu se naše zařízení

propojily. Od té doby jsem měla možnost ovládat jeho telefon. Celková instalace trvala přibližně deset minut.

Průběh instalace



Obr. 2 Instalace do telefonu dítěte. Zdroj: [vlastní]

5.1.3 Funkce aplikace

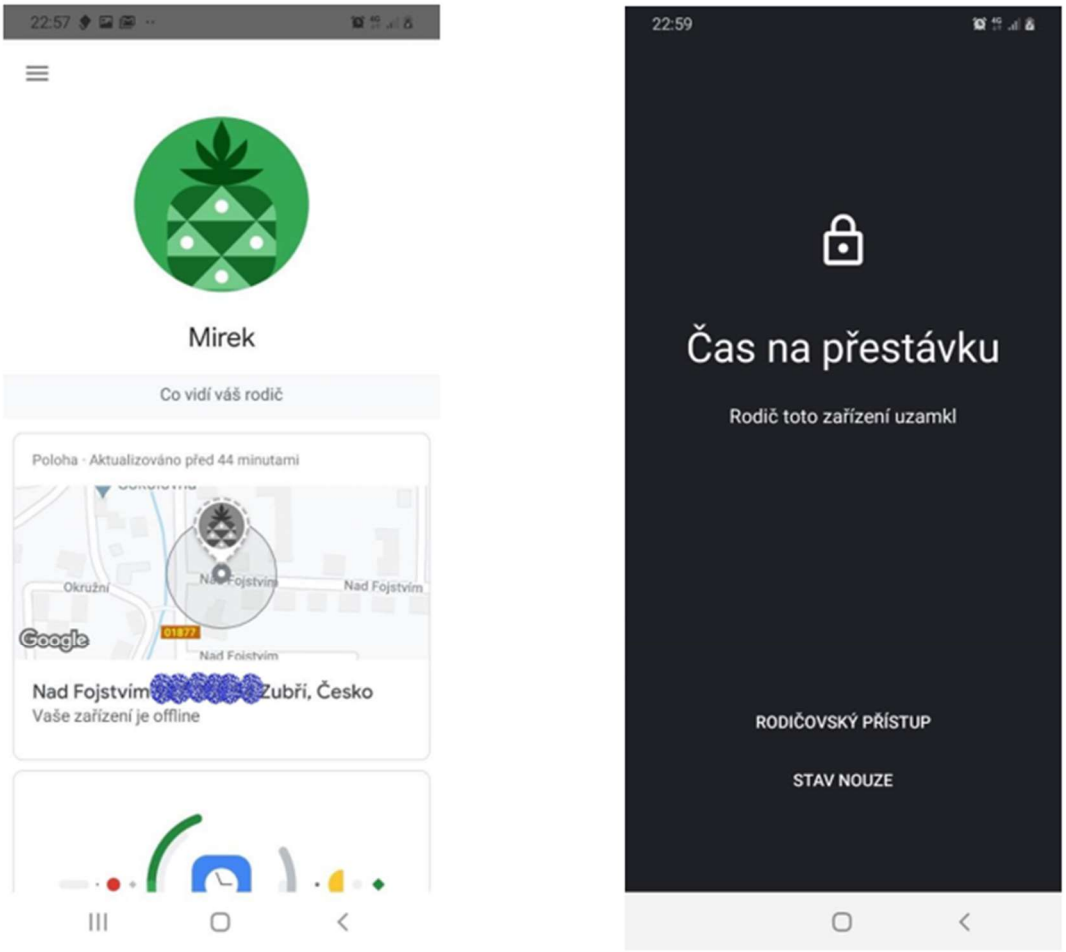
- Sledování aktuální polohy – kdykoliv když rodič bude potřebovat, aktualizuje tuto funkci a ihned se mu ukáže přesná adresa místa, kde se dítě nachází (viz Obr. 3).
- Ovládání času stráveného na zařízení – na každý den jsem mohla nastavit počet hodin, které dítě může strávit na telefonu. Já jsem nastavila pouze tři hodiny denně. Jakmile určený čas vypršel, přišlo dítěti oznámení a dozorované zařízení se uzamklo. Dítě mohlo pouze zvedat telefonické hovory a dovolalo by se například na tísňovou linku, ostatní aplikace nebyly dovoleny. Pro odemknutí telefonu by dítě potřebovalo vědět rodičovský přístupový kod, který jsem si určila při instalování této aplikace.

- Sledování času stráveném na zařízení – zároveň jsem jako rodič mohla z mého telefonu sledovat, kolik času už dítě na telefonu strávilo. Podrobnější přehled navštívených aplikací s rozborem stráveného času u každé aplikace zvlášť tato aplikace také nabízí.
- Večerka – ta byla naplánovaná na každý den stejně a to od 21:00-7:00 hodin. Po uplynutí 21:00 hodiny se zařízení uzamklo a mělo stejnou funkci, jako když byl překročen denní limit. Znova do běžného provozu se zařízení dostalo v 7:00 hodin ráno, kdy zároveň začala běžet nová denní tříhodinová lhůta.
- Uzamčení telefonu na dálku – dále jsem bez jakéhokoliv důvodu mohla uzamknout zařízení na dálku a dítě ho mohlo odemknout, jen pokud znalo rodičovský přístupový kód (viz Obr. 3).
- Blokování a zákaz aplikací – mohla jsem zablokovat nevhodné aplikace nebo nastavit různé limity těmto aplikacím. Například když jsem chlapci zablokovala Facebook, aplikace mu zcela zmizela z telefonu. Nebo jsem mohla omezit pouze některé funkce této aplikace, a to třeba zakázat například přístup fotoaparátu k Facebooku a podobně.

Pokud by dítě chtělo aplikaci ze svého telefonu odinstalovat potřebovalo by souhlas svého rodiče. Ukončení dohledu je velice jednoduché a stačí k tomu pouze jeden krok. Po rozkliknutí nabídky „dohled nad účtem“ rodič potvrdí, že rozumí tomu, že po potvrzení nebude smět spravovat účet Google ani zařízení dítěte.

Co jsem jako rodič ale dělat nemohla, bylo to, že mi aplikace nedokázala ukázat co má dítě právě na obrazovce, zobrazit minulé vyhledávání a s tím spojenou historii procházení v Google. Zobrazit veškerá hesla k jejich účtům. Nemohla jsem také číst e-maily nebo textové zprávy a odposlouchávat hovory, což je logické, jelikož by to zasahovalo do zásad ochrany soukromí. Mazat jeho data v zařízení bylo také zcela nepřípustné.

Funkce aplikace



Obr. 3 Funkce aplikace. Zdroj: [vlastní]

5.1.4 Hodnocení aplikace

Aplikace Family Link může být pro rodiče velice přínosná, a to zejména bohatými funkcemi, které nabízí. Zároveň aplikace působí preventivně a můžete korigovat čas dětí strávený na mobilním telefonu. Výhodou aplikace je, že je vysoce mobilní, snadno přístupná s okamžitou možností kontroly.

5.2 Windows rodičovská kontrola

Je počítačový software, který se poprvé objevil ve Windows 7. Nyní jsou už všechny počítače systému Microsoft vybaveny touto funkcí. Tudíž není zapotřebí tento software

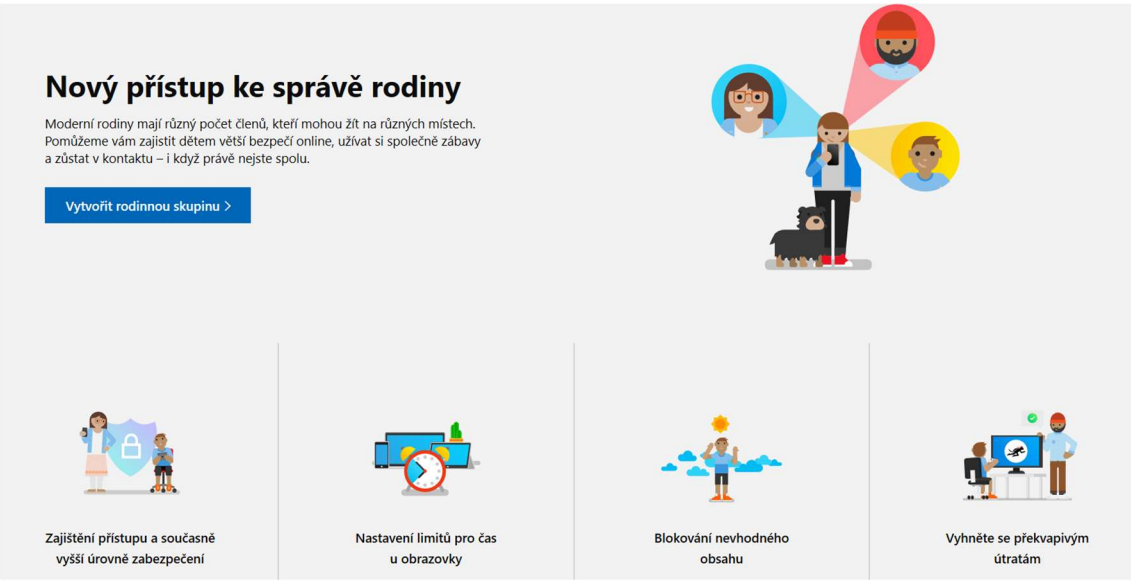
složitě stahovat. (Dvořák, 2019) Tato služba uživatelům nabízí například blokování zakázaných webových stránek k prohlížení a také může omezit dobu strávenou u počítače.

5.2.1 Instalace softwaru

Nejprve je zapotřebí aby se vytvořila rodinná skupina, do které se pozvou členové skupiny, těmi jsou nejčastěji děti a organizátoři skupiny, za které můžeme považovat rodiče a kteří mají následující pravomoce.

- Mohou dávat peníze členům skupiny na nákupy v Microsoft Store, kde mohou členové nakupovat různé aplikace či hry.
- Prohlížet si aktivity a aplikace, které členové skupiny navštěvují. Mohou tak kontrolovat své děti, jaké stránky navštěvují.
- Mohou také u vybraných aplikací a her nastavit věkový limit, díky kterému omezí přístup členů na tuto stránku.
- Nastavit časový limit pro používání zařízení (viz Obr. 6).
- Zobrazit polohu členů rodiny. Podmínkou je instalovaný systém Android s nainstalovanou aplikací Microsoft Launcher u člena skupiny v telefonu.

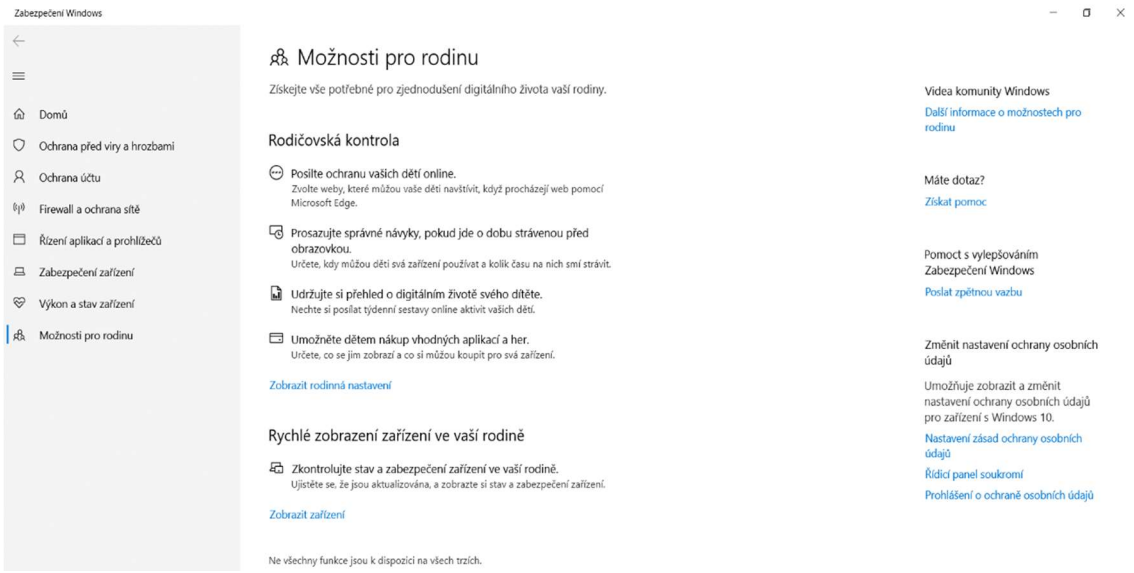
Organizátor pošle pozvání do skupiny členům. Stačí pouze zadat e-mail. Členové pak pouze na svém zařízení přijmou pozvání.



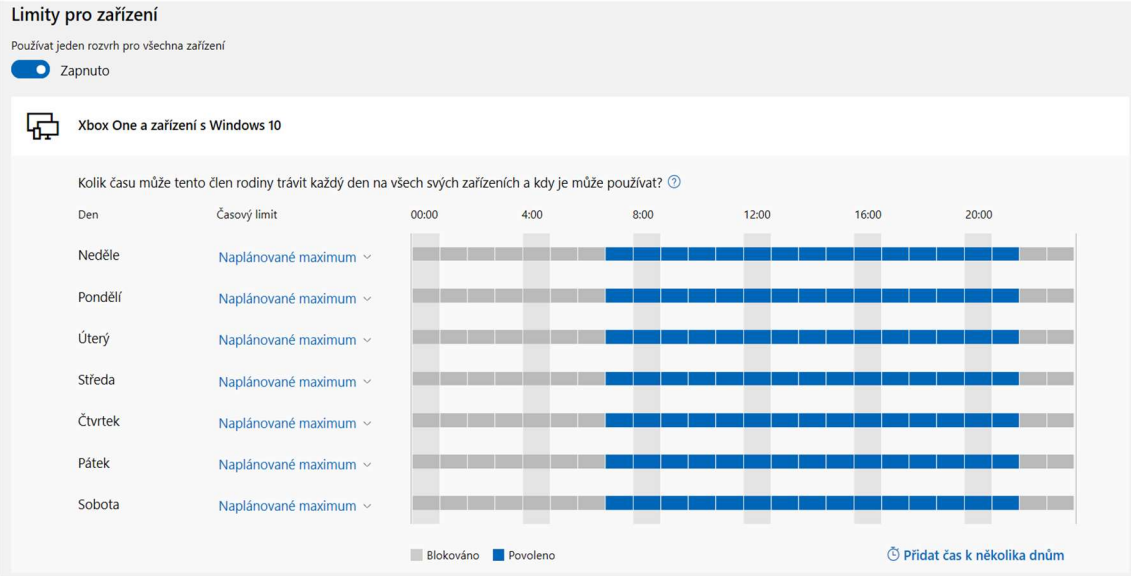
Obr. 4 Vzhled úvodní stránky. Zdroj: [vlastní]

5.2.2 Funkce softwaru

- Limitování času u jednotlivých aplikací – jednou z funkcí, kterou software nabízí je plánované nastavení limitů u aplikací na zařízení vašich dětí. Podmínkou je mít nainstalovaný buďto Windows 10, vlastnit Xbox One nebo na androidových zařízení, kde musíte mít zvlášť nainstalovanou aplikaci Microsoft Laucher. Je velmi praktické, pokud vlastníte všechny tyto typy zařízení, že při přihlášení dítěte se čas sčítá na všech zařízeních. Například pokud dítěti nastavíte dvouhodinový limit na Facebooku, může strávit pouze dvě hodiny celkově, nikoliv na každém zařízení zvlášť. Taková možnost časového omezení jednotlivých aplikací, jakou nabízí tento software, aplikace Family Link nenabízela.
- Filtrování obsahu – pomoci filtru můžeme určit, na jaké webové stránky dítě bude mít přístup, jaké může hrát hry, nebo jaké aplikace v Microsoft Store může nakupovat. Pokud určité stránky zablokujete, dítě vám může poslat žádost. Je jen na vás, jaká pravidla si nastavíte.
- Žádost o povolení nakupování – aby dítě mohlo nakupovat v aplikaci Microsoft Store, bude mu rodič muset k tomu dát povolení. Bez jeho souhlasu si dítě nebude smět nic koupit. Ta stejná funkce může být nastavena i pro herní konzoli Xbox One.



Obr. 5 Hlavní nastavení. Zdroj: [vlastní]



Obr. 6 Funkce limitů. Zdroj: [vlastní]

5.2.3 Hodnocení softwaru

Výhodou softwaru je, že je zdarma a v počítači který má novější Windows je už nainstalován, tudíž nemusíme nikde komplikovaně nic stahovat. Poměrně jednoduché je i samotné ovládání. Přínosy softwaru jsou velice podobné jako tomu bylo u mobilní aplikace. Je jen otázkou, zda děti tráví víc času u počítače nebo mobilu a na základě toho zvážit, který z těchto otestovaných softwarů je pohodlnější.

6 NAVRHOVANÁ OPATŘENÍ

Cílem mé práce bylo navrhnout určitá bezpečnostní opatření. Jelikož je mezi dětmi a dospělými velký rozdíl, rozhodla jsem se tyto vývojové skupiny rozdělit.

6.1 Navrhované opatření na základě výstupů dotazníku

Na základě výsledků otázky číslo 9 jsem se rozhodla dětem pomoct a vysvětlit, jak si vytvořit dostatečně silné heslo, díky kterému by v budoucnu mohli předejít napadení účtu.

Silné heslo

Heslo se může považovat za prvotní a základní ochrannou hradbu proti případným útočníkům. Problém dnešní doby je povinnost uživatele vytvořit si ke každé webové službě heslo. Není však možné pamatovat si všechny hesla, neboť odborníci doporučují si ke každé službě zvolit jiné. V praxi se potom stává, že uživatel zvolí jedno stejné heslo na všechny účty. Tento případ je jeden z největších chyb, kterých se uživatel dopouští. Pachatel si zjistí heslo u méně zabezpečených služeb, jimiž jsou například diskuzní fóra, a tohle heslo potom použije u těch více zabezpečených účtů jako je například Facebook. Za snadno uhodnutelná hesla se považují běžná samostatná slova, jména blízkých osob, datum narození, jména domácích mazlíčků a posloupnost čísel a písmen. Silné heslo můžeme například vymyslet podle následujícího způsobu. (Kohout, c2018)

Jak ho správně vytvořit?

Místo slova si vymyslíme lehce zapamatovatelnou větu.

Například ***„Dne devátého dubna má moje sestra Mája narozeniny.“***

Z každého slova použijeme začáteční písmeno a číslovku změníme na číslo.

To znamená: ***d9dmmsmn***

Některá písmena můžeme změnit na velká.

Heslo bude vypadat: ***d9dMmSmN***

Své heslo je zapotřebí dále ochraňovat, a to zejména tím, že se nikomu nebude sdělovat, že si ho nebudeme psát na papír, nebo do poznámek v telefonu. Dále bychom měli vědět, že je velmi nebezpečné se přihlašovat například v nákupním centru nebo internetových

kavárnách, kde je přístup veřejného připojení k internetu a prostory tak můžou být vybaveny monitorovacím programem. (Kohout, c2018)

6.2 Navrhovaná opatření pro děti

V rámci praktické části mé bakalářské práce jsem si pro děti připravila tzv. kartu opatření, neboli jak se cítit bezpečně v online světě (viz. příloha P I). Dětem jsem se pomocí obrázků snažila napodobit bezpečné chování tak, aby předcházely rizikům a zbytečným problémům. Některá preventivní opatření už sice zazněla, tudíž nejsou žádnou novinkou. Dočtete se o nich v časopisech, mediích nebo na internetu. Obrázky k nim jsou už ale vlastní tvorbou. Karta by tak měla na děti působit preventivně. Obsahuje 5 následujících bodů:

- Nezveřejňuj na sociálních sítích nikdy aktuální informace, jako jsou například fotky z dovolených. Můžeš tak ohrozit majetek své rodiny. Tyto informace mohou nalákat třeba pachatele majetkových trestných činů.
- Nikdy na sociální sítě neumísťujte vyzývavé fotografie. Každý, kdo je alespoň průměrně znalý internetu, tyto fotky může v programu na úpravu fotek upravit a následně je zneužít proti vám.
- Nikdy si nedomlouvejte schůzku s nikým cizím. Nemůžete vědět, kdo se opravdu na druhé straně počítače skrývá. Může to být budoucí velmi dobrý přítel, anebo také starší osoba, která nemá v úmyslu se s vámi kamarádit. Pokud ale schůzku i přesto budete chtít uskutečnit, informujte o tom vaše rodiče. Je důležité jim říct čas a místo setkání a také popsat osobu, se kterou se máte setkat.
- Nezapomeň, že na sociálních sítích komunikuješ stejným způsobem, jakým bys komunikoval ve skutečnosti. Proto se nikomu neposmívej, nedělej si legraci z jeho fotek a podobné věci. I tímto se můžeš zároveň cítit na sociálních sítích v bezpečí a dá se to považovat za určitý druh opatření. Můžeš si tak být trochu jistější, že ti nikdo nebude mít v plánu podobné věci oplácet.
- Nikomu neříkej své heslo od svého účtu. Mohlo by se stát, že by se ti do něj někdo přihlásil. Nemusí to dělat se zlým účelem. Bude se chtít například trochu pobavit a napíše tvému idolovi nebo zesměšňující příspěvek, vydávající se tvým jménem. I taková legrace ale může někdy mrzet. To samé platí i v případě odhlašování z cizího zařízení! Vždy se nezapomeň odhlásit.

6.3 Navrhovaná opatření pro dospělé a zejména rodiče

Opatření pro dospělé a rodiče mohou být velice podobné jako ty pro děti. To, že by nikde a nikomu neměli říkat svá hesla a podobné věci, dospělí ví. Za jedno z bezpečnostních opatření lze považovat například to, že jako rodič půjdete příkladem svým dětem a nebudete na sociální sítě vkládat a umisťovat různé soukromé fotky, kde jsou i vaše děti. Takový nešvar se v posledních letech stal velice populárním a dá se říct, že zejména matky vkládají na svůj profil úplně všechno. Narušují tím soukromí nejen svoje, ale i svých dětí. V tomhle směru by měli být rodiče opravdu obezřetnější.

Na některých sociálních sítích je možnost dvoufázového ověření. To například na Facebooku nastavíte v sekci „Nastavení“ kde potvrdíte, že chcete použít dvoufázové ověření. To slouží zejména k tomu, že pokud Facebook zaregistruje přihlášení z jiného nebo podezřelého zařízení, požádá vás o zadání vašeho hesla nebo ověřovacího kódu, který vám Facebook pošle na váš mobilní telefon.

I přesto, že jste dospělí vám důrazně doporučuji, nepřidávat si cizí lidi do přátel. A to zejména ze dvou důvodů. Tím prvním z nich je to, že pokud si nastavíte kontrolu soukromí například na Facebooku, vámi vložené příspěvky se budou zobrazovat pouze vašim přátelům. Pokud si ale budete přidávat kohokoliv, je takové bezpečnostní opatření nabízené danou sociální sítí zcela zbytečné. Slouží to zejména k tomu, aby nikdo cizí neviděl vaše příspěvky, neprohlížel si fotografie a nějak nesledoval vaši aktivitu. Druhým důvodem jsou podvodníci, kteří se na sociálních sítích často vyskytují. Zejména staré dámy, kterou jsou většinou ovdovělé či v penzi naletí podvodníkům, kteří se vydávají za vojáky a žádají o peníze. Mnoho žen takovým podvodům naletí a peníze, které se dají počítat ve stovkách tisíců, opravdu pošlou. Proto s nikým takovým nekomunikujte.

ZÁVĚR

Cíle mé bakalářské práce byly naplněny v jednotlivých kapitolách. V teoretické části byly vysvětleny pojmy řešené problematiky. Na základě dotazníkové šetření jsem zjistila nejpopulárnější sociální síť u dětí, kterou je Messenger a také mě překvapil vysoký výsledek odpovědí uživatelů sociálních sítí, které nedosahují věku ani 12 let a mají založený účet na takové síti. Také byla navržena a doporučena bezpečnostní opatření jak pro děti, tak pro dospělé.

Je těžké najít opatření, které dokáží opravdu zaručit bezpečnost na sociálních sítích a internetu. V mnoha případech ale můžeme následná rizika alespoň zmírnit. Záleží, jak k tomu budeme všichni přistupovat. Proto je dobré dbát na doporučení různých odborníků.

Jediné opatření, které mě napadá a zajistilo by stoprocentní zabezpečení je nezakládat si profil či účet na sociální síti. Jedině tak můžete předejít tomu, že vás někdo bude přes sítě vydírat, obtěžovat, nebo nějak napadat. Chápu, v dnešní době to je bohužel téměř nepředstavitelné. Dnešní doba nás nutí k tomu, abychom si kupovali co nejmodernější a nejvýkonnější technologie. Pro následující generaci budou chytré telefony, hodinky, robotické vysavače a podobné vymoženosti už zcela normální věcí. Sociální sítě bude mít kde kdo, naopak kdo účet nebude mít vytvořený, bude vyčnívat ze společnosti.

Mnohým lidem přirostl telefon k rukám a nedokáží si bez něj představit obyčejný den. Proto je velice důležité ten čas na něm strávený alespoň nějakým způsobem omezit. Začít si všímat jeden druhého, komunikovat mezi sebou, místo hraní online her si zahrát obyčejné deskové hry, vyrazit do přírody, kde si můžeme od všech těchto sociálních sítí odpočinout.

SEZNAM POUŽITÉ LITERATURY

- DVOŘÁK, Jakub. Ohlídejte si děti na internetu. Pomůže správný software. *IDNES* [online]. 2019 [cit. 2020-05-25]. Dostupné z: https://www.idnes.cz/technet/software/kontrola-dite-internezt.A190410_083216_software_dvr
- ECKERTOVÁ, Lenka a Daniel DOČEKAL. *Bezpečnost dětí na Internetu: Rádce zodpovědného rodiče*. Brno: Computer Press, 2013. ISBN 978-80-251-3804-5
- HOŠKOVÁ, Petra. Sociální sítě frčí aneb co to je Instagram. *PTL: Specialista na on-line marketing* [online]. 2018 [cit. 2020-05-25]. Dostupné z: https://www.ptl.cz/instagram-a-socialni-site/
- HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: Psychologie internetové oběti, pachatele a kriminality*. Praha: Juhaňák-Triton, 2012. ISBN 978-80-7387-545-9.
- Kazuistiky: Ryan Patrick Halligan. *E-bezpečí* [online]. 2019 [cit. 2020-05-25]. Dostupné z: https://www.e-bezpeci.cz/index.php/72-kazuistiky/1425-ryan-patrick-halligan-usa-2003
- KLUSKA, Vladislav. Facebook přejmenuje Instagram a WhatsApp. Dá více najevo, že patří pod něj. *Živě* [online]. 2019 [cit. 2020-05-25]. Dostupné z: https://www.zive.cz/clanky/facebook-prejmenuje-instagram-a-whatsapp-da-vice-najevo-ze-patri-pod-nej/sc-3-a-199659/default.aspx
- KOHOUT, Roman. Desatero pro rodiče. In: *Internetem bezpečně* [online]. c2018 [cit. 2020-05-25]. Dostupné z: https://www.internetembezpecne.cz/ke-stazeni/
- KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně na internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.
- KULHÁNKOVÁ, Hana a Jakub ČAMEK. *Fenomén facebook*. Kladno: Čamek-BigOak, 2010. ISBN 978-80-904764-0-0.
- MAMCHUR, Viktoriya. *Bezpečnost na sociálních sítích* [online]. Praha, 2011 [cit. 2020-05-25]. Dostupné z: https://is.ambis.cz/th/yzy9n/Bezpecnost_na_socialnich_sitich__BP.pdf. Bakalářská práce. Bankovní institut vysoká škola Praha. Vedoucí práce Ing. Antonín Vogeltanz.

- NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2020-05-25]. Dostupné z: https://www.nukib.cz/cs/o-nukib/
- projektu. *E-bezpečí* [online]. c2008-2020 [cit. 2020-05-25]. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu
- projektu. *Internetem bezpečně* [online]. c2018 [cit. 2020-05-25]. Dostupné z: https://www.internetembezpecne.cz/o-projektu/
- PETROWSKI, Thorsten. *Bezpečí na internetu pro všechny*. Liberec: Dialog, 2014. ISBN 978-80-7424-066-9.
- Real life stories: Jessica Logan. *Pure Sight: Online child safety* [online]. c2005-2018 [cit. 2020-05-25]. Dostupné z: https://www.puresight.com/Real-Life-Stories/jessica-logan-1990-2008.html
- ROGERS, Vanessa. *Kyberšikana*. Praha: Portál, 2011. ISBN 978-80-7367-984-2.
- Smluvní podmínky. *Facebook* [online]. 2019 [cit. 2020-05-25]. Dostupné z: https://www.facebook.com/legal/terms
- Sociální sítě. *Internetem bezpečně* [online]. 2018 [cit. 2020-05-25]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/socialni-media/socialni-site/
- ŠEVČÍKOVÁ A KOLEKTIV, Anna. *Děti a dospívající online: Vybraná rizika používání internetu*. Praha: Grada Publishing, 2014. ISBN 978-80-247-5010-1.
- Vzdělávání. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2020-05-25]. Dostupné z: https://www.nukib.cz/cs/vzdelavani/
- Your life is online. Protect it! *EUROPOL* [online]. c2020 [cit. 2020-05-25]. Dostupné z: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/your-life-online-protect-it
- ZICH, Jakub. Antiviry: Nejlepší antivirové programy 2020. *Váš pomocník* [online]. c2020 [cit. 2020-05-25]. Dostupné z: https://vas-pomocnik.cz/antiviry

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

GPS	Global Positioning Systém, radionavigační systém pro určení polohy.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost.
SMS	Short message service, systém krátkých zpráv.

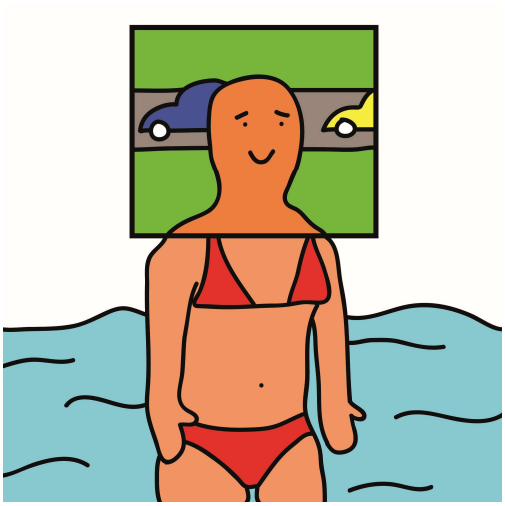
SEZNAM OBRÁZKŮ

SEZNAM TABULEK

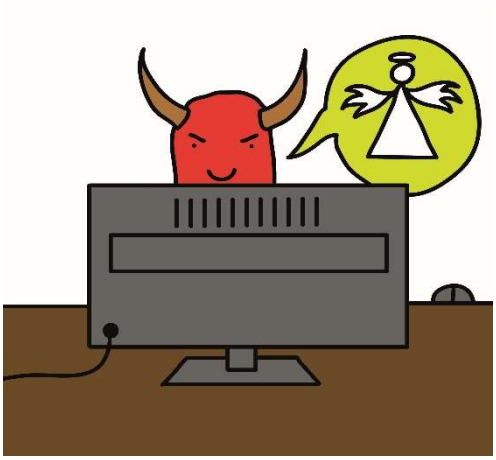
SEZNAM PŘÍLOH

PŘÍLOHA P I: OBRÁZKOVÉ KARTY PRO DĚTI

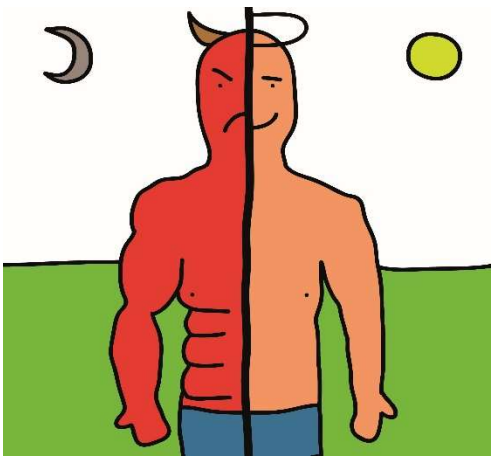
Nezveřejňuj informace, které by mohly ohrozit tebe nebo tvou rodinu.



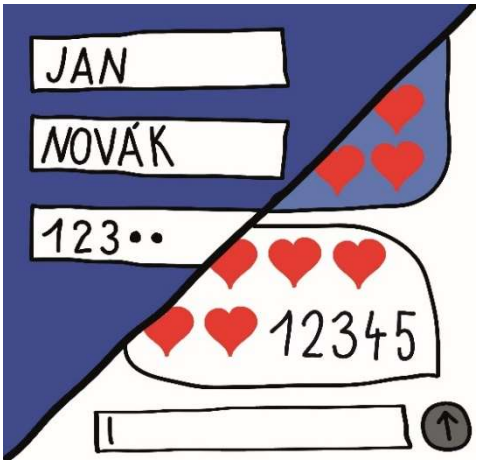
Nezveřejňuj své intimní fotografie na internet.



Nepiš si s cizími lidmi, nevíš, kdo se skrývá za monitorem.



Nechovej se na sociálních sítích jinak než v reálném životě.



Nikomu nedávej své heslo.

PŘÍLOHA P II: DOTAZNÍKOVÉ ŠETŘENÍ

Ahoj,

jsem studentka bakalářského studia na univerzitě Tomáše Bati, oboru Ochrana obyvatelstva. V mé bakalářské práci se zabývám problematikou sociálních síti. Chtěla bych Tě požádat o vyplnění tohoto dotazníku, který mi poslouží k zjištění potřebných informací pro mou bakalářskou práci.

Prosím, označ křížkem „X‘‘ odpověď.

1) Jsi?
   - ☐ Dívka
   - ☐ Chlapec

2) Kolik ti je let?
   - ☐ 9-12
   - ☐ 13-18

3) Máš založený účet na nějaké ze sociálních sítí?
   - ☐ Ano
   - ☐ Ne

4) Pokud ano, tak na jaké?
   - ☐ Facebook
   - ☐ Messenger
   - ☐ Instagram
   - ☐ Jiné (napiš, na které):

     _____

5) Proč sis účet na této sociální síti založil?
   - ☐ Chci být v kontaktu s příteli
   - ☐ Chci poznat nové lidi
   - ☐ Mají to všichni mí kamarádi, tak nechci kazit partu
   - ☐ Cítím se sám/sama
   - ☐ Mám problémy s navazováním osobního kontaktu
   - ☐ Jiná důvod (napiš jaký)?

     _____

6) Víš, od kolika let si můžeš vytvořit profil na této sociální síti?
   - ☐ Profil si může založit každý, kdo chce. A je jedno kolik má roků.
   - ☐ Profil si můžu založit od …….. let

7) Ví tvoji rodiče o tom, že máš založený profil na sociální síti?
   - ☐ Ano
   - ☐ Ne

8) Mluvíš se svými rodiči o tom, co vůbec děláš na internetu, jaké stránky navštěvuješ, s kým se kamarádíš a s kým si píšeš?
   - ☐ Ano
   - ☐ Ne (z jakého důvodu)?

     _____

9) Myslíš, že se na tvůj profil nikdo cizí nemůže přihlásit?
   - ☐ Ano, může
   - ☐ Ne, nemůže

10) Máš vytvořené silné heslo, které jen tak někdo nezjistí? To znamená, že v něm používáš háčky, čárky, číslice a další speciální znaky (-,*^%)
   - ☐ Ano
   - ☐ Ne

11) Přidáváš na svůj profil fotky, a různé aktuálnosti (např.: že jsi na dovolené, že máš nové telefonní číslo, že ses přestěhoval)?
   - ☐ Ano, přidávám
   - ☐ Ne, nepřidávám

12) Už jsi přes sociální síť poznal nového kamaráda, kterého si ve skutečnosti ještě nikdy neviděl ale jen si s ním píšeš?
   - ☐ Ano, poznal
   - ☐ Ne, nepoznal

13) Potvrdíš přátelství někomu, koho ve skutečnosti vůbec neznáš?
   - ☐ Ano, potvrdím
   - ☐ Ne, nepotvrdím

14) Vyhrožoval ti přes sociální sítě někdo, lákal tě na schůzku, chtěl po tobě někdo tvé intimní fotografie?
    - ☐ Ano
    - ☐ Ne

15) Pokud by si měl v budoucnu nějaký výše zmíněný problém, komu by ses svěřil?
    - ☐ Nikomu, styděl bych se
    - ☐ Někomu z rodiny (rodičům, sourozenci, babičce, dědovi)
    - ☐ Kamarádovi, kamarádce
    - ☐ Někomu jinému: _____

16) Cítíš se díky těmto sociálním sítím šťastnější?
    - ☐ Ano, cítím se šťastnější
    - ☐ Ne, necítím

Díky, za Tvůj čas.

Tereza