Západočeská univerzita v Plzni

FAKULTA PEDAGOGICKÁ
KATEDRA VÝPOČETNÍ A DIDAKTICKÉ TECHNIKY

MOŽNOSTI RODIČOVSKÉ KONTROLY BEZPEČNOSTI DĚTÍ NA INTERNETU

BAKALÁŘSKÁ PRÁCE

Jiří Bauer

Informatika se zaměřením na vzdělávání.

Vedoucí práce: PhDr. Lucie Rohlíková, Ph.D.

Plzeň 2019

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, 1. června 2019

.....

vlastnoruční podpis

Chtěl bych poděkovat své vedoucí bakalářské práce PhDr. Lucii Rohlíkové, Ph.D. za odborné vedení, za pomoc a rady při zpracování této práce.

ZDE SE NACHÁZÍ ORIGINÁL ZADÁNÍ KVALIFIKAČNÍ PRÁCE.

OBSAH

ÚVOD

Motto: „Čeští rodiče svým dětem na internetu důvěřují a spoléhají na „čestné“ slovo. Většina z nich neumí dětem filtrovat online obsah“. (Kopecký, Szotkowski, 2018)

Je všeobecně známo, že v současné době je přístup k celosvětové síti internet (World wide web) nepostradatelnou součástí života nejen dospělých, ale i součástí života našich dětí různého věku, včetně dětí předškolního věku. Nejde ho jen tak zakázat nebo vypnout. Teoreticky ano, přeci jenom máme jako rodiče nějaké slovo, byl by to ale krok špatným směrem. Degradovali bychom dítě ve společnosti vrstevníků a časem i v dnešní "digitální" společnosti. Být "na síti" dnes musí být v určité míře každý. Na komunikaci, využívání digitálních zdrojů k práci, vzdělávání a jiným potřebným činnostem je náš svět čím dál více závislý.

Cílem této práce je na základě analýzy prostředí internetu, jeho negativních vlivů na psychiku, zdraví a chování dětí, vyhledat a popsat různé nástroje a možnosti rodičovské kontroly bezpečnosti dětí na internetu včetně technického zabezpečení dětských zařízení a sestavit seznam pravidel, která je třeba rodiči dodržovat, aby tak zajistili dětem jejich bezpečný a zdravý vývoj. Dalším cílem je prezentovat tyto informace rodičům ve srozumitelné formě pomocí jednoduchých webových stránek.

Cílová věková kategorie dětí nebyla v zadání určena, proto jsou zde uvedeny všechny možnosti, které mohou aplikovat rodiče na různé kategorie dětí podle jejich věku, sociální a psychické vyspělosti a úrovně předchozí výchovy nebo momentální situace.

V první kapitole (analytické části) se budeme věnovat analýze prostředí internetu, zjištění, jak je pro děti vlastně důležitý, jakými prostředky se k internetu připojují, jaká rizika jim prostřednictvím internetu hrozí a jak na ně reagují.

Teoretická část práce je rozdělena na dvě kapitoly. V první kapitole si popíšeme možnosti ochrany zařízení dětí proti napadení malwarem, základní bezpečnostní prvky operačních systémů, proč jsou důležité, a přiblížíme si aplikace, kterými je možno ochranu zvýšit.

Ve druhé kapitole teroretické části si popíšeme konkrétní možnosti kontroly a správy aktivit dětí na internetu pomocí nastavení operačních systémů, nastavením prohlížečů,

speciálních aplikací a dalších technických prostředků. U jednotlivých možností zabezpečení a kontroly budou vysvětleny některé jejich funkce, ovládání a cenová dostupnost.

V prakticé části se na základě analýzy a teoretické části práce pokusíme sestavit seznam doporučení pro rodiče, podle nichž by se měli řídit při kontrole bezpečnosti dětí na internetu. Poté vytvořit webové stránky, které mají srozumitelnou formou přiblížit tuto problematiku a možnosti jejího řešení rodičům.

Hlavním přínosem této práce je tedy zvýšení informovanosti rodičů o tomto problému a možnostech, jak tento problém mohou ovlivňovat pomocí ochranného a kontrolního softwearu, dalších technických prostředků a dodržováním doporučených pravidel.

1 SEZNÁMENÍ S PROBLEMATIKOU RIZIKOVÝCH AKTIVIT DĚTÍ NA INTERNETU

1.1 CO JE TO INTERNET

Internet se často nazývá také World Wide Web (www), což se dá přeložit jako „Celosvětová síť“ (pavučina). Skládá se z miliónů propojených zařízení, jako jsou servery, směrovače (routery), přepínače, zařízení a mobilní zařízení např. tablety a mobilní telefony. Sítě ipřipojená zařízen jsou spolu se zařízeními, které jsou v ní připojeny, neustále modernizovány. Přenos, vyhledávání a zobrazování dat v jakékoliv podobě se neustále zrychluje.

Trochu historie (Gruntorád, 2017): Za otce zakladatele internetu je možné označit tři vědce: Vintona Cerfa[1], Roberta Khana[2] a Tima Berners-Lee[3].

Myšlenkou spojení několika zařízení do malé sítě se v 70. letech 20. století zabýval americký vědec Vinton Cerf, který poprvé toto spojení zrealizoval v roce 1971.

Teprve v letech 1989-1991, (což je pro nás dospělé docela nedávno) přišel Tim Berners-Lee s myšlenkou hypertextové sítě založené na prohlížení pomocí prohlížečů a klikacích odkazů, jak je známe dnes.

Na počátku 90. let, konkrétně v létě roku 1991 byl internet zpřístupněn veřejnosti. V roce 1992 Tim Berners-Lee nahrál na web první fotografii.

Internetová síť ještě v roce 1998 měla jen 150 miliónů uživatelů. (Vrabec, 1998) Největší podíl internetových uživatelů v té době byl připojen v USA a Kanadě, nejméně 20%, naproti tomu v České republice internet v té době využívalo podle Vrabce pouhých 4% obyvatel. Dnes používá internet několik miliard lidí na celém světě a drtivá většina obyvatel ČR.

Spočítejme si tedy, kolik uplynulo let od spuštění prvního prohlížeče, v němž si nějaká skupina vědců a jiných nadšenců za veliké peníze mohla na „něco“ kliknout a zobrazit? A jaká byla rychlost této sítě? Od zpřístupnění internetu veřejnosti roku 1991 plynulo 28 let

[1] Vinton Cerf - americký informatik, který je označován za „otce internetu“
[2] Robert Khan - americký elektrotechnik, který spolu s Vintem Cerfem vytvořil TCP/IP
[3] Tim Berners-Lee – v současné době ředitel konsorcia W3C,

a vysokorychlostní „síť sítí“ nesrovnatelných parametrů se síti v 90. letech minulého století je propojena celá planeta.

V praxi to znamená, že data, komunikaci a media jsme schopni posílat rychle na kterékoliv místo na planetě, na kterém je koncové zařízení propojené se „sítí sítí“. Zároveň také ale jsme schopni během okamžiku vyhledat a zobrazit informace umístěné kdekoliv na síti na jednom ze svých připojených zařízení. Mnoho témat a informací můžeme zobrazit i bezděčně při hledání něčeho jiného nebo jen při bezděčném „brouzdání“. Na naše koncová zařízení může někdo zaútočit z kteréhokoliv místa na planetě, desítky tisíc kilometrů vzdáleného nebo z vedlejšího bytu. Cílem může být nás poškodit, pokoušet se zcizit naši identitu, peníze, majetek, citlivá data nebo nám může nějaká osoba nebo skupina osob jen obyčejně lhát, chtít podsunout nepravdivé informace a tak ovlivnit naše myšlení nebo i chování.

A to se týká především našich dětí.

1.2 Rozdílné vnímání internetu dětmi a rodiči.

My dospělí jsme na tom mnohem lépe než naše děti. Jsme již zkušení a dokážeme zkušenosti, které jsme získali v běžném životě uplatnit na "život" internetový. U dětí, zejména v předškolním věku však tyto zkušenosti ještě nejsou. Jsou důvěřivé a přejímají informace z internetu bez vnitřního ověření zkušenostmi z normálního světa.

Rozdíl ve vztahu k internetu mezi dětmi a dospělými je podle mého názoru dobře popsán v knize „Bezpečnost dětí na internetu: Rádce zodpovědného rodiče“ od kolektivu autorů vedeným Lenkou Eckertovou a Danielem Dočekalem, která se zabývá bezpečnosti dětí na internetu obecně.

Podle Marka Prenskyho (Eckertová 2013, Marcprensky.com., 2017) existují termíny „Digital natives“ (Digitální domorodci) a „Digital immigrants“ (Digitální přistěhovalci).

1.2.1 DIGITÁLNÍ PŘISTĚHOVALCI

To jsme my rodiče. Narodili jsme se a prožili velkou část života bez internetu v té podobě, jak ho známe dnes. Mladší rodiče se jistě s internetem již setkali, ale vždy jeho použití bylo limitováno technickými parametry sítí nebo zařízení. Linky i zařízení byly poměrně pomalé pro přenos multimédií.

Vývoj více, či méně sledujeme a účastníme se ho. Podstatnou, větší či menší část života jsme však prožili bez něj. Protože máme tyto zkušenosti, internet rádi využíváme, bereme však internet většinou jako alternativu, doplněk reálného života, možnost vzdělávat se, bavit se, komunikovat.

1.2.2 DIGITÁLNÍ DOMORODCI

Digitální domorodci jsou naše děti. Digitalizace a multimedializace života běžných lidí a veřejného života prostřednictvím internetu se tedy začíná prosazovat již od začátku 90. let min. století. Technologie sítí i používaných zařízení směrem k opravdové multifunkčnosti a multimedialitě, tak jak ji známe nyní, začal zhruba před cca 10 ti lety. Dá se říct, že těmito domorodci v této internetové „vysokorychlostní multimedialitě" jsou děti, kterým je dnes 15 let a méně. Podle Lenky Eckertové se ale i starší děti cítí v ICT[6] jako doma, proto je můžeme za tyto domorodce také považovat. Tyto děti se sice nenarodily v době opravdu multifunkčních, multimediálních zařízení, ale díky svému útlému věku při seznámení s nimi je považují za neoddělitelnou součást života. Vzhledem k možnosti být připojen k síti neomezeně dlouhou dobu a i při jiných (offline) aktivitách být online, se stává život na síti pro děti důležitější než pro nás, rodiče. Stává se hybridním. S větším podílem online aktivit a menším podílem běžného života.

1.2.3 STÍRÁNÍ ROZDÍLU MEZI ONLINE A OFFLINE

Rozumějme aktivity, které vykonáváme bez připojení k internetové síti jako OFFLINE aktivity. Ty, při nichž jsme k internetu z nějakého důvodu připojení, nazvěme ONLINE aktivity.

VRABEC, Vladimír. Internet a hromadné sdělovací prostředky. *Ika*

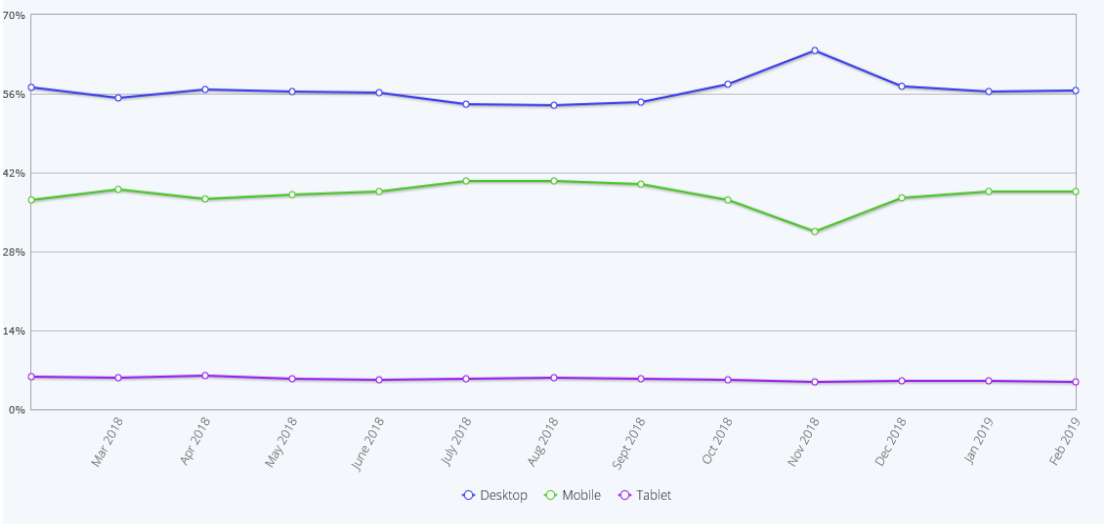
Podle Lenky Eckertové a kol. (2013, Bezpečnost dětí na internetu), rozdíl mezi online a offline aktivitami u dětí mizí. Opravdová mobilita rychlé sítě je předurčena k neustálému online připojení pomocí chytrých mobilních telefonů. Proto i aktivity, při kterých dříve děti byly (a musely) být offline jsou nyní čím dál tím více pod vlivem aktivit online. Vzhledem k jednoduché dosažitelnosti, malé fyzické náročnosti a možností rychlé online zábavy pomalu online aktivity vytlačují ty offline.

1.3 JAK SE DĚTI PŘIPOJUJÍ K INTERNETU?

Podle měření společnosti GS Statcounter.com[7], která se zabývá mimo jiné i měřením počtu přístupů k internetu podle typu zařízení, je zřejmé, že v roce 2018 bylo v Evropě uskutečněno zhruba 56% z počítačů, 43 % z mobilních zařízení telefonů a tabletů[8]

Z těchto statistik vyplývá, že je potřeba při řešení otázky bezpečnosti dětí na internetu stejným způsobem zohlednit osobní počítače i mobilní zařízení. Principy jsou podobné, jak si řekneme v dalších kapitolách.

Graf poměru přístupů podle zařízení. Evropa, únor 2018-únor 2019 (obr. 1)



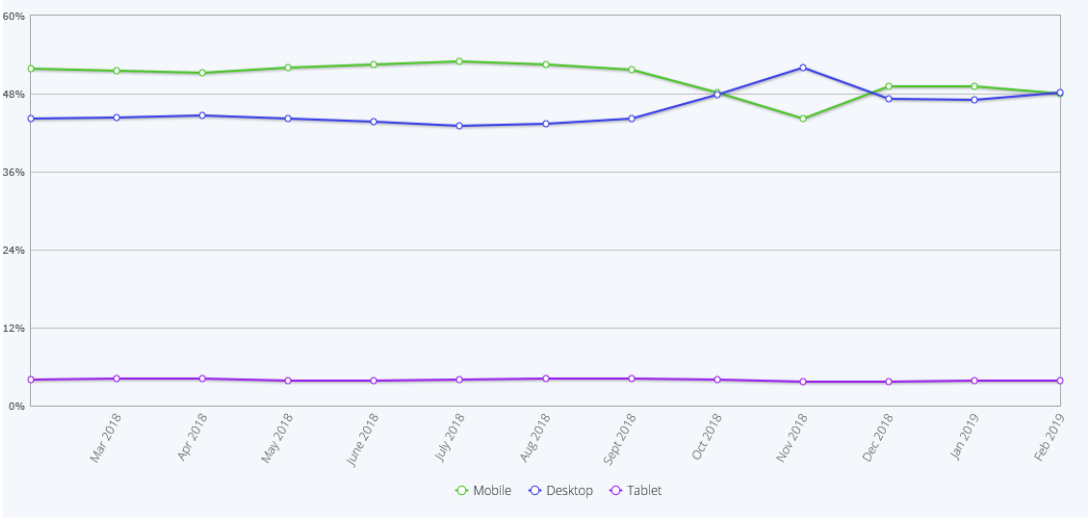
Obrázek 1 - Graf počtu přístupů podle zařízení. Evropa, únor 2018-únor 2019. GS-Statcounter http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/europe)

ros [online]. 1998, ročník 2, číslo 8 [cit. 2019-03-06]. urn:nbn:cz:ik-10272. ISSN 1212-5075. Dostupné z: http://ikaros.cz/node/10272

http://gs.statcounter.com

[8] Měření GS Statcounter. Zdroj [online] http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/europe)

Graf poměru přístupů podle zařízení. Svět, únor 2018-únor 2019 (obr. 2).



Obrázek 2 - Graf poměru přístupů podle zařízení. Svět, únor 2018-únor 2019. GS-Statcounter, http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/worldwide

1.4 Srovnání rizik v závadnosti internetu a jiných médií

Ve srovnání internetových zdrojů a zdrojů z ostatních médií dojdeme k závěru, že internet je mnohem obtížnější kontrolovat než ostatní média a to ze tří důvodů:

- **Média jako televizní a rozhlasové vysílání nebo tisk jsou lépe kontrolovatelná.**

Monitorování těchto médií je lépe proveditelné z důvodu „omezenosti“ jejich počtu a nutnosti sdělovat každou informaci všem případným divákům, posluchačům nebo čtenářům stejně.

- **Vydavatel mediálního obsahu je vždy znám a tedy postižitelný.**

V České republice tento dozor vykonává Rada pro rozhlasové a televizní vysílání, policie a soudy. Při porušení etiky nebo zákona uděluje povinným subjektům pokuty nebo při hrubém porušování je oprávněna odebrat jim licenci na vysílání.

- **Závadné informace lze i zpětně lehce dohledat.**

na uložištích nebo v tištěné podobě a lze je tedy využít i pro případné právní spory a postihy. Proto je i v zájmu médií se těchto praktik vyvarovat. Využívá dobře známé a bezpečné (těžce napadnutelné) kanály (TV, video, radio, tisk).

Internet je naopak médium, na kterém je možno využít anonymity, časové omezenosti existence zdrojů a předkládání těchto zdrojů subjekty, které (pokud jsou vůbec známy) nejsou k dispozici pro případný postih. V praxi to znamená, že závadný obsah není v okamžiku vyšetřování již k dispozici, tedy není dokazatelný nebo je uložen na již nedosažitelném místě, popř. není znám nebo dosažitelný jeho předkladatel.

1.5 Rizika vznikající při komunikaci

Podstatnou částí činnosti dětí na internetu je komunikace. Probíhá pomocí mnoha způsobů například prezentace a kontaktování na sociálních sítích, pomocí e-mailů, veřejných fór a chatovacích místností, ale i pomocí neveřejných chatovacích místností, messengerů a aplikací typu messenger nebo Skype, které jsou schopny v reálném čase přenášet videa a fotografie.

1.5.1 Kyberšikana

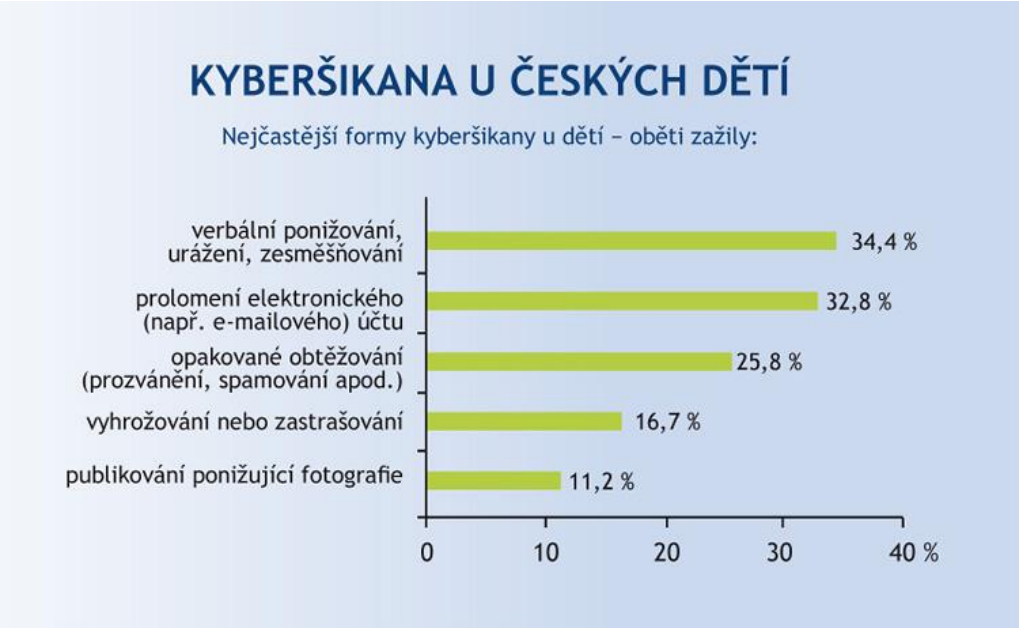
Šikana obecně je agresívní, úmyslné a opakované jednání či chování uskutečňované proti jednotlivci nebo skupině, který/á se nemůže snadno bránit (Whitney a Smith, 1993, Olweus, 1999). U dalších autorů je šikana chápána jako forma obtěžování založená na nerovnováze sil a systematickém zneužívání moci (Smith a Sharp, 1995, dále Rigby, 2002). Další definice říká, že Kyberšikana je specifický druh šikany, který využívá internet, mobilní telefony a další nástroje moderních komunikačních technologií za účelem ublížení a zesměšnění jiné osoby. (Hulanová, 2012)

Centrum prevence rizikové virtuální komunikace Univerzity Palackého v Olomouci provedlo průzkum s názvem „Nebezpečí elektronické komunikace 2“, jehož se zúčastnilo více než 12 500 žáků základních a středních škol z celé České republiky. Podle výsledků tohoto průzkumu se s kyberšikanou setkalo téměř 60 %t dětí ve věku 11–17 let.

Autoři zprávy (Kopecký, Krejčí 2011) zde uvádějí nejzávažnější formy kyberšikany:

- ponižování, urážení, zesměšňování nebo jiné verbální ztrapňování,
- publikování ponižujících záznamů (fotografií, videí a audiozáznamů),
- vyhrožování a zastrašování,
- vydírání,
- obtěžování (např. telefonováním, prozváněním,
- **spamováním).**umisťování pornografie na místě, které je dětem přístupné.

Podle výzkumů v této oblasti 72,96 % dětí uvádí na sociálních sítích údaje, podle kterých může být vysledováno, jako je jméno a příjmení. Svou e-mailovou adresu zveřejňuje necelých 63 % dětí a přibližně 22 % dětí dokonce své telefonní číslo. (Kopecký, Szotkowski, Krejčí, 2012)



Obrázek 3 - Druhy kyberšikany u českých dětí Nebezpečí elektronické komunikace 2 (2011)

1.5.2 SEXTING

Sextingem nazýváme situace, kdy si děti, převážně pubertálního věku vzájemně posílají své intimní fotografie. Z již citovaných výzkumů a výzkumné zprávy „Nebezpečí internetové

komunikace III“ vyplývá, že hlavními důvody tohoto počínání je nuda, snaha navázat kontakt s osobou jiného pohlaví nebo sebepropagace.

Z uvedené výzkumné zprávy vyplývá, že v roce 2011 umístilo své vlastní sexuální materiály na internet 8,25 procenta dětí. 9,7 procenta je odeslalo jinému člověku (například příteli, přítelkyni, kamarádu, kamarádce) a že sexuální materiály odesílají převážně děti ve věku vyšším než 15 let.

1.5.3 NAVAZOVÁNÍ VIRTUÁLNÍCH KONTAKTŮ S NEZNÁMÝMI OSOBAMI - (KYBERGROOMING)

Většina uživatelů vystupuje na internetu pod určitou identitou. Ta může být pravá, nepravá nebo anonymní. Velmi často děti komunikují pomocí přezdívek a očekávají to samé od svých protějšků. Kybergroomingem pak nazýváme snahu vylákat z dítěte pod nepravou identitou jeho intimní fotografie a videa za účelem vydírání a často také za účelem vylákání dítěte na schůzku mimo ochranu rodičů nebo kamarádů. Zde existuje velká pravděpodobnost, že cílem schůzky bude dítěti ublížit.

1.5.4 KYBERSTALKING

Výrazem kyberstalking označujeme aktivity, kdy útočník svou oběť neustále dlouhodobě obtěžuje s cílem narušit její duševní rovnováhu. Formy stalkingu jsou různé a většinou je útočník kombinuje. Jsou to především hrozby, falešná obvinění, urážení, shromažďování informací, napadání identity a dat, vybavení oběti, neustálé obtěžování prostřednictvím e-mailů nebo sociálních sítí. Dále napodobování oběti nebo objednání zboží jménem oběti. Nezřídka se útočník snaží o fyzický kontakt, který může přerůst ve fyzické napadení oběti.

1.5.5 ZÁVISLOST DÍTĚTE NA INTERNETU (INTERNETOVÝCH HRÁCH)

Dotazníkové šetření k tomuto tématu a vyhodnocení provedla Pavla Skleničková, která ho zveřejnila ve svém článku[10] na serveru E-Bezpečí[11]. Položila žákům 2. stupně základních škol otázku, zda se cítí lépe online (na internetu) nebo offline.

10 Závislosti a chování na internetu u dětí 2. stupně ZŠ 12. 8. 2012 [online] Dostupný na https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/online-zavislosti/518-zavislost2st
11 Projekt E-Bezpečí - Centrum prevence rizikové virtuální komunikace
Pedagogická fakulta Univerzity Palackého V Olomouci dostupný [online] na https://www.e-bezpeci.cz/index.php

Zde citujeme odpovědi dotázaných dětí:

Téměř polovina žáků (43 žáků ze 100 žáků) se cítí lépe, když je on-line. Podívejme se na některé odpovědi žáků:

- „Virtuální svět je zábavnější.“ (chlapec, 14–15 let)
- „Mohu si psát s někým starším, kdežto osobně se stydím.“ (dívka, 13 let)
- „Lepší komunikace.“ (chlapec, 12-13 let)
- „Nemusím si tam na nic hrát a hlavně je vše jednodušší.“ (chlapec, 12-13 let)
- „Je to lepší, můžu tam dělat, co chci a nikdo to neví.“ (dívka, 12-13 let)
- „Útěk z reality, od problémů, hodně přátel.“ (chlapec, 12-13 let)
- „V normálním světě nemám tolik kamarádů jako na internetu.“ (chlapec, 13 let)
- „Otevřenější komunikace, je lehčí se seznámit.“ (dívka, 12-13 let)
- „Jsem neustále mezi přáteli. Kdykoliv řeším své problémy.“ (chlapec, 12- let)

Z těchto odpovědí Pavla Skleničková shrnuje důvody, proč se tolik dětí cítí na internetu lépe než v reálném životě:

- anonymita, možnost přetvářky a lhaní
- absence pravidel a sankcí reálného světa
- odreagování a zábava
- větší otevřenost
- redukce úzkosti, pocit bezpečí při problémech v reálném světě.

Podle Pavly Skleničkové (www.e-bezpeci.cz, 2012) si menší děti tyto důvody neumějí sice pojmenovat, ale chovají se v souladu s nimi. Starší děti již je pojmenovat do jisté míry umějí, ale chápou je (jak jsme si ukázali na odpovědích dětských respondentů) jako pozitiva, potřebují také vedení rodičů. Skleničková zde uvádí, že rodiče musí dětem vysvětlovat a učit je, v jaké míře je dobré internet využívat.

Současně jim ukázat a umožňovat, aby objevily také zajímavá pozitiva reálného světa. Dodává, že děti si musí uvědomit, že v reálném světě existuje řada aktivit, které se ve virtuálním světě nevyskytují a nelze je virtuálně nahradit.

1.6 RIZIKOVÝ OBSAH

Rizikový obsah může být samozřejmě cíleně vyhledáván, hlavně staršími dětmi. Děti v útlém věku, pro které je nejvíce rizikový, se s ním však nejčastěji setkávají náhodně při pohybu na internetu za jiným účelem.

Děti mohou být vyděšeny, rodičům se však stydí svěřit z důvodu studu a viny, že stránky navštívily. Proto je velmi důležité se postarat o zamezení nechtěného (nebo chtěného) přístupu k takovémuto obsahu jak pomocí technických prostředků, tak komunikací s dětmi o tomto tématu.

Rizikový obsah na internet rozděluje Kamil Kopecký takto[12]:

- nelegální obsah
- legální obsah, ale nelegálně zpřístupnění dětem
- legální, ale proděti závadný obsah

1.6.1 NELEGÁLNÍ OBSAH

- **Dětská pornografie a nelegální sexuální praktiky**

pornografie zachycující násilí či neúctu k člověku, sex se zvířetem, nabídka dětské prostituce apod.

- **Obsah spojený s extremismem**

porušující mezinárodní i české normy spojené s ochranou lidských práv, obsah diskriminující konkrétní skupinu osob na základě rasové, náboženské či jiné odlišnosti, obsah zaměřený na nenávistnou propagandu.

[12] Kamil Kopecký, „Děti a závadný obsah na internetu“ 25. červen 2015[online] dostupný na https://www.e-bezpeci.cz/index.php/temata/dali-rizika/1037-deti-a-zavadny-obsah-na-internetu

- **Nelegální obchodování, nelegální nabídka drog a zakázaných látek**

nabídka psychotropních látek, jejich prekursorů, jedů, nelegální prodej zbraní, výbušnin atd.

- **Obsah porušující autorská práva**

film, hudba a software. V ČR lze legálně stáhnout si film či hudbu pro "svou potřebu". Zákon však upravuje, že musí jít o dílo (na programy se volné užití díla nevztahuje:

  - zveřejněné,
  - nesmí být prolomena jeho ochrana,
  - nesmí být pořízeno při jeho projekci v kině,
  - nesmí být dále šířeno (tedy např. sdíleno, kopírováno,
  - nesmí proběhnout veřejná projekce, nesmí být půjčováno
  - nesmí být půjčováno

1.6.2 LEGÁLNÍ OBSAH A JEHO NELEGÁLNÍ ZPŘÍSTUPNĚNÍ DĚTEM

Další kategorii rizikového obsahu tvoří materiály, které jsou v zásadě legální, ale nejsou určeny dítěti a jejich předkládání dítěti může být považováno za nelegální. Jedná se zejména o pornografické materiály.

Pornografie, zobrazovaná bez nelegálních praktik, je v zásadě obsahem legálním, nicméně její zpřístupňování dítěti je nelegální, tedy trestné. Trestné je:

  - **nabízení či přenechání pornografie dítěti**
  - umisťování pornografie na místě, které je dětem přístupné.

Osoba, která tedy dítěti pornografii zpřístupňuje, se může dopustit např. trestného činu „Šíření pornografie“, ale také např. „Ohrožování výchovy dítěte“.

1.6.3 LEGÁLNÍ, ALE PRO DĚTI ZÁVADNÝ OBSAH

Mezi legální, ale závadný obsah řadíme vše, co může být na internetu zveřejněno, ale co může děti negativně ovlivňovat. Může podporovat sebepoškozování, poruchy příjmu potravy, nespavost. Řadíme sem také násilný a nesnášenlivý obsah, nebezpečné (smrtelné

nebo zraňující) scény, informace spojené se sebevražedným chováním (a asistovanými sebevraždami), záznamy šikany a kyberšikany apod. (Kopecký,2015).

1.7 MOŽNOSTI OVLIVŇOVÁNÍ CHOVÁNÍ, KOMERCÍ A INFORMACEMI

Je otázkou, jak ochránit naše děti před dezinformacemi a obchodními sděleními zaměřenými pod rouškou zajímavosti nebo „objektivity“ na zisk nebo ovlivňování osob (v našem případě dětí).

Ať už se jedná o akci tajné služby některého státu nebo o prodej vlasového přípravku, je to především na nás, abychom dítěti poskytli informace vedoucí k tomu, aby bylo schopné rozlišit na základě zkušeností s naplněným reálným životem a informací získaných od rodičů nebo starších sourozenců ovlivněných rodiči, kamarádů ovlivněných rodiči atd., jestli informace může být pravdivá. U malých dětí lze zakázat mediální stránky. U starších dětí (ze zkušeností s vlastními dětmi odhaduji od počátku školního věku) již si to nemůžeme dovolit. Vzhledem k tomu, že radši preferují zprávy z internetu než z TV nebo radia, mohou být stigmatizována v kolektivu nevědomostí o určitých důležitých událostech.

Na druhou stranu jsou tyto mediální stránky zdrojem neustálých dezinformací, především z oblasti politiky, obchodu a showbyznysu. Vzhledem k provázanosti důležitých a nedůležitých, zavádějících nebo vyloženě nepravdivých informací na jednom (několika dítětem preferovaných) místech není možné toto nechat bez povšimnutí. Je třeba vysvětlovat dětem, co může být pravda, co je normální, a co již ne. I přes to, že na některých serverech lze vybrat okruhy témat, které budou na mediální stránce zobrazeny (ovšem až po přihlášení dítěte uživatelským účtem a heslem v prohlížeči, kde se může jednoduše odhlásit) a možnostem jako blokování reklamy (AdBlock - bude vysvětleno v kapitole „Nastavení prohlížečů) dopodrobna nemůžeme nikdy nastavit, jaké informace našemu dítěte stránka poskytuje. Na rodičích tak v tomto případě zůstává odpovědnost, jak dítě s informacemi naloží. Ideální stav je bezproblémová a důvěrná komunikace „dítě-rodič-dítě“. Tedy, že se dítě nebojí rodiči svěřit a rodič mu poskytuje dostatečnou zpětnou vazbu. Je to otázka důvěry, kterou je třeba budovat stejně jako v běžném životě.

1.8 Kybernemoci

Nepřiměřeným nebo špatným používáním elektronických zařízení při přistupování k internetu mohou vzniknout zdravotní potíže fyzického nebo psychického rázu ovlivňující fyzické nebo duševní zdraví dítěte. Podle Kopeckého a Szotkowskiho (2018) mezi nejznámější kybernemoci patří:

- **Syndrom falešného zvuku (fantomové vibrace)**

Jedná se poruchu projevující se pocitem neexistujícího zvonění mobilního telefonu, případně vibrací. Dítě má mnohokrát denně potřebu zkontrolovat telefon, protože má pocit, že někdo volá nebo píše.

- **Syndrom počítačové myši (myšitida)**

Termínem myšitida označujeme onemocnění vznikající při nadměrném používání počítačové myši. Dochází k poškozování vazů zápěstí, předloktí, a dokonce i v oblasti lokte.

- **Nomofobie a syndrom FOMO**

Mezi kybernemoci lze podle Kopeckého a Szotkowskiho zařadit také tzv. nomofobii a syndrom FOMO. Nomofibie je druhem závislosti. Jedná se o strach dítěte z toho, že mobilní telefon nebude moci z nějakého důvodu používat. Nomofobie je druhem závislosti. Jedná se sice o vysokoškolské studenty, ale lze předpokládat, že tyto návyky získali již v dětství.

- **Technostres**

Technostres definoval v roce 1984 americký psychoterapeut Craig Brod jako „moderní nemoc způsobenou neschopností jedince vyrovnat se s novými informačními a komunikačními technologiemi (ICT) psychicky zdravým nebo pozitivním způsobem“ (Brod, 1984). Další autoři (Rosen, Weilová, 1997) definují technostres jako „civilizační chorobu, specifický druh stresu, projevující se nutkavou potřebou být neustále on-line, být „na příjmu“ a vstřebávat další a další informace.“

- **Technoference**

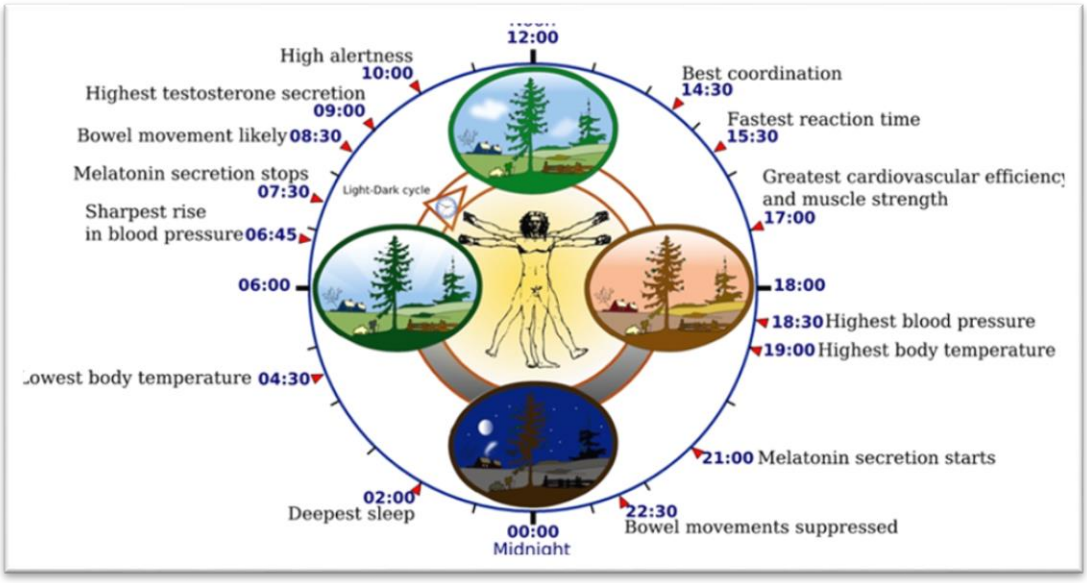
Podle autorů se technoferencí označuje porucha vyznačující se neustálou potřebou kontrolovat mobilní telefon nebo email apod. Toto neustále přerušuje jiné běžné aktivity jako je konverzace, jídlo, sport nebo hra. Technoference negativně zasahuje také do přátelských a rodinných vztahů.

- **Kyberchondrie**

Podle Kopeckého a Szotkowskiho kyberchondrie (cyberchondria) souvisí s hypochondrií, postižený vyhledává příznaky neexistujícího onemocnění na internetu, vznikají neurózy, úzkosti a iracionálním obavy o vlastní zdraví. Díky obrovskému množství informací, které lze vyhledat a neodbornosti čtenáře, mohou být tyto informace špatně pochopeny nebo vytrženy z kontextu.

- **Narušení biologických hodin (cirkadiánního cyklu)**

Autoři Kopecký a Szotkowski dále pokládají otázku, zda rodiče někdy přemýšleli o tom, proč by děti, neměli před spaním hrát s mobilními telefony nebo používat jiná LCD zařízení. Vysvětlují zde roli tzv. cirkadiánního rytmu, tedy rozlišování dne a noci. Tělo začíná hormon melatonin, který zklidňuje organismus před spánkem na základě setmění. Pokud dítě sleduje display, jehož vyzařované světlo je svou vlnovou délkou velmi podobné světlu dennímu, produkce hormonu vůbec nezapočne nebo je výrazně omezena.



Obrázek 4 - Cirkadiánní cyklus člověka. https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/dalsi-temata/1338-kybernemoci-uvod-do-problematiky

U dětí pak dochází k nespavosti, oslabení imunity, zvyšuje se pravděpodobnost vzniku rakoviny, poruch spánku, vznik kardiovaskulárních onemocnění apod.

Na některých zařízeních lze potlačit modrou složku světla, které display vyzařuje. Tato funkce se většinou nazývá Noční režim (Nightshift).

- **Kyberzávrať**

Termínem kyberzávrať popisují K. Kopecký a R. Szotkowski jako dezorientaci dítěte a pocity závrati v novém nebo nepřehledném digitálním prostředí nebo při příliš rychlém scrollování obrazovkou případně sledováním videa s rychlými efekty a střihy. Tato dlouhodobě překonávaná závrať se může projevit v následném chování dítěte.

- **Digitální amnézie (Google efekt)**

Termín digitální amnézie označuje rychlé zapomínání informací, které si nemusíme pamatovat, ale lze je rychle vyhledat na internetu. Lidé postiženi digitální amnézií si spíše pamatují, kde informace najít, ale samotné informace si nepamatují.

- **Vznik úzkostí a depresí z obsahu internetu**

Vilma Hušková[13] z Úřadu Rady pro rozhlasové a televizní vysílání[14] tvrdí, děti nikdy v historii nebyly vystaveny takovému množství rizikových mediálních obsahů jako v současnosti. Podle Hruškové se tyto skutečnosti jednoznačně podílejí na formování dětské psychiky, děti na ně reagují odlišně, od otupění a lhostejnosti k utrpení jiných, u citlivých dětí pak zvýšenou úzkostností a strachem v reálném světě o sebe a své blízké. Nereálně a přehnaně hodnotí nebezpečí, kterému v běžném životě oni nebo i společnost čelí.

1.9 NEBEZPEČÍ INTERNETOVÝCH AKTIVIT DĚTÍ PRO OKOLÍ - RODINU

Při výčtu nebezpečí vznikajících při aktivitách dětí na internetu nesmíme zapomenout na nebezpečí vyplývající z jejich aktivit pro rodiče.

Především se jedná o nebezpečí zcizení citlivých dat, jako jsou čísla bankovních karet, čísla a hesla bankovních účtů, hesla e-mailů nebo zařízení, hesla k bezdrátovým sítím apod.

Tyto údaje lze pak zneužít pro krádež financí nebo identity dětí nebo rodičů. Jak na to si přiblížíme v dalších kapitolách.

[13] Vilma Hrušková. Mediální analytik z Úřadu Rady pro rozhlasové a televizní vysílání
[14] Úřad pro rozhlasové a televizní vysílání (RRTV)

2 MOŽNOSTI TECHNICKÉ OCHRANY ZAŘÍZENÍ DĚTÍ

V této kapitole si vysvětlíme rizika malweru, a způsoby zabezpečení zařízení proti jejich napadení. Jedním z kritérií výběru byla i cena produktů. Pokud v kategorii neexistuje kvalitní produkt zdarma nebo je placená verze výrazně lépe vybavena, je zde uvedena s upozorněním, že je placená.

2.1 CO TO JE MALWARE?

Přibližme si nyní, s jakými hrozbami v této oblasti se můžeme setkat. To se netýká pouze OS Windows, ale producenti malware napadají všechny operační systémy.

Termínem malware je v praxi označován nebezpečný nebo škodlivý software obecně, tedy všechny jeho následující formy:

- **Virus**

je jakýkoliv škodlivý software, který se může samovolně šířit dál v zařízení nebo počítačové síti většinou bez vědomí uživatele, přičemž má ještě jinou funkci, kterou uživateli škodí.

- **Adware**

je software, který po napadení zařízení nejčastěji zobrazuje reklamy na www stránkách v internetovém prohlížeči, které prodává autor tohoto adwaru. Adware není přímo nebezpečný, ale spíše obtěžující.

- **Spyware**

je velmi nebezpečná forma škodlivého programu. Jedná se o tzv. „špióny“. Spyware nasazený do zařízení, či mobilních zařízení vždy nějakým způsobem zjišťuje a odesílá informace obsažené v tomto zařízení nebo o aktivitách uživatele zařízení. Může jít o monitorování stisků kláves, internetové komunikace, použitých aplikacích, odesílání snímků obrazovky nebo fotografií, souborů apod.

- **Keyllogery**

jsou podskupinou spyware a jsou specializovány pro odečítání stisků kláves a přiřazení stisků ke konkrétní činnosti na zařízení nebo přímo i v prohlížeči internetových stránek. Takto se nejčastěji získávají hesla a čísla bankovních karet!

- **Trojský kůň**

je klíč k překonání ochrany a získání přístupu k zařízení nebo zařízení využívajícímu internet, s cílem následného nasazení nějakého jiného škodlivého softwaru.

- **Rootkit**

je zákeřný „maskovací“ software, který se spouští již spolu se startem operačního systému. Funguje tak, že skrývá adresáře, ve kterých je další škodlivý software umístěn a škodlivé procesy, které se spouští v operačnímu systému. Dokáže „zamaskovat“ jejich přítomnost.

- **Ransomware**

je druh malwareu, který po průniku do zařízení nějakým způsobem znepřístupní data nebo celý operační systém. Toho může dosáhnout zašifrováním dat pomocí klíče, který zná jen útočník, změnou master boot record, diskového oddílu nebo uzamknutím operačního systému. Poté se zobrazuje výzva k zaplacení určitého poplatku za zpřístupnění dat.

- **Phishing**

je podvodná metoda, kterou se útočník pokouší získat od uživatele citlivá údaje – čísla platebních karet, hesla atd. Nejčastěji se toto děje podsouváním falešných www stránek například bank a jejich internetového bankovnictví.

- **Scareware**

je nežádoucí software označovaný jako scareware vás má nejprve vyděsit a poté přinutit k nějaké činnosti. Obvykle se navenek tváří seriózně. Může jít třeba o program, který „proskenuje“ zařízení a najde v něm neexistující hrozbu. Za její „odstranění“ musíte zaplatit.

Před nezvanými návštěvníky je tedy třeba ochránit všechna zařízení v domácnosti, tedy počítače, tablety i mobilní telefony.

2.2 BEZPEČNOSTNÍ PRVKY OPERAČNÍCH SYSTÉMŮ

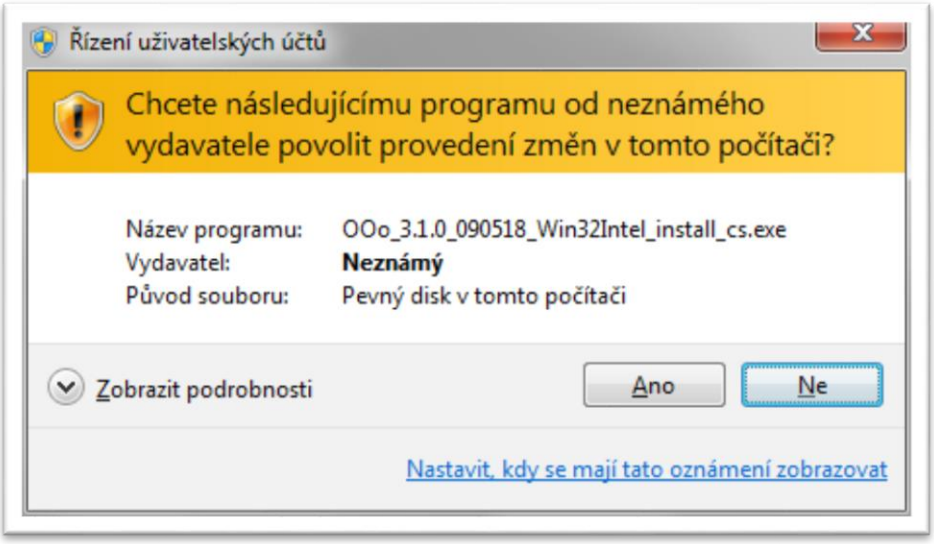
Část této starosti za nás řeší výrobci OS. Každý operační systém je již v základu vybaven některými bezpečnostními funkcemi, které zajišťují základní ochranu před hrozbami zvenčí.

- **Firewall**

V domácích podmínkách je Firewall software, oddělující nežádoucí provoz mezi dvěma sítěmi (naší domácí a internetem). Firewall data propouští jedním nebo druhým směrem podle určitých předem definovaných pravidel. Brání tak zejména před neoprávněnými průniky do sítě a odesílání dat ze sítě bez vědomí a souhlasu uživatele. Firewall má mnoho možností nastavení, ty jsou však většinou určena pro zkušené uživatele. My nebudeme toto téma dále rozebírat. Důležité však je aby firewall na našem zařízení zůstal vždy zapnutý.

- **Řízení uživatelských účtů (UAC)**[15]

Zejména v systému Windows (od verze Windows 7) je vestavěna tato utilita, jejíž účelem je kontrolovat, zda aktivity, které probíhají na zařízení, provádí skutečně uživatel nebo zda nedošlo k útoku zvenčí. Útočník by mohl zvenku provádět např. instalace škodlivého softwaru. V případě, že UAC zaznamená aktivitu, (např. instalaci nějaké aplikace) zeptá se uživatele, zda tuto aktivitu provádí on sám. V případě, že uživatel tuto aktivitu neprovádí, je možné ji zamítnout (nebo povolit). Tento nástroj se dá vypnout, ale není to doporučeno.



Obrázek 5- Dialogu UAC https://www.cnews.cz/novinky-windows-7-rizeni-uzivatelskych-uctu-uac/

[15] UAC- User Account Control – utilita f. Microsoft

- **Aktualizace operačního systému a aplikací**

Výrobce každého operačního systému dbá na to, aby vydával jeho aktualizace. Ty mají za cíl odstranit postupně objevované chyby v zabezpečení a funkčnosti systémů. Proto je nezbytně nutné je mít v systému povoleny. Ve výchozím nastavení všech operačních systémů je nastaveno přijímání aktualizací na automatické. Systém se tedy sám aktualizuje a uživatel se nemusí o nic starat. V nastaveních OS lze různými způsoby aktualizace zakázat nebo přikázat operačnímu systému, aby se dotazoval uživatele na povolení k instalaci.

Volit tyto možnosti však důrazně nedoporučuji.

- **Aplikace - použití důvěryhodných zdrojů**

Operační systémy Android, různé distribuce Linuxu nebo IOS na počítačích či mobilních zařízeních využívají způsob instalace aplikací z tzv. „Repozitářů" (Zdrojů). Tedy z nějakého „Centrálního úložiště" aplikací pro příslušný OS, které se nachází na chráněných serverech. Tvůrci aplikací musejí nejdříve správci aplikací na serveru předat informace jako je zdrojový kód aplikace a další. Aplikace je poté prověřena na přítomnost škodlivých kódů a teprve po prověření je uložena na server a povolena její nabídka uživatelům ke stažení a používání. Tyto úložiště obsahují již desetitisíce různých aplikací, které jsou zdarma nebo jsou zpoplatněny. V systému Android známe tuto službu pod názvem „Google Play"[16], v systému IOS pod názvem „App Store"[17]. Ve verzi Windows 8 a 10 pak „Microsoft Store"[18]. Předcházející model stahování z různých zdrojů zůstal jako alternativa zachován, ale opět ho nelze doporučit

U různých dalších distribucí Linuxu se setkáváme s označením "Repozitáře". V nastavení těchto OS je možno toto změnit a instalovat aplikace i z jiných, neověřených zdrojů, například z jiných stránek, SD karet apod., ale tuto možnost opět výrazně nelze doporučit.

Ve výchozím nastavení lze z těchto úložišť stahovat a instalovat bez jakéhokoliv omezení. Základním nástrojem těchto úložišť je možnost aktivace rodičovského zámku, pomocí něhož můžeme vybrat obsah, který považujeme vhodný pro své dítě. Dítěti se pak

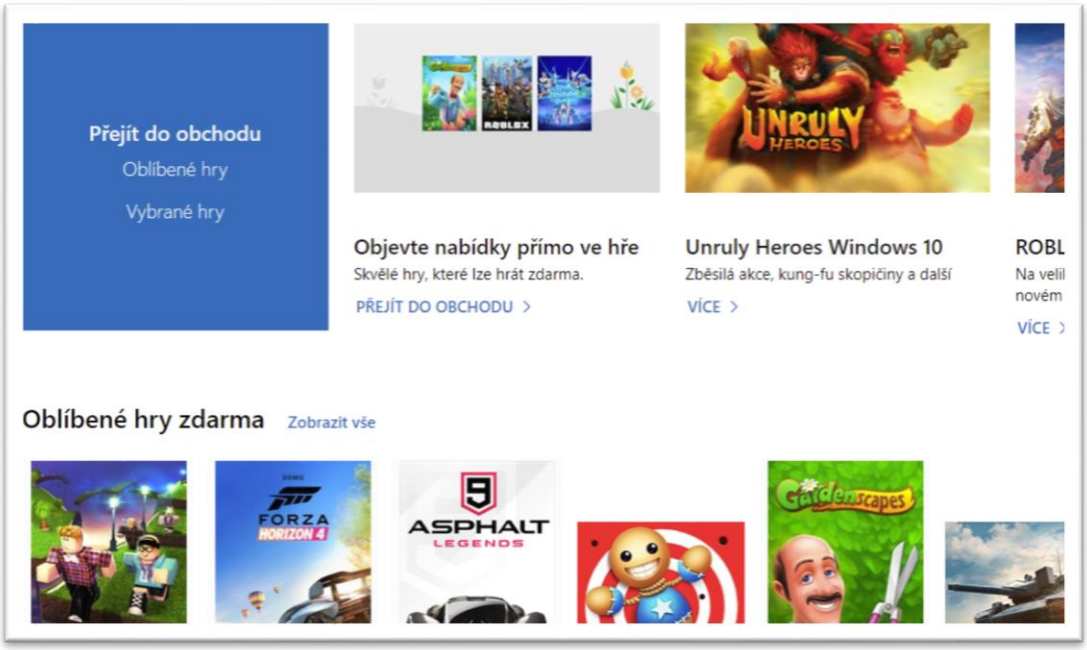
16 Google Play- úložiště aplikací OS Android (Google Inc.)aplikace dostupná z OS Google Android.
17 Mezinárodní systém PEGI (Pan European Game Information) Zdroj:[online]. Dostupné na https://pegi.info/
18 Microsoft Store: Centrální, chráněné úložiště aplikací. Zdroj[online] dostupné na https://www.microsoft.com/cs-cz/store/b/home

zobrazuje jen obsah, který vývojáři označili podle mezinárodní normy PEGI[19] jako vhodný pro námi zvolenou kategorii.

Číselné označení normy není nutně označením věku. Je proto vhodné ověřit si, jaký obsah se v jednotlivých kategoriích vyskytuje:

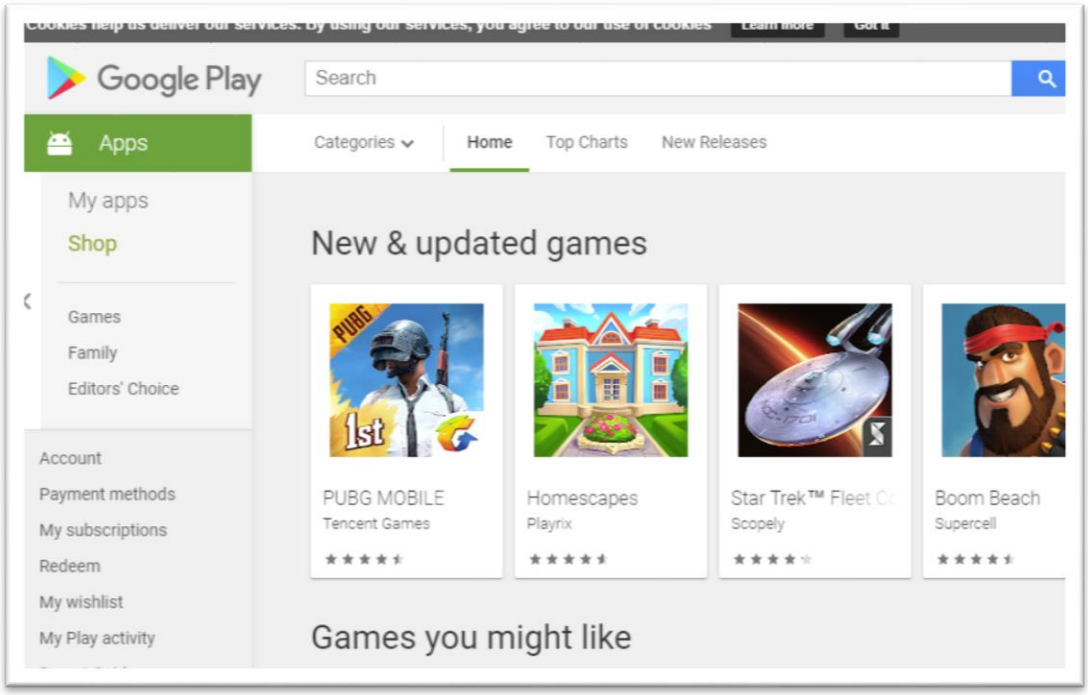
- **PEGI 3 -vhodná pro nejmenší děti (hry typu puzzle, pohádky, dětská hudba apod.).**
- **PEGI 7 - už se mohou objevovat scény nahánějící strach (např. ve hrách).**
- **PEGI 12 - může obsahovat jistou formu náznaku násilí a nahoty.**
- **PEGI 16 - může obsahovat scény nahoty a násilí s mírným projevem,**
- PEGI 18 **- je kategorie obsahu pro dospělé, tedy obsah není omezen.**

Ukázky úložišť aplikací jednotlivých systémů jsou na obrázcích 6, 7, a 8:

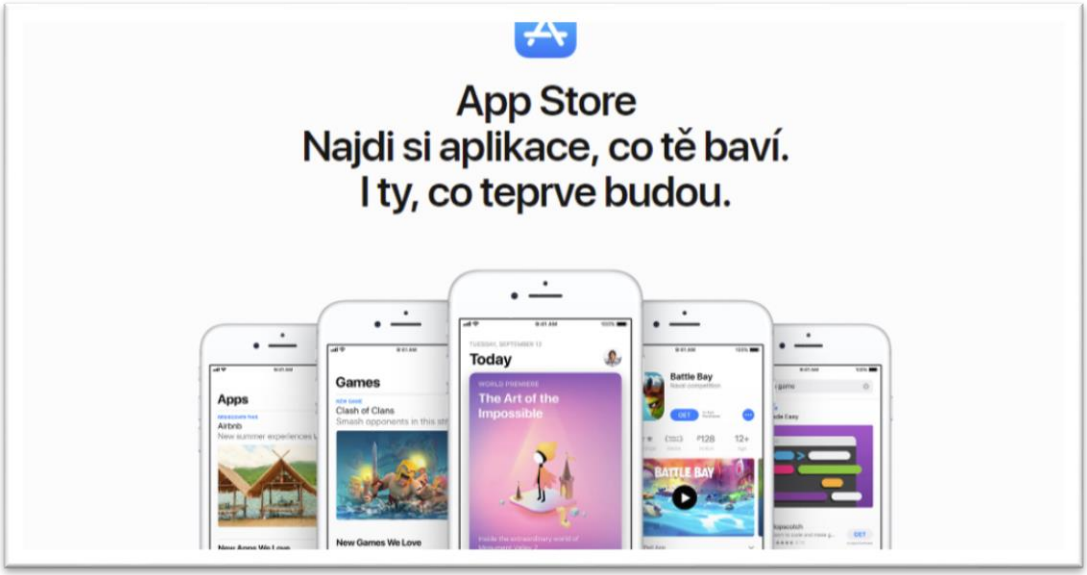


Obrázek 6 - Windows Store pro zařízení s OS Windows 8 a 10. [online] printscreen https://www.microsoft.com/cs-cz/store/b/home

[17] App Store- úložiště aplikací OS IOS (Apple, aplikace) dostupná z OS iOS.



Obrázek 7 -Google play (webové prostředí) [online] printscreen https://play.google.com/store)



Obrázek 8 - prostředí AppStoru pro IOS. [online] https://www.apple.com/cz/ios/app-store/

2.3 OCHRANA PROTI NAPADENÍ ZAŘÍZENÍ DÍTĚTE (ANTIVIROVÉ PROGRAMY)

Firewall, aktualizace operačního systému a instalace bezpečných aplikací popř. UAC jsou tedy velice důležité. Přesto mnoho hackerů a škodlivého software je schopno do systému proniknout. Navíc nás nemusí ochránit před nástrahami, které jsou aktivní při našich návštěvách interaktivních stránkách, které mohou samy o sobě obsahovat např. nebezpečné skripty, phishing apod.

Proto je velice důležité, aby operační systém byl chráněn ještě Antivirovým programem.

Antivir je aplikace, která pomocí uložených databází známého malware nebo na základě podobnosti nových škodlivých kódů, dokáže rozpoznat hrozící nebezpečí a zablokovat jej dříve, než nás ohrozí. Toto provádí pomocí různých modulů a v různém rozsahu, podle verze, kterou nainstalujeme.

Většinou platí, že placené verze programů mají větší rozsah ochrany. Bezplatné Antiviry často obtěžují reklamou.

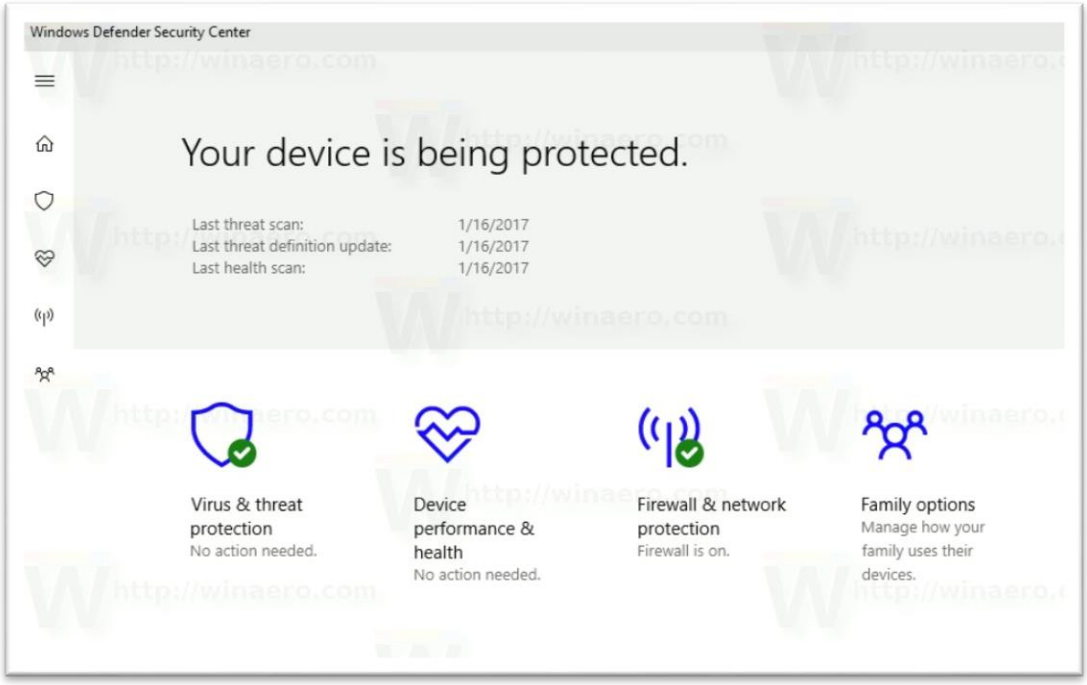
2.3.1 ANTIVIRY SE ZÁKLADNÍ OCHRANOU (DOSTUPNÉ ZDARMA)

- **Windows Defender**

Windows Defender je součástí systému Windows již od verze Windows Vista. V této verzi je však vhodné doplnit systém některým z dalších plnohodnotných antivirových programů. Pokud antivirový program doinstalujeme do zařízení, Windows Defender se automaticky vypne, aby nedocházelo ke kolizím. Podle firmy Microsoft je Windows Defender od verze Windows 10 již mimo jiné plnohodnotným antivirem[21]. Po instalaci operačního systému Windows 10 je plně funkční a není třeba ho nijak nastavovat. Informace o možných hrozbách získává z cloudového prostoru firmy Microsoft.

[21] Microsoft. Windows Defender pro Windows 10 [online] dostupné na: https://www.microsoft.com/cs-cz/windows/comprehensive-security

Prostředí programu Windows Defender (obr. 9)



Obrázek 9-Prostředí programu Windows Defender. Zdroj[online] https://siliconangle.com

V případě, že dáme přednost jinému antivirovému programu, je možné ho doinstalovat. Modul ochrany Windows Defenderu před viry a hrozbami se automaticky znefunkční.

- **Avast Free Antivirus**

Je český antivirus se základní ochranou. Jeho stažení a používání je zdarma. Prostředí programu je kompletně v českém jazyce. Blokuje malware, spyware. V této neplacené verzi nedokáže ochránit před spamem. V základní verze není vybaven vlastním firewallem. Ochranu před spamem a vyšší zabezpečení internetového bankovnictví nebo rodičovskou kontrolu má až placená verze programu. Nevýhodou je také, že hůře než placená verze programu blokuje stránky s phishingem Další informace najdete v kapitole „Antiviry placené“.

Aplikace je v základní verzi zdarma a vhodná pro OS Windows, Android i IOS. Stáhnout lze z aplikací AppStore, Google play nebo na adrese https://www.avast.com

- **AVG Antivirus FREE**

AVG Antivirus Free patří je bezplatný antivirový program. Jeho výhodou je snadná obsluha a české uživatelské prostředí. Slabá stránka antiviru AVG spočívá v horším blokování

zavirovaných internetových stránek. Pro tento program platí informace podobné jako u produktu Avast Free Edition.

Aplikace je v základní verzi zdarma a vhodná pro OS Windows, Android i iOS. Stáhnout lze z aplikací App Store, Google Play nebo na adrese https://www.avg.com.

- **Avira Antivirus FREE**

Je německý antivirus se základní ochranou. Jeho stažení a používání je taktéž zdarma. Prostředí programu je v anglickém jazyce. Blokuje malware, spyware. V neplacené verzi neochrání před spamem a též není vybaven vlastním firewallem. Ochranu před spamem a vyšší zabezpečení internetového bankovnictví nebo rodičovskou kontrolu má až placená verze programu.

2.3.2 Antiviry s rozšířenými funkcemi (placené) a srovnání funkcí a účinnosti

Placené verze antivirových aplikací jsou vždy vybaveny dalšími funkcemi, které dále rozšiřují úroveň ochrany proti internetovým hrozbám.

Tyto verze antivirových programů disponují speciálními moduly, jako jsou:

- **Anti-spam**

Odstraní nevyžádaný spam, tedy nevyžádané obtěžující e-maily, které zařízení nebo MZ zahlcují zbytečnými a nebezpečnými daty. Tuto funkci lze využít, pokud přijímáme e-maily přímo do zařízení pomocí instalované aplikace (typicky Microsoft Outlook). Pokud se s emaily spoléháme na webovou formu poštovního klienta, například www.seznam.cz nebo www.volny.cz, www.gmail.com, můžeme se spolehnout na anti-spam majitele těchto serverových aplikací.

- **Herní mód/režim**

Tato funkce pozastaví oznámení antivirového programu tak, aby nerušila při hraní her. Antivir pak likviduje hrozby „tiše“.

- **Banking**

ochrana internetového bankovnictví, zadávání čísel karet a hesel. Vyšší zašifrování informací, přenášených mezi uživatelem a bankou a kontrola přístupu třetích stran.

- **Šifrování dat**

Důkladnější šifrování dat. Znemožňuje útočníkům rozšifrovat přenášená data.

- **Rodičovská kontrola**

Touto funkcí disponují vyspělé antivirové programy, bohužel jen v placených verzích, kromě již zmíněné aplikace Windows Defender, kterou jsem již zmiňoval. V nejednom případě však placené antiviry poskytují větší možnosti a variabilitu než WD. Pro tento účel existují však specializované aplikace, které si popíšeme později.

- **Zabezpečení webkamery**

Některé viry jsou schopny bez vědomí uživatele zapínat kameru a přenášet obraz útočníkovi. Ten ho pak může zneužít např. k vydírání dítěte.

- **Kontrola domácí sítě**

Tato funkce neustále kontroluje a brání případným neoprávněným přístupům do rodinné Wi-Fi sítě.

- **Správa hesel**

Díky této funkci si lze uložit všechna hesla do jednoho, maximálně zabezpečeného místa v zařízení.

- **Rozšířený Firewall**

Jak již jsme si řekli, firewall je základní obrannou funkcí OS, která zařízení uchrání před hackery. Placené verze antivirů mají svůj sofistikovanější firewall, který v případě instalace nahradí ten systémový.

I když antiviry jsou z uživatelského pohledu podobné, existují mezi nimi rozdíly ve funkčnosti, ceně a kvalitě odhalování hrozeb.

Srovnání placených verzí antivirů z hlediska úspěšnosti odhalení a likvidace hrozby[22]: (Virus Bulletin, 2018)

Antivirový program	Počet testů	Úspěšný	Neúspěšný	Procento úspěšnosti
ESET	103	100	3	97,30%
Microsoft (firemní produkty)	43	41	2	95,3 % *
Norton (Symantec)	66	58	8	87,7 % *
BitDefender	69	59	10	86,80%
Avira	69	56	13	80,00%
Kaspersky	105	85	20	82,00%
F-Secure	70	53	17	75,7 % *
AVG	92	67	25	74,20%
Avast!	96	69	27	73,80%
McAfee	72	49	23	68,1%*
* některé antiviry se nezúčastnily testu VB100				

Tabulka 1 - Přehled úspěšnosti antivirových programů v testu [online] https://www.antivirovecentrum.cz/antiviry/srovnani.aspx

Zde je srovnání 5 antivirů z hlediska vybavenosti funkcemi provedené společností Testado[25] (Smejkal, 2019)

Antivir	Eset Family Security	Kaspersky Internet Security	AVG Internet Security	Avast Internet Security	Norton Security Deluxe
	9,1	**9**	**8**	**8**	**7,5**
Cena na 1 rok	1 590 Kč	799 Kč	1 199 Kč	1 190 Kč	699 Kč
Antispyware	✓	✓	✓	✓	✓
Herní mód	✓	✓	×	✓	✓
Nízké sys. nároky	✓	✓	×	✓	✓
Podpora v češtině	✓	✓	✓	✓	✓
Jednoduchá obsluha	✓	✓	✓	✓	✓
Ochrana plateb	✓	✓	✓	×	✓
Firewall	✓	✓	✓	✓	✓
Šifrování dat	✓	×	✓	✓	✓
Webkamera	✓	✓	✓	×	✓
Ochrana domácí sítě	✓	✓	✓	✓	✓
Rodičovská kontrola	✓	✓	×	×	×
Antispam	✓	✓	✓	✓	✓
Správa hesel	×	×	✓	×	✓

Tabulka 2- Přehled funkcí a ceny placených antivirových programů 2019 [online]https://www.testado.cz/nejlepsi-antiviry/)

[22] Porovnání účinnosti antivirů: Zdroj[online]: https://www.antivirovecentrum.cz/antiviry/srovnani.aspx,
[25] Testado.cz -recenzní online magazín. Testuje IT produkty. Zdroj [online] https://www.testado.cz

3 KONTROLA A SPRÁVA AKTIVIT DĚTÍ V OS WINDOWS, IOS A ANDROID

V této kapitole si přiblížíme základní možnosti kontroly, správy času a aktivit dětí na internetu pomocí nastavení operačních systémů, prohlížečů a specializovaných aplikací i domácích routerů.

Operační systémy Windows a iOS disponují vestavěnými funkcemi kontroly a správy dětských aktivit. V systému Android je pak nutno stažení aplikace firmy Google. K dispozici jsou i další aplikace pro všechny systémy.

3.1 KONTROLA A SPRÁVA AKTIVIT V OPERAČNÍM SYSTÉMU WINDOWS

Mobilní veřejností proběhla zpráva společnosti Microsoft o postupném ukončení verze Windows 10 Mobile.[29] Poslední informace naznačují, že Microsoft vyvíjí nový operační systém pro mobilní zařízení s názvem „Andromeda“[30], údaje však do dnešní doby nebyly potvrzeny. Z tohoto důvodu a z důvodu malého zastoupení OS Windows na mobilních zařízeních dětí, se v této pokapitole budeme věnovat výhradně počítačům s OS Windows.

Funkce "Rodičovská kontrola" se poprvé objevila ve Windows Vista a 7. S příchodem Windows 10 se proměnila na „Možnosti pro rodinu“. Slouží k nastavení a kontrole využívání Windows a internetu dětmi. Umožňuje:

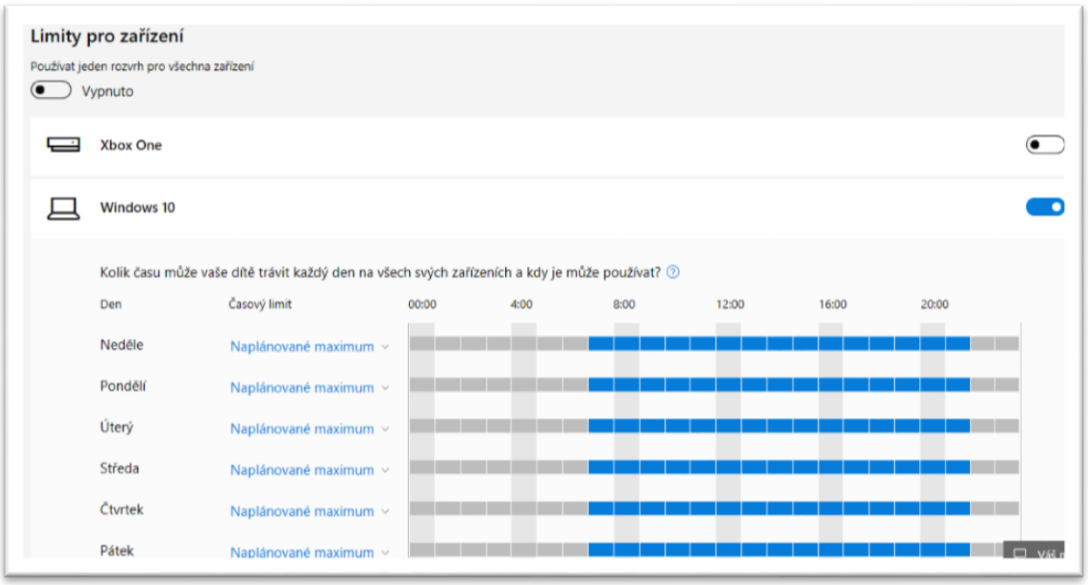
- sledovat, co přesně děti na zařízení dělají pomocí logování
- povolovat a kontrolovat čas, který na zařízení tráví.
- blokovat určité weby
- povolit jen určité weby
- blokovat vybrané aplikace
- povolit/zamítnout platby za aplikace

[29] Ukončení podpory Windows 10 Mobile.[zdroj]online https://support.microsoft.com/cs-cz/help/4485197/windows-10-mobile-end-of-support-faq
[30] Andromeda- zdroj[online]http://touchmobile.cz/co-bude-dal-s-windows-10-mobile-a-existujici-telefony-windows/

Utilitu ve Windows Vista a 7 spustíme tak, že klikneme na Start -> Ovládací panely a na Rodičovská kontrola. Pro zřízení skupiny (rodiny) a zařazení jejích členů musíte mít zřízen „Účet Microsoft“. Taktéž každý člen rodiny, jemuž chcete aktivity spravovat.

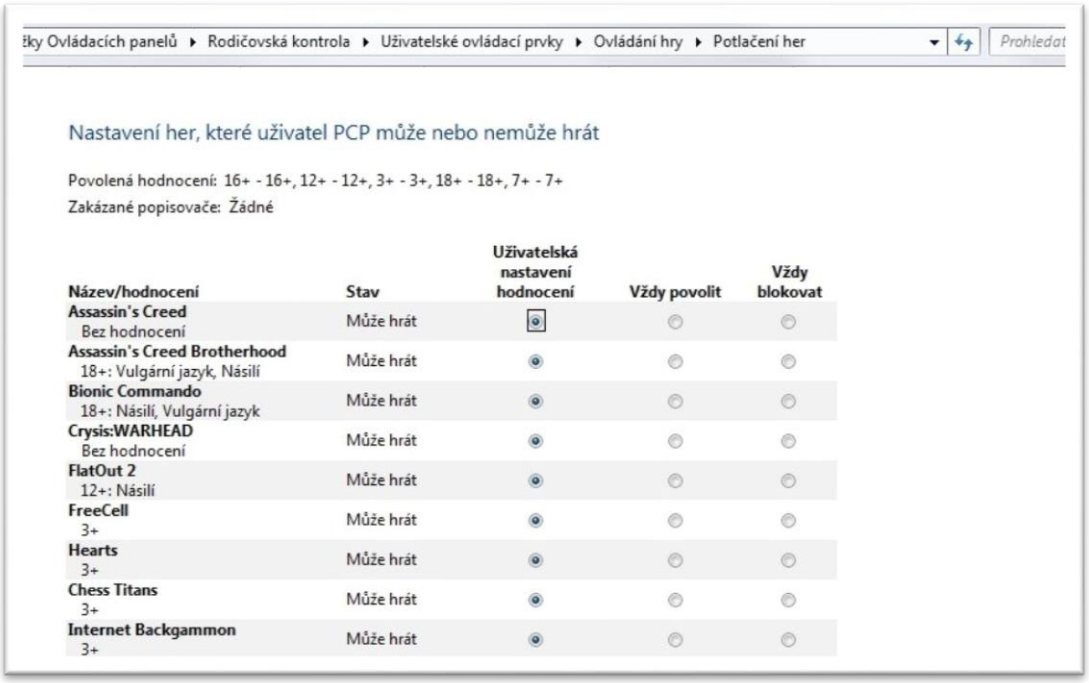
Potřebné účty zřídíme postupem: Ovládací panely -> Účty -> Rodina a jiní uživatelé. Aby se daly účty v rodině spravovat, je třeba, aby se všichni členové přihlašovali těmito účty již do OS Windows. Tato aplikace však funguje pouze na zařízeních s OS Windows a při přihlášení dítěte na zařízení pod svým Účtem Microsoft. Pro procházení internetu musí používat Microsoft Edge nebo Internet Explorer. V případě nastavení blokuje ostatní webové prohlížeče, aby dítě nemohlo pomocí nich kontrolu obcházet. Při testování však (dle vlastního zjištění) blokování nefungovalo pro prohlížeč Firefox (verze 54).

Ukázka prostředí aplikace „Rodičovská kontrola“. Na této stránce je možné nastavit čas, po který dítě smí zařízení využívat (obr. 10).



Obrázek 10-Ukázka nastavení aplikace. Printscreen Windows 10.

Mezi dalšími možnostmi nastavení najdeme například omezení spouštění aplikací zařízení s OS Windows, konkrétně zde spouštění her (obr. 11)



Obrázek 11-Nastavení kontroly her.[online] www.pcporadenstvi.cz

Další aplikace vytvořené pro kontrolu a správu v zařízeních s OS Windows

V systému Windows lze podobně, jako v ostatních OS lze pomocí aplikace Microsoft Store[31] nebo z jiných zdrojů online nainstalovat další aplikace pro kontrolu a správu zařízení vybavené OS Windows 10, 8,7 (mnohdy tyto aplikace fungují i na OS Windows XP, ale výrobci většinou kompatibilitu nezaručují).

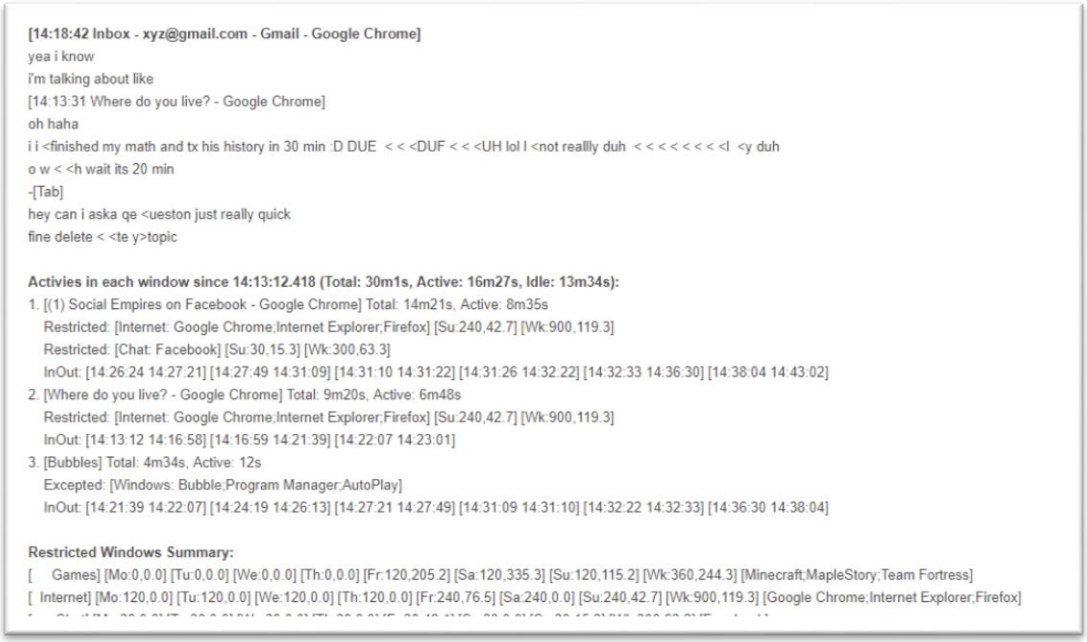
Zde jsou některé aplikace, které jsou zajímavou alternativou k aplikaci Rodina a navíc disponují zajímavými funkcemi:

- **Screen Watcher**

Tato aplikace je zdarma. Pomocí aplikace lze nastavovat denní a týdenní limity pro různé aplikace s určitými klíčovými slovy ve svém názvu. Monitoruje také dobu využívání aplikací a prohlížeče. Například je možno vytvořit pravidlo pro omezení určité sociální sítě na 60 minut denně. Z těchto pravidel je možno vytvořit výjimky například pro stránky se

[31] Microsoft Store – aplikace vestavěná do OS Windows-Centrální úložiště aplikací.
Také dostupné online na https://www.microsoft.com/cs-cz/store/apps/windows.

vzdělávacím obsahem. V případě zadání aplikace pořizuje screenshoty obrazovek a zaznamenávat konverzaci dítěte na sociálních sítích a chatech. Získaná data ukládá do logu nebo je odešle rodiči e-mailem.[32]



[14:18:42 Inbox - xyz@gmail.com - Gmail - Google Chrome]
yea i know
i'm talking about like
[14:13:31 Where do you live? - Google Chrome]
oh haha
i i <finished my math and tx his history in 30 min :D DUE < < <DUF < < <UH lol I <not reallly duh < < < < < < < <I <y duh
o w < <h wait its 20 min
-[Tab]
hey can i aska qe <ueston just really quick
fine delete < <te y>topic

Activies in each window since 14:13:12.418 (Total: 30m1s, Active: 16m27s, Idle: 13m34s):
1. [(1) Social Empires on Facebook - Google Chrome] Total: 14m21s, Active: 8m35s
   Restricted: [Internet: Google Chrome;Internet Explorer;Firefox] [Su:240,42.7] [Wk:900,119.3]
   Restricted: [Chat: Facebook] [Su:30,15.3] [Wk:300,63.3]
   InOut: [14:26:24 14:27:21] [14:27:49 14:31:09] [14:31:10 14:31:22] [14:31:26 14:32:22] [14:32:33 14:36:30] [14:38:04 14:43:02]
2. [Where do you live? - Google Chrome] Total: 9m20s, Active: 6m48s
   Restricted: [Internet: Google Chrome;Internet Explorer;Firefox] [Su:240,42.7] [Wk:900,119.3]
   InOut: [14:13:12 14:16:58] [14:16:59 14:21:39] [14:22:07 14:23:01]
3. [Bubbles] Total: 4m34s, Active: 12s
   Excepted: [Windows: Bubble;Program Manager;AutoPlay]
   InOut: [14:21:39 14:22:07] [14:24:19 14:26:13] [14:27:21 14:27:49] [14:31:09 14:31:10] [14:32:22 14:32:33] [14:36:30 14:38:04]

Restricted Windows Summary:
[Games] [Mo:0,0.0] [Tu:0,0.0] [We:0,0.0] [Th:0,0.0] [Fr:120,205.2] [Sa:120,335.3] [Su:120,115.2] [Wk:360,244.3] [Minecraft;MapleStory;Team Fortress]
[Internet] [Mo:120,0.0] [Tu:120,0.0] [We:120,0.0] [Th:120,0.0] [Fr:240,76.5] [Sa:240,0.0] [Su:240,42.7] [Wk:900,119.3] [Google Chrome;Internet Explorer;Firefox]

Obrázek 12 - Log aplikace ScrrenWatcher.[online] https://sites.google.com/site/goppieinc/pc-screen-watcher/sample-email

- **Verity Internet Parental Controls**

Jedná se o shareware. Aplikaci lze vyzkoušet zdarma, ale pro další používání je nutno ji zakoupit nebo platit měsíční poplatek (cca 49USD /cca 3USD za měs.) Blokuje specifické programy nebo webové stránky, zaznamenává dobu spuštění software, navštívené stránky, chatování pomocí snímků obrazovky. Pomocí aplikace lze nastavit denní limity použití zařízení, aplikace nebo webové stránky na přihlášení uživatele systému Windows. Umožňuje různá nastavení pro každé dítě přihlášené do Windows. Aplikace umožňuje rodiči přístup k informacím prostřednictvím webového rozhraní chráněného heslem nebo automatických e-mailů[33].

[32] Screen Watcher. Zdroj [online[dostupný na https://sites.google.com/site/goppieinc/home
[33] Verify Internet Parental Control. Aplikace NCH software. Zdroj [online] dostupné na https://www.nchsoftware.com/childmonitoring/index.html

- **iProtectYou**

Umožní filtrovat závadný obsah internetu a disponuje funkcemi rodičovské kontroly. Je možno sledovat aktivity uživatelů a omezovat přístup k určeným aplikacím nebo blokovaným webům podle plánu. Je možné určit, které programy mohou přistupovat k internetu. Podává podrobné statistiky o provozu na zařízení.[34]

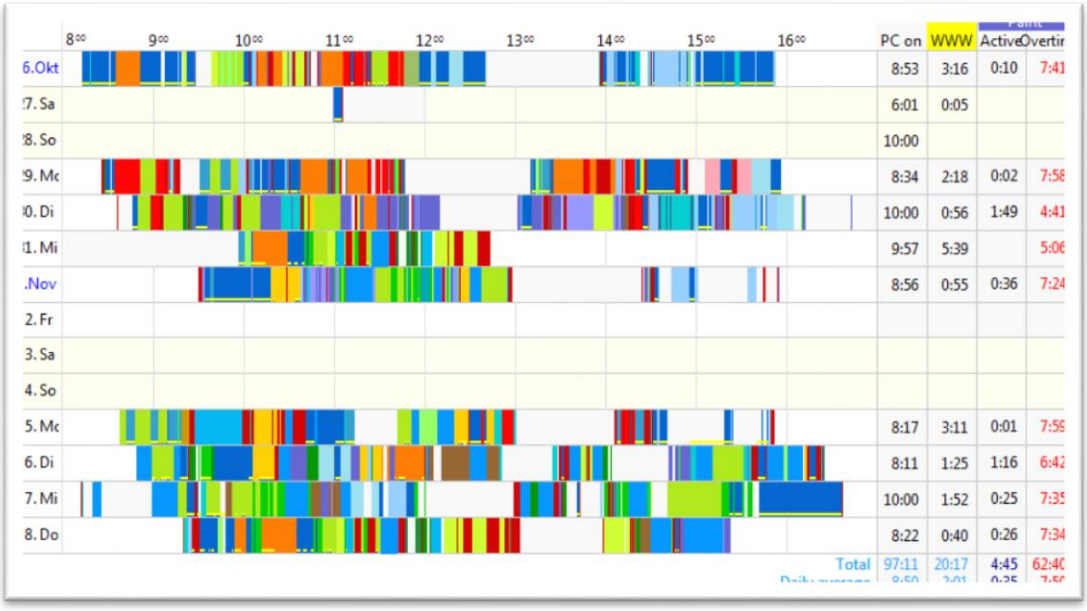
Další aplikace, které jsou zaměřeny především na „produktivitu" dítěte na zařízení:

- **ManicTime 3.4**

Aplikace je v individuální verzi zdarma, v serverové verzi za poplatek. Pomocí různých satistik aplikace sleduje na pozadí Windows práci na zařízení, častost i dobu spouštěných aplikací a další aktivity dítěte[35]. Lze ji tedy využít například pro zjištění, zda dítě na zařízení v určený čas studovalo apod.

- **Visual TimeAnalyzer 1.5**

Aplikace je typu shareware. Tedy po vyzkoušení je nutno zaplatit poplatek za další využívání. Je zaměřena sledování produktivity. Podrobně zobrazuje týdenní statistiky, používání počítače, použití programů a webových stránek online. (obr. 13)



Obrázek 13-Výstup Visual TimeAnalyzer. Aplikace Neuber Software. [online] https://www.neuber.com/timeanalyzer/time-tracking.html

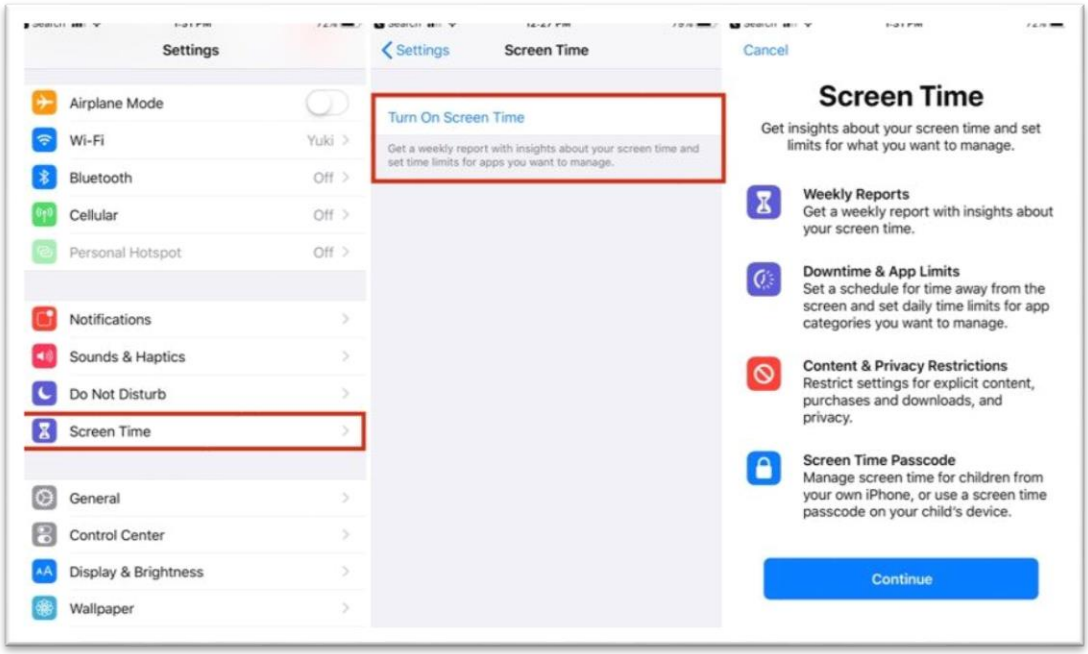
[34] iProtectYou. Aplikace SoftforYou software. Zdroj [online] dostupné na http://www.softforyou.com/ip-index.html
[35] Manic Time. Aplikace NCH software. Zdroj [online] dostupné na https://www.manictime.com/

Program je vybaven funkcí okamžité notifikace online v případě přihlášení dítěte na zařízení[36]. Obrázek ukazuje sestavu časového využití aplikací podle uživatelem přiřazené barvy a souhrnnou statistiku.

3.2 KONTROLA A SPRÁVA AKTIVIT V OPERAČNÍM SYSTÉMU IOS

Systém rodičovské kontroly je na zařízeních s operačním systémem iOS (tedy iPhonu, iPadu a iPodu touch) vestavěn přímo do systému. Spravuje se pomocí nastavení v uživatelském menu zařízení. Nastavení si ukážeme na příkladu telefonu s OS iOS 12.

Spravovat a kontrolovat systém dítěte je možno přímo na jeho zařízení nebo dálkově na svém zařízení. Pak je nejdříve nutno na rodičovském i dětském zařízení nastavit položku Screen Time (čas obrazovky) na „ON“. Tato položka se nachází v aplikaci „Nastavení“. Nastavení je nutno chránit heslem, aby nemohlo být dítětem změněno.(obr. 14)



Obrázek 14-ukázka prostředí nastavení položky Screen Time [online] https://applenovinky.cz/2018/08/navod-jak-nastavit-rodicovskou-kontrolu-a-funkci-screen-time-v-systemu-ios-12/

Pomocí funkce Downtime je možno nastavit čas, po který chceme dítěti využívání zařízení nebo jeho vypnutí v určitý čas. Lze zvolit i režim, při kterém je dítě informováno o blížícím

[36] Visual TimeAnalyzer. Aplikace Neuber Software
Zdroj[online] dostupné na https://www.neuber.com/timeanalyzer/index.html

se vypnutí a získat na žádost ještě 15 min na ukončení činnosti nebo také režim, kdy dítě může pokračovat (ukončit Screen Time).

V nastavení lze zablokovat využívání určitých aplikací nebo zajistit, aby se při jejich otevření dítěti zobrazilo upozornění, že by mělo aplikaci uzavřít.

Další možností je funkce „Limit aplikací“. Pomocí této funkce může rodič přidělit čas pro využití aplikací podle kategorií. Může nastavit omezení pro všechny aplikace a kategorie nebo například sociální sítě, hry, zábavu, kreativitu, produktivitu, vzdělávání, čtení, zdraví a fitness a další.

Další funkce má název „Omezení obsahu“. Zde lze omezit nákupy v App Store, zakázat dítěti odstraňovat aplikace, zakázat přístup k vybraným aplikacím a nastavit omezení věku pro určitý obsah podle normy PEGI. V nastavení lze také blokovat určité weby nebo povolovat jen vhodné. Je zde také možnost zakázat v prohlížečích zobrazování výsledků vyhledávání explicitních výrazů. Je také možno zjistit, kde se nachází kontrolované zařízení.

Další aplikace vytvořené pro kontrolu a správu v zařízeních s OS iOS

- **ParentKit**

Je alternativní aplikace pro vzdálenou kontrolu a správu činností dítěte na zařízení se systémem iOS.. (obr. 15)

Obrázek 15 - Prostředí aplikace ParentKit. [online]
https://itunes.apple.com/us/app/parentkit-parental-controls-for-ios/id600618138?mt=8

ParentKit umožňuje kompletní kontrolu, plánování, kdy má dítě přístup k různým komponentám na svém zařízení, umožňuje blokovat aplikace, filmy, TV pořady a hudbu na základě věku, a to ze svého zařízení nebo pomocí webového rozhraní. Bohužel se jedná opět o shareware. První měsíc lze aplikaci provozovat zdarma, poté za předplatné[37]

3.3 KONTROLA A SPRÁVA AKTIVIT V OPERAČNÍM SYSTÉMU ANDROID

Ve starších verzích operačního systému Android bylo možné spravovat pouze stahování aplikací z Google Play[38]. K tomuto účelu slouží utilita „Rodičovský zámek“. Tato utilita je dostupná a spravuje se v aplikaci Google Play na zařízení dítěte. Pomocí této utility lze nastavit, které aplikace, filmy nebo hudbu dítě může stahovat do svého mobilu s ohledem na nastavení rodiče pomocí výše vysvětlené mezinárodní normy PEGI.

Od verze Google Android 7.0[39] se možnosti kontroly významně rozšířily.

- Aplikace Google Family Link

Dítě musí být vybaveno zařízením min. s touto verzí a vyšší nebo zařízením Chromebook[40] (Chrome v. 71[41] a vyšší), popř. iPhone nebo iPad s OS IOS min. verze 9. Z obchodu Google Play nebo App Store lze stáhnout a nainstalovat utilitu Google Family Link[42]. Po instalaci aplikace a přihlášení pomocí Google účtu[43] dostanou rodiče řadu možností kontroly. Získají například přehled o tom, co si dítě stáhlo z Google Play.

Stažení některých aplikací musí rodič (správce) schválit (povolit) na žádost dítěte. Zároveň správce může sledovat, kolik času tráví dítě v jednotlivých aplikacích. Výstupy mohou být také zasílány formou týdenních a měsíčních souhrnů. Instalaci aplikací mohou rodiče také schvalovat a zamítat. K dispozici jsou také limity používání, kdy rodič může určit, kolik času smí potomek na zařízení během dne strávit. V určených nočních hodinách, kdy má dítě spát, lze telefon nebo tablet vzdáleně uzamknout. Lze také předem naplánovat „večerku“ na

[37] ParentKit – aplikaca. Zdroj [online] https://svetaplikaci.tyden.cz/rodicovska-kontrola-aplikace-ktere-pohlidaji-vase-deti/
[38] Google Play- centrální úložiště aplikací OS Android (Google Inc.)
[39] Operační systém Android 7.0 (Noughat) – Google Inc.
[40] Chromebook – zařízení, většinou notebook s operačním systémem Chrome.(Google Inc.)
[41] Chromium – webový prohlížeč f Google Inc., vestavěný do OS Chrome.
[42] Google Family Link – aplikace pro kontrolu a řízení aktivit dětí v systému Android.
[43] Google účet – účet ve tvaru xxx@gmail.com

určitou večerní hodinu podle kalendáře. Důležitou funkcí je také možnost zjistit, kde se právě zařízení vašeho dítěte nachází. Aplikace Google Family Link také automaticky nabízí aplikace doporučené učiteli, které lze rovnou přidat do zařízení dítěte.

Pro správu a kontrolu je nutno nainstalovat aplikaci jak na zařízení správce (rodiče), tak dítěte. Oba musí mít také založen Google účet, pod kterým se při spuštění zařízení do služby automaticky přihlásí. V okamžiku zařazování zařízení (dítěte) do skupiny musí být zařízení správce (rodiče) a dítěte v těsné blízkosti, aby nedošlo ke zneužití jinou vzdálenou osobou. Kontrola je možná pouze u dětí do 13 let bez jejich souhlasu. Po dovršení věku 13 let jsou dítě i rodič dotázáni, zda chtějí po dohodě v kontrole pokračovat.

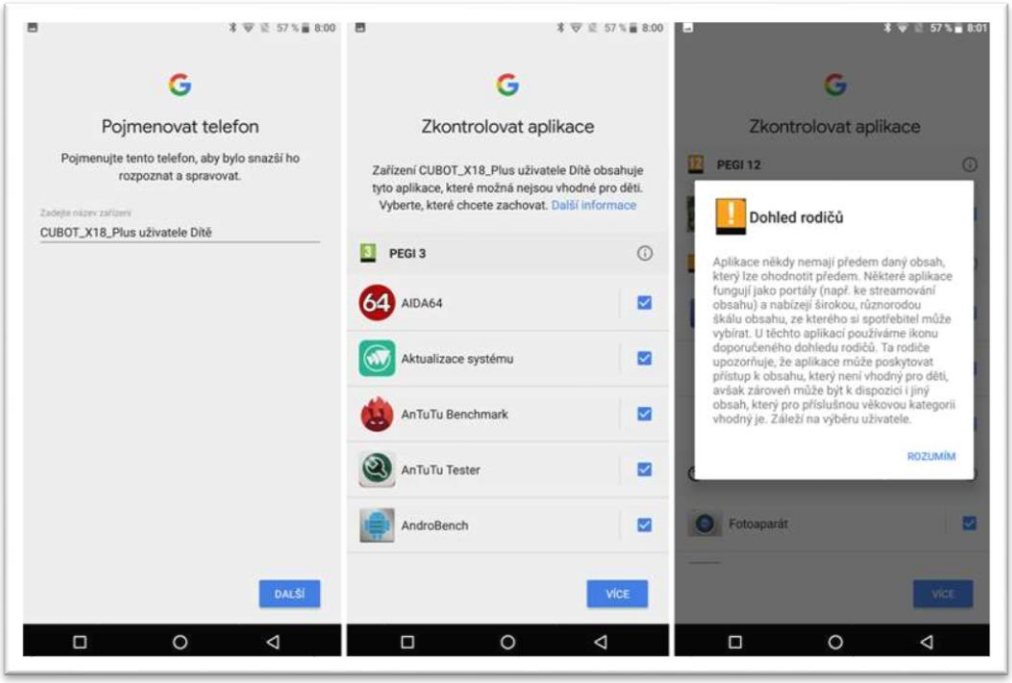
Při zařazování dítěte do služby Google Family Link je nutno:

pro úplnou správu jako správce vlastnit zařízení s OS Android min. ve verzi 4.4, iPhone nebo iPad s OS IOS min. verze 9 popř. Chromebook s podporu Android aplikací, být starší než 18 let, mít účet Google, zřídit a uvést google účet dítěte, uvést jméno dítěte (není ověřováno, lze zadat přezdívku), uvést věk dítěte, uvést číslo platební karty a uvést svůj souhlas.

Některá nastavení lze uskutečnit přes webové stránky families.google.com, nabídka správy zde ale není úplná. Proto je doporučeno využívat aplikaci Google Family Link instalovanou v obou zařízeních. Instalace aplikace na rodičovský telefon se provádí z aplikace Google Play[44] na telefonu rodiče. Po splnění výše uvedených podmínek a krátkém úvodním nastavení, je telefon připraven ke správě zařízení dítěte.

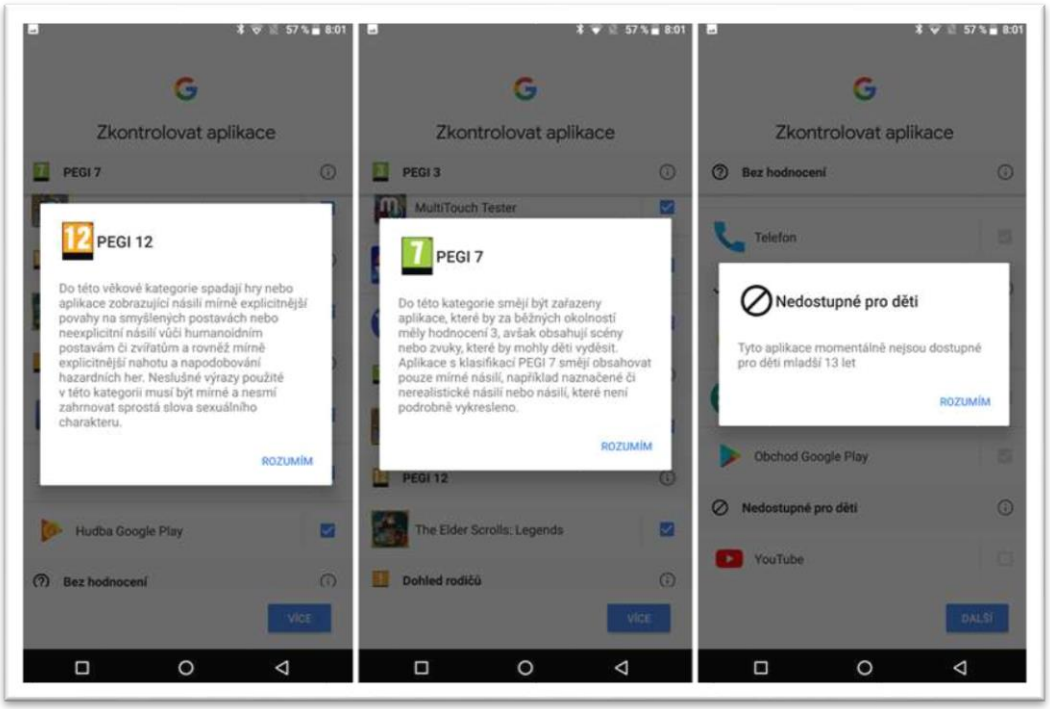
[44] Google Play – centrální úložiště aplikací dostupné po založení Google účtu z prostředí mobilního telefonu se systémem Android.

Nyní je možné stažení aplikace a prověření již nainstalovaných aplikací (obr. 16)



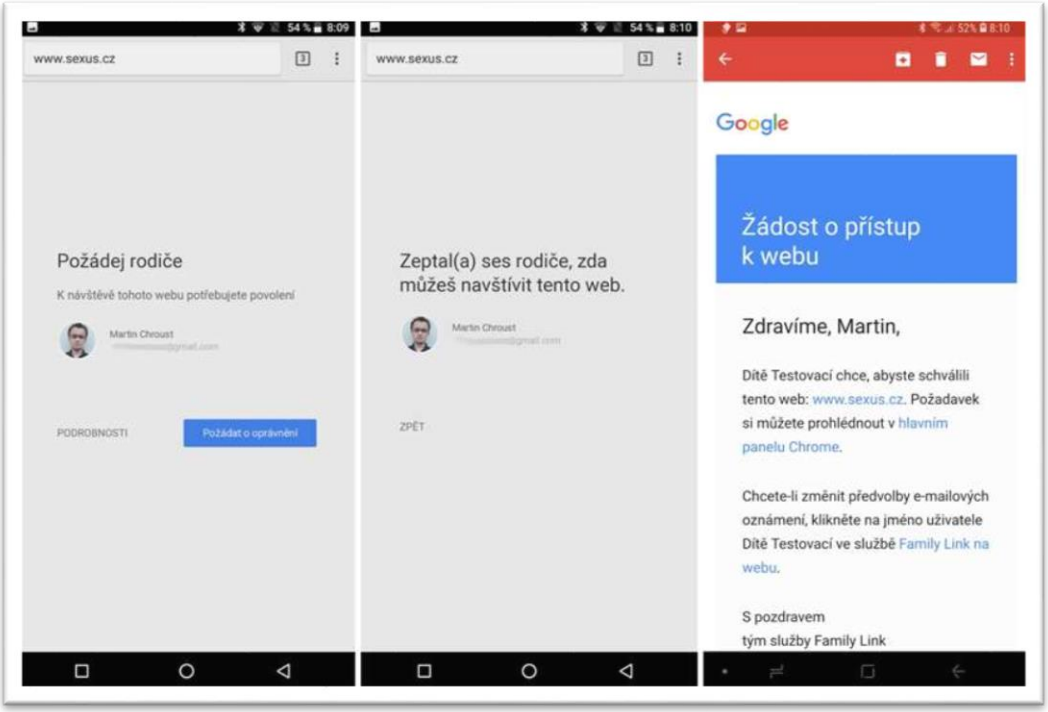
Obrázek 16-ukázka prověření aplikací na zařízení dítěte. [online] www.mobilmania.cz

Po stažení je nutno v aplikaci povolit sebe sama jako správce účtu dítěte. Automaticky je stažena aplikace Family Link Manager. Poté je možno prověřit aplikace v zařízení (obr. 17)



Obrázek 17-Prověření aplikací Google Family [online] www.mobilmania.cz

Z pohledu dítěte vypadá aplikace takto (viz. obr.18)



Obrázek 18-Google Family- zařízení dítěte [online]dostupný z www.mobilmania.cz

Dítě musí rodiče požádat o návštěvu neschválených webů nebo stažení nepovolených aplikací, pokud je to rodičem nastaveno. V případě potřeby je přístup zamítnut. Pokus o smazání účtu správce dítětem je neúspěšný bez znalosti hesla.

Aplikace také umožňuje správu přístupu k webům nastavovat/zamezovat omezení plateb. V aplikaci se dají nastavit časové úseky, kdy dítě může používat zařízení a stanovit čas „večerky“ pro jednotlivé dny v týdnu.

Další aplikace vhodné pro kontrolu a správu v zařízeních s OS Android.

I v systému Android lze pomocí služby Google Play[45] nainstalovat další aplikace, které jsou jednodušší na ovládání a zajišťují některé nástroje kontroly. Existuje velké množství těchto aplikací. Dále uvádíme několik příkladů, které jsou vybrány na základě vlastních zkušeností a také hodnocení aplikací uživateli v Google Play).

[45] Google Play. Aplikace vestavěná do OS Android

- **Kid Zone**

Aplikace se stahuje a instaluje do zařízení dítěte. Po nastavení PIN lze vybrat, které aplikace nainstalované v zařízení bude moci dítě spouštět a nastavit časový limit, po kterém se zařízení zcela odemkne a nastavit na dobu platnosti např. pozadí plochy zařízení.

- **Control - App Time Limit - Remote Lock**

Tato aplikace umí to samé, co předchozí (Kid Zone) s tím rozdílem, že zařízení dítěte lze spravovat na dálku pomocí zařízení rodiče.

3.4 UNIVERZÁLNÍ APLIKACE PRO VÍCE OPERAČNÍCH SYSTÉMŮ.

Existují i aplikace určené pro kontrolu a správu aktivit dětí na internetu, které najdeme ve verzích pro všechny hlavní operační systémy, tedy Android, iOS, Mac OS X, Windows 7, 8 a 10. Hlavní výhodou těchto aplikací je, že v rodině mohou být nasazena na zařízení s rozdílnými OS při zachování plně funkčnosti. Lze je stahovat z centrálních úložišť (App Store, Google Play a Windows Store).

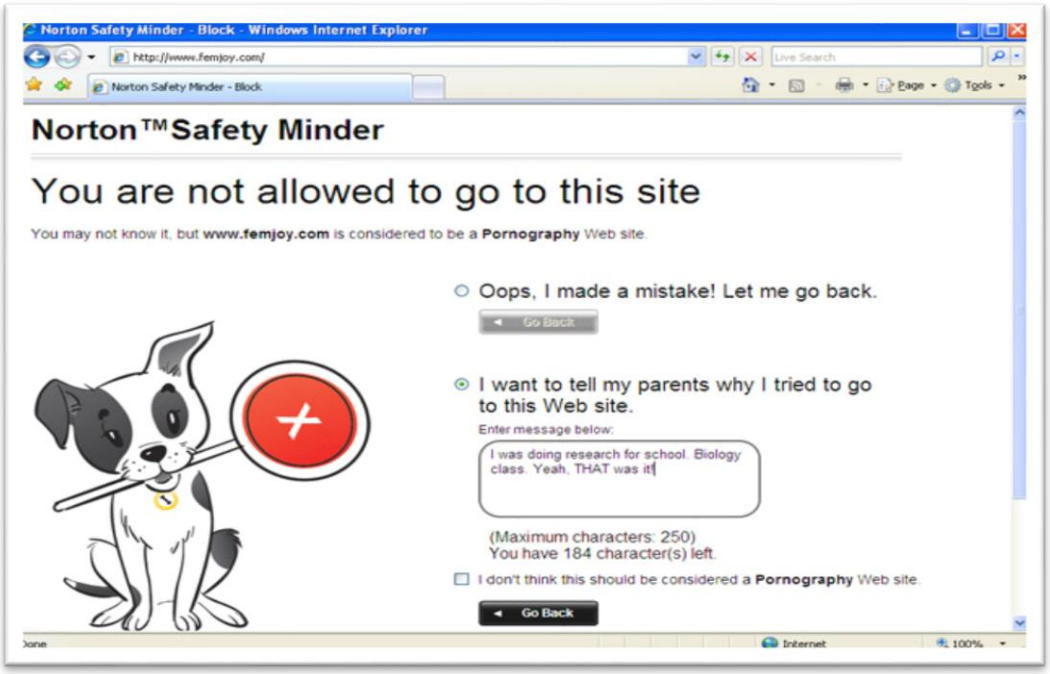
- **Norton Online Family**

Tato aplikace je univerzální a komplexně použitelná. Dokáže propojit a spravovat internetové aktivity dětí na různých zařízeních s různými operačními systémy. Funkčně je přitom podobná již dříve popsané aplikaci Google Family Link. Verze zdarma disponuje všemi funkcemi. Je však po uplynutí 30 dnů zpoplatněna s předplatným na 1 rok ve výši 520,- Kč[48]. Norton Online Family se skládá se ze dvou částí: „rodičovské“ aplikace a „dětské“ aplikace. Klientská část se nainstaluje na zařízení, mobilní telefon, tablet a přitom nezáleží, jaký operační systém využívá. Nastaví a vyberou účty uživatelů (dětí) ke sledování. Přitom dojde ke zřízení účtů na webu společnosti Symantek[49].

Aplikace pomáhá získat přehled o pohybu dětí na internetu, poslat dítěti zprávu nebo zařízení vypnout, ukončit aplikace, sledovat textovou konverzaci dítěte v aplikacích a na sociálních sítích, kontrolovat čas strávený v aplikacích a na internetu mnoho dalšího, a to i zpětně pomocí logů i v reálném čase nebo pomocí emailu, který je rodiči ve zvolených intervalech zasílán.

[48] Zdroj[online] dostupný na https://family.norton.com/web/?ULang=ces
[49] Symantek- společnost produkující bezpečnostní software.

Po patřičném nastavení rodičem, jako správcem rodiny, blokuje v prohlížečích Norton a Chrome nevhodné webové stránky (viz obr. 19)



Obrázek 19-Ukázka blokace stránky Norton. [printscreen] http://www.evbid.com/gallery/family-norton.html#photo_8

Rozdíly ve vybavenosti placené verze. (obr. 21)

Obrázek 20-Rozdíl funkcí [printscreen] http://www.evbid.com/gallery/family-norton.html#photo_12

- **Qustodio Parental Control**

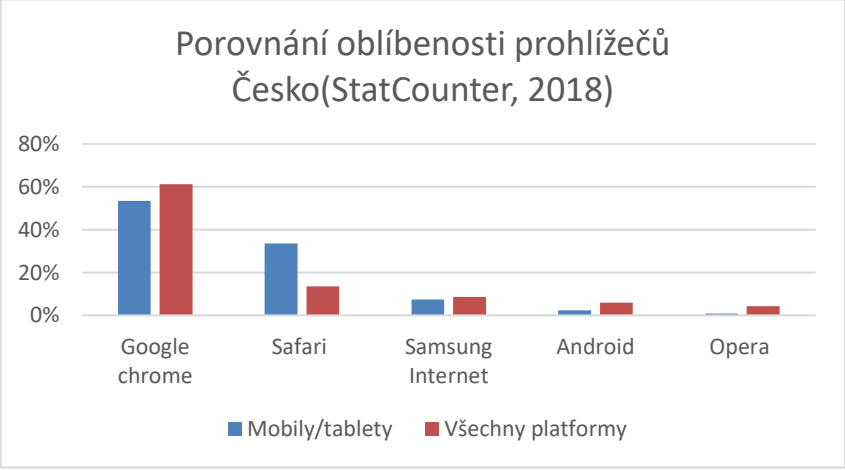
Je univerzální aplikace. Qustudio Parental Control zajišťuje pomocí inteligentních filtrů blokaci nevhodného obsahu, a to i v režimu soukromého prohlížení. Dále zajišťuje ochranu a kontrolu sběrem dat o použití zařízení, monitoring přes webové rozhraní a blokování zvolených aplikací nebo internetových stránek. Základní verze je zdarma. Placená verze je rozšířena o funkce lokalizace zařízení a sledování příchozích a odchozích hovorů a SMS. Aplikace je vhodná pro OS Windows, Android, IOS v placené verzi Premium.[54]

- **OpenDNS**

Cisco[55] FamilyShield je bezplatná služba od OpenDNS[56]. Bezplatná aplikace automaticky blokuje domény, které OpenDNS označil na základě svých informací za nevhodné. Aplikace je zdarma, vhodná pro OS Windows, Android, iOS.

3.5 Webové prohlížeče a možnosti jejich zabezpečení

Nejčastěji používanými prohlížeči webu napříč všemi platformami jsou v České republice podle měření společnosti StatCounter[57] programy Google Chrome, Mozilla Firefox, Apple Safari, Internet Explorer, Opera a Microsoft Edge. Graf oblíbenosti webových prohlížečů v ČR. (graf 1)



Graf 1 - Využívanost prohlížečů 2018 ČR (data StatCounter[online] https://www.markomu.cz/nejoblibenejsi-prohlizece/)

[54] Qustudio P. Control-Aplikace. Zdroj[online] https://www.qustodio.com/en/
[55] Cisco- Americká firma produkující síťová zařízení a bezpečnostní software.
[56] OpenDNS-služba evidující a překládající webová jména serverů.
[57] Využívanost prohlížečů 2018 Česká republika, všechny platformy OS: StatCounter Global Stats(zdroj: dostupný z https://www.markomu.cz/nejoblibenejsi-prohlizece/)

Moderní webové prohlížeče, pokud jsou dobře nastaveny, jsou schopny ochránit naše děti před dalšími nástrahami internetu.

Musíme si však uvědomit, že nastavení v určitém prohlížeči, funguje jen při procházení internetu tímto konkrétním prohlížečem. Starší děti velmi jednoduše použijí jiný prohlížeč.

Jaké možnosti z hlediska zabezpečení mají současné moderní prohlížeče si předvedeme na příkladu Google Chrome. U různých prohlížečů a operačních systémů se možnosti a způsob jejich nastavení mírně liší.

- **Prohlížeč Google Chrome**

Podle posledních statistik zastoupení webových prohlížečů[59] je tedy Google Chrome jedničkou na trhu. Svou pozici si vydobyl především díky své jednoduchosti a rychlosti. Dosahuje také dobrou bezpečnost, které je dosahováno především častými aktualizacemi, které zabezpečují napadnutelná místa. Poskytuje též pokročilou správu přístupu k jednotlivým komponentám zařízení a webu.

- **Blokování cookies**

Cookies slouží k rozlišování jednotlivých uživatelů a personifikaci jejich aktivit. Nejsou přímou bezpečnostní hrozbou pro naše zařízení. Jsou však využívány k tomu, aby sledovaly náš pohyb po internetu, naše zájmy a na základě nich personifikovaly třeba reklamu.

- **Blokování rizikového obsahu**

Pomocí různých doplňků a rozšíření jsou některé prohlížeče schopné zabránit vyhledání a zobrazení tohoto obsahu na základě vyhledávaných slov (např. „sex“, „smrt“, „násilí“ atd.).

- **Blokování reklam a vyskakovacích oken s nevhodným**

Obsahem prohlížeče umějí v základních verzích nebo s rozšířeními omezit zobrazování reklam. Dokáží zablokovat vyskakovací okna s nevhodným obsahem.

- **Blokování obrázků a videí**

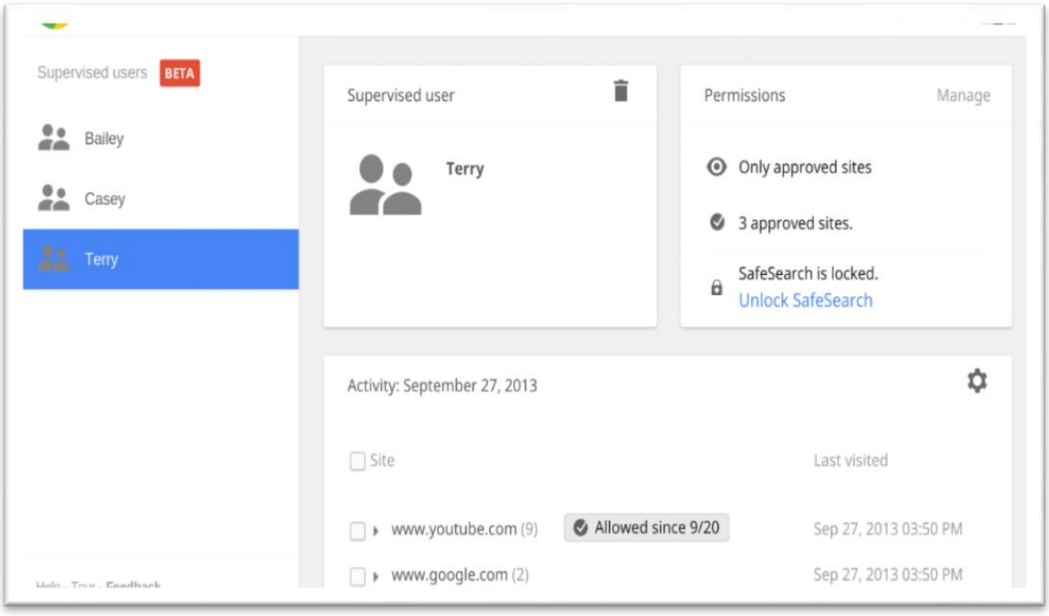
Pomocí Chrome lze blokovat obrázky a videa na zvolených stránkách nebo naopak nastavit jejich zobrazení pouze na určitých stránkách.

[59] Využívanost prohlížečů 2018 Česká republika všechny platformy OS (zdroj: StatCounter [online]dostupný z https://www.markomu.cz/nejoblibenejsi-prohlizece/)

- **Blokování webů a domén**

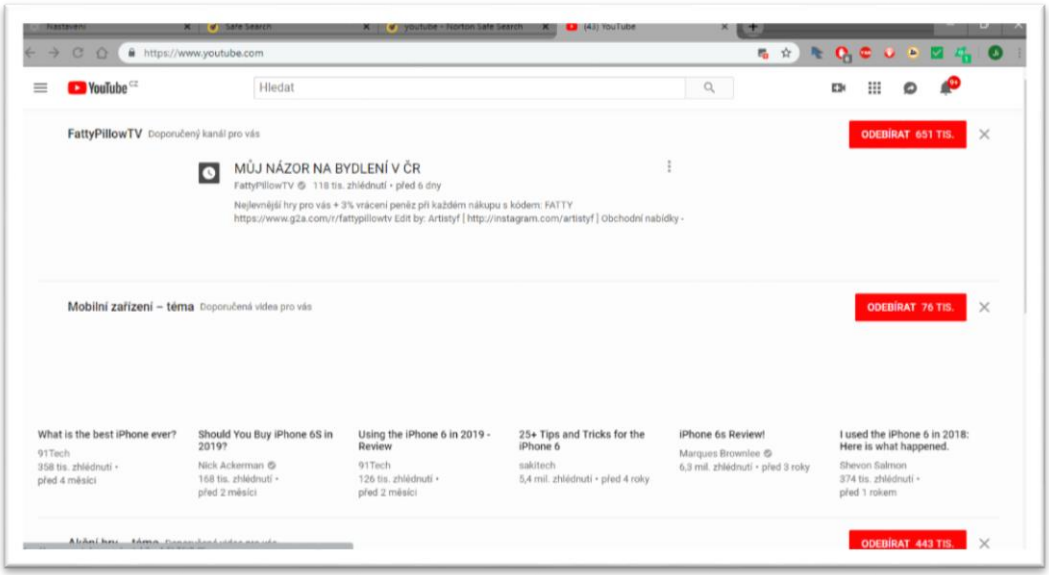
Uživatel (rodič) může povolit nebo blokovat určité weby nebo domény.

Tato nastavení lze provádět odlišně pro různé děti, kterým se však musí zřídit Google účet a zajistit, aby používaly Chrome přihlášení. (viz. obr 21).



Obrázek21- Google chrome. [online] https://antyweb.pl

Stránka YouTube a všechny ostatní stránky po zablokování videa (obr. 23)



Obrázek 22 - Google Chrome, [printscreen] https://www.youtube.com/

Kromě funkcí obsažených v základní verzi nabízí Google Chrome ve všech OS možnost rozšíření funkčnosti pomocí svého Internetového obchodu.[60]

Doporučená rozšíření pro Google Chrome:

- **AdBlock**

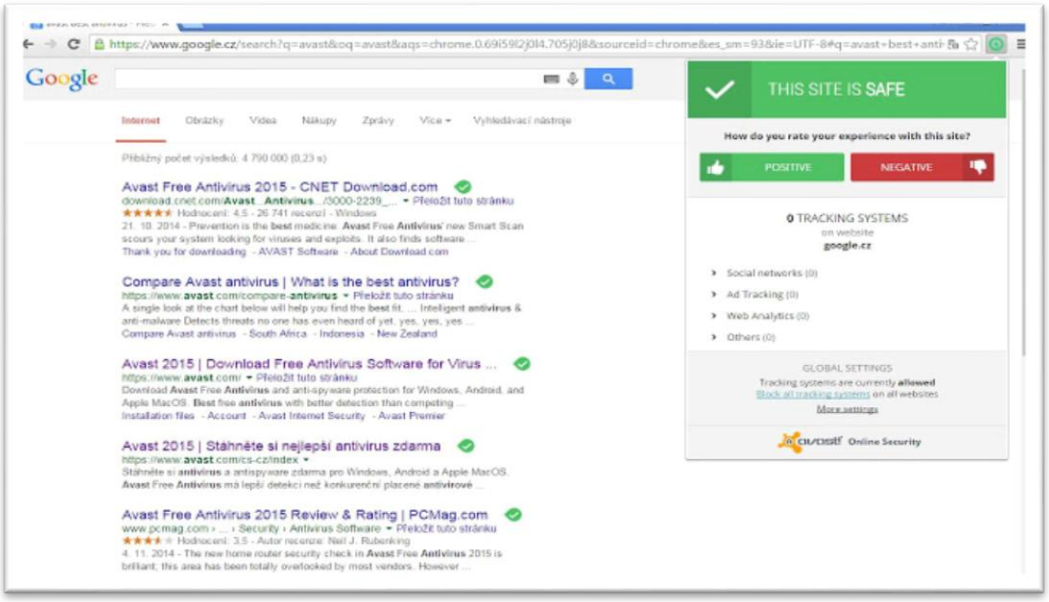
Blokuje nechtěnou reklamu a vyskakovací okna.

- **Personal Blocklist**

Pomocí tohoto rozšíření lze blokovat nechtěné stránky servery nebo celé domény.

- **Avast Online Security**

Sleduje reputaci webů, označuje stránky jako bezpečné nebo nebezpečné ještě před tím, než na ně uživatel vstoupí. Varuje také před phishingovými stránkami.(obr. 23)



Obrázek 23 – Hodnocení stránek Avast Online Security [printscreen] https://chrome.google.com/webstore/detail/avast-online-security/gomekmidlodglbbmalcneegieacbdmki?hl=cs

- **Norton Safe Search**

Toto rozšíření podobně jako Avast Online Security vyhodnocuje bezpečnost stránek při vyhledávání. Při hledání určitého výrazu jsou vyhledané možnosti označené symboly, zda

[60] Internetový obchod Chrome obsahuje aplikace“rozšíření“ prohlížeče Google Chrome[online] dostupný na https://chrome.google.com/webstore/category/extensions?hl=cs

jsou bezpečné či nikoli. Lze také nastavit nebo blokovat přístup k určitým webům. (po instalaci je nutno nastavit NSS jako výchozího vyhledávacího agenta)..

- **Norton Family**

Toto rozšíření je zjednodušenou verzí aplikace Northon Online Family, které se budeme věnovat v kapitole „Kontrola a správa dětských aktivit na internetu“.

- **Prohlížeč Mozilla Firefox**

Firefox je další alternativou prohlížeče Chrome. Disponuje podobnými funkcemi. Firefox se vyznačuje rychlostí i podobnými funkcemi jako Google Chrome. Disponuje také možnostmi rozšíření a nastavením zabezpečení, podporuje synchronizaci mezi zařízeními, ve kterých používáte stejný účet

- **Prohlížeč Microsoft Edge**

Prohlížeč Microsoft Edge je poměrně nový produkt společnosti Microsoft, založený na jádře Chrome a integrovaný do systému Windows 10. V současné době disponuje několika rozšířeními.

- **Prohlížeč Opera**

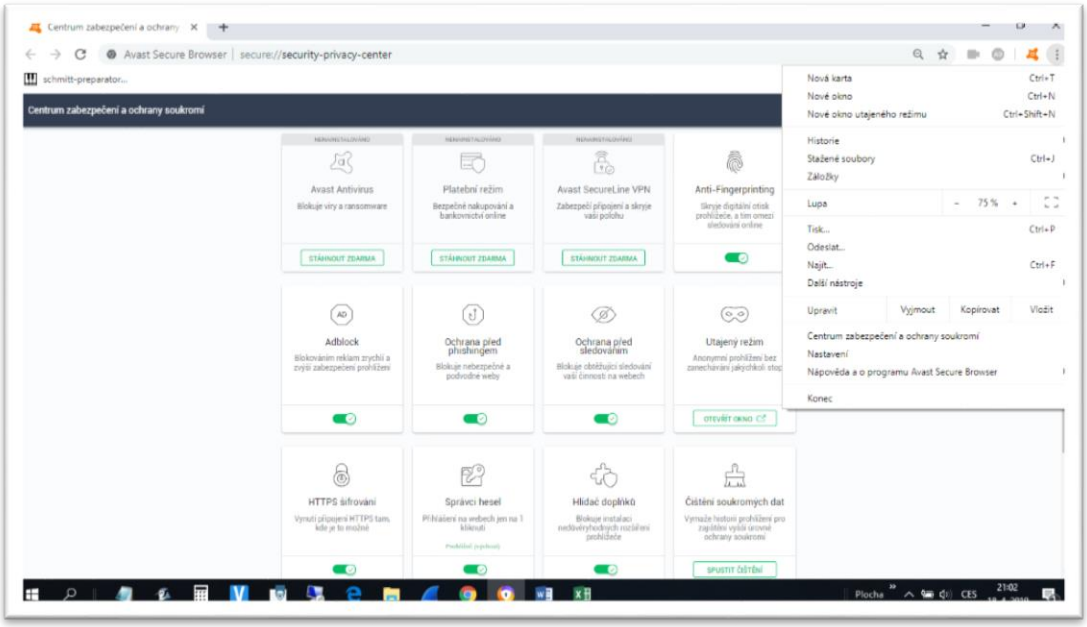
Prohlížeč Opera disponuje funkcemi jako je blokování reklamy, K dispozici je zhruba tisícovka rozšíření.

- **Avast Secure Browser**

Antivirová společnost Avast[61]. Je postaven na základech prohlížeče Google Chrome a doplněn o některé bezpečnostní funkce jako je „Platební režim“, který ochraňuje internetové bankovnictví a nákupů pomocí karet, ochrana soukromí, zabránění sledování a dokonce ochrana proti malwaru, phishingovým podvodům a krádeži identity. Obsahuje modul pro blokování reklamy.

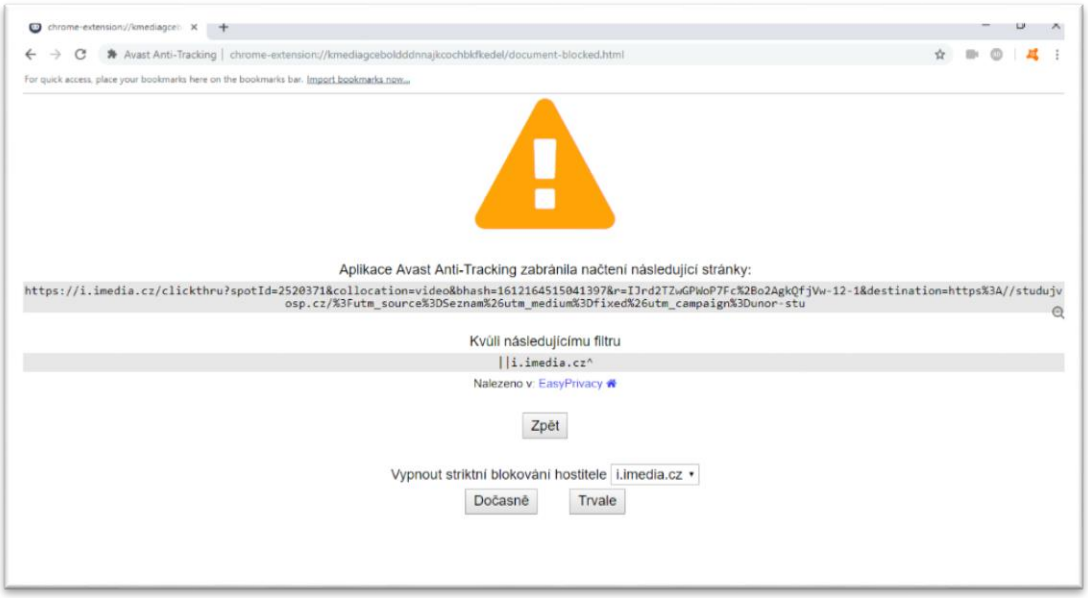
[61] Avast. Česká společnost produkující bezpečnostní aplikace např. antiviry zdroj[online] www.avast.com.

Oproti Chromu je nastavení r. Avast uživatelsky jednodušší pomocí “Centra zabezpečení a ochrany“. (obr. 24)



Obrázek 24 - Centrum zabezpečení a ochrany prohlížeče Avast Secure Browser, [printscreen]

Také dokáže chránit před malware, phishingovými podvody a krádeží identity (obr. 25)



Obrázek 25 - Funkce Anti-tracking, [printscreen] Avast Secure Browser

- **Safari**

je webový prohlížeč vyvinutý společností Apple Inc., který je součástí OS iOS a MacOS. Disponuje rychlým vyhledáváním a možnostmi integrace různých rozšíření a doplňků podobně jako Google Chrom. V současné době je ve verzích pro všechny OS.

- **Prohlížeč Seznam.cz**

Bohužel, zatím není pro naše účely ideální, protože je též vybaven funkcí, která brání v případě navštívení stránek s rizikovým obsahem (např. se sexuální tematikou) uložení do historie procházení.

3.6 Řízení přístupu dětí k internetu pomocí domácího routeru

Zařízení jako je router je schopné ovlivnit pouze zařízení připojená na něj ve stejné síti (bezdrátové nebo pomocí síťového kabelu). Pomocí routeru lze tedy spravovat nastavení u nepřenosných zařízení, tabletů a mobilních připojení bez jiného připojení k internetu (např. pomocí datového tarifu mobilních operátorů). V případě jiného přístupu na internet je nutno použít nastavení jiná nebo kombinaci.

Řízení a kontrola přístupu dětí na internet pomocí routeru ve wi-fi síti je poměrně spolehlivá. Veškerá omezení totiž nastavíme na zaheslovaném domácím routeru, kam dítě nemá přístup. Veškerá omezení jsou aplikována routerem na zařízení dítěte, které určíme, přičemž identifikaci router provádí na základě jedinečné MAC adresy toho konkrétního zařízení. Tuto adresu nemusíme nijak složitě nastavovat, je již od výrobce do každého zařízení vložena a zobrazuje se na routeru mezi připojenými „klienty“. Pomocí této MAC adresy (aniž o tom ví), žádá klient (zařízení) od routeru povolení k přístupu na internet.

Jakou úroveň takovéto ochrany dokážeme nastavit, záleží na našich znalostech, typu routeru a softwaru, který do něj výrobce nainstaloval.

Na každý moderní domácí router se lze podívat přes webové rozhraní a to z jakéhokoli prohlížeče na jakémkoliv zařízení, tedy PC, mobilním telefonu, tabletu, pokud se nachází ve stejné (např. domácí) síti jako router. Také je již k dispozici několik aplikací, které si lze nainstalovat např. na mobilní telefon a tímto způsobem svůj router spravovat. V případě zájmu využijte služby AppStore nebo Google Play.

Jednou z nevýhod tohoto řešení je tedy nemožnost správy běžného, domácího routeru „odkudkoliv“ bez přidělené veřejné adresy. O tuto je potřeba v případě nutnosti spravovat svůj router z jiné sítě než své domácí požádat svého operátora připojení k internetu. Router totiž v základním nastavení dostal tzv. „neveřejnou“ IP adresu, která může být stejná, jako IP adresa tisíců dalších routerů. Další nevýhodou je, že jakkoliv moderní router nedokáže zabránit spouštění již instalovaných aplikací na zařízení dítěte.

Vybavenost funkcemi rodičovské kontroly se dle mého osobního zjištění a porovnávání parametrů moderních, v současnosti nabízených routerů různých cenových kategorií, k mému překvapení neliší, tak abychom nějakým dražším (domácím) routerem mohli nahradit aplikace „Rodičovské kontroly“ softwarovými prostředky. Z dostupných zdrojů například nebylo zjištěno, že by v současné době existovaly dostupné routery, které by dokázaly povolit stahování jen určitých aplikací z nějakého webu např. podle normy PEGI.

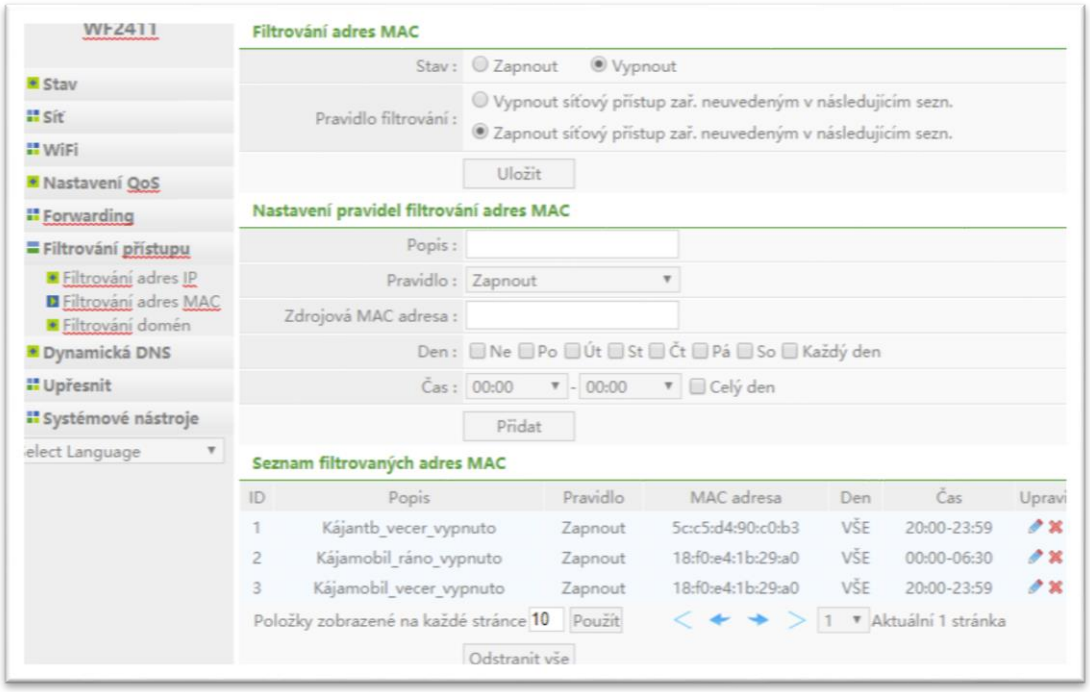
Na příkladu levného domácího routeru **NETIS WF2411** (současná cena 288 Kč[62] na Alza.cz[63]), zapojeného např. v mé domácí síti si můžeme přiblížit možnosti nastavení rodičovské kontroly.

Obrázek 26- Levný domácí router Netis WF2411

K přihlášení budeme potřebovat jen heslo a IP adresu routeru, které získáme z dokumentační příručky, kterou obsahuje balení routeru při jeho koupi. IP adresu většinou

[62] Alza.cz – nabídková cena ze dne 19.4.2019. Zdroj[online] https://www.alza.cz/netis-wf2411.../
[63] Alza.cz – internetový obchod[online]dostupný na www.Alza.cz

výrobce nastavuje na hodnoty 192.168.0.1 nebo 192.168.1.1 u. větších síti např. na 10.0.0.XX. Tuto IP adresu napíšeme do adresního řádku nějakého prohlížeče. Po otevření úvodní stránky routeru vyplníme heslo a dostaneme se do prostředí, kde lze nastavit vše potřebné pro vybraná zařízení (obr. 27)



Obrázek 27- Ukázka nastavení pro 2 zařízení [printscreen] Netis WF2411

Testovaný router NETIS, zapojený v mé domácí síti disponuje nastavením časového plánu, kdy je možné omezit nebo povolit připojení jednotlivých zařízení v domácnosti k internetu pomocí jejich jedinečné MAC adresy. Přitom nezáleží na platformách nebo operačních systémech zařízení.

Na tomto routeru lze také nastavit blokování domén, které chceme zakázat dítěti navštívit (např. omezit všechny domény, kromě .edu a .gov, na kterých se nachází mnoho studijních i jinak důležitých materiálů a informací). V praxi však toto asi nebude přijato s přílišnou radostí.

V případě nutnosti lze na většině v současnosti nabízených routerů (i na našem levném Netis WF2411) nastavit, tzv. QoS[64]. Tímto způsobem lze omezit určitému zařízení šířku pásma nebo přidělit různou šířku různým zařízením v síti. Udává se většinou v procentech.

[64] Quality of Service – Zdroj[online]www.it-slovnik.cz

Těmto zařízením pak router přiděluje data maximálně v určené šířce pásma a od toho se odvíjí rychlost sítě pro to konkrétní zařízení. V praxi to znamená, že všechna zařízení mají rychlost příjmu stejnou, dokud některé z nich nepřijímá taková data, jejichž datový tok přesáhne jemu určenou šířku pásma. Potom se již data v potřebné rychlosti nestačí přenášet. Pak toto zařízení nemůže data (např. video, stahování her) v uspokojivé rychlosti nebo kvalitě přijímat. Tedy škodolibí rodiče mohou omezit stahování her a videa dítěti a zvýšit šířku pásma např. pro svůj notebook nebo Smart TV.

Existují však i routery, které nabízejí praktičtější možnosti nastavení kontroly. Například lze zabránit výsledkům vyhledávání určitých slov, blokovat jen konkrétní weby nebo se spolehnout na blokování již známých stránek vybraných poskytovatelem, producentem routeru nebo jiných služeb, které na základě svých dlouhodobých pozorování označil za nevhodné pro děti. Je také možno vytvářet a sledovat statistiky provozu jednotlivých zařízení nebo přidělovat denní časovou kvótu pro připojení určitého zařízení (v tomto případě se nejedná o pevný časový úsek, ale součet časů kdykoliv za den).

Také mohou posílat e-mailové notifikace nebo umožnit online schválení/odmítnutí požadavku zaslaného dítětem na zobrazení určitého webu.

Příklady takových zařízení mohou být routery **Netgear 6400 100-PS (obr. 29)** (cena 2598 Kč[65], Mall.cz) nebo **Synology RT2600ac** (cena zhruba 6002 Kč[66], Alza.cz). Tyto routery jsou cenově náročnější především z důvodu jiných funkcionalit, ale rodičovská ochrana je u nich na výborné úrovni (snad kromě již zmíněné funkce přístupu k aplikacím podle normy PEGI).

Obrázek 28- Router Netgear 6400 PS-100

[65] Mall.cz – nabídka ze dne 19. 4. 2019. Zdroj [online] www.mall.cz
[66] Alza.cz – akční nabídka ze dne 19. 4. 2019. Zdroj [online] www.alza.cz

Například router Synology RT2600ac se dá navíc ovládat pomocí aplikace DSRouter, kterou lze na zařízeních vybavených systémy Android a iOS spravovat rodičovská nastavení odkudkoliv. Aplikace je ke stažení na centrálních úložištích App Store a Google Play.

4 DOPORUČENÍ PRO NASTAVENÍ DOMÁCÍCH PRAVIDEL POUŽÍVÁNÍ INTERNETU

Tato kapitola byla sestavena pomocí informací získaných z níže uvedených webů a z vlastních poznatků z praxe. Má praxe vyplývá z mého profesního zaměření, při němž se velmi často setkávám s problémy dětí vyplývajících z komunikace na internetu. Taktéž se profesně setkávám s požadavky na zabezpečení zařízení proti neoprávněným průnikům a zneužití.

4.1 DOPORUČENÍ PRO RODIČE

Rodičům lze doporučit tato základní pravidla pro bezproblémový přístup dětí na internet, jejich správný rozvoj a plnohodnotné soužití celé rodiny:

- **Seznamte se s případy internetové kriminality, které mohou ohrožovat vaše dítě.**

Například na stránkách https://www.stream.cz/porady/seznam-se-bezpecne, které provozuje společnost Seznam.cz[67] nebo na zde uvedených serverech.

- **Zabezpečte zařízení (Mobilní zařízení i počítač).**

Tento krok je zcela nezbytný. Tak jako u dospělých, je i zařízení, tablet nebo mobilní telefon dětí napadnutelný. Jak jsme si popsali v předešlé kapitole, existuje více forem hrozeb v této oblasti. Proto je potřeba, aby všechna zařízení, nejen zařízení, ale i tablety a mobilní telefony byly vybaveny firewallem a zabudovaným nebo externím antivirovým programem.

- **Komunikujte s dítětem o nástrahách na internetu**

Děti zejména v mladším věku vnímají internet jako přirozenou součást svého života. Informace, které z něj čerpají, ať už v jakékoliv formě přebírají bez vysvětlení značně nekriticky. Proto je velmi důležité dětem vysvětlovat, které věci jsou správné a které jsou špatné, nepravdivé nebo závadné, co dělat můžou a co raději ne.

- **Zúčastňujte se dětských internetových aktivit a nechte ho zůčastňovat vašich**

Nejlepším místem pro umístění počítače nebo mobilních zařízení při dětských aktivitách na internetu je společný prostor, kde můžete do jisté míry kontrolovat, co dítě na internetu dělá, ale hlavně, což je velmi důležité - komunikovat. Mluvit s dítětem o těchto aktivitách,

[67] Seznam.cz – společnost poskytujícíinformace prostřednictvím svého webu a přidruženým službám. Zdroj[online] https://www.seznam.cz

informacích, které zde nalézá. Vysvětlovat. V případě nutnosti také můžete ihned reagovat na případný rizikový obsah. Dítě se tím učí, co je standardní, nezávadné, pravdivé a naopak. Přejímá prostě vzorce chování z reálného světa a učí se je uplatňovat na ten internetový.

- **Budujte důvěru a komunikujte s dítětem o jeho aktivitách na internetu**

Děti se začínají po internetu pohybovat již ve velice raném, předškolním věku. Takže čím dříve pochopí, že internet není jen studnicí zábavy a moudrosti, ale že je třeba se zde chovat obezřetně tak, jako ve skutečném životě, tím lépe. Musíme však přizpůsobit svůj výklad věku a schopnostem dítěte. Není potřeba přehnaně strašit, ale je potřeba vysvětlovat. Vysvětlete dítěti, že na internetu není "úplně" vše dobré a snažte se, aby sdílelo Váš názor. Pokud nemáte čas, snažte se alespoň sdílet jeho dojmy a pocity z internetu. Sdílejte s dítětem jeho zážitky, co na internetu dělalo a zajímavého vidělo a zaujměte k tomu stanovisko. Podvědomě dítě Vaše rozumná stanoviska přejímá.

- **Ne každý kdo se tváří jako kamarád, je kamarád!**

Internet je do jisté míry médium anonymní. Kdo chce, uvede své pravé jméno, ale kdo nechce, zůstává skryt za přezdívkou/nickem. Je potřeba dítěti vysvětlit, že ke kontaktům, které má na internetu je dobré přistupovat s rezervou (obezřetností). Je velmi jednoduché lhát a přetvařovat se, pokud je člověk anonymní.

- **Nesdělujte dítěti svá hesla, čísla bankovních karet a další citlivé údaje**

Nejde zde o to, že by je dítě vědomě zneužilo (také se to samozřejmě stává), ale najde se mnoho způsobů, jak mohou být někým zneužity. Dávejte pozor, aby čísla karet, která jste zadali do zařízení v dobré víře při platbě v době, kdy bylo dítě přihlášeno (nebo samozřejmě i Vy) nebyla uložena. Je mnoho nákupních a především herních serverů, které mají tuto možnost u plateb přednastavenou. Je využívána k pozdějším opakovaným platbám a je tudíž pro dítě jednoduché (mnohdy i nevědomě) uskutečnit další nákup.

- **Zablokujte vyskakovací okna a zbytečnou reklamu**

Pomocí rozšíření (plug-ins) prohlížečů, lze omezit reklamu s nevhodným nebo nelegálním obsahem, ale při určitém nastavení i většinu reklamy legální.

- **Využijte nebo nainstalujte některý z nástrojů kontroly a správy aktivit**

Zejména u dětí mladšího věku, by tato funkčnost měla být podmínkou vstupu dítěte na internet. Kontrolujte jeho aktivity a řiďte čas, který stráví aktivně nebo „jen“ připojeno na internetu. Dbejte na včasné večerní ukončení aktivit, aby dítě mohlo kvalitně usínat a spát.

Mezi těmito aplikacemi najdeme i takové, které dokáží skrytě monitorovat jakoukoliv činnost dítěte na zařízení, jako jsou stisky kláves, zaznamenávání adres stránek, které dítě navštívilo a čas, po který se na nich zdrželo. S kým a jaké si píše emaily a vzkazy na sociálních sítích, ukládá prohlédnuté fotografie. Tyto informace může odesílat na předem zvolenou e-mailovou adresu. Je na zvážení každého rodiče, zejména u starších dětí (adolescentů), zda toto považuje za etické. Tyto aplikace mohou být použity například až v okamžiku, kdy mají signály, že jejich dítě se stalo obětí závažného útoku. Potom je důležité shromažďovat tato data, případně je předat orgánům činným v trestním řízení, kde mohou být využity pro vysledování pachatele nebo jeho usvědčení.

- **Nenechávejte dítě zařízení "na pospas"**

V mladším věku se dětský mozek teprve utváří a je mnohem větší riziko, že se utvoří závislost, která přetrvává. Pokud s touto závislostí nezačneme bojovat, bude narůstat. Dítě začne mnohdy při špatném vedení internet považovat za svého nejlepšího kamaráda a jedinou možnost seberealizace. Je neskutečně těžké později mu to odpírat. Je nutné udržet jeho zdravý nadhled, udržet převahu jeho zájmů ve skutečném životě nad tím internetovým.

- **Zamezte vzniku depresí nebo úzkostných poruch**

Bohužel, během dlouhé doby, kdy nevěnujeme pozornost náznakům blížící se katastrofy nebo někdy během vteřiny, se ideály mění na zlé sny. Uvědomme si, že dětský mozek, zejména v předškolním věku nemá takové zkušenosti jako náš. Nedokáže mnohdy rozlišit váhu, pravdivost nebo nadsázku informací. Představte si, jak dítě vnímá například velmi známé "zpravodajské" stránky kde je převážná část "informací o společnosti" předkládáno neetickým a negativním způsobem. Pokud se dítěti po této stránce nevěnujeme, může se stát), že dítě skrze internet získá negativní náhled na svět. Mnohdy se u citlivějších dětí jedná o tak výraznou infiltraci, že se mohou rozvinout úzkostné poruchy. S těmito poruchami (pokud je vůbec dítě přizná nebo jsou odhaleny!) je třeba pracovat. Nejprve v

rodinném prostředí, mnohdy však i za pomoci psychologa nebo psychiatra. K těmto stavům nemusí dojít při správné prevenci, vhodné komunikaci a pomocí zde uvedených nástrojů.

4.2 Odkud čerpat další informace

Touto problematikou se zabývá v ČR velice podrobně několik serverů, na kterých se mohou rodiče seznámit s problematikou:

- www.e-bezpeci.cz
- www.internetembezpecne.cz
- www.bezpecnyinternet.cz
- www.vimkamklikam.cz
- www.internetprovsechny.cz
- www.ditekrize.cz

Návody, jak chránit dítě na internetu vydávají i provozovatelé internetových připojení a jejich koordinátoři projektů bezpečnosti. Například zde je odkaz na dokument společnosti UPS[68], která je jedním z největších poskytovatelů internetového (i TV) připojení do domácností:

https://www.upc.cz/pdf/pece-o-zakazniky/navody/internet/bezpecny_internet.pdf

4.3 Kam se obrátit o pomoc?

S mladými „domorodci“ na síti se projevuje určitý sklon páchat přestupky a trestné činy pomocí kybernetických prostředků, tedy pomocí internetu.

V současné době existuje několik možností pro rodiče, kam se obrátit v případě nouze, při podezření na jakékoliv pronásledování nebo zneužívání svého dítěte prostřednictvím internetu nebo napadení zařízení.

[68] UPC – Člen skupiny Liberty Global, největšího světového poskytovatele kabelového připojení k internetu. Zdroj[online] www.upc.cz

- **Dětské krizové centrum[71]**

Tato linka pomoci se specializuje na problematiku zneužívání informačních technologií, internetu, počítačů a mobilních zařízení ve vztahu především k dětem.

Poskytuje pomoc při ohrožení dětí nebo dospívajících kyberšikanou, groomingem, stalkingem a dalšími negativními dopady kyberprostoru, které mohou ovlivňovat jejich vývoj i ve formě trvalých následků. Pomoc si mohou vyžádat i rodiče, dospělí a senioři, kteří se setkali s nebezpečím při využívání informačních technologií.

Problém nebo dotaz lze na linku zaslat prostřednictvím formuláře na stránkách centra na internetové adrese: http://www.ditekrize.cz/, kde lze získat i další kontakty.

- **Stop online**

Tato linka se specializuje na příjem a řešení podezření na nezákonný obsah na internetu, například šíření pornografie, zneužívání dětí, ohrožení kybergroomingem a dalšími negativními jevy.
Problém nebo dotaz lze na linku zaslat prostřednictvím formuláře na stránkách centra na internetové adrese: https://www.stoponline.cz/stoponline/, kde lze získat i další kontakty.

- **Poradna e-bezpečí**

Poradna je provozována Centrem prevence rizikové virtuální komunikace PdF UP v Olomouci (2008-2019). Pomáhá dětem a rodičům, kteří se dostali do obtížné životní situace spojené s internetem či mobilními telefony. Vyhrožování, vydírání, zastrašování za pomoci internetu či mobilního telefonu.

Nahlásit problém nebo položit dotaz lze prostřednictvím formuláře na stránkách poradny na internetové adrese: https://poradna.e-bezpeci.cz/. Do formuláře lze vložit i přílohu (soubor, obrázek, video apod.) Poradna neposkytuje telefonické konzultace, ale jsou zde uvedeny tel. kontakty na Linku bezpečí (116111).

- **Poradna projektu bezpečný internet.cz**

Tato poradna je současně i místem, na kterém lze položit anonymní dotaz nebo nahlásit problém prostřednictvím formuláře. Současně však obsahuje kontakty, na které se může klient obrátit pro rychlejší nahlášení problému podle jeho typu.

[71] DKC – Dětské krizové centrum. Nestátní organizace.

Dále disponuje databází již položených dotazů a jejich doporučená řešení.

Kontaktovat poradnu lze ze stránkys adresou:
http://www.bezpecnyinternet.cz/poradna/default.aspx

- **Linka bezpečí**

Linka pro rodiče, děti a mládež v krizových životních situacích. Linka přijímá i dotazy a problémy související s internetovými hrozbami.

Linka funguje nonstop a bezplatně na čísle **116 111**. Nahlásit problém nebo položit dotaz lze prostřednictvím formuláře nebo chatu na stránkách poradny na internetové adrese: https://www.linkabezpeci.cz/sluzby/napis-nam/

- **CZIRT**

Toto centrum se specializuje na odhalování a řešení útoků na zabezpečení zařízení a sítí, např. spam, virus, scanning, DDOS, hacking, phishing, pharming nebo porušení autorských práv. Informace a nahlášení problému lze získat na adrese:
https://www.csirt.cz/page/2632/kdy-nas-kontaktovat/

5 WEBOVÉ STRÁNKY PRO RODIČE

Pro lepší orientaci rodičů v problematice ochrany a kontroly dětí na internetu jsem k tomuto tématu vytvořil jednoduché webové stránky. Webové jsou dosažitelné na internetové adrese https://juraba.wixsite.com/mysite. Webové stránky jsou vytvořeny webovém editoru Wix.com[72]. Cílem je zvýšit informovanost rodičů o rizicích internetu s použitím výrazného formátování a nabídnout jim informace možnostech, jak chránit a kontrolovat své děti při internetových aktivitách. Součástí webu jsou i stránky se seznamem linek pomoci a odkazy na ně.

Informace jsou prezentovány tak, aby čtenáři maximálně usnadnilya urychlily jejich čtení. Aby ho dokázaly upoutat a navést na profesionální weby s touto problematikou.

- **Struktura webu:**

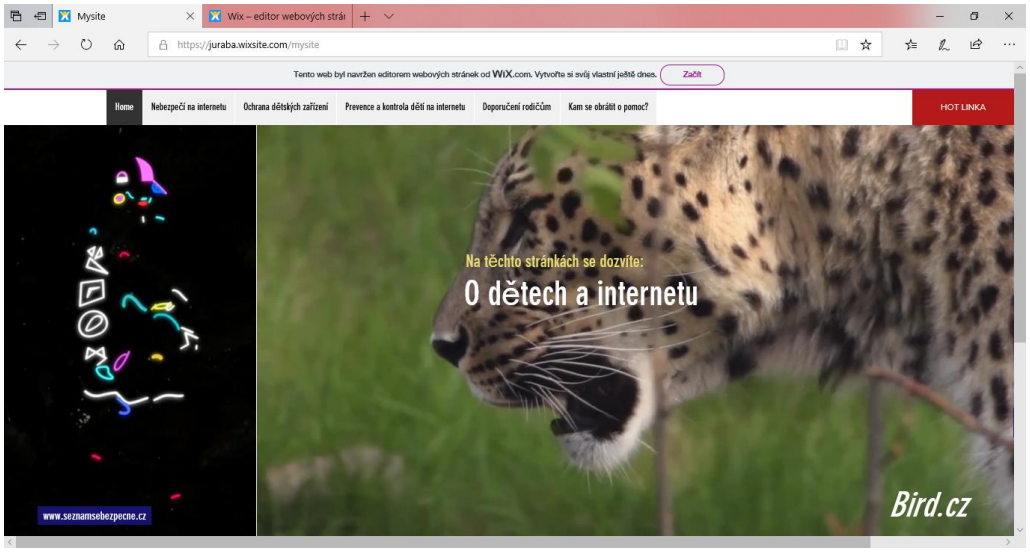
Struktura webových stránek odpovídá struktuře této práce.

- Úvodní stránka
  - Nebezpečí na internetu
    - Jak děti vidí internet
    - Jak se děti připojují
  - Ochrana dětských zařízení
    - Základní prvky ochrany OS
    - Ochrana v OS Windows
    - Ochrana v OS IOS a Android
  - Prevence a kontrola dětí
    - Kontrola v OS Windows
    - Kontrola v OS iOS
    - Kontrola v oS Android
    - Kontrola pomocí domácích routerů

[72] Wix.co – editor webových stránek [online] https://cs.wix.com/

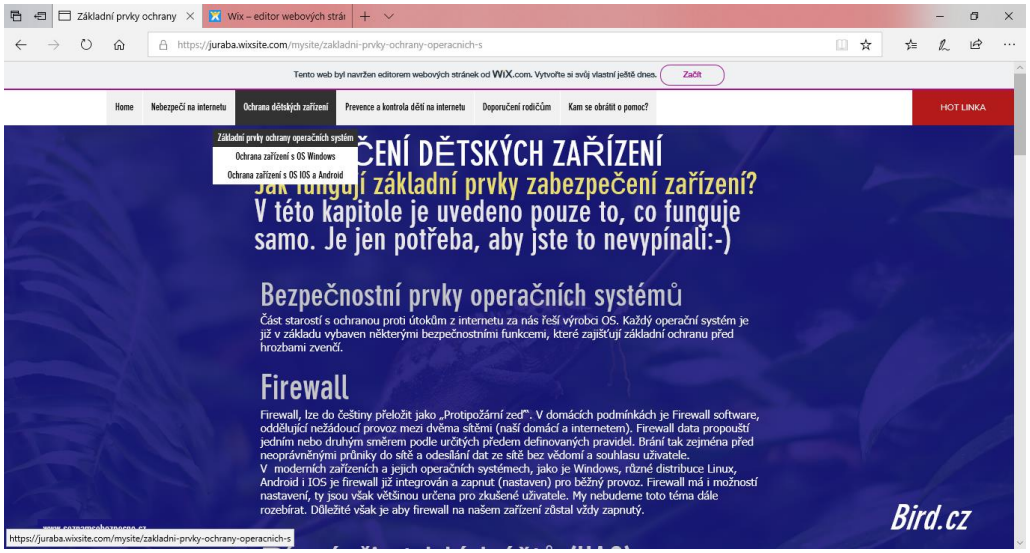
- Dporučení pro rodiče
- Kam se obrátit o pomoc
    - Linky oznamovací a poradenské
    - Seznam webů s touto problematikou a odkazy na ně

Na ukázce je úvodní stránka webu s odkazy na další podstránky (obr. 29).



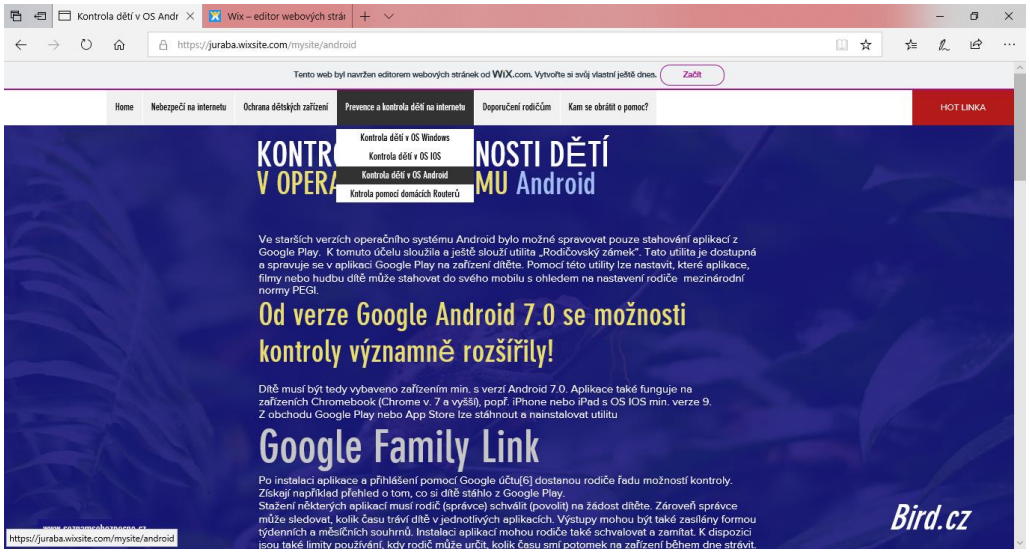
Obrázek 29 – Úvodní stránka webu Zdroj: https://juraba.wixsite.com/mysite

Jedna z dalších podstránek s názvem „Ochrana dětských zařízení“ (obr. 31)



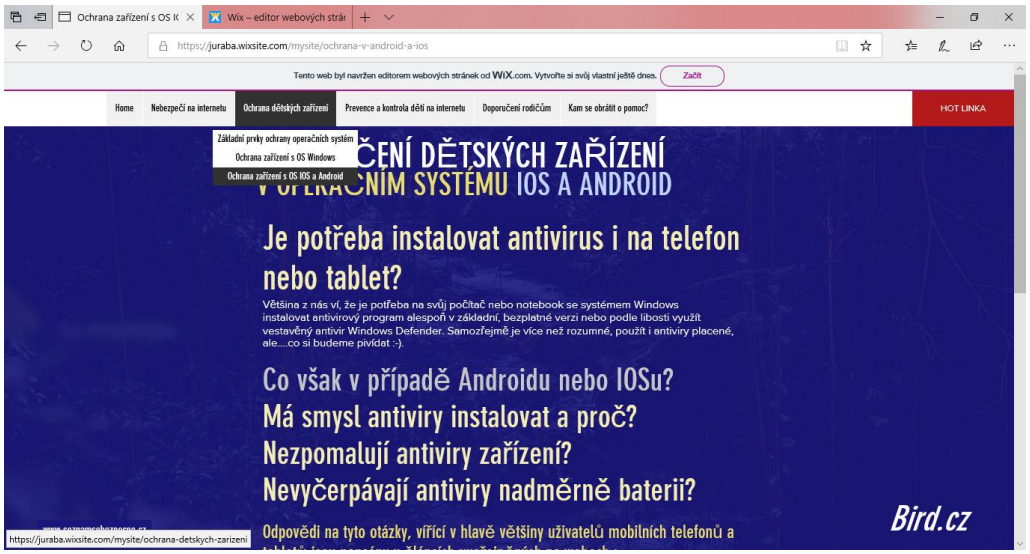
Obrázek 31-Podstránka webu „Ochrana zařízení“[prentscreen] https://juraba.wixsite.com/mysite

Na dalším printscreenu je ukázka podstránky webu „Kontrola dětí v OS Android“(obr. 32)



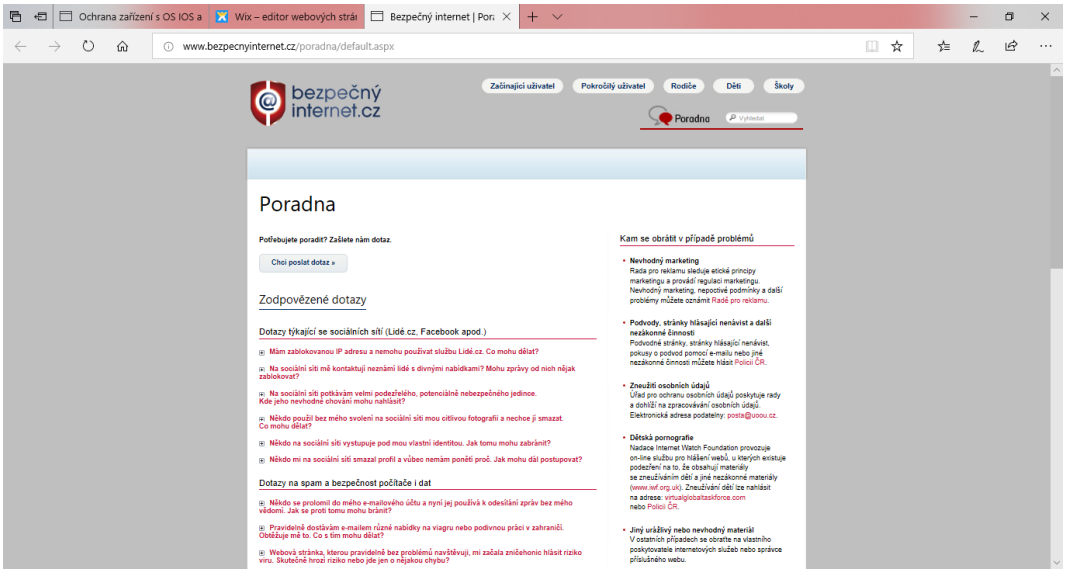
Obrázek 32 - Podstránka „Kontrola dětí v OS Android“ [prentscreen] https://juraba.wixsite.com/mysite

Zde je ukázka podstránky webu „Ochrana zařízení s OS Android“(obr. 33)



Obrázek 33- Podstránka „Ochrana zařízení v systému iOS a Android“ [prentscreen] https://juraba.wixsite.com/mysite

Zde je ukázka cíle odkazu“Poradna“(obr. 34)



Obrázek 34 - Ukázka cíle odkazu „Linky pomoci“ [prentscreen] http://www.bezpecnyinternet.cz/poradna/default.aspx

ZÁVĚR

Tato práce byla zpracována na téma „Možnosti rodičovské kontroly bezpečnosti dětí na internetu“.

Téma ochrany a kontroly bezpečnosti dětí je nutno nahlížet z různých hledisek. Hlediska technického zabezpečení zařízení dětí, psychologických dopadů Internetu na děti, fyziologických dopadů a zajištění osobní bezpečnosti dítěte i nebezpečí vyplývajících z aktivit dítěte pro rodinu. Po provedení analýzy zadání jsem dospěl k závěru, že zde nemohou být řešena témata trestní odpovědnosti a pachatele internetových přestupků nebo trestných činů a příslušné zákony. V jiné práci by bylo možno tyto aspekty rodičům přiblížit, ale vzhledem k dosavadnímu rozsahu této práce a objemu příslušných dat zde toto nebylo možné.

První fází práce byla analýza a popis struktury internetu a jejího překotného vývoje, způsob využívání internetu dětmi a prostředky, které k tomu využívají. V rámci této části práce bylo zjištěno, že děti, které se narodily v době vysokorychlostního internetu, vnímají Internet jinak než většina rodičů. Vlivem neustálého přístupu k internetu se u nich mění poměr „offline“ a „online“ aktivit. Využívají v současné době k aktivitám na internetu nejen počítače, ale ve velké míře i mobilní telefony a tablety. Tento způsob připojení je mnohdy rizikovější než připojení pomocí počítače a přináší nová rizika. Na základě dlouhodobého připojení dětí k internetu se objevují rizika nová, např. některé kybernemoci související z psychikou dítěte nebo riziky vyplývající z neustálé online komunikace. V této části práce jsou popsána rizika a následky, které hrozí dětem v důsledku nekontrolovaného používání internetu a výsledky průzkumů, které k tomuto tématu proběhly.

V teoretické části práce byly popsány konkrétní možnosti zabezpečení zařízení, ochrany a kontroly bezpečnosti dětí pomocí nastavení operačních systémů, prohlížečů, speciálních aplikací a domácích routerů. Bylo zjištěno, že existuje mnoho možností, jak děti chránit a kontrolovat. Vzhledem k pestrosti operačních systémů na zařízení bylo nutno v rámci přehlednosti práce popsat zabezpečení pro jednotlivé OS a poté některé univerzální aplikace.

Při studiu a analýze jednotlivých možností zabezpečení jsem zjistil, že úspěšnost ochrany a kontroly je závislá na věku a vynalézavosti dítěte. Například ochranu nastavením webového

prohlížeče je možné obejít jednoduše využíváním jiného. Je proto důležité kombinovat ho ještě s jinou aplikací nebo nastavením v OS, která zamezí spouštění jiných webových prohlížečů.

Z analýzy parametrů nástrojů ochrany a kontroly vyplývá, že z hlediska úspěšnosti rodičovské ochrany u nepřenosných zařízení (PC) a jiných zařízení připojených přes domácí router (bez současného připojení k jiným sítím), je nejspolehlivější použití kontroly prostřednictvím domácích routerů s pokročilými funkcemi rodičovské kontroly (ta se dá obejít jen velmi těžko), nastavením OS nebo doplněném některých z aplikací určených k rodičovské kontrole a ochraně proti malware na zařízení dítěte. Toto zabezpečení v sobě kombinuje řízení přístupu k internetu, prevenci přístupu k závadnému obsahu i kontrolu obsahu kontaktů dítěte s okolím (případnými útočníky) a ochranu proti malweru. Výhodou tohoto řešení je, že při nastavování routeru jeho nastavení platí pro vybraná zařízení ve vlastní síti bez ohledu na jejich druh nebo OS. Nevýhodou je nastavení omezení routeru jen v jedné síti.

U mobilních zařízení, které disponují připojením k internetu pomocí operátorů datových sítí je situace poněkud odlišná. Musíme na zařízení aplikovat nastavení, která budou platit, ať je dítě kdekoli a připojeno jakýmkoliv způsobem. Potom tedy musíme nastavení uskutečnit v OS Windows a iOS buď nastavením přímo v OS (v OS Android nelze) nebo stažením aplikací, která tato nastavení umožňují. Při rozdílných OS zařízení rodiče a dítěte je třeba dbát, aby aplikace byly použitelné v obou těchto OS nebo spravovatelné z webového portálu.

Zejména starší děti se však dokáží sebelepší kontrolu nějak obejít. Děti je proto také dobře informovat a vychovávat k vlastní zodpovědnosti. Je třeba v tomto ohledu budovat důvěru. Účastnit se internetového života dítěte, poskytovat dítěti radu a oporu. Vysvětlovat, být s dětmi v neustálém kontaktu, jak v reálném, tak ve virtuálním světě.

V dalších kapitole je proto sestaven seznam doporučení pro rodiče k nastavení domácích pravidel používání internetu a kontakty na krizové linky a poradny, kam se mohou obrátit při řešení problémů.

Na podporu rodičů byly vytvořeny jednoduché webové stránky, které je možné možné navštívit na adrese https://juraba.wixsite.com/mysite.

Téma bezpečnosti dětí na internetu je, jak se ukazuje, velice důležité a zasloužilo by větší prostor ve veřejnoprávní nebo jiné televizní stanici. Jak se ukázalo, touto tématikou se zabývá mnoho odborných prací a je prezentována na profesionálních internetových portálech. Aby se však dostaly do pozornosti širší, laické veřejnosti, bylo by možné toto téma medializovat jednoduchou formou zejména v médiích jako je televizní vysílání například formou upoutávek zařazovaných do reklamních bloků podobně jako jsou zařazovány upoutávky týkající se bezpečnosti silničního provozu. V rámci těchto upoutávek by mohly být uvedeny kontakty na zmíněné studie a weby, kde se rodiče mohou podrobně seznámit s problematikou a způsoby, jak ji řešit.

RESUMÉ

Cílem této práce bylo zanalyzovat možnosti rodičovské kontroly bezpečnosti dětí na internetu, doporučit řešení a pravidla, která zaručí větší bezpečnost dětí. Dalším cílem bylo vytvořit webové stránky se stejnou problematikou.

V této práci jsem se věnoval analýze prostředí internetu a jeho využívání dětmi, analýze rizik, která z toho pro ně vyplývají a analýze možností, jak je možné je na internetu chránit. Zohledněna byla hlediska psychologická, fyziologická, technická i rizika osobního kontaktu s případným útočníkem. Součástí práce jsou možnosti rodičovské ochrany, kontroly a komunikace s dítětem o bezpečnosti na internetu. Ze získaných poznatků a dostupných, ověřených zdrojů jsem sestavil doporučená pravidla pro rodiče. Tato práce dále obsahuje i možnosti, kde získat další informace nebo kam se mohou rodiče obrátit pro pomoc v případě ohrožení dítěte nebo s jinými problémy v oblasti internetové bezpečnosti dětí i rodičů.

RESUME

The aim of this work was to analyze the possibilities of parental control of child safety on the Internet, to recommend solutions and rules that will guarantee greater safety of children. Another goal was to create a website with the same issues.
In this work, I focused on analyzing the Internet environment and its use by children, analyzing the risks that arise for them and analyzing how to protect them on the Internet. Psychological, physiological, technical and personal contact with potential attackers were taken into account. Part of the thesis are the possibilities of parental protection, control and communication with the child about internet safety. Based on the acquired knowledge and available, verified sources I have compiled the recommended rules for parents. Furthermore, this work also includes options for obtaining further information or where parents can contact for help in case of a child's threat or other Internet security issues for children and parents.

SEZNAM LITERATURY

1. ECKERTOVÁ Lenka a Daniel DOČEKAL, 2013. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. 1. vyd. Brno: Computer Press. ISBN 978-80-251-3804-5.

1. KOPECKÝ Kamil a René SZOTKOWSKI, 2018. Výzkumná zpráva Rodič a rodičovství v digitální éře. [online]. Seznam.cz, Bezpečný internet.cz, Univerzita Palackého v Olomouci. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/107-rodic-a-rodicovstvi-v-digitalni-ere-2018/file
2. HULANOVÁ Lenka, 2012. Kriminalita páchaná na dětech. Triton. ISBN 978-80-7387-545-9
3. KOPECKÝ Kamil, 2012. Prevence kyberšikany pohledem E-Bezpečí. Slideshare [online]. 10. 11. 2012. Dostupné z: http://www.slideshare.net/kopeckyk/prevencekyberikany-pohledem-ebezpeci
4. KOPECKÝ Kamil a Martin KOŽÍŠEK, 2013. Výzkum rizikového chování českých dětí v prostředí internetu 2013 [online]. Seznam.cz, Bezpečný internet.cz, Univerzita Palackého v Olomouci. Dostupné z: http://www.bezpecnyinternet.cz/kestazeni/bezpecny_internet_prezentace.pdf
5. KOPECKÝ Kamil, René SZOTKOWSKI a Veronika KREJČÍ, 2012. Nebezpečí internetové komunikace III. 1. vydání. Olomouc: Univerzita Palackého v Olomouci. ISBN 978-80-244-3087-4.
6. Projekt E-Bezpečí - Centrum prevence rizikové virtuální komunikace Pedagogická fakulta Univerzity Palackého V Olomouci dostupný [online] na https://www.e-bezpeci.cz/index.php NÁRODNÍ CENTRUM BEZPEČNĚJŠÍHO INTERNETU. http://www.bezpecne-online.cz/
7. SDRUŽENÍ LINKA BEZPEČÍ. http://www.pomoc-online.cz/
8. SEZNAM.CZ, A.S. Desatero bezpečného internetu. Seznam se bezpečně. http://www.seznamsebezpecne.cz/desatero
9. Gruntorád Jan: Historie internetu v datech. ITpoint (CESNET) [online] dostupný na http://www.itpoint.cz/cesnet/clanky/?i=historie-internetu-25-let-cr-11512
10. VRABEC, Vladimír. Internet a hromadné sdělovací prostředky. *Ikaros* [online]. 1998, ročník 2, číslo 8 [cit. 2019-03-06]. urn:nbn:cz:ik-10272. ISSN 1212-5075. Dostupné z: http://ikaros.cz/node/10272

SEZNAM OBRÁZKŮ, TABULEK, GRAFŮ A DIAGRAMŮ