BAKALÁŘSKÁ PRÁCE

Kyberbezpečnost – rizika komunikace na síti

Cybersecurity – Risks of Online Communication

STUDIJNÍ PROGRAM

Specializace v pedagogice

STUDIJNÍ OBOR

Učitelství praktického vyučování a odborného výcviku

VEDOUCÍ PRÁCE

Doc. PhDr. Dana Dobrovská, CSc.

ŠVARCOVÁ

LUCIE

2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Švarcová** Jméno: **Lucie** Osobní číslo: **487660**

Fakulta/ústav: **Masarykův ústav vyšších studií**

Zadávající katedra/ústav: **Institut pedagogických a psychologických studií**

Studijní program: **Specializace v pedagogice**

Studijní obor: **Učitelství praktického vyučování a odborného výcviku**

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Kyberbezpečnost-rizika komunikace na síti

Název bakalářské práce anglicky:

Cybersecurity - Risks of Online Communication

Pokyny pro vypracování:

Prostřednictvím dotazníkového šetření zjistit, zda a do jaké míry si studenti střední školy uvědomují rizika, která s sebou přináší neuvážené chování v kyberprostoru. Bakalářská práce bude mít teoreticko-empirický charakter. V teoretické části budou reflektovány rychle se měnící poznatky o nástrahách v online prostředí. Hlavním cílem empirické sondy bude zjistit rozsah vědomostí studentů o rizicích a identifikovat připravenost studentů tyto vědomosti použít v praxi.

Seznam doporučené literatury:

Dočekal, D. et al. Dítě v síti. Computer press. 2019.
Dočekal, D. Eckertová, L. Bezpečnost dětí na internetu. Computer press 2013
Kchout, R., Kuhlková, S. : Internetem bezpečně: příručka pro děti, 2017.
Vyhnánková, E., Losekool, M. Jak na sítě. Melvil, 2019, ISBN 978-80-7555084-2.

Jméno a pracoviště vedoucí(ho) bakalářské práce:

doc. PhDr. Dana Dobrovská, CSc., katedra inženýrské pedagogiky

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **25.01.2021** Termín odevzdání bakalářské práce: **29.04.2021**

Platnost zadání bakalářské práce: **19.09.2022**

doc. PhDr. Dana Dobrovská, CSc.	Ing. Petr Svoboda, Ph.D., ING.PAED.IGIP	prof. PhDr. Vladimíra Dvořáková, CSc.
podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Studentka bere na vědomí, že je povinna vypracovat bakalářskou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v bakalářské práci.

Datum převzetí zadání Podpis studentky

Švarcová, Lucie. *Kyberbezpečnost – rizika komunikace na síti*. Praha: ČVUT 2021. Bakalářská práce. České vysoké učení technické v Praze, Masarykův ústav vyšších studií.

MASARYKŮV ÚSTAV
VYŠŠÍCH STUDIÍ
ČVUT V PRAZE

Prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracovala samostatně. Dále prohlašuji, že jsem všechny použité zdroje správně a úplně citovala a uvádím je v přiloženém seznamu použité literatury.

Nemám závažný důvod proti zpřístupňování této závěrečné práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Praze dne 28. 4. 2021 Podpis

Poděkování

Velice děkuji mé vedoucí práce doc. PhDr. Daně Dobrovské, CSc. za pomoc a poskytnutí nezbytných informací, bez nichž by tato práce nebyla realizována.

Obrovské poděkovaní patří mému příteli a dcerám za podporu, které se mi od nich dostávalo a za čas, který jsem této práci mohla věnovat.

Abstrakt

V této bakalářské práci zaměřené na studenty středních škol se zabývám kyberbezpečností v souvislosti s aktivním užíváním sociálních sítí. Zajímala jsem se nejenom o rozsah znalostí studentů, ale také o jejich připravenost používat tyto znalosti v praxi. Současně jsem chtěla zjistit, zda probíhá osvěta bezpečného pohybu na sociálních sítích, kým a jak je uskutečňována a zda ji studenti využívají. Praktická část práce byla formou dotazníkového šetření realizována na střední odborné škole v okrese Rakovník.

Klíčová slova

Juniorní centra excelence, kyberbezpečnost, kyberprostor, nauka, online rizika, osvěta, sociální síť, zabezpečení

Abstract

In this bachelor's thesis focused on high school students, I deal with cybersecurity in connection with the active use of social networks. I was interested not only in the extent of students' knowledge, but also in their readiness to use this knowledge in practice. At the same time, I wanted to find out whether the awareness of safe movement on social networks was taking place, by whom and how it was being implemented and whether students used it. The practical part of the work was carried out in the form of a questionnaire survey at a secondary vocational school in the district of Rakovník.

Keywords

Junior centers of excellence, cybersecurity, cyberspace, science, online risks, rising public awareness, social network, security

OBSAH

Úvod **9**
Teoretická část **11**
1 Teenager/adolescent – vymezení pojmu **12**
2 Kyberprostor **13**
2.1 Vlastnosti a rizika kyberprostoru 13
2.2 Digitální stopa v kyberprostoru 13
2.3 Teenageři v kyberprostoru 14
3 Sociální sítě **16**
3.1 Vymezení pojmu, potenciál využití 16
3.2 Teenageři na sociálních sítích 16
3.3 Nejoblíbenější sociální sítě 17
3.4 Online rizika 18
3.4.1 Fake news 19
3.4.2 Zneužití osobních údajů 20
3.4.3 Závislost na internetu (netolismus) 21
3.4.4 Virtuální nenávist 22
3.4.5 Rizika YouTube 22
3.4.6 Rizika Facebooku 22
3.4.7 Rizika Instagramu 23
3.4.8 Kyberšikana 24
3.4.9 Kyberstalking 25
3.4.10 Kybergrooming 25
3.4.11 Sexting 25
3.4.12 Závěr k online rizikům 27
4 Kyberbezpečnost – nauka o bezpečném pohybu **28**
4.1 Kyberbezpečnost a rodina 28
4.2 Kyberbezpečnost a škola 28
4.3 Osvěta – film V Síti, V Síti: Za školou 29
5 Ochrana a zabezpečení zařízení **31**
5.1 Základní pravidla používání zařízení 31
5.2 Problematika hesel 32
5.3 Trestní zákoník 32
5.4 Statistiky PČR 33
6 JCE centra **35**

Praktická část **37**
7 Výzkumné šetření **38**
7.1 Výzkumné cíle 38
7.2 Výzkumný vzorek a výzkumná metoda 38
7.3 Výzkumné otázky a hypotézy 38
7.4 Shrnutí výsledků dotazníkového šetření 58
Závěr **61**
Seznam použité literatury **63**
Seznam obrázků **66**
Seznam grafů **67**
Evidence výpůjček **69**

ÚVOD

Ve velké míře jsou již i malé děti vlastníky zařízení s volným přístupem na internet. Pro teenagery je již „chytrý" mobil naprostou samozřejmostí a nutností.

Potenciál využití internetu je obrovský a nese sebou spoustu výhod. Během chvilky se můžeme ocitnout na druhém konci světa, zeptat se slavných osobností na jejich názory nebo přijít o všechny úspory. To vše za pouhých pár minut, s minimálním počtem kliknutí na klávesnici. Internet má obrovskou MOC a SÍLU. Pomůže stejně tak dobře dostat se na výsluní, jako na samé dno i níže. Každou naší aktivitou v online světě si budujeme a vytváříme své vlastní digitální já. Tento digitální svět je ale prostředím bez hranic a jasně stanovených pravidel čítající spoustou nástrah.

Jak chránit sám sebe a své blízké? Jedinou cestou jsou informace.

Umět správně identifikovat nalezené údaje, umět je vyhodnotit a vhodně použít, TO je bezpečná cesta k bezproblémovému užívání internetu.

Zejména děti a mladiství, kteří spadají do nejzranitelnější skupiny, a pro které se digitální éra a moderní technologie staly všudypřítomnou dennodenní záležitostí je potřeba před nástrahami internetu chránit a zajistit jim dostatečnou gramotnost v oblasti bezpečného pohybu na internetu. Cílem této práce nazvané "Kyberbezpečnost - rizika komunikace na síti" bude v teoretické rovině charakteristika pojmů souvisejících s kyberbezpečností na základě které pak provedu výzkum zaměřený na současné znalosti a praktiky.

Jako první jsem vymezila pojem teenager z pohledu psychologie. V tomto období přechodu mezi dětstvím a dospělostí vstupuje do popředí sexualita a rozvíjí se socializace, proto touha být víceméně neustále online a "in" na sociálních sítích je pro daný věk typická.

V části druhé je definován pojem kyberprostor a jeho vlastnosti. Následuje sekce věnovaná sociálním sítím. Definuji zde pojem, potenciál využití, nejoblíbenější a nejpoužívanější sociální sítě a online rizika hrozící při jejich aktivním využívání.

Čtvrtá kapitola je věnována nauce o bezpečném pohybu na sociálních sítích poskytovaná školou, rodinou či přáteli formou nejaktuálnějších průzkumů. Za zmínku v této sekci stojí zmínka o filmu V Síti, vytvořený jako osvěta nejen pro uživatele sociálních sítí, ale i pro rodiče a školská zařízení.

Obsahem páté části je ochrana a zabezpečení přístupových zařízení a vytvořených účtů na sociálních sítích.

Závěrečná část je věnována Juniorním centrům excelence, jakožto možné variantě implementace do výuky informační bezpečnosti středoškolského vzdělávání.

Teorie je doplněna o nejaktuálnější průzkumy a statistiky k daným tématům a základní paragrafy související s kyberkriminalitou.

V empirické části je proveden výzkum v podobě dotazníkového šetření. Jejím cílem je zjištění, jaký je rozsah znalostí studujících střední odborné školy o rizicích vyplývajících z aktivního užívání sociálních sítí a jaká je jejich připravenost používat tyto znalosti v praxi. Součástí výzkumu bude také zjištění, zda, kde a jak probíhá osvěta bezpečného pohybu na sociálních sítích, kým je uskutečňována a zda ji studující využívají. Zjištění, zda studenti vhodně zabezpečují svá zařízení a vytvořené profily celou sondáž dokreslí.

TEORETICKÁ ČÁST

1 TEENAGER/ADOLESCENT – VYMEZENÍ POJMU

V obecném slova smyslu je adolescence charakterizována jako přechod mezi dětstvím a dospělostí, ve kterém je ukončen proces tělesného a pohlavního vývoje, do popředí vstupuje sexualita, rozvíjí se socializace a utváří se vlastní osobnost jedince (Macek, 2013, s. 10, 13). V tomto období dochází ke kompletnímu ucelení vlastních zkušeností z předchozích vývojových stádií, při kterých si jedinec postupně utvářel svoje vlastní já. (tamtéž, s. 19)

Macek (s. 10) rozděluje adolescenci do tří fází: časnou v rozmezí od 10 (11) -13 let, střední od 14 -16 let a pozdní od 17 do 20 let.

Vágnerová (1999, s. 321) dělí toto období pouze do dvou fází – rané a pozdní adolescence, kdy pozdní adolescencí označuje věk od 15 do 20 let. Dospívání definuje jako životní etapu, ve které dochází k celkové proměně osobnosti jedince, který se musí nejenom vyrovnat se svojí tělesnou proměnou, utvářet si sociální vazby a vlastní osobnost, ale dochází zde také ke snaze zbavit se všech dosavadních dětských vlastností a velké touhy osamostatnit se.

2 KYBERPROSTOR

2.1 Vlastnosti a rizika kyberprostoru

„Internet zrcadlí, zvýrazňuje a zviditelňuje dobré i špatné stránky běžného života."(Boydová, 2017, s. 38).

Vstupem do kyberprostoru se ocitáme v prostředí původně nejpoužívanějších e-mailů, instant messaging, webových stránek s nepřeberným množstvím informací a poskytovaných služeb, aplikací pro online komunikaci, ale i nejmodernějším užívání sociálních sítí, stránek pro sdílení videí, platformy pro blogy apod. A toto všechno činí z lákavého kyberprostoru nejenom pomocníka, ale i skrytého škůdce.

Dle Jirovského je základní vlastností kyberprostoru jeho globální pokrytí, vytvářející otevřené prostředí všem uživatelům z různých států a kontinentů (kteří splní předepsaná kritéria) kdykoli nahlížet na údaje poskytnuté internetem.

Neméně důležitým znakem internetu je jeho decentralizovanost, kdy *„neexistuje centrální autorita, která by o jeho existenci či neexistenci rozhodovala, či ho nějakým způsobem řídila*". (Jirovský, 2007, s. 34).

Další vlastností je otevřenost internetu, v případě které se může každý uživatel volně prezentovat, čímž se kyberprostor stává poskytovatelem obrovského množství entropických informací, ze kterých je velký problém získat ty správné a pravdivé. (tamtéž, s. 33).

Oblíbeností online komunikace je tak stává její veřejná přístupnost a snadná rozšiřitelnost obsahu, oproti komunikaci ve fyzickém světě, kdy nemusí být vyvinuto velkého úsilí pro prosazení nebo oslovení většího publika. Toto sebou nese nejen obrovský potenciál, ale zároveň i možná rizika.

Volně dostupné informace, které jsou do kyberprostoru publikovány individuálně každým jedincem, mohou být relativně „nevinné", ale také vztahující se až příliš k naší osobě, a to nejenom zveřejňováním identifikačních údajů, ale i zveřejňováním detailů o partnerství, osobní prožitky, zkušenosti. (Ševčíková a kol., 2014, s. 56).

2.2 Digitální stopa v kyberprostoru

Technologie, kterými jsme obklopeni, nás hypnotizují. Nejenom monitoring pohybu, ale vše čemu věnujeme největší pozornost, co se nám

líbí, zkrátka každý krok v našem online procesu je zaznamenáván. (Dočekal a kol., 2019, s. 147)

Technologie jsou vyvíjeny tak, aby podporovaly vložený obsah v jeho perzistenci, což v důsledku může vést k asynchronní komunikaci. Vložený obsah je tak díky své perzistenci trvale zaznamenáván. (Boydová, 2017, str. 25)

Virtuální prostředí není prostředím anonymním. Každý, kdo na internetu cokoli vyhledává, nakupuje nebo jen brouzdá na různých webových stránkách, zanechává o své činnosti záznamy. Tyto záznamy se odborně nazývají digitální stopy a i ony sebou nesou rizika. Od marketingových reklamních bannerů až po krádeže osobních údajů, hesel, účtů, profilů kybernetickými predátory. Tyto informace poskytnuté internetu jsou často zneužívány ke kyberšikaně. [1]

Kroky v online prostředí si vytváříme svoji digitální identitu, která do budoucna nezmizí. Je důležité pamatovat na to, že vložením obsahu do kyberprostoru ho přestáváme mít plně pod kontrolou.

2.3 Teenageři v kyberprostoru

Nepochybně je s rozvojem globální komunikace a hojnějším pohybem v kyberprostoru ovlivňována psychika jedince, jeho sociální chování, zvyky i hodnoty. Dnešní děti obklopují moderní technologie již od narození. Zcela rozdílná je jejich komunikace, učení a seznamování se ve srovnání s předchozích generací. Proces setkávání se s přáteli v kyberprostoru a spoluvytváření *online veřejnosti*, je pro současnou mládež „cool", stejně tak jako byly „cool" pro starší generace fastfoodové řetězce, obchodní centra či taneční párty. Potřeba seznamování se, vtipkování, flirtování je stále stejná jako v minulosti.

Pro věkovou skupinu lidí, kteří vyrostli obklopeni počítači, mobilními telefony, videohrami či videokamerami je užíván termín „digitální domorodec". Tito jsou schopni čerpat digitální informace rychleji než „digitální imigranti", což jsou lidé narozeni v 70. letech a dříve, kteří se setkali s digitálním světem až v dospělosti. (Eckertová, Dočekal, 2013, s. 19)

Dle Boydové je teenager ten, kdo hledá nezávislost a vlastní identitu. Teenageři chtějí pochopit dospělý svět a snaží se adaptovat ve veřejném prostoru tím, že sledují a seznamují se s dospělými vzory. *„Teenageři chtějí čas s kamarády trávit po svém, bez dohledu rodičů a na veřejnosti. Online veřejnosti, v nichž pobývají, jim paradoxně nabízejí výrazně vyšší míru soukromí než domov, kde mají neustále za zády rodiče a sourozence*" (Boydová, 2017, s. 33). Pohybem v kyberprostoru si utváří atmosféru důvěrnosti a schopnost mít svoji

sociální situaci pod kontrolou. Tímto hledáním si vlastní cesty je u nich naplňována potřeba soukromí.

3 SOCIÁLNÍ SÍTĚ

3.1 Vymezení pojmu, potenciál využití

Sociální sítě jsou fenoménem současné doby. Na světě neexistuje snad téměř nikdo, kdo by nepřišel do styku se sociální sítí. I ony měly svůj vývoj do dnešní podoby. Stejně jako se vyvíjel Internet, tak i sociální sítě získávaly postupně svoji podobu.

Vůbec první sociální síť SixDegrees.com vznikla v roce 1997.

Vize spuštění prvních sociálních sítí jako MySpace nebo Friendster byla, že se uživatelé seznámí s novými lidmi (přáteli svých přátel) a rozšíří tak svoji základnu. Namísto navazování nových kontaktů se ale uživatelé více zabývali komunikací se svými stávajícími přáteli.

V současné době nelze jednoznačně říci, jaká je nejvhodnější definice sociální sítě.

Dle Černého je termín nejlépe vystižen anglickým „Social network" neboli společenská síť, která *„umožňuje komunikaci a sdílení informací, a to více méně trvalým způsobem, čímž se odlišuje od chatu či telefonu*." Je spojena s určitou skupinou přátel či jiných odběratelů obsahu, mezi nimiž je vytvořen vztah. [2]

Sociální sítě jsou využívány převážně pro komunikaci a sebeprezentaci. Vytvořené profily jsou mezi uživateli propojovány a vznikají tak virtuální přátelství. Uživatelé mohou vytvářet různé skupiny, přidávat fotografie, videa, sledovat aktivitu, komentovat příspěvky, posílat si vzkazy. (Ševčíková a kol., 2014, s. 23)

3.2 Teenageři na sociálních sítích

Využívání sociálních sítí je pro teenagery normou a stalo se běžnou součástí jejich životů, stejně jako sledování televize. Pohyb na internetu je pro ně dennodenní záležitostí, surfují po webech, vyhledávají nové nebo potřebné informace, tráví čas na sociálních sítích. Teenageři si na tento typ komunikace zvykli, naučili se fungovat ve světě, jehož je internet nedílnou součástí.

Dle Českého statistického úřadu používalo v roce 2019 internet již 81 % Čechů starších 16 let, chytrý telefon pak 70 % z nich. Téměř všichni patnáctiletí pak mají doma přístup k internetu a mohou používat mobilní telefon. Téměř polovina patnáctiletých žáků používá o víkendu internet doma více než 4 hodiny. Denně či téměř každý den je 78 % dívek v tomto věku na sociálních sítích a 66 % chlapců hraje na internetu hry. Zatímco v roce 2010 se z mobilního telefonu

připojovala na internet 4 % osob starších 16 let, v roce 2019 to byly téměř dvě třetiny. Nejčastěji tak činí mladí lidé, kde mezi osobami ve věku 16 až 24 let internet v mobilu používá 97 % z nich. [3].

Dalším výzkumem v oblasti chování dětí ve věku 7 až 17 let na internetu nazvaném České děti v kybersvětě z roku 2019 se dozvídáme, že 80 % respondentů ve věku 16 -17 let aktivně užívá sociální sítě (15letí – 78,8 %, 16letí – 79,16 %, 17letí – 80,15 %). Dominantní sítí byl YouTube, Facebook, Facebook Messenger a Instagram. Nejčastěji využívají Google Chrome k prohlížení internetových stránek. Více než polovina dětí, a to 59 % potvrdila, že ve svém mobilním telefonu mají trvalý přístup na internet a jsou tak na Wi-Fi nezávislí. [4].

3.3 Nejoblíbenější sociální sítě

Seřazení sociálních sítí dle aktivity dětí: výzkum [4]

1) YouTube – dětmi nejnavštěvovanější sociální síť (89,51 % dětí ve věku 7 – 17 let [4])

   (pozn. zařazen mezi sociální sítě, protože umožňuje vytvářet uživatelské profily jednotlivých uživatelů a vzájemnou interakci mezi nimi)

   Dle výzkumu nazvaném „Rodič a rodičovství v digitální éře" z roku 2018 je YouTube sledován nejen dětmi, ale i rodiči, a to 87,65 % (z toho 55,8 % méně než 1 hodinu týdně; 27,63 % rodičů zhruba 1 hodinu denně).

   85 % rodičů uvedlo, že nesleduje známé youtubery, oproti dětem, které youtubery pravidelně sledují, a to 58,5 % (dle odpovědí rodičů).

   44 % rodičů hodnotí youtubery negativně, vnímá je jako někoho, kdo nutí děti ke zbytečnému trávení volného času na Youtube.

   33 % rodičů vnímá youtubery jako vhodné vzory. [5]

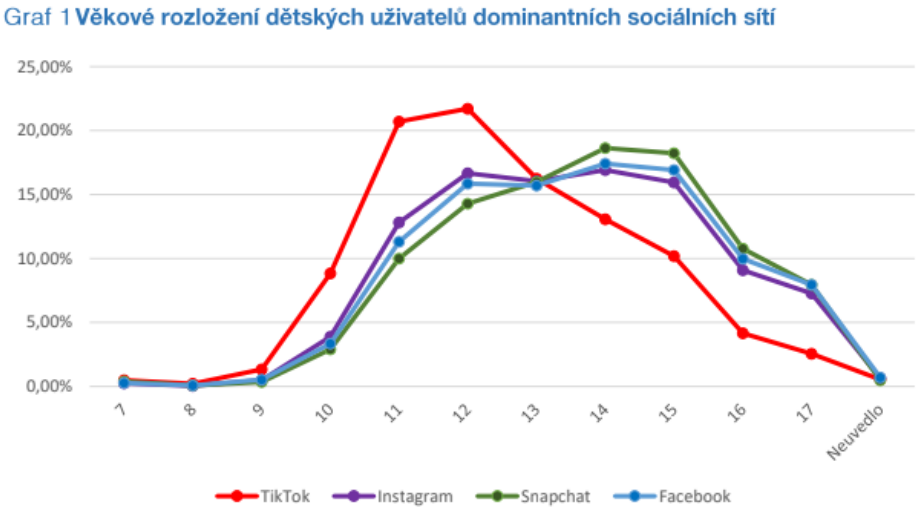
   Na YouTube sledují České děti nejčastěji vtipná videa (žertíky, pranky), výzvy (challange), let´s play videa (hraní her), reakční videa (kritické hodnocení videí jiných youtuberů), vlogy (videodeníčky), food videa (videa o jídle). [4]

2) Facebook (druhá nejnavštěvovanější sociální síť – 72,19 % dětí ve věku 7 – 17 let [4]);
3) .Facebook Messenger (68,98 % dětí ve věku 7 – 17 let [4]);
4) Instagram (98,83 % dětí ve věku 7 – 17 let [4].

Další oblíbené sociální sítě:

- E-mail;

- SMS/MMS;
- WhatsApp Messenger;
- Snapchat;
- TikTok;
- Twich;
- Skype;
- Pinterest;
- Viber [4].



Obrázek 1: Věkové rozložení dětských uživatelů dominantních sociálních sítí

Zdroj: [4].

3.4 Online rizika

Rizika spojená s internetem nejsou oproti offline světě větší či menší, jsou jiná, nová.

Současné nejpoužívanější sociální sítě, jako jsou YouTube, Facebook nebo Instagram jsou masivními propagátory mediálního obsahu, ale ve své podstatě je nezajímá, zda je tento obsah vhodný či nikoli. Propojování dat z poskytnutých údajů okamžitě propojí s reálným životem. Toto mnohdy nesmyslné poskytování dat do všech online zákoutí znamená, že dříve či později se těchto dat někdo zmocní (Dočekal a kol, 2019, s. 139). A otázkou je, jak s nimi naloží.

Dle oblastí, do kterých spadají, rozlišujeme 4 typy rizik (1-4). Tato rizika působí na dítě ve třech kontextech:

a) *dítě jako příjemce* (dítě je vystaveno nežádoucímu obsahu);
b) *dítě jako účastník* (procesu vzájemné interakce a komunikace);

c) *dítě jako pachatel* (aktivním podílením se na nežádoucích jevech).

Dělení rizik dle spádových oblastí:

1) **Komerce**

   a) reklamy, spam, nabádání k poskytnutí peněžních prostředků;
   b) získávání a uchovávání osobních údajů;
   c) gambling, nelegální stahování.

2) **Násilí**

   a) nenávistný či děsivý obsah;
   b) oběť kyberšikany, kyberstalkingu;
   c) pachatel kyberšikany, kaberstalkingu.

3) **Sexualita**

   a) pornografie či jiný sexuální obsah;
   b) setkávání se s neznámými lidmi z internetu, sexuální zneužívání;
   c) vytváření a nahrávání pornografických materiálů.

4) **Hodnoty**

   a) rasistické nebo jiné zkreslené či zavádějící informace a rady;
   b) sebepoškozování, přesvědčování a manipulace ze strany druhých;
   c) poskytování (zavádějících) rad např. ohledně hubnutí nebo sebevraždy. (Ševčíková a kol., 2014, s. 10).

3.4.1 Fake news

Uživatelé internetu, především ti mladší, bez životních zkušeností, jsou konfrontováni s obrovským množstvím obsahu. Ten může být důvěryhodný, kvalitní, ale i nedůvěryhodný a falešný, jde o tzv. **fake news**. Mnozí jedinci informace přijímají jako korektní a nijak o nich nepochybují.

Projekt studentů Masarykovy univerzity „Zvol si info" se snaží o mediální gramotnost v tomto ohledu a definoval pravidla, jak fake news poznat: (https://zvolsi.info/)

1) zdroje – hledejte zdroje, pokud zpráva nemá uveden zdroj nebo je její autor neznámý, je velká pravděpodobnost že se jedná o lež;

2) svalování viny a nálepkování – články hned označí „špatnou" stranu, neposkytují možnost rozebrat věc z více úhlů;
3) vymýšlení faktů – obrovské množství informací ověřovat nelze, ale opět se zaměřit na zdroje, co o nich píšou nejen české, ale i zahraniční weby;
4) manipulace s obrázky – upravené fotografie s šokujícím titulkem;
5) hra s emocemi a dramata – manipulace pomocí emocí, děsivé titulky.

Naopak kvalitní web *„uvádí zdroje a podává informace, ne emoce. Dává prostor oběma stranám, nezaujímá jasné stanovisko a nikomu nic nepodsouvá."* (Dočekal a kol., 2019, s. 179 – 181)

3.4.2 Zneužití osobních údajů

Sociální sítě a jejich funkčnost slouží jako **úložiště osobních údajů**, což je jedním z dalších skrytých rizik. Tyto údaje lze relativně snadno získat a posléze zneužít. Nejsnadnějším zneužitelným osobním údajem bývají zveřejněné fotografie tváře pro jednoznačnou identifikaci oběti. [6] Z výzkumu nazvaném Rodič a rodičovství v digitální éře z roku 2018 vyplynulo, že sami rodiče zasílají fotografie svých dětí. 80 % rodičů zasílá fotografie svým nejbližším příbuzným, 53 % otci dětí a 41 % přátelům na sociální síti. 81,7 % rodičů uvedlo, že sdílejí fotografie, které umožňují dítě identifikovat (podle obličeje), ale neobsahují sexuální podtext, čímž tak dobrovolně prozrazují identitu dítěte.

20 % rodičů sdílí fotografie, na kterých jsou jejich děti částečně obnaženy, a je možné určit jejich identitu. 3,5 % rodičů již sdílelo fotografii obnaženého dítěte v novorozeneckém či kojeneckém věku. [5]

Někteří rodiče provozují tzv. Sherenting, tedy nadměrné sdílení materiálů dětí v online prostředí. 7,13 % dětí uvedlo, že rodiče nahráli na internet jejich fotografie či videa, ačkoli s tím děti nesouhlasily. [4]

Taktéž skrze různé aplikace a hry je sdílení osobních údajů velkým nebezpečím. Jejich šíření a sdílení je zakomponováno v licenčních ujednání, které ale nejsou pečlivě studovány, tudíž je toto riziko velmi opomíjené. [6]

V knize Dítě v síti citoval autor ředitele Applu Tima Cooka následující: *„Informace, které o sobě poskytujeme, jsou proti nám obráceny jako zbraně, cílené s vojenskou přesností. Obchod s osobními údaji se změnil v datově průmyslový komplex."* *„Je to obyčejné sledování. A ty hory dat slouží jen k obohacení těch, co nás sledují."* (s. 136). Využívání běžně poskytovaných osobních

údajů jako je jméno, adresa, telefon či email je již pro různé druhy socnetových kampaní běžnou strategií. Stačí jen propojit údaje s Facebookem a uživatelským profilem a „**match**" existuje a může zdárně cílit na určitou skupinu uživatelů (Dočekal a kol., 2019, s. 137).

K dalším, dnes již běžným a úspěšným marketingovým taktikám na socnetu patří tzv. „**temný post**" či „dark post" (tamtéž, s. 138). Jedná se o nezveřejněný příspěvek na Stránce vytvořený jako inzerce. Příspěvků lze vytvořit velké množství, lze je cílite na různé skupiny lidí dle jejich obsahu. [7] Tyto příspěvky mohou různým skupinám slibovat různé věci a mohou jít dokonce i proti sobě. Zajímavé je, že pokud je např. facebooková centrála upozorněna na tuto činnost, tak nezasáhne IHNED, byť si je vědoma její dezinformační hodnoty. Též si ale uvědomuje, že tato dezinformace je reklamním nosičem a je za ni zaplaceno. Poškozenou stranu centrála informuje, že post bude smazán, ale zároveň ubezpečí plátce a šiřitele postu, že cílová skupina byla zasažena. (Dočekal a kol., 2019, s. 138). Toto ovlivňování mohou využívat například politické strany ke znevýhodnění svého politického protivníka různými negativními algoritmy v jeho neprospěch.

3.4.3 Závislost na internetu (netolismus)

Nelze opominout ani riziko vzniku závislosti, kterou si každodenním nadměrným užíváním informačních technologií způsobujeme. Sociální sítě byly od počátku vytvořeny pro to, aby v uživateli vzbudily závislost. Závislost může mít u každého člověka jiné projevy. Dle Lainera citovaného v knize Dítě v síti je *„Nejkurióznější vlastností online závislosti je, že postižený začne vyhledávat bolest, protože bolest je součástí „svědivého pobytu na síti*." (s. 151). Člověk závislý na internetu svoji závislost buduje především účastí na celém online procesu. Neustálé myšlenky na připojení, snížená sebekontrola, neschopnost přerušit práci s internetem může vést až k rozštěpení osobnosti. Upokojeni pocitem, že se v kyberprostoru nemůže jedinci fyzicky nic stát, v něm vyvolává potřebnou sebedůvěru, se kterou může následně realizovat své sny a vystupovat ve vytoužených rolích. (Jirovský, 2007, s. 35)

Nadměrná potřeba vytváření virtuálních vztahů a neustálá virtuální aktivita plyne většinou z neuspokojivého osobního zázemí uživatele. Nebezpečí, že dotyčný začne dávat přednost online světu před skutečností, kde očekává větší míru pochopení, je značné. (tamtéž, s. 36)

3.4.4 Virtuální nenávist

Internet a s ním spojená anonymita jeho uživatelů bez rozdílu věku a pohlaví je otevřen komukoli. Kdokoli se může vydávat za kohokoli a převážně děti si neuvědomují, jak nebezpečná tato komunikace s virtuálním společníkem může být. Podpora anonymity uživatelů vede k **virtuální nenávisti uživatelů**, kteří se domnívají, že nejsou za své činy zodpovědní. A to i v případě, že je u komentáře reálná fotografie i jméno. Online komunikací si utváříme o druhém představu založenou pouze na vlastních pocitech a přáních. S nadsázkou můžeme říct, že člověk svojí online komunikací částečně hovoří sám se sebou. A nenávist, kterou produkuje, tak ještě více podporuje. Tito lidé šířící své nenávistné hejty ve virtuální rovině mají pocit, že online svět a lidé v něm nejsou skuteční a že právě zde je nastavena svoboda a volnost bez jakýchkoli autorit. I toto může být jedním z důvodů, proč onu činnost záměrně vyhledávají a snaží se z „reality ohraničené mantinely" utéct do „světa bez zábran a postihů". (Dočekal a kol., 2019, s. 164)

3.4.5 Rizika YouTube

V knize Dítě v síti je upozorňováno na YouTube videa, která mají dle autora článku, za úkol podporovat VAŠE názory, byť i NELOGICKÉ, protože se vám to líbí a protože jako uživatel budete tuto síť i dále navštěvovat. A dokud si uživatel neřekne stop nebo nedostane rozum, bude jej tento nastavený algoritmus, sloužící pro zvyšování naší angažovanosti na YouTube, stále zásobovat touto „drogou". (Dočekal a kol., 2019, s. 132). V současné době jsou algoritmy již tak pokročilé, že jen pár vteřin po naší reakci na určitý obsah nám bude nabídnuta koupě nějakého produktu. A pokud toto zafunguje (budeme například při naší činnosti v online prostoru emotivně naladěni a koupi produktu uskutečníme, bude tato koncepce nabídnuta dalším, nám podobným, uživatelům (tamtéž s. 149).

3.4.6 Rizika Facebooku

Facebook byl stvořen tak, aby ovlivňoval základní instinkty jeho uživatele, kteří budou do jeho prostředí vtahováni. Čím vyšší je míra aktivity a online komunikace uživatele, tím více budou zapojováni do aktivit dalších. (Dočekal a kol., 2019, s. 102; 149)

Facebookové algoritmy jsou specializované na výběr a seřazení toho nejvhodnějšího obsahu tak, aby uživatel zůstal na síti co nejdéle (Losekoot, Vyhnánková, 2019, s. 60)

Facebook chce o svých uživatelích vědět vše. Kde a s kým se právě nachází, zda mají vztah, jejich oblíbenou značku oblečení nebo kosmetiky, jaká je jejich politická nebo sexuální orientace.

Zajímá ho ale i to, co uživatelé dělají jinde na internetu. Tedy to, co se děje v prohlížeči, co lze vyčíst z cookies a z těchto informací nám pak nabízí relevantní obsah. Algoritmy se pokoušejí odvodit vzorce, ze kterých následně odhadne preference uživatelů. (Losekoot, Vyhnánková, 2019, s. 60)

Efektivitu své uživatele špehovat si zajišťuje patentováním nových vynálezů, např. vynález, který umožní kameře na telefonu či počítači monitorovat a analyzovat váš výraz a mimiku, jehož zjištěním je vyhodnocení, zda to, co, vidíte, vás baví, nebaví, jste překvapeni, šťastní, znudění apod. (Dočekal a kol., 2019, s. 116). Samozřejmě se jedná pouze o patenty, ale kdoví co nás čeká v budoucnosti? Proč měl zakladatel Facebooku Mark Zuckerberg přelepenu přes web kameru a mikrofonový port notebook lepicí pásku?

3.4.7 Rizika Instagramu

Instagram je označován za obrázkovou síť, kde je předváděn dokonalý svět, kde se uživatelé snaží ukazovat lepší, než ve skutečnosti jsou. Není tedy překvapením, že vyvolává více negativních pocitů v souvislosti s vlastním tělem. (Dočekal a kol., 2019, str. 82). Tendence dětí upravovat svoji osobnost, aby se více líbily nebo dostaly víc lajků, vede k tomu, že již v takto mladém věku jsou dívky schopny podstupovat hladovění, nahrávat své postavy minimálně oblečené.

Tlak Instagramu být krásný a dokonalý je devastující a to zejména, v souvislosti s tělesnou proměnou v období dospívání, kdy je vyzdvihována tělesná atraktivita a zevnějšek se stává cílem i prostředkem. (Vágnerová, s. 329). Touha vylepšování sám/sama sebe vede k tomu, že již ve věku čerstvě dosažené plnoletosti se dívky i chlapci nechávají vylepšovat různými plastickými operacemi. (Dočekal a kol., 2019, s. 166).

Každá sociální síť má své algoritmy nastaveny nepatrně jinak, ale cíl mají společný – zobrazit uživateli takový obsah, který ho bude zajímat.

Užíváním sociálních sítí může vyvolat u uživatelů deprese a negativní pocity. Jsou neustále zavalováni zdánlivě dokonalými fotografiemi či videi, se kterými se v reálném životě těžko vyrovnávají. Výzkum z roku 2017 zveřejněného organizací Royal Society for Public Health uvádí, jaké dopady na duševní zdraví a pohodu mladých lidí ve věku 14 – 24 let mají sociální média. Nejvíce negativních pocitů ukázal Instagram, následovaný Snapchatem a Facebookem, tedy míst,

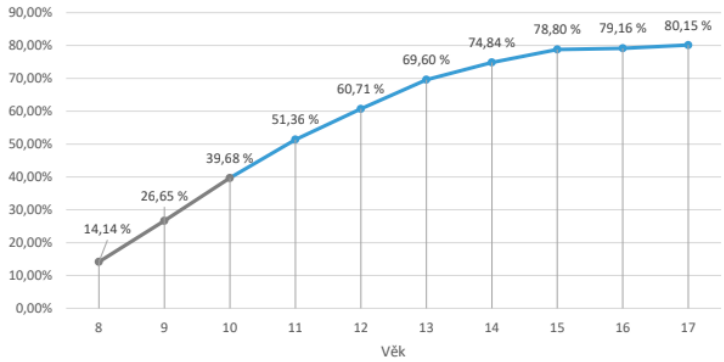
kde se dnešní teenageři pohybují denně a běžně (Dočekal a kol., 2019, s. 81).

3.4.8 Kyberšikana

„Kyberšikana (kybernetická – počítačová šikana, angl. cyberbullying) je druh šikany využívající informační a komunikační technologie (počítače, tablety, mobilní telefony, sociální sítě, emaily apod.) k ublížení druhému (vydírání, ubližování, ztrapňování, obtěžování, ohrožování, zastrašování apod.). Aktéry kyberšikany jsou (obdobně jako u klasické šikany): Agresor – Oběť – Přihlížející (publikum)". [8] Na rozdíl od šikany, kde jsou místa napadení předvídatelná, se s kyberšikanou můžeme setkat prakticky kdykoli a kdekoli, pokud budeme připojeni k internetu anebo k mobilní síti. V digitálním světě se před ní nemáme kam schovat. Nadávka, pomluva, vydírání či zastrašování trvá v rámci kyberútoku mnohem déle oproti reálnému světu, ve kterém se časem vytratí. V elektronickém světě zůstávají informace uložené a je možné se k nim stále dokola vracet, a to nejenom útočníkem. (Kopecký, Krejčí, 2010, s. 6).

Z výzkumu [4] o kybernetické agresi vyplynulo následující:

Tabulka 4. Používání sociálních sítí v jednotlivých věkových kategoriích



Obrázek 2: Používání sociálních sítí v jednotlivých věkových kategoriích

Zdroj [4]

V roce 2018 zažilo 41 % dětí ve věku 8 – 17 let kybernetickou agresi. Nejčastěji (27 %) se jednalo o verbální ublížení prostřednictvím mobilního telefonu či internetu formou ponižování, urážení, zesměšňování či jiného slovního ztrapňování. Následovalo (12,25 %) šíření fotografií prostřednictvím internetu či mobilního telefonu, která měla dotyčného ponížit, zesměšnit, ztrapnit.

K online riziku došlo na platformě Facebook (56,41 %), Facebook Messenger (42,67 %), Instagram (31,65%), SMS/MMS (11,42 %).

Incident z 60 % trval méně než týden. V drtivé většině byli útočníci vrstevníky dítěte – v téměř 30 % se jednalo o spolužáky ze stejné třídy, případně o bývalé kamarády dítěte (16,4 %). Více než v polovině případů byla pachatelem jedna osoba, v pětině případů útočilo více osob, jednalo se o dívky i chlapce.

3.4.9 Kyberstalking

„Kyberstalking lze nazvat nebezpečným pronásledováním. Útočník využívá informační a komunikační technologie k dlouhodobému, opakovanému a stupňovanému kontaktování – pronásledování své oběti, ve které chce úmyslně vyvolat pocit strachu o své soukromí, zdraví nebo život". [9]

3.4.10 Kybergrooming

„Kybergrooming lze vysvětlit jako psychickou manipulaci dítěte dospělým prostřednictvím moderních komunikačních technologií s cílem získat důvěru oběti, vylákat ji na osobní schůzku a zpravidla sexuálně zneužít". [10]

Obětmi jsou nejčastěji děti ve věku 11 – 17 let (častěji dívky), kterým chybí načerpání životní zkušenosti a jejich sociální adaptace a vytváření vlastního identity se u nich teprve vyvíjí. Zpravidla se jedná o děti s nedostatkem sebedůvěry, o děti emočně narušené, děti přehnaně důvěřivé a adolescenti, kteří se s ohledem na vývoj psychologický vývoj sexuální komunikaci nebrání a naopak ji vyhledávají. (Kopecký, Krejčí, 2010, s. 14).

3.4.11 Sexting

„Slovo sexting je spojení slov sex a textování a znamená posílání textového, fotografického, audio a video obsahu se sexuálním podtextem prostřednictvím informačních a komunikačních technologií". [11]

Na internetu jsou přístupné sexuálně laděné obsahy, ať už je jejich vyhledávání záměrné, úmyslné, anebo náhodné. Přitažlivost pro vyhledávání tohoto obsahu je spojena s vývojovou potřebou dospívajících, která je zejména v tomto období aktuální.

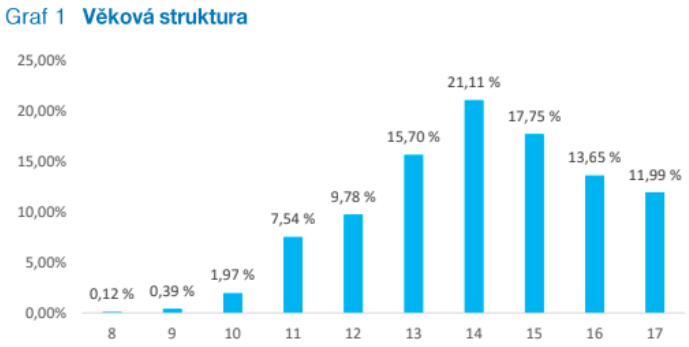
V sborníku studií Děti a online rizika Malíková (2012, s. 148) upozorňuje na teorii Alvina Coopera nazvanou „**triple A engine**", neboli „**motor 3A**" (pojem 3A = zkratka pro anglická slova Accessibility, Affordability, Anonymity; přeloženo do českého jazyka jako přístupnost, dostupnost, anonymita). Sexuálně laděné obsahy jsou v současné době nejen pro dospívající dostupné bez námahy s minimem vynaloženého času. Nepravdivým stvrzením údaje, že uživatel již dosáhl věku 18 let, tak sexuální obsah může shlédnout

i každý neplnoletý uživatel, který již více není poskytovateli kontrolován. Fyzické sexuální dozrávání je mnohdy rychlejší než dozrávání psychické, proto je snaha o vyhledávání informací tohoto typu velice lákavou a v online prostředí poměrně snadnou aktivitou.

Zákon udává věkové omezení 15 let. Posíláním „lechtivých fotografií" dětmi mladšími je již porušováním zákona. (Dočekal a kol., 2019, s. 84). Je to jakýmsi paradoxem České republiky, sexuální styk je od 15 let zákonem povolen, ale až do 18 let je trestné ho jakkoli „dokumentovat" (fotografie, nahrávky) a zveřejňovat. Pro dospívající nemusí být zase až tak škodlivé sledování legální pornografie, neboť může pomáhat překonat stud, zábrany či k uspokojování přirozených potřeb (Eckerová, Dočekal, 2013, s. 86)

Sexting probíhá nejčastěji mezi vrstevníky a partnery, kdy největším rizikem pak bývá ukončení vztahu a protějšek má stále obsah k dispozici. (Dočekal a kol., 2019, str. 84)

Dle výzkumu [12] Univerzity Palackého v Olomouci z roku 2017 vyplynulo, že sexting provozuje více než 15 % dětí ve věku 8-17 let.



Obrázek 3: Věková struktura

Zdroj [12]

Nejčastějším důvodem k rozesílání intimních materiálů jiné osobě bylo upoutání pozornosti, a to u 53 % chlapců a 63 % dívek. Druhým důvodem byl u 50 % chlapců flirt, u dívek činil flirt 61%. Pro realizaci sextingu je nejčastěji využívána platforma Facebook, následovaná Facebook Messengerem a Snapchatem.

Alarmujícím zjištěním bylo, že pouze 38 % respondentů by v případě problémů se sextingem kontaktovalo rodiče, 32,9 % respondentů by se s problémem nesvěřilo nikomu.

Více než 40 % dětí potvrdilo, že v prostředí internetu obdrželo od jiné osoby provokativní erotickou či pornografickou fotografii,

na které je někdo částečně svlečený nebo úplně nahý. 21,5 % dětí přiznalo, že již obdrželo od svého internetového známého erotické či pornografické video.

Z výsledků je patrné, že v případě sextingu je nutné mladistvým nejen neustále připomínat nebezpečí, ale také upevňovat informace o digitálním soukromí a jeho narušování. (Dočekal a kol., 2019, s. 170).

3.4.12 Závěr k online rizikům

Při setkávání s online riziky mohou být uživatelé ovlivňováni různými vlivy, které na ně působí. Jedná se o psychosociální charakteristiku jedince, sociální prostředí, ve kterém se nachází, ať už blízké (rodina, škola, přátelé), ale také kultura, zvyky nebo jemu dostupné příležitosti, které mohou dítě chránit před nebezpečím chránit. (Ševčíková a kol., 2014, s. 11).

Na druhou stranu ale přiměřené užívání sociálních sítí se může na psychice jedince podílet i pozitivně. Snadná a rychlá komunikace bez fyzického kontaktu přináší dobré, povzbudivé pocity. (Dočekal, 2019, s. 83)

Není tedy dobré dívat se na věci jednostranně, uživatelé na sociálních sítích mohou projevovat své názory nebo emoce, kterých při fyzickém kontaktu například z důvodu ostýchavosti či nervozity nejsou schopni.

4 KYBERBEZPEČNOST – NAUKA O BEZPEČNÉM POHYBU

4.1 Kyberbezpečnost a rodina

JUDr. Miroslav Antl v knize Bezpečnost dětí na internetu uvádí že *„Z českého zákona o rodině vyplývá, že rozhodující úlohu ve výchově dětí mají rodiče*". (Eckerová, Dočekal, 2013, s. 9).

Regulují rodiče dětem užívání technologií? Pokud ano, jakými způsoby? Mají přehled o jejich aktivitách v online prostředí? Mají přístup k nežádoucím obsahům?

Do výzkumu v roce 2018 [5] bylo zapojeno 1093 rodičů ve věku 25 – 64 let (86,5 % žen, 13,2 % mužů). Z výzkumu vyplynulo, že s rostoucím věkem dítěte rodiče omezují jeho aktivity méně (7 % 16letých teenagerů, 4 % 17letých teenagerů).

Jako nejčastější formu prevence (76 %) volí rodiče rozhovor s dítětem o nebezpečí internetu, ve kterém rodič seznamuje dítě s riziky.

Více než polovina rodičů uvedla, že v online prostředí nic rizikového nezažila. Přesto však téměř třetina rodičů uvedla, že na internetu zažila slovní urážky, ponižování či zesměšňování. Skoro 18 % rodičů uvedlo, že se v online prostředí stali terčem podvodu.

Více než 80 % rodičů potvrdilo, že mají základní uživatelské dovednosti (napsat, odeslat, přeposlat e-mail; vyhledat dopravní spojení, naplánovat trasu, ověřovat informace v online prostředí, přeložit text do cizího jazyka).

Problém však nastal v oblasti bezpečnosti, kdy 46 % rodičů uvedlo, že umí nastavit bezpečné vyhledávání k blokování nevhodného obsahu ve vyhledávači Google. Pouze 36 % rodičů umí nastavit režim omezeného vyhledávání na YouTube. Pokročilé nastavení mobilního telefonu jako je automatické zálohování, propojení mobilu s online účtem apod. ovládá 39 % rodičů.

Vzhledem k tomu, že děti jsou v kontaktu s mobilním telefonem již od útlého věku, přináší výše uvedený výzkum značně znepokojující data.

4.2 Kyberbezpečnost a škola

Do výzkumu Český učitel ve světě technologií z roku 2020 prováděného Universitou Palackého v Olomouci se zapojilo 2165 pedagogů z celé České republiky ve věku 21 – 78 let.

45 % učitelů potvrdilo, že mají učitelské počítače zabezpečeny proti nevhodnému obsahu z internetu (především pornografii). 23,14 % učitelů uvedlo, že počítače proti nevhodnému obsahu zabezpečeny nemají. Většina správců školní počítačové sítě (96,6 %) uvedla, že jejich škola využívá aktivní firewall.

Téměř polovina dotazovaných učitelů uvedla, že jejich školní WIFI k dispozici jak žákům, tak učitelům.

Co se týče regulace používání mobilních telefonů žáky ve škole, 35,8 % učitelů uvedlo, že v jejich škole je mobilní telefon o přestávce zakázán. 48,68 % učitelů uvedlo, že nevědí, k jakým aktivitám jejich žáci mobilní telefony o přestávkách využívají. 41,8 % učitelů potvrdilo, že jejich žáci využívají moderní technologie k podvádění. [13]

Dle poskytnutého rozhovoru profesora Michaela Šebka pro knihu Dítě v síti *„jsou naše školy už sto let stále stejné. Pořád učí hlavně číst, psát a počítat, což je informatika 19. století. Číst, ale ne rozumět, počítat z hlavy jako stroj.*" (s. 186).

Potřeba učit děti ve škole nikoli fakta, data a informace, která si můžou snadno vyhledat, ale učit rozumět, analyzovat, chápat. Podporovat v žácích flexibilitu, tvořivost, umění komunikovat a sám se vzdělávat (Dočekal a kol., 2019, s. 186-187).

4.3 Osvěta – film V Síti, V Síti: Za školou

Dokument byl natočen ve dvou verzích. První, necenzurovaná, je určena dospělému publiku. Druhá, cenzurovaná, nazvaná V síti: Za školou, se snaží spíše než dítě šokovat, přiblížit prostřednictvím hereckých postav rizika online komunikace. Orientace filmu je cílena na dívky, které vstupují do puberty.

Film nepopisuje rizika, ale pomocí příběhů tří dívek provází světem seznamek a sociálních sítí. Zároveň ale dokumentuje manipulátorské strategie a poukazuje na tenkou linii mezi přechodem z online světa do světa reálného a na následky, které může tento přechod mít. [14]

Co o filmu řekl režisér?

Vít Klusák (režisér V Síti):

„Ti muži jsou především neskonale sobečtí. Vůbec jim nedochází, jak hlubokou rýhu můžou v těch dětských duších zanechat na roky dopředu." [15]

„Na podzim 2017 nás oslovili ze společnosti O2, která si co dva roky nechává zpracovávat studii, jak se chovají české děti v on-line

prostředí. Ze vzorku 27 tisíc dětí vyšla čísla, že pětina dětí zažila, že před nimi někdo během videohovoru masturboval a podobně". [16]

„Sociální sítě jsou především asociální, protože je vytvořili lidé, kteří měli problém se potkávat naživo. Bylo by dobré dětem zdůrazňovat, že sociální sítě nejsou dobrý způsob pro navazování vztahů. V médiích i ve škole bychom měli víc mluvit o tom, jak fungují." [16]

Jak se vyjádřila jedna z hlavních hereček?

Tereza Těžká (herečka V Síti):

„S internetem přišla i spousta dobrých věcí, ale určitě narušil nějaké morální hodnoty, lehce se tam dělají přešlapy a překračují hranice toho, co si člověk dovolí. Spousta lidí si neuvědomuje, že čím dál víc se naše virtuální realita stává naší skutečnou, že nás ovlivňuje to, co na sociální sítě přidáváme. Vytváříme si tam svou identitu, přes niž nás lidé vnímají. Takže je důležité se chránit. V reálu taky nejdu k cizímu člověku, abych mu řekla, kde mám klíče od bytu." [16]

Film vyvrací množství stereotypů o sexuálních predátorech a také o prevenci rizikového chování

1) *Pachatel je dospělý starý muž* – film ukázal, že pachateli nebyli pouze uživatelé středního a seniorského věku, ale i velmi mladí lidé (studenti či čerství absolventi různých škol);
2) *Internet je pro děti zlo* - nejenom autoři projektu, ale i edukativní verze filmu V síti: Za školou hovoří o tom, že internet je pozitivní nástroj a jeho výhody převažují nad negativními jevy;
3) *Jakmile jsme na Internetu, sesypou se na nás predátoři* – film popisuje komunikaci v rámci několika vybraných platforem (uvnitř různých druhů diskusních skupin), netvrdí, že to funguje takto vždy, kdykoli a kdekoli (častější je setkání s agresí či podvodem);
4) *Rodiče by měli na film reagovat zákazem* – tvůrci upozorňují ve všech doprovodných materiálech, že toto je naprostá hloupost;
5) *Data, která film prezentuje, jsou přehnaná* – data jsou čerpána ze dvou rozsáhlých studií [4] a [12], jež byly realizovány na vysokých vzorcích a některé výzkumné otázky byly v rámci online rizik relevantní (např. 20,58 % dětí potvrdilo, že zvou své internetové kamarády na osobní schůzku – nejde tak primárně o nebezpečný online kontakt) [17].

5 OCHRANA A ZABEZPEČENÍ ZAŘÍZENÍ

S neustálým vývojem kyberprostoru se pochopitelně vyvíjí i hackerské útoky nejenom do zařízení, ale i do profilů uživatelů. Proto je potřeba věnovat zvýšenou pozornost zabezpečení vlastního zařízení ale i samotných účtů. Existuje spousta programů k prolomení zabezpečení a přístupových kódů.

5.1 Základní pravidla používání zařízení

Prvotním krokem je zabezpečit připojení k Internetu, na který již v současné době bývá připojen nejen počítač, ale i mobil, tablet, chytrá televize, herní konzole a dalších zařízení stále přibývá. Nejobvyklejším zařízením pro vytvoření Wi-Fi je router. Změnou, od výroby stanovených přístupových údajů docílíme toho, že nás útočník nebude mít šanci nikterak sledovat, krást data či páchat trestnou činnost. Dalším krokem je nejenom pravidelná aktualizace operačního systém, který je součástí zařízení, ale také pečlivá aktualizace softwaru, tedy programů, a to zejména internetových prohlížečů (útok ve smyslu pharming, phishing apod.). Neodmyslitelné je aktivní užívání antivirového programu, chránící před viry a malwarem, stejně tak jako Firewall, který bývá v současné době již do Microsoft Windows automaticky integrován. Abychom předcházeli ztrátě dat, ke které dochází nejenom při kyberútoku, napadení virem, ale i např. poškozením pevných disků je důležité pravidelně zálohovat data. [18]

Pharming je podvodná metoda používaná na Internetu k získání citlivých údajů od obětí útoku. Výkladový slovník kybernetické kriminality ji dále definuje následovně: *„Principem je napadení DNS a přepsání IP adresy, což způsobí přesměrování klienta na falešné stránky internetbankingu, e-mailu, sociální sítě, atd. po zadání URL do prohlížeče. Tyto stránky jsou obvykle k nerozeznání od skutečných stránek banky a ani zkušení uživatelé nemusejí poznat tuto záměnu.*“ (s. 69)

Phishing („rybaření“, „rhybaření“, „házení udic“). Dle výkladového slovníku kybernetické kriminality se jedná o podvodnou metodu, *„usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datům atd.)*“ (s. 70)

Malware je škodlivý software, *„který se šíří z počítače na počítač tím, že se připojí k jiným aplikacím. Následně může působit nežádoucí*

a nebezpečnou činnost. Má v sobě obvykle zabudován mechanismus dalšího šíření či mutací" (Jirásek a kol., 2013, s. 82)

5.2 Problematika hesel

Chraň svá tajemství dobrými hesly a chraň sám/sama sebe bezpečným chováním na internetu.

„Tvoje heslo je jako klíč od domu. Když je ten klíč kvalitní, nikdo si bez něj dveře do domu neotevře. Bude-li ale špatně zhotovený, nebude mít zloděj s otevřením dveří moc práce" (Kohout, Kubíčková, 2017, s. 12)

Jednou z největších chyb současných uživatelů Internetu je užívání stejného hesla pro většinu webových služeb. Je nutné dodržovat zásady pro vytváření hesla, a to: *„délka hesla je minimálně 8 znaků (doporučení 12 – 14), kombinace číslic, malých a velkých písmen a speciálních znaků (!, #, $, & apod.)*". [19]

Existuje velké množství programů, které se prolamováním hesel zabývají.

Důležité je pamatovat na to, že přihlašování se z veřejných zařízení je nebezpečné, jelikož tato zařízení mohou být vybavena monitorovacími programy, které veškerý obsah komunikace dokonale zaznamenají. [19]

5.3 Trestní zákoník

„V 15 – 18 letech se dítě nazývá mladistvým, stává se odpovědným za přestupek a je-li dostatečně rozumově a mravně vyspělé, aby mohlo rozpoznat protiprávnost svého jednání nebo ho ovládat, pak i trestně odpovědným" (Eckertová, Dočekal, 2013, s. 190)

Trestní zákoník č. 306/2009, kterým se mění zákon č. 40/2009 Sb. účinný od 1.1.2010 má v sobě pochopitelně implementovánu i kybernetickou kriminalitu. Níže uvádím výseč nejdůležitějších paragrafů souvisejících s možnými riziky plynoucí z pohybu v kyberprostoru.

Kyberšikana:

- § 146 – ublížení na zdraví;
- § 171 – omezování osobní svobody;
- § 175 – vydírání;
- § 184 – pomluva;
- § 205 – krádež;
- § 352 – násilí proti skupině obyvatel a jednotlivci;
- § 353 – nebezpečné vyhrožování;

- § 354 – nebezpečné pronásledování.

Kybergrooming:

- § 168 – obchodování s lidmi;
- § 171 – omezování osobní svobody;
- § 175 – vydírání;
- § 187 – pohlavní zneužívání;
- § 201 – ohrožování výchovy dítěte;
- § 201 – podvod;
- § 353 – nebezpečné vyhrožování;
- § 354 – nebezpečné pronásledování.

Sexting:

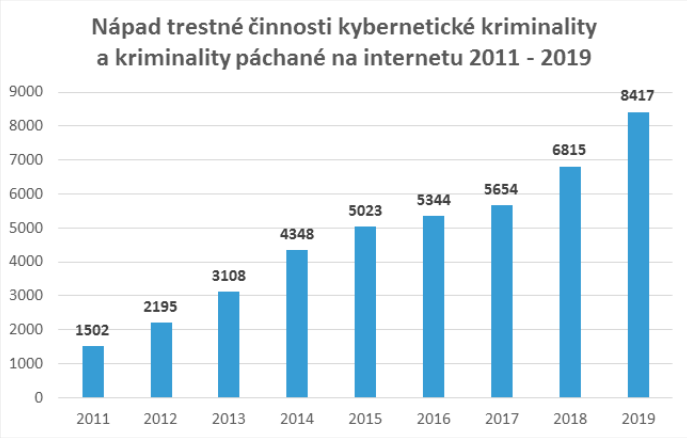
- § 171 – omezování osobní svobody;
- § 185 - znásilnění;
- § 187 – pohlavní zneužití;
- § 192 – výroba a jiné nakládání s dětskou pornografií;
- § 193 – zneužití dítěte k výrobě pornografie;
- § 201 – ohrožování výchovy dítěte;
- § 354 – nebezpečné pronásledování.

Zneužívání osobních údajů:

- § 175 – vydírání;
- § 177 – útisk;
- § 180 – neoprávněné nakládání s osobními údaji;
- § 181 – poškození cizích práv;
- § 184 – pomluva;
- § 209 – podvod;
- § 354 – nebezpečné pronásledování [20].

5.4 Statistiky PČR

Z níže uvedené tabulky „Nápadu trestné činnosti kybernetické kriminality na internetu v letech 2011 – 2019" je patrný vzrůstající počet trestních činů páchaných v kyberprostoru. Nejpočetněji (více než polovina všech evidovaných skutků) jsou zastoupeny podvodná jednání obsahující též pojistné podvody, následuje hacking. [21]



Obrázek 4: Nápad trestné činnosti a kybernetické kriminality páchané na internetu 2011 - 2019

Zdroj [21]

6 JCE CENTRA

Budovat bezpečnostní povědomí a základní znalosti o komunikaci v online prostředí je nezbytné. Jedním z možných řešení výuky kyberbezpečnosti a informační bezpečnosti je zavést nejpozději na střední školy nový trojúrovňový koncept v podobě Juniorních center excelence (dále jen JCE), protože český model vzdělávání a výchovy v oblasti kybernetické bezpečnosti NEODPOVÍDA aktuálním požadavkům a trendům (Sedláček, 2021, s. 6).

JCE nemůže být každá škola s ohledem na technické vybavení, na kvalifikovaný pedagogický sbor, ale každá škola může s pomocí center zavést a zkvalitňovat výuku.

Vznik center si klade za cíl zajistit výuku informační bezpečnosti ve všech RVP, což by následně vedlo ke zvýšení gramotnosti informační společnosti, a to vytvářením návyků pro zodpovědné chování v kyberprostoru. Dalším cílem je udržení konkurenceschopnosti České republiky, neboť má v této oblasti již vybudováno významné postavení. [22]

Průlom v legislativě nastal 1.1.2015, kdy vešel v účinnost Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Tímto zavedením byl přístup ke kyberbezpečnosti měněn nejen z organizačních a technických opatření, v rovině právní (i povinné subjekty mají zákonnou povinnost řešit kyberbezpečnost a přijmout odpovídající kroky, aby zabránily bezpečnostním rizikům) a v oblasti vzdělávání. S tímto zákonem souvisí i známé evropské nařízení o ochraně osobních údajů (GDPR = General Data Protection Regulation) platné od 25.5.2018. [23]

Národní strategie kybernetické bezpečnosti za období 2015-2020 v části F konstatovala: „*Navyšovat povědomí a gramotnost v otázkách kybernetické bezpečnosti jak u žáků a studentů základních a středních škol, tak i u široké veřejnosti, respektive koncových uživatelů, pomocí podpory iniciativ a osvětových kampaní, pořádáním konferencí pro veřejnost apod. Modernizovat stávající vzdělávací programy na základní a středoškolské úrovni a podporovat na vysokoškolské úrovni nové studijní programy, které budou přímo vzdělávat experty na kybernetickou bezpečnost.*“ [24]

Národní strategie kybernetické bezpečnosti na období let 2021-2025 pro oblast vzdělávání a osvěty i nadále „*klade důraz na projekty, které cílí na osvojení návyků potřebných pro bezpečný pohyb na internetu a používání digitálních technologií*“. Tyto projekty jsou nově ve strategii rozšířeny, a to již od úrovně mateřských škol.

Další novinkou bude vzdělávání vybraných cílových skupin, konkrétně se jedná o pedagogické pracovníky a zaměstnance veřejné správy. Další ohroženou skupinou jsou senioři.

Odolný systém zajištění kybernetické bezpečnosti [25, s. 19]

Obrázek 5: Odolný systém zajištění kybernetické bezpečnosti

Zdroj [25]

Ke dni 5.8.2020 je stav JCE center v ČR následující:

- SŠ IPV Čichnova Brno (od roku 2017);
- SPŠ Smíchovská Praha (od roku 2017);
- SŠ IS Dvůr Králové nad Labem (od roku 2018).(Sedláček, 2021, s. 20)

PRAKTICKÁ ČÁST

7 VÝZKUMNÉ ŠETŘENÍ

7.1 Výzkumné cíle

Cílem empirické části bakalářské práce je zjištění, jaký je rozsah znalostí studujících vybrané střední školy o rizicích vyplývajících z aktivního užívání sociálních sítí a jaká je jejich připravenost používat tyto znalosti v praxi. Součástí výzkumu bude také zjištění, zda, kde a jak probíhá osvěta bezpečného pohybu na sociálních sítích, kým je uskutečňována, zda ji studující využívají. Zjištění, zda studenti vhodně zabezpečují svá zařízení a vytvořené profily celou sondáž dokreslí.

7.2 Výzkumný vzorek a výzkumná metoda

S ohledem na cíl bakalářské práce byli vybráni studenti prvních až čtvrtých ročníků střední odborné školy v okrese Rakovník. Z celkového počtu 111 odpovědí se jedná o 74 dívek ve věku 16 - 18 let a 37 chlapců ve věku 17 - 18 let.

Vzhledem k probíhající pandemické situaci a nastavenému distančnímu vzdělávání středoškolských ročníků byl výzkum realizován online v podobě anonymního dotazníkového šetření.

Dotazník byl vytvořen na platformě Survio.com, s úvodním rozlišením na pohlaví dotazovaného a věk. Následují otázky týkající se účelu zřízení profilu, nejčastějšího důvodu užívání, nejpoužívanějších sociálních sítích, otázky na téma bezpečného pohybu a rizik v kyberprostoru, zkušenosti s riziky a ochranou používaných zařízení a vytvořených profilů. Celkem se jedná o 18 otázek. Úplné znění dotazníku je uvedeno v příloze č. 1.

Šetření probíhalo v březnu roku 2021.

7.3 Výzkumné otázky a hypotézy

Dotazník je rozdělen do následujících částí:

- charakteristika respondentů;
- informace o užívání sociálních sítí;
- bezpečnost a znalosti s ní spojené, jejich užití v praxi.

Část 1 – základní charakteristika respondentů z hlediska věku a pohlaví a **informace o užívání sociálních sítí**, kterým odpovídají dotazníkové položky 1 – 6. Zajímala nás četnost a rozsah pohybu

dotazovaných studentů na internetu a sociálních sítích. Položky odpovídají hypotézám 1 a 2.

H1: Všichni dotazovaní studenti bez rozdílu věku a pohlaví tráví na sociálních sítích minimálně dvě hodiny denně.

Formulace hypotézy 1 byla odvozena z výzkumné otázky:

- Kolik času denně tráví studenti na sociálních sítích?

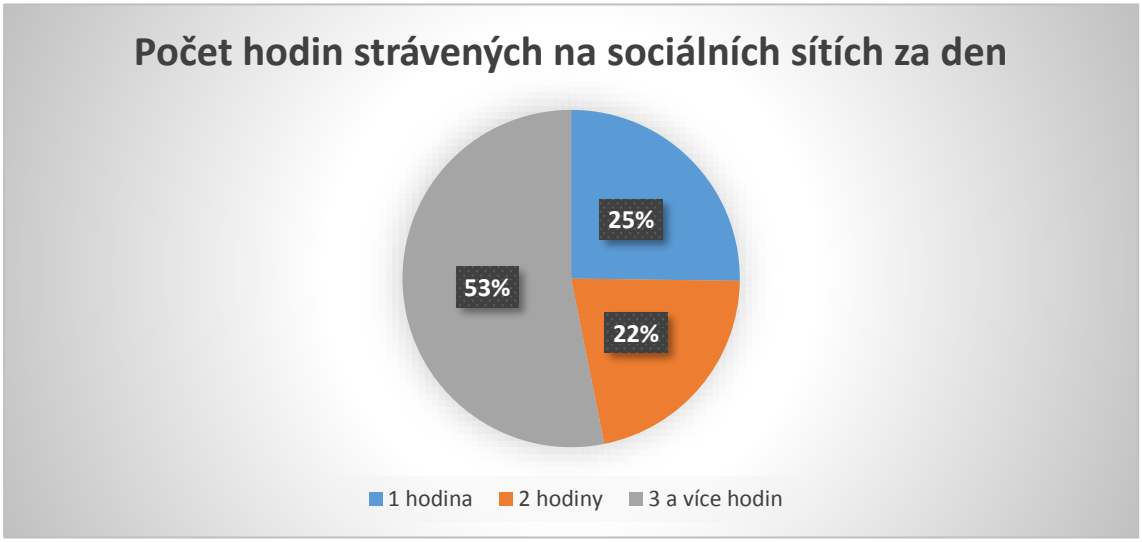
K ověření H1 byly přiřazeny položky č. 1, 2 a 5.

1. Pohlaví

2. Věk

5. Kolik času za den trávíte na sociálních sítích?

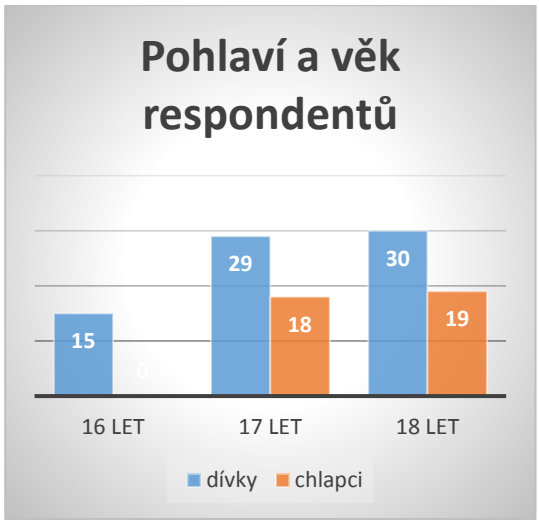
Stanovená hypotéza H 1 byla vyvrácena. 25 % dotazovaných studentů tráví na sociálních sítích i méně než dvě hodiny (graf č. 1).



Graf 1: Počet hodin strávených na sociálních sítích za den

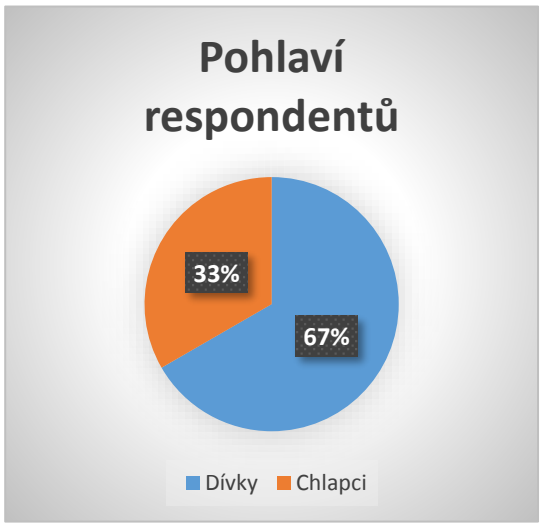
Zdroj: vlastní zpracování

Otázky č. 1, 2 a 5 jsou vyhodnoceny a znázorněny v grafech č. 2 – 4.



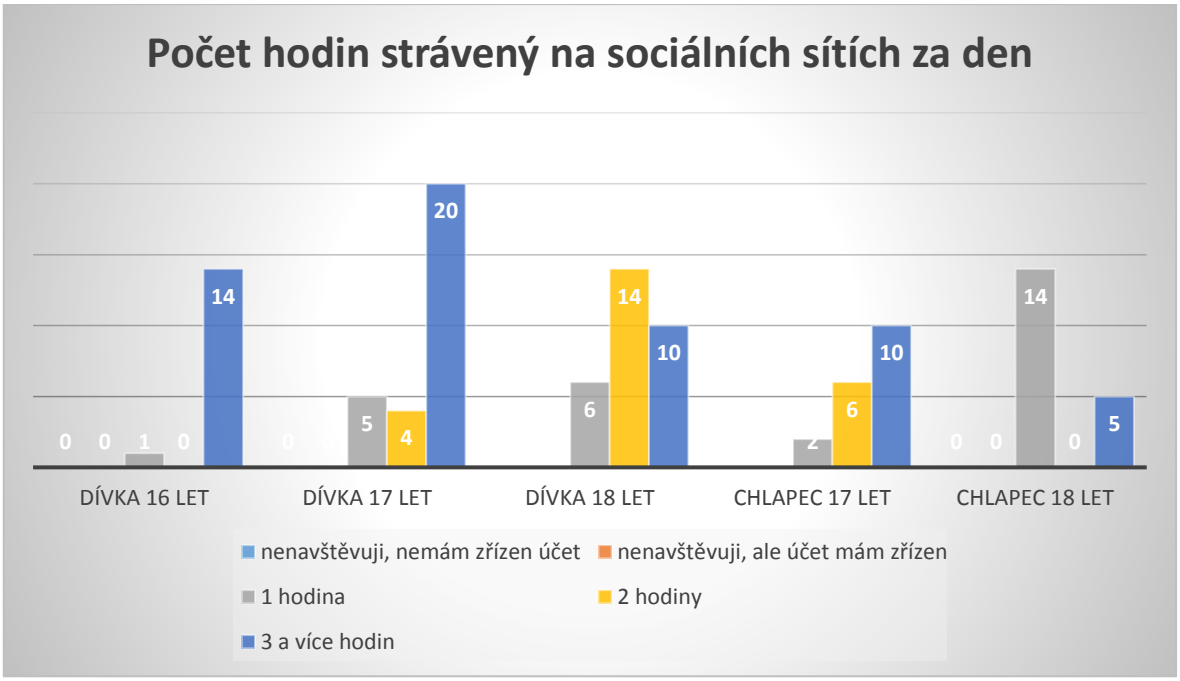
Graf 2: Pohlaví a věk respondentů

Zdroj: vlastní zpracování



Graf 3: Pohlaví respondentů

Zdroj: vlastní zpracování



Graf 4: Počet hodin strávený na sociálních sítích za den

Zdroj: vlastní zpracování

H2: Studenti bez ohledu na věk a pohlaví využívají sociální sítě především ke komunikaci s kamarády.

Formulace hypotézy 2 byla odvozena z níže uvedených výzkumných otázek:

- *Jsou chlapci i dívky stejně aktivní na sociálních sítích?*
- *Jaké sociální sítě nejčastěji studenti využívají?*
- *Jaká je forma/způsob aktivity studentů na sociálních sítích?*
- *K čemu sociální sítě primárně využívají?*

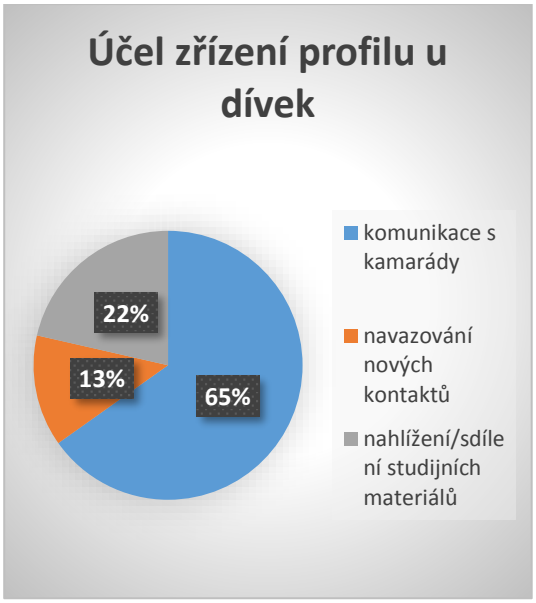
K vyhodnocení H2 byly použity odpovědi na položky č. 3, 4 a 6.

3. Na jakých sociálních sítích máte založen účet, případně je aktivně využíváte?

4. Za jakým účelem jste si účet na sociální síti vytvořili?

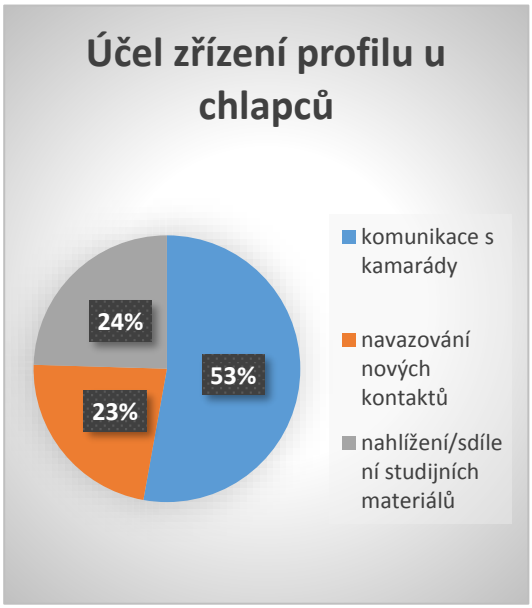
6. Jak byste se charakterizovali v rámci aktivity na sociálních sítích

Chlapci i dívky využívají sociální sítě převážně ke komunikaci s kamarády (viz graf č. 5 a 6), dívky jsou na sociálních sítích aktivnější oproti chlapcům (graf č. 7 a 8). **Hypotéza H2 byla potvrzena.**



Graf 5: Účel zřízení profilu u dívek

Zdroj: vlastní zpracování



Graf 6: Účel zřízení profilu u chlapců

Zdroj: vlastní zpracování

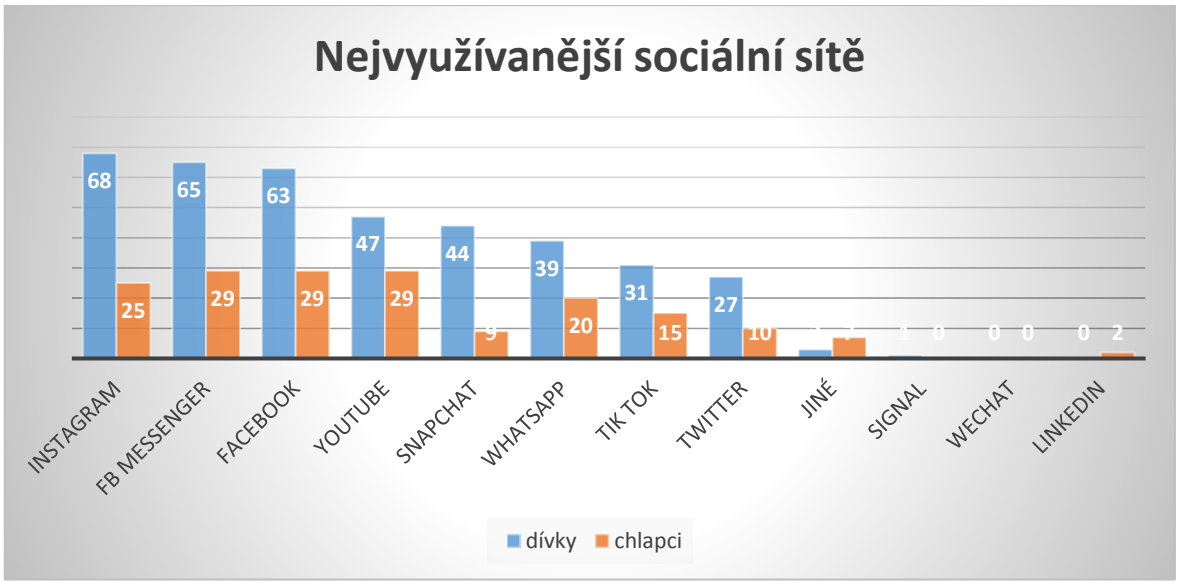
Graf 7: Aktivita na sociálních sítích u dívek

Zdroj: vlastní zpracování

Graf 8: Aktivita na sociálních sítích u chlapců

Zdroj: vlastní zpracování

Otázka č. 3 je vyhodnocena a znázorněna v grafu č. 9.



Graf 9: Nejvyužívanější sociální sítě

Zdroj: vlastní zpracování

Část 2 – bezpečnost na síti, které odpovídají položky 7 – 10 dotazníku se vztahem k H3:

Hypotéza 3 byla konkretizována z těchto výzkumných otázek:

- *Kdo zprostředkoval studentům informace o bezpečném chování na sociálních sítích?*
- *Jsou studenti průběžně informováni/poučováni o tom, jak se na sítích bezpečně pohybovat?*
- *Je hlavním zdrojem poskytování informací škola, rodina nebo kamarádi?*
- *Provádí rodiče aktivně kontrolu pohybu svých dětí na soc. sítích?*

H3: Povědomí o bezpečném pohybu na sociálních sítích před zřízením profilu získávají studenti nejvíce od svých kamarádů/vrstevníků.

K vyhodnocení H3 byly použity odpovědi získané z položek č. 7 – 10.

7. Byli jste v době, kdy jste si zřizovali účet/profil na jakékoli sociální síti informováni/poučeni jak se ní bezpečně pohybovat?

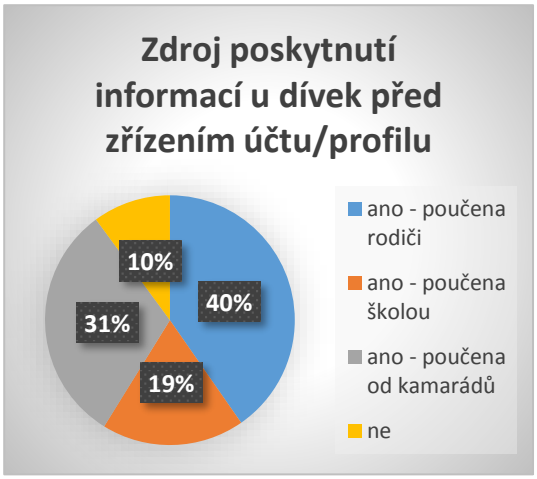
8. Četli jste knihu/příručku/jiný materiál anebo shlédli film od doby zřízení Vašeho účtu/profilu týkající se bezpečného pohybu na sociálních sítích?

9. Pokud ano, kdo Vám materiály poskytl?

10. Nahlížejí rodiče do Vašeho profilu příp. do komunikační aplikace?

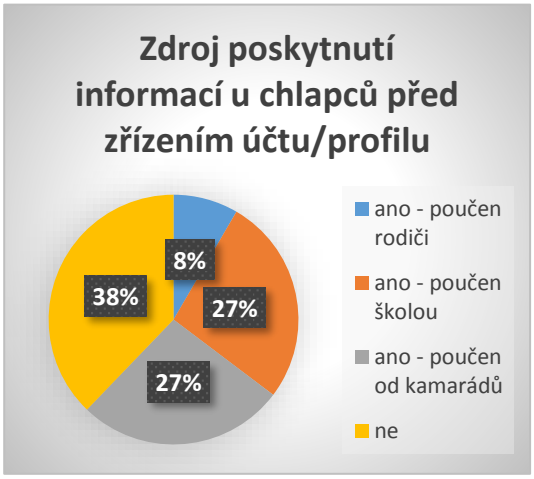
Nejvíce dívek odpovědělo, že bylo před zřízením účtu/profilu poučeno rodiči, nejvíce chlapců uvedlo, že poučeni nebyli vůbec (graf č. 10 a 11). Více než polovina dotazovaných dívek i chlapců konstatovala, že již shlédla/přečetla materiál týkající se bezpečného pohybu na sociálních sítích (graf č. 12 a 13) - tento materiál byl dívkám i chlapcům poskytnut převážně kamarády (graf č. 14 a 15).

Na základě vyhodnocení těchto položek můžeme konstatovat, že **H3 byla vyvrácena.**



Graf 10: Zdroj poskytování informací před zřízením účtu u dívek

Zdroj: vlastní zpracování



Graf 11: Zdroj poskytování informací před zřízením účtu u chlapců

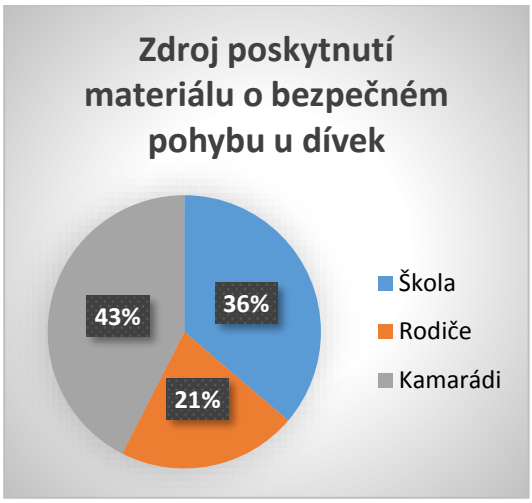
Zdroj: vlastní zpracování

Graf 12: Shlédnutí/přečtení materiálu o bezpečném pohybu u dívek

Zdroj: vlastní zpracování

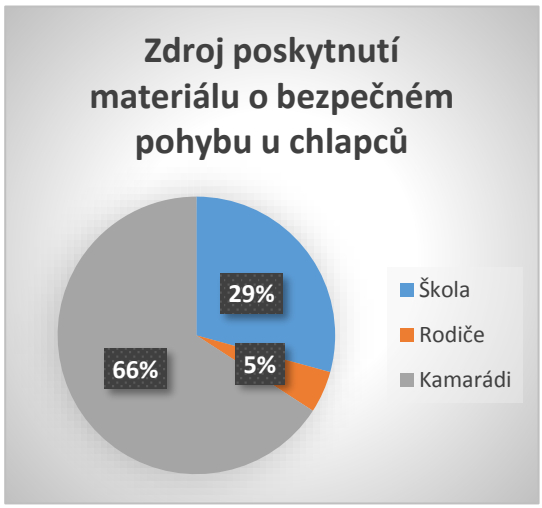
Graf 13: Shlédnutí/přečtení materiálu o bezpečném pohybu u chlapců

Zdroj: vlastní zpracování



Graf 14: Zdroj poskytnutí materiálu o bezpečném pohybu u dívek

Zdroj: vlastní zpracování



Graf 15: Zdroj poskytnutí materiálu o bezpečném pohybu u chlapců

Zdroj: vlastní zpracování

Otázka č. 10 je vyhodnocena a znázorněna v grafu č. 16 a 17.

Graf 16: Nahlížejí rodiče dívkám do komunikační aplikace

Zdroj: vlastní zpracování

Graf 17: Nahlížejí rodiče chlapcům do komunikační aplikace

Zdroj: vlastní zpracování

Část 3 – znalost bezpečnosti a jejich užití v praxi, které odpovídají položky č. 11 – 15. K této části dotazníku je přiřazena hypotéza 4 a 5.

H4: Většina dotazovaných studentů se již setkala alespoň s jedním z rizik hrozících užíváním sociálních sítí - tato rizika by nejčastěji řešili s kamarády nebo rodiči.

Hypotéza č. 4 byla odvozena z níže uvedených výzkumných otázek:

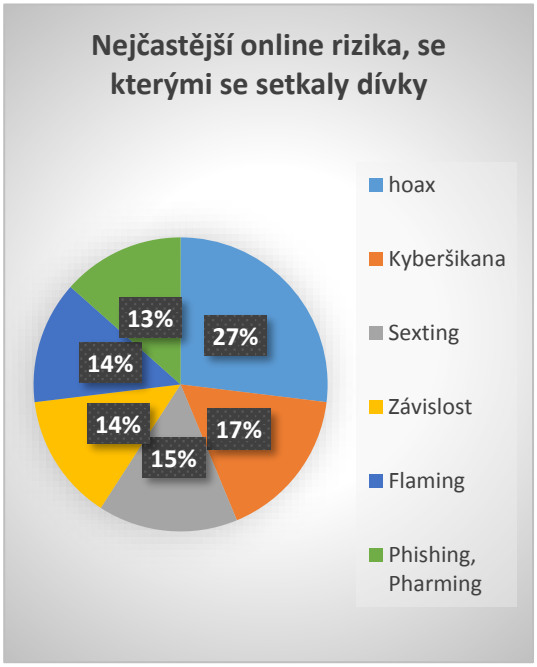
- *S jakými riziky se žáci již setkali?*
- *Komu by se s problémem svěřili?*

K vyhodnocení byly použity odpovědi na položky č. 11 a 12.

11. Setkali jste se již s riziky plynoucími z pohybu na sociálních sítích? Pokud ano, jakými?

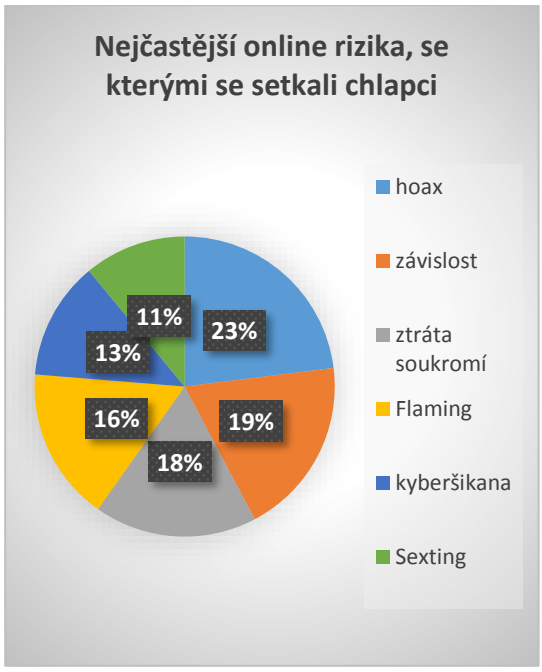
12. S kým jste riziko řešili, případně s kým byste riziko řešili, pokud by nastalo?

Hypotéza H4 byla potvrzena. Oslovení respondenti se již alespoň s jedním z online rizik setkali (graf č. 18 a 19) a nejčastěji by online riziko řešili dívky s rodiči a chlapci s kamarády (graf č. 20 a 21).



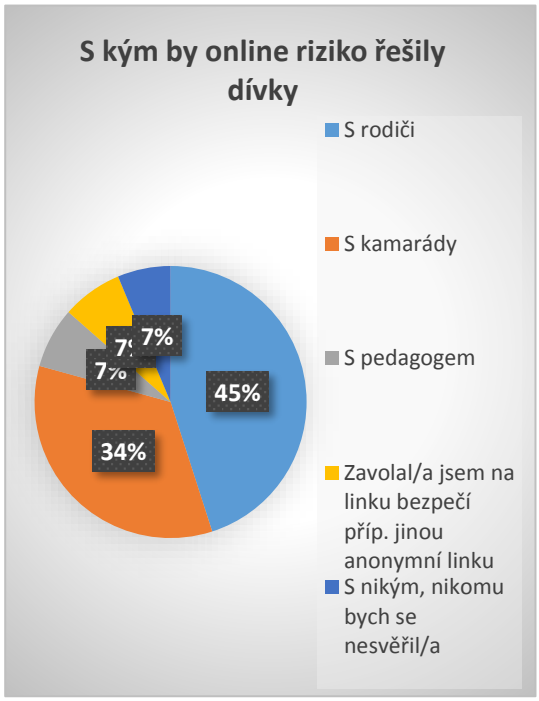
Graf 18: Nejčastější online rizika, se kterými se setkaly dívky

Zdroj: vlastní zpracování



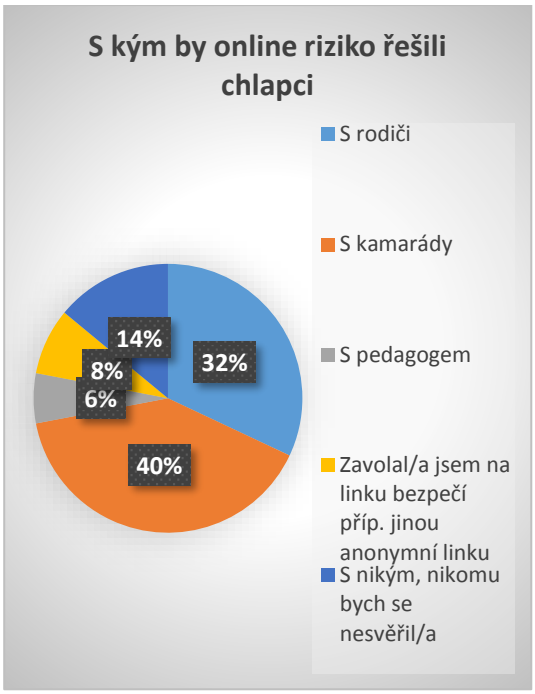
Graf 19: Nejčastější online rizika, se kterými se setkali chlapci

Zdroj: vlastní zpracování



Graf 20: S kým by online riziko řešily dívky

Zdroj: vlastní zpracování



Graf 21: S kým by online riziko řešili chlapci

Zdroj: vlastní zpracování

H5: Alespoň polovina dotazovaných studentů již někdy vložila na sociální sítě materiál s nevhodným obsahem.

Hypotéza č. 5 byla odvozena z níže uvedených výzkumných otázek:

- *Jsou studenti obeznámeni s tím, že jakýkoli obsah, který do virtuálního prostředí vloží, tam zůstane zachován?*
- *Jsou studenti obeznámeni s tím, že jakýkoli nevhodný obsah zaslaný do virtuálního prostředí může být zneužit?*
- *Zabývají se studenti prověřováním nových kontaktů?*

K vyhodnocení byly použity odpovědi na položky č. 13 - 15.

13. Víte, co znamená pojem digitální stopa?

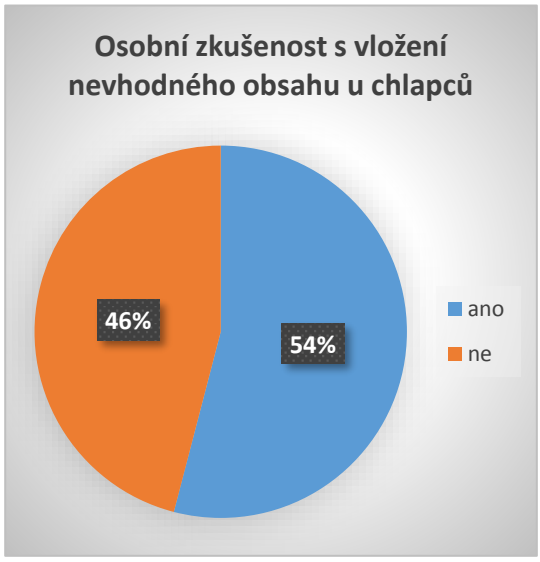
14. Zaslali jste někomu nebo vložili na sociální sítě nějaký obsah (fotografii/video/komentář), který byste rádi vzali zpět?

15. Jakým způsobem prověřujete nové kontakty na sociálních sítích?

Hypotéza H5 byla potvrzena. Ze získaných dat vyplývá, že téměř polovina dívek a více než polovina chlapců již někdy na sociální sítě vložila materiál s nevhodným obsahem (graf č. 22 a 23).

Graf 22: Osobní zkušenost s vložením nevhodného obsahu u dívek

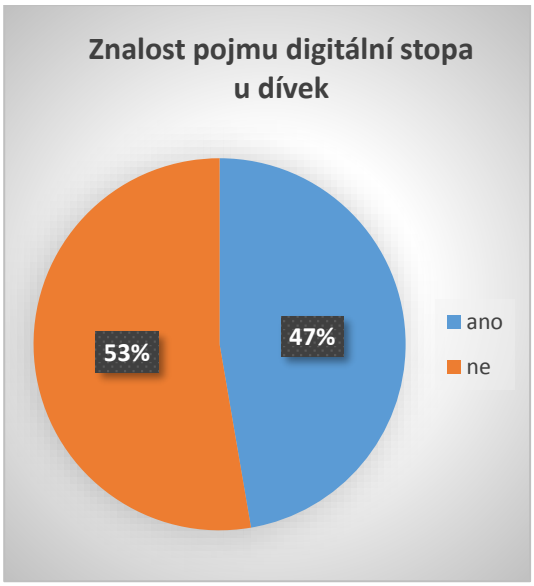
Zdroj: vlastní zpracování



Graf 23: Osobní zkušenost s vložením nevhodného obsahu u chlapců

Zdroj: vlastní zpracování

Otázky č. 13 a 15 jsou vyhodnoceny a znázorněny v grafu č. 24 - 27.

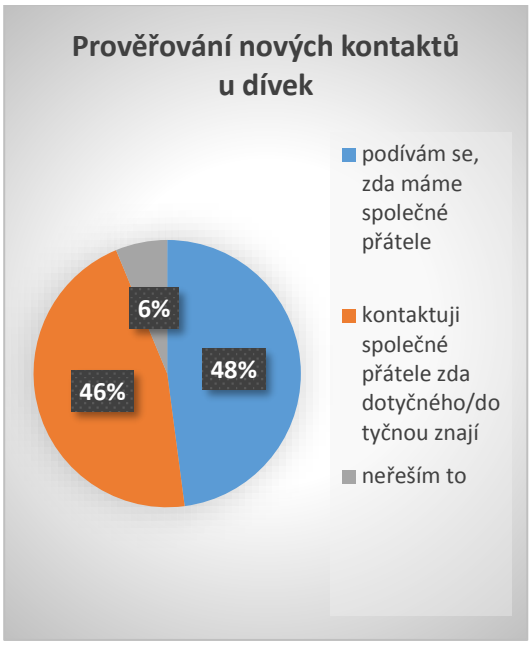


Graf 24: Znalost pojmu digitální stopa u dívek

Zdroj: vlastní zpracování

Graf 25: Znalost pojmu digitální stopa u chlapců

Zdroj: vlastní zpracování



Graf 26: Prověřování nových kontaktů u dívek

Zdroj: vlastní zpracování

Graf 27: Prověřování nových kontaktů u chlapců

Zdroj: vlastní zpracování

Část 4 – ochrana a zabezpečení, které odpovídají položky č. 16 - 18.

Ke zjištění, do jaké míry si studenti zajišťují vlastní bezpečnost na síti, sloužila poslední část dotazníku v souvislosti s poslední hypotézou výzkumného šetření.

H6: Většina dotazovaných studentů má svá zařízení i profil zabezpečen alespoň jedním ze základních zabezpečení.

H6 byla konkretizována z níže uvedených výzkumných otázek a byly k ní přiřazeny položky č. 16 - 18 dotazníku

- *Mají studenti zabezpečena svá zařízení? Jakým způsobem?*
- *Mají studenti zabezpečen svůj profil na sociální síti?*
- *Vědí studenti jak postupovat, pokud se jim někdo naboural do účtu/profilu?*

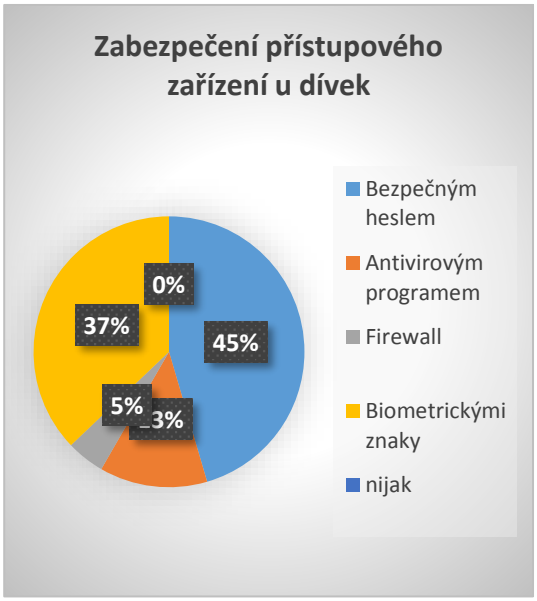
K vyhodnocení byly použity odpovědi na položky č. 16 - 18.

16. Jak máte zabezpečena svá zařízení, které používáte při přístupu na sociální sítě?

17. Jak máte zabezpečen svůj profil?

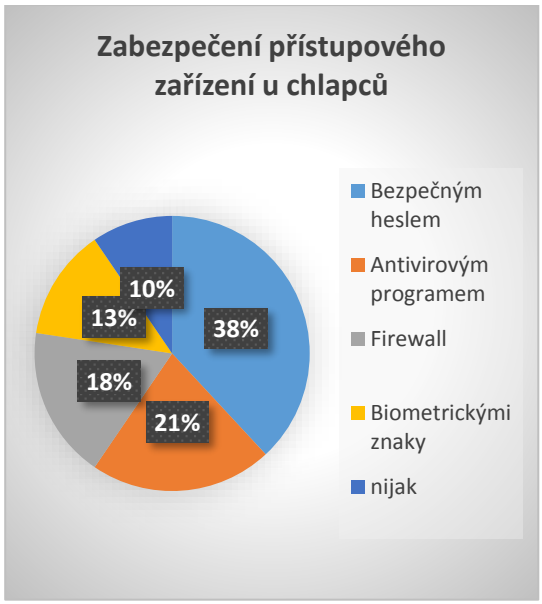
18. Jak byste postupovali v případě nabourání do Vašeho profilu na sociální síti?

Jak vyplývá z níže uvedených dat, respondenti mají svá zařízení (graf č. 28 a 29) i profily (graf č. 30 a 31) zabezpečeny alespoň jedním ze základních zabezpečení. **Hypotéza H6 byla tedy potvrzena.**



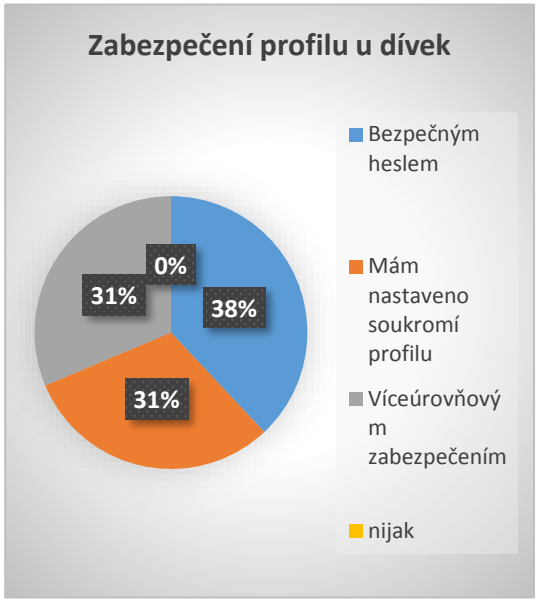
Graf 28: Zabezpečení přístupového zařízení u dívek

Zdroj: vlastní zpracování



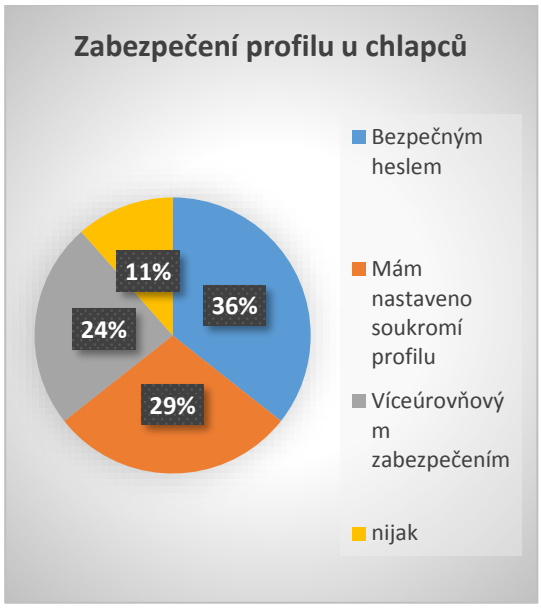
Graf 29: Zabezpečení přístupového zařízení u chlapců

Zdroj: vlastní zpracování



Graf 30: Zabezpečení profilu u dívek

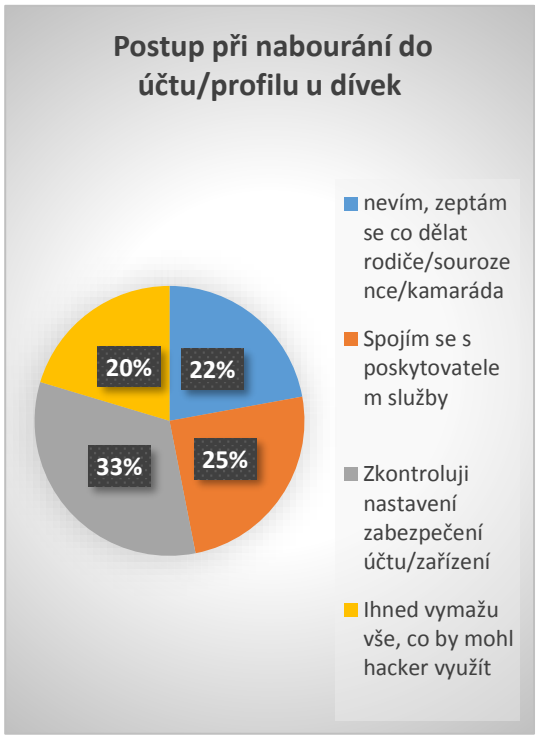
Zdroj: vlastní zpracování



Graf 31: Zabezpečení profilu u chlapců

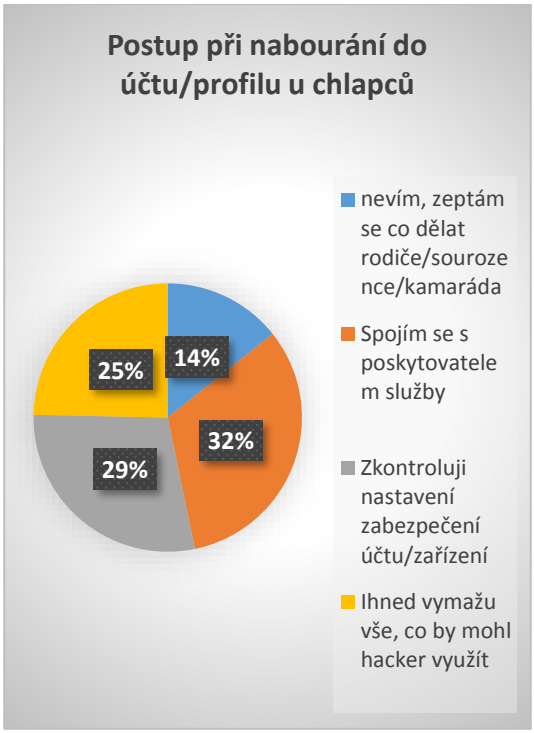
Zdroj: vlastní zpracování

Otázka č. 18 je vyhodnocena a znázorněna v grafu č. 32 a 33.



Graf 32: Postup při nebourání profilu u dívek

Zdroj: vlastní zpracování



Graf 33: Postup při nebourání profilu u chlapců

Zdroj: vlastní zpracování

7.4 Shrnutí výsledků dotazníkového šetření

V první části dotazníku jsem charakterizovala respondenty z hlediska pohlaví a věku a poskytla základní informace o užívání sociálních sítí, jako je účel zřízení profilu, čas strávený na sociálních sítích za den, aktivita na nich a respondenty nejvyužívanější sítě. Pro zjištění těchto dat jsem vytvořila otázky č. 1 - 6 a vztahující se ke dvěma hypotézám.

Hypotéza č. 1 předpokládala, že studenti bez rozdílu věku a pohlaví tráví na sociálních sítích minimálně dvě hodiny denně. **Hypotéza byla vyvrácena** - 25 % dotazovaných studentů tráví na sociální síti i méně než dvě hodiny (1 hodinu). Žádný respondent neuvedl, že sociální sítě nenavštěvuje vůbec a nemá zřízený účet

Hypotéza č. 2 předpokládala, že sociální sítě využívají dotazovaní bez rozdílu věku a pohlaví především ke komunikaci s kamarády. Výsledky naznačují, že vyšší aktivitu na síti (vytváření příspěvků/komentování/sdílení), projevují dívky. **Tato hypotéza byla potvrzena.** Chlapci i dívky využívají sociální sítě převážně ke komunikaci s kamarády.

Do této části dotazníku jsem rovněž zařadila otázku, které sociální sítě jsou respondenty nejčastěji aktivně využívány. Dle odpovědí

děvčat je nejčastější sociální sítí Instagram, Facebook a Facebook Messenger, chlapci uvedli Facebook, Facebook Messenger, Youtube následovaný Instagramem.

Cílem druhé části dotazníku bylo zjištění základní informace o bezpečnosti: od koho získávají studenti informaci o sociálních sítích před zřízením svého profilu, zda a kým jim jsou poskytovány informace o bezpečném pohybu na sociálních sítích a zda rodiče nahlížejí do jejich komunikační aplikace. K tomuto zjištění jsem zformulovala otázky č. 7 - 10.

Hypotéza č. 3 předpokládala, že povědomí o bezpečném pohybu na sociálních sítích před zřízením profilu získávají studenti nejvíce od svých kamarádů/vrstevníků, ale škola je následně v zajišťování gramotnosti o kyberbezpečnosti v této oblasti prioritní.

Tato hypotéza byla vyvrácena. Nejvíce dívek odpovědělo, že bylo před zřízením účtu/profilu poučeno rodiči, nejvíce chlapců uvedlo, že poučeni nebyli vůbec. Více než polovina dotazovaných dívek i chlapců uvedla, že již shlédla/přečetla materiál týkající se bezpečného pohybu na sociálních sítích a tento materiál byl dívkám i chlapcům poskytnut převážně kamarády.

Do této části jsem pro lepší informovanost o bezpečném pohybu studentů zařadila doplňující otázku, zda rodiče nahlíží studentům do komunikační aplikace. Bylo zjištěno, že aktivní kontrola rodiči prováděna z 84 % není, 16 % kladných odpovědí patří kontrole rodičů pouze u dívek.

Část třetí měla za cíl zjistit, zda se již studenti setkali s nějakými online riziky, s kým by nastalá online rizika řešili, zda již na sociální síť vložili nevhodný obsah a zda nové kontakty dostatečně prověřují.

K tomuto zjištění jsem zformulovala otázky v dotazníku č. 11 - 15 a vytvořila hypotézu č. 4 a 5.

Hypotéza č. 4 předpokládala, že většina studentů se již setkala alespoň s jedním z rizik hrozících užíváním sociálních sítí a že tyto rizika by nejčastěji řešili s kamarády nebo rodiči.

Tato hypotéza byla potvrzena. Oslovení respondenti se již alespoň s jedním z online rizik setkali (nejčastějším uváděným rizikem byl hoax u obou pohlaví, u dívek následovala kyberšikana a u chlapců byla druhá v pořadí uváděna závislost na sociálních sítích), nejčastěji by online riziko řešily dívky s rodiči a chlapci s kamarády.

Hypotéza č. 5 předpokládala, že alespoň polovina studentů již vložila na sociální sítě materiál s nevhodným obsahem.

Tato hypotéza byla také potvrzena. Z výsledků průzkumu vyplývá, že téměř polovina dívek a více než polovina chlapců již někdy na sociální sítě vložila materiál s nevhodným obsahem, který by rádi vzali zpět.

Do této části jsem zařadila dvě doplňující položky. První otázka měla zjistit, zda respondenti vědí, co znamená pojem digitální stopa. Na tuto otázku odpovědělo 47 % dívek a 62 % chlapců že tento pojem znají.

Druhá otázka měla zjistit, zda a jak důkladně prověřují dotazovaní studenti nové kontakty. Na tuto otázku odpovědělo 48 % dívek a 41 % chlapců, že se podívají, zda mají společné přátele. 46 % dívek kontaktuje společné přátele, zda dotyčného/dotyčnou znají, 32 % chlapců uvedlo, že toto neřeší.

Poslední část dotazníku měla za cíl zjistit stav ochrany přístupových zařízení a vytvořených profilů na sociálních sítích a koho by dotazovaní nejprve zkontaktovali, pokud by došlo k nabourání jejich profilů.

K tomuto zjištění jsem zformulovala otázky č. 16 - 18 a vytvořila hypotézu č. 6.

Tato hypotéza předpokládala, že většina studentů si je vědoma rizika možnosti nabourání do jejich profilů, a proto mají svá zařízení i profil zabezpečeny alespoň jedním ze základních zabezpečení.

Tato hypotéza byla potvrzena. Respondenti bez rozdílu věku i pohlaví mají svá zařízení i profily zabezpečeny alespoň jedním ze základních zabezpečení, nejčastěji v odpovědích zazněla možnost bezpečného hesla, a to v případě jak přístupového zařízení, tak i profilu.

Na otázku, jak by respondenti postupovali v případě nebourání do jejich profilu, vyplynulo, že největší procento dívek by nejprve zkontrolovalo základní nastavení svého účtu a největší procento chlapců by se spojilo s poskytovatelem služby.

ZÁVĚR

S vývojem moderních technologií je postupně směrována volnočasová aktivita na internet, u mladistvých zejména na sociální sítě. Touto prací jsem chtěla u dotazovaných studentů zmapovat nejenom jejich aktuální činnosti na sociálních sítích, jejich znalosti a zkušenosti s online riziky, ale především získat informaci o tom, zda byli, potažmo kým byli, před vstupem a zřízením účtu na sociálních sítích informováni o bezpečném pohybu na nich. V rámci prevence se mi jevilo toto zjištění jako nadmíru důležité, stejně tak jako získat informace o tom, zda probíhá na školách nebo v rodinách osvěta na téma bezpečného pohybu, rodičovskou kontrolu aktivity svých dětí nevyjímaje.

Pro dokreslení celé práce mě zajímalo i to, zda studenti provádějí ochranu ve smyslu zabezpečení svého zařízení a profilu.

Celkový počet respondentů činil 111, z toho bylo 74 dívek a 37 chlapců.

Z výzkumných otázek a z nich odvozených hypotéz plyne následující závěr:

Teenageři na vybrané střední škole tráví na sociálních sítích alespoň hodinu denně, a to převážně komunikací s kamarády. Dívky jsou aktivnější než chlapci ve smyslu vytváření příspěvků-fotek-videí/komentování/sdílení. Základní poučení o bezpečném pohybu před samotným zřízením účtu na sociálních sítích proběhlo u dívek ve valné většině ze strany rodičů, u chlapců neproběhlo vůbec. Materiál týkající se bezpečného pohybu, po zřízení účtu na sociálních sítích, většina studentů již shlédla či přečetla. Tento materiál byl studentům poskytnut nejčastěji kamarády. Kontrola činnosti svých dětí na sociálních sítích ze strany rodičů z více než 80 % neprobíhá. Většina oslovených studentů se již setkala alespoň s jedním online rizikem na sociální síti, nejčastěji byl uváděn dívkami i chlapci hoax, u dívek následovala kyberšikana, u chlapců závislost na sociálních sítích. Nastalé online riziko dívky řešily (příp. by řešily) převážně s rodiči, chlapci s kamarády. Téměř polovina dívek a více než polovina chlapců již vložila nebo zaslala na sociální sítě fotografii/video/komentář s nevhodným obsahem, který by rádi vzali zpět. Co se týče odpovědí k prověřování nových kontaktů, dívky i chlapci ve skoro polovině odpovědí uvedli, že se podívají, zda mají společné přátele. Dívky pak ještě v téměř shodném měřítku uvedli, že zkontaktují společné přátele, zda dotyčného/dotyčnou znají. Ochranu svých zařízení i profilů si hlídají dívky i chlapci nejvíce bezpečným heslem. V případě, že by byl profil někým nabourán, by největší procento dívek zkontrolovalo základní nastavení svého účtu, chlapci by se spojili s poskytovatelem služby.

Realizace výzkumu probíhala v době pandemické situace, která může být lehce zavádějící s ohledem na nařízené restrikce vládou ČR, kdy jsou víceméně sociální sítě jediným možným kontaktem pro udržení alespoň částečných sociálních vztahů mezi vrstevníky. Tyto restrikce mohou čas strávený na sociálních sítích prodlužovat.

SEZNAM POUŽITÉ LITERATURY

Tištěná literatura

1. **BOYDOVÁ D.** *Je to složitější: sociální život teenagerů na sociálních sítích*. Praha: Akropolis, 2017, ISBN 978-80-7470-165-8
2. **DOČEKAL D. a kol.** *Dítě v síti.* 2019, ISBN 978-80-204-5145-3
3. **ECKERTOVÁ, DOČEKAL.** *Bezpečnost dětí na internetu*. 2013, ekniha, ISBN 978-80-251-3804-5, Číslo publikace 16 699
4. **JIRÁSEK a kol.** *Výkladový slovník kybernetické bezpečnosti* (elektronická publikace). 2013, ISBN 978-80-7251-397-0
5. **JIROVSKÝ V.** *Kybernetická kriminalita*. 2007, ISBN 978-80-247-1561-2
6. **KOHOUT, KUBÍČKOVÁ.** *Internetem bezpečně* (online příručka). 2017, ISBN 978-80-270-3102-3
7. **KOPECKÝ K., KREJČÍ V.** *Rizika virtuální komunikace* (příručka pro uživatele a rodiče), 2010, ISBN 978-80-254-7866-O
8. **KRČMÁŘOVÁ a kol.** *Děti a online rizika* (sborník studií). 2012, ISBN 978-80-904920-3-5
9. **LOSEKOOT, VYHNÁNKOVÁ:** *Jak na sítě.* 2019, ISBN 978-80-7555-084-2
10. **MACEK, P.** *Adolescence*. 2. upravené vydání, Praha: Portál, 2003, ISBN 80-7178-747-7
11. **SEDLÁČEK J.** *Junior centra excelence informační bezpečnosti v ČR* (verze 20), 2021
12. **ŠEVČÍKOVÁ Anna a kolektiv:** *Děti a dospívající online*. 2014, ekniha, Grada Publishing ISBN 978-80-247-9645-1
13. **VÁGNEROVÁ, M.** *Vývojová psychologie*. 1999, ISBN 80-7178-308-0

Elektronické zdroje

[1] Internetem bezpečně, digitální stopa [online]. [cit. 2020-05-26]. Dostupný z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

[2] Metodický portál RVP.cz, úvod do problematiky sociálních sítí [online]. [cit. 2021-03-01]. Dostupný z: https://clanky.rvp.cz/clanek/o/g/15075/UVOD-DO-PROBLEMATIKY-SOCIALNICH-SITI.html/

[3] Český statistický úřad, informační společnost v číslech [online]. [cit. 2020-05-12]. Dostupný z:

https://www.czso.cz/csu/czso/internet-pouziva-pres-80-obyvatel-ceska

[4] Projekt e-bezpečí, věda a výzkum [online]. [cit. 2021-03-25]. Dostupný z: https://www.e-bezpeci.cz/index.php/veda-a-vyzkum/ceske-deti-v-kybersvete-2019

[5] Projekt e-bezpečí, věda a výzkum [online]. [cit. 2021-03-25]. Dostupný z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/107-rodic-a-rodicovstvi-v-digitalni-ere-2018/file

[6] E-bezpečí – Centrum prevence rizikové virtuální komunikace [online]. [cit. 2020-05-11]. Dostupný z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/socialni-site/147-222

[7] Tipy a triky – informační technologie [online]. [cit. 2021-03-28]. Dostupný z: (https://365tipu.cz/2017/09/11/tip888-co-je-to-dark-post-unpublished-post-na-facebooku-k-cemu-je-to-dobre/

[8] Internetem bezpečně, kyberšikana [online]. [cit. 2020-05-12]. Dostupný z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/

[9] Internetem bezpečně, kyberstalking [online]. [cit. 2020-05-12]. Dostupný z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/

[10] Internetem bezpečně, kybergrooming [online]. [cit. 2020-05-12]. Dostupný z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/

[11] Internetem bezpečně, sexting [online]. [cit. 2020-05-12]. Dostupný z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/sexting/

[12] Projekt e-bezpečí, věda a výzkum [online]. [cit. 2021-03-28]. Dostupný z: https://www.e-bezpeci.cz/index.php/veda-a-vyzkum/sexting-vyzkum-2017

[13] Projekt e-bezpečí, výzkumné zprávy [online]. [cit. 2021-03-28]. Dostupný z: https://e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/135-2020-cesky-ucitel-ve-svete-technologii/file

[14] Projekt e-bezpečí, rizikové jevy, kybergrooming [online]. [cit. 2021-03-29]. Dostupný z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybergrooming/1696-komentar-film-v-siti-je-jiny-nez-predchozi-snimky-orientovane-na-oblast-rizikove-komunikace-v-online-prostredi

[15] Lupa.cz, články; Vít Klusák (V síti): Mysleli jsme, že jsme narazili na dno pekla. Pak to ale bylo ještě horší [online]. [cit. 2020-05-11]. Dostupný z: https://www.lupa.cz/clanky/vit-

klusak-v-siti-mysleli-jsme-ze-jsme-narazili-na-dno-pekla-pak-to-ale-bylo-jeste-horsi/

[16] E15.cz, články; Chceme se podílet na řešení, říká o pokleslém chování na internetu režisér filmu V síti Klusák [online]. [cit. 2020-05-11]. Dostupný z: https://www.e15.cz/rozhovory/chceme-se-podilet-na-reseni-rika-o-pokleslem-chovani-na-internetu-reziser-filmu-v-siti-klusak-1367152

[17] Projekt e-bezpečí, z naší kuchyně, komentář: Film V síti [online]. [cit. 2021-03-29]. Dostupný z: https://www.e-bezpeci.cz/index.php/z-nasi-kuchyne/1797-komentar-film-v-siti-vyvraci-drtive-mnozstvi-stereotypu-o-sexualnich-predatorech-a-take-o-prevenci-rizikoveho-chovani-vybirame-nektere-z-nich

[18] Internetem bezpečně, návody, počítač-zabezpečení zařízení [online]. [cit. 2021-03-05]. Dostupný z: https://www.internetembezpecne.cz/internetem-bezpecne/navody/pocitac-zabezpeceni-zarizeni/

[19] Internetem bezpečně, návody, heslo [online]. [cit. 2021-03-05]. Dostupný z: https://www.internetembezpecne.cz/internetem-bezpecne/navody/heslo/

[20] Projekt e-bezpečí, rizikové jevy, Trestná činnost spojená s internetovou kriminalitou [online]. [cit. 2021-03-29]. Dostupný z: https://www.e-bezpeci.cz/index.php/temata/dali-rizika/148-226

[21] Policie ČR, Kyberkriminalita [online]. [cit. 2021-03-29]. Dostupný z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[22] Matematika, fyzika, informatika, metadata pro indexaci [online]. [cit. 2021-03-29]. Dostupný z: http://www.mfi.upol.cz/index.php/mfi/rt/metadata/509/0

[23] Matematika, fyzika, informatika, metadata pro indexaci [online]. [cit. 2021-03-29]. Dostupný z: http://mfi.upol.cz/index.php/mfi/rt/metadata/496/0

[24] Databáze strategií, portál strategických dokumentů [online]. [cit. 2021-03-04]. Dostupný z: https://www.databaze-strategie.cz/cz/cr/strategie/narodni-strategie-kyberneticke-bezpecnosti-cr-na-obdobi-let-2015-az-2020?typ=struktura

[24] Národní úřad pro kybernetickou a informační bezpečnost, strategie/akční plán [online]. [cit. 2021-03-31]. Dostupný z: https://nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

SEZNAM OBRÁZKŮ

Obrázek 1: Věkové rozložení dětských uživatelů dominantních sociálních sítí 18
Obrázek 2: Používání sociálních sítí v jednotlivých věkových kategoriích 24
Obrázek 3: Věková struktura 26
Obrázek 4: Nápad trestné činnosti a kybernetické kriminality páchané na internetu 2011 - 2019 34
Obrázek 5: Odolný systém zajištění kybernetické bezpečnosti 36

SEZNAM GRAFŮ

Graf 1: Počet hodin strávených na sociálních sítích za den 39
Graf 2: Pohlaví a věk respondentů 40
Graf 3: Pohlaví respondentů 40
Graf 4: Počet hodin strávený na sociálních sítích za den 41
Graf 5: Účel zřízení profilu u dívek 42
Graf 6: Účel zřízení profilu u chlapců 42
Graf 7: Aktivita na sociálních sítích u dívek 43
Graf 8: Aktivita na sociálních sítích u chlapců 43
Graf 9: Nejvyužívanější sociální sítě 44
Graf 10: Zdroj poskytování informací před zřízením účtu u dívek 45
Graf 11: Zdroj poskytování informací před zřízením účtu u chlapců 45
Graf 12: Shlédnutí/přečtení materiálu o bezpečném pohybu u dívek 46
Graf 13: Shlédnutí/přečtení materiálu o bezpečném pohybu u chlapců 46
Graf 14: Zdroj poskytnutí materiálu o bezpečném pohybu u dívek . 47
Graf 15: Zdroj poskytnutí materiálu o bezpečném pohybu u chlapců 47
Graf 16: Nahlížejí rodiče dívkám do komunikační aplikace 48
Graf 17: Nahlížejí rodiče chlapcům do komunikační aplikace 48
Graf 18: Nejčastější online rizika, se kterými se setkaly dívky 49
Graf 19: Nejčastější online rizika, se kterými se setkali chlapci 50
Graf 20: S kým by online riziko řešily dívky 50
Graf 21: S kým by online riziko řešili chlapci 51
Graf 22: Osobní zkušenost s vložením nevhodného obsahu u dívek .. 52
Graf 23: Osobní zkušenost s vložením nevhodného obsahu u chlapců 52
Graf 24: Znalost pojmu digitální stopa u dívek 53
Graf 25: Znalost pojmu digitální stopa u chlapců 53
Graf 26: Prověřování nových kontaktů u dívek 54
Graf 27: Prověřování nových kontaktů u chlapců 54
Graf 28: Zabezpečení přístupového zařízení u dívek 55
Graf 29: Zabezpečení přístupového zařízení u chlapců 56
Graf 30: Zabezpečení profilu u dívek 56
Graf 31: Zabezpečení profilu u chlapců 57
Graf 32: Postup při nebourání profilu u dívek 57

Graf 33: Postup při nebourání profilu u chlapců 58

EVIDENCE VÝPŮJČEK

Prohlášení:

Dávám svolení k půjčování této bakalářské práce. Uživatel potvrzuje svým podpisem, že bude tuto práci řádně citovat v seznamu použité literatury.

Jméno a příjmení: Lucie Švarcová

V Praze dne: Klikněte nebo klepněte sem a zadejte datum. Podpis:

Jméno	**Oddělení/ Pracoviště**	**Datum**	**Podpis**