Univerzita Hradec Králové
Pedagogická fakulta
Ústav sociálních studií

Kyberkriminalita z pohledu žáků druhého stupně základních škol

Diplomová práce

Autor: Bc. Dan Machatý
Studijní program: N0111A190018 Sociální pedagogika
Studijní obor: Sociální pedagogika
Vedoucí práce: doc. PhDr. Václav Bělík, Ph.D.
Oponent práce: Mgr. Vlastislav Kučera, Ph.D.

Hradec Králové 2024

Univerzita Hradec Králové
Pedagogická fakulta

Zadání diplomové práce

Autor:	**Bc. Dan Machatý**
Studium:	P22P0498
Studijní program:	N0111A190018 Sociální pedagogika
Studijní obor:	Sociální pedagogika
Název diplomové práce:	**Kyberkriminalita z pohledu žáků druhého stupně základních škol**
Název diplomové práce AJ:	Cybercrime from the point of view of second grade elementary school students

Cíl, metody, literatura, předpoklady:

Diplomová práce se zabývá kyberkriminalitou z pohledu žáků druhého stupně základních škol. Teoretická část se zabývá vymezením kyberkriminality, rizikovými jevy v ICT prostoru a prevencí. Zvláštní zřetel je kladen na druhy kyberkriminality a s nimi spojenou legislativu. Empirická část prezentuje výsledky kvantitativního výzkumného šetření.

KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. 521 s. ISBN 978-80-88168-15-7.

KOLOUCH, Jan, BAŠTA, Pavel et al. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. 560 s. ISBN 978-80-88168-34-8.

PORADA, Viktor a Karel RAIS. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatelství CERM, 2021. 468 s. ISBN 978-80-7623-065-1.

SMEJKAL, Vladimír. *Kybernetická kriminalita. 3. rozšířené a aktualizované vydání.* Plzeň: Aleš Čeněk, s.r.o., 2022. 1166 s. ISBN: 978-80-7380-849-5.

ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie. 148 s. ISBN 978-80-7552-758-5.

Zákon č. 40/2009 Sb., trestní zákoník.

Zadávající pracoviště:	Ústav sociálních studií, Pedagogická fakulta
Vedoucí práce:	doc. PhDr. Václav Bělík, Ph.D.
Oponent:	Mgr. Vlastislav Kučera, Ph.D.

Datum zadání závěrečné práce: 28.2.2023

Prohlášení

Prohlašuji, že jsem diplomovou práci Kyberkriminalita z pohledu žáků druhého stupně základních škol vypracoval pod vedením vedoucího práce doc. PhDr. Václava Bělíka, Ph.D. samostatně a uvedl jsem všechny prameny a literaturu.

V Hradci Králové dne

Poděkování

Chtěl bych poděkovat vedoucímu práce doc. PhDr. Václavu Bělíkovi, Ph.D. za odborné vedení práce, konzultace a cenné rady. Také bych chtěl poděkovat všem ředitelům, ředitelkám, učitelům a učitelkám základních škol, kteří se podíleli na vyplňování a distribuci online dotazníku.

Anotace

MACHATÝ, Dan. *Kyberkriminalita z pohledu žáků druhého stupně základních škol.* Hradec Králové: Pedagogická fakulta Univerzity Hradec Králové, 2024. 75 s. Diplomová práce.

Diplomová práce se zabývá kyberkriminalitou z pohledu žáků druhého stupně základních škol. Úvod teoretické části se zaměřuje na kyberkriminalitu z pohledu kybernetického světa. Zde je věnována pozornost kyberprostoru jakožto prostředí pro páchání kyberkriminality a digitální stopě. Dále jsou popsány sociální sítě a její druhy. Další kapitola rozebírá projevy kyberkriminality. V jednotlivých podkapitolách jsou detailně analyzovány a poslední podkapitola pojednává o kyberkriminalitě z pohledu legislativy. Závěr teoretické části se orientuje na kyberkriminalitu a její prevenci u dětí, kde je představen životní styl dětí, druhy prevence včetně školních dokumentů a také preventivní programy. Empirická část byla zaměřena na zkušenosti žáků druhého stupně základních škol s kyberkriminalitou a jejich povědomí o této problematice. Výzkumné šetření bylo zpracováno kvantitativní metodou formou anonymního online dotazníku a z velké části se opíralo o výzkum Vnímání kyberkriminality mezi dětmi. Respondenty byli žáci druhého stupně základních škol z východočeského regionu.

Klíčová slova: kyberkriminalita, žáci, základní škola, zkušenost

Annotation

MACHATÝ, Dan. Cybercrime from the point of view of second grade elementary school students. Hradec Králové: Faculty of Education University of Hradec Králové, 2024. 75 pp. Diploma Thesis.

The thesis deals with cybercrime from the perspective of second grade primary school students. The introduction of the theoretical part focuses on cybercrime from the perspective of the cyber world. Here, attention is paid to cyberspace as an environment for committing cybercrime and the digital footprint. Furthermore, social networks and its types are described. The next chapter discusses the manifestations of cybercrime. Each subchapter analyses them in detail and the last subchapter discusses cybercrime from the perspective of legislation. The conclusion of the theoretical part focuses on cybercrime and its prevention in children, where the lifestyle of children, types of prevention including school documents as well as prevention programmes are presented. The empirical part focused on the experience of second grade primary school students with cybercrime and their awareness of this issue. The research investigation was processed by a quantitative method in the form of an anonymous online questionnaire and was largely based on the research Perceptions of Cybercrime among Children. The respondents were second grade pupils of primary schools from the East Bohemia region.

Keywords: cybercrime, pupils, primary school, experience

Prohlášení

Prohlašuji, že diplomová práce je uložena v souladu s rektorským výnosem č. 13/2022 (Řád pro nakládání bakalářskými, diplomovými, rigorózními, dizertačními a habilitačními pracemi na UHK)

Datum…….. Podpis studenta …….

Obsah

Úvod

Tato diplomová práce se zabývá kyberkriminalitou u žáků druhého stupně základních škol. Teoretická část analyzuje situaci kyberkriminality v naší republice. Úvodní kapitola popisuje kyberprostor jakožto prostředí pro páchání kybernetické kriminality a dále digitální stopu a sociální sítě včetně jejích typů. Následující kapitola je zaměřena na projevy kyberkriminality, u kterých jsou uvedeny definice, druhy a také možnosti prevence. V závěru této kapitoly je věnována pozornost kyberkriminalitě z pohledu legislativy. Třetí kapitola teoretické části se věnuje životnímu stylu dětí a prevenci. Jsou zde popsány školní preventivní dokumenty a také další preventivní programy. Informace jsou čerpány od autorů, kteří se tomuto tématu věnují zejména Kolouch a Kopecký. Z internetových zdrojů byl nejvíce využíván web Policie České republiky a Internetem bezpečně. Ze zákonů to byl Zákon č. 40/2009 Sb., trestní zákoník.

Praktická část je orientována na žáky druhého stupně základních škol. V jejím úvodu jsou uvedeny rešerše studií, které řeší toto téma. Cílem práce je zanalyzovat kyberkriminalitu u žáků druhého stupně základních škol v České republice. Cílem výzkumného šetření je zjistit, jaké zkušenosti mají žáci druhého stupně základních škol s kyberkriminalitou a jaké je jejich povědomí o této problematice. Ve výzkumném šetření je použita kvantitativní metoda pomocí online dotazníkového šetření, které se inspiruje výzkumem Vnímání kyberkriminality mezi dětmi z roku 2018. Výzkumná data jsou zpracovávána pomocí MS Excell. Hypotézy jsou ověřovány metodou Chí – kvadrát testu nezávislosti pro čtyřpolní kontingenční tabulku a znázorněnými grafy a tabulkami.

Téma diplomové práce bylo zvoleno vzhledem k mé zkušenosti s touto problematikou, a také protože je toto téma velmi aktuální. Je všeobecně známo, že závislost dětí na internetu a moderních technologiích roste, což vede k nárůstu počet případů kyberkriminality napříč populací, včetně dětí a mládeže. Potěšil mě také zájem oslovených základních škol o výsledky tohoto šetření. Je vidět, že základní školy si uvědomují závažnost této problematiky a chtějí být v této oblasti dostatečně informovány, aby případně mohly jevům kyberkriminality předcházet.

1 Kyberkriminalita v prostoru kybernetického světa

V úvodní kapitole teoretické části této diplomové práce se budeme věnovat nejprve kyberprostoru jako prostředí, kde se kyberkriminalita odehrává. Dále si představíme digitální stopu a také sociální sítě a její druhy.

Dle § 2 písm. a) zákona o kybernetické bezpečnosti se rozumí kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací. (Zákon č. 181/2014 Sb., o kybernetické bezpečnosti) Kolouch říká, že: ,,Kyberprostor je také možné definovat jako prostor kybernetických aktivit či jako prostor vytvořený informačními a komunikačními technologiemi, který vytváří virtuální svět jako paralelu k prostoru reálnému‘‘. (Kolouch, 2016, s. 43) Kolouch řadí ke znakům kyberprostoru decentralizovanost, globálnost, otevřenost, hojnost na informace včetně lží, polopravd a nesmyslů, interaktivnost a schopnost ovlivňovat názory skrze uživatele. Hlavní úlohu v kyberprostoru hrají technologie a služby navázané na ně. Čím dál tím častěji lze vnímat, že úkony ve virtuálním světě mohou mít dopady ve světě reálném. Kyberprostor má svá specifika oproti reálnému světu, tudíž v něm nebudou platit stejná pravidla. Klíčovým prvkem současné doby je rychlost a dostupnost přenášených dat. Uživatele nezajímá, jakým způsobem dochází k přenosu dat do informačních sítí vložených ani odkud pochází adresát přenášených dat, či místo, kde jsou data uložena, a tak je zapříčiněno odhmotnění obsahu od tělesné struktury informačních sítí. (Kolouch, 2016)

Dokument Cyberspace Operations Concept Capability Plan 2016-2028 definuje kyberprostor následovně: ,,Kyberprostor je globální oblastí v informačním prostředí, který se skládá ze vzájemně závislé sítě infrastruktur informačních technologií, včetně internetu, telekomunikačních sítí, počítačových systémů a vestavěných procesorů a zařízení‘‘. (Cyberspace Operations Concept Capability Plan 2016-2028, 2010, s. 6, online) Kolouch, Bašta a kol. uvádějí, že kyberprostor se skládá celkem ze 3 vrstev: fyzické, logické a sociální. **Fyzická vrstva** obsahuje pojmy ,,geographic component‘‘, čímž se rozumí přesná lokalizace síťových prvků v reálném světě a fyzické síťové komponenty, které pojímají infrastrukturu ve formě kabelů, řídících prvků sítě (routerů) a dalších zařízeních. Toto uspořádání má své opodstatnění. V kyberprostoru lze jednoduše překročit mezistátní geopolitické hranice, avšak v reálném světě se nacházejí stále omezení, která plynou z podstaty hmotného světa. **Logická vrsva** v sobě nese

logické síťové komponenty, tedy logická propojení mezi síťovými uzly, která jsou prováděna pomocí komunikačních protokolů. Pod pojmem uzly si lze představit počítače, telefony a jiná síťová zařízení. **V sociální vrstvě** se pracuje s pojmy kyberosobnost a osobnost. Kyberosobností je myšlena identifikace osoby na síti, příkladem může být e- mailová adresa, číslo telefonu a další. Osobnost pojímá skutečné osoby, které jsou připojeny k sítí. Platí, že jeden člověk může mít více kyberosobností, příkladem mohou být různé e-maily na více zařízeních, a naopak jedna kyberosobnost může zahrnovat více skutečných osob, které používají jeden hromadný sdílený účet. (Kolouch, Bašta a kol, 2019) Smejkal popisuje kyberprostor jako kombinaci virtuálních vlastností, jenž se vymykají geografickým hranicím a fyzické infrastruktury patřící do pravomoci nezávislých států. Navzdory tomu, že kybernetický prostor poskytl výhodný přístup k informacím a jednoduché komunikaci s neustále přibývajícím počtem lidí, tak přispěl svou existencí ke zločinu, hackerským útokům a ohrožení bezpečnosti států. (Smejkal, 2022)

1.1 Digitální stopa

Smejkal ve své publikaci uvádí, že každý technologický nástroj, jenž získává, zpracovává nebo sdílí či uschovává data, za sebou zanechá záznamy o svém působení. Takové záznamy jsou z kriminalistického pohledu stopami. Jedná se o digitální stopy, které můžeme vymezit jako jakékoliv informace s vypovídající hodnotou, které jsou uložené či sdílené v digitální podobě. Jinými slovy lze také říci, že digitální stopa představuje fyzikální záznam nehmotné informace, která je zakódována do digitálního rozměru. (Smejkal, 2022)

,,Ve světě ICT platí jedno pravidlo: pokud kdykoliv cokoliv nahrajete, přenesete, zprostředkujete, vložíte do kyberprostoru, zůstane to tam „navždy“. (Kolouch, 2016, s. 135)

Kolouch uvádí, že lze rozdělit digitální stopy podle toho, jestli je uživatelé mohou či nemohou ovlivnit na stopy ovlivnitelné a neovlivnitelné. **Digitální stopa ovlivnitelná** zahrnuje všechny informace, jenž o sobě uživatel dobrovolně a sám předá jiné osobě, ať fyzické, právnické nebo např. ISP. Zmíněný pojem předání v praxi znamená poslání e- mailu, přidání příspěvku do diskuse či fóra, sdílení všech typů médií (foto,video,audio aj.) napříč sociálními sítěmi. Také si můžeme představit registraci a využívání všech služeb, které se nacházejí v kyberprostoru (operační systémy, e-maily, sociální sítě,

seznamky, chaty, blogy, webové stránky, cloudové služby, datová úložiště a další). Nad těmito digitálními stopami ovlivnitelnými může mít uživatel určitý stupeň kontroly a záleží pouze na něm samotném, zda zveřejní své údaje a informace o sobě dalším osobám. **Digitální stopa neovlivnitelná** většinou vzniká v důsledku vzájemné interakce dvou počítačových systémů nebo na základě operací počítačového systému a jeho přidruženého softwaru. Příkladem takových stop mohou být informace, které pocházejí z operačního systému jako například chybová hlášení ze systému Windows nebo systémové informace. Dále sem řadíme i jiná data a informace, která jsou ukládána v důsledku funkčnosti systému, aniž by bylo nutné je předávat dál, například, pokud počítačový systém nikdy nebyl připojen k žádné síti či jinému počítačovému systému. Jestliže má uživatel dostatek zkušeností, může velké množství neovlivnitelných digitálních stop upravit, maskovat či utajit prostým anonymním režimem webového prohlížeče, který dokáže vypnout cookies. Charakteristickým příkladem neovlivnitelné digitální stopy je připojení počítačového systému k internetu, jenž využívá IP adresu nebo MAC adresu, které jsou dále sdíleny s ostatními informacemi ISP. (Kolouch, 2016)

1.2 Sociální sítě

Černá a Černý říkají, že sociální síť určuje typ služby, která poskytuje komunikaci, sdílení dat a informací všem jejím uživatelům, a tím se odlišuje od jiných druhů komunikace jako je např. chat nebo telefon. (Černá, Černý, 2015, online) Kolouch zmiňuje další typický odlišující znak od běžné komunikace, a to interaktivnost. Na sociálních sítích je ke standardní komunikaci připojována obsahová část, čímž je myšleno tvoření a sdílení fotografií, videí, odkazů, či dokumentů vzájemně mezi jednotlivými uživateli. Nedílnou součástí sociálních sítí je také vytváření profilů, které představují konkrétní osoby. Nicméně podle stanovených smluvních podmínek můžou tyto profily korespondovat s reálnými i smyšlenými osobami. Sociální komunikace ve sféře sociálních sítí je přímo závislá na počtu aktivních uživatelů. Jak už bylo zmíněno na začátku této podkapitoly, sociální síť představuje službu poskytovanou internetovým připojením, a to v kyberprostoru podle uzavřených smluvních podmínek. Na základě těchto podmínek lze o uživatelích zjistit nespočet informací často soukromých, které můžou být ve shodě s těmito uzavřenými podmínkami sdíleny dalším lidem a uchovávány téměř neomezenou dobu. (Kolouch, 2016) Kohout a Karchňák upozorňují na rizika užívání sociálních sítí, protože jejich uživatelé z hlediska bezpečnosti s nimi neumí zacházet.

Uživatelé obvykle nepřikládají patřičnou důležitost užívání sociálních služeb, a v důsledku této nevědomosti mohou být osobní údaje, které jsou zadané při registraci, poskytnuty třetím stranám. Podobně je tomu se sdílením informací jako jsou názory, fotografie a další. Pokud uživatelský profil není dostatečně zabezpečený a chráněn před zneužitím, přináší to určitá rizika. Všechny osobní údaje představují cenné zboží, se kterým digitální svět často obchoduje. Tyto údaje mohou být využity k marketingovým účelům, ale také mohou sloužit k páchání trestné činnosti. (Kohout, Karchňák, 2016)

1.3 Typy sociálních sítí

Dle Černého a Černé je nabídka sociálních sítí velice obsáhlá a aktuální trendy předpovídají, že množství jejich uživatelů poroste, a to díky vzrůstajícímu počtu různých služeb, zaměření nebo míře ochrany soukromí. Jednotlivé sítě se liší také v oblasti komunikace a respektování soukromí. (Černá, Černý, 2015, online) Kopecký a Krejčí řadí mezi nejznámější sociální sítě Facebook, Instagram, YouTube, Snapchat, TikTok, X(Twitter), LinkedIn, OnlyFans a Internetové seznamky. Web Internetem bezpečně uvádí ještě navíc jako nejužívanější sociální sítě Ask.fm, Omegle, Musical.ly (nyní součástí TikToku) a Badoo. (INTERNETEM BEZPEČNĚ, online)

Facebook

Černá a Černý říkají, že Facebook je největší sociální síť, která poskytuje sdílení statusu (informací), videí, obrázků a odkazů. Podstatou projektu je zeď, která prezentuje aktivity a události, na nichž se podílejí vaši přátelé. Facebook nemá žádné ohraničené téma, kterým by se řídil a primárně slouží k zábavě a neformální komunikaci. Významnou úlohu tu mají také hry, kterých se účastní milióny uživatelů. Na Facebooku jsou soukromé informace těmi nejpodstatnějšími. Pokud má člověk úmysl se připojit do některé sítě, je zapotřebí se seznámit se způsobem komunikace a tématy, které se tu promítají. (Černá, Černý, 2015, online) Web Internetem Bezpečně uvádí dle statistik, že Facebook je lídr sociálních sítí, což potvrzuje přes 2 miliardy aktivních uživatelů na celé planetě. Na Facebooku se mohl v České republice registrovat kdokoliv starší 13 let už od roku 2006. (Internetem Bezpečně, online) Kopecký a Krejčí navíc zmiňují ostatní funkce a nástroje, které Facebook nabízí: vytváření skupin, událostí, stránek, přímé odesílání zpráv, videohovory a další. K nejnovějším funkcím patří **Facebook Reels** nebo

Facebook Stories. Facebook Reels, funkce inspirovaná aplikací TikTok, poskytuje uživatelům tvořit a sdílet krátké videoklipy, které mohou zahrnovat různorodé vizuální efekty a hudbu. Facebook Reels představuje jednu z možností Facebooku, jak udržet krok s konkurencí z oblasti sociálních médií. Facebook Stories je funkce, která se inspirovala sítí Snapchat a dává možnost svým uživatelům sdílet fotografie a videa, která se automaticky odstraní za 24 hodin. Facebook Stories má usnadňovat sdílení obsahu v reálném světe. (Kopecký, Krejčí, 2023, online)

Messenger

Kopecký a Krejčí uvádí, že Facebook Messenger, dnes již pod novým názvem Meta Messenger, je aplikace určená pro odesílání zpráv tzv. instant messaging, která byla na počátku součástí hlavní platformy Facebook, přičemž na webové verzi stále integrována je. Uživatelé v této aplikaci mohou zasílat zprávy, fotografie, videa a vést hlasové či video hovory s dalšími facebookovými uživateli. (Kopecký, Krejčí, 2023, online)

Instagram

Dobosiová popisuje, že přihlášení uživatelé mohou na síť přidávat své fotky, dávat na ně tzv. ,,like'', komentovat je a přidávat jiné uživatele do sledování nebo potvrzovat sledování od ostatních uživatelů. Dále uvádí, že Instagram není pouze platforma pro sdílení fotek z každodenního života, ale jeho podstatou je vytvoření malých uměleckých děl. Pomocí několika filtrů, které Instagram umožňuje, lze vytvořit za pár minut z obyčejné fotky, fotku profesionální. Intagram je definován dvěma slovy: fotografie a komunita. (Dobosiová, 2015, online) Kopecký a Krejčí popisují oblíbenou funkci tzv. **Instagram Stories**, která poskytuje uživatelům posílat soukromé zprávy a vytvářet příběhy, které jsou zobrazeny po omezený čas, což je obvykle 24 hodin, a poté se automaticky odstraní. Uživatelé mají možnost sdílet své zážitky a události formou krátkých a spontánních příběhů. V příbězích se mohou vyskytovat různé emoji, kresby, filtry a prvky podporující interaktivitu jako jsou otázky a ankety. Populární funkcí jsou tzv. **Instagram Reels**, což jsou krátká videa nepřekračující délku 60 sekund, která se zobrazují nepřetržitě jako na síti TikTok. Uživatelé mohou vytvářet a sdílet videa s hudbou, efekty, textem a jinými interaktivními elementy. (Kopecký, Krejčí, 2023, online)

Snapchat

Dle Tredéze se jedná o typ sociální sítě, kde hlavní podstatou je fotografie či krátké video. Tato síť je mezi mladou generací velmi oblíbená a poskytuje možnost časového omezení, po kterou si přátelé budou moct fotografii prohlédnout. To může vyvolat mylný pocit bezpečí, že se fotografie nebude dál sdílet. To potvrzuje existence několika kolekcí explicitních fotografií mladých jedinců, které byly vytvořeny např. způsobem screenshotu displeje mobilního telefonu. (Internetem Bezpečně, online) Trédez upozorňuje, aby se neposílaly fotky s vědomím, že jednou zmizí, protože kdokoliv si může pořídit ,,printscreen'', což je snímek obrazovky. (Tredéz, 2018)

YouTube

Základem této sítě je sdílení videa mezi veřejností. Přispívat na tuto platformu může kdokoliv, protože zde nejsou žádné technické požadavky. YouTube lze rozdělit na dvě skupiny uživatelů, a to na přispěvatele a publikum. Pasivní publikum se nemusí registrovat, a proto mohou uživatelé anonymně pozorovat videa bez jakéhokoliv časového omezení. Registrovaní uživatelé mají možnost nahrávat vlastní videa, vytvářet playlisty a komentovat videa jiných uživatelů, ale i vlastních. Podobně jako na Facebooku tu existuje tlačítko ,,Líbí se mi'', ale liší se od něj tlačítkem ,,Nelíbí se mi''. Obsah, který nalezneme na YouTube je velmi pestrý. Můžeme tu najít videa hudební, sportovní, vzdělávací a osvětová. YouTube lze zařadit i ve vyučování jako ukázku nebo formu prezentace učiva. (Dobosiová, 2015, online)

Vedle možnosti vytvořit si vlastní playlist z oblíbených písniček, si české děti oblíbily fenomén tzv. Youtuberů. Málokterý náctiletý jedinec nemá svého oblíbeného Youtubera, což je člověk, který se zabývá tvorbou videií různého obsahu a snaží se vytvořit komunitu uživatelů, kteří ho budou sledovat a podporovat. (Internetem Bezpečně, online)

TikTok

Dle Kopeckého a Krejčí je TikTok mobilní aplikací a sociální sítí původem z Číny, která se zaměřuje na sdílení krátkých videí (15-60 vteřin). Tato videa se dají upravovat různými nástroji. Svou popularitu získal díky tomu, že umí tvořit virální trendy a komunity, které dál sdílejí svůj obsah. Mezi jeho přednosti patří jednoduchost, přístupnost a kreativita.

TikTok je známý svým originálním algoritmem, jenž umí využívat umělou inteligenci a podle interakcí a chování uživatele na síti či aplikaci, mu ukazuje videa, která by uživatele mohla zajímat. Právě tento způsob pomáhá poskytovat lehkou a rychlou konzumaci obsahu a díky tomu se stal TikTok tak oblíbeným. Kdokoliv tu může být tvůrcem obsahu, aniž by s tím měl jakékoliv zkušenosti. Navzdory jeho celosvětové popularitě čelí několika problémům, a to hlavně kvůli ochraně soukromí uživatelů. To je zapříčiněno původem TikToku, protože zde jsou obavy, které se týkají využívání a sběru osobních údajů. Kritici uvádějí, že tato platforma by mohla sdílet uživatelské údaje čínské vládě, a to představuje nebezpečné důsledky pro soukromí a bezpečí uživatelů. Dokonce kvůli těmto informacím byl TikTok v řadě států omezen nebo zakázán. TikTok se dále potýká s problémem týkající se obsahu, který je tu předáván. Nacházejí se zde případy videí s urážlivým, diskriminačním či nebezpečným obsahem. Objevují se tu ale i šíření nepravdivých informací i dezinformací. (Kopecký, Krejčí, 2023, online)

Omegle

Kopecký a Krejčí sdělují, že Omegle byla webová platforma, která sloužila pro online chatování, ale v listopadu roku 2023 ukončila činnost z důvodu šíření pornografie (také dětské), online kybersexu nebo např. vydírání. Server Omegle dále čelil politickému a legislativnímu tlaku, který byl vyvíjený na ochranu dětí před sexuálním zneužíváním v online prostoru. Praxe vypadá tak, že provozovatelé musí zajistit, aby na platformách které spravují, nedocházelo k sexuálnímu zneužívání, což bylo na Omegle běžné a rozšířené. Jejím hlavním znakem byla anonymní komunikace mezi uživateli, kteří byli vybráni zcela náhodně pro textový či video chatování. Nebylo zapotřebí žádné registrace ani osobních údajů, a to znamenalo rychlý a jednoduchý přístup k chatu. (Kopecký, Krejčí, 2023, online)

Ask.fm

Dle webu The cybersmile foundation, je Ask.fm sociální síť, kde si uživatelé mohou vytvářet profily a pokládat ostatním uživatelům anonymní otázky. Uživatelé, kteří se ptají na něco, si mohou nastavit, jestli informace o svém profilu chtějí zveřejnit ostatním nebo se ptát ostatních uživatelů anonymně. Odpovídat na otázky lze i formou fotografií, videí i GIFy. Děti, které chtějí využívat Ask.fm by měly být starší 13 let, není ale tajemstvím,

že se tu najdou i osoby mladší a vůbec se tím netají. (The cybersmile foundation, 2024, online)

X (Twitter)

Dle Kopeckého a Krejčí, je X (Twitter) sociální sítí, která umožňuje sdílet zprávy tzv. tweety. Tweety jsou omezeny 280 znaky (u platících uživatelů až 4000 znaků) a můžou zahrnovat text, odkazy, obrázky či videa. Twitter patří mezi nejnavštěvovanější sociální sítě na světě a největší uživatelskou základnu má ve Spojených státech amerických. (Kopecký, Krejčí, 2023, online)

Internetové seznamky

Nejpopulárnějšími seznamkami jsou Tinder, Pinkilin, Grindr, Badoo, Beatiful People, Luxy, Bumble, Bristir, Happn, Elite Date, eDarling a další. Primárně mají sloužit k navazování různorodých mezilidských vztahů a mohou se zaměřovat na konkrétní cílovou skupinu např. seniory, osoby s konkrétní sexuální orientací nebo dokonce seznamky pro děti. Mezi výhody těchto online seznamek patří, že pomáhají nalézt partnery či přátelé se stejnými zájmy a hodnotami. Nevýhodou je však existence falešných profilů, které mohou být zneužity k podvodům, vydírání (blackmailing), uživatelé ne vždy hovoří pravdu a riziko představuje také nesmírné množství osobních údajů včetně těch citlivých jako intimní fotografie apod., které se dají zneužít. (Kopecký, Krejčí, 2023, online)

Úvodní kapitola diplomové práce se zaměřuje na kyberprostor, který představuje prostředí k páchání trestné činnosti. Nejprve popisuje několik definic kybernetického prostoru a charakterizuje 3 vrstvy, z nichž se skládá. Upozorňuje také na fakt, že vedle výhod kyberprostoru jako je například snadná komunikace nebo rychlý přístup k informacím, existují taky nevýhody v podobě páchání zločinu a hackerských útoků ohrožení vlád. První podkapitola hovoří o digitální stopě, což je záznam činností, které už nelze z prostředí internetu vymazat. Dále ji dělí na dva typy – ovlivnitelnou a neovlivnitelnou. Další podkapitola se zabývá sociálními sítěmi, konkrétně jejich definicemi a riziky, které s sebou může přinášet. Třetí podkapitola nabízí výčet nejužívanějších sociálních sítí jako je například Facebook,Instagram, YouTube, TikTok a další. Druhá kapitola se bude zabývat jednotlivými projevy kyberkriminality.

2 Projevy kyberkriminality

,,Nejobecněji je možné kyberkriminalitu definovat jako jednání namířené proti počítačovému systému, počítačové síti, datům či uživatelům nebo jako jednání, při němž je počítačový systém použit jako nástroj pro spáchání trestného činu. Neopomenutelnou skutečností pro to, aby bylo možné uplatnit definici kyberkriminality, je fakt, že počítačová síť, respektive kyberprostor, je pak prostředím, v němž se tato činnost odehrává''. (Kolouch, Bašta, 2019, s. 83)

Policie ČR definuje kyberkriminalitu jako ,,trestnou činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání''. (Policie ČR, online) Daňhelka ve výzkumné zprávě Vnímaní kyberkriminality mezi dětmi sděluje, že kyberkriminalita je vnímána jako kriminalita páchaná v kyberprostoru. Jedná se o obsáhlou skupinu trestných činů, které mezi sebou často nemají téměř žádnou souvislost. Dále odkazují na rozsáhlou existenci definic, co kyberkriminalita představuje. (Daňhelka, 2018, online) Kolouch a Bašta hovoří o tom, že neexistuje jednotná definice kyberkriminality, protože se rozvíjí jak využívání informačních a komunikačních prostředků, tak se vyvíjí i jejich zneužívání k páchání trestné činnosti. Kyberkriminalita prezentuje nejrozšířenější oblast pro veškerou trestnou činnost, která je páchána v prostředí informačních a komunikačních prostředků. Častokrát je tzv. ,,klasická trestná činnost'' převáděna do kyberprostoru, z důvodu rychlosti a efektivnosti páchání trestné činnosti, což může být např. šíření materiálů zobrazujících zneužívání dětí, podvody a jiné. V této souvislosti vznikají nové útoky, které ještě nebyly právem řešeny. (Kolouch, Bašta, 2019)

2.1 Kyberkriminalita na sociálních sítích

Následující podkapitola se zaměřuje na kyberkriminalitu páchanou na sociálních sítích. Policie ČR uvádí jako nejrozsáhlejší kyberšikanu, kybergrooming, kyberstalking a stalking. (Policie ČR, online)

Kyberšikana

Dle Hulánové je kyberšikana specifická forma šikany, která se vyskytuje na internetu, mobilních telefonech nebo na jiných moderních komunikačních technologií a má za cíl poškodit nebo zesměšnit jiného člověka. (Hulánová, 2012) Kohout popisuje kyberšikanu jako ,,klasickou šikanu'', která se přenesla do virtuálního světa a dává možnost agresorovi využít takové prostředky, jež mohou mít daleko větší důsledky na oběť než ve fyzickém světě. Kyberšikana dává možnost opakovaným útokům na jednotlivce díky využívání informačních a komunikačních technologií a životnosti dat v kyberprostoru. Kyberšikana může být kombinována se šikanou ,,klasickou'', např. nahrávání fyzického útoku oběti a následné sdílení tohoto útoku na internet. Obecně lze říci, že ke kyberšikaně je nezbytné používání informační a komunikační technologie nebo poskytované služby v kyberprostoru. (Kohout, 2016) Server Internetem Bezpečně upozorňuje, že důsledky kyberšikany mají mnohem větší dopad v porovnání s klasickou formou šikany:

- Oběť často nemůže identifikovat agresora a neví, proč ji ubližuje.
- Do kyberšikany se může zapojit větší počet útočníků, kteří mohou ponížení oběti pozorovat.
- Akt kyberšikany zůstane v kyberprostoru už navždy, což představuje stres pro oběť. Navíc intenzita tohoto aktu neklesá a nepřichází žádná úleva.
- S kyberšikanou se pojí pocit bezmoci a postižený neví, jak se má proti tomu bránit. (Internetem Bezpečně, online)

Kohout dále charakterizuje následující znaky kyberšikany:

- Pocit anonymity (Agresor si myslí, že je na internetu nedohledatelný.)
- Neomezenost útoku (Útočník může šikanovat bez ohledu na čas, prostor a zaútočit na každého jedince.)
- Neomezený okruh útoku útočníků (Útočníkem může být každý.)
- Neomezený prostor a prostředky (Agresor může útočit přes hanlivé poznámky, komentáře, sociální sítě, fotografie, videa aj.)
- Obtížná zjistitelnost (Oproti klasické šikaně se kyberšikana nemusí projevovat vnějšími znaky jako mohou být modřiny nebo ukradené peníze.)
- Trvalost (Útočící SMS, emaily, fotografie, videa apod. mají větší trvalost než fyzické útoky a agresoři se k nim vracejí. (Kohout, 2016)

Preventisté Policie ČR vymezují tyto formy kyberšikany:

- Publikace záznamu (Jde o sdílení videa, zvuku, textové online komunikace pomocí kamery, telefonu či jiného zařízení, který účelně zesměšňuje oběť, ruší soukromí nebo zahrnuje akt páchané šikany či násilí.)
- Falšování identity (Mezi falšovaní identity lze řadit falešné blogy a profily na sociálních sítích nebo prezentacích menších sociálních skupin, např: školní web, online komunity a různé formy ztrapňování.)
- Ukradení identity (útočník rozpozná heslo oběti, dostane se do jejího internetového profilu a díky tomu může škodit oběti, např: zcizení elektronického účtu ..).
- Ponižování a pomlouvání.
- Provokování a napadání uživatelů v online komunikaci.
- Zveřejňování cizích tajemství s cílem poškodit oběť.
- Vyloučení z virtuální komunity.
- Obtěžování.

Dále Preventisté Policie ČR uvádějí následující pokyny, jak se nejlépe chránit před kyberšikanou:

- Nebuďte přehnaně důvěřiví, nikdy nevíte, kdo je druhé straně.
- Nesdělujte citlivé informace (osobní údaje, osobní fotografie, hesla k účtům, apod).
- Respektujte ostatní uživatele.
- Seznamte se s pravidly služeb internetu a GSM sítí.

V případě už probíhajícího útoku, radí policisté České republiky podniknout tyto kroky:

- Říct o útocích dospělé osobě nebo známému.
- Zamítnout přístup agresora k vám, změnit svůj virtuální profil.
- Přerušit s pachatelem komunikaci a nepřemýšlet o pomstě.
- Snažit se útočníka identifikovat a vypátrat ho.
- Ukládat si potenciální důkazy, které mohou pomoci při vyšetřování (zprávy, videozáznamy, odkazy …).

- V případě probíhající šikany ve vašem okolí nebuďte pasivní, oběť podporujte a poskytněte pomoc. (Policie ČR, online)

Kybergrooming

Kopecký, Szotkowski a Dobešová definují kybergrooming jako ,,chování uživatelů virtuálního světa, které má za cíl vyvolat u vyhlédnuté oběti falešnou důvěru a po čase ji přimět k osobnímu setkání''. (Kopecký, Szotkowski, Dobešová, 2021, s. 14) Kopecký (2015, online) uvádí, že následkem tohoto setkání může být sexuální zneužití oběti, fyzické násilí, zneužití oběti pro dětskou prostituci či k výrobě dětské pornografie. Kybergrooming představuje formu psychické manipulace, která je prováděna prostřednictvím internetu, mobilních telefonů a jiných moderních komunikačních technologií. (Kopecký, 2015, online) Na tuto skutečnost odpovědělo trestní právo novou skutkovou podstatou trestného činu navazování nedovolených kontaktů s dítětem dle par. § 193 odst. b trestního zákoníku. (Zákon č. 40/2009 Sb., trestní zákoník) Dalším trestným činům, které jsou spojené s kyberkriminalitou se věnuje podkapitola 2.5 s názvem Kyberkriminalita z pohledu legislativy.

Kopecký Szotkowski a Dobešová charakterizují tzv. kybergroomery. Kybergroomeři se snaží o vzájemnou spolupráci a tvořit tzv. sítě predátorů, kde pak mohou společně vyhledávat, soustřeďovat a sdílet dětskou pornografii. V některých situacích i unášejí předem vybrané oběti. Z tohoto důvodu je pro ně charakteristická snaha o zabezpečení příhodných podmínek, kvůli bezpečnému přístupu k oběti a jistotě, tedy že oběti nebudou vzdorovat a zachovají diskrétnost. Díky tomu zamezí riziku odhalení zneužívání dítěte i vlastní totožnosti. Když se podíváme na jejich osobnost, tak mezi nimi nalezneme jedince s nízkým i vysokým sociálním postavením. Ačkoliv je veřejnost pokládá za pedofily, ve skutečnosti tomu však ve většině případů není, protože se zaměřují na děti straší 13 let, jedná se tedy o tzv. hebefily či efobofily, což znamená, že je přitahují dospívající dívky a chlapci, kteří se nachází v období puberty a dospívání. (Kopecký, Szotkowski, Dobešová, 2021)

Kohout a Karchňák uvádějí, že kybergroomingu může čelit prakticky každá osoba, zejména jde hlavně o dívky ve věku 11-17 let, které často využívají informační a komunikační technologie, mají nedostatečnou sebedůvěru a pocit osamělosti, neuvědomují si rizika internetové komunikace a nebrání se manipulaci. (Kohout,

Karchňák, 2016) V této souvislosti Kopecký a kol. (2015) sdělují tyto specifické rysy kybergroomingu:

- Manipulace - (Kybergrooming v sobě nese různé typy manipulativního jednání, např: uplácení, lichocení, dárky, peníze atd. Jaký typ tohoto jednání si nakonec útočník vybere, závisí na jeho typu osobnosti a osobnosti dítěte, například agresoři mohou u dítěte vyvolat pozitivní emoce až lásku, anebo naopak se může jednat o zastrašování a vydírání).
- Dostupnost obětí – (Díky moderním informačním a komunikačním technologiím mají útočníci neomezený výběr potenciálních obětí. Mají možnost oslovit dítě odkudkoli, a ještě přitom zůstat v anonymitě).
- Budování ,,vztahu'' – (Během komunikace s dítětem je pro pachatele podstatné si u něj vydobýt důvěru, získat si ho na svou stranu a podělit se o sexuální prožitky. Dle některých výzkumníků si pachatelé vybírají odlišné způsoby, např: nejdříve se zajímají, jaké má dítě koníčky a poté ho utvrzují v tom, že mají totožné zájmy. Agresoři jsou v průběhu komunikace s dětmi co nejvíce pozitivní, spolehliví a přívětiví, protože je nutné, aby jim děti nekompromisně věřily. Někdy se stalo, že se oběti do útočníka zamilovaly).
- Sexuální témata v komunikaci s dítětem – (Kdykoliv v průběhu konverzace s dítětem zařadí útočník vědomě sexuální témata. Může se jednat o flirtování, sexuální vulgarity, pornografické stránky či materiály. Vzájemné vyměňování takovýchto intimních materiálů je nebezpečné, protože může vést k vydírání. Agresoři takto činí také proto, aby zmenšili zábrany dítěte ve vztahu k sexu a sexuální témata se stala pro konverzaci běžným jevem).
- Posuzování rizik – (Zde se útočník rozmýšlí, jaký postup zvolit, aby nebyl vypátrán a povedlo se mu úspěšně dítě zmanipulovat a sexuálně zneužít. Z hlediska technické ochrany využívají pachatelé několik různých počítačů, upravují si IP adresy, disponují celou škálou podvodných online účtů. Poté přecházejí z veřejných chatů a sociálních sítí k soukromé konverzaci prostřednictvím osobních emailů, instant messengerů nebo mobilních telefonů.
- Podvádění – (Pro oběť je velice složité rozeznat, že její virtuální přítel na internetu nemluví pravdu, protože v mnoha případech si nevšímá výstražných faktorů, které se objevují v komunikaci. Pachatelé v některých situacích využívají falešnou identitu dítěte ke komunikaci s jiným dítětem a až při osobním setkání vyjde

najevo útočníkova pravá identita. Několik dětských obětí si uvědomuje, že jsou v kontaktu s dospělým jedincem, který jim lže a stejně ve spojení pokračují. (Kopecký a kol., 2015)

Kopecký (2015, online) z hlediska prevence považuje za efektivní způsob, jak s kybergroomingem bojovat, všeobecnou primární prevenci a výuku dětí v oblasti bezpečného používání internetových služeb, a to hlavně sociálních sítí. Existuje také celá řada preventivních programů, které budou detailněji rozebrány v závěru teoretické části. Podstatné je také informovat o nebezpečných formách komunikace rodiče, kteří tvoří nejvýznamnější článek prevence a mohou mít pozitivní vliv na děti už od raného věku. (Kopecký, online, 2015)

Je nezbytné zmínit rizikový jev, který se objevuje současně s kybergroomingem,a to **webcam trolling** a **kybersex.** Kopecký, Szotkowski a Dobešová sdělují, že na počátku se webcam trolling vyznačoval jako činnost tzv. internetových trollů, kteří pomocí webových kamer podněcovali ostatní jedince na internetu k emocionální odezvě, aby se pobavili. Postupně se tento fenomén proměňoval a v současnosti ho využívají kybergroomeři k vylákání intimních materiálů z vytipované oběti. (Kopecký, Szotkowski, Dobešová, 2021) Kybersex dle Hulánové značí online komunikaci, která má vyvolat sexuální vzrušení, příkladem může být vzájemné posílání zpráv sexuálního podtextu. Kybersex se stává škodlivým, pokud jednomu z účastníků je konverzace nepříjemná, např. svou vulgaritou. V takových případech se může jednat o posílání pornografických obrázků, návrhy zasílání intimních fotografií, vydírání a jiné další obtěžování. (Hulánová, 2012) Ševčíková v této souvislosti doplňuje, že aktuální kybersex značí veškerou sexuální aktivitu v online prostředí. Takovými sexuálními aktivitami může být vyhledávání partnerů pro bezplatný sex v reálném světě, které se může odehrávat na erotických seznamkách a v různých sexuálně orientovaných skupinách. Velký počet tradičních sexuálních aktivit byl nahrazen online formou jako je například vyhledávání a poskytování placených sexuálních služeb či online sledování pornografie. (Ševčíková In: Blinka a kol, 2015) Dále se budeme více věnovat dalšímu projevu kyberkriminality, a to sextingu.

Sexting

O zjevném propojení sextingu s kybergroomingem hovoří Kopecký, Szotkowski a Dobešová, protože díky citlivým materiálům, získá pachatel výhodu nad obětí a může

ji ovládat, vydírat a vyvíjet psychický nátlak s výhružkou, že určitý obsah uveřejní. V této souvislosti můžeme mluvit i o kyberšikaně a sexuálním vydírání (sextortion), které směřuje k tzv. eskalovanému sextingu. Eskalovaný sexting nastává v momentě, kdy začne nekontrolované šíření sextingových materiálů skrze všelijaké platformy. Následkem je ztráta společenské prestiže pověsti i oběti. (Kopecký, Szotkowski, Dobešová, 2021)

Hollá poukazuje na nejednotnou definici sextingu, která by přesně charakterizovala typy, účastníky, nástroje a základ tohoto jevu. Obecně se dá ovšem konstatovat, že sexting byl definován jako vytváření a umožňování poskytování texů, obrázků či videí se sexuálním a erotickým obsahem. (Hollá, 2016) Kopecký a kol. označují sexting jako ,,elektronické rozesílání textových zpráv, vlastních fotografií či vlastního videa se sexuálním obsahem, ke kterému dochází v prostředí virtuálních elektronických médií zejména internetu. Často jsou k sextingu využívány mobilní telefony či tablety. (Kopecký a kol, 2015, 43. s)

Szotkowski a kol. ve své publikaci uvádějí různá dělení sextingu. Nejprve rozlišují ,,self sexting'' a ,,peer sexting''. Self sexting představuje sdílení vlastních sextingových materiálů, jedná se o tzv. ,,sexty''. Peer sexting je forma sextingu, u které dochází k zasílání sextů jiné osoby. Peer sexting je nejfrekventovanější u vrstevníků neboli kamarádů a známých. V praxi však dochází k propojení těchto dvou typů sextingu, kdy se počáteční soukromý materiál, který je určený dané osobě (self texting), dostane do držení třetí strany (peer sexting) a v tomto tkví největší riziko sextingu. Další dělení rozděluje sexting na experimentální a přitěžující. Experimentální sexting znamená chování, které je u dospívajících charakterizováno potřebou flirtovat, objevováním romantických vztahů, vzbuzováním pozornosti vrstevníků či experimentováním v sexu. Přitěžující sexting se člení podle toho, jestli ho páchají dospělí nebo děti a podle cíle, zda jde o záměr ublížit (poškození oběti kvůli pomstě) nebo materiál necitelně zneužít (nejde o úmysl škodit oběti, ale jde o šíření materiálu bez souhlasu dané osoby). Autoři na závěr shrnují, že experimentální sexting je méně nebezpečný než přitěžující, ale důsledky sextingu se mohou objevit až později. (Szotkowski a kol., 2020)

Výsledky Výzkumu rizikového chování českých dětí v online prostředí z roku 2014, které provádělo Centrum prevence rizikové virtuální komunikace na Pedagogické fakultě Univerzity Palackého v Olomouci v kooperaci s firmou Seznam.cz, ukazují,

že 9,86 % dětí umístilo na internet své intimní fotografie či videa, kde jsou nazí úplně nebo zčásti. Celkem 12,14 % respondentů, z celkového počtu 28 232 respondentů, přiznalo, že takovýto obsah někomu zaslalo prostřednictvím internetu nebo mobilního telefonu. (Výzkum rizikového chování českých dětí v prostředí internetu 2014, online) V roce 2020 se konal podobný výzkum – Sexting a rizikové seznamování českých dětí v kyberprostoru, který byl taktéž zpracován centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci v součinnosti se společností 02 Czech Republic. Oproti výsledkům z roku 2014 se zvýšil počet dětí, které na internetu posílají jiným osobám své intimní materiály. Činí tak více než 15 % dětí v České republice. Důvodem může být posun ve vnímání lidské sexuality, transformace partnerských vztahů v prostředí internetu, konformita, nedostatečná prevence a přispět tomu mohou také nevhodné vzory, kterými se děti inspirují. (Sexting a rizikové seznamování českých dětí v kyberprostoru, 2017, online) Server sexting.cz uvádí, že děti se věnují sextingu hlavně v partnerských vztazích. Pod intimními materiály si lze nejčastěji představit ,,dárky'' pro přítele nebo přítelkyni, popřípadě odpovědi na tyto dárky. Intimní materiály se významně uplatňují také v případě, pokud jde o flirtování. V 35,47 % případů jsou využívány pro tento záměr. Dále jsou tyto materiály odesílány z legrace, nudy nebo pramení z touhy získat uznání v online komunitě. Znepokojujícím zjištěním je fakt, že více než 7 % dětí, které provozují sexting, bylo nuceno k tomuto chování někým jiným, a tedy posílání intimního materiálu nebylo dobrovolné. (Sexting.cz – vše, co chcete vědět o sextingu, online)

Web www.tonevymazes.cz, na kterém pracuje Policie ČR spolu s bezpečnostní firmou Eset uvádí pokyny k provozování bezpečnějšího sextingu:

- Fotografii umístěnou na internet, už nelze nikdy zaručeně vymazat, proto je podstatné na počátku zvážit, zda je nezbytné sdílet intimní fotku či video.
- Pořizovat a sdílet intimní fotografie a videa mohou osoby starší 18 let.
- Osobu, které posíláme fotografie, bychom měli znát osobně a mít v ní důvěru. Intimní fotografie může sdílet totiž i partner/ka.
- Posílejte fotografie jen osobě, která vás o ně vyzvala, popřípadě souhlasila s jejím zasláním.
- Zkontrolujte, že se nacházíte ve správném chatu, aby nedošlo ke sdílení neoprávněným osobám.

- Fotka by neměla obsahovat váš obličej, mateřská znaménka, výrazná tetování nebo piercing a další znaky, podle kterých by vás mohl někdo poznat.
- Důležité jsou také detaily na pozadí fotky. Neměly by ukázat vaší totožnost a místo bydliště, např. váš výhled z okna, domácí mazlíček apod. Dávejte pozor i na odraz v zrcadle.
- Vypněte funkci sdílení polohy v telefonu ještě před vznikem a sdílením fotografie, aby nebylo možné zjistit, kde jste fotografii pořizovali.
- Fotografie sdílejte pomocí aplikace s koncovým šifrováním, abyste měli jistotu, že komunikace setrvá pouze mezi vámi a příjemcem.
- Používejte funkci mizejících zpráv s možností upozornění, abyste byli informování o pořízení screenshotu.
- Zabezpečte své aplikace a účty na sociálních sítích bezpečným heslem a využívejte vícefázová ověření při přihlášení (ověření SMS kódem, otisky prstu).
- Fotky v nejlepším případě ihned po odeslání smažte, jak ze svého mobilu, tak i aplikace, přes kterou byly sdíleny.
- V případě, že si chcete nějaké fotky uchovat v telefonu, mějte přístup k fotkám zabezpečený otiskem prstu či rozpoznáním obličeje,
- Vypněte synchronizaci vaší fotogalerie do cloudu. Předejdete tak možnému odcizení fotek v případě napadení hackerů. (To nevymažeš, online)

Kyberstalking

Web Internetem Bezpečně popisuje kyberstalking jako nebezpečné pronásledování, kdy pachatel systematicky zneužívá informační a komunikační technologie k dlouhodobému, opakovanému a stupňovanému kontaktování své oběti. Jeho cílem je záměrně u oběti vyvolat pocity strachu, které se týkají jejího soukromí, zdraví či života. (Internetem Bezpečně, online) Kolouch uvádí, že kyberstalking představuje jednání, kdy útočník opakovaně kontaktuje oběť pomocí SMS zpráv, e-mailů, telefonních hovorů, messengerů a dalších nástrojů. (Kolouch, 2016) Web Internetem Bezpečně sděluje, že kyberstalking se navíc může objevovat ve formě opakovaného komentování příspěvků oběti na sociálních sítích, vkládání příspěvků na profily sociálních sítí oběti, krádeže identity oběti a její následné vystupování pod jejím jménem, oslovování oběti skrze falešnou identitu, monitorování počítače oběti speciálními programy, zveřejňování informací

ze života oběti a jiné. (Internetem Bezpečně, online) Kolouch charakterizuje chování kyberstalkerů, pro které jsou typické vytrvalost a systematičnost a také mají vytvořeno několik falešných identit, díky kterým získávají přístup ke svým obětem. (Kolouch, 2016)

Projekt 02 Chytrá škola realizovaný Nadací 02, uvádí na svých webových stránkách následujících 10 tipů, jak se bránit stalkerovi:

1. ,,Dejte stalkerovi najevo, že o jeho zájem nestojíte''.
2. ,,Neodpovídejte mu na vzkazy, nechoďte s ním na schůzky''.
3. ,,Změňte návyky, choďte a jezděte jinudy, nakupujte jinde''.
4. ,,Pokud už opravdu musíte mít profil na sociální síti, vytvořte si nový a pod jiným jménem, aby vás stalker hůř našel''.
5. ,,Schovejte si důkazy jako výhružné SMS, snímky chatů a e-maily''.
6. ,,Stalkera si zablokujte na všech sociálních sítích a platformách''.
7. ,,Pokud agresora znáte, nebojte se na něj přímo ukázat, říct o něm svému okolí''.
8. ,,Chraňte se. Myslete na své bezpečí''.
9. ,,Mluvte otevřeně s ostatními o tom, co se děje''.
10. ,,Pokud kyberstalking nebo stalking překračuje únosnou hranici, obraťte se na policii''. (02 Chytrá škola, online)

Tato podkapitola se věnovala kyberkriminalitě páchané na sociálních sítích. Věnovali jsme se kyberšikaně, kybergroomingu, kyberstalkingu a jevům příbuzným jako například kybersex či webcam trolling. Každý jev jsme definovali, uvedli různá dělení a typy, které se mohou vyskytovat a dále taky možnosti prevence. Dále se budeme věnovat podvodným jednáním na internetu.

2.2 Podvodná jednání

Zde se zaměříme na podvodná jednání, kde se podrobně budeme věnovat phishingu, spamu a online podvodům.

Phishing

Kolouch definuje phishing jako ,,podvodné či klamavé jednání, jehož cílem je získat informace o uživateli, jako jsou např. uživatelské jméno, heslo, číslo kreditní karty, PIN aj''. (Kolouch, 2016, s. 246) McCarthy a Weldon-Siviy užívají obecnější definici, phishing popisují jako ,, pokus vylákat z uživatelů osobní informace nebo finanční

údaje''. (McCarthy a Weldon-Siviy, 2013, s. 127) Základem phishingu, jak uvádí Kolouch, je zužitkování sociálního inženýrství, které se vyznačuje přesvědčováním a manipulací s lidmi, jehož záměrem je provedení určité činnosti nebo získání informací, jež by dotyční jedinci za jiných okolností neposkytli. Phishing se objevuje i v reálném světe v podobě různých podvodů, nicméně virtuální forma dává možnost útočníkovi šířit podvodné zprávy nesmírnému množství potenciálních obětí s minimálním úsilím. K phishingu dochází nejen prostřednictvím e-mailů, ale také v rámci rychlých zpráv (Skype,ICQ), sociálních sítí, SMS a MMS zpráv, chatů a podvodných nabídek práce nebo zboží. Níže se budeme těmto typům věnovat podrobněji, včetně falešných aplikací v prohlížeči a dalších forem phishingu.

Nejčastější formou phishingu, se kterou se můžeme setkat, je zasílání tzv. phishingových e-mailů oběti, kde však na první pohled není zřejmé, že jde o podvodnou zprávu. Takový e- mail často obsahuje odkaz, na který je uživatel vyzýván kliknout. (Kolouch,2016) Tento odkaz ve shodě s webem Policie České republiky může přesměrovat uživatele na falešnou internetovou stránku, již je takřka k nerozeznání s oficiální stránkou. (Policie České republiky, online) Kopecký a kol. popisují případ takovýchto falešných webových stránek, kdy se uživatel po kliknutí na odkaz v e-mailu dostane na stránku www.mojebanka.cn místo na oficiální stránku www. mojebanka.cz. Autoři zmiňují, že si jen malá část uživatelů všimne nesrovnalosti v chybné koncovce domény nebo celé adrese (Kopecký a kol, 2015). Policie ČR dále informuje, že mnohdy jde o zneužití přihlašovacích oken internetového bankovnictví. Nic netušící uživatelé do okénka správně vyplní jméno a heslo, čímž neúmyslně tyto údaje poskytnou pachatelům, kteří jim ihned poté kradou peníze z jejich účtu. Internetové podvody jsou záměrné a snaží se v uživateli vyvolat důvěru, aby útočníci získali značnou výhodu nebo se mohli lehce vyvinit z nezákonné činnosti. Dalším typickým znakem je časový tlak. Poškozený si ze začátku nemusí uvědomovat, že jde o trestný čin. Pozná to až v momentě, kdy má zablokovaný počítač nebo se dozví o neoprávněném čerpání finančních prostředků z účtu. (Policie České republiky, online)

Kolouch uvádí další formy phishingu. Pharming je více nebezpečná forma phishingu, protože tento útok cílí na DNS (Domain Name System) server, kde se překládá jméno domény na IP adresu. Stačí tedy, aby uživatel zadal v internetovém prohlížeči adresu webového serveru, kam se chce dostat. Poté nedojde k propojení na danou IP adresu oficiálního serveru, ale na falešnou IP adresu útočníka. Postup je dále stejný jako

u phishingu popsaného výše. Dalším typem je spear phishing. Ten se odlišuje od klasického phishingu , kde dochází více k náhodným útokům tím, že se zaměřuje většinou na konkrétní skupinu, organizaci, jednotlivce, informaci a data. Vishing představuje telefonický phishing, při kterém se pachatel snaží od uživatele zjistit citlivé informace za pomocí účelné manipulace a přesvědčování. Útočník se vydává za pracovníka banky či jiné instituce, aby zakryl svou pravou identitu. Smishing se podobá vishingu či phishingu s rozdílem, že využívá SMS zprávy k rozesílání zpráv. Cílem útočníků je přesvědčit uživatele k zavolání na placenou linku, poslání dárcovské SMS či kliknutí na pochybný odkaz. (Kolouch, 2016)

McCarthy a Weldon-Siviy z hlediska prevence uživatelům doporučují, aby nikdy neaktualizovali ani nezadávali číslo bankovního účtu, přihlašovací údaje, rodné číslo, přihlašovací jméno a heslo k instant messages a žádné další osobní informace bez ohledu na to, že stránka působí jakkoliv přesvědčivě. Oprávněné stránky bank a elektronických podniků totiž nikdy nezasílají e-maily, které by vyžadovaly čísla účtů, hesla ani další osobní informace. (McCarthy a Weldon-Siviy, 2013)

Spam

Kohout a Karchňák označují spam neboli spamming jako posílání nevyžádaných e-mailů. Jde o hromadné šíření elektronické pošty, kde se většinou objevují reklamní sdělení. (Kohout a Karchňák, 2016) Kolouch (2016) ve své knize uvádí, že v širším slova smyslu se za spam považují jakékoli doručené nevyžádané zprávy (zprávy obsahující viry, trojské koně a jiné). (Kolouch, 2016) V současnosti se můžeme setkat dle Kohouta a Karchňáka se spamem také v diskuzních fórech a různých messengerech. V případě, že dané zařízení nemá dostatečné zabezpečení, může po útoku viru samo rozesílat spam, aniž by o tom uživatel věděl. Velká část spamových e-mailů v sobě zahrnuje malware, což je škodlivý kód, jenž může z počítače odcizovat osobní data uživatele. Kolouch (2016) charakterizuje formu spamu, případně i scamu, a to hoax. Hoax jsou řetězové zprávy, jež obsahují nepravdivé, zkreslené, zavádějící nebo další podvodné informace. Příklady hoaxu mohou být varování před útoky, jednotlivé druhy nebezpečí, žádosti o pomoc, projevy slavných osobností, obrázky a videa v prezentacích, hrající si zvířátka (kočičky) a jiné. (Kolouch, 2016)

Z hlediska ochrany proti spamu autoři doporučují nezveřejňovat svou e-mailovou adresu, pokud to není nezbytné. V případě, že ji musíte někomu sdělit, pište

ji v následujícím formátu: jmeno(zavinac)domena.cz, kdy místo znaku zavináče ho napíšete slovem. Program či robot shromažďující e-maily s cílem dále rozesílat spam, totiž e-mailovou adresu v tomto tvaru nezpracuje a vynechá ji. Buďte opatrní při potvrzování registrací a objednávek a pečlivě uvažte souhlas se zasíláním reklamních sdělení, abyste předešli potenciálnímu spamu. Pokud vám přijde spam do elektronické pošty, v žádném případě ji neotvírejte, nahlašte ho a poté smažte. Neklikejte na odkazy či různá tlačítka. Jestliže jste někde dali souhlas zasílání reklamního sdělení, v úplném závěru této zprávy se obvykle nachází tlačítko ,,odhlásit''. (Kohout a Karchňák, 2016)

Scam

Kopecký, Szotkowski a Kubala popisují odlišné formy online podvodů, které shrnují pod název SCAM. Se scamem přijdou do kontaktu děti i dospělí využívající internetové služby. Scam se roznáší hlavně skrze spam, avšak také v omezeném rozsahu díky sociálním sítím. (Kopecký, Szotkowski, Kubala, 2022)

Kolouch popisuje jako jeden z typů scamu tzv. Scam 419, což je označení e-mailů, jenž jsou známější pod názvem Nigerijské dopisy. Tato forma podvodného jednání znázorňuje příklad přenosu normální kriminality z fyzického světa do světa online prostředí. (Kolouch, 2016) Kopecký, Szotkowski a Kubala doplňují, že tyto dopisy nabízejí okamžité zbohatnutí. Aby se tak stalo, je nutné uhradit všelijaké poplatky, daně, pojištění a další. V realitě žádného bohatství nedosáhneme, protože význam tohoto podvodu spočívá v ochotě platit menší finanční obnos za účelem vydělání milionů. Završnik představuje konkrétní příklad takovýchto dopisů. Jedná se o e-mail sdělující pochybnou angličtinou uživateli, že mu bohatý strýc (o němž nikdy neslyšel) odkázal miliony dolarů v podobě zlatých prutů. Aby je získal, musí však zaplatit menší zálohu. (Završnik, 2017)

Autoři Kopecký, Szotkowski a Kubala dále uvádějí další formu online podvodu, a to tzv. podvody s m-platbami (platby skrze mobilní telefon). Ten se zakládá na skutečnosti, že útočník duplikuje profil našeho známého, který vypadá důvěryhodně (nakopíruje tam jeho fotku, jméno, příjmení a jiné informace z původního profilu a následně nás kontaktuje o pomoc. Snaží se od nás zjistit kód, který nám byl doručen na náš mobilní telefon. Tento kód má ověřovat finanční transakci, kterou může být například platba v internetovém obchodě. V momentě, kdy bychom kód sdíleli našemu ,,známému'', je velice pravděpodobné, že peníze z našeho účtu budou odcizeny.

Podobně cílený podvod, který se týká platební karty, je CVV (card verification value) či CVC (card verification code). Jedná se o číslo vyskytující se na zadní straně platební karty, jenž má autorizovat transakci. Toto číslo se zadává při každé online platbě, proto je důležité být pozorný, kde toto číslo vyplňujeme. Dalšími aktuálně rozšířenými podvody v online prostředí jsou podvody spojené s nákupem a prodejem zboží zvlášť na inzertních serverech, například Sbazar. Pachatelé na oko jeví zájem o dané zboží, a poté zasílají odkaz s falešnou platební bránou, který vyžaduje všechny potřebné údaje o kreditní kartě uživatele. V případě vyplnění, můžou uživatelé přijít o své finance na bankovním účtu. Abychom předcházeli těmto jevům, je nezbytné dětem ukázat a vysvětlit, jak mohou být online nákupy prostřednictvím platebních karet nebezpečné. Děti by měly každou transakci konzultovat s rodiči bez ohledu na výši platby a zároveň mít nastavené potvrzování online plateb pomocí mobilního telefonu. (Kopecký, Szotkowski, Kubala, 2022)

V této podkapitole jsme se věnovali podvodnému jednání, kam můžeme zařadit phishing, spam a online podvody (scam). Tyto jednotlivé formy podvodného jednání jsme představili, uvedli jejich konkrétní příklady a na závěr uvedli rady, kterými se řídit, abychom se mohli co nejefektivněji proti těmto útokům bránit. Následuje podkapitola, kde se soustředíme na internetové pirátství.

2.3 Internetové pirátství

Kolouch (2016) sděluje, že pojem Internetové pirátství je obecným pojmem pro kriminalitu a dopouští se porušování práva duševního vlastnictví. V častých případech je internetové pirátství omezeno pouze na autorské právo. Autor vymezuje dvě oblasti práva duševního vlastnictví. První oblastí je autorské právo, příkladem jsou původní literární a umělecká díla, hudební skladby, počítačové programy. Druhou oblast představují průmyslová práva, jejichž příkladem mohou být patenty na vynálezy, ochranné známky a jiné. (Kolouch, 2016)

Kopecký, Szotkowski a Kubala informují, že jakýkoli obsah na internetu podléhá Zákonu č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů. Tento zákon zajišťuje ochranu literárních, vědeckých a uměleckých děl, například hudby, filmu, výkresů, ale i počítačové programy (hry, aplikace) a další. Autoři ve shodě s tímto zákonem uvádějí, že bezplatným stahováním pro osobní potřebu (offline) jako jsou právě hry, filmy či hudba, uživatel nepáchá nic

protizákonného. Avšak tento obsah nesmí dál šířit, organizovat veřejné projekce díla na veřejnosti nebo promítat většímu počtu lidí a dále uživatel nesmí vyžadovat finanční obnos za nelegální obsah. Výjimkou jsou počítačové programy, které se nesmí stahovat ani pro osobní potřebu. To se netýká programů označovaných jako freeware,shareware, trial a jiné druhy programů, jež jsou zdarma. Typickým nástrojem pro stahování větších souborů je tzv. BitTorent, jehož stahováním a šířením uživatelé porušují zákon. Torrent je souborem, který zahrnuje informace o tom, kdo jej sdílí, jak se člení, jakou se vyznačuje velikostí apod. Při stahování prostřednictvím torrentů dochází současně k jeho rozesílání, a to je protizákonné jednání. (Kopecký, Szotkowski, Kubala, 2022) McCarthy a Weldon-Siviy zmiňují nejčastěji nelegálně stahované položky, kterými jsou hudba, filmy, programy a videohry. (McCarthy a Weldon-Siviy, 2013)

Internetové pirátství se týká porušování práv duševního vlastnictví a zejména autorských práv. Tato forma kriminality se často zaměřuje na obsah, který podléhá ochraně autorského práva. Jedná se o literární a umělecká díla, hudbu a počítačové programy. Bezplatné stahování pro vlastní potřebu není nelegální, avšak šířením obsahu, veřejnou projekcí a komerčním využitím se uživatel dopouští protiprávního jednání. Poslední podkapitola detailně popisuje hacking, jako projev kyberkriminality.

2.4 Hacking

Web Policie ČR popisuje hacking jako jednání, při kterém dochází k narušování dat, systémů a také zneužívání zařízení. Nejčastěji jde o jednání pachatele, který pronikne přes zabezpečení počítačového systému a získá citlivé údaje o oběti. Nedílnou součástí takovýchto jednání je také rozesílání škodlivých kódů, implementace tzv. backdoorů do přístupných softwarů a jiných. V současnosti se stává více frekventovanější napadení e-mailových adres, účtů na sociálních sítí, internetového bankovnictví, jejichž důsledkem je ztráta soukromí, citlivých informací a také financí. S tímto se pojí další trestná činnost jako je vydírání, stalking, krádeže z účtů a různé podvody. Dalším druhem hackingu může být porušování tajemství dopravovaných zpráv, který se nejčastěji projevuje tzv. sniffingem, jenž se vyskytuje při využívání nezabezpečených wi-fi připojení, manipulaci s e-mailovými servery nebo i v nynější době při napadení domácích routerů. (Policie České republiky, online) Kolouch (2016) říká, že sniffing představuje nelegální odposlech a záznam komunikačního provozu. Aby se jednalo o kyberkriminalitu, musí

tak pachatel činit bez vědomí uživatele. Ze zadržených dat získaných pomocí sniffingu může pachatel vytáhnout a složit citlivé informace o oběti, například přihlašovací údaje, e- mailovou adresu, komunikaci a další. Mezi další skupinu útoků se řadí DoS útoky. DoS v překladu ,,odepření či odmítnutí služby'' znamenají formu útoku na internetovou službu, jejímž hlavním cílem je vyřadit nebo snížit výkon napadeného technického zařízení. Smyslem tohoto útoku je zahltit infikovaný počítačový systém nebo síťový prvek opakovanými požadavky na činnosti, které má systém vykonat. DoS útok lze rozpoznat podle abnormálně zpomalených poskytovaných služeb, úplné nebo dočasné nedostupnosti služby, například webové stránky a jiné. DoS útok má zdroj pouze jeden a je poměrné lehké se mu ubránit, to však neplatí u DDoS útoku, kde je zdrojů více a jsou náhodně rozmístěny, což napomáhá k utajení identity pachatele. Šulc poznamenává, že v případě útoku DDoS se nám daná služba může ukazovat jako nefunkční či nedostupná. (Šulc, 2018) Kolouch zmiňuje nejčastěji se vyskytující aktivity hackerů, mezi ně patří sociální inženýrství, prolamování hesel, skenování portů, zneužívání malware k proniknutí do počítačového systému, phishing, cros site script a odposlech komunikace. (Kolouch, 2016)

Tato podkapitola se věnuje hackingu. Uvedli jsme, co hacking znamená, jaké jsou jeho nejčastější formy a techniky. V další kapitole budeme analyzovat kyberkriminalita z hlediska současné legislativy.

2.5 Kyberkriminalita z pohledu legislativy

V páté podkapitole budeme rozebírat projevy kyberkriminality, popsané v předchozí části, z hlediska legislativy. Web E-bezpečí sděluje, že mnohé pojmy trestní zákon neuvádí, nicméně pod sebe shrnuje odlišné trestné činy, které mohou útočníci páchat. Některé trestné činy se objevují u více pojmů (E-bezpečí, 2009, online)

Kyberšikana

Server E-bezpečí uvádí, že kyberšikanu jako pojem trestní zákoník nezná, avšak v souvislosti s kybešikanou se pachatel může dopouštět těchto trestných činů uvedených v trestním zákoně: Ublížení na zdraví dle § 146, Omezování osobní svobody dle § 171, Vydírání dle § 175, Pomluva dle § 184, Krádež dle § 205, Podvod dle § 209, Poškozování cizí věci dle § 228, Násilí proti skupině obyvatel a jednotlivci § 352, Nebezpečné

vyhrožování dle § 353, Nebezpečné pronásledování (stalking) dle § 354 (E-bezpečí, 2009, online)

V rámci kyberšikany se mohou objevovat i násilné projevy směřující proti etnické, rasové či jiné skupině. Web Policie ČR píše, že se může jednat i o následující trestné činy: Hanobení národa, rasy, etnické nebo jiné skupiny osob dle § 355, Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod dle § 356 a také Šíření poplašné zprávy podle § 357. (Policie České republiky, online)

Kybergrooming

Tento pojem upravuje trestní zákoník dle § 193 odst. B Navazování nedovolených kontaktů s dítětem – ,,Kdo navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle § 187 odst. 1 - Pohlavní zneužití, § 192 – Výroba a jiné nakládán s dětskou pornografií, 193 – Zneužití dítěte k výrobě pornografie, § 202 odst. 3 – Svádění k pohlavnímu styku nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta''. (Zákon č. 40/2009 Sb., trestní zákoník.) Web E-bezpečí uvádí další možné trestné činy ve spojitosti s kybergroomingem: Obchodování s lidmi § 168, Omezování osobní svobody § 171, Vydírání § 175, Ohrožování výchovy dítěte § 201, Podvod § 209, Nebezpečné vyhrožování § 353, Nebezpečné pronásledování § 354 trestního zákoníku. (E-bezpečí, 2009, online)

Sexting

Kopecký a Szotkowski popisují trestné činy spojené se sextingem, které podléhají trestnímu zákoníku a těmi jsou: Výroba a jiné nakládání s dětskou pornografií § 192, Zneužití dítěte k výrobě pornografie § 193, Sexuální nátlak § 186, Pohlavní zneužití § 187, Znásilnění § 185, Nebezpečné pronásledování § 354, Účast na pornografickém představení § 193a nebo také Navazování nedovolených kontaktů s dítětem § 193b a Svádění k pohlavnímu styku § 202 trestního zákoníku. (Kopecký a Szotkowski, 2019, online) Server E-bezpečí navíc konstatuje, že pachatel dopouštějící se sextingu, porušuje trestní zákoník dle § 171 Omezování svobody a § 201 Ohrožování výchovy dítěte. (E- bezpečí, 2009, online)

Zneužití osobních údajů

Pod skupinu trestných činů spojených se zneužitím osobních údajů můžeme zařadit podvodná jednání a internetové pirátství. (viz 2.2 a 2.3) Web E-bezpečí uvádí tyto trestné činy uvedené v trestním zákoníku, jichž se mohou pachatelé dopouštět, jedná-li se o zneužití osobních údajů: Vydírání § 175, Útisk § 177, Neoprávněné nakládání s osobními údaji § 180, Poškození cizích práv § 181, Porušování tajemství dopravovaných zpráv § 182, Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí § 183, Pomluva § 184, Podvod § 209, Lichva § 218, Zneužívání vlastnictví § 229, Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi § 270 a Nebezpečné pronásledování § 354 trestního zákoníku. (E-bezpečí, 2009, online)

Hacking

K hackingu se podle webu Policie ČR pojí trestný čin dle § 230 trestního zákoníku Neoprávněný přístup k počítačovému systému a nosiči informací. Dále to může být trestný čin dle § 182 trestního zákoníku Porušování dopravovaných zpráv. (Policie České republiky, online)

Tato podkapitola se zaměřovala na protiprávní jednání u jednotlivých projevů kyberkriminality dle trestního zákoníku. U každé uvedené formy kyberkriminality jsme uvedli paragraf, dle kterého je upraven v trestním zákoně. Některé trestné činy se vyskytují u více pojmů. Následuje závěrečná kapitola teoretické části, která nese název Kyberkriminalita z pohledu dětí, kde se budeme věnovat životnímu stylu dětí, škole jako prevenci a v neposlední řadě také preventivním programům z oblasti kyberkriminality.

3 Kyberkriminalita a její prevence u dětí

Třetí kapitola se věnuje kyberkriminalitě z pohledu dětí. Nejdříve první podkapitola popisuje životní styl dětí, který se v současné době pojí zejména s internetem. Následuje podkapitola věnující se škole jako prevenci a v závěru kapitoly zmiňujeme příklady preventivních programů.

3.1 Životní styl dětí

Kraus definuje životní styl následovně ,,životní styl je charakterizován jako široký komplex činností a s nimi spjatých, postojů, norem, hodnot, návyků, které mají trvalý ráz a jsou pro každého individuálně specifické – vystihují osobitost jeho chování''. (Kraus, 2015, s. 92) Tentýž autor uvádí, že životní styl jedince a jeho primární charakteristické rysy podléhají vnějším a subjektivním/individuálním faktorům. Vnějšími faktory se myslí všeobecné, celospolečenské či v užším pojetí skupinové (například rodinné) životní podmínky. Vnitřními faktory jsou konkrétní potřeby jednotlivce, hodnoty, zájmy, životní cíle, dovednosti,schopnosti a další. (Kraus, 2015)

Ve shodě se Šmahetem jsou dnešní děti vystavování nepřetržitému vlivu digitálním médiím, kterými se myslí počítače, notebooly, mobily, herní konzole tablety a jiná zařízení. Děti nejčastěji využívají tato zařízení k přístupu na internet, zábavě jako například hraní her, ale hlavně k vzájemné online komunikaci. Autor dále zmiňuje, že internet může představovat různá rizika, ale také hlavně příležitost. Příležitostí se myslí vzdělávání, zlepšování psané komunikace (například v cizím jazyce), učení se sebereprezentaci, práce s různými programy, tvoření webových stránek, programování atd. (Šmahet In: Ševčíková a kol., 2015) Bakošová zmiňuje, že současné komunikační technologie se značně podílejí na nárůstu podnětů, kvůli kterým je dětská organismus zaplavován. Zvyšuje se počet dětí s neurotickými příznaky, hyperaktivitou a smyslovými poruchami. Podle posledních údajů více než 10 % dětí na základních školách potřebuje péči psychologa. Dále výzkumy varují, že dlouhodobým sledováním televize, internetu, hraním počítačových her apod. dochází k přetížení smyslů. Důsledkem je skutečnost, že děti zůstávají bez zájmu, emocionálně zakrňují a reagují pouze na silné a agresivní podněty, jakými jsou například zvuky či pohyby. (Bakošová, 2017) Spitzer ve svém díle řadu negativních vlivů médií, například hraní násilných her vede k násilnictví, otupělosti, sociální osamělosti. Dalším negativním aspektem může být

nespavost, která patří k nežádoucím efektům používání digitálních médií. Nedostatek spánku může vést i k depresím, které naopak narušují spánek. (Spitzer, 2014)

Kraus ve své publikaci sděluje, že dnešní postmoderní společnost můžeme vnímat jako prostředí, které má velký vliv na formování kyberprostoru, jenž je specifický svým časovým rozmezím a aktivně ovlivňuje čas fyzického světa. Kyberprostor překonal prostorové omezení a dal tak možnost všem uživatelům být neustále online a sdílet jeden společný čas na celém světě. Masová média mají nepoměrně větší vliv než intencionální výchova, kterou má na starost škola nebo jiné výchovné instituce. Masmédia účinkují v procesu funkcionální výchovy, kde je jedinec formován prostředím, kterému se přizpůsobuje. Z toho vyplývá, že možnosti efektivní intervence do vztahu média – mladistvý reipient jsou velmi omezené a často ne příliš účinné. Autor zmiňuje Rámcový vzdělávací program, který na tuto problematiku reaguje zařazením mediální výchovy do škol. Hlavním cílem je naučit mládež efektivně využívat média pro své účely a nikoliv aby se stala jejím otrokem. Důležitou úlohu v tomto boji s médii hrají pedagogové a rodiče.

V uvedené podkapitole jsme se věnovali životnímu stylu dětí ve vztahu s masmédii, které mají čím dál tím větší vliv na dnešní mládež. Popsali jsme klady a zápory digitálních médií a závěr podkapitoly se věnoval vlivům masmédií na výchovu. Na to navazuje další podkapitola, která nese název Škola jako prevence.

3.2 Škola jako prevence

V další podkapitole se zaměříme na prevenci ve školním prostředí a její druhy. Dále uvedeme dokumenty, kterými se škola z hlediska prevence řídí a popíšeme školský poradenský systém.

Úrovně prevence

Čech uvádí, že ,,pojmem prevence označujeme všechna opatření směřující k předcházení a minimalizování jevů spojených s rizikovým chováním a jejich důsledků. Jedná se zejména o předcházení a minimalizaci různých souvisejících poruch a onemocnění, poškození, úrazů atd. a dále pak samotných projevů rozmanitých typů rizikového chování, které ohrožují společnost a jedince v ní''. (Čech In Miovský a kol, 2015, s. 143)

Bělík a Hoferková popisují **primární prevenci** jako ,,komplex činitelů, kteří působí na jedince. Jedná se především o rodinu a školu, ale také o působení lokálního prostředí především prostřednictvím občanských sdružení''. (Bělík a Hoferková, 2016, s. 19) Dále tito autoři zmiňují tzv. těžiště primární prevence'', na které působí výchova, vzdělávání, volnočasové aktivity, poradenství a práce s hodnotami dětí a mládeže. Primární prevence se orientuje na populaci, která se s ní ještě nesetkala a její nedostatek můžeme označit za chybu aktuální společnosti. Na závěr autoři zdůrazňují, že důležitou úlohu v primární prevenci by měly hrát škola a rodina. (Bělík a Hoferková, 2016) Metodické doporučení k primární prevenci rizikového chování u dětí, žáků a studentů ve školách a školských zařízeních uvádí dělení primární prevence na **specifickou primární prevenci** a **nespecifickou primární prevenci.** Do specifické primární prevence zahrnujeme aktivity a programy, jež jsou cíleny specificky na předcházení a snižování výskytu daných forem rizikového chování. Jde o:

- **všeobecnou prevenci**, která se orientuje na širší obyvatelstvo, aniž by v minulosti byl zkoumán rozsah problému a rizika,
- **selektivní prevenci**, jenž se specializuje na žáky, u kterých můžeme prediktovat zvýšený výskyt rizikového chování,
- **indikovanou prevenci**, ta je určena jednotlivcům a skupinám, u nichž byl registrován vyšší výskyt rizikových faktorů v oblasti chování, problematických vztahů v rodině, ve škole či s vrstevníky.

Nespecifická prevence pak zahrnuje jakékoli aktivity, které podporují zdravý životní styl a přijetí pozitivního sociálního chování skrze smysluplné využívání a organizaci volného času, tedy zájmových, sportovních a volnočasových aktivit a dalších programů směřující k dodržování daných společenských pravidel, zdravého rozvoje osobnosti, k odpovědnosti za svou osobu a své jednání. (Metodické doporučení k primární prevenci rizikového chování u dětí a mládeže (dokument **č.j.**21291/2010-28, 2010, online) Čech doplňuje, jestliže přestanou fungovat strategie na stupni selektivní a indikované prevence, je na řadě prevence **sekundární** a **terciární**. Sekundární a terciární prevence je určena osobám se závažnými formami rizikového chování, které nelze odstranit obvyklými preventivními opatřeními (drogové závislosti, sexuální agrese a další). Cílem sekundární a terciární prevence je zamezení možným recidivám a eliminování co nejvíce rizik, která souvisejí s určitým typem rizikového chování a životního stylu jednotlivce. V rámci terciární prevence je řeč o reedukaci, to znamená

vědomé posilování pozitivních vlastností osobnosti, které nedosáhly dostatečného vývoje a resocializaci, což je usměrnění závislého nebo problémového jedince, například po výkonu trestu, k novým životním hodnotám jako je smysluplné trávení volného času, čas s rodinou atd. (Čech In:Miovský a kol, 2015, 143-148 s.)

Školský poradenský systém

Bělík a Hoferková sdělují, že ve školním prostředí uskutečňují prevenci hlavně pedagogové v oblasti tzv. školského poradenského systému. Ten se skládá ze školských poradenských pracovišť (pedagogicko-psychologické poradny, speciálně pedagogická centra a zařízení preventivně výchovné péče – střediska výchovné péče) a specializovaných pedagogických pracovníků, mezi které patří školní metodik prevence, výchovný poradce, školní psycholog, školní speciální pedagog a sociální pedagog. Autoři také vyzdvihují důležitou úlohu třídních učitelů, protože právě ti znají nejlépe, čím se děti trápí a jaký problém řeší. (Bělík, Hoferková, 2016)

Dokumenty Ministerstva školství, mládeže a tělovýchovy

Podstatným dokumentem je **Národní strategie primární prevence rizikového chování dětí a mládeže na období 2019-2027**. ,,Národní strategie 2019-2027 je základním strategickým dokumentem MŠMT, který tvoří/vytváří základní rámec politiky primární prevence rizikového chování v České republice''. (Národní strategie primární prevence rizikového chování dětí a mládeže na období 2019-2027, 2019, s. 4, online) Tento dokument navazuje na Národní strategii primární prevence rizikového chování z období 2013-2018. Současná Národní strategie 2019-2027 stanovuje základní pilíře politiky primární prevence, kterými jsou systém, koordinace, legislativa, vzdělávání, financování, monitoring, hodnocení a výzkum. (Národní strategie primární prevence rizikového chování dětí a mládeže na období 2019-2027, 2019, online)

Dalším důležitým dokumentem MŠMT je **Minimální preventivní program**. Čech označuje minimální preventivní program (MPP) jako hlavní nástroj školní prevence. Minimální preventivní program při správném rozvržení má plnit úlohu komplexního systémového prvku v uskutečňování preventivních aktivit v základních a speciálních školách, ve školských zařízeních pro výchovu mimo vyučování a školských zařízeních pro výkon ústavní a ochranné výchovy a také preventivně výchovné péče. K realizaci MPP se zavazuje každá škola a zároveň podléhá kontrole České školní inspekce. (Čech

In: Miovský, 2015, 143-148 s.) Bělík a Hoferková uvádějí, že za zpracování MPP je odpovědný školní metodik prevence. MPP se vytváří na jeden školní rok a jeho vyhodnocení je součástí výroční zprávy o činnosti školy (Bělík a Hoferková, 2016)

Bělík a Hoferková konstatují, že ,,základním dokumentem pro realizaci prevence na školách, který slouží jako výchozí bod pro tvorbu minimálního preventivního programu, je **školní preventivní strategie**''. (Bělík a Hoferková, 2016, s. 75) Dle Metodického doporučení k primární prevenci rizikového chování u dětí, žáků a studentů ve školách a školských zařízeních je školní preventivní strategie dlouhodobým preventivním programem, který je koncipován tak, aby účinně odpovídal podmínkám určité školy, jejího okolí a zároveň respektoval rozdíly ve školním prostředí. Primárně slouží jedincům z nejvíce ohrožených skupin (minoritám, cizincům, dětem, pacientům), kteří potřebují pomoct se zajištěním jejich lidských práv a povinností. Zároveň přispívá ke zdravému životnímu stylu, tedy tělesnému a duševnímu pocitu blaha (výchova ke zdraví, duševní hygiena, pohybové aktivity a jiné). (Metodické doporučení k primární prevenci rizikového chování u dětí a mládeže (dokument **č.j.**21291/2010-28, 2010, online)

V této podkapitole jsme se věnovali tématu škola jako prevence. Nejdříve jsme uvedli jednotlivé úrovně prevence, dále jsme představili školský poradenský systém a jeho části. Na závěr této podkapitoly jsme uvedli dokumenty MŠMT upravující prevenci ve školách, kterými jsou Národní strategie primární prevence rizikového chování dětí a mládeže na období 2019-2027, Minimální preventivní program a Školní preventivní strategie. Poslední dva uvedené dokumenty vycházejí z dokumentu Metodické doporučení k primární prevenci rizikového chování u dětí a mládeže (dokument **č.j.**21291/2010-28, 2010). Třetí podkapitola navazuje na preventivní programy týkající se prevence kyberkriminality.

3.3 Preventivní programy

V této podkapitole představujeme celorepublikové projekty tvoří preventivní programy a projekty, které se zaměřují na prevenci v oblasti kyberkriminality.

E-Bezpečí

Realizátorem Projektu E-Bezpečí je Centrum prevence rizikové virtuální komunikace Univerzity Palackého v Olomouci (dále Centrum PRVok). PRVok představuje certifikované univerzitní pracoviště zaměřující se primárně na kyberšikanu, kyberstalking, kybergrooming, hoax a spam, sexting, sociální inženýrství v online prostředí, sdílení osobních údajů v prostředí sociálních sítí a ostatní rizikové komunikační jevy. Centrum PRVoK navazuje spolupráci s několika známými firmami, jakými jsou například Google, Seznam.cz, 02 Czech republic, Vodafone, IBM, Allegro Group, Policií ČR, Národní centrálou proti organizovanému zločinu a mnoha dalšími institucemi. (Univerzita Palackého v Olomouci, online)

Webové stránky E-Bezpečí uvádějí, že se projekt orientuje na prevenci, vzdělávání, výzkum, intervenci a osvětu, které jsou propojeny s rizikovým chováním v online prostředí. Během posledních let projekt poskytuje pozitivní využívání IT ve vzdělávání a běžném životě. Mezi hlavní témata, kterými se tento projekt zabývá patří tyto:

- kyberšikana a sexting,
- kybergrooming,
- kyberstalking a stalking,
- rizika sociálních sítí,
- hoax,spam a fake news,
- online závislosti,
- youtubering,
- zneužití osobních údajů v prostředí elektronických médií.

Dále web E-Bezpečí představuje cílové skupiny, které tvoří žáci a studenti od 1. stupně ZŠ, učitelé, preventisté sociálně patologických jevů, metodici prevence, policisté, manažeři prevence kriminality, vychovatelé, OSPOD pracovníci a samozřejmě také rodiče. Základním prvkem tohoto projektu je terénní práce. Ta probíhá prostřednictvím přednášek, diskuzí a preventivních vzdělávacích akcí. Cílem těchto akcí je identifikovat rizikové jevy na internetu a poskytnout tak návody a strategie k prevenci a obraně před potenciálními pachateli. Přednášky a diskuse vysvětlují různé nebezpečné scénáře a nabízejí konkrétní řešení a opatření k minimalizaci rizikového chování. Základní myšlenkou je vytvořit obraz problému prostřednictvím modelových situací a skutečných případů, které účastníkům pomohou lépe pochopit problematiku

a identifikovat možná rizika. Tato sezení jsou interaktivní a multimediální, doprovázená prezentacemi a videoukázkami, které pomáhají přiblížit abstraktní pojmy a zásady online bezpečnosti na konkrétních příkladech a situacích. Tento přístup zvyšuje účinnost školení a poskytuje účastníkům praktické nástroje, které jim umožní chránit se v digitálním prostředí. (E- Bezpečí, online)

Tvoje cesta onlinem

Tvoje cesta onlinem je název preventivního projektu založený v roce 2019 a je vedený Policií ČR v kooperaci s ČSOB (Československou obchodní bankou). Hlavním cílem tohoto programu je seznámit mladé lidi s možnými riziky, která na ně číhají na internetu a také prevence. Projekt ukazuje dětem způsoby, jakými se online predátoři prezentují v online prostředí a jak přistupují ke svým potenciálním obětem a vědomě manipulují s jejich myšlením, které využívají ve svůj prospěch. Tento projekt je určen žákům druhého stupně základních škol, jejich rodičům a všem dospělým osobám. Policisté, kteří se zaměřují na preventivní práci s dětmi, poskytují informace koho kontaktovat v případě nouze a také zmiňují konkrétní rizika spojená s online komunikací. Důležitou součástí je interaktivní přístup, jenž má upoutat pozornost dětí a zajistit, aby byl sdílený obsah na sociálních sítích pro ně lépe pochopitelný. Projekt se zaměřuje také na rodiče jako klíčový faktor prevence. Jsou pro ně připravovány semináře a besedy, které jim umožní získat základní informace o zajištění bezpečnosti svých dětí na internetu. Přednášejícími na těchto akcích jsou speciálně vyškolení policisté a odborní ambasadoři z ČSOB. (Policie ČR, online)

Safer Internet Centrum Česká republika

Safe Internet Centrum ČR (SIC CZ) je společnou aktivitou čtyř organizací, které díky svým znalostem, dovednostem a nadšením dělají pro děti a mládež internet bezpečnějším. Koordinátorem SIC CZ je sdružení CZ.NIC od roku 2019 a dalšími partnery jsou Linka bezpečí, Dětské krizové centrum a vzdělávací program společnosti Člověk v tísni. Společnou práci těchto organizací tvoří tři pilíře: centrum prevence, linka důvěry a horká linka pro nahlašování nelegálního digitálního obsahu. Centrum prevence se orientuje na aktivity, které mají zvýšit povědomí a prohlubování znalostí dětí, učitelů, vychovatelů a rodičů o bezpečnosti na internetu. Linka důvěry a Dětské krizové centrum pomáhá dětem a mladým lidem s řešením náročných životních situací, se kterými se mohou setkat

v rámci online prostředí jako je kyberšikana, sexting, šikana a mnohé další. Uvedené služby jsou bezplatné všem dětem a dospělým z České republiky a využívat jej mohou na svých telefonech, chatu a e-mailu. Činnost SIC CZ má mezinárodní dosah, je totiž součástí sítí Insafe a INHOPE, které sdružují centra bezpečnějšího internetu a horké linky v Evropě i ve světě. Za Českou republiku prezentují vývoj a trendy v oblasti online bezpečnosti v zahraničí. Aktivity a služby Safer Internet Center Česká republika jsou spolufinancovány Evropskou komisí, a to programu Digitální Evropa. (Safer Internet Centrum ČR, online)

Kraje pro bezpečný internet

Nové technologie představují fenomén, se kterým je nutno umět pracovat po manuální i hlavně po mentální stránce. Je zapotřebí být odolný vůči hoaxům, umět zodpovědně nakládat se svými i cizími osobními údaji, a také vědět jaké kroky podniknout, když se staneme obětí kyberšikany, sextingu a dalších projevů kyberkriminality. Zodpovědné chování v kyberprostoru je klíčové, a tak je nezbytně nutné učit jej naše děti. Na základě těchto skutečností vznikl projekt Kraje pro bezpečný internet. Projekt Kraje pro bezpečný internet existuje díky iniciativě Asociace krajů ČR, která usiluje zlepšit informovanost o možných rizicích na internetu a také o možnostech prevence. Aktivitami projektu je pořádání e-learningových lekcí, videospotů a vědomostního soutěžního kvízu. Realizaci projektu zastřešuje několik organizací, těmi jsou společnost PC HELP,a.s., Program prevence kriminality Ministerstva vnitra ČR, Microsoft a Gordic. Na organizaci a financích projektu se podílí 13 krajů ČR. (Kraje pro bezpečný internet, online)

Uvedli jsme 4 preventivní programy zabývající se kyberkriminalitou u nás. Projekt E- Bezpečí je realizovaný Centrem prevence rizikové virtuální komunikace Univerzity Palackého v Olomouci a zaměřuje se na prevenci a vzdělávání v oblasti kybernetických hrozeb a rizikového chování online. Poskytuje terénní práci prostřednictvím přednášek a diskuzí s cílem najít a snížit rizika online komunikace. Druhým uvedeným projektem je Tvoje cesta onlinem, který je veden Policií ČR a ČSOB. Primárním cílem tohoto programu je seznámit mladé lidi s možnými riziky, která se objevují v online prostředí a prevence. Projekt je určen žákům druhého stupně základních škol, rodičům a všem dospělým jedincům. Posledním zmíněným programem je Safer Internet Centrum ČR. Ten vznikl za aktivity organizací, které se snaží dělat internet pro děti a mládež bezpečnějším a méně rizikovým. Koordinátorem SIC CZ je sdružení CZ.NIC od roku 2019 a dalšími

partnery jsou Linka bezpečí, Dětské krizové centrum a vzdělávací program společnosti Člověk v tísni. Společná práce zmíněných organizací se odvíjí od tří pilířů, kterými jsou: centrum prevence, linka důvěry a horká linka pro nahlašování nelegálního digitálního obsahu. Projekt Kraje pro bezpečný internet se zaměřuje na zvýšení informovanosti o rizicích v online prostředí a možnostech prevence. Organizuje e-learningové akce, videospoty a vědomostní soutěžní kvíz. Následující kapitola se věnuje praktické části diplomové práce.

4 Kyberkriminalita z pohledu žáků druhého stupně základních škol

Čtvrtá kapitola Kyberkriminalita z pohledu žáků druhého stupně základních škol se zaměřuje na praktickou část diplomové práce. Kapitola zkoumá zkušenosti žáků druhého stupně základních škol s kyberkriminalitou, jejich povědomí o kyberkriminalitě a to, od koho chtějí získávat informace o kyberkriminalitě. Dále budou uvedeny rešerše výzkumů, které se vztahují k tomuto tématu. Praktická část se z velké části opírá o výzkumnou zprávu Vnímání kyberkriminality mezi dětmi, která vznikla v rámci Projektu Kraje pro bezpečný internet (viz 3.3 Preventivní programy). Tento a další výzkumy si představíme v následující podkapitole.

4.1 Rešerše výzkumů zabývajících se kyberkriminalitou

Vnímání kyberkriminality mezi dětmi

Jak již bylo uvedeno výše, výzkum Vnímání kyberkriminality mezi dětmi vznikl v rámci projektu Kraje pro Bezpečný internet. Kyberkriminalita patří k druhům kriminality, u kterých je zaznamenáván značný nárůst počtu trestných činů. Výzkum se věnoval analýze kyberkriminality, způsobu vnímání a chápaní kyberkriminality u dětí a také jednotlivým typům jednání na internetu a sociálních sítí, která shledávají povolenými anebo naopak trestnými. Součástí výzkumu byla také prevence kybekriminality a její vnímání u dětí. Cílovou skupinu tvořili žáci druhého stupně základních škol. Jednalo se tedy o žáky 6. až 9. tříd ve věku od 11 do 16 let. Výzkumu se zúčastnili základní školy i některá víceletá gymnázia z jedenácti krajů. Celkem se výzkumu zúčastnilo 50 917 respondentů. Metodiku výzkumu tvořilo kvantitativní dotazníkové šetření formou anonymních online dotazníků, které byly následně rozesílány do základních škol. Distribuci měli na starost krajští koordinátoři projektu Kraje pro bezpečný internet, školští koordinátoři prevence a školní metodici prevence. Dotazník byl vyhotoven v programu Google Forms. Hlavním cílem výzkumu byla analýza znalostí a zkušeností žáků s kyberkriminalitou a s rizikovými jevy vyskytující se na internetu. Část otázek v dotazníku se soustředila na využívání sociálních sítí a absolvované preventivní programy.

Co se týče výsledků, tak za nejužívanější sociální sít byl označen Messenger, celkově 79,8 % žáků. Z hlediska informací o bezpečném chování na internetu, jsou žáci nejčastěji informováno od učitelů, což je celkově 76,4 % respondentů a druhé místo patří

policistům (17,5 %). Ve druhé části dotazníku, která se zaměřovala na znalost kyberkriminality, označovali žáci nejčastěji phishing jako trestný (83 %), vyhrožování přes internet tvořilo 82 % a odpovědi vztahující se k neoprávněnému přístupu k počítačovému systému byly mezi 65 % a 83 %. Nejmenší znalost závadového jednání byla u odpovědí, která se vztahovala k porušování autorských práv, což bylo 39 % u nahrávání obsahu na internet po 46% u stahování placených her z úložišť. Třetí část dotazníku se orientovala na to, co je kyberkriminalita a co je podle žáků na internetu zakázané. Výsledky této části ukázaly, že žáci mají velmi nízké povědomí o legálnosti a nelegálnosti daného jednání. To ukazuje například tento výrok „posíláme si s kamarádkou (14 let) a ona mi pošle fotografii, kde je svlečená“ pojmenovalo jako trestné pouhých 60 % žáků. Poslední část otázek se vztahovala ke zkušenostem žáků s kyberkriminalitou. Dle předpokladů si žáci nejčastěji stahují hudbu (82,1 %) a videa (54,2 %). Nejvíce se vyskytujícími druhy kyberkriminality, kterých se žáci dopouštěli, byly různé formy neoprávněných přístupů k počítačovému systému. Dále to bylo porušování autorských práv, kdy téměř 10 % žáků potvrdilo porušení zákona.

Užívání digitálních technologií je u dětí v dnešní době značným trendem, a proto by škola i rodiče měli usilovat o preventivní vzdělávání v oblasti bezpečného užívání těchto technologií, protože mohou být jak ku prospěchu, ale také mohou napáchat značnou škodu. Fakt, že 15 % žáků se dopustilo potenciálně trestného jednání, je znepokojující. Celkově žáci ví velmi málo o tom, co kyberkriminalita je a také, co mohou a nesmí dělat. Žáci nejsou jen oběťmi, ale také pachateli kyberkriminality, a proto je zapotřebí upravit preventivní působení. Také je nutné více zapojit do preventivního působení pedagogy a Policii ČR, protože právě od nich chtějí žáci získávat informace o bezpečném chování na internetu. (Daňhelka, 2018, online)

EU Kids Online 2020

EU Kids Online je nadnárodní výzkumná síť, jejímž cílem je šířit znalosti o příležitostech, rizicích a bezpečnosti evropských dětí na internetu. Tato síť působí ve více než 30 zemích a spojuje výzkumné zkušenosti z různých zemí, oborů a metod.

EU Kids Online 2020 je zpráva, která prezentuje výsledky rozsáhlého průzkumu ohledně přístupu dětí k internetu, jejich online praktik, dovedností a také online rizik a příležitostí, se kterými se děti dostávají do kontaktu. Průzkumu se zúčastnilo 25 101 dětí ve věku 9-16 let v 19 evropských zemích v období od podzimu 2017 do léta

2019. Cílem zprávy je poskytnout ucelený pohled na internetové prostředí z hlediska dětí a identifikovat jak negativní, tak pozitivní aspekty jejich online zkušeností. Analyzované oblasti zahrnují přístup k internetu, online praktiky, dovednosti, jak se chránit před riziky, a také různé situace, se kterými se děti online setkávají. Celkově se jedná o podrobný průzkum, který přináší hodnotné poznatky ohledně dětského užívání internetu v Evropě.

Pro tento výzkum byla zvolena kvantitativní metoda formou dotazníku. Dotazník je založen na výzkumech jako EU Kids Online 2010 a Kids Online 10 a byl upraven pro potřeby této studie. Dotazník obsahuje základní otázky, které jsou hlavními otázkami dotazníku, a nepovinné otázky, které se zabývají vybranými tématy do větší hloubky nebo obsahují doplňující otázky. Jednotlivé země si mohly vybrat jednu nepovinnou otázku podle svých preferencí, ale základní otázky byly všechny povinné. Výsledky této zprávy jsou založeny pouze na základních otázkách. Dotazník se ve většině zemí distribuoval ve dvou částech kvůli jeho délce a složitosti. Dotazník je k dispozici v plné verzi pro starší děti a ve zkrácené verzi pro mladší děti. Každá země měla možnost rozhodnout, které otázky nebudou pokládány mladším dětem.

Výsledky v České republice ukázaly, že především starší děti tráví více času na internetu a čelí tak větším rizikům, které se v online prostředí vyskytují, což však neznamená, že se s danými riziky nutně musí setkat. Například jen 41 % dětí se cítí znepokojeně a rozrušeně při kontaktu se sexuálně explicitním obsahem v kyberprostoru. Nadpoloviční většina respondentů pociťuje štěstí a má převážně kladné zkušenosti s online schůzkami, kdy dané lidi znali pouze z internetu. Celkem 67 % setkání se odehrává s vrstevníky a jen 7 % s dospělými. Rozdíly mezi pohlavími jsou patrné v několika oblastech. Dívky jsou častěji žádány o sdílení intimních informací a také se více dostávají do styku s online obsahem podporující extrémní štíhlost. Zatímco chlapci se častěji setkávají s kybernetickou agresí a počítačovými viry z různých her a aplikací. Celkově mají dívky větší negativní online zkušenosti než chlapci, a to o 8 procentních bodů. Rozdíly mezi 6-15 procentními body, jsou touto studií označovány jako malé.

V České republice jsou děti vystavovány nebezpečnému online obsahu kvůli emočním problémům a vyhledáváním senzací. Pozitivní rodinné prostředí tvořilo ochranný faktor vůči online rizikům. Autoři se shodují, že by se rodiče měli více zaměřit na budování dobrých vztahů se svými dětmi, aby předcházeli jakékoli formě

kyberkriminality. (Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U.,2020 ,online)

Nebezpečné výzvy pohledem českých dětí (výzkumná zpráva)

Výzkum byl zpracován v kooperaci s Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci v roce 2020. Výzkum se zaměřuje na výzvy, se kterými se děti v online prostředí setkávají, jakým způsobem na ně reagují, na jakém místě s nimi přicházejí do kontaktu apod. Informace byly zjišťovány pomoci online dotazníku, který byl distribuován do všech základních a středních škol v České republice. Celkový počet respondentů byl 4952, kteří byli ve věku od 12-19 let. Autoři zjistili, že jako riziko internetového prostředí respondenti vnímají primárně zneužití osobních údajů, kyberšikanu či internetové abuzéry (,,úchyly, pedofily apod.''). Většina respondentů nemá zkušenost s nebezpečným chováním na internetu, tedy například kyberšikanou, podvodnými e-maily, phishingem, rizikovými výzvami, sextingem, vyhrožováním či vydíráním. Respondenti, kteří se již setkali s nebezpečným chováním na internetu, mají největší zkušenost s kyberšikanou, sextingem nebo hacknutím účtu. V případě, pokud by se respondenti ocitli v nebezpečí, tak o tom poví hlavně rodičům, kamarádům nebo rodině. Nadpoloviční většina respondentů byla srozuměna, že na internetu mohou narazit na škodlivý obsah, nejvíce informací dostávali ve škole nebo doma. (Střílková, Kopecký, 2020, online)

4.2 Výzkumný cíl a stanovení hypotéz

Výzkumný cíl: Zjistit zkušenosti, jaké mají žáci druhého stupně základních škol s kyberkriminalitou a jaké je jejich povědomí o této problematice.

Výzkumný problém: Téma této práce je kyberkriminalita u dětí.

H1: Dívky mají větší zkušenosti s kyberkriminalitou než chlapci.

Dle výzkumu EU Kids Online 2020 uvedeného v předchozí kapitole, mají dívky větší negativní online zkušenosti než chlapci. Nutno zmínit, že rozdíly mezi pohlavími jsou malého rozměru. (Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. 2020, online)

H2: Nadpoloviční většina zkoumaných žáků se z pohledu kyberkriminality nechová bezpečně.

Výzkum Vnímání kyberkriminality mezi dětmi poukázal na skutečnost, že žáci disponují nedostatečnými znalostmi o rizikovém chování na internetu a kyberkriminality celkově. To podporuje například zjištění v oblasti porušování autorských práv. Zde totiž jen necelých 40 % žáků označilo porušování autorských práv jako kyberkriminalitu. Dalším příkladem byly otázky zabývající se zasíláním nahých fotografií osob mladších 15 let, které označilo jako trestné jen 66,7 % žáků. Proto je důležité se zaměřovat prevenci a zvýšit znalost žáků o nebezpečných jevech v kyberprostoru (Daňhelka, 2018, online). Hypotéza je testovaná na základě témat, která byla řešena ve výše uvedeném výzkumu. Hypotéza bude dokázána, pokud výzkumné šetření odhalí, že nadpoloviční počet respondentů se dopouští takového jednání, které je považováno za trestné.

H3: Nejčastěji chtějí žáci dostávat informace o kyberkriminalitě od učitelů.

Dle výzkumu Vnímání kyberkriminality mezi dětmi, chtějí být žáci informováni od učitelů v průběhu výuky, uvedlo to 40 % respondentů. Výsledek může pomoci při zvolení vhodného preventivního programu pro žáky. (Daňhelka, 2018, online)

H4: Nadpoloviční většina se nesetkala s nebezpečným chováním na internetu.

Výzkumná zpráva Nebezpečné výzvy pohledem českých dětí uvádí, že se většina respondentů nesetkala s nebezpečným chováním na internetu. Tím je myšlena kyberšikana, podvodné e-maily, phishing, rizikové výzvy, sexting, vyhrožování a vydírání. (Střílková, Kopecký, 2020, online)

4.3 Popis metodologie

Výzkumné šetření bylo z velké části inspirováno dotazníkem z výzkumné zprávy Vnímání kyberkriminality mezi dětmi z roku 2018, protože přesně odpovídá zkoumané problematice. Pro výzkumné šetření jsme využili kvantitativní metodu formou anonymního online dotazníku vytvořeného pomocí Microsoft Forms. Dotazník byl distribuován přes e-mailové adresy daných základních škol. Sběr dat probíhal od listopadu roku 2023 do března 2024. Dohromady bylo osloveno přes 22 základních škol. Součinnost pro sběr dat však poskytlo jen 5 z nich. Celkem se zúčastnilo výzkumného šetření 191 respondentů. Dotazníky byly vyplňovány při hodinách informatiky, což bylo doporučením autorů výzkumu Vnímání kyberkriminality mezi dětmi. Doba vyplňování online dotazníku se pohybovala dle MS Forms okolo 15-18 minut. Dotazník se skládal z celkem 106 položek.

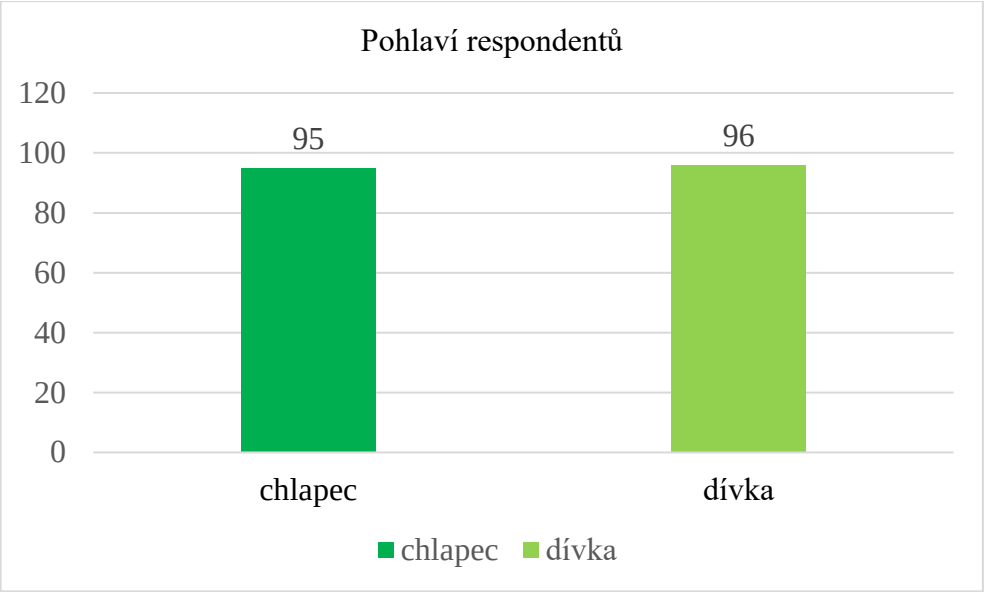
Dotazník měl několik částí. První část zjišťovala pohlaví a doprovodné položky sloužící ke zjištění zkušeností dětí s kyberkriminalitou. V otázce č. 4 mohli respondenti označit více možností. Všechny ostatní položky byly inspirovány výzkumem Vnímání kyberkriminality mezi dětmi z roku 2018. Následovala otázka ,,Co je podle tebe kybekriminalita'', kde respondenti vybírali z 53 výroků, zda se jedná o kyberkriminalitu či nikoliv. Další část tvořilo celkem 26 dichotomických otázek zkoumajících zkušenosti dětí s kyberkriminalitou. Poté respondenti odpovídali na 20 otázek s hodnotící škálou, kde označovali odpovědi podle závažnosti jednání. Poslední 2 otázky se zabývaly informovaností žáků o kybekriminalitě a také zjišťováním, od koho by takové informace rádi získávali. Zde měli respondenti možnost výběru více odpovědí.

4.4 Charakteristika respondentů

Respondenty byly žáci druhého stupně základních škol, tedy ve věku od 11 do 16 let. Sběr dat probíhal na základních školách ve Východních Čechách za spolupráce ředitelů/ředitelek a jednotlivých učitelů. V průběhu sběru dat jsem dostával pozitivní zpětnou vazbu od škol, že během vyplňování vznikaly zajímavé diskuze týkající se kyberkriminality. Pozitivní zjištění je také fakt, že výsledky tohoto šetření školám nejsou lhostejné, protože požadují výsledky a následné doporučení na základě zjištěných skutečností.

4.5 Zpracování výzkumného šetření

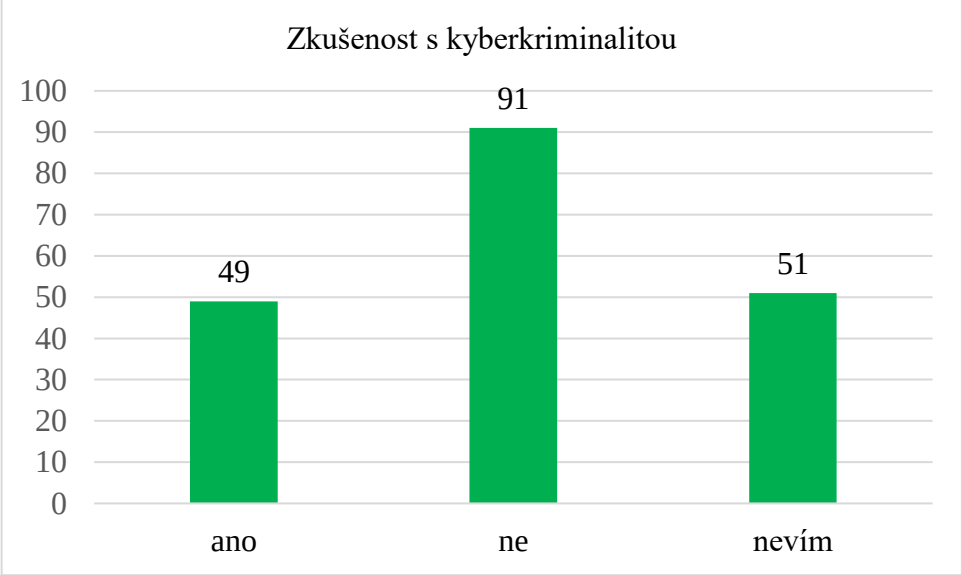
Položka č. 1: **Jsem chlapec/dívka.**



Graf č. 1 – **Pohlaví respondentů**

První položka zjišťovala pohlaví respondentů. Z uvedeného grafu lze vypozorovat, že rozložení žáků z hlediska pohlaví bylo rovnoměrné – 95 chlapců a 96 dívek.

Položka č. 2: **Máš nějakou zkušenost s kyberkriminalitou?**



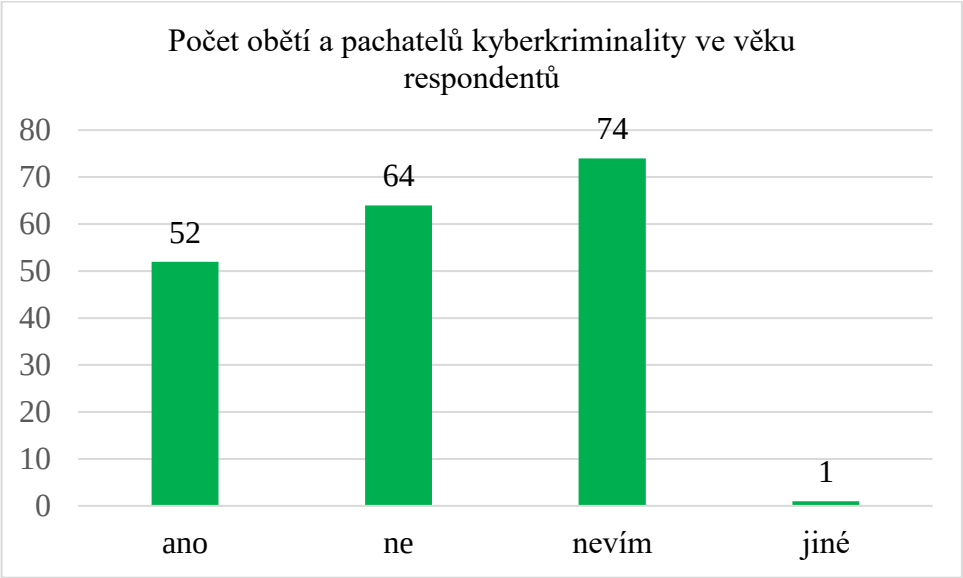
Graf č. 2 – **Zkušenost s kyberkriminalitou**

Druhá položka se zaměřovala na zkušenost respondentů s kyberkriminalitou. Nejčastěji respondenti uváděli, že s kybekriminalitou nemají žádnou zkušenost, celkem

jich bylo 91, což činí 48 %. S kybekriminalitou se setkalo 49 (26 %) žáků a 51 (27 %) z nich odpovědělo, že neví.

Položka č. 3: **Znáš někoho v tvém věku, kdo se stal obětí nebo iniciátorem (pachatelem) kyberkriminality?**

Třetí položka zkoumala, zda respondenti znají vrstevníka, který se setkal s kyberkriminalitou buď jako oběť či byl pachatelem.

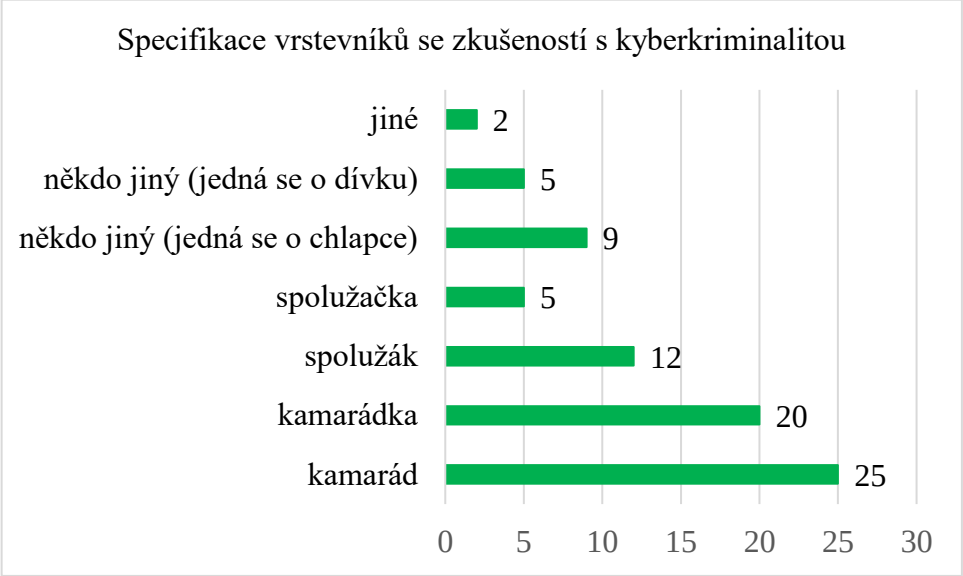


Graf č. 3 - **Počet obětí a pachatelů kyberkriminality ve věku respondentů**

Nejčastěji žáci odpovídali, že neví, zda někoho takového znají v počtu 74, což činí (39 %). Celkem 64 (34 %) respondentů nezná vrstevníka, který by přišel do kontaktu s kyberkriminalitou. Naopak 53 (27 %) žáků uvedlo, že ví o někom, kdo se s kyberkriminalitou setkal.

Položka č. 4: **Pokud si v přechozí otázce zvolil/a odpověď ,,Ano'', uveď prosím, o koho se jednalo.**

Položka č. 4 rozvíjela předchozí položku a zjišťovala detailněji, o jaké vrstevníky se zkušeností s kyberkriminalitou se jednalo. Respondenti zde mohli zvolit více možností.

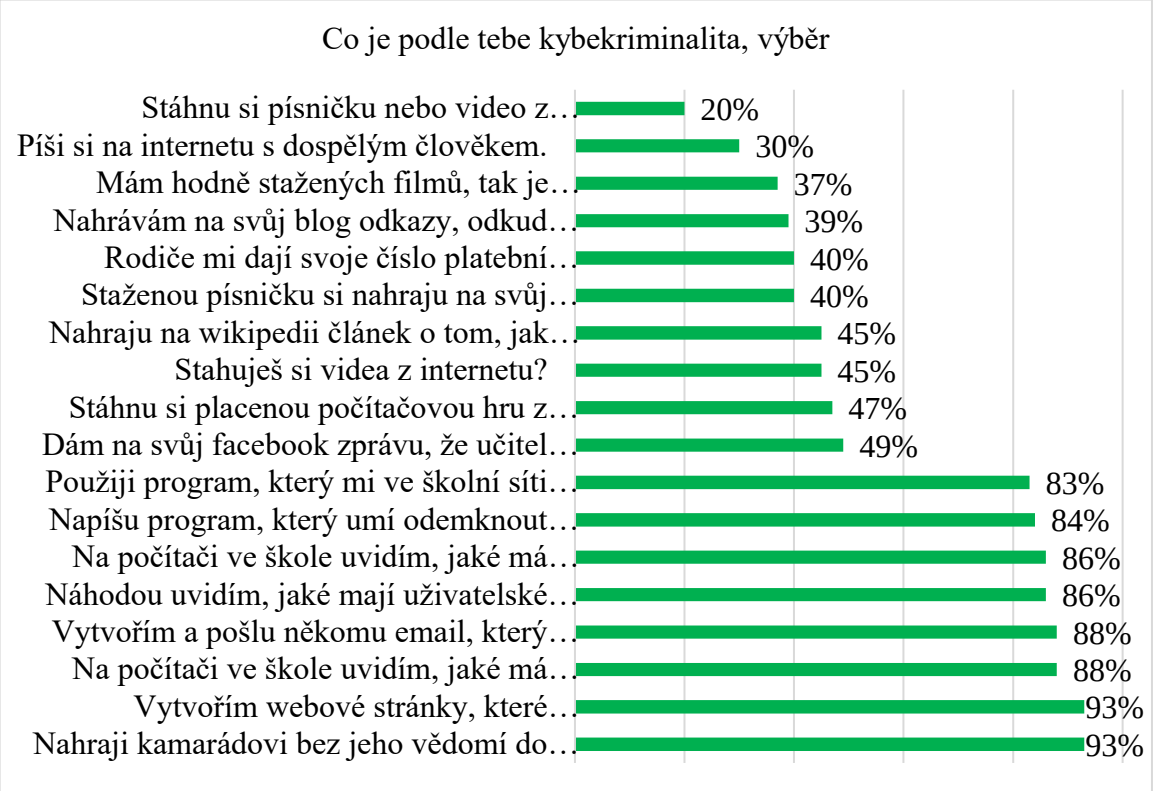


Graf č. 4 – **Specifikace vrstevníků se zkušeností s kyberkriminalitou**

Nejvíce šlo o kamarády (25) a kamarádky (20) respondentů. O něco méně bylo spolužáků (12) a chlapců (9), u nichž nebyl specifikován, v jakém vztahu jsou s respondenty. Nejméně se jednalo o spolužačky (5),dívky (5) v neznámém vztahu s žáky a 2 respondenti zvolili odpověď jiné. Celkem z této položky bylo zjištěno, že zkušenosti s kyberkriminalitou má 43 chlapců a 30 dívek.

Položky č. 5-57: **Co je podle tebe kyberkriminalita.**

U těchto položek jsme zjišťovali pomocí různých výroků povědomí žáků o tom, co je kyberkriminalita. Vždy měli na výběr pouze možnosti ,,ano'' a ,,ne''. V níže znázorněném grafu uvádíme výběr odpovědí respondentů na položky č. 5 až č. 57. Kompletní výsledky odpovědí uvádíme v příloze B.



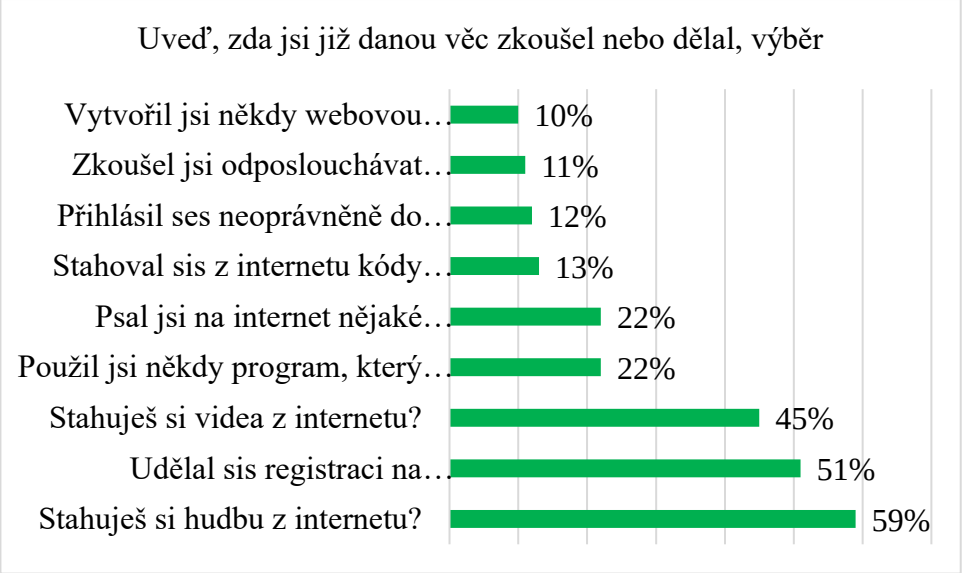
Graf č. 4 – **Co je podle tebe kyberkriminalita, výběr**

Respondenti označovali dále nejčastěji příklady **phishingu** ,,vytvořím webové stránky, které vypadají jako přihlašovací stránka internetového bankovnictví, ale při přihlášení mi stránka pošle jméno a heslo uživatele (93 %)'' či ,,vytvořím a pošlu někomu email, který vypadá jako zpráva z banky, aby poslal zpět svoje jméno a heslo'' (88 %) a také **hackingu**, kdy se hlavně jednalo o příklady neoprávněného přístupu k počítačovému systému. ,,na počítači ve škole uvidím, jaké má učitel či učitelka heslo do elektronické žákovské a zkusím se přihlásit za ně a přepíšu nějaké známky'' (88 %), ,,na počítači ve škole uvidím, jaké má učitel či učitelka heslo do elektronické žákovské a zkusím se přihlásit za ně a prohlédnu si prostředí žákovské'' (86 %) nebo ,,napíšu program, který umí odemknout nelegálně stažené windows'' (84 %) a podobný příklad ,,použiji program, který mi ve školní síti zjistí heslo, které zadávají ostatní spolužáci do sítě'' (83 %).

Nejméně respondenti volili příklady týkající se **porušování autorských práv** (nahrávání a stahování hudby,videa a her na internetu). Výroky ,,mám hodně stažených filmů, tak je nahraju na server, aby si je ostatní taky mohli stáhnout a nemuseli si je hledat sami'', označilo za kyberkriminalitu jen 37 % a následující výrok ,,nahrávám na svůj blog odkazy, odkud si mohou lidi stahovat filmy'' považuje za trestný pouhých 39 % žáků. Další oblastí, kterou žáci označovali nejméně, byla forma **kybernetické agrese** konkrétně vůči škole a učitelům, například v položce ,,nahraju na wikipedii článek o tom, jak je škola pitomá'', se jedná o kyberkriminalitu jen u 47 % dotazovaných. Další položka ,,dám na svůj facebook zprávu, že učitel či učitelka je pitomý/-á'', je trestná pro 49 % žáků.

Položky č. 58–83: **Uveď, zda jsi již danou věc zkoušel nebo dělal.**

Další část položek se zaměřovaly na zkušenosti respondentů s kyberkriminalitou. Vybírali z možností ,,Ano'' a ,,Ne'', zda danou věc udělali či ji zkoušeli. V následujícím grafu uvádíme výběr odpovědí ,,Ano'', tedy že mají zkušenost s uvedeným výrokem. V příloze C diplomové práce jsou uvedeny kompletní výsledky těchto položek.



Graf č. 5 - **Uveď, zda jsi již danou věc zkoušel nebo dělal, výběr**

Největší zkušenost mají žáci se stahováním hudby na internetu, odpovědělo tak 59 %, dále 51 % respondentů uvedlo, že při registraci na internetu uvedli jiné údaje než své skutečné. Videa z internetu si stahuje celkem 45 % dětí. Ve výzkumu Vnímání kyberkriminality mezi dětmi byly tyto zkušenosti taktéž nejčastější. Avšak znepokojujícím faktem jsou odpovědi, kterými se již žáci dopouštějí trestného jednání. Například na otázku ,,použil jsi někdy program, který ti umožnil se přihlásit do cizí wifi

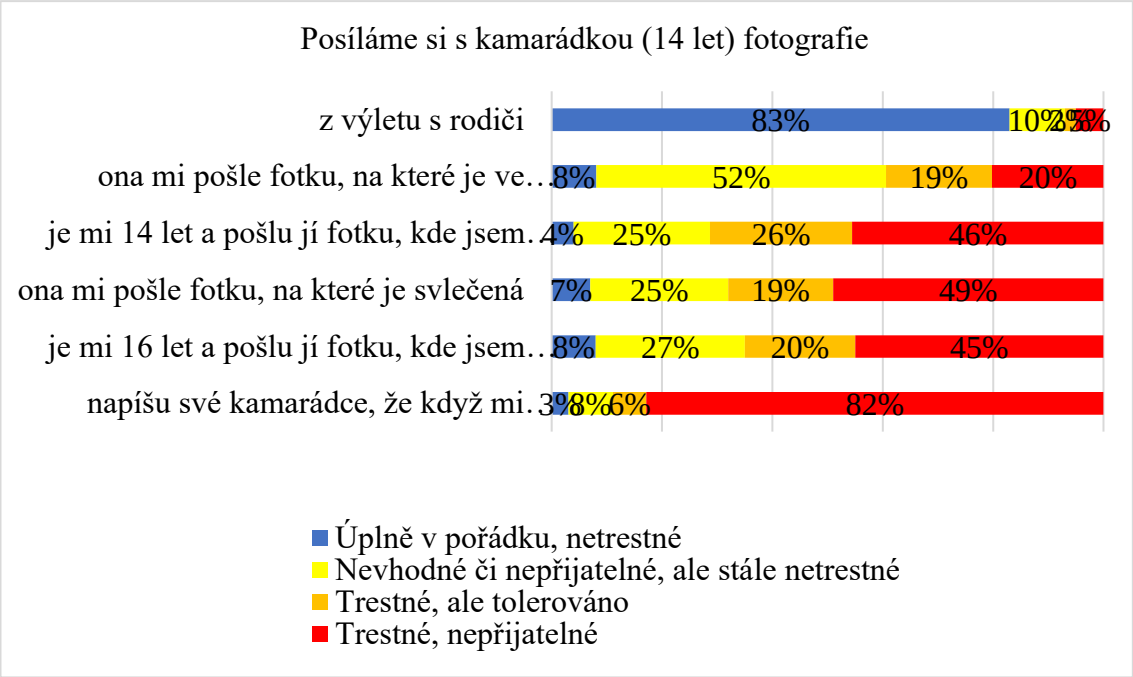
sítě'', odpovědělo kladně 22 % (42) respondentů, z toho 29 chlapců. Na otázku ,,psal jsi na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťani, apod.)'', odpovědělo taktéž 22 % dětí. Nicméně mnohem šokujícím je zjištění, že se žáci dopustili různých forem phishingu a hackingu, ať už se jednalo o stahování kódů platebních karet z internetu (13 %), neoprávněné přihlašování do internetového bankovnictví (12 %), odposlouchávání provozu v počítačové síti (11 %) a další. Zkušenost s dalšími příklady kyberkriminality má 10 % – 22 % respondentů.

Položky č. 84–104: **Uveď, zda je pro tebe jednání škodlivé či trestné.**

V těchto položkách nás zajímalo, jaké jednání přisuzují respondenti k jednotlivým situacím, tedy co považují za trestné a netrestné. Měli na výběr označit jednu z celkem čtyř předem určených odpovědí: ,,Úplně v pořádku, netrestné'', ,,Nevhodné či nepřijatelné, ale stále netrestné'', ,,Trestné, ale tolerováno'' a ,,Trestné, nepřijatelné''. Výsledky uvážíme níže ve znázorněných grafech. Dle Daňhelky a projektu Kraje pro bezpečný internet byla v této skupině položek zahrnuta témata, která se zabývala zasíláním fotografií, online komunikací s cizí osobou, neoprávněnými přístupy k blogu a také nahráváním videa na internet. Žáci vybírali z příkladů, které byly jak legální, tak i trestné. (Daňhelka, 2018, online)

Pro tuto část byly zvoleny boxy otázek týkajících se zasílání fotografií, internetové komunikace s cizí osobou, neoprávněných přístupů k blogu, a nahrávání videa na internet. V možnostech byly uvedeny příklady jak zcela legálních jednání, tak jednání trestných. V příloze D jsou znázorněny kompletní výsledky těchto položek.

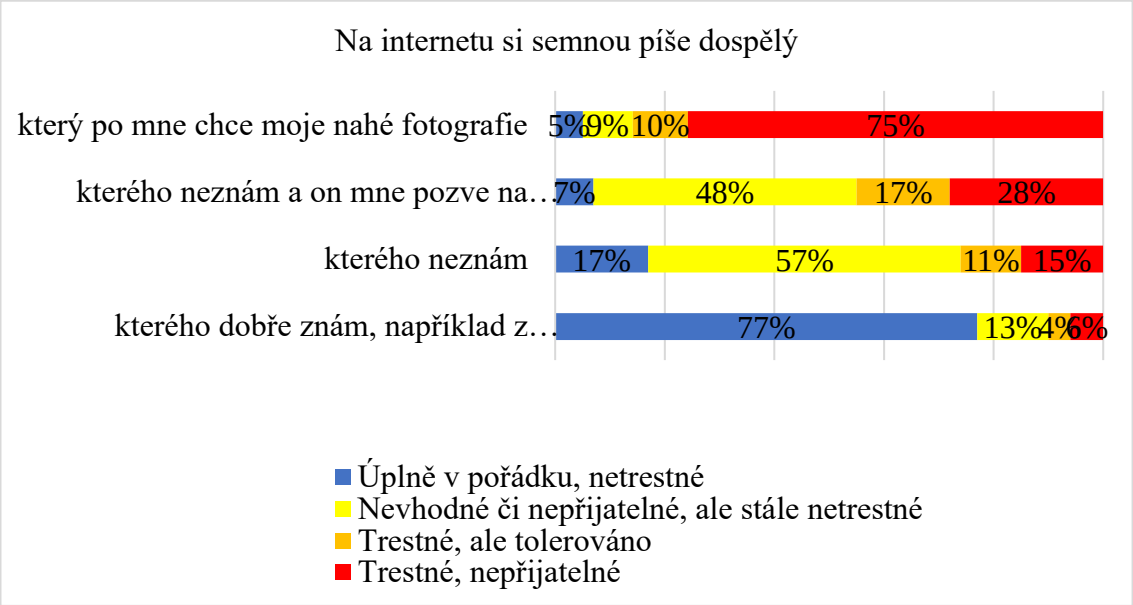
Položky č. 84–89: Uveď, zda je pro tebe jednání škodlivé či trestné: **Posíláme si s kamarádkou (14 let) fotografie:**



Graf č. 6 – **Posíláme si s kamarádkou (14 let) fotografie**

Na grafu č. 6 můžeme vypozorovat, že situaci ,,ona mi pošle fotku, na které je svlečená'', označilo celkem 68 % žáků za trestnou. Obdobně tomu bylo u položky ,,je mi 14 let a pošlu jí fotku, kde jsem nahý/nahá ve sprše'', kterou považuje za protiprávní 72 % respondentů. Příklad ,,ona mi pošle fotku, na které je ve spodním prádle'' ukazuje, že pro většinu žáků (60 %) se o kyberkriminalitu nejedná. 88 % respondentů označilo příklad ,,napíšu své kamarádce, že když mi nepošle další fotku, tak tu nahou, kterou mi již poslala, zveřejním na internetu'' za trestný.

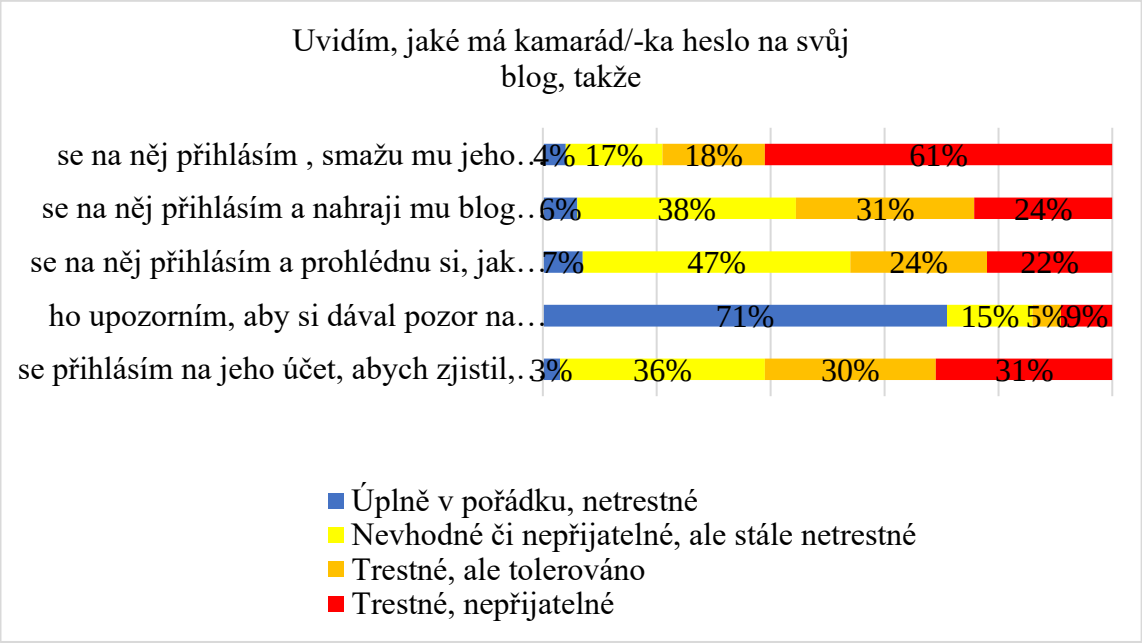
Položky č. 90–94: Uveď, zda je pro tebe jednání škodlivé či trestné: **Na internetu si semnou píše dospělý:**



Graf č. 7 – **Na internetu si semnou píše dospělý**

Tento graf znázorňuje výsledky odpovědí položek č. 90-94, kdy respondenti vybírali závažnost jednání, při kterém si píšou na internetu s dospělou osobou. Nejvíce trestné shledávají respondenti odpověď ,,který po mě chce moje nahé fotografie'', a to v 85 %. Avšak situaci ,,kterého neznám a on mě pozve na schůzku'', označilo za protiprávní jen 45 % žáků. Za legální jednání 90 % žáků považovalo výrok ,,kterého dobře znám, například z tábora apod.'' a ,,kterého neznám'', označilo 74 %.

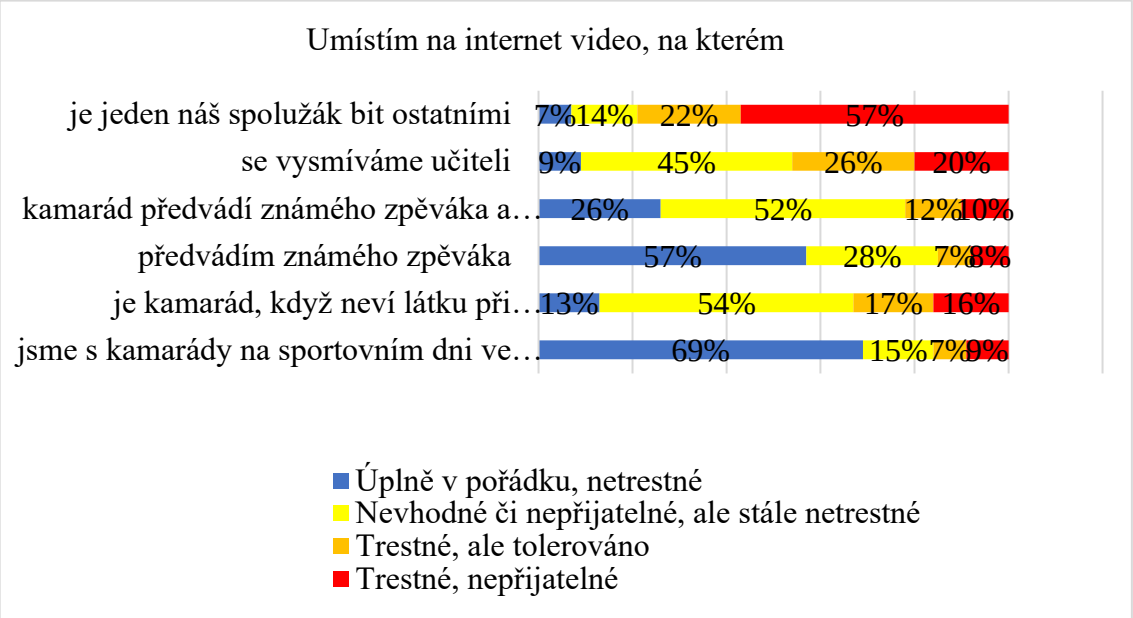
Položky č. 95–98: Uveď, zda je pro tebe jednání škodlivé či trestné: **Uvidím, jaké má kamarád/-ka heslo na svůj blog, takže:**



Graf č. 8 – **Uvidím, jaké má kamarád/-ka heslo na svůj blog, takže**

Z výše uvedeného grafu můžeme zjistit, že nejčastěji žáci označovali výrok ,,se na něj přihlásím, smažu mu jeho obsah a nahraji tam odkazy na porno stránky'', učinilo tak 79 %. Podobné odpovědi můžeme sledovat u příkladů ,,se na něj přihlásím a nahraji mu na blog několik vtipů'' a ,,se na něj přihlásím a prohlédnu si, jak má blog dělaný''. U prvního zmíněného příkladu předpokládá protiprávní jednání 55 % žáků a u druhého 46 %. Znepokojující zjištění lze vysledovat u situace ,,se přihlásím na jeho účet, abych zjistil, zda jsem heslo viděl dobře'', protože jen 61 % respondentů, se domnívá, že jde o kyberkriminalitu. Za nejvíce legální jednání považují respondenti výrok ,ho upozorním, aby si dával pozor na zabezpečení'', vybralo jich tak 86 %.

Položky č. 99–104: Uveď, za je pro tebe jednání škodlivé či trestné: **Umístím na internet video, na kterém:**

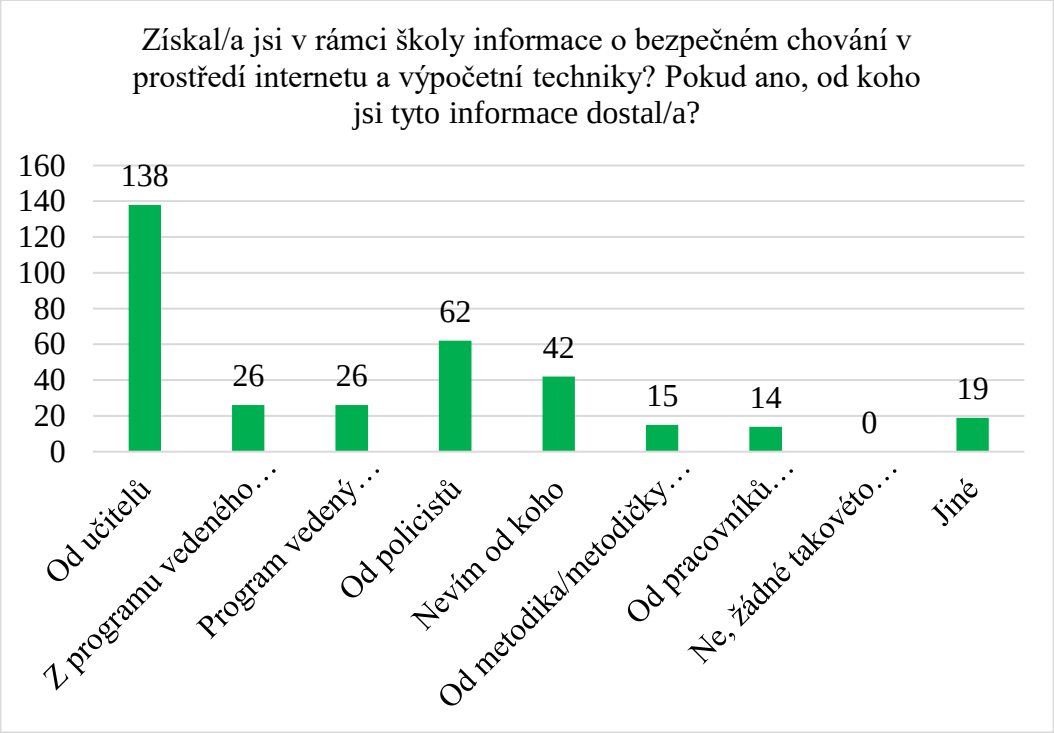


Graf č. 9 – **Umístím na internet video, na kterém**

Tento graf znázorňuje, jaké jednání, zda trestné či legální, přisuzovali daným výrokům, když umístí příslušné video na internet. Za nejvíce trestné jednání respondenti označili ,,je jeden náš spolužák bit ostatními'', celkem jich bylo 79 %. Poněkud vyrovnané odpovědi můžeme najít na situaci ,,se vysmíváme učiteli'', zde je totiž 54 % žáků přesvědčeno, že se nejedná o protiprávní jednání, opak tvrdí 46 %. U těchto výroků byla většina žáků (78 % - 85 %) názoru, že se jedná o netrestné jednání: ,,kamarád předvádí známého zpěváka a vůbec mu to nejde'', ,,předvádím známého zpěváka'' a ,,jsme s kamarády na sportovním dni ve škole''. Položku ,,je kamarád, když neví látku při zkoušení u tabule'' označilo za trestnou 33 % žáků.

Položka č. 105: **Získal/a jsi v rámci školy informace o bezpečném chování v prostředí internetu a výpočetní techniky? Pokud ano, od koho jsi tyto informace dostal/a?**

Touto položkou jsme zjišťovali, zda jsou žáci informování o bezpečnosti chování na internetu a výpočetní techniky a od koho tyto informace dostávají. Zde mohli respondenti vybrat více možností.

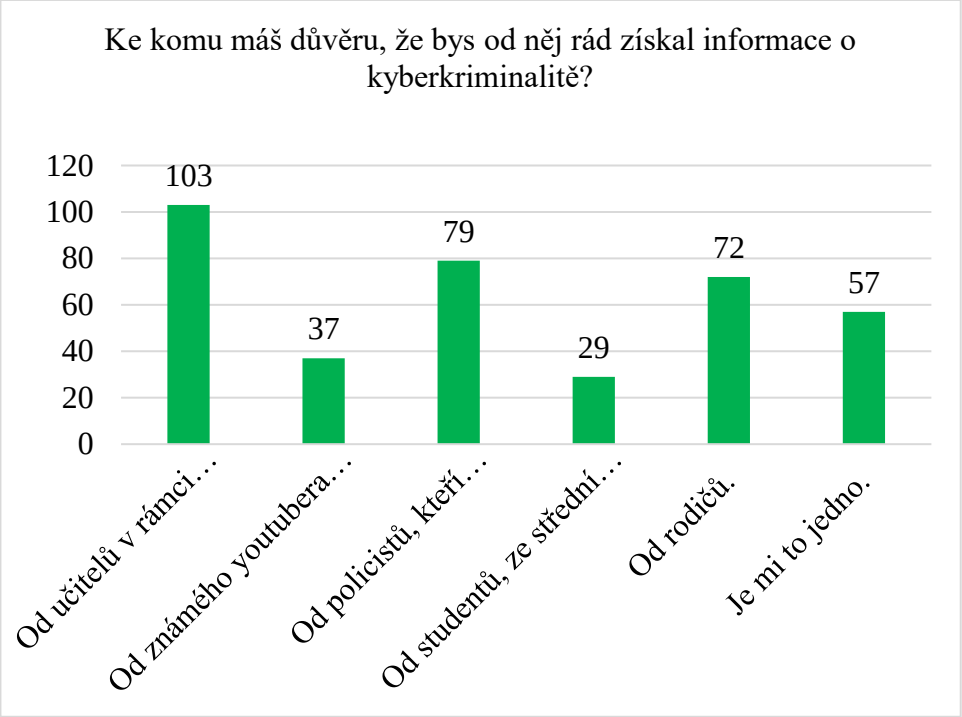


Graf č. 10 – **Získal/a jsi v rámci školy informace o bezpečném chování v prostředí internetu a výpočetní techniky? Pokud ano, od koho jsi tyto informace dostal/a**

Z uvedeného grafu můžeme vidět, že bezkonkurenčně nejvíce informací týkající se bezpečnosti v prostředí internetu dostávají žáci od učitelů (138), poté od policistů (62) a 42 žáků uvedlo, že neví, od koho tyto informace převzali. Pozitivním jevem je, že nikdo z respondentů neuvedl možnost ,,ne, žádné takovéto informace nemáme''. Možnost ,,jiné'' vybralo 19 respondentů, avšak už neuvedli, od koho takové informace dostali.

Položka č. 106: **Ke komu máš důvěru, že bys od něho rád získal informace o kyberkriminalitě?**

Zde jsme zkoumali, komu respondenti důvěřují tak, že by od něho dostávali rádi informace o kyberkriminalitě. Také u této položky mohli respondenti zvolit více možností.



Graf č. 11 – **Ke komu máš důvěru, že bys od něho rád získal informace o kyberkriminalitě**

Nejradši by žáci získávaly informace o kyberkriminalitě od učitelů během výuky (103). Dále od policistů, kteří kyberkriminalitu vyšetřují (79) a od rodičů (72). Možnost ,,je mi to jedno'' zvolilo 57 žáků. Ze všech uvedených subjektů by žáci nejméně rádi dostávali informace o kyberkriminalitě od studentů ze středních či vysokých škol (29) a od známého youtubera nebo zpěváka během preventivního programu (37). Seznam grafů je uveden v příloze A.

4.6 Verifikace a testování hypotéz

H1: Dívky mají větší zkušenosti s kyberkriminalitou než chlapci.

$H1_0$: Mezi pohlavím respondentů a jejich zkušenostmi s kyberkriminalitou není významná statistická souvislost.

$H1_A$: Mezi pohlavím respondentů a jejich zkušenostmi s kyberkriminalitou je významná statistická souvislost.

Tato hypotéza byla statisticky ověřována a jejím účelem bylo zjistit, zda existuje významná statistická souvislost mezi pohlavím respondentů a jejich zkušenostmi s kyberkriminalitou. Potřebná data jsme získali z položek č. 1,2,3 a 4. Navíc jsme připočítali k položce č. 2: **,,Máš nějakou zkušenost s kyberkriminalitou?''**, ještě data z položky č. 3: **,,Znáš někoho v tvém věku, kdo se stal obětí nebo iniciátorem (pachatelem) kyberkriminality?''**, kterou detailněji rozvíjela položka č. 4, kde jsme zjistili pohlaví daných vrstevníků se zkušeností s kyberkriminalitou, jednalo se o 43 chlapců a 30 dívek. Dle níže uvedené tabulky můžeme vidět, že zkušenost s kyberkriminalitou má **73 chlapců** a **49 dívek**, což je celkem 122 žáků. Dále 51 respondentů nemá tušení o zkušenosti s kyberkriminalitou a u dvou respondentů neznáme pohlaví, protože u nich byla zvolena možnost ,,Jiné''. Bez zkušenosti s kyberkriminalitou je 91 žáků. Pro testování byla zvolena metoda Chí – kvadrát testu nezávislosti pro čtyřpolní kontingenční tabulku. Na hladině významnosti 0,05 (95 %) se předpokládá, že nastane $H1_0$.

Tabulka č. 1 - Četnost zkušenosti respondentů s kyberkriminalitou vůči pohlaví

Pohlaví respondentů	**Zkušenost respondentů s kyberkriminalitou**		∑
	Ano	Ne	
Dívka	49	44	93
Chlapec	73	47	120
∑	122	91	213

Pozn: 51 respondentů uvedlo, že neví, zda mají zkušenost s kyberkriminalitou. Celkem 2 dotazovaní neuvedli pohlaví.

Výsledky testu: Hodnota testového kritéria vyšla $\mathbf{x^2 = 1{,}422}$ a kritická hodnota testového kritéria Chí – kvadrát (x^2), což je pro 1. stupeň volnosti a hladinu významnosti 0,05 odpovídá $\mathbf{x^2 = 3{,}841}$. Po porovnání testového kritéria $x^2 = 1{,}422$ s kritickou hodnotou testového kritéria $x^2 = 3{,}841$ nám vyšlo, že námi vypočítaná hodnota testového kritéria je **menší** než daná kritická hodnota testového kritéria x^2, a proto **přijímáme $\mathbf{H1_0}$** a $H1_A$ zamítáme na hladině významnosti 0,05.

Hypotézu zamítáme i na základě tabulky č. 2 uvedené v příloze E, která nám ukazuje, že rozdíly ve zkušenostech s kyberkriminalitou z hlediska pohlaví jsou

minimální, až na pár příkladů, kdy mají chlapci větší zkušenost s kyberkriminalitou než dívky.

H2: Nadpoloviční většina zkoumaných žáků se z pohledu kyberkriminality nechová bezpečně.

Z grafu č. 4 uvedeného výše můžeme vidět, že oblast porušování autorských práv jako je nahrávání a stahovaní hudby, her, filmů a agrese na internetu, většina žáků neoznačila za kyberkriminalitu. Když se podíváme na graf č. 7, zjistíme, že možnost ,,na internetu si semnou píše dospělý, kterého neznám a on mě pozve na schůzku'', označilo za trestné jednání pouze 45 % žáků a z toho pouze 28 % vybralo ,,trestné, nepřijatelné'', tudíž většina žáků nepovažuje tento příklad za trestný. Graf č. 8 nám ukazuje, že příklad ,,uvidím, jaké má kamarád/-ka heslo na svůj blog, takže se na něj přihlásím a prohlédnu si, jak má blog dělaný'', označilo za nelegální jednání 54 % žáků. Z grafu č. 9 se dozvíme, že příklad ,,umístím na internet video, na kterém se vysmíváme učiteli'', je pro většinu žáků (54 %) netrestný. Na základě těchto výsledků proto **přijímáme** H2.

H3: Nejčastěji chtějí žáci dostávat informace o kyberkriminalitě od učitelů při výuce.

Žáci chtějí být informováni o kyberkriminalitě nejčastěji od učitelů ve výuce, což nám ukazuje graf č. 11, a proto **přijímáme H3**

H4: Nadpoloviční většina se nesetkala s nebezpečným chováním na internetu.

Z grafu č. 2 jsme se dozvěděli, že se s kyberkriminalitou nesetkalo 91 (48 %) respondentů a zkušenost s ní má 49 (26 %) žáků, dalších 51 (27 %) jich uvedlo, že o zkušenosti s kyberkriminalitou neví. Vyřadíme-li respondenty, kteří o zkušenosti s kyberkriminalitou neví, nadpoloviční většinu pak tvoří žáci, kteří s kyberkriminalitou zkušenost nemají. Graf č. 5 znázorňuje, ačkoliv se jedná pouze o výběr příkladů, že většina respondentů se s uvedenými příklady dosud nesetkala. Kompletní výsledky uvedené v příloze C této práce, však také podporují toto tvrzení, proto **H4 přijímáme.**

4.7 Výsledky výzkumného šetření

Výzkumné šetření zkoumalo zkušenosti žáků s kyberkriminalitou, jejich povědomí o této problematice a také zjišťovalo, od koho chtějí žáci dostávat informace o kyberkriminalitě. Výsledky z položky č. 2 ukázaly, že zkušenost s kyberkriminalitou má 26 % respondentů. Na zkušenosti žáků s kyberkriminalitou se zaměřovaly také položky č. 58-83. Největší zkušenost mají žáci se stahováním hudby (59 %) a videa (45 %) na internetu a uváděním jiných údajů než skutečných při registraci na internetu (51 %). Z projevů kyberkriminality se však nejčastěji respondenti (22 %) dostali do styku s nepovoleným přístupem do počítačového systému (použití programu pro přihlášení do cizí wifi sítě) a také s psaním nenávistných příspěvků proti nějaké skupině osob. Alarmujícím zjištěním je, že výsledky dalších příkladů ukázaly, že žáci mají zkušenost se všemi uvedenými příklady, a to v rozmezí 10 % - 22 %. Jednalo se o projevy kyberkriminality, které jsou popsané v druhé kapitole teoretické části této práce, tedy o kyberkriminalitu na sociálních sítích, podvodné jednání, internetové pirátství a hacking. Například ke stahování kódů platebních karet z internetu se přiznalo 13 %, k neoprávněnému přihlašování do internetového bankovnictví (12 %), odposlouchávání provozu v počítačové síti (11 %) a další.

Položky č. 5-57 měly za cíl zjistit, jaké mají respondenti povědomí o tom, co kyberkriminalitou je a není. Žáci prokázali největší znalost v oblasti phishingu, kde například výrok ,,vytvořím webové stránky, které vypadají jako přihlašovací stránka internetového bankovnictví, ale při přihlášení mi stránka pošle jméno a heslo uživatele'' označilo 93 % či situaci ,,vytvořím a pošlu někomu email, který vypadá jako zpráva z banky, aby poslal zpět svoje jméno a heslo'' označilo 88 % dotazovaných. Dále mají respondenti značné povědomí o hackingu, zejména neoprávněného přístupu do počítačového systému. To dokazují například tyto výroky ,,na počítači ve škole uvidím, jaké má učitel či učitelka heslo do elektronické žákovské a zkusím se přihlásit za ně a přepíšu nějaké známky'', který označilo za trestný 88 % dotazovaných, nebo ,,na počítači ve škole uvidím, jaké má učitel či učitelka heslo do elektronické žákovské a zkusím se přihlásit za ně a prohlédnu si prostředí žákovské'', je pro 86 % kyberkriminalita či ,,napíšu program, který umí odemknout nelegálně stažené windows'', v tomto příkladě se jedná o kyberkriminalitu pro 84 % žáků. Naopak nejmenší povědomí bylo zjištěno v oblasti porušování autorských práv, konkrétně u stahování filmů, či počítačových her a jejich nahrávání na internet. Například u ,,mám hodně stažených

filmů, tak je nahraju na server, aby si je ostatní taky mohli stáhnout a nemuseli si je hledat sami'', považuje za kyberkriminalitu pouhých 37 % žáků a ,,nahrávám na svůj blog odkazy, odkud si mohou lidi stahovat filmy'', pokládá za protiprávní jen 39 % dotazovaných.

V položkách č. 84-104 rozeznávali legální a trestné jednání na příkladech, které se zabývaly posíláním fotografií, online komunikací s cizí osobou, neoprávněným přístupem k blogu, a nahráváním videa na internet. Nejprve žáci řešili závadnost jednání u příkladu s posíláním fotografií s kamarádkou, které je 14 let. Příklad ,,ona mi pošle fotku, na které je svlečená'', je trestná pro 68 % dotazovaných a téměř stejný je výsledek i u položky ,,je mi 14 let a pošlu ji fotku, kde jsem nahý/nahá ve sprše'', tu označilo jako trestné jednání 72 % žáků. Následoval příklad týkající se internetové komunikace s dospělým. Jako trestné jednání nejčastěji respondenti (88 %) označili situaci ,,který po mě chce moje nahé fotografie''. Naopak legální jednání bylo nejvíce (90 %) zaznamenáváno ,,kterého dobře znám, například z tábora, apod''. Překvapujícím zjištěním byla situace ,,kterého neznám a on mě pozve na schůzku'', která je trestná jen pro 45 %. Dále žáci řešili příklad, kde umístí video na internet. Nejčastější volenou odpovědí z hlediska protiprávního jednání bylo tvrzení "přihlásím se, smažu jeho obsah a nahraji odkazy na pornografické stránky", které zvolilo 79 % studentů. Legální jednání volili žáci nejvíce u výroku ,,ho upozorním, aby si dával pozor na zabezpečení'', a to 86 %. Zajímavý výsledek jsme vysledovali u příkladu ,,přihlásím se a nahraji nějaké vtipy'', který označilo jako trestný 55 % žáků. V případě ,,přihlásím se a podívám se, jak je jeho blog udělaný'', se o trestném jednání domnívá 46 % žáků a pouze u 61 % respondentů se jedná o kyberkriminalitu v příkladu ,,se přihlásím na jeho účet, abych zjistil, zda jsem heslo viděl dobře''. Na závěr v rámci těchto otázek řešili žáci příklad, kdy umístí video na internet. Trestné jednání bylo nejvíce zaznamenáno u položky ,,je jeden náš spolužák bit ostatními'', odpovědělo tak 79 % žáků. U příkladů ,,předvádím známého zpěváka'' a ,,jsme s kamarády na sportovním dni ve škole'', se pro většinu respondentů o kyberkriminalitu nejedná. Na příkladu ,,se vysmíváme učiteli'', byly odpovědi téměř vyrovnané, protože protiprávní jednání předpokládá 46 %, kdežto o legálnosti jednání je přesvědčeno 54 % žáků.

V položce č. 105 jsme se dozvěděli, že nejvíce informací o kyberkriminalitě dostávají žáci od učitelů při výuce, počet odpovědí byl 138. Položka č. 106 ukázala, že nejraději by respondenti byli informováni o kyberkriminalitě od učitelů v rámci

výuky, kde byl počet odpovědí 103 a poté od policistů, kteří kyberkriminalitu vyšetřují (79) a od rodičů (72). Nejméně chtějí žáci dostávat informace o kyberkriminalitě od youtuberů či známých zpěváků během preventivního programu.

V rámci tohoto výzkumného šetření byly stanoveny 4 hypotézy. První hypotéza zkoumala statistickou souvislost mezi pohlavím respondentů a jejich zkušeností s kyberkriminalitou, tedy že dívky mají větší zkušenost s kyberkriminalitou než chlapci. Pomocí Chí - kvadrát testu nezávislosti jsme zjistili, že žádná taková statistická souvislost neexistuje, a proto jsme H1 zamítli. Toto tvrzení doplňuje i tabulka č. 2 uvedená v příloze, kde jsou výsledky odpovědí z hlediska pohlaví vyrovnané téměř u všech příkladů. Druhá hypotéza se zaměřovala na to, jak bezpečně se chovají žáci z pohledu kyberkriminality. Výsledky grafů č. 4,7,8,9 ukázaly, že se nadpoloviční většina žáků chová z pohledu kyberkriminality nebezpečně, a tudíž jsme H2 přijali. Třetí stanovená hypotéza sledovala, od koho chtějí žáci dostávat nejčastěji informace o kyberkriminalitě. Nejčastější odpovědí bylo od učitelů při výuce a na základě toho jsme přijali H3. Čtvrtá hypotéza zjišťovala výskyt nebezpečného chování na internetu. Na výsledcích, které uvádějí grafy č.2,5 a také tabulek v příloze práce můžeme vidět, že se nadpoloviční většina s nebezpečným chováním na internetu nesetkala, H4 jsme proto přijali.

Výzkumným cílem bylo zjistit, jaké zkušenosti mají žáci druhého stupně základních škol s kyberkriminalitou a jaké je jejich povědomí o této problematice a tento cíl byl splněn. Výsledky tohoto výzkumného šetření nelze generalizovat na celou populaci z důvodu malého výzkumného vzorku a také respondenti nemuseli vždy odpovídat upřímně podle pravdy.

Závěr

Cílem diplomové práce byla analýza kyberkriminality u žáků druhého stupně základních škol v České republice a tento cíl byl splněn. Diplomová práce je členěna na teoretickou a praktickou část. Teoretická část představuje základní poznatky o problematice kyberkriminality. Úvodní kapitola je zaměřena na kyberprostor, digitální stopu, sociální sítě a její typy. Druhá kapitola se zabývá jednotlivými projevy kyberkriminality. Zřetel je kladen na definice, druhy a možnosti prevence. Třetí kapitola se věnuje životnímu stylu dětí a prevenci, zejména školním preventivním dokumentům a také preventivním programům.

Praktická část je prezentována ve čtvrté kapitole této práce. V úvodu této kapitoly jsou uvedeny příklady studií, které se tématem kyberkriminality zabývají. Výzkumné šetření bylo realizováno kvantitativní metodou formou online dotazníkového šetření. Respondenty byli žáci druhého stupně základních škol z východočeského regionu. Sběr dat byl zahájen v listopadu 2023 a ukončen v březnu 2024. V tomto období byly oslovovány základní školy s prosbou o vyplnění online dotazníkového šetření a nakonec poskytlo sounáležitost celkem 5 z nich. Výzkumný vzorek tvořilo 191 respondentů. Byly stanoveny 4 hypotézy na základě odborné literatury a vědeckých studií. První hypotéza byla testována pomocí Chí – kvadrát testu nezávislosti, která nedokázala významně statistickou souvislost mezi pohlavím respondentů a zkušeností respondentů s kyberkriminalitou. Druhá hypotéza zkoumala, jak se žáci z pohledu kyberkriminality chovají bezpečně a na základě výsledků znázorněných v jednotlivých grafech byla přijata. Třetí hypotéza zjistila, že žáci chtějí být nejčastěji informováni o kyberkriminalitě od učitelů při výuce, a proto byla taktéž přijata. U čtvrté hypotézy bylo výsledky prokázáno, že se nadpoloviční většina studentů nesetkala s nebezpečným chováním na internetu, byla tím potvrzena. Cílem výzkumného šetření bylo zjistit zkušenosti, jaké mají žáci druhého stupně základních škol s kyberkriminalitou a jaké je jejich povědomí o této problematice. Tohoto cíle bylo dosaženo. K zajímavým výsledkům tohoto šetření patří zjištění, že se žáci nejvíce orientují v oblasti týkající se phishingu a hackingu. Naopak ze zjištěných výsledků je patrné, že žáci mají malé povědomí v oblasti porušování autorských práv, a také kybernetické agrese. Nejvíce alarmujícím zjištěním však bylo, že zkušenost s uvedenými příklady kyberkriminality měli respondenti v rozmezí 10-22 %. To může být zkresleno možnými nepravdivými odpověďmi.

Diplomová práce by mohla být užitečná základním školám, včetně jejich pracovníků, aby se na rizikové jevy mohli efektivně připravit, a také jim předcházet.

Seznam použitých zdrojů

Tištěné zdroje

BAKOŠOVÁ, Zlatica. *Rodina, tolerancia inakosti a kvalita života detí a mládeže: Pedagogika na križovatke nových výziev: konvergencie tradícií a inovátorstva vo výchove a vzdelávaní smerujúce ku kvalitnému životu detí a mládeže v reálnom svete.* Bratislava: Univerzita Komenského v Bratislave vo Vydavateľstve UK, 2017. ISBN 978-80-223-4353-4.

BĚLÍK, Václav a SVOBODA HOFERKOVÁ, Stanislava. *Prevence rizikového chování ve školním prostředí: pro studenty pomáhajících oborů*. First edition in Tribun EU. Brno: Tribun EU, 2016. 141 s. ISBN 978-80-263-1015-0.

ČECH, Tomáš. Prevence. In: MIOVSKÝ, Michal a kol. *Výkladový slovník základních pojmů školské prevence rizikového chování*. Druhé, přepracované a doplněné vydání. Praha: Klinika adiktologie 1. LF UK v Praze a VFN v Praze, 2015. 143-148 s. Monografie. ISBN 978-80-7422-391-4.

HOLLÁ, Katarína. Sexting a kyberšikana. Vydanie: prvé. Bratislava: Iris, 2016. 165 s. ISBN 978-80-8153-061-6.

HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. 217 s. ISBN 978-80-7387-545-9.

KOHOUT, Roman a KARCHŇÁK, Radek. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary, 2016. 67 s. ISBN 978-80-260-9543-9.

KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. 521 s. ISBN 978-80-88168-15-7.

KOLOUCH, Jan, BAŠTA, Pavel et al. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. 560 s. ISBN 978-80-88168-34-8.

KOPECKÝ, Kamil a kol. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Olomouc: Univerzita Palackého v Olomouci, 2015. 170 s. ISBN 978-80-244-4861-9.

KOPECKÝ, Kamil; SZOTKOWSKI, René a DOBEŠOVÁ, Pavla. *Riziková komunikace a seznamování českých dětí v kyberprostoru*. Olomouc: Univerzita Palackého v Olomouci, 2021. 112 s. ISBN 978-80-244-5914-1.

KOPECKÝ, Kamil, SZOTKOWSKI, René a KUBALA, Lukáš. *Bezpečné chování na internetu pro kluky a pro holky: (náměty na výukové aktivity)*. Olomouc: Univerzita Palackého v Olomouci, 2022. 157 s. ISBN 978-80-244-6197-7.

KRAUS, Blahoslav. *Sociální deviace v transformaci společnosti*. Hradec Králové: Gaudeamus, 2015. 210 s. ISBN 978-80-7435-575-2.

KRAUS, Blahoslav et al. *Životní styl současné české rodiny*. Hradec Králové: Gaudeamus, 2015. 246 s. ISBN 978-80-7435-544-8.

MCCARTHY, Linda, ed. a WELDON-SIVIY, Denise, ed. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha: CZ.NIC, 2013. 316 s. ISBN 978-80-904248-6-9.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. 1166 s. ISBN 978-80-7380-849-5.

SPITZER, Manfred. *Digitální demence: jak připravujeme sami sebe a naše děti o rozum*. Brno: Host, 2014. 341 s. ISBN 978-80-7294-872-7.

SZOTKOWSKI, René a kol. Sexting u českých dětí. Olomouc: Univerzita Palackého v Olomouci, 2020. 264 s. ISBN 978-80-244-5793-2.

ŠEVČÍKOVÁ, Anna. Sexuální chování, internet a závislost. In: BLINKA, Lukáš a kol. *Online závislosti: jednání jako droga?: online hry, sex a sociální sítě: diagnostika závislosti na internetu: prevence a léčba*. Praha: Grada, 2015. s. 131-153. Psyché. ISBN 978-80-210-7975-5.

ŠMAHET,David. Děti na internetu. In: ŠEVČÍKOVÁ, Anna a kol. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014. s. 19-34. Psyché. ISBN 978-80-210-7527-6.

ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. 147 s. ISBN 978-80-7380-737-5.

TRÉDEZ, Emmanuel. *Sociální sítě - a to funguje jak?: všechno, co vás zajímá, když jste online*. Ilustroval HALFBOB, přeložil Zuzana KLIMŠOVÁ. Malé a velké otázky. Praha: Svojtka & Co., 2018. 47 s. ISBN 978-80-256-2416-6.

ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. ix, 135 s. Právní monografie. ISBN 978-80-7552-758-5.

Elektronické zdroje

02 CHYTRÁ ŠKOLA. Co je kyberstalking. In: *02 Chytrá škola.* [online]. 2018. [cit. 2024-01-21]. Dostupné z: https://o2chytraskola.cz/clanky/online-bezpecnost/kyberstalking/co-je-kyberstalking.

CENTRUM PREVENCE RIZIKOVÉ RIZIKOVÉ VIRTUÁLNÍ KOMUNIKACE. *Sexting a rizikové seznamování českých dětí v kyberprostoru*. [online]. Olomouc: Univerzita Palackého v Olomouci, 2017. 31 s. [cit. 2024-01-21]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/133-sexting-vyzkumna-zprava-1-6-update/file.

THE CYBERSMILE FOUNDATION. *ASK.FM*. [online]. 2024 [cit. 2023-11-27]. Dostupné z: https://www.cybersmile.org/advice-help/category/askfm.

Cyberspace Operations: Concept Capability Plan 2016-2028. [online]. [cit. 2023-05-04]. s. 6. Dostupné z: https://irp.fas.org/doddir/army/pam525-7-8.pdf.

CZ.NIC. Safer Internet Centrum [online]. [cit. 2024-01-21]. Dostupné z: https://www.bezpecnyinternet.cz/cs/o-nas/. prevence rizikové virtuální komunikace. 2020. [cit. 2024-01-21]. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=2092.

ČERNÁ, Monika a Michal ČERNÝ. *Úvod do problematiky sociálních sítí*. [online]. [cit. 2023-05-04]. Dostupné z: https://clanky.rvp.cz/clanek/o/g/15075/UVOD-DO-PROBLEMATIKY-SOCIALNICH-SITI.html.

DAŇHELKA, Tomáš. *Vnímání kyberkriminality mezi dětmi výzkumná zpráva*. [online]. Jihlava: Projekt Kraje pro bezpečný internet, 2018. [cit. 2024-01-27]. Dostupné z: http://www.vyzkum-mladez.cz/zprava/1568019261.pdf.

DOBOSIOVÁ, Martina. *Kategorie současných sociálních sítí a aktuální sociální sítě.* In: Metodický portál [online]. 2015. [cit. 2023-11-25]. Dostupný z www: <https://clanky.rvp.cz/clanek/20145/KATEGORIE-SOUCASNYCH-SOCIALNICH-SITI-A-AKTUALNI-SOCIALNI-SITE.html>. ISSN 1802-4785.

E-BEZPEČÍ. Informace o projektu. In: *E-bezpečí* [online]. [cit. 2024-04-01]. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu.

E-BEZPEČÍ. Trestná činnost spojená s internetovou kriminalitou. In: *E-bezpečí* [online]. 2009. [cit. 2024-04-01]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/dali-rizika/148-226.

ESET SOFTWARE SPOL. S R.O. *To nevymažeš* [online]. Praha: Classic 7 Business Park, 2024. [cit. 202-01-21]. Dostupné z: https://www.tonevymazes.cz/.

KOPECKÝ, Kamil a KREJČÍ, Veronika. *Sociální sítě – úvod do problematiky*. [online]. Olomouc: Univerzita Palackého v Olomouci, 2023. [cit. 2024-01-27]. ISBN 978-80-244-6370-4. Dostupné z: https://e-bezpeci.cz/index.php/ke-stazeni/odborne-studie/166-socialni-site-uvod-do-problematiky-2023-kopecky-krejci/file.

KOPECKÝ, Kamil. *Pediatrie pro praxi*. [online]. 2015, roč. 16, č. 5. Olomouc: Solen, 2015. [cit. 2024-01-07]. ISSN 1803-5264. Dostupné z: https://www.pediatriepropraxi.cz/pdfs/ped/2015/05/09.pdf.

KOPECKÝ, K., SZOTKOWSKI, R. Sexting a právo. [online]. 2019 E-Bezpečí, roč. 4, č. 2, s. 62-65. Olomouc: Univerzita Palackého, 2019. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=1681.

KRAJE PRO BEZPEČNÝ INTERNET. *Informace o projektu* [online]. 2021. [cit. 2023-11-27]. Dostupné z: https://www.kpbi.cz/o-projektu.

INTERNETEM BEZPEČNĚ. Sociální sítě. In: *Internetem bezpečně* [online]. 2018. [cit. 2023-11-27]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/socialni-media/socialni-site/.

INTERNETEM BEZPEČNĚ. Kyberstalking. In: *Internetem bezpečně* [online]. 2018. [cit. 2024-01-22]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/.

Metodické doporučení k primární prevenci rizikového chování u dětí, žáků a studentů ve školách a školských zařízeních (dokument **č.j.**21291/2010-28, 2010). 2010. Ministerstvo školství, mládeže a tělovýchovy [online]. 2010 [cit. 2024-01-07]. Dostupné z: https://www.msmt.cz/vzdelavani/socialni-programy/metodicke-dokumenty-doporuceni-a-pokyny?highlightWords=metodick%C3%A9+doporu%C4%8Den%C3%AD.

Národní strategie primární prevence rizikového chování dětí a mládeže na období 2019-2027. 2019. Ministerstvo školství, mládeže a tělovýchovy [online]. [cit. 2024-01-07]. Dostupné z: https://www.msmt.cz/uploads/narodni_strategie_primarni_prevence_2019_27.pdf.

POLICIE ČESKÉ REPUBLIKY. Informační servis. *Preventivní projekt Tvoje cesta onlinem* [online]. [cit. 2024-02-12]. Dostupné z: https://www.policie.cz/clanek/preventivni-projekt-tvoje-cesta-onlinem.aspx.

POLICIE ČESKÉ REPUBLIKY. Prevence. *Pomoc obětem tč – Počítačová kriminalita.* [online]. [cit. 2024-01-23]. Dostupné z: https://www.policie.cz/clanek/pomoc-obetem-tc-pocitacova-kriminalita.aspx.

POLICIE ČESKÉ REPUBLIKY. Útvary Policie ČR. *Jednotlivé druhy kyberkriminality* [online]. [cit. 2023-11-27]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.

POLICIE ČESKÉ REPUBLIKY. Útvary Policie ČR. *Kyberkriminalita* [online]. [cit. 2023-11-27]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx.

POLICIE ČESKÉ REPUBLIKY. Útvary Policie ČR. *Preventisté radí – Prevence kyberšikana* [online]. [cit. 2023-11-27]. Dostupné z: https://www.policie.cz/clanek/prevence-kybersikana.aspx.

SEXTING.CZ – VŠE, CO CHCETE VĚDĚT O SEXTINGU [online]. [cit. 2024-01-21]. Dostupné z: www.sexting.cz.

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. Dostupné z: https://doi.org/10.21953/lse.47fdeqj01ofo.

STŘÍLKOVÁ, Pavla, KOPECKÝ, Kamil. *Nebezpečné výzvy pohledem českých dětí (výzkumná zpráva)*. [online]. Olomouc: Univerzita Palackého v Olomouci Centrum prevence rizikové virtuální komunikace. 2020. [cit. 2024-01-21]. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=2092.

UNIVERZITA PALACKÉHO V OLOMOUCI. [online]. Olomouc: Univerzita Palackého v Olomouci, 2024 [cit. 2024-02-11]. Dostupné z: https://veda.upol.cz/pracoviste/vyzkumna-pracoviste/centrum-prevence-rizikove-virtualni-komunikace/.

VÝZKUM RIZIKOVÉHO CHOVÁNÍ ČESKÝCH DĚTÍ V PROSTŘEDÍ INTERNETU. [online]. Olomouc: Univerzita Palackého v Olomouci. 2014. 20 s. [cit. 2024-01-21]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prostedi-internetu-2014-prezentace.

Legislativa

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

Zákon č. 40/2009 Sb., trestní zákoník.

Seznam příloh

Příloha A: Seznam grafů

Příloha B

Tabulka č. 2 – Na internetu se nesmí dělat, kompletní výsledky

Na internetu se nesmí dělat, kompletní výsledky	počet	procenta
Stáhnu si placenou počítačovou hru z internetu, kterou někdo nahrál na internetové úložiště, například na uložto.cz.	90	47 %
Přijdu k počítači ve škole, je otevřený prohlížeč, a když dám zpět, tak se mi otevře spolužákův facebook. Když už jsem na jeho facebooku, tak si ho prohlédnu.	126	66 %
Nahraji kamarádovi bez jeho vědomí do počítače program, abych se mohl dívat, co na počítači dělá.	178	93 %
Nahrávám na svůj blog odkazy, odkud si mohou lidi stahovat filmy.	74	39 %
Vytvořím webové stránky, které vypadají jako přihlašovací stránka internetového bankovnictví, ale při přihlášení mi stránka pošle jméno a heslo uživatele.	177	93 %
Mám hodně stažených filmů, tak je nahraju na server, aby si je ostatní taky mohli stáhnout a nemuseli si je hledat sami.	71	37 %
Použiji heslo a uživatelské jméno uživatele, které mi poslali webové stránky, které napodobují vzhled facebooku.	155	81 %
Nahraji na internet do diskuzního fóra cracky k počítačovým hrám ke stažení.	118	62 %
Náhodou uvidím, jaké mají uživatelské jméno a heslo na internetové bankovnictví a podívám se na jejich účet.	165	86 %
Stáhnu si písničku nebo video z internetu a pouštím si ji.	38	20 %
Zkusím odhadnout heslo, které má kamarád na facebooku a přihlásit se za něj.	146	76 %
Dám na svůj facebook zprávu, že učitel či učitelka je pitomý/-á.	94	49 %
Přijdu k počítači, uvidím, že se kamarád neodhlásil z facebooku, tak mu něco napíšu na jeho facebook.	157	82 %
Na počítači ve škole uvidím, jaké má učitelka či učitel heslo do elektronické žákovské a zkusím se přihlásit za ně a prohlédnu si prostředí žákovské.	164	86 %
Stahuji si z internetu programy pro crackování her.	131	69 %
Náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo a podívám se na jeho profil na internetu.	149	78 %
Zkusím se připojit jako administrátor do školní sítě, abych viděl, jak je zabezpečená.	142	74 %

Na internetu se nesmí dělat, kompletní výsledky, pokr.	počet	procenta
Náhodou uvidím, jaké kamarád zadal uživatelské jméno a heslo do jeho facebooku, použiju ho a podívám se na jeho facebook.	154	81 %
Nabízím na internetu za nabití kreditu zaslání staženého filmu nebo programu.	128	67 %
Nahrávám na svůj blog odkazy, odkud si mohou stáhnout cracky k počítačové hře.	132	69 %
Na kamarádovu zeď na facebooku umístím video, na kterém je zachycen on v trapné situaci, která mu je nepříjemná.	150	79 %
Na počítači ve škole uvidím, jaké má učitel či učitelka heslo do elektronické žákovské a zkusím se přihlásit za ně a přepíšu nějaké známky.	168	88 %
Vytvořím a pošlu někomu email, který vypadá jako zpráva z banky, aby poslal zpět svoje jméno a heslo.	168	88 %
Udělám si doma sbírku cracků k programům nebo hrám.	125	65 %
Napíšu program, který umí odemknout nelegálně stažené windows.	161	84 %
Stáhnu si z internetu volně dostupný kód počítačového viru a pošlu ho z legrace kamarádovi.	157	82 %
Na kamarádovu zeď na facebooku napíši vulgární nadávky směřované na jeho osobu.	144	75 %
Použiji program, který mi zjistí heslo do cizí wifi sítě.	152	80 %
Nahraji na internet program, který umí odemknout zkušební verzi windows, aby šla používat pořád.	121	63 %
Dám na svůj facebook zprávu, že by měli jít cikáni do plynu.	137	72 %
Spolužák mne naštval, tak se na něj domluvím se spolužáky a všichni mu budeme posílat na sociálních sítích zprávy, že je fakt strašný a měl by se raději zabít.	156	82 %
Použiji program, který zablokuje provoz nějaké webové stránky svými stálými dotazy.	142	74 %
Změním pomocí cracku zakoupenou počítačovou hru, aby ji mohli používat všichni.	134	70 %
Nahraju na wikipedii článek o tom, jak je škola pitomá.	86	45 %

Na internetu se nesmí dělat, kompletní výsledky, pokr.	počet	procenta
Zjistím si heslo k blogu kamaráda a na jeho blog nahraju za něj nějaké vtipné hlášky.	140	73 %
Dám na facebookovou zeď kamaráda zprávu, že by měli být uprchlíci nahnáni zpět do moře.	143	75 %
Náhodou zjistím heslo k blogu kamaráda a na jeho blogu smažu jeho zprávy a místo nich dám odkazy na porno stránky.	157	82 %
Použiji program, který mi ve školní síti zjistí, kdo si co píše na chatu.	150	79 %
Použiji program, který mi ve školní síti zjistí heslo, které zadávají ostatní spolužáci do sítě.	159	83 %
Pošlu své kamarádce či kamarádovi (14 let) svojí fotku ve spodním prádle.	122	64 %
Na internetu si stáhnu číslo kreditní karty a použiju ho na platební bráně k zaplacení počítačové hry.	152	80 %
Pošlu spolužákovi zprávu, že si na něj před školou s kamarády počkáme a že dostane pěstí.	122	64 %
Přepíšu na wikipedii článek o nějaké osobnosti, kde si vymyslím vtipné hlášky místo skutečnosti.	125	65 %
Píši si na internetu s dospělým člověkem.	58	30 %
Pošlu své kamarádce či kamarádovi (14 let) svojí fotku ze sauny, kde jsem nahý.	147	77 %
Napíšu svému kamarádovi či kamarádce, že když mi nepošle další fotku, tak tu, kterou mi již poslal/-a, zveřejním na internetu.	156	82 %
Staženou písničku si nahraju na svůj blog, aby si ji ostatní taky mohli stáhnout.	77	40 %
Kamarádka (14 let) mi pošle svoji fotku ve spodním prádle.	117	61 %
Pošlu email na policii, že na letišti je bomba	153	80 %
Nainstaluji v rozporu se školním řádem do školního počítače nějakou svoji hru.	118	62 %
Rodiče mi dají svoje číslo platební karty, abych ji mohl používat, a já si s ní zaplatím počítačovou hru na telefon.	76	40 %
Kamarád či kamarádka (14 let) mi pošle svojí fotku, na které se nahý /nahá sprchuje.	140	73 %
Počítačový virus zablokuje počítač a musím někam poslat peníze, aby mi ho zase odblokoval.	156	82 %

Příloha C

Tabulka č. 3 - Uveď, zda jsi danou věc zkoušel nebo dělal, kompletní výsledky

Uveď, zda jsi danou věc zkoušel nebo dělal, kompletní výsledky	Počet Ano	Procenta Ano	Počet Ne	Procenta Ne
Rozesílal jsi spamové emailové zprávy, nebo sis nainstaloval program, který to dělá?	33	17 %	158	83 %
Rozesílal nebo přeposílal jsi na facebooku či jinde odkazy na soutěže typu "klikni a vyhraj" (například vyhraj iphone, atd.)?	36	19 %	155	81 %
Vytvořil jsi někdy webovou stránku, která se snaží vypadat jako stránka někoho jiného a ve skutečnosti shromažďuje zadané údaje?	19	10 %	172	90 %
Připojoval ses bez dovolení na facebookový profil někoho jiného?	32	17 %	159	83 %
Připojoval ses bez dovolení do cizího emailu?	33	17 %	158	83 %
Použil jsi někdy program, který ti umožnil se přihlásit do cizí wifi sítě?	42	22 %	149	78 %
Zkoušel jsi odposlouchávat provoz v počítačové síti?	21	11 %	170	89 %
Přihlásil ses neoprávněně k cizí webové stránce?	27	14 %	164	86 %
Přihlásil ses neoprávněně do cizího internetového bankovnictví?	22	12 %	169	88 %
Použil jsi bez svolení cizí platební kartu na internetu?	32	17 %	159	83 %
Posílal jsi někomu nahé fotografie osoby mladší 15 let (svoje nebo i cizí)?	31	16 %	160	84 %
Poslal jsi někomu schválně počítačový vir nebo jiný škodlivý program?	26	14 %	165	86 %
Pozměnil jsi bez oprávnění nějaký počítačový program?	34	18 %	157	82 %
Stahuješ si hudbu z internetu?	112	59 %	79	41 %
Stahuješ si videa z internetu?	86	45 %	105	55 %
Nahráváš staženou hudbu na internet, nebo tam nahráváš odkazy, odkud je lze stáhnout?	38	20 %	153	80 %
Nahráváš stažená videa na internet, nebo tam nahráváš odkazy, odkud je lze stáhnout?	40	21 %	151	79 %

Uveď, zda jsi danou věc zkoušel nebo dělal, kompletní výsledky, pokr.	Počet Ano	Procenta Ano	Počet Ne	Procenta Ne
Psal jsi na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťani, apod.)?	42	22 %	149	78 %
Poslal jsi někdy přes internet výhružný email nebo zprávu?	33	17 %	158	83 %
Požadoval jsi prostřednictvím internetu, nebo sociálních sítí, po někom něco udělat, jinak mu provedeš něco nepříjemného (například zveřejníš jeho fotografie nebo video, apod.)?	27	14 %	164	86 %
Šikanoval jsi někoho přes internet nebo na sociálních sítích?	30	16 %	161	84 %
Psal sis na internetu nebo sociálních sítích komunikaci s erotickým obsahem?	40	21 %	151	79 %
Stahoval sis z internetu kódy platebních karet cizí osoby?	25	13 %	166	87 %
Použil jsi internetové bankovnictví cizí osoby bez jejího vědomí?	24	13 %	167	87 %
Udělal sis registraci na internetu, kde jsi uvedl jiné údaje, než skutečné?	97	51 %	94	49 %
Objednal sis na internetu zboží na jiné údaje, než skutečné?	35	18 %	156	82 %

Příloha D

Tabulka č. 4 – Uveď, zda je jednání podle tebe škodlivé či trestné, kompletní výsledky

Posíláme si s kamarádkou (14 let) fotografie	1 Počet	2	3	4	1 Procenta	2	3	4
z výletu s rodiči	159	19	3	10	83 %	10 %	2 %	5 %
ona mi pošle fotku, na které je ve spodním prádle	16	99	37	39	8 %	52 %	19 %	20 %
je mi 14 let a pošlu jí fotku, kde jsem nahý/ nahá ve sprše	7	47	49	88	4 %	25 %	26 %	46 %
ona mi pošle fotku, na které je svlečená	14	47	37	93	7 %	25 %	19 %	49 %
je mi 16 let a pošlu jí fotku, kde jsem nahý /nahá v sauně	15	51	39	86	8 %	27 %	20 %	45 %
napíšu své kamarádce, že když mi nepošle další fotku, tak tu nahou, kterou mi již poslala, zveřejním na internetu	6	16	12	157	3 %	8 %	6 %	82 %
Na internetu si se mnou píše dospělý,	1 Počet	2	3	4	1 Procenta	2	3	4
kterého dobře znám, například z tábora, apod.	148	24	8	11	77 %	13%	4 %	6 %
kterého neznám	32	109	21	29	17 %	57 %	11 %	15 %
kterého neznám a on mne pozve na schůzku	13	91	33	54	7 %	48 %	17 %	28 %
který po mne chce moje nahé fotografie	10	18	20	143	5 %	9 %	10 %	75 %

Pozn: 1 – úplně v pořádku netrestné, 2 – nevhodné či nepřijatelné, ale stále netrestné, 3 – trestné, ale tolerováno, 4 – trestné nepřijatelné

Uvidím, jaké má kamarád/-ka heslo na svůj blog, takže	1 Počet	2	3	4	1 Procenta	2	3	4
se přihlásím na jeho účet, abych zjistil, zda jsem heslo viděl dobře	6	68	58	59	3 %	36 %	30 %	31 %
ho upozorním, aby si dával pozor na zabezpečení	136	29	9	17	71 %	15 %	5 %	9 %
se na něj přihlásím a prohlédnu si, jak má blog dělaný	14	89	46	42	7 %	47 %	24 %	22 %
se na něj přihlásím a nahraji mu blog několik vtipů	12	73	60	46	6 %	38 %	31 %	24 %
se na něj přihlásím se, smažu mu jeho obsah a nahraji tam odkazy na porno stránky	7	33	34	117	4 %	17 %	18 %	61 %
Umístím na internet video, na kterém	1 počet	2	3	4	1 procenta	2	3	4
jsme s kamarády na sportovním dni ve škole	132	29	13	17	69 %	15 %	7 %	9 %
je kamarád, když neví látku při zkoušení u tabule	25	103	32	31	13 %	54 %	17 %	16 %
předvádím známého zpěváka	108	54	13	16	57 %	28 %	7 %	8 %

Umístím na internet video, na kterém	1 počet	2	3	4	1 procenta	2	3	4
kamarád předvádí známého zpěváka a vůbec mu to nejde	50	99	22	20	26 %	52 %	12 %	10 %
se vysmíváme učiteli	17	85	50	39	9 %	45 %	26 %	20 %
je jeden náš spolužák bit ostatními	13	27	42	109	7 %	14 %	22 %	57 %

Pozn: 1 – úplně v pořádku netrestné, 2 – nevhodné či nepřijatelné, ale stále netrestné, 3 – trestné, ale tolerováno, 4 – trestné nepřijatelné

Příloha E

Tabulka č. 5 - Uveď, zda jsi danou věc zkoušel nebo dělal vůči pohlaví respondentů

Uveď, zda jsi danou věc zkoušel nebo dělal vůči pohlaví respondentů	Počet Ano	Procenta Ano	Ano Dívky	Ano Chlapci
Rozesílal jsi spamové emailové zprávy, nebo sis nainstaloval program, který to dělá?	33	17 %	11	22
Rozesílal nebo přeposílal jsi na facebooku či jinde odkazy na soutěže typu "klikni a vyhraj" (například vyhraj iphone, atd.)?	36	19 %	13	23
Vytvořil jsi někdy webovou stránku, která se snaží vypadat jako stránka někoho jiného a ve skutečnosti shromažďuje zadané údaje?	19	10 %	6	13
Připojoval ses bez dovolení na facebookový profil někoho jiného?	32	17 %	13	19
Připojoval ses bez dovolení do cizího emailu?	33	17 %	14	19
Použil jsi někdy program, který ti umožnil se přihlásit do cizí wifi sítě?	42	22 %	13	29
Zkoušel jsi odposlouchávat provoz v počítačové síti?	21	11 %	9	12
Přihlásil ses neoprávněně k cizí webové stránce?	27	14 %	11	16
Přihlásil ses neoprávněně do cizího internetového bankovnictví?	22	12 %	8	14
Použil jsi bez svolení cizí platební kartu na internetu?	32	17 %	11	21
Posílal jsi někomu nahé fotografie osoby mladší 15 let (svoje nebo i cizí)?	31	16 %	13	18
Poslal jsi někomu schválně počítačový vir nebo jiný škodlivý program?	26	14 %	5	21
Pozměnil jsi bez oprávnění nějaký počítačový program?	34	18 %	12	22
Stahuješ si hudbu z internetu?	112	59 %	58	54
Stahuješ si videa z internetu?	86	45 %	44	42
Nahráváš staženou hudbu na internet, nebo tam nahráváš odkazy, odkud je lze stáhnout?	38	20 %	15	23

Uveď, zda jsi danou věc zkoušel nebo dělal vůči pohlaví respondentů – pokračování	Počet Ano	Procenta Ano	Ano Dívky	Ano Chlapci
Nahráváš stažená videa na internet, nebo tam nahráváš odkazy, odkud je lze stáhnout?	40	21 %	18	22
Psal jsi na internet nějaké nenávistné příspěvky proti nějaké skupině osob (například romové, uprchlíci, křesťani, apod.)?	42	22 %	18	24
Poslal jsi někdy přes internet výhružný email nebo zprávu?	33	17 %	12	21
Požadoval jsi prostřednictvím internetu, nebo sociálních sítí, po někom něco udělat, jinak mu provedeš něco nepříjemného (například zveřejníš jeho fotografie nebo video, apod.)?	27	14 %	8	19
Šikanoval jsi někoho přes internet nebo na sociálních sítích?	30	16 %	9	21
Psal sis na internetu nebo sociálních sítích komunikaci s erotickým obsahem?	40	21 %	15	25
Stahoval sis z internetu kódy platebních karet cizí osoby?	25	13 %	5	20
Použil jsi internetové bankovnictví cizí osoby bez jejího vědomí?	24	13 %	9	15
Udělal sis registraci na internetu, kde jsi uvedl jiné údaje, než skutečné?	97	51 %	45	52
Objednal sis na internetu zboží na jiné údaje, než skutečné?	35	18 %	12	23

Příloha F: Seznam tabulek