ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ

Katedra zdravotnických oborů a ochrany obyvatelstva

Analýza kyberkriminality na základních školách v České republice

Anylysis of Cybercrime on the Elementary Schools in the Czech Republic

Diplomová práce

Studijní program:	Ochrana obyvatelstva
Studijní obor:	Civilní nouzové plánování

Autor diplomové práce:	Bc. Jiří Dvořák
Vedoucí diplomové práce:	doc. PhDr. Barbora Vegrichtová, Ph.D., MBA

Kladno 2020

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Dvořák**	Jméno:	**Jiří**	Osobní číslo:	**484168**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra zdravotnických oborů a ochrany obyvatelstva**				
Studijní program:	**Ochrana obyvatelstva**				
Studijní obor:	**Civilní nouzové plánování**				

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Analýza kyberkriminality na základních školách v České republice

Název diplomové práce anglicky:

Analysis of Cybercrime on the Elementary Schools in the Czech Republic

Pokyny pro vypracování:

Diplomová práce bude prověřovat povědomí žáků základních škol v České republice o kyberkriminalitě. V teoretické části budou popsány základní pojmy z oblasti informačních a komunikačních technologií a také jednotlivé projevy kyberkriminality se zaměřením na kyberšikanu, sexting, kyberstalking a kybergrooming. Na teoretickou část bude navazovat část výzkumná, kde bude pomocí dotazníkových šetření zkoumána úroveň povědomí o kyberkriminalitě u dětí na vybraných základních školách ve Středočeském kraji. Na základě dotazníků bude realizována beseda, která bude mít za cíl povědomí dětí zlepšit a současně se zaměřit na uvědomění si rizikového chování na síti internet. Přínos besedy bude později prověřen testováním proškolených subjektů. Účinnost besedy bude vyhodnocena pomocí SWOT analýzy se zaměřením na rozdíly mezi městskými a venkovskými školami. V rámci problematiky budou uvedeny i případové studie. Závěrem budou navržena opatření, jak kyberkriminalitě páchané na dětech v České republice předcházet. Celý projekt bude koncipován v zájmu ochrany dítěte v rámci prevence Policie ČR.

Seznam doporučené literatury:

[1] KOLOUCH, Jan, CyberCrime, Praha: CZ.NIC, 2016, ISBN 978-80- 88168-15-7
[2] ZAVRŠNIK, Aleš, Kyberkriminalita, Praha: Wolters Kluwer, 2017, Právní monografie, ISBN 978-80-7552-758-5
[3] SMEJKAL, Vladimír, Kybernetická kriminalita, Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s., ISBN 978-80-7380-501-2

Jméno a příjmení vedoucí(ho) diplomové práce:

PhDr. Barbora Vegrichtová, Ph.D., MBA

Jméno a příjmení konzultanta(ky) diplomové práce:

Mgr. Monika Donevová

Datum zadání diplomové práce: **23.09.2019**
Platnost zadání diplomové práce: **18.09.2021**

prof. MUDr. Leoš Navrátil, CSc., MBA, dr.h.c.	prof. MUDr. Ivan Dylevský, DrSc.
podpis vedoucí(ho) katedry	podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Student(ka) bere na vědomí, že je povinnen(a) vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

27.9. 2019	
Datum převzetí zadání	Podpis studenta(ky)

PROHLÁŠENÍ

Prohlašuji, že jsem diplomovou práci s názvem Analýza kyberkriminality na základních školách v České republice vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně dne 31.03.2020

…….

Bc. Jiří Dvořák

PODĚKOVÁNÍ

Rád bych tímto poděkoval a vyslovil uznání všem, kteří mi pomáhali a podporovali mě při vzniku této práce. Především patří dík vážené paní doc. PhDr. Barboře Vegrichtové, Ph.D., MBA za vedení mé diplomové práce, za rady a za cenné připomínky, které mi poskytla. Mé poděkování patří taktéž paní Mgr. Monice Donevové, jakožto odborné konzultantce. Zároveň děkuji všem respondentům z řad žáků základních škol ve Středočeském kraji.

ABSTRAKT

Obsahem této diplomové práce je problematika kyberkriminality u žáků základních škol ve Středočeském kraji.

Práce je rozdělena na část teoretickou a výzkumnou. V teoretické části je kladen důraz na popsání základních pojmů z oblasti informačních a komunikačních technologií a také na jednotlivé projevy kyberkriminality se zaměřením na kyberšikanu, sexting, kyberstalking a kybergrooming. Na teoretickou část úzce navazuje část výzkumná, ve které jsou vymezeny cíle práce, hypotézy, jsou zde popsány metody výzkumu, vymezen výzkumný vzorek a prostředky k dosažení relevantního výsledku.

K dosažení zvoleného cíle je zvolena metoda sběru dat prostřednictvím anonymních dotazníkových šetření, kdy je zkoumána úroveň povědomí o kyberkriminalitě u dětí na vybraných základních školách ve Středočeském kraji. Na základě těchto šetření je realizována beseda, která má za cíl povědomí dětí zlepšit a současně se zaměřit na uvědomění si rizikového chování na síti internet. Přínos besedy je poté prověřen testováním proškolených subjektů. Účinnost besedy je dále vyhodnocena pomocí SWOT analýzy se zaměřením na rozdíly mezi městskými a venkovskými školami. V rámci problematiky jsou do práce zahrnuty také případové studie. Závěrem jsou navržena opatření, jak kyberkriminalitě páchané na dětech v České republice předcházet. Celý projekt je koncipován v zájmu ochrany dítěte v rámci prevence Policie ČR.

Klíčová slova

Kyberkriminalita; kyberšikana; sexting; kyberstalking; kybergrooming; Policie ČR; základní škola; žáci.

ABSTRACT

This thesis focuses on the issue of cybercrime among elementary school pupils in the Central Bohemia region of the Czech Republic.

The thesis includes a theoretical section and a research section. The theoretical section outlines the basic concepts of IT and communication technologies and various types of cybercrime including cyber bullying, sexting, cyber stalking and cyber grooming. This theoretical basis is then applied in the research part of the thesis, which defines the goals and hypotheses as well research methodology, the study sample and means employed to generate relevant results.

In order to achieve the set goals, data were collected through anonymous questionnaires that examined the level of cybercrime awareness among the pupils of selected elementary schools in the Central Bohemia region. The collected data then served as a basis for a discussion with the children with the aim of increasing their awareness and highlighting the risks of they may encounter online. The impact of the discussion is then measured by a follow-up test among the participants. The effectiveness of the discussion is also evaluated through a SWOT analysis with a particular emphasis on the differences between urban and rural schools. The thesis also discusses several case studies. The thesis conclusion then proposes measures to combat and prevent cybercrime targeting Czech children. The entire project is designed in the interest of child protection as part of preventive efforts of the Police of the Czech Republic.

Key words

Cybercrime; cyber bullying; sexting; cyber stalking; cyber grooming; Police of the Czech Republic; elementary school; pupils.

Obsah

1 ÚVOD

Termínem kyberkriminalita (nebo také kybernetická kriminalita, kriminalita počítačová či kriminalita internetová) jsou označovány útoky v tzv. kyberprostoru spočívající v trestné činnosti ve vztahu k uloženým datům v počítačovém systému nebo v trestné činnosti, při nichž je počítač prostředkem k jejich páchání. Je však nutné poznamenat, že v dnešní době „SmartThings“ lze páchat kybernetické útoky i z jiných zařízení než jen z počítačů a zároveň lze páchat kybernetické útoky, při nichž jsou tato zařízení jejich předmětem. Dobrým příkladem tomu jsou chytré mobilní telefony, tablety a další nositelná, přenosná nebo pevně stojící chytrá zařízení. Klasické počítače postupně ustupují do pozadí a budoucnost je spatřována v přenosné elektronice kompaktní velikosti a nízké hmotnosti. Také proto byl v odborné literatuře pojem „počítač“ vystřídán pojmem „informační a komunikační technologie“.

Ať chceme, či nikoliv, informační a komunikační technologie jsou na vzestupu. Když se v roce 1926 uskutečnil v Londýně první přenos obrazu, nikdo nečekal, že se televizory stanou nedílnou součástí každé domácnosti. Když se první mobilní telefony pro veřejnost začaly objevovat v 50. letech 20. století jako vybavení automobilů, nikdo nepředpokládal, jak výkonná zařízení budou nosit po kapsách lidé v 21. století. Informační technologie jsou všude kolem nás. Stále častěji můžeme slyšet o chytrých hodinkách, reproduktorech, světlech, zásuvkách, ale také o chytrých pračkách, myčkách, sušičkách, ledničkách a tento seznam se neustále rozrůstá. Dnešní trendy udávají směr ovládat jakékoliv zařízení z jakéhokoliv místa na světě a veškerá data mít uložena na tzv. cloudových službách. Na jednu stranu se zdá být takový přístup správný. Uživatel může mít neustále k dispozici důležitá data, kontakty na důležité osoby nebo jen užívat automatické vyplňování formulářů v síti internetu. Možností je skutečně mnoho a autoři aplikací se předhánějí ve vývoji dalších a dalších služeb, ale za jakou cenu?

A právě v tento moment vstupuje na pomyslnou scénu kyberkriminalita, jejíž obětí se může stát dnes již prakticky kdokoliv a v širším pojetí také jakékoliv chytré zařízení. Nebezpečí je mnoho a jednotlivé případy poškozených se stále častěji objevují ve sdělovacích prostředcích a webových publikacích. U kyberkriminality obecně platí fakt, že pachatelé jsou stále sofistikovanější, vymýšlejí stále nové způsoby, jak se k zájmovým datům dostat a jakmile je jedno nebezpečí zažehnáno, objeví se vzápětí nové. Zřejmě nejvýznamnější roli hraje fakt, že v případě dostatečných znalostí, schopností a dovedností může být kyberkriminalita poměrně „bezpečnou" metodou, jak si zajistit finanční prostředky bez zbytečného rizika. Dlouho již neplatí, že se pachatele vloupání do rodinného domu nepodařilo orgánům činným v trestním řízení vypátrat. S vývojem informačních technologií došlo k výraznému posunu v oblasti zabezpečení, a ať již mluvíme o elektronickém zabezpečovacím systému nebo o pouhém systému kamer, dnes již nelze spáchat na veřejnosti téměř nic, co by se nedalo díky pokroku v technice nějakým způsobem vysledovat. A právě proto se u kyberkriminality bavíme o relativní bezpečnosti. Útočníka sedícího za počítačem na opačné straně země a ukrytého za pokročilým softwarem k utajení totožnosti již není tak snadné odhalit.

Fenomén kyberkriminality doprovází také vysoká míra latence, kdy poškození jen zřídka věc oznamují orgánům činným v trestním řízení. Důvodem k tomuto jednání může být stud ze strany poškozeného nebo nedůvěra v Policii České republiky. A není se čemu divit, kyberkriminalita má oproti jiným druhům kriminality jen velmi nízkou míru objasněnosti. I když se kybernetická kriminalita týká každého z nás, tato práce bude zaměřena na nejohroženější skupinu osob, a tou jsou právě děti. Ale co z této mladé generace osob činí tak snadné cíle? A v čem vlastně mladí lidé nejvíce chybují? Proč se stávají tak často obětmi kybernetických trestných činů? Také na tyto otázky se budeme snažit najít odpovědi v následujících kapitolách.

Toto téma diplomové práce jsem si vybral hned z několika důvodů. Předně jsem policista a v této základní složce IZS jsem začal působit před více než 18 lety. Za tuto dobu jsem prošel základním útvarem v rámci Policie České republiky Středočeského kraje a nyní působím na pozici policejního komisaře ve skupině kybernetické kriminality v teritoriálním území Praha západ. Při své činnosti jsem se již setkal s mnoha druhy kybernetických útoků, kdy za jedny z nejnebezpečnějších považuji útoky cílené na děti školou povinné. Je dokázáno, že s nástupem školní docházky dochází k formování osobnosti, rozšiřování znalostí a získávání všeobecného přehledu. A právě v této chvíli se děti poprvé setkávají s virtuálním světem, ve kterém se můžou stát kýmkoliv a dělat téměř cokoliv. Se světem, který nemá konec ani začátek, je návykový, líbivý, ale zároveň skýtá spoustu skrytých hrozeb. Mezi ohroženější věkovou skupinu však patří, z důvodu častějšího využívání informačních a komunikačních technologií, děti starší. Svou prací chci jednak dokázat fakt, že jsou děti na základních školách nedostatečně informovány o nástrahách kyberprostoru, a dále, že díky včasné informovanosti je možné snížit počet obětí kyberkriminality páchané na dětech. Z výše uvedených důvodů provádím besedy na druhém stupni základních škol ve Středočeském kraji a na základě prováděného výzkumu nastavuji besedu dle potřeb žáků. Následně se při besedách zaměřuji na zjištěné mezery v informovanosti a tyto se snažím zlepšit a přispět tak k ochraně této mladé generace osob.

2 CÍL PRÁCE A HYPOTÉZY

Teoretická část diplomové práce pojednává o rozsáhlé problematice kyberkriminality. Jsou v ní popisovány základní pojmy z oblasti informačních a komunikačních technologií a nejčastější projevy kyberkriminality se zaměřením na kyberšikanu, sexting, kyberstalking a kybergrooming.

Praktická část diplomové práce má za úkol zkoumat úroveň povědomí o kyberkriminalitě u dětí na vybraných základních školách ve Středočeském kraji, verifikovat nebo falzifikovat stanovené hypotézy a navrhnout opatření, jak kyberkriminalitě páchané na dětech v České republice předcházet. Prostředkem k dosažení těchto cílů je zvolena metoda sběru dat formou anonymních dotazníkových šetření. Na základě těchto šetření je realizována beseda, která má za úkol povědomí dětí zlepšit a současně se zaměřit na uvědomění si rizikového chování na síti internet. Přínos besedy je poté prověřen testováním proškolených subjektů. Účinnost besedy je dále vyhodnocena pomocí SWOT analýzy se zaměřením na rozdíly mezi městskými a venkovskými školami. V rámci problematiky budou uvedeny i případové studie. Celý projekt je koncipován v zájmu ochrany dítěte v rámci prevence Policie ČR.

2.1 Cíl práce

Pro naplnění účelu diplomové práce byl stanoven následující cíl:

Najít způsob, jak ochránit děti tam, kde selhává rodina, škola, stát. Učinit žáky základních škol odolnějšími vůči nástrahám kyberprostoru a docílit zvýšení gramotnosti v dané oblasti.

Za účelem splnění vytyčeného cíle byly stanoveny následující dílčí úkoly:

- Na základě podrobného studia knižních a internetových publikací přinést ucelený náhled do problematiky kyberkriminality;
- na základě získaných dat z dotazníkového šetření provést analýzu výsledků a následně realizovat besedu dle potřeb žáků základních škol;
- přínos besedy později opětovně prověřit testováním proškolených subjektů;
- účinnost besedy vyhodnotit pomocí SWOT analýzy se zaměřením na rozdíly mezi městskými a venkovskými školami;
- v rámci problematiky provést případové studie potvrzující zranitelnost žáků základních škol.

2.2 Hypotézy

V diplomové práci byly stanoveny následující hypotézy:

Hypotéza 1: *Úroveň povědomí o kyberkriminalitě u dětí na vybraných základních školách ve Středočeském kraji není na dostatečné úrovni.*

Hypotéza 2: *Nedostatečná informovanost žáků základních škol ve Středočeském kraji o kyberkriminalitě může mít za následek neopatrné jednání v síti internet.*

Hypotéza 3: *Je možné informovanost žáků základních škol ve Středočeském kraji o kyberkriminalitě zlepšit řízenou diskuzí ze strany příslušníka Policie ČR.*

Hypotéza 4: *Rozdíly v informovanosti žáků v městských a venkovských základních školách o kyberkriminalitě jsou minimální.*

3 PŘEHLED SOUČASNÉHO STAVU

Aby bylo možné hlouběji proniknout do problematiky kybernetické kriminality, je třeba si nejprve vymezit základní pojmy z oblasti informačních a komunikačních technologií. Do této části jsou rovněž zařazeny nejčastější projevy kyberkriminality se zaměřením na kyberšikanu, sexting, kyberstalking a kybergrooming.

3.1 Vymezení základních pojmů

3.1.1 Počítač

Kyberkriminalita bývá často nazývána kriminalitou počítačovou. Ale co je vlastně počítač? Pro tento pojem existuje celá řada definic:

„Za počítač je možné označit zařízení, které se vyznačuje následujícími rysy: zařízení obsahuje centrální procesorovou jednotku, schopnou řídit se programovým kódem a schopnou ovládat přidružené periferie a další části počítače; dále zařízení obsahuje médium pro ukládání dat (paměť, disk aj.). Mezi nepovinné prvky počítače se pak řadí zařízení pro vstup dat (klávesnice, myš aj.), zobrazovací zařízení (nejčastěji se jedná o monitor, ale může se jednat i o projektor či jiné zobrazovací zařízení) a jiné periferie“ (Havelka, 1997, s. 85).

„Počítačem je každá funkční jednotka schopná provádět výpočty a operace bez lidského zásahu a podle určitého programu, zařízení na zpracování, uchovávání a využívání dat, která převádí na číselné kódy“ (Kuchta, 2008, s. 224).

“V nejobecnějším smyslu lze za počítač považovat přístroj, který může být naprogramován za účelem samostatné realizace aritmetických a logických operací“ (Polčák, Púry, Harašta, 2015, s. 84).

Co se týče podoby dnešního počítače, tu zná jistě každý. Technologický pokrok však umožnil lidstvu vměstnat výkon a funkce dřívějšího počítače do zařízení mnohem menších rozměrů, jakým je dnes chytrý mobilní telefon

nebo tablet. Mezi další chytrou elektroniku můžeme dále řadit chladničky, pračky, sporáky, mikrovlnné trouby, chytrá auta a mnoho dalších. A ten stejný pokrok umožnil, že i tato zařízení mohou být terčem trestné činnosti. Také proto byl pojem „počítač“ vystřídán výrazem „informační a komunikační technologie“ neboli ICT (Kolouch, 2016).

3.1.2 Internet

Pojem internet není nutné v dnešní době představovat. Dějiny internetu jsou spojeny se vznikem počítače a jeho připojení do počítačových sítí. Jedná se o celosvětový systém propojených počítačových sítí, ve kterých mezi sebou počítače komunikují pomocí TCP/IP protokolů. Každý počítač připojený do sítě musí mít přidělenou vlastní IP adresu, která je v rámci dané sítě unikátní. IP adresa je přidělena danému systému staticky (manuálně) nebo dynamicky, kdy se o její přidělení stará (automaticky) DHCP server ve směrovači (routeru). IP adresa je unikátní soubor znaků a můžeme ji dělit na veřejnou (dostupnou z celé sítě internet) a neveřejnou (privátní), skrytou za veřejnou IP adresou zařízení poskytovatele internetu (Kolouch, 2016).

V rámci jedné sítě se tedy nemůžeme setkat se situací, kdy jsou připojena dvě zařízení se stejnou IP adresou. A to je jedna z mála výhod při objasňování kybernetické kriminality. Všeobecně totiž platí, že každá interakce v síti internet za sebou zanechává digitální otisk a tímto může být právě IP adresa přistupujícího uživatele. Vzniká pak digitální stopa, kterou autor Završnik charakterizuje jako soubor *„elektronických důkazů, bez nichž zpravidla kyberkriminalitu nelze vyšetřovat. Nejsou ovšem důležité pouze pro kyberkriminalitu, neboť se současně s digitalizací celé řady aktivit ve společnosti, která se pokládá za informační, stávají důležitými pro odhalování pachatelů a vyšetřování všech forem kriminality“* (Završnik, 2017, s. 64).

Je tedy zřejmé, že digitální stopou není jen IP adresa, ale soubor všech elektronických důkazů, které vznikají interakcí uživatele v kyberprostoru.

3.1.3 Webová stránka

Pojem webová stránka označuje to, co uvidí uživatel po zadání webové adresy do adresního řádku prohlížeče. Ovšem ke správné funkci webové stránky jsou nutné dvě věci. Je třeba vlastnit internetovou doménu a internetový hosting.

V předchozí kapitole byl vymezen jednoznačný identifikátor v síti, IP adresa. A protože internetovou doménou rozumíme taktéž jednoznačný identifikátor, i ona musí být v síti unikátní. Aby nebylo nutné pamatovat si IP počítače, ke kterému chceme v síti internet přistoupit, používají se doménová jména. Příkladem tomu může být server seznam.cz, který má IP adresu: 2a02:598:4444:1::2: Pro úplnost je třeba dále uvést, že se o překlad IP adresy na srozumitelná doménová jména stará DNS server a že se o správu domén CZ stará spol. Nic.cz

Internetovým hostingem (webhostingem) rozumíme prostor na cizím serveru pro webové stránky. Všechna data webové stránky se tedy nacházejí na internetovém hostingu poskytovatele.

Vytvořit webovou stránku není nikterak náročnou činností. Za tímto účelem existuje celá řada redakčních systémů pro nasazení vlastního řešení se znalostmi programování či mnoho online placených či neplacených služeb, které znalosti programování nepožadují. Vyžadují však umístění reklamy nebo hrazení nákladů spojených s provozem. V dnešní době tak může mít webové stránky opravdu každý a s minimálními náklady. Dále je třeba uvést, že není vyžadováno přímé ověření totožnosti osoby při nákupu domény ani hostingu, což se mnohdy negativně projevuje v případě odkrývání kybernetické kriminality.

3.1.4 Kyberprostor

Kyberprostor (angl. Cyberspace) představuje pomyslné místo v celosvětové síti internet, ve kterém se uživatel při jeho procházení pohybuje. Zároveň se jedná o klíčový prvek pro kybernetickou kriminalitu. Zjednodušeně by se dalo říct, že se jedná o virtuální svět tvořený informačními a komunikačními technologiemi, který nemá konec ani začátek. Kyberprostor je možné dělit na následující tři části:

- Viditelný a vyhledávači přístupný prostor pro běžné uživatele, nazývaný „Surface Web“ který zaujímá jen asi 4 % celého kyberprostoru;
- vyhledávači nedostupný prostor sloužící především pro firemní účely „Deep Web“;
- a jako poslední „Dark Web“, neboli prostor vytvořený především pro nezákonné účely, dostupný pouze na základě znalostí konkrétní adresy s nekontrolovatelnými a necenzurovatelnými daty (Kolouch, 2016).

Ale která z těchto částí je pro uživatele nebezpečnější? Je to část první, která je využívaná nejčastěji a kde se za anonymitou internetu může skrývat prakticky kdokoliv? Nebo část druhá, která sice není veřejnosti přístupná, ale velmi často obsahuje know-how firem, a tudíž skýtá příležitost pro průmyslovou špionáž? Anebo je to část třetí, která je sice bez znalostí konkrétní adresy nedostupná, ale skrývá prostor vytvořený přímo pro nelegální aktivity? Na toto téma lze vést sáhodlouhé diskuze a odpověď zřejmě nebude nikdy jednoznačná. V této práci se budeme věnovat části první neboli „Surface Webu“, části přístupné pro vyhledávače i uživatele. S touto částí kyberprostoru se setkávají již děti předškolního věku. Ať je to pouhé procházení obrázků nebo dívání se na pohádky, již v této době dochází k prvnímu kontaktu s virtuálním světem a nebezpečí se skýtá skutečně mnoho.

3.1.5 Kyberkriminalita

Kyberkriminalita je jednoznačně jedním z nejčastěji skloňovaných termínů dnešní doby. Tento pojem má obdobný charakter jako *„násilná kriminalita“*, *„kriminalita mladistvých“*, *„ekonomická kriminalita“ apod. Takovýmito názvy jsou označovány skupiny trestných činů mající určitý společný faktor, jako např. způsob provedení, osobu pachatele (alespoň druhově) apod. Ve své podstatě přitom může jít o velmi různorodou směsici trestných činů, spojených oním společným faktorem (počítačem, programem, daty)“* (Smekal, 2015, s. 19).

Na kybernetickou hrozbu reagoval i český právní systém. Nový trestní zákoník, č. 40/2009, zavedl s účinností od 1. ledna 2010 v oblasti trestního práva hmotného řadu zásadních změn. Tyto změny se dotkly již existujících skutkových podstat trestných činů a také došlo k zavedení skutkových podstat nových. Nové skutkové podstaty trestných činů, uvedené v hlavě páté pod ustanovením § 230 až § 232, přímo reagují na tuto problematiku jako na nový druh kriminality. Nový trestní zákoník tedy rozeznává trestné činy páchané ve vztahu k datům (uloženým informacím) a trestné činy páchané ve vztahu k datům (uloženým informacím), při nichž je počítač prostředkem k jejich páchání.

3.1.6 Kybernetický útok

Kybernetický útok (angl. Cyberattack) lze definovat jako určité protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné autority. Kybernetický útok tak může cílit jak na chyby v úsudku, kde hraje hlavní roli lidský faktor nebo přímo na informační a komunikační technologie, a to za účelem jejich „ovládnutí“. Jednání útočníka však pokaždé směřuje ke stejnému zájmu. Tímto zájmem je získání přístupu k počítačovému systému nebo jeho části za účelem způsobit poškození a získat citlivé či strategicky důležité informace (Jirásek, Novák, Požár, 2015).

3.1.7 Sociální inženýrství

Pojem sociální inženýrství je v odborné literatuře popsán jako „*způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace*“ (Jirásek, Novák, Požár, 2015, s. 107).

Sociální inženýrství nevyužívá technologická zařízení k prolamování hesel nebo k získávání tzv. „zadních vrátek“ k přístroji uživatele. Je založeno na zcela jiné strategii. Tou strategií je uvést uživatele v omyl a on poskytne cenná data sám. Pochopitelně není útočník ve většině případů úspěšný, avšak díky této neinvazivní metodě může oslovit mnohem více uživatelů. V případě sociálního inženýrství nepřichází útočník do osobního kontaktu s poškozenými a informační a komunikační zařízení se stává prostředkem k páchání jeho trestné činnosti. Sociální inženýrství je založeno na specifických způsobech lidského rozhodování a jeho účelem je přesvědčit uživatele k chybě úsudku. Zjednodušeně řečeno získat klamem informace, které by se jiným způsobem získat nepodařilo (Kolouch, 2016).

Na základě shora uvedených skutečností lze konstatovat několik faktů. Předně, internet je pro člověka pomocník a jeho pozitiva se prolínají do jeho soukromého i pracovního života. Existuje však také druhá strana této pomyslné mince. Jakákoliv data již jednou uložená v této celosvětové síti nelze odstranit pouhým jedním stiskem tlačítka na myši. Pokud se jednou objeví na internetu nějaká citlivá data, téměř okamžitě dochází k jejich šíření a prakticky tomu nelze zabránit. Život bez počítače, chytrého telefonu a další „důležité“ elektroniky si dnes již asi nikdo nedokáže představit. Bez těchto věcí by nemohla vzniknout celosvětová síť internet. Bez internetu by neexistoval kyberprostor. A bez tohoto by nemohla existovat kyberkriminalita. Kyberkriminalita je tak důsledek technologického pokroku lidstva a v současné době neexistují možnosti jejího úplného vymýcení.

3.1.8 Sociální sítě

Sociální sítě jsou jednoznačným fenoménem dnešní doby a zároveň se jedná o jeden z nejstěžejnějších prvků této práce. Dle provedeného výzkumu probíhá drtivá většina internetového provozu dětí na základních školách právě prostřednictvím sociálních sítí a jen málokdo si uvědomuje jejich nebezpečnost. Pojem sociální síť se do odborné literatury dostal až po roce 2004, kdy vznikla jedna z nejznámějších sociálních sítí, Facebook.

Autoři Jirásek, Novák, Požár vnímají tento pojem v novodobé publikaci jako: *„propojenou skupinu lidí, kteří se navzájem ovlivňují. Tvoří se na základě zájmů, rodinných vazeb nebo z jiných důvodů. Tento pojem se dnes také často používá ve spojení s internetem a nástupem webů, které se na vytváření sociálních sítí přímo zaměřují (Facebook, Lidé.cz apod.), sociální sítě se mohou vytvářet také v zájmových komunitách kolem určitých webů, například na jejich fórech*“ (Jirásek, Novák, Požár, 2015, s. 107).

Zjednodušeně by se dalo říct, že jde hlavně o spojení lidí a sdílení dat. Ovšem k tomuto dochází prostřednictvím sítě internet a lidé se mnohdy osobně vůbec neznají. Když se k tomuto faktu přičte ještě naivita a důvěřivost dětí, stává se ze sociálních sítí v rukou útočníka účinná zbraň 21. století.

Podle tiskové zprávy Českého statistického úřadu z 19. listopadu 2018 již využívá sociální sítě více než 50 % osob v ČR. Vyjádření Českého statistického úřadu: *„Počet Čechů, kteří používají sociální sítě, letos překročil 50% hranici.*

V absolutních počtech to je 4,5 milionu osob starších 16 let. Sociální sítě však neoslovují Čechy v předdůchodovém a důchodovém věku. Každý druhý Čech také na internetu sleduje videa, nejvíce k tomu používá stránky typu YouTube (44 %)“ (ČSÚ, ©2018).

3.2 Nejčastější projevy kyberkriminality

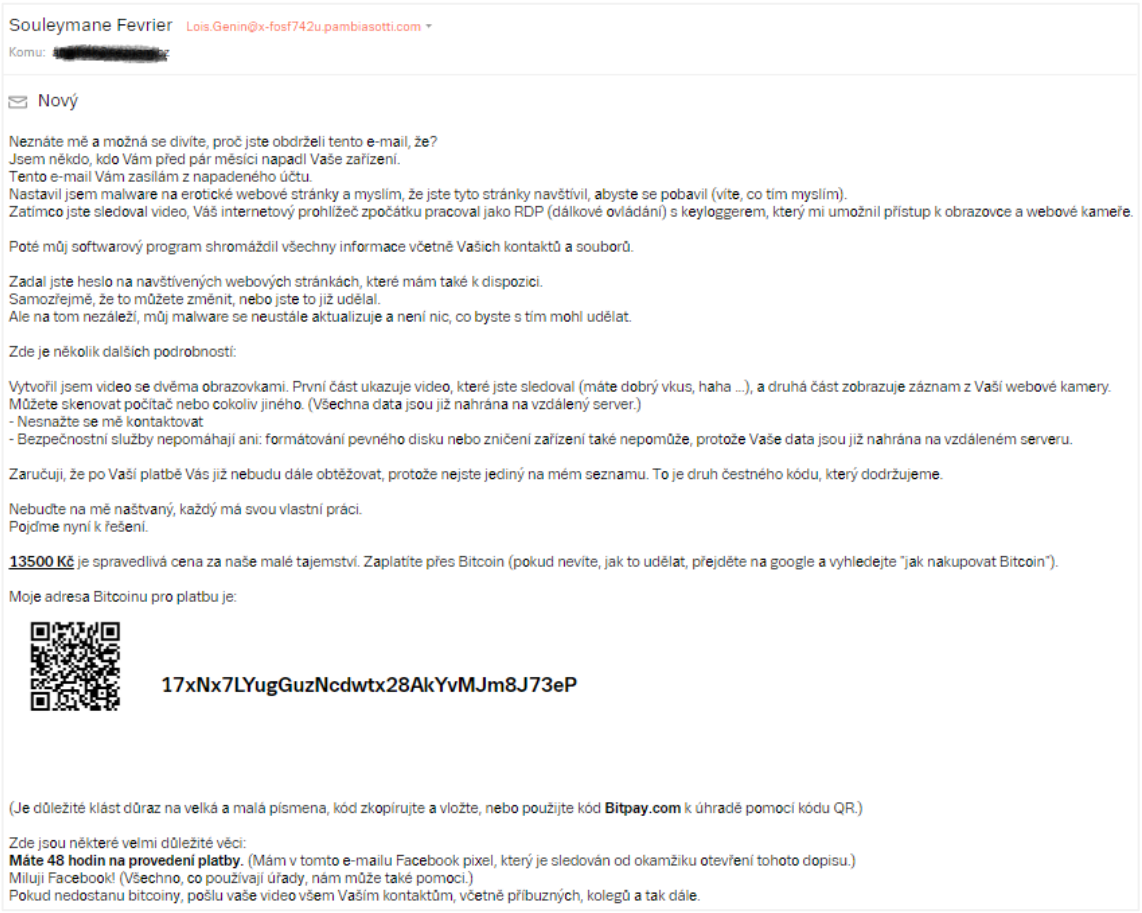
V předchozí kapitole byly vymezeny základní a nejdůležitější pojmy z oblasti informačních a komunikačních technologií pro tuto práci. Tato část je zaměřena na nejčastější projevy kybernetické kriminality, které nás budou provázet i v následující výzkumné části.

3.2.1 Phishing

Phishing (známý zejména pod slovem rhybaření nebo nesprávně rybaření) je jednou z nejrozšířenějších podvodných technik, užívaných za účelem získání citlivých údajů a dat prostřednictvím celosvětové sítě internet. S phishingem se nejčastěji setkáváme u podvodných emailů, které nabádají uživatele ke změně hesla nebo přihlášení se do nějaké z online služeb. Email se na první pohled tváří seriózně, ale po kliknutí na odkaz v emailu je uživatel přesměrován na webovou stránku s jinou internetovou doménou. Pokud si uživatel nevšimne adresního řádku v počítači, může zadáním přihlašovacích údajů do dané služby poskytnout útočníkovi přístup ke svým datům (Kolouch, 2016).

Výskyt phishingových útoků je v dnešní době jedním z nejčastějších útoků vůbec. Útočníci se snaží cílit na málo obezřetnou skupinu obyvatel a za pomoci lstí vylákat z člověka finanční prostředky nebo zájmová data. Typickým příkladem phishingových útoků jsou situace, kdy muž, vydávající se za vysoce postaveného důstojníka americké armády, osloví ženu za účelem dopisování. Komunikace probíhá standardním způsobem do doby, než útočník získá důvěru oběti. V této chvíli poprosí o půjčení malého obnosu peněz pro svou dceru nebo syna na studium. Ve většině případů poškození zašlou útočníkovi částku opakovaně a nikdy se nedočkají jejího vrácení. Komunikace probíhá ve většině případů formou překladu z Google překladače a obětí stejného podvodného profilu uživatele bývá více.

S obdobným útokem jsem se setkal již také. Konkrétně mi byla doručena do emailové schrány od poskytovatele seznam.cz zpráva následujícího znění:



Souleymane Fevrier Lois.Genin@x-fosf742u.pambiasotti.com

Komu: [redacted]

Nový

Neznáte mě a možná se divíte, proč jste obdrželi tento e-mail, že?
Jsem někdo, kdo Vám před pár měsíci napadl Vaše zařízení.
Tento e-mail Vám zasílám z napadeného účtu.
Nastavil jsem malware na erotické webové stránky a myslím, že jste tyto stránky navštívil, abyste se pobavil (víte, co tím myslím).
Zatímco jste sledoval video, Váš internetový prohlížeč zpočátku pracoval jako RDP (dálkové ovládání) s keyloggerem, který mi umožnil přístup k obrazovce a webové kameře.

Poté můj softwarový program shromáždil všechny informace včetně Vašich kontaktů a souborů.

Zadal jste heslo na navštívených webových stránkách, které mám také k dispozici.
Samozřejmě, že to můžete změnit, nebo jste to již udělal.
Ale na tom nezáleží, můj malware se neustále aktualizuje a není nic, co byste s tím mohl udělat.

Zde je několik dalších podrobností:

Vytvořil jsem video se dvěma obrazovkami. První část ukazuje video, které jste sledoval (máte dobrý vkus, haha ...), a druhá část zobrazuje záznam z Vaší webové kamery.
Můžete skenovat počítač nebo cokoliv jiného. (Všechna data jsou již nahrána na vzdálený server.)
- Nesnažte se mě kontaktovat
- Bezpečnostní služby nepomáhají ani: formátování pevného disku nebo zničení zařízení také nepomůže, protože Vaše data jsou již nahrána na vzdáleném serveru.

Zaručuji, že po Vaší platbě Vás již nebudu dále obtěžovat, protože nejste jediný na mém seznamu. To je druh čestného kódu, který dodržujeme.

Nebuďte na mě naštvaný, každý má svou vlastní práci.
Pojďme nyní k řešení.

13500 Kč je spravedlivá cena za naše malé tajemství. Zaplatíte přes Bitcoin (pokud nevíte, jak to udělat, přejděte na google a vyhledejte "jak nakupovat Bitcoin").

Moje adresa Bitcoinu pro platbu je:

17xNx7LYugGuzNcdwtx28AkYvMJm8J73eP

(Je důležité klást důraz na velká a malá písmena, kód zkopírujte a vložte, nebo použijte kód **Bitpay.com** k úhradě pomocí kódu QR.)

Zde jsou některé velmi důležité věci:
Máte 48 hodin na provedení platby. (Mám v tomto e-mailu Facebook pixel, který je sledován od okamžiku otevření tohoto dopisu.)
Miluji Facebook! (Všechno, co používají úřady, nám může také pomoci.)
Pokud nedostanu bitcoiny, pošlu vaše video všem Vašim kontaktům, včetně příbuzných, kolegů a tak dále.

Obrázek 1 - Doručený email od spol. seznam.cz

Tento phishingový útok je však ještě specifičtější. Mimo svůj hlavní účel, kdy jde o to uvést uživatele v omyl, obsahuje další prvek navíc. Tím prvkem je výhrůžka s výstrahou, že pokud nebude platba uhrazena, dojde k rozeslání videa na sociální sítě. V uvedeném případě se jednalo pouze o planý poplach, neboť útočník nevytvářel žádný specifický software ani nedisponoval inkriminovaným videem, ale i přesto v několika případech k uhrazení „výpalného“ docházelo.

Při své dlouholeté praxi jsem se již setkal s phishingovými útoky i na základních školách. V těchto případech nejde primárně o získání finančních prostředků, neboť těmito obvykle děti nedisponují. Jde o útoky za účelem

získání zájmových dat, kterými jsou lechtivé fotografie či videa a jiná data s nimi spojená.

3.2.2 Malware

V odborné literatuře je pojem malware vnímán jako „*obecný název pro škodlivé programy. Mezi škodlivý software patří počítačové viry, trojské koně, červy, špionážní software.*“ (Jirásek, Novák, Požár, 2015, s. 115).

Je třeba si uvědomit, že se tvůrcem škodlivého software nemůže stát každý. Na rozdíl od Phishigu je třeba mít určité znalosti z oblasti programování. Ovšem i tento projev kyberkriminality je velice rozšířený. Všeobecně stačí uvést uživatele v omyl, nabídnout mu software k nápravě domnělého stavu a poté již útočníkovi nic nebrání ve vzdálené interakci na dotčeném zařízení. Základnou pro malwarové útoky býval v dřívější době operační systém Windows. Díky pokroku v informačních a komunikačních technologiích se dnes nejčastěji cílí na chytrá zařízení (mobilní telefony, tablety). Předmětem útoku bývají zpravidla přístupové údaje do internetových bankovnictví, multimédia a osobní informace. Do skupiny malware se řadí i tzv. „vyděračský software“ ransomware.

3.2.3 Ransomware

Jedná se o škodlivý software, který zašifruje data a nabízí jejich rozšifrování po zaplacení výkupného (z anglického „ransom“ – výkupné). Ransomware se nejčastěji objevuje ve firmách, obecních nebo městských úřadech, školách a dalších institucích, kde ztráta dat může napáchat velké škody. Tento software se dostává do počítačů interakcí uživatele. Bývá umístěn na webových stránkách nebo je součástí příloh emailu. Tento škodlivý software provádí zašifrování obsahu pevného disku a vyžaduje zaplacení určité částky (nejčastěji ve virtuální měně) s odkazem, že po uhrazení dojde k obnově dat. Po zaplacení požadované částky však k obnově dat nedochází (Kolouch, 2016).

I když není malware a ransomware nejčastějším problémem žáků základních škol, jde o velmi důležitý mezník. Již při seznamování se s kyberprostorem by měli mít lidé informace o nebezpečnosti instalování neznámých aplikací a otevírání příloh od neznámých odesílatelů. Pokud dodržuje uživatel internetu určitá pravidla bezpečnosti, jsou nebezpečí jeho viktimizace (neboli procesu, v němž se člověk stává obětí trestného činu) značně minimalizována.

3.2.4 Spam

Pojem spam (spamming) není třeba dlouze představovat, neboť jej zná jistě každý. V odborné literatuře je spamming vnímán jako „*Hromadné rozesílání nevyžádaných zpráv elektronickými prostředky – nejčastěji elektronickou poštou*“ (Jirásek, Novák, Požár, 2015, s. 115).

Autor Kolouch ve své publikaci poukazuje na fakt, že lze pojem spam chápat ve dvou rovinách. V užším slova smyslu se jedná o hromadné šíření nevyžádaného sdělení, v širším slova smyslu jde o všechny nevyžádané zprávy, včetně zpráv obsahující viry, trojské koně apod. (Kolouch, 2016).

Spam ke svému šíření využívá různých komunikačních kanálů informačních a komunikačních technologií. Nejčastěji dochází k šíření spamu prostřednictvím emailu, nějakého z messengerů (Skype, WhatsApp, apod.) nebo SMS zpráv. Obsahem takového spamu bývají obchodní či reklamní sdělení, nabídky z oblasti finančnictví, zdravotnictví nebo nevyžádaná sdělení typu Hoax, Clickbait apod.

Vzhledem k rozšířenosti výše zmíněných informačních kanálů i mezi žáky základních škol, týká se škodlivost spamu také jich.

3.2.5 Podvodné webové stránky

V souvislosti s neustálou bdělostí v síti internet bych se rád stručně zmínil také o podvodných webových stránkách. Vzhledem k dostupnosti a snadné

realizaci vlastních webových stránek viz kapitola *Webová stránka*, jsou i tyto zneužívány pro trestnou činnost. Proto je třeba dodržovat následující pravidla:

- vždy kontrolovat adresní řádek v prohlížeči
- nevěřit všemu, co se na internetu nachází.

V případě podvodných webových stránek pachatelé cílí na nepozornost uživatele. Uživatelé jsou obvykle prostřednictvím emailu nabádáni ke změně hesla internetového bankovnictví nebo k jiné bankovní operaci. Pokud je uživatel nepozorný, může vložit svá citlivá data na úplně jinou webovou stránku místo na oficiální web bankovního domu. A to, že jsou už i někteří žáci základních škol uživateli platebních karet vyplývá také z provedeného výzkumu. V druhém případě jde o webové stránky s tzv. Hoax zprávami, Clickbait a podvodnými nabídkami viz níže.

3.2.6 Scam

Jako Scam jsou hromadně označována jednání, kdy pachatel uvede prostřednictvím informačních a komunikačních technologií v omyl jiného za účelem výdělku. Jde o zajímavou ukázku toho, kdy je klasický podvod převeden do virtuálního prostředí. Tento výraz je znám také jako Nigerijské dopisy nebo podvody. Autor Završnik tento výraz vnímá následovně: „*Nigerijské podvody („podvody 419“), které od uživatele vyžadují zálohu (členství), po jejímž složení má údajně následovat poukázání obří sumy peněz. Nigerijské dopisy nejsou zvlášť důmyslné svým mechanismem a teorie je řadí k zálohovým schématům. Typickým příkladem je e-mail, v němž je uživateli lámanou angličtinou oznámeno, že mu zámožný strýc (o němž ještě neslyšel) odkázal miliony dolarů v podobě zlatých prutů, k jejichž získání je nutné nejprve uhradit poměrně malou zálohu*“ (Završnik, 2017, s. 48).

3.2.7 Hoax (Fakenews)

Tímto termínem jsou označovány řetězové poplašné, nepravdivé, falešné, zkreslené, zavádějící nebo jinak šokující zprávy typu „*pošli to dalším 10 lidem nebo se to stane i tobě*“. Jde o jednu z podob Scamu a nejrozšířenější Hoaxy je možné nalézt například na webových stránkách http://www.hoax.cz/cze/ (Kolouch, 2016).

Aktuálně nejrozšířenější hoaxy z výše uvedeného webu:

- Slovenčina – nejtěžší jazyk na světě
- Whatsapp Gold – Martinelli
- Nebezpečný moderní jogurt
- Kdo vede vlčí smečku
- INVITATION - Olympijská pochodeň
- LIDL rozdává bezplatnou kartu k 88. výročí
- Krev pro dítě s leukémií B-Rh - únor 2019
- Zpoplatnění WhatsApp
- SMS MAGNA děti v nouzi
- Microsoft rozdává peníze

3.2.8 Clickbait

Tímto termínem jsou označovány návody na kliknutí na příspěvky s často šokujícími názvy. Základnou k šíření těchto zpráv jsou sociální sítě a autorovi takového příspěvku jde o co největší počet oslovených uživatelů v co možná nejkratší době. Čím víc šokující zpráva, tím více kliknutí a tím více odměny ve formě finančních prostředků z reklamy. Typickým příkladem toho je webová stránka tynavody.cz, která se tváří jako lifestylový magazín. Minimum textu, žádné zdroje, mnoho reklam, líbivé až šokující nadpisy článků a rozřešení na další stránce. I takto by se dala shrnout zmíněná webová stránka. Posledních 5 příspěvků ke dni 18.10.2019 z webu tynavody.cz:

- Jaký máte tvar prstu? A co to o Vás prozrazuje?
- Jak zjistit, že Vás podvádí? Tyto znaky všechny odhalí.
- Několik fotografií z historie, které ve Vás vyvolají strach.
- Jen jeden šálek denně tohoto nápoje před spaním a zbavíte se tuku nadobro.
- Hlavní důvody toho, proč by děti neměly používat mobily.

A obdobných webových stránek je více. Důvodem, proč byla pro názornost zvolena právě tato webová stránka, je aktuální četnost příspěvků na sociálních stránkách a dále jistá míra sofistikovanosti ze strany majitele. Úskalí spojená s majitelem doménového jména byla již zmíněna v kapitole *Webová stránka*. V tomto případě jde však o jinou situaci. Ve verzi internetového prohlížeče pro stolní počítače jsou reklamy zakázané. Ve verzi internetového prohlížeče pro mobilní zařízení jsou naopak jen stěží počitatelné. Ale proč? Důvod je zřejmý. Autor se s největší pravděpodobností obává o svůj účet na serveru poskytujícím reklamy. Rozzlobený uživatel by totiž snadno mohl, za pomoci automatických nástrojů, jeho reklamní účet ohrozit falešnými kliky. Ale v případě mobilního zařízení už to tak snadné není. Dále je nutné poznamenat, že tyto webové stránky nejsou jen „nositelem“ reklam, ale mohou také obsahovat škodlivé kódy typu malware. Je tedy nezbytné informovat i o této hrozbě.

Společenská škodlivost tohoto projevu kyberkriminality je poměrně nízká. Nedochází k cílení na informační nebo komunikační technologie ani na data v nich uložená. Avšak rozhodně nejde o praktiky správné a můžeme se jen domnívat, zda autor příspěvků ví, na jakou skupinu obyvatel ve skutečnosti cílí. Pokud bych měl provést rekapitulaci, základnou pro šíření těchto zpráv jsou jednoznačně sociální sítě. A podle výzkumu ČSU z roku 2018 je 4,5 milionu osob starších 16 let uživateli sociálních sítí. Webové stánky s tímto obsahem proto stále existují a zřejmě i nadále existovat budou. A jaká skupina

osob sdílí na sociálních sítí každou zajímavou až šokující zprávu? Jednoznačně děti bez životních zkušeností a s dosud trochu zkresleným pohledem na svět.

3.2.9 Podvodné nabídky

Velmi častým projevem kyberkriminality na internetu jsou také podvodné nabídky. Jedná se o velmi úspěšnou formou scamu, kdy tyto nabídky našel ve své emailové schránce jistě již každý. Nejčastěji jde o *„princip tzv. „pyramidy" či „letadlo". Jde o nabídky výhodných prací z domova, „zaručené" metody zhodnocení peněz (s nejvyššími úroky), nabídky na půjčku (s nejnižšími úroky), „skvělé" pracovní příležitosti aj*" (Kolouch, 2016, s. 240).

Uživatelé, kteří se k podobné nabídce přihlásí, jsou povinni zaplatit „mírný" poplatek pro zařazení do slibovaného programu. Po zaplacení této částky však logicky k předání slibované „zaručené" metody či sdělení „skvělé" pracovní příležitosti nedochází.

Závěrem je třeba uvést, že je internet bezesporu velkým pomocníkem, ale nelze věřit striktně všemu, co se zde nachází. Ať se jedná o dospělého člověka nebo o dítě, je vždy třeba zkoumat také zdroj informace, a hlavně zachovávat jistá pravidla bezpečného chování.

3.2.10 Kyberšikana

Je jedním z nejdiskutovanějších témat na základních školách. Jedná se o velmi rozšířený jev moderní doby a již se jí věnovalo několik význačných studií. V dnešní době konečně dochází k její prevenci i ze strany učitelů na základních školách.

Aby bylo možné blíže vymezit kyberšikanu, je třeba nejprve přiblížit pojem šikany „běžné". Šikana spočívá v chování, jehož záměrem je opakovaně ubližovat jinému člověku, zahrnuje jak fyzický útok, tak i útok slovní, který může vyústit až k vyhrožování či vydírání. Většina případů šikany se odehrává ve škole, na cestě do školy nebo ze školy. Nebezpečí jednání spočívá

v dlouhodobém trýznění, což má negativní vliv na správný duševní a fyzický vývoj dítěte (PČR, ©2019).

U kyberšikany je tomu obdobně, avšak veškeré útoky probíhají prostřednictvím informačních a komunikačních technologií: „*Druh šikany, který využívá elektronické prostředky, jako jsou mobilní telefony, e-maily, pagery, internet, blogy a podobně k zasílání obtěžujících, urážejících či útočných mailů a SMS, vytváření stránek a blogů dehonestujících vybrané jedince nebo skupiny lidí*“ (Jirásek, Novák, Požár, 2015, s. 85).

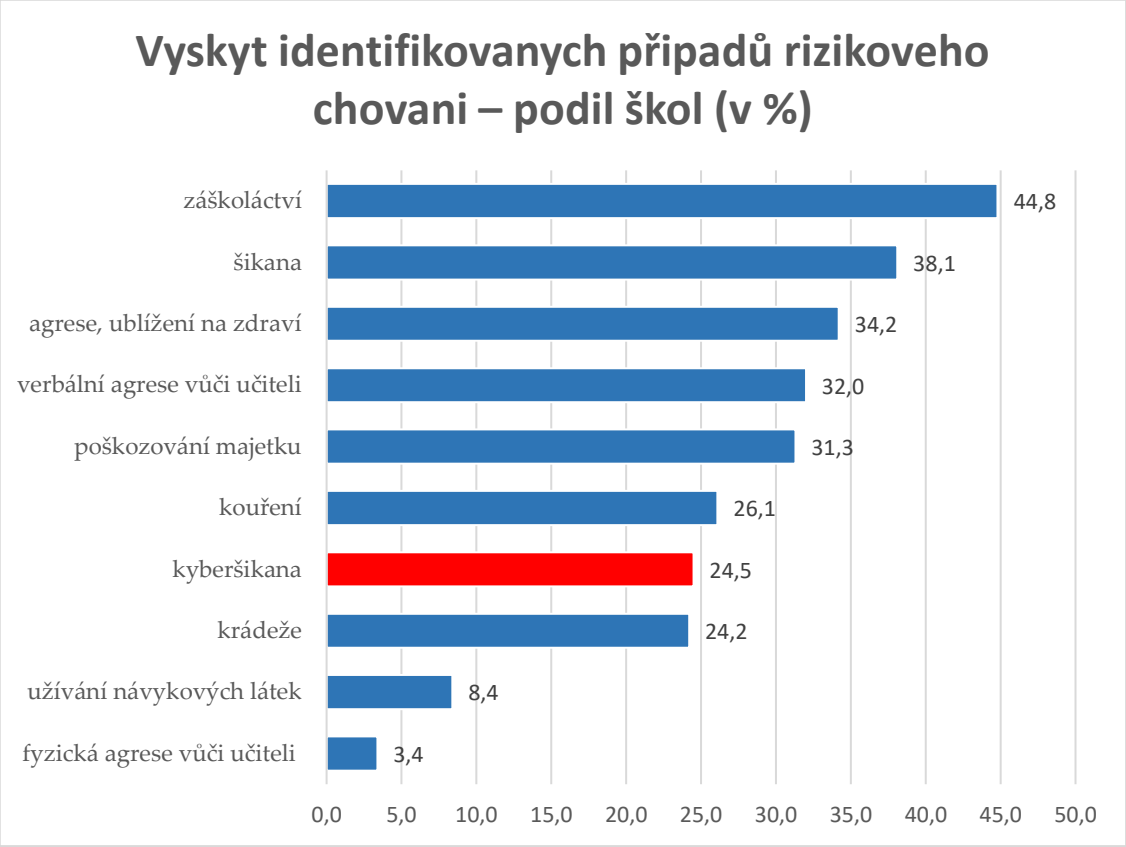
Klasickým následkem kybešikany je nízké sebevědomí, zhoršení školního prospěchu, ztráta přátel, samotářské chování a další. Na rozdíl od šikany „běžné“ existuje u kyberšikany jeden zásadní rozdíl. Tímto rozdílem je délka trvání trýznivého chování. Běžné formy šikany trvají obvykle několik minut, a i když si jejich následek odnáší oběť v sobě jako trauma, šikana končí v bezpečí domova, o školní vyučování a celkově za dohledu dospělých. Kyberšikana trvá podstatně déle, ponižující příspěvky, fotografie nebo i videa mohou na sociálních sítích a jiných webových stránkách zůstat k pobavení ostatních i několik měsíců. Takto postižené osoby obvykle o problému nechtějí mluvit a v ojedinělých případech za to mohou zaplatit i cenu nejvyšší.

Ukázkovým příkladem toho byla dvanáctiletá dívka Amanda Todd z Kanady, která se nechala na chatu přesvědčit od neznámé osoby k vyfotografování a zaslání svých obnažených ňader. Zhruba o rok později byla Amanda opět kontaktována neznámou osobou s žádostí o další fotografie. Amanda omítla a její fotografie s obnaženými ňadry byla poté vystavena jako profilová fotografie na sociální síti Facebook. Bohužel tato fotografie započala nekončící šikanu a Amanda spáchala, po dlouhém trápení, v patnácti letech sebevraždu (BBC, ©2019).

Podobně smutných případů je více, ale Amanda Todd je zřejmě neznámějším případem. Ne vždy je chyba ze strany poškozeného vykoupena cenou nejvyšší,

ale minimálně traumatem na celý život určitě ano. Z pohledu trestního zákoníku č. 40/2009 Sb. (dále jen TZ) může svým jednáním pachatel shora uvedeného jednání naplnit skutkovou podstatu trestných činů: Ublížení na zdraví dle ustanovení § 146 (v případě fyzické újmy), Těžkého ublížení na zdraví dle ustanovení § 145 (v případě těžké újmy na zdraví), Vydírání dle ustanovení § 175 (v případě nucení něco konat pod pohrůžkou násilí) a Nebezpečného pronásledování dle ustanovení § 354 (v případě obtěžování a pronásledování).

Že se v případě kyberšikany jedná o aktuální téma hovoří i Výroční zpráva České školní inspekce České republiky, která v roce 2018 zveřejnila následující statistiky na svých webových stránkách csicr.cz:



Obrázek 2 - Výroční zpráva České školní inspekce 2017/2018 str. 73

Z výše uvedených dat je zřetelné, že ve školním roce 2016/2017 doznala kyberšikana téměř 25 % identifikovaných případů, což již není zanedbatelná hodnota a dělá to z kyberšikany nový trend dnešní doby.

Česká školní inspekce České republiky provedla také meziroční srovnání identifikovaných případů rizikového chování žáků – podíl škol (v %), kdy zveřejněné výsledky můžeme pozorovat na následující tabulce:

Tabulka 1 - Výroční zpráva České školní inspekce 2017/2018 str. 73

Druh rizikového chování žáků	2013-2014	2014-2015	2015-2016	2016-2017
fyzická agrese vůči učiteli	2,4	3,4	6,2	3,4
užívání návykových látek	9,4	8,2	10,8	8,4
krádeže	21,3	26,3	24,6	24,2
kyberšikana	13,9	23	20,5	24,5
kouření	23,2	22,6	25	26,1
poškozování majetku	27	33,2	30,9	31,3
verbální agrese vůči učiteli	26,4	32,9	33,1	32
agrese, ublížení na zdraví	27,9	33,7	32,9	34,2
šikana	30,3	41	35,5	38,1
záškoláctví	39,1	45,7	43,5	44,8

Z uvedené tabulky je patrné, že vyjma roku 2015 – 2016 dochází k meziročnímu růstu kyberšikany v řádech několika jednotek procent. Když vezmeme v potaz rok 2013 – 2014 a provedeme porovnání s rokem 2016 – 2017, jedná se již o nárůst o 10,6 %, a to již rozhodně není zanedbatelná hodnota. Byť mohou být výsledky zkreslené vysokou latencí, jsou alarmující.

Více než doporučeným postupem v případě kyberšikany u dítěte je věc oznámit dospělé osobě. A i kdyby se jednalo pouze o osobu ze strany učitelského sboru, tato bude vždy lépe vědět, jaké stanovisko zaujmout.

V době dokončování této práce byla ze strany České školní inspekce České republiky vydána nová Výroční zpráva České školní inspekce 2018/2019, kde je na str. 72 patrný nárůst kyberšikany ve školním roce 2017-2018 na 29,9 %. Potvrzuje se tedy předpoklad každoročního růstu tohoto projevu kyberkriminality.

3.2.11 Sexting

Tento pojem bych osobně nezařadil přímo do projevů kyberkriminality, ale do závadového jednání s ní spojeného. Výraz vznikl ze slov „sex“ a „text“ a jedná se o zasílání zpráv se sexuálním obsahem prostřednictvím informačních a komunikačních technologií. Tyto materiály obvykle vznikají v rámci partnerských vztahů a představují riziko v případě, kdy jeden z partnerů fotografie či videa svého partnera zveřejní (Jirásek, Novák, Požár, 2015).

Tyto materiály však vznikají i mimo partnerské vztahy. Provedeným výzkumem bylo zjištěno, že 4,9 % z dotazovaných respondentů na základních školách zaslalo někomu, byť jen zčásti, svou obnaženou fotografii. A v některých případech není třeba chodit žákům ani do soukromí. Na svých sociálních sítích své spoře oděné fotografie vystavují sami a zcela dobrovolně. Nabízí se tak příležitost ze strany pachatele tyto děti oslovit, získat si jejich důvěru a tyto materiály pod různými záminkami a přísliby vylákat.

Závažnost takového jednání sice není tak vysoká, jako v případě kyberšikany, ale způsobený následek může být mnohdy ještě vyšší. Zveřejnění takové fotografie či videa na internetu bývají Policií ČR kvalifikována jako přestupková jednání. V některých případech, kdy je poškozená osoba nucena něco konat, lze skutek kvalifikovat také jako trestný čin Vydírání dle ustanovení § 175 TZ.

Avšak potrestání osoby, která tyto materiály zveřejnila, není zcela jistě úměrné vzniklé újmě poškozeného. Na začátku jde „pouze“ o jednu hloupou obnaženou fotografii, na konci může být trauma na celý život. Fotografie putující po sociálních sítích, známých, školách, zaměstnáních systematicky boří veškerá získaná postavení, hodnoty a ničí vytyčené cíle. I v tomto případě je vhodné odvolat se na případ kanadské dívky Amandy Todd, která za jednu obnaženou fotografii zaplatila cenu nejvyšší. V případě takové fotografie v síti internet můžeme hovořit nejen o viktimizaci primární (újmě způsobené

bezprostředně jako důsledek spáchané trestné činnosti), ale také o viktimizaci terciální (dlouhodobé dopady újmy dříve postižené oběti).

Vzhledem k závažnosti jednání vzniklo také několik projektů určených k prevenci. Jedním z nich je webová stránka sexting.cz, která obsahuje ucelené informace od pojmu počínaje, prevencí konče. Tato webová stránka se dále odkazuje na projekt Centra prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci z roku 2012, kdy bylo zjištěno, že sexting v ČR realizuje cca 7-9 % populace dětí. A 7,23 % dětí na internet v roce 2012 umístilo svou "sexy" fotografii nebo video, byť obnažené jen z části. A jak tomu bude asi o 10 let později, kdy jsou informační a komunikační technologie na vzestupu? I na tuto otázku se budu v následující části snažit najít odpověď. Technologie v posledních letech doznaly výrazných změn. Vcelku kvalitní fotoaparát je nyní součástí každého mobilního telefonu nebo tabletu a bude zajímavé sledovat, jak se děti na základních školách staví k problematice zvané sexting.

Také v tomto případě je doporučeným postupem věc oznámit dospělé osobě. A opět, i kdyby se jednalo pouze o osobu ze strany učitelského sboru, tato bude vždy lépe vědět jaké stanovisko zaujmout.

3.2.12 Kyberstalking

Aby bylo možné vymezit termín kyberstalking, je nutné nejprve přiblížit termín stalking. Tento termín má synonymum v ustanovení § 354 TZ jako Nebezpečné pronásledování. Toto ustanovení je charakterizováno prof. Šámalem následovně:

„Kdo jiného dlouhodobě pronásleduje tím, že

- *vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým,*
- *vyhledává jeho osobní blízkost nebo jej sleduje,*

- *vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje,*
- *omezuje jej v jeho obvyklém způsobu života, nebo*
- *zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu,*

a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti" (Šámal, 2012, s. 3290-3302).

Obdobně, jako tomu bylo u kyberšikany, i v případě kyberstalkingu dochází k výše popsanému závadovému jednání prostřednictvím informačních a komunikačních technologií. Mezi formy kyberstalkingu řadíme zasílání zpráv, e-mailů, telefonáty a prozvánění, opakované komentování příspěvků oběti na sociálních sítích, kontaktování oběti pod falešnou identitou atd. Motivem tohoto závadového jednání může být snaha poškodit oběť před společností, opětovné navazování vztahu po odmítnutí, vydírání oběti atd. K naplnění skutkové podstaty trestného činu Nebezpečného pronásledování je dále třeba vzbudit důvodnou obavu o život, zdraví poškozeného nebo jemu blízkých osob, a to bez ohledu na to, zda k pronásledování dochází prostřednictvím informačních a komunikačních technologií či nikoliv.

Kyberstalking bych osobně mezi nejzávažnější projevy kybernetické kriminality na základních školách neřadil. Dochází k němu jak u dospělých, tak svou mírnější formu najdeme i zde. O mírnější formě hovořím proto, že v případě dětí se jednání omezuje pouze na pronásledování v kyberprostoru. Dle autorky Čírtkové je telefonování obětem známo v 85 % případech, zasílání SMS v 47 % a zasílání e-mailů v 35 %. Poté již pachatel přechází z kyberprostoru a k ničení majetku dochází v 26 %, a dokonce ke vniknutí do bytu oběti dochází v 18 % (Čírtková, 2008).

I přesto může mít intenzivní forma Kyberstalkingu za následek nesprávný psychický nebo fyzický vývoj dítěte. Ze strany dítěte dochází k nestandardnímu

chování, zhoršení prospěchu, vyhýbání se společnosti apod. I v tomto případě je více než doporučené jednání věc oznámit minimálně pedagogovi základní školy, který bude vědět vždy nejlépe, jaké opatření přijmout.

3.2.13 Kybergrooming

Autoři Jirásek, Novák, Požár charakterizují tento pojem jako: „*chování uživatelů internetových komunikačních prostředků (chat, ICQ atd.), kteří se snaží získat důvěru dítěte a s cílem ho zneužít (zejm. sexuálně) či zneužít k nelegálním aktivitám*“ (Jirásek, Novák, Požár, 2015, s. 115).

Jedná se o psychickou manipulaci dítěte dospělým prostřednictvím informačních a komunikačních technologií s cílem získat důvěru oběti, vylákat ji na osobní schůzku a zpravidla sexuálně zneužít. Jedná se o trestní jednání, které je uvedeno v ustanovení § 193b TZ jako Navazování nedovolených kontaktů s dítětem. Toto ustanovení je charakterizováno následovně: „*Kdo navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, 193, § 202 odst. 2 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta*“.

Ze strany pachatele dochází k prvnímu kontaktu s dětmi nejčastěji prostřednictvím instant messengerů (Facebook Messenger, Skype), sociálních sítí (Instagram, Facebook, Twitter, …) a nejčastějšími obětmi jsou dívky trpící nedostatkem sebedůvěry a pocitem osamění. Průběh celého jednání je vždy obdobný. Nejprve dochází k získání důvěry a snaze izolovat oběť od okolí a přátel. Posléze dochází ze strany útočníka k získání osobních materiálů k případnému vydírání a poté k osobní schůzce se sexuálním podtextem. V některých případech může vzniknout i emocionální závislost oběti na útočníkovi.

Toto jednání lze jednoznačně zařadit mezi nezávažnější formy kyberkriminality vůbec a za svou více než desetiletou praxi u Služby kriminální policie a vyšetřování jsem se s tímto případem nesetkal. Důvodem bude zřejmě

také vysoká míra latence, kdy poškození (dívky i chlapci) se ze studu nikomu nesvěří a Policie ČR se o tomto jednání nedozví.

Závěrem bych rád uvedl, že tímto byl ukončen výčet základních pojmů z oblasti informačních a komunikačních technologií a také nejdůležitějších projevů kyberkriminality. Mezi tyto nejčastější projevy je možné dále řadit například: hacking, cracking, DoS, DDoS, Sniffing a další. Ovšem s těmito už se žáci základních škol téměř nesetkávají, a tudíž nejsou předmětné pro tuto práci.

Tato část práce měla za cíl poukázat na fakt, že se nebezpečí v kyberprostoru skrývá skutečně mnoho. Výše popsanými projevy kyberkriminality jsou přímo ohroženy všechny děti základních škol samostatně pracující v síti internet. Jsem přesvědčen, že pokud nebude existovat intenzivní výuka zaměřená na kyberbezpečnost, k těmto případům docházet zkrátka bude. Když dále vezmu v potaz vysokou míru latence tohoto druhu kriminality, výsledky uveřejňované ve výročních zprávách ČSÚ a ČŠI jsou přímo alarmující. Žáci základních škol jsou i přes svou částečnou informovanost neopatrní až laxní a nestřeží si dostatečně své soukromí. Často nepoužívají odlišná hesla do internetových služeb, na web umisťují své spoře oblečené fotografie a bez problémů naváží kontakt s člověkem, kterého nikdy před tím neviděli. A nejsmutnější na tom celém je fakt, že když už dojde k závadovému jednání, poškozená strana věc ze strachu neoznámí a nemůže tak dojít k přerušení aktivit pachatele.

Policie České republiky od roku 2012 provozovala internetový formulář pro anonymní hlášení závadového obsahu a aktivit na internetu. Prostřednictvím tohoto nástroje bylo přijato mnoho oznámení ze stran občanů. Ke dni 24. května 2018 však doznali experti Ministerstva vnitra a Policie České republiky fakt, že tento nástroj již splnil svou roli. V současné době je vyvíjen nástroj nový, sofistikovanější, který bude přímo reagovat na nově vzniklé hrozby. Hlášení závadových aktivit na internetu však může probíhat stále,

a to prostřednictvím formuláře sdružení CZ.NIC, se kterým Policie ČR spolupracuje. Tento formulář se nachází na internetové adrese stoponline.cz (PČR, ©2018).

Jak již bylo nastíněno v předchozích kapitolách, tato jednání jsou škodlivá, a to nejen dětem základních škol. Z pohledu trestního práva můžeme hovořit o viktimizaci primární (újmě způsobené bezprostředně jako důsledek spáchané trestné činnosti), dále také o viktimizaci sekundární (která nastává po spáchání trestné činnosti a dochází k ní v souvislosti s jejím vyšetřováním) a konečně můžeme hovořit o viktimizaci terciální (ke které dochází v důsledku těžké, dlouhodobé újmy), kdy již dochází ke změně chování oběti. Osobně tedy vnímám tento projekt jako přínosný pro zdravý fyzický i psychický vývoj dítěte.

4 METODIKA

4.1 Popis výzkumu a jeho nástroje

Pro vypracování praktické části diplomové práce byla zvolena metoda kvantitativního výzkumného šetření pomocí anonymního dotazníku, viz příloha č. 1. a metoda SWOT, která je zahrnuta v kapitole *Výsledky*.

Dotazníková metoda sběru dat patří k nejrozšířenějším metodám sběru informací a slouží k získávání empirických údajů vhodných k další analýze. Tato metoda sběru dat byla zvolena pro svoji jednoduchost, a protože poskytuje dostatečný časový prostor respondentům pro svou odpověď. Dotazníkem lze zkoumat názory, postoje a znalosti jedinců v dané problematice a zároveň zachovat jejich anonymitu. Vzhledem k poměrně nízkému věku a nesmělosti respondentů se jedná se o nejvhodnější metodu ke sběru dat pro tuto práci.

Pro tyto potřeby byl vytvořen anonymní nestandardizovaný dotazník s celkovým počtem 23 otázek. Z těchto otázek jsou 4 otázky polootevřené a 19 otázek je uzavřených. Otázky i odpovědi byly formulovány tak, aby byly jasné, stručné a výstižné. Pokud nebylo uvedeno jinak, respondenti volili pouze jednu odpověď. Dotazník má logickou posloupnost s cílem potvrdit nebo vyvrátit stanovené hypotézy. Dotazník lze rozdělit na část úvodní, kde se nacházejí pokyny k jeho vyplnění, část věnovanou osobě respondenta, část zaměřenou na škodlivá jednání v síti internet a nejčastější projevy kyberkriminality a část závěrečnou, kde byla očekávána trocha vlastní invence dětí.

Předkládaný dotazník byl vytvořen ve spolupráci se zkušeným pedagogem vzdělaným v oblasti školského managementu a zároveň ředitelem Mateřské školy Zlonice Mgr. Janou Dvořákovou a učitelkou Základní školy Kladno Mgr. Martou Červinkovou. Dotazníková šetření tak byla maximálně přizpůsobena

myšlení žáků základních škol, a to za účelem získání co možná nejvíce relevantních dat bez nežádoucího zkreslení výsledků.

Na základě výsledků dotazníkového šetření byla ze strany policisty ÚO Praha venkov – západ realizována beseda, která měla za cíl odstranit nedostatky v informovanosti o kyberkriminalitě a současně se zaměřit na uvědomění si rizikového chování na síti internet. Beseda byla sestavena vždy s ohledem na slabé stránky žáků za účelem maximálního přínosu. Toto bylo následně prověřeno testováním proškolených subjektů, kdy v poslední části besedy proběhl test pozornosti a zkouška nově nabytých vědomostí. Za účelem zachování stejného výzkumného vzorku probíhalo testování žáků bezprostředně po realizaci besedy a získaná data je tak možné dále porovnávat a zpracovávat.

Účinnost této besedy byla dále vyhodnocena pomocí SWOT analýzy se zaměřením na rozdíly mezi městskými a venkovskými školami. SWOT analýza patří mezi nejčastěji využívanou analytickou metodou zaměřenou na zhodnocení vnitřních a vnějších faktorů ovlivňujících úspěšnost konkrétního záměru. Poskytuje podklady pro formulaci rozvojových směrů, aktivit a strategických cílů. Spočívá v rozboru a hodnocení současného stavu pomocí Strengths (silných stránek), Weaknesses (slabých stránek), Opportunities (příležitostí) a Threats (hrozeb), a je tedy vhodným nástrojem pro analyzování získaných dat.

4.2 Časový harmonogram sběru dat

Výzkumné šetření probíhalo v časovém rozmezí 2 let. Již od roku 2018 byly ze strany Policie ČR OÚ Praha venkov – západ navštěvovány základní školy ve Středočeském kraji a v těchto byly konány besedy na téma kyberkriminality. Základní školy byly vybírány náhodně, ale bylo přihlíženo také k aktuálnímu nápadu trestné činnosti v této oblasti. Tyto aktivity ze strany policisty byly

prováděny nad rámec jeho pracovních povinností a v rámci prevence před tímto druhem kriminality.

4.3 Výzkumný vzorek

Výzkum byl zaměřen na žáky základních škol ve Středočeském kraji a probíhal celkem ve třech městských a ve třech venkovských školách. Konkrétně se jednalo o města: Roztoky, Smečno, Mníšek pod Brdy a obce Stehelčeves, Horoměřice, Velké Přílepy. Některé školy byly navštíveny také opakovaně a besedy byly prováděny se žáky základních škol od šesté třídy. Byl získán soubor dat od celkového počtu 563 respondentů. Avšak pro zachování maximální přínosnosti a možnosti porovnávání mezi školami, byl výzkumný vzorek zredukován na jednu osmou a jednu devátou třídu v každé škole. V základní škole, kde nebyla devátá třída, byly výzkumným vzorkem třídy sedmá a osmá. Touto redukcí vznikl soubor dat, který obsahuje celkem 328 respondentů ze stran žáků základních škol. Dotazníky byly vždy zadávány osobně před besedou, a tudíž jejich návratnost a zpracování činí 100 %. Stejně je tomu také v případě následného testování proškolených subjektů.

5 VÝSLEDKY

V diplomové práci byl stanoven jeden hlavní cíl a celkem pět dalších dílčích úkolů. Tyto budou blíže popsány v následující části. V úvodu je třeba konstatovat, že každý bod byl plněn dle nejlepšího vědomí a svědomí autora. Autentičnost dat je zaručena osobním sběrem informací a osobním testováním stejného výzkumného vzorku osob. Výsledky nejsou zaokrouhlovány, a je tak zaručena maximální přesnost. Besedy na základních školách byly realizovány formou hravého učení za využití informačních technologií, předem připravených prezentací a skutečných kriminálních případů z kriminalistické praxe.

5.1 Hlavní cíl práce

Hlavním cílem diplomové práce je najít způsob, jak ochránit děti tam, kde selhává rodina, škola, stát. Učinit žáky základních škol odolnějšími vůči nástrahám kyberprostoru a docílit zvýšení gramotnosti v dané oblasti.

K naplnění tohoto cíle je třeba nejprve provést dílčí úkoly níže a tento cíl bude proto podrobně prozkoumán, popsán a splněn v závěru kapitoly *Výsledky*.

5.2 Soubor dílčích úkolů

5.2.1 Ucelený náhled do problematiky kyberkriminality

Prvním dílčím úkolem bylo přinést, na základě podrobného studia knižních a internetových publikací, ucelený náhled do problematiky kyberkriminality.

Toto bylo provedeno v teoretické části diplomové práce, kde byly popsány základní pojmy z oblasti informačních a komunikačních technologií a nejčastější projevy kyberkriminality se zaměřením na kyberšikanu, sexting, kyberstalking a kybergrooming. V této části byla promítnuta i vlastní zjištění spolu s uvedením několika praktických příkladů.

5.2.2 Dotazníkové šetření, analýza dat a realizace besedy

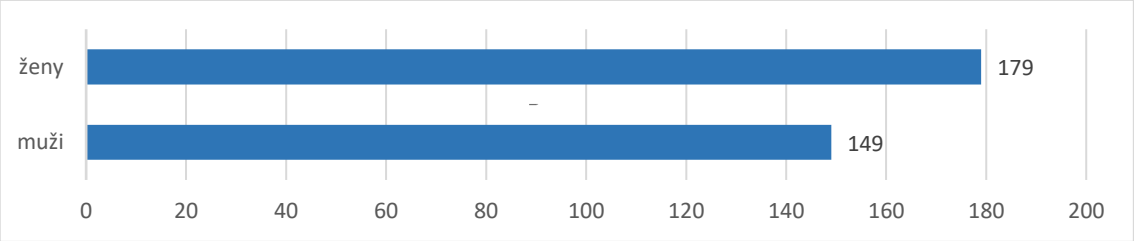
Druhým úkolem bylo na základě získaných dat z dotazníkového šetření provést analýzu výsledků a následně realizovat besedu dle potřeb žáků základních škol.

Je nutné poznamenat, že autor této práce a zároveň policista zařazený ve skupině kybernetické kriminality Praha venkov – západ začal provádět besedy a dotazníková šetření ještě před tvorbou diplomové práce. Besedy byly prováděny za účelem prevence již od roku 2018. Získaná data z dotazníkových šetření byla podrobena redukci na tři městské a na tři venkovské základní školy dle zadání práce. Veškerá tato data byla posléze analyzována a včetně odůvodnění podstaty otázek shrnuta v následující části.

Otázky č. 1 až 6 byly věnovány osobě respondenta, zjišťovaly základní informace k jeho osobě a sebehodnocení. V této části bylo zjišťováno, jak žáci využívají síť internet a jak hodnotí své znalosti nástrah v kyberprostoru.

Otázka č. 1 - Pohlaví

- žena
- muž

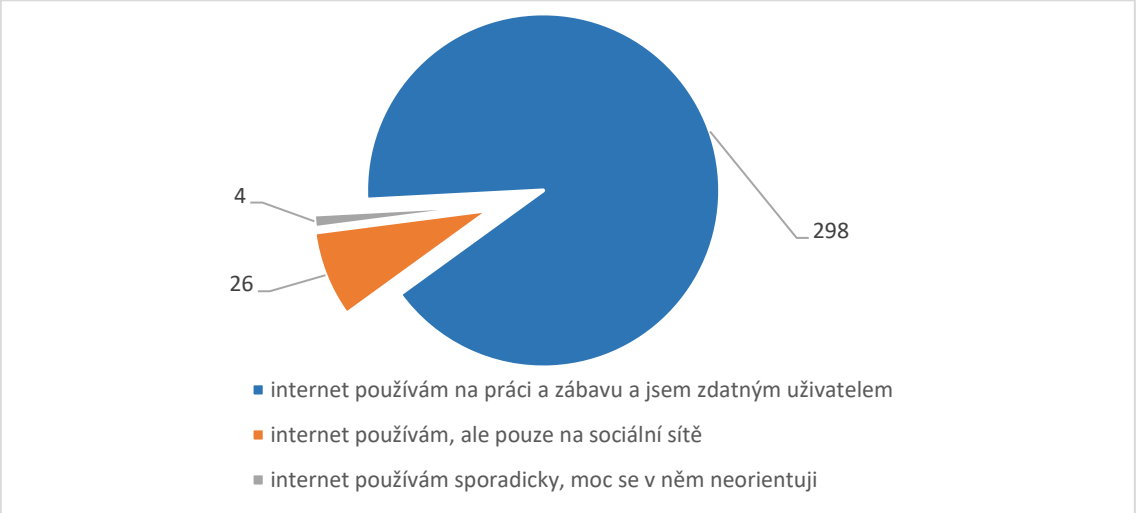


Obrázek 3 - Pohlaví respondentů

Otázkou č. 1 bylo zjištěno, že se výzkumu účastní celkem 179 žen a 148 mužů, což činí procentuálně 54,57 % ve prospěch žen. Toto hledisko bude později podstatné pro zkoumání odlišného chování v síti internet. Bylo totiž zjištěno, že jinak přistupují k nebezpečí v síti internet chlapci a jinak dívky.

Otázka č. 2 - Jak zdatně si počínáte v síti internet?

- internet používám na práci a zábavu a jsem zdatným uživatelem
- internet používám, ale pouze na sociální sítě
- internet používám sporadicky, moc se v něm neorientuji



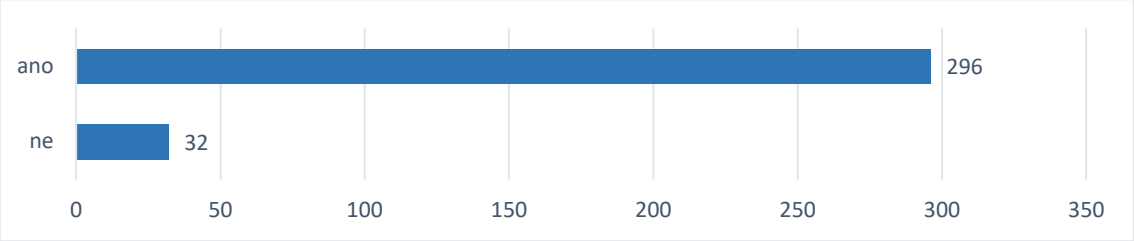
Obrázek 4 - Počínání respondentů v síti internet – sebehodnocení

Otázka č. 2 měla za cíl přimět žáky k sebehodnocení. Bylo zjištěno, že se celkem 298 žáků domnívá, že si v síti internet počíná zdatně, 26 žáků používá internet pouze na sociální sítě a 4 žáci se v internetu pohybují sporadicky. Z tohoto zjištění vyplývá, že 90,85 % žáků se hodnotí v užívání internetu jako zdatný uživatel. Jak však bylo zjištěno později, i tito žáci se při používání internetu dopouštějí fatálních chyb.

Mezi nejčastější chyby patří především sdělování osobních údajů dalším osobám a zasílání intimních fotografií prostřednictvím sociálních sítí. Žáci základních škol nevnímají tato jednání jako potenciální nebezpečí. Žijí v domnění, že kyberprostor je bezpečné místo, neboť jde pouze o místo virtuální. Tímto však přímo nahrávají skutečným internetovým predátorům.

Otázka č. 3 - Myslíte si, že již u osob Vašeho věku existují rizika při užívání celosvětové sítě internet?

- ano
- ne

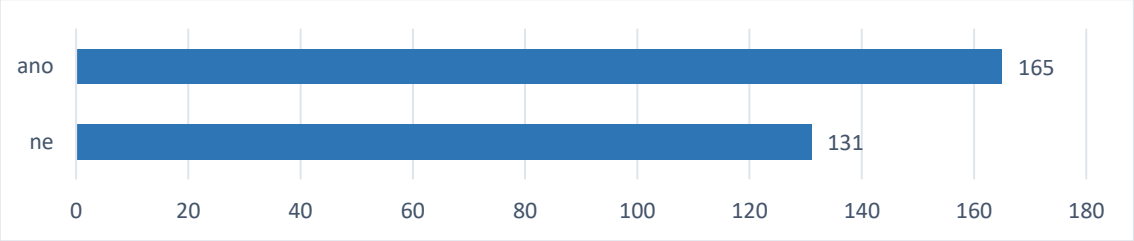


Obrázek 5 - Existence rizik v síti internet

Otázka č. 3 byla zaměřená na otázku, zda i ve svém věku registrují rizika při užívání sítě internet. Z celého počtu 328 respondentů se 296 z nich domnívá, že ano a 32 respondentů se domnívá, že rizika neexistují. 32 osob se může zdát jako zanedbatelné číslo, ale v procentuálním vyjádření je to činí 9,76 %. Je tedy patrné, že téměř 10 % respondentů si neuvědomuje rizika při užívání sítě internet, a to je hodně.

Otázka č. 4 - Pokud ano, jste dostatečně připraveni na tato rizika (nástrahy)?

- ano
- ne



Obrázek 6 - Připravenost respondentů na rizika v síti internet

Otázka č. 4 byla zaměřena na uživatele, kteří odpověděli v předchozí otázce ano. Otázka má za cíl zjistit, zda jsou žáci základních škol dostatečně připraveni na nástrahy sítě internet. 165 respondentů se domnívá, že ano a 131 osob si myslí, že připraveni nejsou. V procentuálním vyjádření to činí celkem 44,26 %, nepřipravených osob. Obě otázky utváří alarmující obraz o dnešní

mladé generaci osob. Zjištěné údaje jsou naprosto neuspokojivé a nelze se pak divit stále se zvyšujícímu počtu trestních oznámení na Policii ČR pro některý z kybernetických útoků.

Tabulka 2 - Statistika kybernetických deliktů ve Středočeském kraji

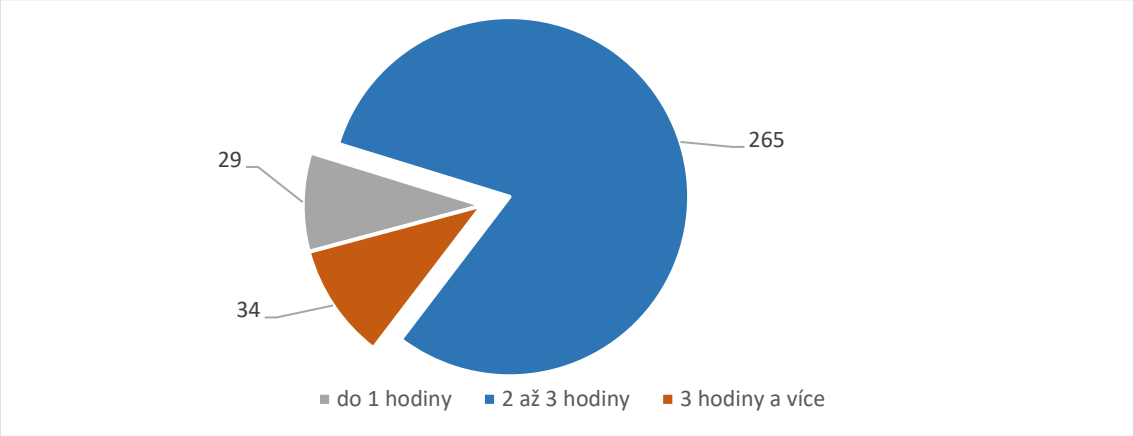
V letech	Počet kybernetických deliktů
2015	3
2016	31
2017	20
2018	28
2019	45

Výše uvedená tabulka znázorňuje vývoj kybernetických deliktů ve Středočeském kraji, kde osobou poškozenou je dítě ve věku do 15 let. Z uvedených dat je patrné, že až na rok 2016, kde byl enormní nárůst kybernetických deliktů, dochází ke každoročnímu nárůstu oznámených trestných činů a přestupků. Když vezmeme v potaz latentní kriminalitu, tedy kriminalitu skrytou, neoznámenou orgánům činným v trestním řízení, můžeme se dostat na hodnoty daleko vyšší. Uvedená data jsou získána ze statistického vykazování Policie ČR Středočeského kraje se souhlasem služebního funkcionáře Praha venkov – západ.

Autoři Kuchta & Válková (2005) uvádějí, že se míra latence liší podle druhu trestné činnosti. Větší míra latence se předpokládá u drogové kriminality, domácího násilí, sexuálních činů mezi rodinnými příslušníky, zneužívání dětí, organizovaného zločinu a hospodářské kriminality. Ale zcela jistě by se mezi tyto druhy kriminality daly řadit i kybernetické trestné činy. Oběť se ve většině případů obává další újmy a ze strachu tak oznámení neučiní. I toto téma bylo podrobně probíráno na pořádaných besedách se žáky základních škol. Žákům bylo několikrát opakováno, že je důležité svěřit se s problémem minimálně jedné dospělé osobě.

Otázka č. 5 - Kolik času denně strávíte online? (weby, sociální sítě, …)

- do 1 hodiny
- 2 – 3 hodiny
- 3 hodiny a více

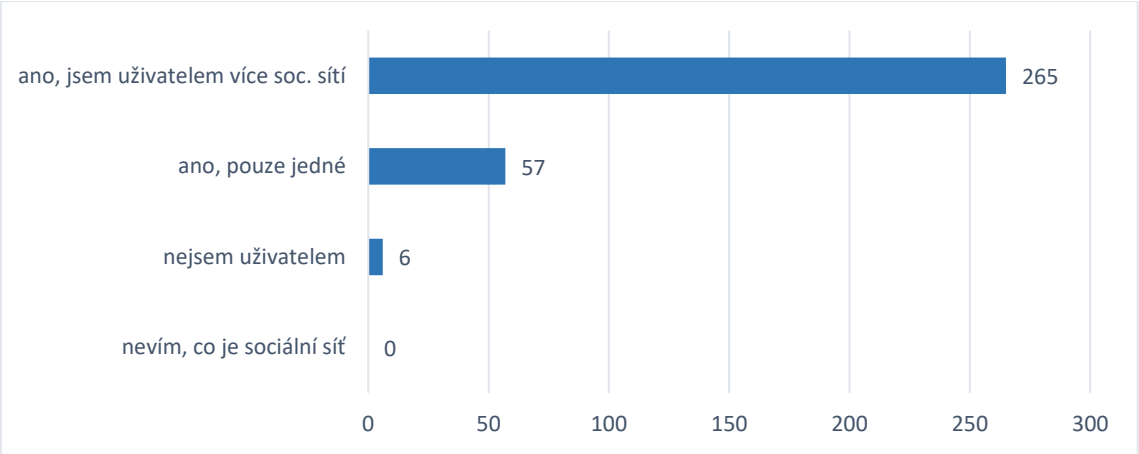


Obrázek 7- Strávený čas online

Otázka č. 5 měla za cíl vytvořit obraz o tom, kolik hodin denně tráví žáci základních škol v síti internet. Do jedné hodiny tráví na internetu 29 žáků, od 2-3 hodin celkem 265 žáků a 3 hodiny a více celkem 34 žáků. Výsledek není nikterak zarážející, do jedné hodiny tráví online 29 žáků, 2-3 hodin celkem 265 žáků a více jak 3 hodiny celkem 34 žáků. Zde stojí za zmínku poslední údaj, kdy 34 žáků je celkem 10,37 %. Na daném modelu je patrné, že se více než 10 % mladých lidí uchyluje v ¼ svého denního času do online světa. Je zde tedy vidět i vývoj, kterým se dnešní společnost vydává. Mladí lidé dříve trávili čas společnými aktivitami, dnes dávají přednost samotě, ale zároveň společnost vyhledávají ve světě online.

Otázka č. 6 - Jste uživatelem nějaké sociální sítě?

- ano, jsem uživatelem více sociálních sítí
- ano, pouze jedné
- nejsem uživatelem
- nevím, co je sociální síť



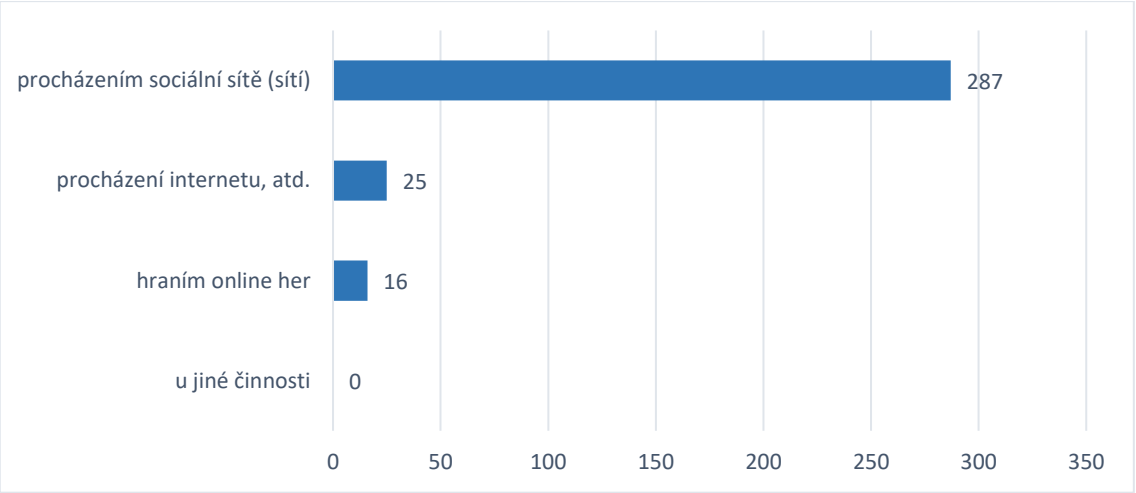
Obrázek 8 - Členství v sociálních sítích

Otázka č. 6 přímo navazovala na otázku pátou a zjišťovala, zda jsou žáci základních škol uživatelé sociálních sítí. Bylo zjištěno, že neexistuje nikdo, kdo by pojem sociální síť neznal. Na druhou stranu celkem 6 osob uvedlo, že není uživatelem sociální sítě. U třech osob bylo v průběhu diskuze toto vyvráceno, ale 3 osoby skutečně žádnou sociální síť nevyužívaly. Jednalo se vesměs o žáky z chudších vrstev, bez chytrého telefonu a počítače v domácnosti. Touto otázkou bylo dále zjištěno, že celkem 57 osob je uživatelem pouze jedné sociální sítě a 265 osob je uživatelem více sociálních sítí. V procentuálním vyjádření tento počet činí celkem 80,79 % osob, které využívají více jak jednu sociální síť. V diskuzi se žáky bylo probíráno i toto téma a bylo zjištěno, že je pro online osobnost důležité být dostupný na vícero sociálních sítích. Dodává to prý na popularitě a prestižnosti dané osoby.

Další dotazníková část je již zaměřena na škodlivá jednání v síti internet a nejčastější projevy kyberkriminality.

Otázka č. 7 - U jaké činnosti na internetu trávíte nejvíce času?

- procházení internetu, čtení článků a novinek apod.
- procházením sociální sítě (sítí)
- hraním online her
- u jiné činnosti, popište ……

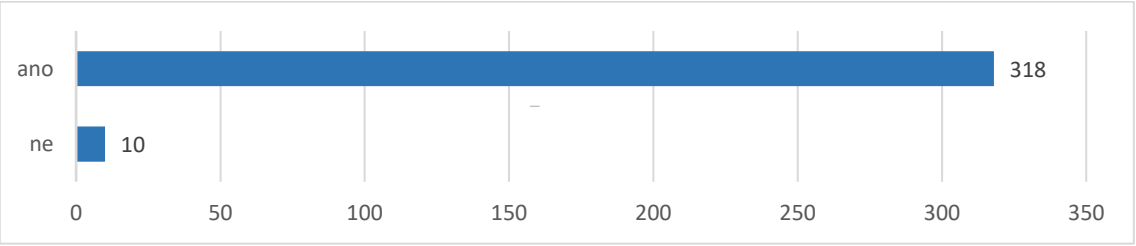


Obrázek 9 - Činnosti v síti internet

Otázka č. 7 navazovala na otázku předchozí a měla za cíl zjistit, u jaké činnosti v síti internet tráví žáci nejvíce času. Bylo zjištěno, že procházením internetu tráví nejvíce času 25 dotazovaných osob, hraním online her pouze 16 osob a otevřenou otázku nezvolil žádný žák. Nejvíce času tráví mladí lidé procházením sociálních sítí a tuto volbu zvolilo celkem 287 z nich. V procentuálním vyjádření to činí celkem 87,50 %. Jedná se o další důkaz toho, že dochází k pomalé migraci skutečného světa do toho virtuálního. Začíná být důležitější virtuální osobnost než osobnost skutečná. Mladí lidé, kteří nemají průběžně aktualizované profily a dostatek „Like it" (To se mi líbí) jsou prostě mimo. Také z tohoto důvodu o sobě žáci prozrazují na sociálních sítích mnohem více informací, než je bezpečné.

Otázka č. 8 - Setkali jste se již s termínem kyberkriminalita/PC kriminalita?

- ano
- ne



Obrázek 10 - Šetření k pojmu kyberkriminalita

Otázka č. 8 byla zaměřena na všeobecně známý termín „kyberkriminalita“ příp. „PC kriminalita“ a měla za cíl zjistit, zda se žáci s tímto termínem již v minulosti setkali. Celkem 318 respondentů uvedlo, že se s termínem setkalo, ale 10 respondentů uvedlo, že nikoliv. 10 respondentů činí zanedbatelných 3,05 %, ale právě zde vzniká jistý předpoklad pro jejich viktimizaci. Není zcela jisté, zda jde ze strany žáků pouze o nezájem nebo laxnost v této oblasti. Avšak aby žák 8. nebo 9. třídy základní školy nikdy neslyšel o shora uvedených termínech, to bohužel nevrhá dobré světlo ani na rodinné zázemí, ani na základní školu.

Otázka č. 9 - Setkali jste se někdy s následujícími termíny? (pokud ano, tyto označte)

- ☐ Phishing
- ☐ Ransomware
- ☐ Malware
- ☐ Podvodné stránky
- ☐ Spam
- ☐ Hoax
- ☐ Cracking
- ☐ Hacking
- ☐ DoS, DDoS
- ☐ Sniffing

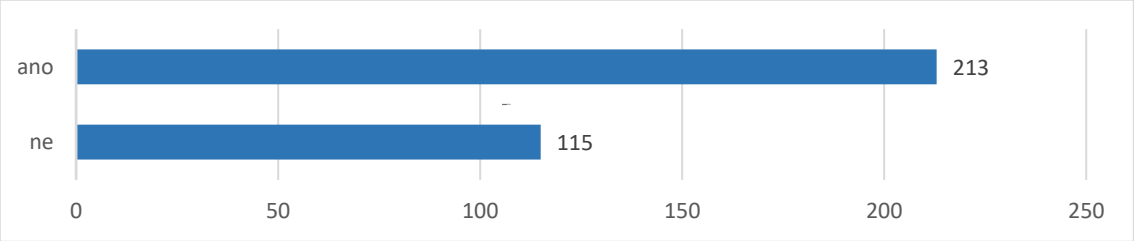
Tabulka 3 - Povědomost o odborných termínech

Termíny z oblasti kyberkriminality	Procentuální vyjádření
Phishing	46,2 %
Ransomware	23,4 %
Mallware	78,7 %
Podvodné stránky	54,4 %
Spam	89,2 %
Hoax	67,7 %
Cracking	66,9 %
Hacking	74,5 %
DoS, DDoS	13,7 %
Sniffing	2,1 %

Otázka č. 9 zjišťovala, jak jsou na tom žáci s odbornými termíny. Provedeným výzkumem bylo zjištěno, že se nejedná o špatný výsledek a žáci jisté povědomí skutečně mají viz tabulka s procentuálním vyjádřením. Zde je však nutné poznamenat, že jde o odborné názvy, které není bezpodmínečně nutné znát. V dané věci jde spíše o jednání, která jsou pod termíny spatřovány, což bude obsahem dalších otázek.

Otázka č. 10 - Pokusil se Vás někdo neznámý uvést prostřednictvím internetu v omyl podvodnou nabídkou, výhrou nebo žádostí o pomoc apod.? (na vzniklé škodě, nebo zda jste na toto jednání reagovali, nezáleží)

- ano
- ne



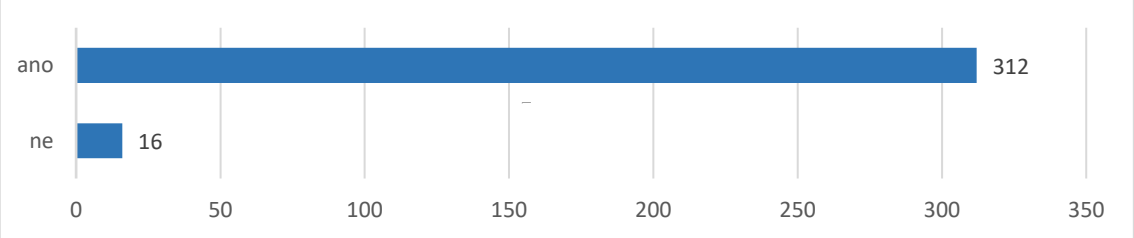
Obrázek 11 - Náchylnost k podvodům

Otázka č. 10 byla přímo zaměřena na Phishing, který by měl být znám pro 46,2 % žáků. Otázka měla za cíl zjistit, zda na ně bylo již v minulosti cíleno podvodnou nabídkou, výhrou, žádostí o pomoc apod. Bylo zjištěno, že 115 respondentů popsané jednání neregistruje, ale celkem 213 respondentů uvedlo, že se s daným fenoménem již setkali. V procentuálním vyjádření to činí celkem 64,94 % osob, na které již bylo v minulosti cíleno popsaným podvodným způsobem. I když se v našem případě jedná o osoby bez vlastních finančních prostředků, nelze tato jednání považovat za méně škodlivá. Ano, existuje zde reálný předpoklad, že dítě základní školy nezašle prostřednictvím internetu finanční hotovost jiné osobě. Ovšem toto není pravidlem. I tyto děti mnohdy disponují svým bankovním účtem a obětmi podvodu se tak stát jednoduše mohou. Nehledě na to, že tato podvodná jednání nemusí nutně

směřovat na finanční hotovost. Mohou být zaměřena na získání osobních údajů nebo mohou cílit na chyby v úsudku uživatele za účelem klikání na reklamy. Vzhledem k okolnostem jsou zjištěné hodnoty až alarmující a prováděné besedy lze tedy považovat za více než přínosné.

Otázka č. 11 - Nalezli jste na internetu nějakou nepravdivou informaci nebo podvodnou webovou stránku?

- ano
- ne

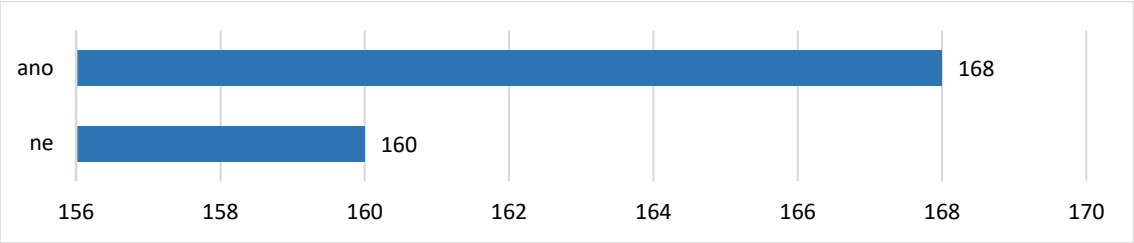


Obrázek 12 - Nepravdivé informace na internetu

Otázka č. 11 cílila na pravdivost informací na internetu, Hoax, Clickbait. Žáci v drtivě většině odpověděli, že se již setkali nepravdivou informací v internetu. Žáci v drtivě většině odpověděli, že se již s nepravdivou informací na internetu setkali. V procentuálním vyjádření se s nepravdivou informací setkalo již 95,12 % osob, naopak s nepravdivou informací se nesetkalo 4,88 % osob. Tento údaj je rozhodně povzbuzující, neboť je patrné, že i mladí lidé registrují relativní nepravdivost informací a měli by být schopni správné interakce. Do jaké míry jsou však žáci schopni nepravdivost informací rozlišit, nelze s určitostí říct. Vzhledem k nedostatku zkušeností a sofistikovanosti pachatelů však nelze brát výsledek 95,12 % jako index odolnosti mladých lidí proti nepravdivosti informací v síti internet.

Otázka č. 12 - Upozornil Vás již v minulosti antivirový software na škodlivý kód ve formě mallware, trojského koně nebo viru? (při procházení internetu)

- ano
- ne



Obrázek 13 - Škodlivé kódy, viry, mallware

Otázka č. 12 zjišťovala, zda byli žáci informování o škodlivém kódu prostřednictvím antivirového programu. Výzkumným šetřením bylo zjištěno, že celkem 168 žáků již v minulosti upozorněno bylo a 160 žáků nikoliv. V procentuálním vyjádření činí počet 160 žáků celkem 48,78 %. Vysvětlení může být několik. Buď nenavštěvují žáci webové stránky s pochybným obsahem (pornografickými materiály, cracky, online autorská díla apod.). Nebo žáci tyto hlášky jednoduše ignorují. Instalovaný antivirový software ve stolních PC je považován za standardní výbavu, a je tedy s touto podmínkou v otázce počítáno. Pokud se jedná o mobilní zařízení, závadné webové stránky přímo poukazují na napadení škodlivým kódem a vybízejí k užití jejich antivirového software. Tento software však mnohdy přináší do mobilního zařízení i „přidanou hodnotu“ ve formě škodlivých funkcí způsobujících přinejmenším únik zájmových dat.

Otázka č. 13 - Setkali jste se někdy s následujícími termíny? (pokud ano, tyto označte)

- ☐ kyberšikana
- ☐ sexting
- ☐ kyberstalking
- ☐ kybergrooming

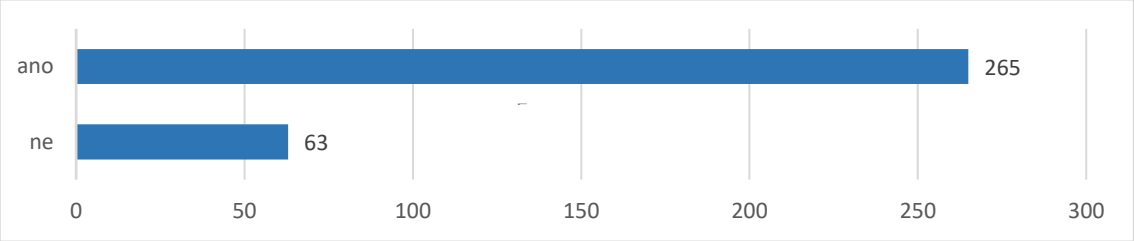
Tabulka 4 - Povědomost o odborných termínech II.

Termíny z oblasti kyberkriminality	Procentuální vyjádření
kyberšikana	96,4 %
sexting	63,1 %
kyberstalking	42,6 %
kybergrooming	2,3 %

Otázka č. 13 byla cílena na všeobecně známé termíny kyberšikana, sexting, kyberstalking a kybergrooming. Výsledek není nikterak překvapivý. 96,4 % respondentů zná termín kyberšikana, 63,1 % zná termín sexting, 42,6 % zná termín kyberstalking a jen pouhé 2,3 % respondentů zná termín kybergrooming viz tabulka s procentuálním vyjádřením. Opět je nutné poznamenat, že není bezpodmínečně nutné znát odborné názvy, ale je třeba znát jednání, která jsou pod termíny spatřovány. Tato jednání budou předmětem následujících otázek.

Otázka č. 14 - Už jste se setkali s tím, že někdo někoho ponižoval nebo šikanoval přes internet? (zasílání obtěžujících, ponižujících zpráv, napadání na sociálních sítích, fyzické napadání oběti spojené s natáčením videa apod.)

- ano
- ne



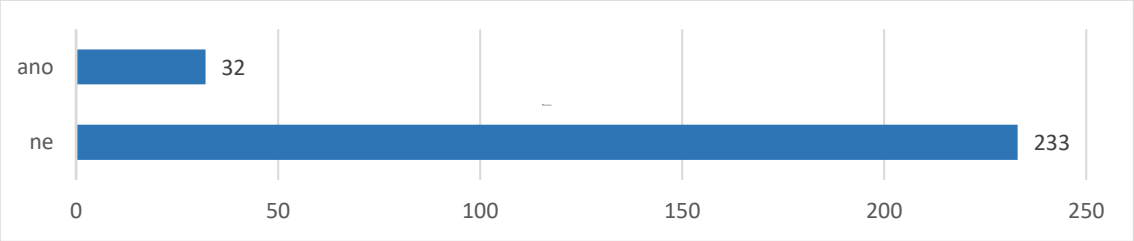
Obrázek 14 - Šikana a ponižování na internetu

Otázka č. 14 byla cílena na problematiku kyberšikany. Měla za účel zjistit, zda se žáci základních škol již s tímto termínem setkali. Celkem 265 žáků uvedlo, že ano a celkem 63 žáků uvedlo, že nikoliv. V procentuálním vyjádření se tak jedná o 19,20 % žáků, kteří prý nikdy nepřišli s kyberšikanou do styku. Po vyhodnocení výzkumného šetření se však zdá být výsledek poněkud zkreslený. V otázce č. 7 bylo zjištěno, že celkem 87,50 % žáků využívá při procházení internetu nejčastěji sociální sítě. A právě sociální sítě jsou to pomyslné pískoviště, kde je ponižování na denním pořádku. Lze tedy předpokládat, že mladí lidé vnímají kyberšikanu v tom nejtěžším možném slova smyslu a některé lehčí formy jako šikanu vůbec nereflektují. Také tomuto

tématu byla při provedených besedách přisuzována nejvyšší důležitost, včetně přihlédnutí k trestně právnímu postihu v případě protiprávního jednání.

Otázka č. 15 - Stalo se jednání popsané výše přímo Vám? (odpovídejte, jen pokud jste označili v předchozí otázce ano)

- ano
- ne



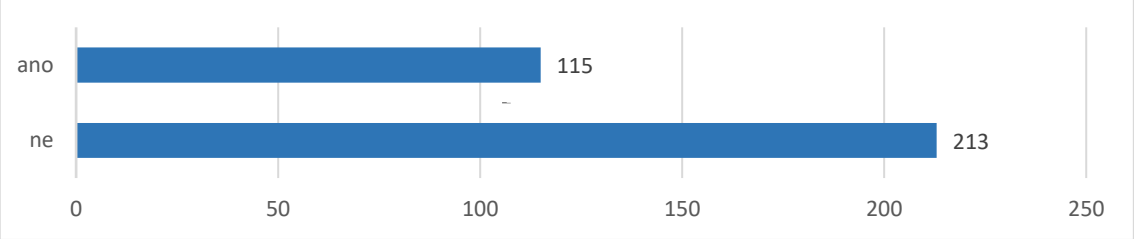
Obrázek 15 - Šikana a ponižování na internetu – vlastní

Otázka 15 byla určena jen pro ty, co se s kyberšikanou setkali. Měla za cíl zjistit, zda se toto jednání stalo přímo jim. Na tuto otázku odpovědělo celkem 233 žáků, že nikoliv, ale celkem 32 žáků uvedlo, že se stali obětí kyberšikany. V procentuálním vyjádření je to 9,76 % z celkového počtu žáků, ale zároveň 12,08 % z počtu žáků odpovídajících na tuto otázku. Je tedy nutné vycházet z hodnoty 12,08 % žáků, kteří mají osobní zkušenost s kyberšikanou, a to je vysoké číslo. Zástupci škol při besedách přiznávají, že je kyberšikana problémem dnešní doby. Žáci základních škol trpí depresemi spojenými s nedostatečnou popularitou na sociálních sítích. Zjednodušeně uvádějí, že se množí případy zhoršení školního prospěchu kvůli málo „Like it" příspěvkům u statusů nebo fotografií. Žáci se mnohdy přestávají snažit ve skutečném světě, aby veškerou svoji energii mohli vydávat ve světě virtuálním. A právě zde nastává problém. Jsou poté mladí lidé schopni se řádně začlenit do společnosti? Nebudeme se na českých školách v budoucnu setkávat se „šílenými střelci", jako tomu již bývá v USA? Na další vývoj si zřejmě budeme muset ještě počkat. V této části je třeba uvést, že zodpovědnost v otázce prevence před šikanou a kyberšikanou leží zejména na rodině a škole, nikoliv

na orgánech činných v trestním řízení. I tak byla otázka kyberšikany, potažmo šikany jedním z nejdůležitějších bodů řízené diskuze se žáky. Policejní orgán při této příležitosti poukázal i na trestně právní postih v případech spáchání provinění dle ustavení § 175 TZ (Vydírání) a dle ustanovení § 354 TZ (Nebezpečné pronásledování).

Otázka č. 16 - Už jste se setkali s tím, že někdo ve Vašem okolí zaslal prostřednictvím internetu svojí intimní (částečně intimní) fotografii (video) jiné osobě?

- ano
- ne



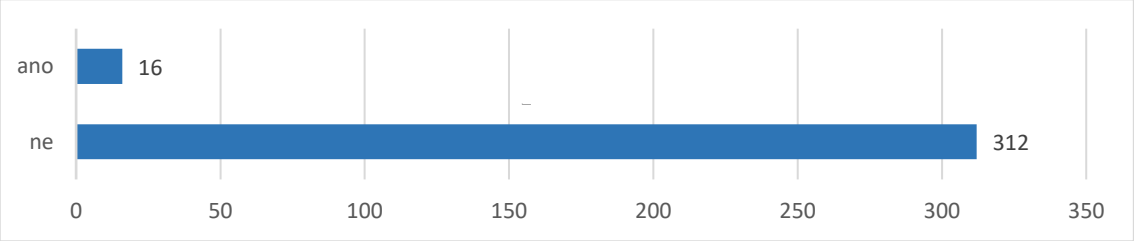
Obrázek 16 - Zasílání intimních fotografií

Otázka č. 16 byla zaměřena na problematiku sextingu. Měla za cíl zjistit, zda znají někoho, kdo zaslal prostřednictvím internetu svoji, byť jen zčásti, intimní fotografii. Celkem 213 respondentů uvedlo, že nikoliv, ale celkem 115 osob uvedlo, že ano. V procentuálním vyjádření to činí celkem 35,06 % žáků, kteří se s tímto jevem setkali. A to je rozhodně alarmující údaj. Mohlo by to snad znamenat, že se v síti internet nachází relativně vysoké procento intimních materiálů žáků osmých a devátých tříd základní školy? Když vezmeme v potaz, jak nebezpečné jednání se za tímto jevem skrývá, opět musíme poukázat na smysl prováděných besed. Tohoto jevu si všímá i český televizní seriál mall.tv s názvem #martyisdead. Jde o příběh žáka základní školy, který zašle prostřednictvím internetu neznámé dívce video, na kterém masturbuje. Je poté vydírán a příběh končí smrtí chlapce. Seriál má celkem 8 dílů a popisuje jednotlivé fáze předcházející tragické události a rozplétání

celého příběhu s rodiči a přáteli poté. Thriller #martyisdead zvítězil na festivalu Seriál Killer a stal se vítězem druhého ročníku mezinárodního soutěžního festivalu televizních a online seriálů Serial Killer v roce 2019. I tento příběh byl inspirovaný skutečnými příběhy a obdobně jako u Amandy Todd, viz kapitola *Kyberšikana* v teoretické části práce, je třeba na tato jednání neustále poukazovat. Autor diplomové práce se na základě svého profesního zařazení setkává s několika případy ročně. V lehčích případech jde o pouhé zasílání zčásti obnažených fotografií přes sociální sítě, v těžších případech závadné jednání přeroste v trestný čin dle ustanovení § 175 TZ (Vydírání).

Otázka č. 17 - Zaslal(a) jste Vy osobně někdy někomu prostřednictvím internetu svojí intimní (částečně intimní) fotografii (video)?

- ano
- ne

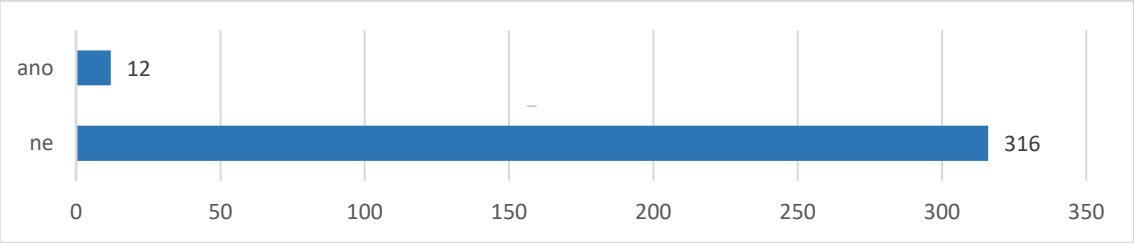


Obrázek 17 - Zasílání intimních fotografií – vlastní

Otázka č. 17 byla opět zaměřena na sexting. Otázka zjišťovala, zda respondenti sami zaslali někomu, prostřednictvím internetu, byť jen zčásti, intimní materiály. Výsledkem je 312 osob, které uvedly, že nikoli, ale celkem 16 osob přiznalo, že svou intimní fotografii již v minulosti zaslalo. V procentuálním vyjádření je to celkem 4,88 % žáků, kteří neregistrovali nebezpečí a dopustili se tak jednoho z nejnebezpečnějších chování v síti internet vůbec. U této otázky bylo přihlédnuto dále k pohlaví žáků, kdy byl zjištěn zajímavý údaj. Z celkového počtu 16 osob bylo 9 chlapců a 7 dívek. Pokud jsou získaná data správná, znamená to, že více obnažených fotografií zasílají chlapci.

Otázka č. 18 - Už jste se setkali s tím, že Vás někdo pronásledoval prostřednictvím informačních a komunikačních technologií za účelem kontaktování? (neustálé zasílání zpráv, e-mailů, telefonáty a prozvánění, opakované komentování příspěvků na sociálních sítích apod.)

- ☐ ano
- ☐ ne

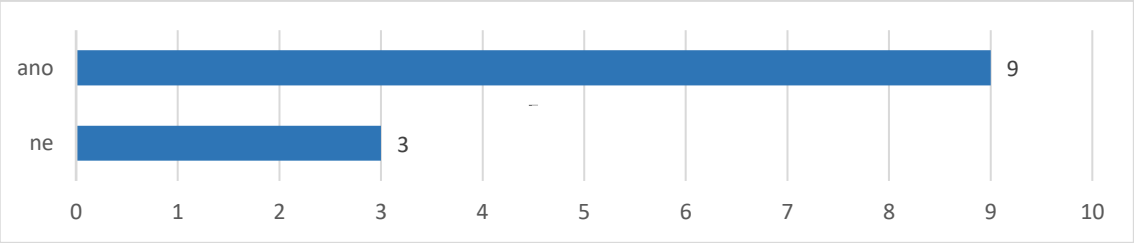


Obrázek 18 - Pronásledování po internetu

Otázka č. 18 byla zaměřena na problematiku kyberstalkingu. Tato otázka měla za cíl zjistit, zda se žáci základních škol již s tímto jednáním v minulosti setkali. Celkem 316 respondentů uvedlo, že se s tímto nikdy nesetkalo, ale 12 osob uvedlo, že ano. V procentuálním vyjádření to činí celkem 3,66 % osob, které mají zkušenosti s pronásledováním přes internet.

Otázka č. 19 - Stalo se jednání popsané výše přímo Vám? (odpovídejte, jen pokud jste označili v předchozí otázce ano)

- ☐ ano
- ☐ ne



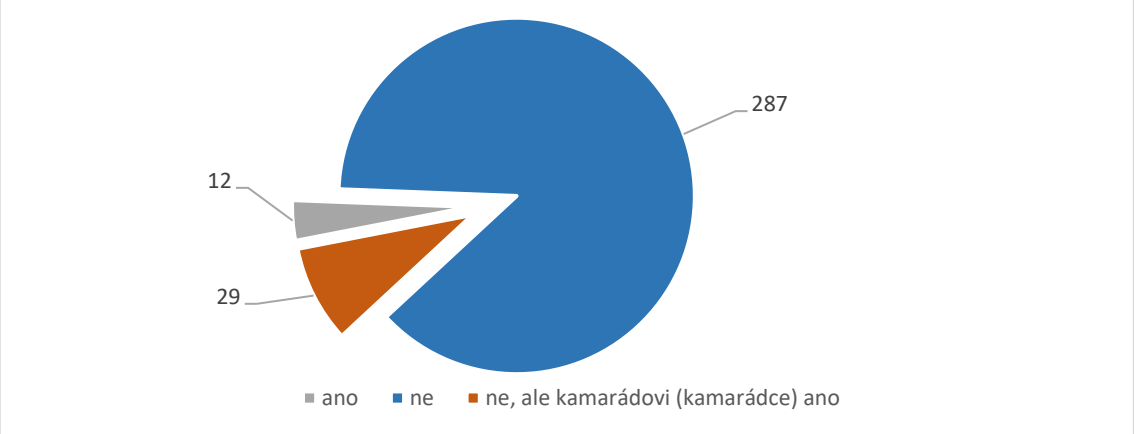
Obrázek 19 - Pronásledování po internetu - vlastní

Otázka č. 19 měla za cíl zjistit, zda se stalo popsané jednání výše právě dotazovaným osobám. Výzkumným šetřením bylo zjištěno, že celkem 75 % respondentů uvedlo, že ano. V řeči konkrétních čísel se jedná o 9

pronásledovaných žáků z 328, což činí 2,74 % z nich. I když je toto závadné jednání více spatřováno u dospělých osob, vyskytuje se tedy i mezi žáky základních škol.

Otázka č. 20 - Už jste se setkali s tím, že Vás někdo neznámý kontaktoval prostřednictvím sociálních sítí a chtěl navazovat bližší kontakt? (ať už pouhé dopisování nebo následné dotazování se na osobní údaje, případně vyžadování osobní schůzky)

- ano
- ne
- ne, ale kamarádovi (kamarádce) ano



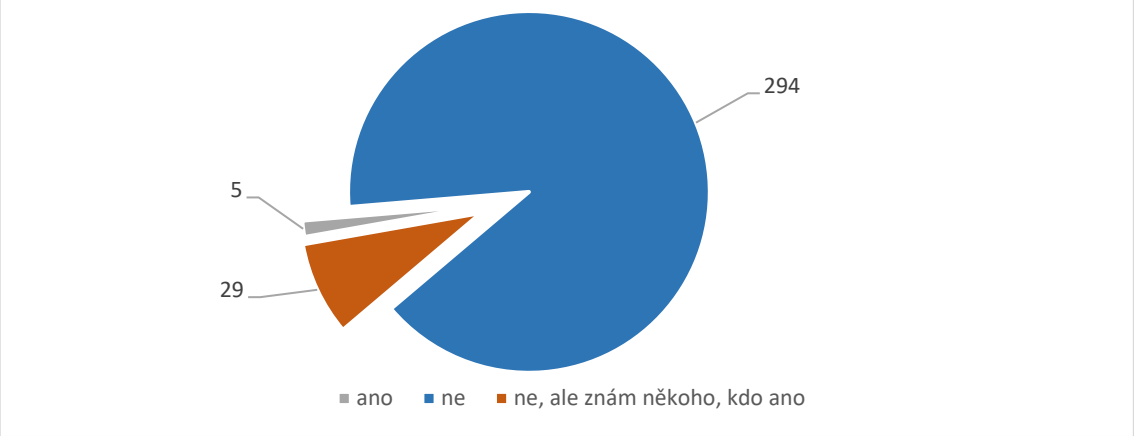
Obrázek 20 - Navazování bližšího kontaktu

Otázka č. 20 byla zaměřena na kybergrooming. Měla za cíl zjistit, zda se žáky základních škol pokoušel někdo neznámý kontaktovat prostřednictvím sociálních sítí a chtěl navazovat bližší kontakt. I když nelze konstatovat, že ve věci musí být okamžitě spatřováno nebezpečí kybergroomingu, i tato data jsou přínosem. Celkem 12 žáků z celkového počtu 328 respondentů uvedlo, že popsané jednání osobně zaznamenali a celkem 29 žáků uvedlo, že se toto jednání stalo jejich známému nebo kamarádce. V procentuálním vyjádření můžeme hovořit o 12,5 % žáků základních škol, kteří se setkali s navazováním kontaktu od neznámé osoby prostřednictvím sociálních sítí, což je rozhodně nebezpečně vysoký údaj. Mezi těmito osobami nemusí být nutně pachatel

trestného činu dle ustanovení § 193b TZ (Navazování nedovolených kontaktů s dítětem), ale také tam být může.

Otázka č. 21 - Sdělil(a) jste někdy neznámé osobě prostřednictvím sítě internet některý ze svých osobních údajů? (datum narození, heslo do internetové služby, telefonní číslo, své bydliště apod.)

- ano
- ne
- ne, ale znám někoho, kdo ano



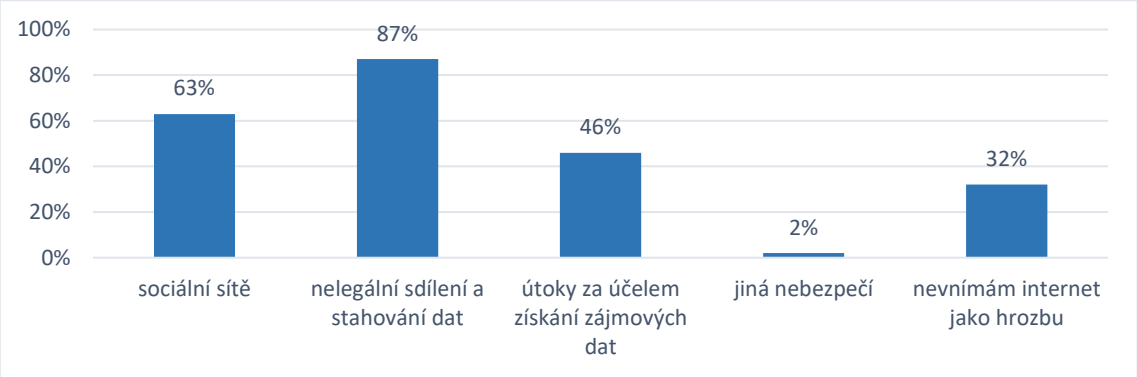
Obrázek 21 - Sdělování osobních informací neznámé osobě

Otázka č. 21 měla za cíl zjistit bezpečnost chování respondentů v síti internet. Vyhodnocením výzkumného šetření bylo zjištěno, že celkem 5 žáků zaslalo neznámé osobě prostřednictvím sítě internet některý ze svých osobních údajů a celkem 29 žáků někoho takového zná. Jedná se o vcelku zajímavý model, neboť co vede žáka základní školy k zaslání některého ze svých osobních údajů neznámé osobě? Je to ta dříve zjištěná snaha být populárním? Stane se obětí Phishingu nebo jde pouze nevědomost a neopatrnost? Zřejmě bude souviset jedno s druhým a opět je nutné zdůraznit a poukázat na účel a smysl prováděných besed. Před nástrahami v kyberprostoru je třeba děti varovat, nastínit jim skutečné příběhy z praxe a poté už jen doufat, že se právě ony nestanou obětmi kybernetických trestných činů.

V závěrečné části dotazníkového šetření byla očekávána trocha vlastní invence dětí. Záměrem bylo získat od dětí jejich vlastní nápady a názory.

Otázka č. 22 - Co vnímáte jako největší nebezpečí v síti internet? (možno označit více možností)

- sociální sítě
- nelegální sdílení a stahování dat
- útoky na počítače za účelem získání zájmových dat
- nebo jiná nebezpečí, vypište……
- nevnímám internet jako hrozbu



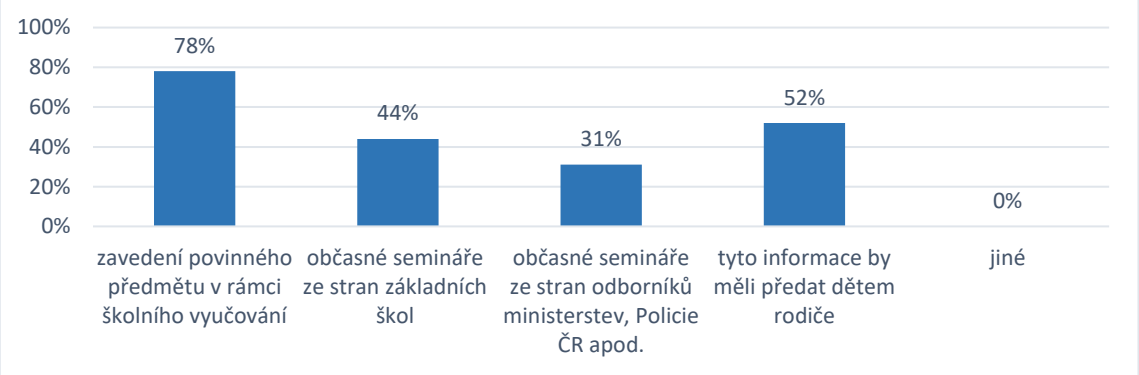
Obrázek 22 - Největší nebezpečí v síti internet

Otázka č. 22 měla za cíl zjistit, co vnímají mladí lidé jako největší nebezpečí v síti internet. Mnohdy totiž vnímané nebezpečí nekoresponduje s nebezpečím skutečným a zde to rozhodně platí také. Žáci základních škol v této otázce mohli volit více odpovědí a výsledky jsou následující. Jako největší nebezpečí v síti internet vidí v nelegálním sdílení a stahování dat. Tuto možnost zvolilo celkem 87 % žáků. Sociální sítě vidí jako největší hrozbu 63 % žáků, útoky za účelem získání zájmových dat 46 % žáků a volbu jiné nebezpečí zvolily celkem 2 % žáků. Zajímavým údajem je výsledek 32 % žáků, kteří neregistrují internet jako hrozbu. Téměř denně a téměř ve všech sdělovacích kanálech se dozvídáme o podvodných jednáních, sextingu, vydírání, ale jedna třetina oslovených žáků základních škol nevnímá v síti internet žádné nebezpečí.

A to rozhodně správné není. Vzhledem k výsledkům provedeného výzkumu nebyl očekáván v řádech jednotek procent tento výsledek.

Otázka č. 23 - Jak by podle Vás měla vypadat příprava na rizika spojená s užíváním internetu?

- zavedení povinného předmětu v rámci školního vyučování
- občasné semináře ze stran základních škol
- občasné semináře ze stran odborníků ministerstev, Policie ČR apod.
- tyto informace by měli předat dětem rodiče
- nebo jiné, vypište…….



Obrázek 23 - Příprava na zvládání rizik v síti internet

Otázka č. 23 měla za cíl zjistit, jak by měla vypadat příprava na rizika spojená s užíváním internetu z pohledu žáka základní školy. Otázka byla takto koncipována záměrně, neboť měla odhalit podobu prevence z pohledu této mladé generace osob školou povinných. Opět bylo možné vybrat více odpovědí a výsledky jsou následující. Celkem 78 % žáků se domnívá, že nejlepší prevencí by bylo zavedení nového povinného předmětu v rámci školní výuky. To překvapivým výsledkem není. Při diskuzi jevili žáci zájem a bylo vidět, že je problematika zajímá a baví. Celkem 52 % žáků se domnívá, že by měli tyto informace dětem předat rodiče. Vcelku zajímavý výsledek. Ovšem z policejní praxe je patrné, že rodiče v dané oblasti neexcelují o nic více než jejich děti. V podstatě by se dalo říct, že jsou téměř stejně náchylní k viktimizaci. Liší se jen předmět zájmu, kdy na dospělého člověka je cíleno spíše za účelem získání

finančních prostředků. Celkem 44 % žáků se domnívá, že by pomohly občasné semináře ze strany základní školy. I když jsou některá témata probírána v rámci občanské výchovy, zřejmě ne dostatečně. A celkem 31 % žáků se domnívá, že by měli semináře na školách provádět odborníci ze stran ministerstev a Policie ČR. Názory dětí na základních školách jsou rozhodně zajímavé.

Pokud bych měl jako autor výzkumného šetření a specialista v oblasti kybernetické kriminality nyní zhodnotit stav vědomostí žáků základních škol, tak tento je rozhodně neuspokojivý. A právě i na základě těchto informací došlo k verifikaci hypotézy č. 1, neboli *úroveň povědomí o kyberkriminalitě u dětí na vybraných základních školách ve Středočeském kraji není na dostatečné úrovni*. Zároveň byla na základě stejných informací verifikována hypotéza č. 2, neboli *nedostatečná informovanost žáků základních škol ve Středočeském kraji o kyberkriminalitě může mít za následek neopatrné jednání v síti internet.*

Po zpracování dotazníkového šetření byly se žáky základních škol realizovány besedy na základě jejich potřeb vyplývajících z dat dotazníkového šetření. Tato sezení probíhala v učebnách základních škol s interaktivní tabulí, na které byla promítána předem připravená prezentace. Besedy byly realizovány ze strany policisty zařazeného ve skupině kybernetické kriminality Praha venkov – západ a byla při nich vyžadována aktivní účast žáků. V průběhu besedy byly žákům přiblíženy nejčastější projevy kybekriminality doprovázené skutečnými případy z praxe a byly zodpovídány položené dotazy. Beseda trvala celkem dvě vyučovací hodiny a za tuto dobu získali žáci mnoho užitečných informací.

5.2.3 Prověření přínosu besedy

Třetím dílčím úkolem bylo prověřit přínos besedy testováním proškolených subjektů. Za účelem zachování stejného výzkumného vzorku bylo provedeno otestování žáků bezprostředně po realizaci besedy. V posledních 10 minutách

času proběhl test pozornosti a zkouška nově nabytých vědomostí. Test byl koncipován formou otázky: *„Jakých je 10 nejdůležitějších pravidel chování v síti internet?“*

Odpovědi žáků postupně sestavily následující soubor pravidel:

1. *Nikomu neposílej svou fotografii a už vůbec ne intimní! Svou intimní fotografii neposílej ani kamarádovi nebo kamarádce, neukládej ji v mobilu, na cloudu a ani nikde jinde!*
2. *Nedávej nikomu neznámému přes internet svou adresu, telefon ani jiné osobní údaje! Nevíš, kdo se skrývá za monitorem na druhé straně.*
3. *Pokud je nějaký problém, svěř se dospělému! VŽDY!*
4. *Nedomlouvej si schůzku přes internet, aniž bys o tom někomu řekl!*
5. *Neodpovídej na neslušné, hrubé nebo vulgární emaily a zprávy!*
6. *Chovej se na internetu tak, aby nedošlo ke zbytečnému eskalování situace!*
7. *Udržuj svá hesla v tajnosti a pravidelně je aktualizuj!*
8. *Neotevírej přílohy zpráv, které přišly od neznámého odesílatele!*
9. *Nevěř každé informaci, kterou získáš na internetu!*
10. *Pokud se dozvíš o závadovém jednání, neignoruj ho. Řeš ho! Nevzdávej se!*

Po sestavení předchozích pravidel byl učiněn dotaz, zda byla beseda přínosem či nikoliv. Žáci shodně uvedli, že spoustu věcí neznali a že jejich pohled na internet se nyní změní. Spokojeni byli také členové učitelského sboru, kteří často projevili zájem o další spolupráci, ať již při plánování obdobných besed pro mladší ročníky, tak besed na téma trestně právní odpovědnosti dětí.

Vzhledem k uvedenému lze konstatovat, že tato práce splnila svůj účel a je přínosným nástrojem pro naši mladou generaci. A i kdyby tato práce pomohla jen jedinému z nich nestát se obětí některého z kybernetických trestných činů, mělo to celé smysl.

5.2.4 Vyhodnocení účinnosti besedy pomocí SWOT analýzy

Čtvrtým dílčím úkolem bylo vyhodnotit účinnost besedy pomocí SWOT analýzy se zaměřením na rozdíly mezi městskými a venkovskými školami. Při plnění tohoto úkolu byl získán soubor sjednocených a vyhodnocených poznatků, které mohou sloužit jako podklady pro formulaci dalších směrů a zaměření prováděných besed.

V rámci této analýzy byly identifikovány silné stránky (Strenghts), slabé stránky (Weaknesses), příležitosti (Opportunities) a hrozby (Threats), které budou popsány v následující části diplomové práce. Při zkoumání těchto faktorů a jejich dosazování do kvadrantů SWOT matice bylo vycházeno z celé řady informací. Jedná se zejména o data získaná v rámci provedeného výzkumného šetření, informace získané během prováděných besed a materiály získané z konečného testování proškolených subjektů za účelem prověření přínosu besedy.

Tabulka 5 - Vyhodnocení účinnosti besedy pomocí SWOT analýzy

SWOT analýza		
Interní faktory	**Silné stránky (Strenghts)**	**Slabé stránky (Weaknesses)**
	• Odbornost a kvalifikovanost přednášejícího • Snadná dostupnost odborníka z praxe • Žádné finanční náklady pro školy	• Mnoho informací najednou • Neschopnost soustředění dětí • Nedostatek času vzhledem k obsáhlosti tématu
Externí faktory	**Příležitosti (Opportunities)**	**Hrozby (Threats)**
	• Získání základního přehledu o hrozbách v kyberprostoru • Získání velkého množství znalostí v krátkém čase • Získání odolnosti vůči hrozbám	• Nebezpečí zneužití informací k páchání trestné činnosti • Nezájem ze strany některých základních škol

Z provedené SWOT analýzy vyplývá hned několik významných skutečností. Jako první budou mapovány faktory interní povahy neboli faktory, které je možné ovlivnit. Mezi silné stránky tedy řadíme odbornost a kvalifikovanost přednášejícího. Vzhledem ke skutečnosti, že jsou besedy prováděny policejním komisařem zařazeným ve skupině kybernetické kriminality, lze jistě hovořit o odbornosti a nejvyšší možné kvalifikovanosti této osoby provádět besedy na téma kyberkriminality. Jsou uváděny případy z praxe a na nich je demonstrováno závadové jednání pachatele, ale také poškozeného. Vždy jsou shrnuty chyby poškozeného a poukázáno na důsledky z činu plynoucí. Další silnou stránkou je snadná dostupnost. Mnohdy jsme se setkali se situací, že školy mají objednány odborníky na daná témata i několik měsíců, a to již může být pozdě. Mezi hlavní povinnosti Policie ČR patří i působit preventivně. V případě oslovení ze strany školy dochází téměř k okamžité reakci a se školou je domluven co možná nejbližší možný termín besedy. Může tak probíhat preventivní výukový blok nebo může jít o reakci na již provedené závadové jednání. Policejní komisař se již setkal s oběma druhy žádosti o provedení besedy. Jako poslední silnou stránku je možné zmínit nulové finanční náklady pro školy. Policie ČR je státní organizací a jako taková nevyžaduje za své služby finanční odměnu. Policejní komisař prováděl besedy po dohodě se služebním funkcionářem, který má tímto na preventivní činnosti taktéž svou zásluhu. O přínosu a kvalitě prováděných besed hovoří dále zpětné vazby zástupců škol, které jsou přiloženy k práci jako příloha č. 3 a č. 4 – děkovné dopisy.

Mezi slabé stránky můžeme jednoznačně zařadit množství informací a nedostatek času. Délka jednotlivých besed vždy činila dvě nebo tři vyučovací hodiny s přestávkami. Celkem se tedy jednalo o hodinu a půl až dvě a čtvrt hodiny čistého času. Za tuto dobu museli žáci získat přehled o důležitých pojmech, nabýt povědomí o nejčastějších druzích kyberkriminality a závěrem dokázat popsat nejdůležitější zásady chování v kyberprostoru. I když je tato

doba vzhledem k obsáhlosti tématu velmi krátká, bylo zjištěna ještě jedna slabá stránka. Žáci základních škol nejsou schopni, ani po tuto krátkou dobu, plného soustředění. Také z tohoto důvodu byly navázány bližší vazby se zástupci škol a nejsou vyloučena opakovaní besed nebo případné nadstavbové semináře. Některé školy již byly navštíveny opakovaně a je plánována návštěva dalších.

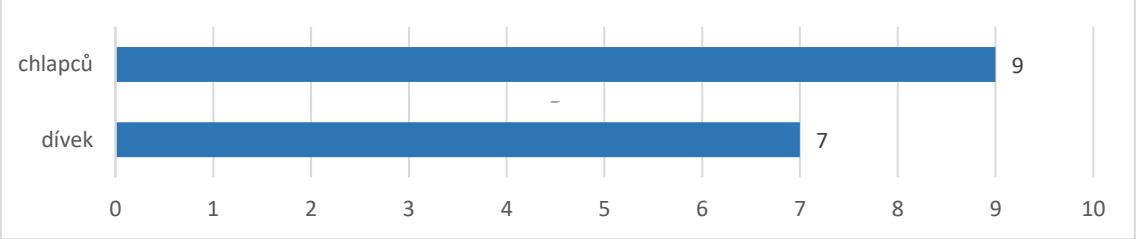
V druhé části se zaměříme na faktory externí povahy neboli faktory, které ovlivnit nemůžeme. Mezi příležitosti je tedy možné zařadit získání základního přehledu o hrozbách v kyberprostoru. Jak již bylo uvedeno, besedy jsou doprovázeny případy z praxe a snahou policejního komisaře je maximálně se přiblížit dětem a poskytnout jim informace v co možná nejsrozumitelnější formě. U praktických případů byl vždy patrný zvýšený zájem posluchačů, z čehož lze vyvodit vhodně volený směr diskuze. Z tohoto bodu dále vyplývá, že mohli žáci získat velké množství znalostí v krátkém čase a tudíž se mohly stát odolnějšími vůči hrozbám v kyberprostoru. Na základě získaných informací by měly být proškolené osoby schopny odhadnout nebezpečnost svého jednání v síti internet. Měly by být schopny nepodlehnout podvodům, vyvarovat se kyberšikaně, kybergroomingu a vždy si dobře promyslet zasílání intimních materiálů prostřednictvím internetu. Co si však žáci základních škol z celé besedy zapamatují nebo co budou dodržovat, záleží už jen na nich.

A konečně, mezi hrozby lze jednoznačně zařadit jisté nebezpečí vyplývající ze zneužití poskytnutých informací. Policejní komisař při besedách neposkytoval návody na krytí závadového jednání v síti internet, ale za účelem správného pochopení problematiky muselo být v několika případech demonstrováno jednání obou zúčastněných stran. Byly hledány chyby a špatná rozhodnutí u poškozené osoby a tyto mnohdy korespondují s chybami pachatele. Mezi další hrozbu bychom zařadili absolutní nezájem ze strany některých škol. V úplných začátcích předcházelo pořádání besed oslovování škol, zda mají o besedu na toto téma zájem, či nikoliv. Ač mají besedy

neoddiskutovatelný význam pro bezpečnost dětí v kyberprostoru, na jedné nejmenované základní škole se setkal policejní komisař s absolutním nezájmem ze strany odpovědné osoby z řad učitelského sboru. V této škole diskuze s dětmi doposud bohužel neproběhla.

Co se týče rozdílů v účinnosti provedených besed mezi městskými a venkovskými školami, tak tyto jsou naprosto zanedbatelné, a nelze je proto vyjádřit statistickými daty. Lidská společnost je rozdělena na ty, kteří důvěřují více škole městské a na ty, kteří upřednostňují školu venkovskou. I když by měly školy své žáky připravovat dle předem stanovených vytyčených stanov, existuje zde celá řada faktorů, které mohou mít na žáky zásadní vliv. K těmto jevům můžeme jednoznačně zařadit lidský faktor ve osobě pedagoga; rušivý element, ve formě nepřizpůsobivých žáků; velikost a odbornost učitelského sboru; umístění školy; počet žáků ve třídě a další. Policejním komisařem skupiny kybernetické kriminality nebyly mezi školami žádné rozdíly zjištěny. Byl patrný drobný rozdíl v přístupu, kdy žáci venkovských základních škol při besedách více spolupracovali, ale to může být dáno i počtem dětí ve třídách. Otestování žáků bezprostředně po realizaci besedy probíhalo ve svižném tempu a žáci prokázali, že si z besedy odnášejí spoustu cenných informací.

Daleko zajímavějším kritériem bylo zkoumat rozdíly mezi odpověďmi chlapců a dívek na klíčové otázky. Provedeným výzkumem bylo totiž zjištěno, že 9 chlapců a „jen“ 7 dívek již zaslalo v minulosti prostřednictvím sítě internet intimní materiál.



Obrázek 24 - Poměr zasílání intimních materiálů napříč pohlaví

V této části diplomové práce je vhodné opět poukázat na seriál inspirovaný skutečnými událostmi #martyisdead. I zde byl cílovou skupinou právě chlapec a ne dívka. Jedná se tedy o poměrně zajímavý jev. Znamená to tedy, že je navzdory našemu očekávání více cíleno na chlapce než dívky?

Tento závěr jsme se tedy pokusili ověřit policejními statistikami s následujícím výsledkem. V roce 2019 bylo spácháno celkem 45 deliktů, kde je poškozenou osobou dítě do 15 let viz *Tabulka 2 - Statistika kybernetických deliktů ve Středočeském kraji*. Z těchto 45 poškozených však bylo 27 dívek a „jen" 18 chlapců. Za účelem ověření správnosti naší teorie byl dále prověřen také rok 2018. V roce 2018 bylo spácháno celkem 28 deliktů, kde je poškozenou osobou dítě do 15 let viz zdroj výše. Z těchto 28 poškozených bylo 21 dívek a „jen" 7 chlapců. A jdeme dál. V roce 2017 bylo spácháno celkem 20 deliktů, kde je poškozenou osobou dítě do 15 let. Z těchto 20 poškozených bylo 16 dívek a „jen" 4 chlapci. Je samozřejmě nutné počítat se střední až vyšší mírou latence, ale i tak může jít o vyvrácení výsledku získaného výzkumným šetřením. Uvedená data jsou získána ze statistického vykazování Policie ČR Středočeského kraje se souhlasem služebního funkcionáře Praha venkov – západ. Tomuto jevu se budeme dále věnovat v závěru kapitoly *Diskuze*.

5.2.5 Provedení případových studií

Mezi další dílčí úkol bylo zařazeno provedení vhodných případových studií. Tento úkol byl zvolen záměrně, neboť v rámci uceleného náhledu do problematicky, je podstatné demonstrovat nebezpečí kyberprostoru také na praktických příkladech. V této části tak boudou popsány skutečné případy z praxe, které se dotýkají žáků základních škol. Vzhledem ke svému zaměření a rozsáhlosti, bude tento úkol podrobně popsán, prozkoumán a splněn v kapitole *Diskuze*.

5.3 Vyhodnocení stanovených hypotéz

V diplomové práci byly stanoveny celkem 4 hypotézy, které budou blíže popsány v následující části.

Hypotéza 1: *Úroveň povědomí o kyberkriminalitě u dětí na vybraných základních školách ve Středočeském kraji není na dostatečné úrovni.*

S touto hypotézou přímo souvisela otázka č. 3 a č. 4.

- V otázce č. 3 bylo zjišťováno, zda se respondenti domnívají, že již u osob jejich věku existují rizika při užívání celosvětové sítě internet. Bylo zjištěno, že celkem 90,2 % respondentů se domnívá, že ano, ale celkem 9,8 % se domnívá, že žádná rizika neexistují.
- Na otázku č. 3 přímo navazovala otázka č. 4, která měla za cíl oslovit pouze vzorek respondentů, kteří si rizika na internetu uvědomují. Tito respondenti byli dotazováni, zda jsou dostatečně připraveni na rizika spojená s užíváním celosvětové sítě internet. Bylo zjištěno, že celkem 50,3 % všech respondentů se domnívá, že ano a celkem 39,9 % všech respondentů se domnívá, že ne.

Na základě shora uvedených výsledků lze konstatovat, že došlo k jednoznačné verifikaci hypotézy č. 1.

Hypotéza 2: *Nedostatečná informovanost žáků základních škol ve Středočeském kraji o kyberkriminalitě může mít za následek neopatrné jednání v síti internet.*

S touto hypotézou přímo souvisela otázka č. 17 a č. 21

- V otázce č. 17 bylo zjišťováno, zda někdo z respondentů zaslal prostřednictvím internetu svojí intimní fotografii. Odpověďmi bylo zjištěno, že celkem 95,1 % respondentů nezaslalo prostřednictvím internetu svou obnaženou fotografii, ale alarmujících 4,9 % takovou fotografii již v minulosti někomu zaslalo.

- V otázce č. 21 bylo zkoumáno další neopatrné chování se v síti internet. Bylo zjišťováno, zda některý z respondentů sdělil v minulosti prostřednictvím sítě internet některý ze svých osobních údajů neznámé osobě. Bylo zjištěno, že celkem 98,5 % respondentů si počínalo v síti internet správně a osobní údaje neznámé osobě prostřednictvím sítě internet neznámé osobě nesdělilo. Naopak 1,5 % respondentů se doznalo k tomu, že se v minulosti tohoto jednání dopustilo. Dalších 3,7 % z 98,5 % respondentů přiznalo, že zná někoho, kdo se tohoto jednání dopustil.

Na základě shora uvedených výsledků lze konstatovat, že došlo k verifikaci hypotézy č. 2. I přes to, že se procenty vyjádřené výsledky mohou zdát zanedbatelné, v celých číslech již zanedbatelné nejsou.

Hypotéza 3: *Je možné informovanost žáků základních škol ve Středočeském kraji o kyberkriminalitě zlepšit řízenou diskuzí ze strany příslušníka Policie ČR.*

Hypotéza č. 3 přímo souvisí s jedním z dílčích úkolů diplomové práce. Jde o opětovné testování proškolených subjektů za účelem prověření přínosu a účinnosti besedy. Zjištěné výsledky jsou podrobně popsány v kapitole *Prověření přínosu besedy.*

Prověřením přínosu a účinnosti besed bylo zjištěno, že je možné povědomí o kyberkriminalitě ze strany příslušníka Policie ČR zlepšit, a tudíž došlo k verifikaci hypotézy č. 3.

Hypotéza 4: *Rozdíly v informovanosti žáků v městských a venkovských základních školách o kyberkriminalitě jsou minimální.*

Rozdíly v informovanosti žáků v městských a venkovských základních školách byly popsány v kapitole *Vyhodnocení účinnosti besedy pomocí SWOT analýzy*.

Výzkumným šetřením bylo zjištěno, že rozdíly v informovanosti žáků v městských a venkovských školách jsou skutečně minimální. Z tohoto důvodu je nutné konstatovat, že došlo k verifikaci hypotézy č. 4.

5.4 Doporučená opatření

Na tomto místě by bylo vhodné položit si několik zásadních otázek. Jak kyberkriminalitě páchané na dětech v České republice předcházet? Je možné rizikovému chování dětí v síti internet zabránit? Lze vymýtit útoky vedené na tyto děti? Na základě výzkumného šetření a praktických zkušeností jsme nuceni konstatovat, že způsob, jak úplně vymýtit kyberkriminalitu páchanou na dětech zatím neexistuje. Avšak počet obětí je za jistých okolností možné redukovat. Děti musí získávat informace o nebezpečnosti a škodlivosti některých chování v kyberprostoru opakovaně a nejlépe v rodině i ve škole. Z praktické zkušenosti policejního komisaře vyplývá, že obětmi jsou především děti bez jakékoliv předchozí přípravy na skrytá nebezpečí v síti internet. Dále bývá více než obvyklé, že také jejich rodiče jsou na tom se znalostmi obdobně, a nemohou tak své děti na nebezpečí připravit. A není se čemu divit. Kyberkriminalita je fenoménem dnešní doby a pokud se o problematiku dospělé osoby nezajímají z vlastní iniciativy, neorientují se. Nezdají se být dostatečné ani základy probírané v hodinách občanské výchovy v rámci povinné školní docházky. A nejsou dostatečné ani besedy prováděné policejním orgánem nebo zástupci jiných institucí. Těchto několik málo vyučovacích hodin během 9 let školní docházky jednoduše nemůže dostačovat. A vzhledem k uvedeným skutečnostem se nabízejí následující možnosti řešení.

Jedním z řešení by mohla být kontrola a cenzura internetu. Tímto směrem se například vydala komunistická Čína a již od února roku 2018 omezuje nezákonný obsah, a to včetně VPN (síťového tunelu umožňujícího například překonat omezení vázané na IP adresu dané země nebo služby). Toto řešení však v naší demokratické zemi spadá spíše do sekce „science fiction“.

K této otázce se ostatně vyjadřuje i autor Smekal svým tvrzením: *„Internet jako celek si nelze přivlastnit, ani jej ovládat“* (Smekal, 2015, s. 59). Bez ohledu na státní zřízení, zavedení tohoto řešení se v České republice nejeví jako příliš vhodné. Důvody můžeme spatřovat v absenci kontrolních mechanismů, v náročnosti na hardware, software, ve finanční stránce věci, a hlavně ve ztrátě svobody vyplývající ze základních kořenů našeho demokratického státu. Existují však vhodnější způsoby a tyto si představíme nyní.

Prvním reálným řešením by mohlo být přijetí nových pedagogů z řad odborníků a zavedení nového školního předmětu se zaměřením na bezpečnost a chování v kyberprostoru. Tento předmět by mohl být vyučován od druhého stupně základních škol s rozsahem dvě hodiny týdně. Policejní komisař je přesvědčený, že je téma nakolik obsáhlé, že by neměl být problém s jeho zařazením do povinných stanov v rámci školního vyučování.

Druhým a zároveň zřejmě nejvhodnějším řešením je rozšíření předmětu „informační technika“, který se již na základních školách vyučuje. Rozšíření by se týkalo právě bezpečnosti chování v kyberprostoru a opět by jej vyučovali ideálně odborníci z dané oblasti. Žáci by v předmětu získávali znalosti nejen z oblasti hardware a software, ale také z oblasti kyberprostoru a jeho bezpečnosti či spíše nebezpečnosti. Policejní komisař přepokládá, že k tomuto kroku musí dříve či později přistoupit i zástupci ministerstva školství a že toto rozšíření povinné školní docházky bude přínosem pro školy i jejich žáky. Pokud se na věc podíváme i z dlouhodobého hlediska, mělo by dojít ke zvýšení kybernetické gramotnosti u všech generací osob a k následnému poklesu kyberkriminality.

6 DISKUZE

Výzkumná část diplomové práce byla zaměřena na zjištění nejčastějších chyb, kterých se dopouštějí žáci základních škol při procházení sítě internet. Tyto nedostatky byly analyzovány a na jejich základě byl popsán způsob prevence závadového jednání, a to cestou řízené diskuze se žáky v celkem šesti základních školách ve Středočeském kraji. Beseda se žáky vyústila v konečné testování žáků s jasným závěrem, jak rizikovému chování předcházet. Účinnost besedy byla dále vyhodnocena pomocí SWOT analýzy se zaměřením na rozdíly mezi městskými a venkovskými školami. Vzhledem ke zjištěným zanedbatelným rozdílům byla pozornost upřena na daleko zajímavější prvek, a to jsou rozdíly v odlišném chování chlapců a dívek. Zjištěné výsledky byly dále porovnány se současnými televizními snímky inspirovanými skutečnými příběhy a dále s policejními statistikami. Výzkumná část vyústila v doporučená opatření, jak kyberkriminalitě páchané na dětech v České republice předcházet.

Tato diplomová práce je již od svého počátku zaměřena na děti školou povinné. Ovšem to neznamená, že nejsou ohroženy i generace jiné. Za účelem uceleného náhledu do problematiky je vhodné se krátce zmínit i o těchto. Na základě praktických zkušeností bych osobně zařadil poškozené osoby do celkem tří skupin. Do první skupiny bych zařadil děti školou povinné. Tato skupina osob nemá vesměs své bankovní účty a je na ně cíleno zejména za účelem zaslání intimních materiálů, viz tato diplomová práce. Druhou skupinou jsou mladí lidé v produktivním věku, mají zaměstnání, rodinu a svůj volný čas tráví svými koníčky a zábavou. Na tyto osoby je nejčasněji cíleno za účelem získání finančních prostředků. Konkrétně můžeme hovořit o Phishingu, neboli jednání se znaky Podvodu dle § 209 TZ. Tito lidé však většinou dobře ovládají informační a komunikační technologie a mají zájem o dění kolem sebe. Důležitým hlediskem je samozřejmě vzdělání a sociální zázemí, ale když opomeneme tento fakt, jde o osoby vůči této trestné činnosti

téměř imunní. Třetí skupinu osob jsou lidé po produktivním a až v důchodovém věku. Tito lidé již často nedokáží rozlišit skutečnost od fikce. Jsou důvěřiví a informačním a komunikačním technologiím nerozumí nebo rozumí jen z části. Na tyto osoby je opět cíleno za účelem získání finančních prostředků a tato skupina osob se stává, společně s dětmi, skupinou nejohroženější.

Tato práce se však i nadále bude věnovat naší mladé generaci osob, dětem školou povinných. V této části diplomové práce se zaměříme na shrnutí získaných výsledků s ohledem na cíle práce. Provedeme komparaci dat se zahraničními autory a rozebereme některé skutečné policejní případy z praxe.

Shrnutí vlastních zjištění a získaných výsledků

Píše se rok 2009 a lidé si konečně uvědomují potřeby zavedení nových skutkových podstat do zákona č. 140 z roku 1961. Kyberkriminalita pomalu nabírá na intenzitě, ale zákon trestního práva hmotného, který je více než 40 let starý, tato nová jednání neregistruje. Nový trestní zákoník, č. 40/2009, zavedl s účinností od 1. ledna 2010 v oblasti trestního práva hmotného řadu zásadních změn a již konečně reaguje na nově vzniklé hrozby. Ale jako by se zastavil čas také v jiných oblastech. Do dnešního dne není na základních školách bezpečnost internetu zařazena ve stanovách. Okrajově je zmiňována v hodinách občanské výchovy, ale toto téma si přeci zaslouží mnohem víc. Na základě získaných výsledků lze jednoznačně konstatovat, že děti na základních školách jsou na nástrahy kyberprostoru připraveny nedostatečně. Že by školství spoléhalo na rodinu? Z vlastní zkušenosti mohu s klidným svědomím sdělit, že rodina mnohdy spoléhá právě na školství. Měl by snad připravovat na tato nebezpečí otec vyučený jako automechanik? Nebo matka vyučená jako kuchařka? Neměly by mít všechny děti právo na stejné vzdělání jako třeba v případě matematiky? Položme si otázku. Je důležitější znát hlavní město Grónska nebo vědět, že nesmím prostřednictvím internetu nikomu zaslat své

osobní údaje nebo intimní materiály? Je třeba uvést, že se tímto nesnažím dělat z dětí nesvéprávné ovce. Ano, měly by to zřejmě vytušit samy. Ale proč tedy k tomuto závadnému jednání v hojné míře stále dochází?

Z provedeného výzkumného šetření bylo zjištěno, že povědomí dětí o kyberkriminalitě lze snadno zvýšit. A zvýšení tohoto povědomí se přeci musí zákonitě odrazit v bezpečnějším pohybu dětí v kyberprostoru. Čili nemůžeme rovnou hovořit o předcházení rizikovému jednání dětí v kyberprostoru? A neměl by to být právě cíl dnešní společnosti? Ovšem tím jediným prostředkem jsou v současnosti právě mnou prováděné besedy na základních školách. Vzhledem k jejich počtu a intenzitě je však nelze považovat za dostatečné a dostáváme se tedy opět k mnou navrhovanému opatření, viz následující.

V předchozí kapitole bylo nastíněno hned několik řešení našeho problému. Nejvhodnějším řešením by bylo zřejmě rozšíření předmětu „informační technika“, který je již na základních školách vyučován. Rozšíření by se týkalo bezpečnosti chování v kyberprostoru a jeho rozšíření by vyžadovalo přijmout do řad kantorů skutečně kvalifikované odborníky z praxe. Žáci by v předmětu získávali znalosti nejen z oblasti hardware a software, ale také z oblasti kyberprostoru a jeho nástrah. Netvrdím, že je to snadný úkol. Odborníky nebude lehké získat, ani vhodně ocenit, ale osobně tento směr vnímám jako jediný správný krok našeho školského systému. Vždyť naše děti jsou přeci naše budoucnost.

Srovnání se zahraničními autory

Nebezpečnosti v kyberprostoru si v dnešní době všímá celá řada významných autorů. Jsou publikovány knihy, vycházejí návody na chování se v síti internet nebo i letáky pro poškozené. Ale není tomu tak jen v České republice. Kybernetická kriminalita je celosvětovým problémem a v této části se

budeme věnovat komparaci našich pravidel chování se v kyberprostoru a pravidel sestavených dvěma univerzitními profesory ve Wisconsinu v USA.

Těmito profesory jsou Justin W. Patchin, Ph.D. a Sameer Hinduja, Ph.D., kteří strávili více než deset let studiem otázek souvisejících se zneužíváním informačních a komunikačních technologií vůči dětem. Na základě svých pozorování napsali několik knižních publikací a sestavili tzv. „desatero zásad pro děti" jak se chovat v mezních situacích – publikováno v knize Cyberbullying Prevention and Response. Některá jejich díla jsou volně ke stažení na známé webové stránce https://cyberbullying.org/, která je v provozu již od roku 2003 a která disponuje mnoha cennými informacemi, výzkumy a daty ke stažení. I když je toto „desatero" zaměřeno zejména na kyberšikanu, dá se stejně dobře aplikovat také pro jiná jednání.

V následující části si tyto zásady stručně představíme a provedeme porovnání s naším souborem pravidel, viz kapitola *Prověření přínosu besedy*. Soubor zásad od autorů výše je do českého jazyka přeložen volně a originál v anglickém jazyce se nachází v příloze č. 5.

1. *OZNÁMIT ŠKOLE – závadové jednání oznamte škole, byť anonymně;*
2. *DŮKAZNÍ PROSTŘEDEK – pořiďte snímek obrazovky, uložte obrázek, zprávu nebo zaznamenejte, co vidíte;*
3. *OZNÁMIT NA WEBU – existují služby pro hlášení závadového jednání;*
4. *OZNÁMIT DOSPĚLÉMU – může to být rodič, učitel, poradce, atd;*
5. *SOUDRŽNOST – ukažte poškozené osobě, že není sama. Pošlete jí povzbuzující text nebo snímek;*
6. *PRACUJTE SPOLEČNĚ – síla spočívá v počtu lidí. Povzbuzujte ostatní, aby pomohli nahlásit závadná jednání;*
7. *ZASTAVTE JEDNÁNÍ – pokud znáte osobu, která někomu ubližuje, vysvětlete jí, že se to dělat nesmí. Pokud mlčíte, s jednáním souhlasíte;*
8. *NEPŘIDÁVEJTE SE – pokud vidíte šikanu, jakkoliv ji nepodporujte;*

9. *CHOVEJTE SE BEZPEČNĚ – nezveřejňujte něco, co by mohlo díky emocím zbytečně eskalovat;*
10. *NEVZDÁVEJTE SE – vždy přemýšlejte o tom, co ještě lze udělat pro zastavení kyberšikany (Patchin, Hinduja, 2018).*

V podstatě by se dalo říct, že se, až na bod č. 5 a č. 6, kdy jsou žáci nabádáni ke společným akcím, soubor pravidel sestavený americkými profesory a spisovateli až příliš neliší od pravidel stanovených v této práci. Naopak vnímám náš soubor pravidel jako komplexnější a ucelenější vzhledem k cíli této práce. Jak již bylo uvedeno v úvodu, soubor pravidel od amerických autorů je spíše cílen na šikanu, a proto nelze poněkud užší zaměření amerických autorů vnímat jako nějakou chybu. Z mého pohledu je však škoda vydat odborné doporučení pro šikanu a nezahrnout do něho například sexting, který se šikanou velmi úzce souvisí.

V každém případě jsme v tomto porovnání zjistili, že naše cesta je správná a v naší preventivní činnosti nebyla opomenuta žádná důležitá skutečnost. Náš soubor pravidel je přímo cílen na žáky základních škol a nabádá k opatrnosti napříč všemi hrozbami v síti internet.

Závěrem této kapitoly by bylo vhodné provést jakési zhodnocení předchozího zjištění. V podstatě by se dalo říct, že zjištění korespondují s očekáváním. Žáci základních škol mají o hrozbách v kyberprostoru nedostatečné vědomosti a dopouštějí se tak zbytečných a mnohdy fatálních chyb. Často nevědí, co považovat za skutečnost a co za fikci, co je správné a co by se naopak dělat nemělo. Mají zkreslené představy o reálném světě a jsou důvěřiví k neznámým lidem. Naopak musím poznamenat, že žáky problematika kyberprostoru zaujala a jsou schopni o aktuálních tématech sami hovořit a svěřit se s problémy. Je to jeden z dalších důvodů, proč posílit výuku za základních školách tímto směrem. Děti jsou schopny správně reagovat na hrozby, jen je nutné je o hrozbách nejprve informovat.

Případové studie

Za účelem naplnění další dílčího úkolu, byly do práce zahrnuty vhodné případové studie. V této části tak boudou popsány skutečné případy z praxe, které přímo souvisí s nebezpečím pro žáky základních škol.

Denně jsou v České republice spáchány desítky, ne-li stovky kybernetických útoků, a to ve všech různých formách, viz předchozí kapitoly. Díky obavám ze sekundární viktimizace a strachu z odsouzení blízkého okolí, bývá oznámeno orgánům činným v trestním řízení jen malé procento z nich. Jistou roli hraje také nedůvěra v Policii ČR a anonymita kyberprostoru. Vyšetřování kybernetických zločinů je velmi složité, ale zjištění pachatele není mnohdy nemožné. Předmětem této kapitoly je převedení výše uvedených teoretických dat na skutečné případy z praxe. V úvodu je třeba zmínit, že dle ustanovení § 115 zákona č. 273/2008 Sb. (Zákon o policii ČR) *„policista nebo zaměstnanec policie jsou povinni zachovávat mlčenlivost o skutečnostech, se kterými se seznámili při plnění úkolů policie nebo v souvislosti s nimi, a které v zájmu zabezpečení úkolů policie nebo v zájmu jiných osob vyžadují, aby zůstaly utajeny před nepovolanými osobami. Tato povinnost trvá i po skončení služebního nebo pracovního poměru.“* A z tohoto důvodu jsou veškeré osobní údaje, jména, města a další data, která by mohla vést k odhalení těchto skutečností smyšlená. Případy jsou však skutečné a je na nich možné prezentovat naivitu mladých lidí, nedostatky v jejich povědomí, neopatrnost při pohybu v kyberprostoru a nebezpečnost takového jednání ze strany pachatele.

Případová studie s jednáním se znaky sextingu a vydírání

Dne 18. dubna 2015 se dostavila na Obvodní oddělení Policie České republiky Hostivice paní Olga Nováková za doprovodu své dcery Marie Novákové. Marie je žačkou deváté třídy základní školy, a právě dovršila věku 15 let. Paní Olga Nováková uvedla, že nalezla v tabletu své dcery komunikaci s nějakou

dívkou jménem Zuzana Slavíková, která po Marii vyžadovala zaslání obnažených fotografií. Dcera Marie se matce přiznala, že této osobě zaslala jednu fotografii v podprsence, a to prostřednictvím sociální sítě Facebook. Tuto fotografii však již z komunikace odstranila a nelze ji již dohledat. Na základě povinnosti vyplývající ze zákona č. 141/1961 Sb. (Zákona o trestním řízení soudním) byla věc policisty řádně zadokumentována a byla cestou mezinárodní spolupráce vyžádána kompletní záloha účtu s uživatelským jménem „Zuzana Slavíková“ (dále pachatel) od spol. Facebook. V této části je třeba poznamenat, že soud v České republice přikazuje společnosti v USA k vydání zájmových dat. Už z tohoto je patrné, že vše funguje pouze na základě mezinárodních dohod a neplatí zde lhůty na vyřízení žádosti. Obdobně jako Facebook i další velké společnosti odpovídají na žádosti na základě škodlivosti jednání. V jiné lhůtě tedy bude vyřízena žádost týkající se dětské pornografie a v jiné lhůtě bude vyřízeno podezření z pomluvy. V tomto konkrétním případě spol. Facebook vyhodnotila událost jako případ s nízkou prioritou a odpověď se zájmovými daty dorazila až 10. června 2017, tj. po více jak dvou letech od oznámení! Konkrétně byly doručeny dva DVD disky s obsahem pornografických materiálů dívek mladších 15 a 18 let. Z těchto materiálů bylo zjištěno, že k závadovému jednání docházelo od února roku 2015 do března roku 2017. Tudíž byla Marie Nováková jednou z prvních poškozených v dané věci. Po řádném prostudování a analýze získaných dat bylo zjištěno, že pachatel vždy nalezl na sociální síti Facebook mladou dívku s vyplněnými profilovými informacemi (přátelé, zájmy, místa) a tuto zkontaktoval za účelem dopisování. Tato komunikace probíhala několik týdnů i měsíců v naprostém pořádku. Když však pachatel pojal pocit, že již získal dostatečnou důvěru, „svěřil“ se s problémem nedostatečně vyvinutých ňader. Po následném dopisování přikročil pachatel k dalšímu kroku. Zaslal poškozené k posouzení fotografii obnažených dívčích ňader s tím, že jsou to ňadra Zuzany Slavíkové. Následovalo ujišťování ze strany poškozené, že jsou ňadra hezká,

ale to pachateli logicky nestačilo. Jeho hlavním záměrem bylo získat obnaženou fotografii poškozené. Provedenou analýzou dat bylo zjištěno, že již v tuto dobu některé dívky přestaly komunikovat. A to lze považovat za rozhodně správný postup. Většina dívek však neregistrovala nebezpečí a fotografii zaslala. V několika případech pachatel pokračoval ve své roli a vyžadoval fotografie další. V jiných případech už vyžadoval fotografie přímo. Z kamarádky Zuzany Slavíkové se tak stala doslova noční můra a dívky musely plnit její příkazy, pod pohrůžkou zveřejnění intimních záběrů.

V dané věci je třeba shrnout několik poznatků. Poškozenými byly desítky dívek osmých a devátých tříd základních škol. Mezi obnaženými fotografiemi byla i nahá fotografie poškozené Marie Novákové. Pokud by tedy uvedla pravdivé informace, jednalo by se o případ s vysokou prioritou a poškozených dívek by mohlo být mnohem méně. Pachatel páchal své protiprávní jednání více jak dva roky a za tuto dobu získal více jak 5 GB zájmových dat. Pachatele se Policii ČR podařilo ustanovit, psychickou újmu dívek však vynahradit nelze.

Případová studie s jednáním se znaky kyberšikany

Jak již bylo zmíněno v předchozí kapitole, zodpovědnost v otázce prevence před šikanou nebo před kyberšikanou leží zejména na rodině a škole, nikoliv na orgánech činných v trestním řízení. Trestný čin šikany trestní zákoník nezná, ale dle povahy jednání je možné tato jednání kvalifikovat jako trestný čin Vydírání (§ 175 TZ), Loupeže (§ 173 TZ), Ublížení na zdraví (§ 146 TZ) nebo Poškozování cizí věci (§ 228 TZ). Když se však orgány činné v trestním řízení o takovém jednání dozvědí, zahajují úkony v trestním řízení (z povinnosti vyplývající ze zákona č. 141/1961 Sb. viz výše). Důkazem tohoto je případ, který se udál v roce 2019. Dne 14. října 2019 se dostavil na Obvodní oddělení Policie České republiky v obci Řevnice pan Zdeněk Macháček za doprovodu svého syna Lukáše Macháčka. Lukáš je ve věku 14 let, je žákem osmé třídy základní školy a stal se obětí šikany a kyberšikany. Oznamovatel Zdeněk Macháček

uvedl, že je jeho syn opakovaně týrán ze strany spolužáků a ani rodiče, ani škola tomuto jednání opakovaně nezabránili. Jednání spočívá v nucení pod pohrůžkou násilí, aby jeho syn něco konal. Dále docházelo ke krádežím jeho svačiny a školních pomůcek a k zesměšňování jeho syna na internetu. Lukáš Macháček je při tomto týrání natáčen a poté jsou videa k pobavení žáků umísťována do soukromých skupin na sociálních sítích.

V dané věci je třeba shrnout několik poznatků. Jednoznačně došlo k selhání v rodinném prostředí podezřelých. Můžeme zde spatřovat také jisté selhání v prostředí školy, neboť právě pedagog by měl tato jednání zpozorovat jako první. Popsaná jednání vykazují znaky hned několika trestných činů, a i když bude nízký věk podezřelých hrát významnou roli, oznámení skutku Polici ČR bylo správné řešení. A konečně, zjištění pachatelů v tomto případě není složité. Závěrem je třeba konstatovat, že tento případ je něčím zvláštní. Předchozí případová studie popisovala situaci, kdy je dítě týráno prostřednictvím internetu a dítě totožnost tyrana nezná. Samozřejmě není vyloučen fakt, že pachatel svou oběť zná, ale to je věcí jinou. V našem případě je totožnost pachatelů známa. Jedná se tedy o nezvratný důkaz, že krutého a nemilosrdného jednání není schopna pouze cizí osoba. Tohoto jednání jsou schopni také žáci základních škol a je velice důležité na to nezapomínat.

Případová studie s jednáním se znaky podvodného jednání

Dne 23. května 2019 se na Obvodní oddělení Policie České republiky Mníšek pod Brdy dostavil pan Petr Brabenec za doprovodu svého syna Tomáše Brabence. Tomáš je ve věku 14 let žákem osmé třídy základní školy a stal se obětí podvodu. K celé události došlo dne 12. května 2019 a závadové jednání proběhlo prostřednictvím sociální sítě Facebook. Dne 12. května 2019 kolem 18:00 hod. obdržel Tomáš Brabenec žádost o přátelství od svého spolužáka Petra Strejce. Petr již měl založený účet na sociální síti Facebook několik let, ale nyní zaslal novou žádost o přátelství se zprávou, že svůj starý účet ruší

a že již bude k zastižení pouze zde. Tomáš přijal nový účet mezi své přátele a starý účet odstranil. Následně spolu začali komunikovat a komunikace probíhala asi 30 minut o obecných věcech. Po této době byl Tomáš dotázán na telefonní číslo otce. Petr Strejc (dále pachatel) svou žádost odůvodnil tím, že by rád měl na svého nejlepšího kamaráda ještě jedno číslo. Tomáš telefonní číslo pachateli sdělil a opět komunikovali, ale tentokrát přímo o online hraní her. Asi o dalších 20 minut později pachatel napsal Tomášovi, že na číslo otce nechal vygenerovat nějaký kód z online hry Counter-Strike a že si mohou zahrát. Tento kód mu ale musí Tomáš poslat, aby mohli být ve stejném týmu. Tomáš tedy skutečně šel, půjčil si otce telefon a přijatý kód poskytl pachateli na druhé straně. Pachatel na základě tohoto kódu uskutečnil nákup jedné z online služeb za bezmála 3 tisíce korun ku škodě otce Petra Brabence.

V dané věci je třeba shrnout několik poznatků. Tomáš Brabenec se spolehl na slovo spolužáka, aniž by ho viděl nebo příběh ověřil. Tomáš Brabenec poskytl této osobě telefonní číslo otce, a dokonce mu zaslal i obdržený ověřovací kód. Dále, Petr Brabenec měl svůj mobilní telefon mimo svůj dosah. Pachatele shora uvedeného skutku se policistům doposud vypátrat nepodařilo.

Na zmíněných případech je patrné, že vylákání zájmových dat od mladých lidí není nikterak složité. Ale proč tomu tak je? Také na toto téma byl proveden pod záštitou již zmíněného online seriálu #martyisdead rozhovor s mužem, který zneužil 39 dětí. Rozhovor je dostupný online na internetové televizi mall.tv a končí vyvozením obdobných závěrů, na které poukazuje i tato práce. Nedostatek povědomí, nedostatek zkušeností, důvěřivost, strach, pohodlnost nebo nezájem o dění kolem a vliv okolí. To vše dělá z dětí základních škol až příliš snadné cíle, a to nejen pro páchání kybernetické trestné činnosti. Rozhovor s tímto mužem moderuje Luděk Staněk, který je známý především z pořadu Události Luďka Staňka.

Předmětem rozhovoru je následující skutek: *„Mezi roky 2007 a 2012, dva tehdy skautští vedoucí, pod skautskými přezdívkami „Piškot“ a „Meluzín“ zneužili dohromady 39 obětí ve věku 12 až 18 let. Obžaloba jim prokázala, že kontaktovali desítky chlapců prostřednictvím internetu, na sociálních sítích se vydávali za dívky a posílali jim nahé fotografie. Následně od nich požadovali snímky a videa zachycující chlapce při masturbaci. Na základě získaných záznamů pak chlapce vydírali a některé nutili k sexu. Podle rozsudku některé nezletilé chlapce znásilnili, a to opakovaně. Oba byli odsouzeni k deseti letům vězení. Po 2/3 požádal jeden z dvojice, „Meluzín“ o prominutí zbytku trestu, v čemž mu soud koncem loňského roku vyhověl.“*

Rozhovor s odsouzeným mužem je v délce asi 40 minut a přináší šokující svědectví muže, který oslovil až tisíc obětí prostřednictvím sociálních sítí. Na videu popisuje způsoby a sofistikovanost svého jednání, aby získal zájmová data. V rozhovoru dále uvádí, že je daleko snadnější cílit na chlapce než dívky, neboť právě chlapci jsou ochotni zaslat intimní materiály častěji. Tohoto jevu jsme si také všimli vyhodnocením výzkumného šetření. Naprosto šokující je také závěr rozhovoru, kdy na přímo položenou otázku, zda se dokáže vžít do svých obětí uvádí: „*myslím si, že tohle těžko pachatel pochopí.*“ A právě zmíněný rozhovor byl inspirací k natočení zmíněného seriálu #martyisdead. Tento seriál, rozhovor s odsouzeným a potažmo také tato diplomová práce, by měla v konečném důsledku sloužit jako materiál k prevenci před ohavnostmi páchanými na našich dětech.

V souvislosti s naší problematikou je vhodné zmínit ještě jeden aktuální projekt. Tímto projektem je dokumentární film od koproducenta a mediálního partnera České televize „V síti“. Na webových stránkách csfd.cz (Česko–Slovenská filmová databáze) je snímek popsán následovně: „*3 herečky, 3 pokojíčky, 10 dní a 2458 potenciálních sexuálních predátorů. Tři dospělé herečky s dětskými rysy se vydávají na sociální sítě, aby v přímém přenosu prožily zkušenost dvanáctiletých dívek online. Ve věrných kopiích dětských pokojů chatují a skypují*

s muži, kteří je na netu aktivně vyhledali a oslovili. Drtivá většina těchto mužů požaduje sex přes webkameru, posílá fotky svých penisů a odkazy na porno. Děti jsou dokonce vystaveny vydírání. Predátorské taktiky se postupně obracejí proti svým strůjcům: Z lovců se stávají lovení".

Za 10 dní, 2458 sexuálních predátorů. Jedná se o děsivá čísla? Rozhodně ano! V době vzniku této diplomové práce výše zmíněný dokumentární film neexistoval. Dokonce jsem nezaznamenal ani náznak toho, že by se podobný projekt chystal. Dokumentární film V síti měl být ve svém zrodu pouze krátkým reklamním spotem. Jenže realita je tak šokující, že dostal daleko větší prostor. Snímek jako jeden z mála zachycuje skutečná nebezpečí 21. století pro naše děti v celovečerním filmu. Možná také proto se těší enormnímu zájmu a vysloužil si od diváků hodnocení 91 %.

Na tento dokument zareagovaly také školy. Za poslední měsíc byl zaznamenán enormní nárůst žádostí o provedení besedy se žáky. Že by si lidé konečně uvědomili, co se skutečně děje? Bude už konečně na tyto hrozby reagovat i náš školní systém? A dostane bezpečnost v kyberprostoru více prostoru i na základních školách? To nyní nelze předpovědět, ale osobně se domnívám, že jsme na dobré cestě. Dokumentární snímek V síti je jen dalším podpůrným důkazem našeho tvrzení. Tvrzení, že jsou naše děti v ohrožení. Že je třeba na tato nebezpečí již reagovat. A že již včera bylo pozdě.

Přes všechna naše očekávání bychom rádi v závěru poukázali ještě na jeden zajímavý aspekt. Provedeným výzkumným šetřením bylo zjištěno, že chlapci jsou ochotni zaslat intimní materiály častěji než dívky. Tento závěr by také podpořen rozhovorem s mužem, který zneužil 39 dětí a jehož případ byl inspirací k natočení seriálu #martyisdead. I tento muž, se skautskou přezdívkou „Meluzín" uvádí, že navzdory své sexuální orientaci cílil na chlapce. Důvodem byl fakt, že právě u chlapců je získání intimních materiálů snadnější než získání intimních materiálů od dívek. Ovšem dokumentární snímek V síti počítá

s obětmi pohlaví ženského. Za 10 dní, 2458 sexuálních predátorů. To je faktický údaj snímku V síti. Ale ani jeden sexuální predátor neobdržel intimní fotografii dívky. Ano, jedná se o děj nahraný a dle scénáře, ale jaká je skutečná úspěšnost takového sexuálního predátora získat od dívky intimní materiály? Pachatel „Meluzín“ uvádí, že nízká. Tak kdo je vlastně tou ohroženější skupinou osob? Jsou to chlapci nebo dívky? Policejní statistiky hovoří jasně, v žebříčku registrované kriminality dominují dívky. Ale co když chlapci jen tato jednání neoznamují. Co když se orgány činné v trestním řízení o těchto jednáních jednoduše nedozví? Tyto otázky by zcela určitě zasloužily bližší prozkoumání. Osobně si dovedu představit rozsáhlé výzkumné šetření na všech základních školách v České republice s jasně vyvozenými závěry. Myslím, že tento cíl by mohl být dobrým základem pro zpracování přínosné rigorózní práce.

7 ZÁVĚR

Hlavním cílem této práce bylo najít cestu. Způsob, jak ochránit děti tam, kde selhává rodina, škola, stát. Učinit žáky základních škol odolnějšími vůči nástrahám kyberprostoru a docílit zvýšení gramotnosti v dané oblasti. Odvážím se tvrdit, že na základě prováděných besed na šesti základních školách ve Středočeském kraji došlo k prokazatelnému zvýšení povědomí o kyberkriminalitě a spokojenost ze strany školních zařízení je patrná i z ocenění ve formě děkovných dopisů. A tato práce je jen malou ukázkou toho, že tato cesta je správná.

Výzkumným šetřením bylo zjištěno, že největšími chybami bývají nedostatky v kybernetické gramotnosti a až přílišná důvěra. Takto mladí lidé jsou poté zataženi do noční můry, ze které nevidí východisko. Jsou bezradní, nedokáží věc správně vyhodnotit a jsou schopni se pod pohrůžkou zveřejnění již dříve zaslaných materiálů podvolovat pachateli i opakovaně. Pokud by po návštěvách v základních školách mělo v hlavách žáků zůstat jen jedno jediné pravidlo, toto zní následovně: „AŤ JIŽ MÁŠ JAKÝKOLIV PROBLÉM, VŽDY SE SVĚŘ DOSPĚLÉ OSOBĚ“. Toto pravidlo provázelo celou besedu a bylo i hlavním výstupním bodem celého vyhodnocení účinnosti.

V řadách Policie České republiky působím již více než 18 let. Tuto práci jsem si zvolil již na střední škole a cítím ji jako své poslání. Za svou kariéru jsem se setkal s mnoha šťastnými, ale i smutnými konci. Není nic horšího než oznamovat rodičům smrt vlastního dítěte. A také až smrtí můžou končit některé extrémní kybernetické útoky vedené na naše děti. Ve své práci budu proto i nadále pokračovat. I nadále budu provádět besedy na základních školách a pokud konečně začne naše školství na tyto hrozby reagovat, rád přeorientuji svoji kariéru tímto směrem. Vždyť co je víc než naše děti?

8 SEZNAM POUŽITÝCH ZKRATEK

ICT - Informační a komunikační technologie

TCP – Transmission Control Protocol

IP- Internet Protocol

DHCP - Dynamic Host Configuration Protocol

DNS – Domain Name System

ČSU – Český statistický úřad

PČR – Policie České republiky

ÚO – Územní odbor

TZ – Trestní zákoník č. 40/2009Sb.

ČŠI – Česká školní inspekce

VPN - Virtual Private Networks

9 SEZNAM POUŽITÉ LITERATURY

Monografie

1. ČÍRTKOVÁ, Ludmila. Moderní psychologie pro právníky. Praha: Grada Publishing, 2008. Stalking, s.1-150. ISBN 978-80-247-2207-8
2. HAVELKA, Jiří a kol. Výkladový slovník výpočetní techniky a komunikací. 1. Vyd. Praha: Computer Press, 1997. ISBN 80-7226-023-5.
3. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti. [online]. 3. aktualizované vydání Praha: AFCEA, 2015. ISBN 978-80-7251-397-0. Dostupné z: http://afcea.cz/cesky-slovnik-pojmu-kyberneticke-bezpecnosti/.
4. KOLOUCH, Jan, Cyber Crime, Praha: CZ.NIC, z.s.p.o, 2016, ISBN 978-80-8816-815-7.
5. KUCHTA, J., & VÁLKOVÁ. H. Základy kriminologie a trestní politiky. Praha: C. H. Beck, 2005. ISBN 80-7179-813-4.
6. KUCHTA, Josef a kol. Kurs trestního práva. Trestní právo hmotné. Zvláštní část. Praha: C. H. Beck, 2009. ISBN 978-80-7400-047-8.
7. PATCHIN, J. W. & HINDUJA, S., 2012, Cyberbullying Prevention and Response, ISBN: 978-0415892377.
8. POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kolektiv. Elektronické důkazy v trestním řízení. Brno: Masarykova univerzita, Právnická fakulta, 2015. ISBN 978-80-210-8073-7.
9. SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s. Pro praxi. ISBN 978-80-7380-501-2
10. ŠÁMAL, Pavel a kol. Trestní zákoník II. § 140 až 421. Komentář. 2. vyd. Praha: C. H. Beck, 2012. ISBN 974-80-7400-4285.
11. ZAVRŠNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017, ix, 135. Právní monografie. ISBN 978-80-7552-758-5.

Zákony

1. Zákon č. 273/2008 Sb., o Policii České republiky
2. Zákon č. 140/1961 Sb., trestní zákon (zrušen ke dni 01.01.2010)
3. Zákon č. 141/1961 Sb., o trestním řízení soudním
4. Zákon č. 40/2009 Sb., trestní zákoník

Články

1. Kvalita a efektivita vzdělávání a vzdělávací soustavy ve školním roce 2017/2018: Výroční zpráva České školní inspekce [online]. 2018, 2018(978-80-88087-20-5) [cit. 2019-10-22]. Dostupné z: https://www.csicr.cz/Csicr/media/Prilohy/Obr%C3%A1zky%20ke%20%C4%8Dl%C3%A1nk%C5%AFm/2018/Vyrocni-zprava-CSI-2017-2018_final-verze.pdf.
2. Kvalita a efektivita vzdělávání a vzdělávací soustavy ve školním roce 2018/2019: Výroční zpráva České školní inspekce [online]. 2019, 2019(978-80-88087-23-6) [cit. 2020-03-01]. Dostupné z: https://www.csicr.cz/Csicr/media/Prilohy/PDF_el._publikace/V%c3%bdro%c4%8dn%c3%ad%20zpr%c3%a1vy/VZ-CSI-2018-2019.pdf.
3. Více než polovina Čechů používá sociální sítě [online]. Praha: Český statistický úřad, 2018 [cit. 2019-10-15]. Dostupné z: https://www.czso.cz/csu/czso/vice-nez-polovina-cechu-pouziva-socialni-site
4. Výzkum rizikového chování českých dětí v prostředí internetu [online]. 2013, 2013 [cit. 2019-10-22]. Dostupné z: http://www.bezpecnyinternet.cz/kestazeni/bezpecny_internet_prezentace.pdf

Elektronické zdroje

1. #martyisdead [online]. mall.tv: nic.cz, 2019 [cit. 2020-02-16]. Dostupné z: https://www.mall.tv/martyisdead?gclid=Cj0KCQiA7aPyBRChARIsAJfWCgJzGbto4ZEVWxltNjUDXdQ7VTYElnbFFM0xqQsogx7-xW0oo3p_k_8aAqQqEALw_wcB
2. BBC. Amanda Todd: Memorial for teenage cyberbullying victim. 17. 10. 2012. [cit. 15. 10.2019] Dostupné z: http://www.bbc.co.uk/newsbeat/article/19960162/amanda-todd-memorialfor-teenage-cyberbullying-victim
3. PATCHIN, J. W. & HINDUJA, S., Tanding up to Cyberbullying: Top Ten Tips for Teens. Https://cyberbullying.org/ [online]. 2018, 2018, , 1 [cit. 2020-02-28]. Dostupné z: https://cyberbullying.org/standing-up-to-cyberbullying-tips-for-teens
4. Šikana: Rodiče pozor! Šikana mezi dětmi je skryté nebezpečí! [online]. Praha: PČR, 2019 [cit. 2019-10-15]. Dostupné z: https://www.policie.cz/clanek/preventivni-informace-sikana.aspx
5. V síti. Česko-Slovenská filmová databáze [online]. Česko, 2020 [cit. 2020-03-09]. Dostupné z: https://www.csfd.cz/film/720753-v-siti/prehled/

10 SEZNAM POUŽITÝCH OBRÁZKŮ

11 SEZNAM POUŽITÝCH TABULEK

12 SEZNAM PŘÍLOH

Příloha 1 – dotazník prověřující znalosti o kyberkriminalitě na zákl. školách

Příloha 2 – výsledek šetření ČSU k využívání internetu/sociálních sítí r. 2018

Příloha 3 – děkovný dopis ze Základní školy Velké přílepy

Příloha 4 – děkovný dopis ze Základní školy Smečno

Příloha 5 – Top Ten Tips for Teens (desatero zásad pro děti)

Příloha 1

Pro vypracování dotazníku je zapotřebí označit vždy pouze jednu odpověď, vyjma otázek č. 9, 13, 22 a 23, kde je možno označit odpovědí více. V případě, že se jedná o otázku s možností doplnění odpovědi, snažte se psát stručně a výstižně. Závěrem upozorňuji, že žádná z odpovědí není špatná a výsledek pouze vystihuje Váš osobní názor. Děkuji za spolupráci.

1. **Pohlaví**
   - □ žena
   - □ muž
2. **Jak zdatně si počínáte v síti internet?**
   - □ internet používám na práci a zábavu a jsem zdatným uživatelem
   - □ internet používám, ale pouze na sociální sítě
   - □ internet používám sporadicky, moc se v něm neorientuji
3. **Myslíte si, že již u osob Vašeho věku existují rizika při užívání celosvětové sítě internet?**
   - □ ano
   - □ ne
4. **Pokud ano, jste dostatečně připraveni na tato rizika (nástrahy)?**
   - □ ano
   - □ ne
5. **Kolik času denně strávíte online?** (weby, sociální sítě, …)
   - □ do 1 hodiny
   - □ 2 – 3 hodiny
   - □ 3 hodiny a více
6. **Jste uživatelem nějaké sociální sítě?**
   - □ ano, jsem uživatelem více sociálních sítí
   - □ ano, pouze jedné
   - □ nevím, co je sociální síť
   - □ nejsem uživatelem

7. **U jaké činnosti na internetu trávíte nejvíce času?**

- □ procházení internetu, čtení článků a novinek apod.
- □ procházením sociální sítě (sítí)
- □ hraním online her
- □ u jiné činnosti, popište ……

8. **Setkali jste se již s termínem kyberkriminalita/PC kriminalita?**

- □ ano
- □ ne

9. **Setkali jste se někdy s následujícími termíny?** (pokud ano, tyto označte)

- □ Phishing
- □ Ransomware
- □ Malware
- □ Podvodné stránky
- □ Spam
- □ Hoax
- □ Cracking
- □ Hacking
- □ DoS, DDoS
- □ Sniffing

10. **Pokusil se Vás někdo neznámý uvést prostřednictvím internetu v omyl podvodnou nabídkou, výhrou nebo žádostí o pomoc apod.?** (na vzniklé škodě, nebo zda jste na toto jednání reagovali, nezáleží)

- □ ano
- □ ne

11. **Nalezli jste na internetu nějakou nepravdivou informaci nebo podvodnou webovou stránku?**

- □ ano
- □ ne

12. **Upozornil Vás již v minulosti antivirový software na škodlivý kód ve formě mallware, trojského koně nebo viru?** (při procházení internetu)

- □ ano
- □ ne

13. **Setkali jste se někdy s následujícími termíny?** (pokud ano, tyto označte)
    - kyberšikana
    - sexting
    - kyberstalking
    - kybergrooming
14. **Už jste se setkali s tím, že někdo někoho ponižoval nebo šikanoval přes internet?** (zasílání obtěžujících, ponižujících zpráv, napadání na sociálních sítích, fyzické napadání oběti spojené s natáčením videa apod.)
    - ano
    - ne
15. **Stalo se jednání popsané výše přímo Vám?** (odpovídejte, jen pokud jste označili v předchozí otázce ano)
    - ano
    - ne
16. **Už jste se setkali s tím, že někdo ve Vašem okolí zaslal prostřednictvím internetu svojí intimní (částečně intimní) fotografii (video) jiné osobě?**
    - ano
    - ne
17. **Zaslal(a) jste Vy osobně někdy někomu prostřednictvím internetu svojí intimní (částečně intimní) fotografii (video)?**
    - ano
    - ne
18. **Už jste se setkali s tím, že Vás někdo pronásledoval prostřednictvím informačních a komunikačních technologií za účelem kontaktování?** (neustálé zasílání zpráv, e-mailů, telefonáty a prozvánění, opakované komentování příspěvků na sociálních sítích apod.)
    - ano
    - ne

19. **Stalo se jednání popsané výše přímo Vám?** (odpovídejte, jen pokud jste označili v předchozí otázce ano)
    - ☐ ano
    - ☐ ne
20. **Už jste se setkali s tím, že Vás někdo neznámý kontaktoval prostřednictvím sociálních sítí a chtěl navazovat bližší kontakt?** (ať už pouhé dopisování nebo následné dotazování se na osobní údaje, případně vyžadování osobní schůzky)
    - ☐ ano
    - ☐ ne
    - ☐ ne, ale kamarádovi (kamarádce) ano
21. **Sdělil(a) jste někdy neznámé osobě prostřednictvím sítě internet některý ze svých osobních údajů?** (datum narození, heslo do internetové služby, telefonní číslo, své bydliště apod.)
    - ☐ ano
    - ☐ ne
    - ☐ ne, ale znám někoho, kdo ano
22. **Co vnímáte jako největší nebezpečí v síti internet?** (možno označit více možností)
    - ☐ sociální sítě
    - ☐ nelegální sdílení a stahování dat
    - ☐ útoky na počítače za účelem získání zájmových dat
    - ☐ nebo jiná nebezpečí, vypište……
    - ☐ nevnímám internet jako hrozbu

23. Jak by podle Vás měla vypadat příprava na rizika spojená s užíváním internetu?

- zavedení povinného předmětu v rámci školního vyučování
- občasné semináře ze stran základních škol
- občasné semináře ze stran odborníků ministerstev, Policie ČR apod.
- tyto informace by měli předat dětem rodiče
- nebo jiné, vypište…….

Příloha 2

ČESKÝ STATISTICKÝ ÚŘAD

Český statistický úřad | Na padesátém 81 | 100 82 Praha 10

TISKOVÁ ZPRÁVA

19. listopadu 2018

Více než polovina Čechů používá sociální sítě

V roce 2018 jsou k internetu připojeny již čtyři pětiny českých domácností (81%) a podobný podíl jich má i počítač (78 %).Největší nárůst byl zaznamenán vpoužívání tabletu. Přibývá uživatelů, kteří k internetu přistupují prostřednictvím mobilního telefonu.

„Meziročně vzrostl podíl domácností vybavených tabletem z 24 % na 32 %.Z domácností s dětmi má pak tablet více než polovina z nich," uvádí předseda Českého statistického úřadu Marek Rojíček.

Díky rozmachu chytrých telefonů rapidně přibývá uživatelů, kteří používají telefon k přístupu na internet. Zatímco v roce 2010 se z mobilního telefonu připojovala na internet 4 % osob,v roce 2018 je to již 58 %. Přitom čtyři z pěti takových osob si platí mobilní data.

„Plných 95 % osob ve věku 16 až 24 let používá chytrý telefon. Mezi seniory nad 65 let je to však jen 14 %. Klasický tlačítkový telefon bez operačního systému je mezi seniory stále oblíbený, používá ho 77 % z nich," upozorňuje Martin Mana, ředitel odboru statistik rozvoje společnosti ČSÚ.

Počet Čechů, kteří používají sociální sítě, letos překročil 50% hranici. V absolutních počtech to je 4,5 milionu osob starších 16 let. Sociální sítě však neoslovují Čechy v předdůchodovém a důchodovém věku. V rámci evropské osmadvacítky používají Češi této věkové kategoriesociální sítě nejméně.Každý druhý Čech také na internetu sleduje videa, nejvíce k tomu používá stránky typu YouTube (44 %). Oblíbené jsou též internetové televize (26 %) a stránky běžných TV stanic (24 %).

V internetových obchodech nakupuje už 54 % osob starších 16 let,nejvíce oblečení a obuv, jak upozorňuje Lenka Weichetová z odboru statistik rozvoje společnosti ČSÚ: *„Oblečení a obuv nakupuje v e-shopech 19 % mužů a 37 % žen. 15 % mužů dále nakupuje elektroniku, 14 % sportovní potřebya 13 % jiné vybavení domácnosti. 24 % žen nakupuje kosmetiku, 11 % hračky a 9 % potraviny."*

Pětina osob si na internetu rezervuje ubytování. I přes rostoucí popularitu ubytování v soukromí Češi stále bookují především hotely, penziony a další komerční zařízení. Ubytování v soukromí si v roce 2018 zajistilo 5 % Čechů, výrazně méně ve srovnání s ostatními zeměmi EU.

65 % Čechů používá informační technologie také v práci. S počítačem pracuje 56 %zaměstnaných a 28 % používá jiná IT zařízení, jako elektronické pokladny, IT zařízení v dopravních prostředcích či CNC stroje.

Více informací naleznete v nové publikaci ČSÚ Využívání informačních a komunikačních technologií v domácnostech a mezi jednotlivci – 2018:https://www.czso.cz/csu/czso/vyuzivani-informacnich-a-komunikacnich-technologii-v-domacnostech-a-mezi-jednotlivci.

Kontakty
Jan Cieslar
tiskový mluvčí ČSÚ
T274 052 017|M604 149 190
E jan.cieslar@czso.cz|Twitter@statistickyurad

Příloha 3


LIBČICKO HOSTIVICKO ŘEVNICKO MNÍŠECKO MÚ ČERNOŠICE
Bezpečná PRAHA ZÁPAD
děláme naše domovy bezpečnými...
Vyhledat...
ÚVODNÍ STRÁNKA MAPA KRIMINALITY PREVENCE KRIMINALITY DOPRAVNÍ INFORMACE O NÁS KONTAKT
24
LED
Beseda se žáky ZŠ ve Velkých Přílepech
Ve středu 23. ledna 2019 policista SKPV s kolegyní z oddělení tisku a prevence navštívili žáky osmé a deváté třídy ZŠ v obci Velké Přílepy.
Zde s žáky besedovali na dnes aktuální téma kyberkriminality, kde probrali její jednotlivé projevy. Můžeme konstatovat, že se žáci aktivně zapojovali a beseda se jim líbila.
Děkujeme paní ředitelce Mgr. Bc. Pavlíně Ben Saidové za pozitivní zpětnou vazbu:
Z důvodu zvýšení povědomí o kybernetické kriminalitě se dne 23. 1. 2019 v Základní škole Velké Přílepy konala beseda s panem por. Bc. Jiřím Dvořákem, jehož doprovázela tisková mluvčí Policie pro Prahu venkov – ZÁPAD paní por. Bc. Jana Dětská.
V úvodu nechali žáky vyplňovat dotazník, díky němuž si mohli uvědomit, co lze pod kybernetickou kriminalitu zahrnout. Byla pro ně připravena hezká prezentace, která byla oporou pro zajímavé povídání pana Dvořáka. Velmi se mi líbil jeho uvolněný způsob komunikace s žáky ve věku 14 let – 15 let. Podařilo se mu s nimi okamžitě navázat kontakt, díky němuž s ním velmi ochotně spolupracovali a nebáli se vyjadřovat k představeným pojmům nebo s ním sdílet své osobní zkušenosti a představy.
Probrali spolu významy pojmů týkajících se kybernetické kriminality: phishing, ransomware, hacking, spam, fakenews, hoax. Hovořili spolu i o tématu žákům velmi blízkém, a to o šíření a stahování filmů, které je dnes zcela běžně praktikováno velkou částí dětí a mladistvých. Významné místo dostal sexting. Žáci v období dospívání často dostatečně nevyhodnotí, že zveřejňování některých odhalenějších fotografií jim může jednou přinést velké problémy. Téma bylo přiblíženo na skutečných případech. Jako velmi silný moment dnešního preventivního programu vnímám video o Amandě Todd, která se ve svém životě dopustila několika chyb, za něž nakonec zaplatila cenu nejvyšší, a to ztrátu svého života.
Věřím, že dnešní povídání otevřelo žákům oči a přispěje k tomu, aby si více vážili sami sebe a dokázali odolávat různým nástrahám, i když se tak zprvu nejeví.
Děkuji toto smysluplné setkání.
Mgr. Bc. Pavlína Ben Saidová
Ředitelka školy
Dejte to vědět ostatním:
Nábor nových policistů
NOVÁ MOBILNÍ APLIKACE!
Prověřte si věci v pátrání
Poslední příspěvky
Vloupání do rodinného domu 18.11.2019
BÝT VIDĚN! – základní pravidlo všech účastníků silničního provozu nejen za snížené viditelnosti 18.11.2019
Šíření informací po sociálních sítích o lákání nezletilého chlapce do černého vozidla na Hostivicku 24.10.2019
Krádež věcí z chaty 22.10.2019
Zloděj řádil na stavbě 21.10.2019
Krádež věcí z vozidla 18.10.2019
Uzavírka dálnice D4 při demolici mostu u obce Řitka 17.10.2019
Partnerem projektu jsou Obecní a Městské úřady vyjmenovaných obcí, Obecní policie a Policie ČR.
NAJDETE NÁS NA FACEBOOKU
Bezpečná PRAHA ...
228 To se mi líbí
Tohle se mi líbí
Sdílet
CHCE BÝT NEUSTÁLE V OBRAZE?
Nabízíme Vám možnost odběru novinek. TIP: Nově je možné vybrat kategorii odběru nových příspěvků dle Vašeho bydliště!
Odběr novinek!
PŘIHLÁŠENÍ | REGISTRACE
Přihlásit
Islemag, redakční systém WordPress
Podpořte nás

Příloha 4

ZÁKLADNÍ ŠKOLA SMEČNO, OKRES KLADNO
ŠKOLSKÁ 284, SMEČNO, 273 05
příspěvková organizace
tel.: 317 471 401-5 IČ 48705721

Poděkování

Základní škola Smečno, okres Kladno zastoupená ředitelkou školy Ing. Lenkou Bechyňskou **děkuje** por. Bc. Jiřímu Dvořákovi za uspořádání besed pro žáky 8.a 9. tříd dne 10. 6. 2019. Dopolední blok besed trval celkem 5 vyučovacích hodin. Ústředním tématem byla kyberšikana. Por. Bc. Jiří Dvořák čerpal ze své praxe u Policie ČR. Závažné a společensky nebezpečné téma se snažil žákům vysvětlit na příkladech z praxe. Během besedy probíhala živá komunikace mezi lektorem a žáky. V poslední části programu byla probrána trestní odpovědnost mladistvých. Spolupráce s por. Bc. J. Dvořákem byla velmi přínosná a pokud by to bylo možné, tak bychom rádi spolupracovali i nadále.

Ing. Lenka Bechyňská, ředitelka školy

Základní škola Smečno, okres Kladno
Školská 284, 273 05 Smečno
příspěvková organizace ①
tel.: 317 471 401-5 IČ: 48705721

Ve Smečně 11.6. 2019

Příloha 5

Standing up to Cyberbullying

Top Ten Tips for Teens

Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D.

Don't be a bystander—stand up to cyberbullying when you see it. Take action to stop something that you know is wrong. These **Top Ten Tips** will give you specific ideas of what **you can do** when you witness cyberbullying.

1. **REPORT TO SCHOOL.** If the person being cyberbullied is someone from your school, report it to your school. Many have anonymous reporting systems to allow you to let them know what you are seeing without disclosing your identity.

2. **COLLECT EVIDENCE.** Take a screenshot, save the image or message, or screen-record what you see. It will be easier for an adult to help if they can see—and have proof of—exactly what was being said.

3. **REPORT TO SITE/APP/GAME.** All reputable online environments prohibit cyberbullying and provide easy tools to report violations. Don't hesitate to report; those sites/apps will protect your identity and not "out" you.

4. **TALK TO A TRUSTED ADULT.** Develop relationships with adults you can trust and count on to help when you (or a friend) experience something negative online. This could be a parent, teacher, counselor, coach, or family friend.

5. **DEMONSTRATE CARE.** Show the person being cyberbullied that they are not alone. Send them an encouraging text or snap. Take them aside at school and let them know that you have their back.

6. **WORK TOGETHER.** Gather your other friends and organize a full-court press of positivity. Post kind comments on their wall or under a photo they've posted. Encourage others to help report the harm. There is strength in numbers.

7. **TELL THEM TO STOP.** If you know the person who is doing the cyberbullying, tell them to knock it off. Explain that it's not cool to be a jerk to others. But say something—if you remain silent, you are basically telling them that it is ok to do it.

8. **DON'T ENCOURAGE IT.** If you see cyberbullying happening, don't support it in any way. Don't forward it, don't add emojis in the comments, don't gossip about it with your friends, and don't stand on the sidelines.

9. **STAY SAFE.** Don't put yourself in harm's way. When your emotions are running high, resist posting something that may escalate the situation. Don't hang out online where most people are cruel. Never physically threaten others.

10. **DON'T GIVE UP.** Think creatively about what can be done to stop cyberbullying. Brainstorm with others and use everyone's talents to do something epic!

CYBERBULLYING RESEARCH CENTER