Bezpečnostní aspekty kyberšikany na základních školách

Markéta Hovorková

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav počítačových a komunikačních systémů

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Markéta Hovorková**
Osobní číslo:	**A19475**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**Prezenční**
Téma práce:	**Bezpečnostní aspekty kyberšikany na základních školách**
Téma práce anglicky:	**Safety Aspects of Cyberbullying in Primary Schools**

Zásady pro vypracování

1. Proveďte literární rešerši na téma kyberšikany.
2. Zaměřte se na základní školy a popište nejčastější formy kyberšikany.
3. Proveďte analýzu kyberšikany na vybrané základní škole.
4. Vytvořte vhodné edukační materiály zabývající se kyberšikanou a prevencí.
5. Navrhněte obsah semináře týkající se prevence kyberšikany na základních školách.

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

Seznam doporučené literatury:

1. KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně na internetu. Praha: Grada, 2016. ISBN 978-80-247-5595-3.
2. KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.
3. VÁGNER a Vanessa ROGERS. Kyberšikana. Praha: Portál, 2011. ISBN 978-80-7367-984-2.
4. HOLLÁ, Katarína. Sexting a kyberšikana. Bratislava: IRIS, 2016. ISBN 9788081530616.
5. KOPECKÝ, Kamil. Rizikové formy a chování českých a slovenských dětí v prostředí internetu. Olomouc: Universita Palackého v Olomouci, 2015. ISBN 978-80-244-4861-9.

Vedoucí bakalářské práce: **doc. Ing. Jiří Vojtěšek, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **2. prosince 2022**
Termín odevzdání bakalářské práce: **24. května 2023**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Ing. Petr Šilhavý, Ph.D. v.r.
garant oboru

Ve Zlíně dne 8. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně, dne 22.5.2023

Markéta Hovorková v.r.
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá problematikou kyberšikany především na základních školách. Teoretická část vymezuje samotný pojem kyberšikana a jeho specifické formy, které jsou v dnešní době aktuální. Praktická část obsahuje analýzu situace na vybrané základní škole. Pro analýzu byla využita forma anonymního dotazníkového šetření. Výstupem jsou také vytvořené elektronické materiály, konkrétně edukační videa a letáky pro děti, pedagogy a rodiče týkající se kyberšikany, jejich forem a způsobů, jak ji řešit, popř. se jí bránit.

Klíčová slova: kyberšikana, formy kyberšikany, základní školy, kyberagresor, oběť, sociální sítě

ABSTRACT

In the Bachelor thesis there will be worked up the topic of cyberbullying among elementary school students. The aim of the theoretical part is to define the terms such as cyberbullying and its specific types having currently the greatest impact on individuals. The practipal part of the Bachelor thesis deals with analysis of situation at the selected school. There will be used a questionnaire method. The data output consists of electronic materials regarding educative videos and leaflets for pupils, teachers and parents reflecting the cyberbullying and its forms and ways to address it, or possibly defend against it.

Keywords: cyberbullying, forms of cyberbullying, elementary schools, cyberbullying, victim, social networks

Mé poděkování patří panu doc. Ing. Jiřímu Vojtěškovi, Ph.D. za trpělivost, vedení, ochotu a čas, který mi v průběhu zpracování bakalářské práce věnoval.

„Tajemstvím života je sedmkrát padnout a osmkrát vstát.“ – Paulo Coelho

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

OBSAH

ÚVOD

Bakalářská práce se zabývá bezpečnostními aspekty kyberšikany na základních školách. Každý zná nebo se setkal s pojmem šikana, ale kyberšikana je pojem relativně nový, o to více se ale rozšiřuje především u mladé generace. Práce tedy popisuje nejen šikanu jako takovou, ale definuje také rozdíly mezi klasickou šikanou a kyberšikanou. Kyberšikana má řadu forem a typů například kybergrooming, kyberstalking, krádež identity, flaming, trolling, sexting a další. Pokud se bavíme o kyberšikaně, musíme si také nadefinovat co je to kyberprostor, který slouží jako prostor, kde se samotná kyberšikana uskutečňuje. Jedná se o prostředí internetu a konkrétní sociální sítě, které jsou vlivem rozvoje moderní společnosti čím dál více popularizovány. Mnohdy se zárodky kyberšikany vyskytují v prostředí školy a je nutné, aby škola byla schopna zajistit určité bezpečnostní aspekty, či preventivní kroky proti vzniku kyberšikany. Existují různé organizace, na které se mohou děti, rodiče či kdokoli jiný obrátit v případě, že se přímo či nepřímo setkají s kyberšikanou. Důležité je podívat se na kyberšikanu také z hlediska legislativního, především nebezpečným pronásledováním, pomluvou, šířením pornografie, vydíráním, podvodem a dalšími.

Výzkum z oblasti kyberšikany bude v práci realizován formou dotazníkového šetření na konkrétní základní škole. Toto dotazníkové šetření bude zaměřeno na zjištění míry povědomí o problematice kyberšikany mezi žáky. Cílem bude zjistit, zda žáci vědí, jak velké riziko podstupují, když se stanou součástí virtuálního světa a co vše riskují svým nesprávným působením na sociálních sítích. Dále bude následovat také analýza a intepretace zjištěných dat.

Téma práce bylo zvoleno záměrně, a to z toho důvodu, že se jedná o téma a problém aktuální moderní společnosti, a to obzvlášť mladé generace, na kterou je práce cílena. Kyberšikana je brána jako druh šikany, přičemž vzhledem k anonymitě, kterou internet či jiné moderní technologie poskytují, je daleko rafinovanější a nebezpečnější než šikana klasická. Snadný přístup k informačním technologiím bere většina společnosti jako samozřejmost a možnost anonymního vystupovaní na internetu dává jedinci z psychologického hlediska větší moc. Jedinci tak mají příležitost vyjádřit své urážlivé názory, které jsou mnohdy plné agrese, skoro beztrestně. Hlavním cílem práce bylo zjistit povědomí v obecné rovině, ale také to, zda žáci vědí, kam se obrátit v případě, když pomoc již potřebují. Výstupy z realizovaného výzkumu budou sloužit jako pomůcka pro žáky, pedagogy, rodiče i pro širokou veřejnost k prohloubení informovanosti v dané problematice.

I. TEORETICKÁ ČÁST

1 ŠIKANA

Šikana je řazena mezi závažné sociálně – patologické jevy. V dnešní době, která je ve velké míře zaměřena na sociální rozdíly ve společnosti, se tedy můžeme s šikanou setkat již u dětí předškolního věku. Právě výše zmíněné socioekonomické rozdíly mezi jednotlivci, mohou být prvním impulsem k šikaně. Nemusí se jednat pouze o problematiku v socioekonomické oblasti, ale i patrné rozdíly ve vzhledu, tělesné handicapy či jiná znevýhodnění, která nejsou společností plně přijímána, mohou vést k šikaně [1].

1.1 Definice pojmu

Kraus a Hroncová ve své publikaci definují šikanu jako *„úmyslné jednání namířené proti jinému jedinci, případně skupině lidí, jehož podstatou je útok proti lidské důstojnosti“* [2]. Pojem šikana je odvozen z francouzského slova *chicane,* význam v sobě nese záměrné obtěžování, týrání a pronásledování. Jde o záměrné a úmyslné použití fyzické síly, psychického ubližování vůči slabším jedincům nebo skupině [3].

V případě tradiční (fyzické) šikany se bavíme o nejrůznějších podobách útoků. Jedná se o fyzické útoky v podobě přímé agrese, krádeže, psychické týrání a v neposlední řadě ničení cizího majetku. Mezi dětmi či mladistvými, se setkáváme také s urážkami, nadávkami či jinou formou ponižování. Zde také hovoříme o šikaně v přímé formě. Lovasová definuje šikanu jako *„sociálně patologický jev, kdy dochází k omezování zejména osobní svobody a svobody rozhodování, je ponižována lidská důstojnost a mnohdy je obětem ubližováno na zdraví či majetku“* [4].

Můžeme se setkat také s formou nepřímé šikany. Zde se bavíme o situacích, kdy je jedinec šikaně přítomen, ale aktivně se na ni nepodílí, přítomnost šikany ignoruje a neupozorní na ni. Stává se tak přihlížejícím účastníkem. Zde je ale nutné dobře vyhodnotit, zda se jedná o pasivní formu šikany či o absenci nebo nízkou míru vyvinutého sociálního cítění. Šikana má své charakteristické rysy, které ji definují. Jedním z rysů je **záměrnost**, jedná se o činnost s předem stanoveným úmyslem a cílem. Dalším z rysů je **nepoměr a nerovnováha sil agresora a oběti.** Jedná se primárně o nepoměr sil v oblasti fyzické či v počtu agresorů vůči oběti. Může se jednat i o psychickou převahu, a to v situaci kdy si agresor z pravidla vybírá psychicky méně odolné jedince. Dalším důležitým specifickým rysem je **opakování**. Tento rys je velmi důležitý, a to z toho důvodu, že jedná-li se o jednorázový útok, nemůžeme zde mluvit o šikaně.

Jak bylo zmíněno již výše, je důležité si uvědomit, že šikana není problém, který se týká pouze dětí či mládeže. Počátky můžeme sledovat již v předškolním věku dítěte následně pak ve všech následujících školních zařízeních. Jedná se o jev, který se stal součástí i velkého procenta dnešních rodin, kdy nejčastěji dochází k šikaně mezi sourozenci, ale můžeme se také setkat se šikanou v partnerských vztazích. Zde už je ale velmi malá hranice mezi šikanou a domácím násilím. S šikanou se můžeme setkat i na pracovišti jak ze strany kolegů, tak ze strany nadřízených. Právě na základě toho, v jakém prostředí probíhá, jaká je věková kategorie účastníků, jakou formu má či jaký je vztah účastníků vůči sobě, můžeme šikanu dále dělit dle specifických kritérií [5].

Aktéři kyberšikany

1. **Agresor –** Jedná se o takového člověka, který vyhledává a vyvolává konflikty. Využívá prostředků fyzické síly, nicméně v určitých případech lze mluvit i o agresi verbální, kdy agresor slovně napadá či vyhrožuje druhé osobě (oběti). V řadě odborných publikací, se autoři shodují v tom, že samotná agresivita se vytváří již v raném věku života. Značnou roli hraje temperament jedince, který právě v jedinci probouzí jistou vznětlivost, podrážděnost, impulzivitu [6].

   Psychologické studie uvádí, že agresor bývá vůči obětem bezcitný, bezohledný. Sám se domnívá, že jeho chování je správné a necítí vinu. Často se snaží zodpovědnost za své činy přenést na oběť a zbavit se tak zodpovědnosti za protiprávní čin, kterého se dopustil. Jedná se např. o věty typu: *Neměl si mě provokovat, říkal sis o to* apod. [7].

2. **Oběť** – Vymezení tohoto pojmu z hlediska šikany není vůbec snadné. V obecné rovině a z hlediska legislativy se obětí rozumí: *„Fyzická osoba, které bylo nebo mělo být trestným činem ublíženo na zdraví, způsobena škoda nebo majetková újma nebo na jejíž úkor se pachatel trestným činem obohatil nebo měl obohatit“* [6]. Neexistuje žádný universální popis toho, jak má oběť vypadat. Profil oběti se může charakterizovat různými způsoby. Každý agresor si najde oběť dle svých kritérií. Mnohdy je ale výběr agresora velmi nahodilý a je mu jedno, kdo je obětí. Do jisté míry můžeme na základě informací a společných rysů z reálných kazuistik sestavit profil oběti. Na jejich základě byly vypozorovány určité společné znaky u jednotlivých obětí. Často se obětí stávají děti, které vyrůstají v neúplné, sociálně slabší rodině či děti homosexuálních párů. Dále se jedná o jedince, kteří se od svých

vrstevníků liší, ať už vzhledově nebo povahově. Může se jednat o děti, které jsou zakřiknuté nebo např: děti, které se dobře učí, chovají se slušně k učitelům. Co se týká fyzických odlišností, tak nejčastěji se obětí šikany stávají děti s nějakým druhem postižení, děti tělesně ne tak zdatné, obézní či naopak příliš hubení. V dnešní době se velmi často setkáváme i s šikanou, která je založena na rasové odlišnosti [4].

1.2 Vývoj šikany a její stádia

Oběti šikany se nacházejí mnohdy v situaci, kdy již akutně potřebují pomoc od svého okolí. Ale ve většině případů nejsou schopni si o pomoc říct. Důvod, proč se snaží tohle utrpení držet co nejdéle v tajnosti, jsou různé. Primárně jde o strach ze msty agresora. Někdy se může jednat o strach z reakce rodičů. Například: dítě má strach, že mu nebudou rodiče věřit. U chlapců se může jednat o strach ze selhání v očích svého otce, že se nedokáže ubránit jako chlap. Mnohdy mají děti strach se svěřit z důvodu, že nechtějí přijít o poslední přátelé tím, že budou „žalovat“. Chceme-li zjistit, zda se dítě stalo obětí šikany, je nutné se na dítě zaměřit celistvě. To, že se dítě, které je obětí šikany uzavře do sebe, je smutné, apatické či plačtivé, není pravidlem. Jsou případy, kdy se oběť šikany začne projevovat tím, že je drzá na autority, je vulgární, vyrušuje v hodinách, a to jen proto, aby dotyčný stoupl v očích kamarádů či právě samotných agresorů. Známky šikany lze mnohdy pozorovat i podle vnějších změn (např. často ušpiněné oblečení, modřiny, odřeniny apod). Tyto známky nemusí být pravidlem, ale často bývají spolehlivým varovným signálem.

Přímé varovné signály – chování okolí vůči dítěti

- posmívání, urážky, úmyslné ponižování, zesměšňování, nadávky
- opakovaná kritika a zpochybňování
- opakované schovávání, poškozování či krádež osobních věcí
- výsměch, pohrdání
- poškození oděvu, osobních věcí
- tělesné napadání
- vyžadování podřazenosti, plnění příkazů

Nepřímé varovné signály – chování samotného dítěte, vzhled

- strach chodit do školy
- záškoláctví
- viditelný strach
- špatný spánek, noční můry
- opakované ztráty věcí, peněz
- často žádá o peníze od rodičů pod jinou záminkou
- snaží se být v blízkosti dospělé osoby
- smutná nálada, apatie [4].

Stádia šikany

V následující podkapitole budou zmíněna jednotlivá stádia vývoje šikany, které mohou sloužit jako impulz pro rodiče a okolí jako varovný signál přítomnosti negativních vlivů.

***První stádium* – Zrod ostrakismu**

***Ostrakismus* –** samotný pojem pochází z athénské historie, význam slova ostrakismus znamená vyloučení a vypovězení jedince z dané skupiny [8].

V prvním stádiu tedy dochází k mírné převážně psychické formě násilí. Oběť je jedinec, který je zbytkem skupiny neoblíben a neuznáván. Ostatní členové jej odsuzují, vyčleňují, pomlouvají. Již v této fázi se lze bavit o zárodečné fázi šikany s předpokladem negativního vývoje.

***Druhé stádium* – Fyzická agrese a přitvrzování, manipulace**

Nastává v situacích, které mohou mít zátěžový charakter, což ve školním prostředí může znamenat např. písemnou práci, zkouškové období apod. V takových situacích se stávají z ostrakizovaných jedinců tzv. hromosvody. Vybíjí si svou zlost a nepříjemné pocity na slabších jedincích. Většinou svou agresí skrývají svůj strach, obavy.

***Třetí stádium* – Klíčový moment, vytvoření jádra**

Začíná se tvořit „jádro“, které je tvořeno skupinou agresorů. Společně spolupracují a systematicky trýzní předem vybranou oběť. Jak bylo zmíněno výše, většinou se jedná o jedince slabší. Vzniká zde také tzv. pyramida šikanování, která se skládá z oběti,

agresora či skupiny agresorů, ale neopomenutelným členem jsou také spolužáci, kteří sice přímo nešikanují, ale přihlížejí mu a oběti nepomohou.

Čtvrté stádium – **Většina přijímá normy**

Normy agresorů jsou přijaty většinou a stanou se nepsaným zákonem pro zbytek skupiny. A platí zde nepsané pravidlo „Nejsi s námi, jsi proti nám“. Což vede k tomu, že ze strachu okolí přijme daná pravidla a mnohdy se i žáci, kteří jsou ukáznění a mírní chovají krutě a přechází také do přímé šikany.

Páté stádium – **Totalita neboli dokonalá šikana**

V této konečné fázi už jsou definitivně přijata pravidla agresorů a dochází již k tzv. vykořisťování. Žáci jsou rozděleni na otroky a otrokáře. Otrokáři mají všechna práva a otroci naopak žádná [9].

2 KYBERŠIKANA

Tato kapitola se zabývá jednou z forem šikany, a to je kyberšikana. Jedná se o takovou formu šikany, která se odehrává prostřednictvím internetu, mobilních telefonů, sociálních sítí apod. Právě i prostřednictvím těchto médií dochází k poškození jedince či skupiny jedinců.

2.1 Definice pojmu

Definice kyberšikany má několik podob, stejně tak jako v případě tradiční šikany nelze určit jednu primární definici. Každý autor na problematiku nahlíží jinak. Jedná se o druh šikany, který má kořeny v tradiční (školní šikaně). První autor, který pojem kyberšikana vůbec použil, byl autor Besley. V roce 2004 ji definoval jako: *„Využívání informačních a komunikačních technologií, jako jsou e-maily, mobilní telefony, pagery, textové zprávy a instant messaging, k podpoře úmyslného, opakovaného a nepřátelského chování jednotlivce nebo skupiny, které je určeno, aby ublížilo ostatním.“* Od zrodu kyberšikany došlo k rozsáhlým změnám, které zapříčinil primárně rozvoj moderních technologií. Ty měly sloužit k pozitivnímu využití ve společnosti. Dostavil se ale i opačný efekt dopadu technologií. Lidé začali techniku a virtuální prostor využívat jako prostředek k ubližování druhému jedinci či skupině [10].

Ministerstvo školství, mládeže a tělovýchovy definuje kyberšikanu jako *„zneužití informačních a komunikačních technologií* (dále jen ICT)*, zejména pak mobilních telefonů a internetu, k takovým činnostem, které mají někoho záměrně ohrozit, ublížit mu. Podobně jako u šikany tváří v tvář se jedná o úmyslné chování, kdy je oběť napadána útočníkem nebo útočníky. Povaha a provedení útoků pak určují její závažnost* [11].“

Nejčastější projevy kyberšikany:

- Zasílání nevyžádaných, urážlivých, zastrašujících zpráv (SMS, e-mail, chat…).
- Šíření pomluv a lživých informací prostřednictvím sociálních sítí.
- Vytváření fiktivních profilů, internetových stránek blogů s lživým, ponižujícím obsahem, který se vztahuje ke konkrétní osobě.
- Krádež identity.
- Záměrná, cílená provokace v diskusních fórech.
- Obtěžování formou nevyžádaných a opakovaných hovorů, zpráv apod. [12]

Tabulka 1 poukazuje na rozdíly mezi šikanou a kyberšikanou.

Tradiční (školní) šikana	Kyberšikana
Rysy	
Opakování – agresor opakovaně napadá oběť v průběhu času. Jedná – li se o jednorázový útok, nejedná se v tomto případě o šikanu.	Opakování – v případě kyberšikany stačí jediný „útok“, který může mít několik forem. Nejčastější formou bývá zveřejnění obsahu, který má ponižující charakter. Následné šíření a přeposílání tohoto obsahu se díky veřejné povaze virtuálního prostředí stává **opakováním**. Tím pádem se agresor jediným aktem může dopustit kyberšikany, která pak trvá už delší čas.
Mocenská nerovnováha – mocenská nerovnováha není jen v oblasti fyzické síly, ale také v psychické oblasti. Kdy psychická a sociální nevyspělost může vést k nerovnováze mezi mocí agresora a oběti.	Mocenská nerovnováha – oběť nedokáže obtěžování technologicky zabránit. Nerozhoduje fyzická síla, ale agresor zde využívá své technické znalosti.
Přímá	
Fyzická (fyzické násilí, poškozování majetku, krádeže věcí). V tomto případě se jedná o čin, který je vidět, je zřetelné, kdo je aktérem. Kdo je v roli oběti a kdo v roli útočníka.	Fyzická (např. úmyslné pořizování intimních či jiných fotografií či videí oběti a jejich umisťování na internet). Oběť ji nemůže předvídat, je nečekaná.
Verbální (např. nadávky, urážky, ponižování).	Verbální (např. urážlivé, výhružné e-maily či SMS, nebo zprávy na sociálních sítích).
Neverbální (např. obscénní gesta).	Neverbální (např. posílání výhružných nebo obscénních obrázků, nevyžádaná korespondence se sexuálním podtextem).
Nepřímá	

Sociální (např. vylučování někoho ze skupiny).	Sociální (např. vylučování někoho z online skupiny).
Verbální (např. šíření pomluv a lživých informací).	Verbální (např. zveřejnění soukromé konverzace či informací, šíření pomluv na internetu).
	Podvádění vydáváním se za někoho jiného, falešné profily, krádež identity.

Tabulka 1: Porovnání kyberšikany a šikany

2.2 Formy kyberšikany

Neexistuje jednotné rozdělení forem kyberšikany. Každý autor na danou problematiku nahlíží jinak. Někteří autoři pod kyberšikanu zahrnují všechny druhy spojené s problematikou kriminální činnosti ve virtuálním prostoru. Jiní ji zase dělí z hlediska místa, kde ke kyberšikaně dochází (mobilní telefon, internet) a také prostředky (kanály šíření, sociální sítě, blogy) prostřednictvím kterých dochází k realizaci.

Kyberstalking (pronásledování)

Opakované pronásledování oběti, pomocí informačních technologií. Agresor (stalker) stupňuje pravidelnost a intenzitu pronásledování. Obsah zpráv a vzkazů, taktéž graduje na hrubosti [14].

V oběti se hromadí obavy a strach o vlastní život a o bezpečí svých blízkých. Nejčastěji se s kybarstalkingem setkáváme u bývalých partnerů [15].

Harassement (obtěžování)

Obtěžování v kyberprostoru se vyznačuje především opakovaným posíláním nevyžádaných zpráv, telefonátů, emailů apod [16].

Denigration (ponižování, pomlouvání)

Jedná se o: *„Rozšiřování pomluv a lží o někom, s cílem poškodit jeho pověst nebo vztahy* [17].*“*

Jelikož vše probíhá ve virtuálním prostředí, prostřednictvím moderních technologií a virtuálně v kyberprostoru, je pro oběť velmi těžké se bránit. Ve virtuálním prostředí dochází k šíření informací podstatně rychleji než v reálném životě [13].

Kybergrooming

Jedná se o nepřímou formu kyberšikany, kdy útočník pod falešnou identitou a falešnou záminkou láká nezletilé oběti na schůzku prostřednictvím ICT za účelem následného sexuálního zneužití [10].

Útočníci si vybírají oběti, které se vyznačují ekonomicky nízkým statusem, jedince (děti) ze zanedbaných či sociálně slabších rodin atd. Těmto obětem je nabízena finanční odměna za schůzku, či fotografie a videa s kompromitujícím obsahem sloužícím např. k dětské pornografii [16].

Scénář kybergroomingu má nepsaná pravidla, kdy se útočník vydává za osoby věkově srovnatelné s obětí. Následně s nezletilou osobou naváže kamarádský vztah a vybuduje v oběti důvěru. Tu si získá na základě sdělení svých problémů, které se ve většině případu velmi ztotožňují s problémy oběti. Následně po získání kompromitujícího materiálu se v oběti snaží vzbudit pocit viny, a to především vzhledem k citlivosti informací, které mu oběť sdělila. U oběti pak dochází k sociální izolaci. Následná schůzka nemusí vždy napoprvé končit útokem, ale naopak může směřovat k upevnění vztahu s obětí. Délka kontaktu se odvíjí od schopností a zkušeností agresora [18].

Flaming (flame = hořet)

„Flaming (flame = hořet) je termín, označující nepřátelské chování uživatelů na internetu, které obvykle doprovází urážky, nadávky, vyhrožování apod. Flaming je obvykle spojen se sociálním prostředím diskusních fór, webového chatu příspěvků, ale může však být realizován i prostřednictvím e-mailu.“ Nejčastěji se s flamingem setkáváme na platformách, kde mohou jedinci veřejně komentovat, vytvářet příspěvky. Zde se flamer = útočník projevuje vulgární až agresivní reakcí na posty (příspěvky), na který má odlišný názor. Reakce nebývají nijak propracované a smysluplné, zato jsou plné vulgarismů. Zde je důležité nezaměňovat *flamera* za *trolla*. Troll je osoba, která také působí ve veřejných diskuzích, s tím rozdílem, že se snaží uměle vytvářet konflikt a vyvolávat negativní diskuse mnohdy o problematice která s příspěvkem nijak nesouvisí [19].

Sexting

Sexting můžeme definovat jako zasílání zpráv, videí, převážně s intimním obsahem a sexuálním podtextem [20]. Tento fenomén se nejčastěji řeší u dětí a mladistvých. V tomto období není u jedinců ještě plně rozvinut pocit zábran, a tak si dost dobře neuvědomují

možná rizika a následky. Ale tento problém se netýká jen skupiny dětí a mladistvých, ale často tyto materiály vznikají i v partnerských vztazích. Kde si člověk nepřipouští, že by mohlo dojít ke zneužití takových materiálů. Nejčastěji se tak stává po rozchodu partnerů, kdy se jeden druhému snaží ublížit a pomstít se. V tomto případě přechází sexting k sextortion [21].

Happy slapping (veselé fackování)

Jedná se o situace, kdy je neznámý člověk napaden a samotný útok je jedním z útočníků natočen. Natočené video je následně zveřejněno na internetu [22]. Procházka ve své publikaci poradenské psychologie uvádí, že v případě happy slappingu mluvíme o jedné z nejčastější formě kyberšikany [23].

Outing and trickery (prozrazení a podvádění)

Při prozrazení neboli outingu se jedná o druh kyberšikany, při které útočník zveřejní fotografie, videozáznamy, informace o oběti, které oběť nikdy nezamýšlela zveřejnit [10].

Při podvádění (trickery) přesvědčuje útočník oběť, aby mu prozradila tajemství a citlivé informace, které by následně mohl zveřejnit na internetu [17].

Ostatní formy kyberšikany

V předchozí podkapitole byly zmíněny formy kyberšikany, které mají za cíl oběti ublížit nebo ji nějakým způsobem poškodit. Existují další formy kyberšikany, které jsou odlišné tím, že mají za cíl oběť okrást o důležitá data.

Phishing

Je jeden z mnoha druhů napadení v kyberprostoru. Tento druh napadení má za cíl získat citlivé údaje od uživatele. Phishingové napadení je možné odhalit, ale uživatel musí být velmi pozorný. Ve většině případů se u phishingových napadení objevují pravopisné chyby, cizí jazyk nebo znaky, které do zprávy či e-mailu nepatří. Obvykle se útočníci snaží tyto citlivé údaje od uživatelů získat pomocí podvodných e-mailů, nebo zpráv přes sociální sítě. Jedna z možností je, že uživateli přijde zpráva na Facebook od jeho známého (obvykle má tento člověk napadený profil) s prosbou o číslo. Poté co oběť pošle jeho číslo, přijde jí do textové zprávy kód, který útočník zpětně vyžaduje. Pokud tento kód útočníkovi sdělí, může se v měsíčním vyúčtování objevit vyšší částka než obvykle.

Pharming

Stejně jako phishing má pharming stejný cíl, a to zmanipulovat oběť tak, aby sdělila své citlivé údaje. Tyto podvodné praktiky jsou značně podobné a také se objevuje jejich kombinace. Pharming, na rozdíl od phisningu, využívá jinou strategii a je těžší jej rozpoznat. Pharmingový útok vypadá tak, že se uživatel ocitne na falešné internetové stránce, aniž by o tom věděl, protože útočník pomocí doménového serveru přepíše IP adresu [24].

2.3 Specifické znaky kyberšikany

Jak bylo zmíněno výše, kyberšikana nepředstavuje jednotný samostatný jev, nýbrž se jedná o jednu z forem **psychické** šikany. Cíleně je zde uváděna psychická šikana, protože na rozdíl od tradiční (školní) šikany neprobíhá kyberšikana tváří v tvář, kdy se účastníci znají a jsou v přímém osobním kontaktu a znají své nejbližší okolí, přátele či rodinu. Kyberšikana se odehrává ve virtuálním světě, který zajišťuje agresorovi jistou míru anonymity. Poskytuje mu tak větší možnosti pro útoky [17].

1. **Anonymita**

Díky principu virtuálního světa, na kterém funguje celý internet, jsou útočníci relativně anonymní. Na sociálních sítích a všeobecně na internetu vystupují pod falešným profilem, emailovou adresou či telefonním číslem z čehož vyplývá, že oběť útočníka nemá, jak identifikovat. Toto mnohdy vede k posílení odvahy agresora, a jeho útoky mohou mít stupňující se charakter. Anonymita na internetu není nikdy stoprocentní. Jedná se pouze o relativní anonymitu, protože v případě dostatečné technické zdatnosti a technického vybavení mohou experti v oboru identitu agresora v některých případech dohledat. Mnohdy ale nastává problém pachatele z právního hlediska z takového protiprávního činu usvědčit [23].

2. **Čas a místo**

Při tradiční (školní) šikaně, kdy dochází k setkávání agresora a oběti můžeme předpokládat, kdy k útoku dojde. V případě kyberšikany bohužel nelze předpovídat, kdy útok přijde. Vzhledem ke každodennímu využívání ICT je oběť neustále pod tlakem a ani v domácím prostředí není v bezpečí. K útoku může dojít ve kteroukoli denní i noční hodinu [23].

3. **Velké publikum a přesah**

Velmi kritický dopad na psychiku oběti má veřejná povaha virtuálního světa. Zejména možnost sdílení obsahu. Agresorovi stačí příspěvek publikovat pouze jednou, a právě ono zmíněné velké publikum, se dále stará o špinavou práci za útočníka právě tím, že obsah dál šíří. Rychlost šíření příspěvků na internetu je enormně vysoká až nekontrolovatelná [25].

4. **Změna charakteru oběti a útočníka**

Vzhledem k tomu, že celý útok se odehrává ve virtuálním anonymním prostoru, tak útočníkem nemusí být jen jedinec fyzicky zdatný, ale zpravidla stačí jen dobrá znalost technologií. Právě anonymita prostředí, ve kterém se vše odehrává, nuluje rozdíly ať už věkové, rasové či rozdíly v pohlaví. Obětí tak nejsou zpravidla slabší jedinci, může se jednat také o osoby společensky vysoce postavené.

5. **Prakticky neidentifikovatelné následky**

Vzhledem k tomu, že násilí v kyberšikaně není pácháno fyzicky. Je velmi těžké ji dokázat. Absence modřin, oděrků a podlitin ale neznamená, že nemá oběť doživotní následky. Ty jsou mnohdy horší než v případě fyzické agrese. Stává se to, že oběť se do sebe uzavře a ze strachu odmítá komunikovat se svým okolím o svých problémech. Má strach z reakce okolí. Psychické následky mohou oběti dovést až k myšlenkám na sebevraždu či k samotné sebevraždě [26].

2.3.1 Typy kyberšikany

Rozdělit kyberšikanu můžeme na dva základní typy. Kyberšikana ***přímá*** a ***kyberšikana v zastoupení.***

Kyberšikana přímá – dochází ze strany agresora k přímým útokům např. v podobě zpráv. Agresor je přímým konatelem protiprávní činnosti.

Formy přímých útoků

- Posílání SMS, e-mailů, zpráv přes messenger
- Zcizení profilů na sociálních sítích a jejich následné zneužívání
- Šíření osobních, lživých informací, rozesílání intimních fotografií
- Slovní napadání prostřednictvím skupinových chatů při hraní her
- Nabourávání herních či osobních účtů

- Šíření spamů či jiných virů prostřednictvím e-mailu apod.

Nepřímá kyberšikana (kyberšikana v zastoupení) –V případě kyberšikany v zastoupení, využívá agresor k útoku jiné osoby. Tito jedinci ve většině případů netuší, že se stali nástrojem něčí pomsty někomu druhému. Dochází zde k tomu, že agresor je zde pouze jakýmsi prvním impulzem a spouštěčem. On poskytne prvotní impuls ke vzniku kybernásilí a zbytek pak nevědomky vykonají ostatní účastníci v kyberprostoru. Jedná se o situace, kdy například agresor disponuje videem s choulostivým obsahem oběti, ten jej zveřejní na internetu a ostatní uživatelé, kteří obsah shlédnou a nějakým způsobem ho hanlivě komentují, se taktéž nevědomky dopouštějí kyberšikany. Stává se i to, že útočník si založí falešný profil pod identitou oběti nebo se dokonce naboural oběti do reálného účtu a kontaktuje tak blízké a přátele oběti [22].

2.3.2 Aktéři kyberšikany

1. ***Kyberagresor –*** Agresorem na poli kyberšikany bývá jedinec, který disponuje jinými zbraněmi k ubližování, než je fyzická síla, ale jeho zbraní je právě zdatnost v oblasti ICT. Po emoční stránce nejsou všeobecně agresoři schopni vcítit se do druhých, proto se svými agresivními útoky nepřestávají a často si ani neuvědomují, že ostatním ubližují. Právě díky relativní anonymitě, kterou jim virtuální svět poskytuje, se také často s obětí nesetkávají tváří v tvář, čímž nevidí jejich bolest a trápení. Následkem toho agresor také necítí pocit viny a nemá výčitky svědomí a jeho útoky mohou mít vzestupnou tendenci [13].

   Typy kyberagresorů:

   a) **Vtipálek –** kyberagresor v tomto případě upravuje, videa a fotky jedinců v nepovedené a neúměrné legraci, neuvědomuje si následky svých činů.

   b) **Neúmyslný kyberagresor –** Tento typ kyberagresora se většinou činu dopustí pod vlivem vzteku a afektu a nejedná cílem úmyslně zranit a poškodit. Jednají většinou v reakci na podnět (diskuse, debaty) V případě obvinění z kyberšikany bývá překvapen, protože si neuvědomuje to, že jeho jednání je v rozporu se zákonem.

   c) **Pomstychtivý andílek –** jedná se o jedince, který již zkušenosti s kyberšikanou či šikanou má. On sám nebo někdo z jeho blízkého okolí se stal sám obětí, což ho vede k tomu se mstít s pocitem, že koná dobro.

d) **Sprostá holka –** nejčastěji se jedná o dívky, které „útočí“ na jiná děvčata nebo chlapce z důvodu zahnání nudy. Svým konáním se snaží získat si obdivovatele a sledující. Myslí si, že tím získá popularitu mezi vrstevníky. Ve chvíli, kdy začíná opadat sledovanost a pozornost ze strany okolí, kyberagresor od svého počínání opouští.

e) **Bažící po moci –** V tomto případě se jedná o nejzávažnější typ agresora. Jeho cílem je manipulovat a ovládat své oběti prostřednictvím strachu. Útočník vystupuje jako silný, autoritativní a nebojácný jedinec. Po obětech vyžaduje, aby dělali přesně to, co on požaduje právě pod nátlakem a výhružkami [26].

2. ***Oběť*** **–** oběti jsou jedinci, kteří bývají velmi často nějakým způsobem zranitelní. Mnohdy se jedná o jedince, kteří mají velmi nízké sebevědomí a často bývají úzkostní. Tyto osoby mívají i problém v oblasti sociálních vztahů a hůře navazují nová přátelství, mají problémy v komunikaci. Dalším charakteristickým prvkem, kterým se oběť vyznačuje, může být určitý druh postižení ať už mentální či fyzické. Může se jednat o jakoukoli jinou další odlišnost, jako bylo uvedeno výše v kapitole o šikaně. Charakteristické znaky oběti v případě šikany i kyberšikany jsou velmi shodné. Ale v případě kyberšikany se může jednat i o takové jedince, kteří se vymezují základnímu profilu, který je pro oběti typickým. U kyberšikany se může jednat o jedince fyzicky zdatného jedince bez psychických problémů. Obětí se zde může stát jednoduše kdokoli bez ohledu na pohlaví, věk, rasovou příslušnost apod. [17]. Určité rozdíly v následcích mezi fyzickou šikanou a kyberšikanou shledává Vágnerová v tom, že každý jednotlivý útok v případě fyzické šikany je svým způsobem jednorázová ukončená záležitost. V případě kyberšikany se jedná o stálý a trvalý tlak na jedince, který se neustále vrací a díky úložišti na sociálních sítích se obsah snadno uchovává [25].

   Ve většině případů se obětí stávají jedinci, kteří žijí velmi aktivně na sociálních sítích a on-line životem. Amanda Lenhart ve svém výzkumu uvádí, že nejčastěji se obětí kyberšikany stávají dospívající, kteří aktivně užívají sociální sítě jako je Facebook, My Space, Instagram apod [27].

3. ***Přihlížející*** **–** Jedná se o takové jedince, kteří se stávají součástí kyberšikany a mnohdy o tom ani neví, jelikož nevidí modřiny a přímé násilí. Ale v kyberprostoru už pouhé zhlédnutí, přeposílání videa nebo kompromitujícího materiálu stačí [10].

2.4 Kyberšikana ve školním prostředí

Následující kapitola bude zaměřena na kyberšikanu ve školním prostředí. Jak bylo zmíněno již výše, kyberšikana je druh šikany, která probíhá v kyberprostoru tudíž je pro školu velmi těžké se do jejího řešení zapojit nebo ji dokonce jen detekovat. V dnešní době se bohužel s klasickou šikanou setkáváme prakticky na každé škole a vzhledem k tomu, že je kyberšikana druhem šikany je mezi nimi velká provázanost. Michal Kolář jako jeden z mnoha autorů, kteří se zabývají problematikou šikany a kyberšikany ve své publikaci uvádí, *„aby mohl člověk vyřešit problém s kyberšikanou nebo vůbec odhalit její přítomnost, musí mít ten dotyčný jedinec dostatečné znalosti a dovednosti v oblasti ICT.“* Dále je důležitá informovanost ve znalosti klasické šikany [28].

Zde vyvstávají otázky, kdy a do jaké míry by se měl pedagog problematikou kyberšikany zabývat. Jde o to, že je-li dítě šikanováno právě virtuálně na internetu a ostatní kamarádi či spolužáci se mu posmívají na to konto právě ve škole je tento případ klasifikován jako tradiční šikana nikoli kyberšikana. Škola by se dle MŠMT [11] měla kyberšikanou zabývat hned od prvního momentu, kdy se o ní dozví. Obzvláště je to nutné řešit v tom případě, kdy k pořízení kompromitujícího materiálu dojde právě na území školy, i když je dále využit na ublížení v internetovém prostředí. Proto by se škola měla aktivně podílet na boji proti kyberšikaně. Dále by měla zajistit zdravé klima, minimalizovat možnosti vzniku problémů, případně poskytnout pomocnou ruku a minimalizovat dopady na oběť, když už ke vzniku problému došlo [29].

2.4.1 Bezpečnostní aspekty a prevence kyberšikany

V případě prevence kyberšikany se setkáváme s dvojím úskalím. Prvním z nich je fakt, že je mnohdy podceňována a samotné ignorování její přítomnosti v dnešní moderní společnosti vede akorát k prohloubení samotného problému. Další problém v prevenci bývá ze strany rodičů, a to z toho důvodu, že ti nemají dostatečný přehled nad tím, jak dítě technologie využívá. Často se setkáváme ze strany rodičů s argumentem, že děti jsou technologicky dál. Rodiče přenášejí odpovědnost na školu, zejména tak na hodiny ICT. Hlavní příčinou vzniku kyberšikany bývají tzv. ***nulové hranice*** – dítě vyrůstá, aniž by mělo pevně stanovené hranice v reálném životě a už vůbec ne v internetovém prostředí. Není ale důvod hranice stanovit pouze pomocí příkazů a zákazů. Ve fungujících rodinách většinou vycházejí dobře nastavené mantinely přirozenou cestou. To, že má dítě stanovené hranice, neznamená, že ve vztahu ke svým rodičům je nesvobodné. Svoboda má také hranice, a pokud jsou správně nastavené,

jsme v bezpečí a víme, co můžeme očekávat. Jako nutnost prevence je dostatečná informovanost a osvěta již u dětí, které bývají velmi důvěřivé a lehce ovlivnitelné [17].

Základním předpokladem kvalitní prevence ze strany školy je přiznat si, že i kyberšikana stejně jako šikana se ve škole může vyskytovat. Proto je nutné pracovat na tom, aby se problému dalo předejít nebo v případě již vzniklého problému na něj uměla škola reagovat. Proto je dobré pracovat na preventivních programech. Stanovit správný postup při prevenci bývá mnohdy obtížné. Pouhé odstranění závadného materiálu ze sítě není řešením. Ano, může šíření poněkud zpomalit, ale pokud kompromitující materiál již někdo získal k sobě do počítače, je pravděpodobné, že jej bude šířit na více platformách. Potom už se jedná o lavinovou reakci. Zdárným příkladem je příběh Ghislaina Razy známý také pod názvem Star Wars Kid. Jednalo se o situaci, kdy Ghislain Raz jakožto fanoušek Hvězdných válek natočil choreografii, kde bojuje s imaginárním světelným mečem. Video se dostalo mezi jeho spolužáky, kteří video publikovali veřejně na sociální sítě. Lidé se veřejně vyjadřovali k tělesným proporcím, a ne příliš zdařilému ztvárnění zamýšlené choreografie. Ghislain takovou pozornost neunesl a skončil v psychiatrické léčebně.

Jak už bylo zmíněno v předchozích kapitolách, tak se kyberšikana jako jedna z forem šikany řadí mezi společenské neboli sociálně patologické jevy. Stejně tak jako šikana vzniká primárně tam, kde je pro ni vhodné prostředí, což ve většině případů bývá právě tam, kde není prevence. Podle školní inspekce je škola povinna řešit projevy šikany, ale také přijímat a realizovat co možná největší možná preventivní opatření [30]. Školský zákon uvádí, že *„školy a školská zařízení jsou povinny zajišťovat bezpečnost a ochranu zdraví dětí, žáků a studentů v průběhu všech vzdělávacích a souvisejících aktivit, a současně vytvářet podmínky pro jejich zdravý vývoj a pro předcházení vzniku sociálně patologických jevů.“* [31].

2.4.2 Přímé kroky v prevenci kyberšikany ve školním prostředí

Prevence v oblasti kyberšikany je v dnešní době nutností. Vzhledem k cílové skupině, na kterou je práce zaměřena, se práce zabývá primárně prevencí na půdě školy a školských zařízení. Neopomenutelná je také prevence v rodině.

Preventivní výchova a společné vzdělávání **–** S žáky je pracováno na upevňování mezilidských vztahů v kolektivu i mimo něj a je nastavováno zdravé školní a třídní klima. Pedagog zodpovídá za rozvoj a upevňování vztahů, přičemž k realizaci využívá všemožných her na zmírnění agrese a podporuje morální hodnoty jedinců i kolektivu. Právě podpora

těchto schopností a dovedností by měla vést k tomu, aby žáci byli schopni rozeznat šikanu a kyberšikanu od škádlení, a hlavně aby věděli, co dělat v případě, když se v jejich blízkosti šikana či kyberšikana objeví [28].

Realizační tým – V případě, kdy už jsou zachyceny jakékoli známky náznaku šikany či kyberšikany, je nutné zajistit vhodný tým odborníků, kteří budou na řešení daného problému spolupracovat. Nezbytností je přítomnost třídního učitele, metodika prevence, výchovného poradce, vedení školy a v krajním případě i školní psycholog.

Obecný postup řešení šikany/kyberšikany na půdě školy:

1. Při zachycení nevhodného až nežádoucího chování na půdě školy (i mimo ni) nikdy **nezlehčujeme, nedegradujeme** a k situaci přistupujeme s vážností a respektem.
2. Rozhovor s obětí a agresorem je vždy **diskrétní** a vedený **odděleně**. Nikdy nesmíme dovolit, aby oběť byla jakkoli konfrontována s agresorem. Musí být v první řadě zajištěna **bezpečnost** dětí. Sbírání informací je nutné pro následnou komunikaci s rodiči oběti, rodiči agresorů či příslušnými orgány jako je orgán sociálně-právní ochrany dětí (OSPOD) či Policie ČR apod.
3. Nemáme-li dostatečné informace v dané problematice a sami si nejsme jisti, jak situaci řešit, neváháme využít rad **odborníků.**
4. Musí být svolán **realizační tým**, kdy je uskutečněn právě rozhovor s agresorem či agresory, je-li jich více. Ale i takový rozhovor musí dodržet pravidlo, že každý z nich je vyslýchán samostatně. Dále je nutné dohlédnout na to, aby se nemohli společně na výpovědi domluvit. Z takto svolané výchovné rady je potřeba udělat zápis.
5. Je vyžadována **zvýšená důslednost** ze strany pedagogických i nepedagogických pracovníků při dodržování řádů, pravidel a stanovených norem.
6. **Prevence ve výuce** – sám pedagog by měl být schopen pracovat s prostředím tak, aby záměrně neutvářel napětí, stres či jiné podněty, které vedou žáky k následnému uvolnění, které se může projevovat i agresivní či jinak škodlivou formou. Mezi konkrétní nevhodné situace můžeme zařadit ***veřejné vyhlašování výsledků testů, srovnání žáků mezi sebou, ponižování a zesměšňování žáků, křik, vyhrožování, neohlášené testy apod*** [32].

2.5 Sociální sítě

Sociální sítě jsou platformy, které nabízí uživatelům určité aktivity, možnosti a různý obsah. Obsah může být dál regulován specifickou skupinou uživatelů dané platformy. Bez uživatelů by sociální sítě ztrácely význam. Na sociálních sítích se můžeme často setkat s pojmem **influencer.** Jedná se o člověka, který obsahem, jenž nahrává na internet, ovlivňuje větší skupinu lidí. Ve většině případů se kyberšikana a ostatní formy kyberšikany odehrávají prostřednictvím sociálních sítí. V následujících podkapitolách budou zmíněny některé oblíbené sociální sítě a jejich rizika [33].

2.5.1 Facebook

Sociální síť Facebook je velmi oblíbená napříč všemi věkovými kategoriemi. Tato sociální síť funguje tak, že si uživatelé přidávají do přátel své známé, rodinu a přátelé mohou zveřejňovat své fotografie, statusy a příběhy na jejich profil. Také je zde možnost chatovat mezi všemi uživateli této sociální sítě. Uživatelé mohou zveřejňovat příspěvky pouze pro své přátele, ale také veřejně pro všechny uživatele, kteří jsou na Facebooku zaregistrováni.

Při používání této sociální sítě je potřeba si uvědomit, že je minimálně vhodné se chovat obezřetně v tom co zveřejňujeme. Neměli bychom zveřejňovat naše adresy, fotografie našich domů a celkově majetku. Také bychom určitě neměli veřejně psát, že budeme mimo naše bydliště, protože pokud jsou příspěvky veřejné, nikdy nevíme, kdo využije této příležitosti a vykrade nás. V neposlední řadě je velice důležité ověřovat si, zda si píšeme s člověkem, kterého známe a nevydává se za něj někdo jiný. Také je důležité mít přehled o tom, s kým si píší děti, protože existují vážná rizika jako je kyberstalking, kybergrooming.

Na Facebooku uživatelé zveřejňují různé kompromitující fotografie, které mohou být příčinou kyberšikany. V poslední době se také vyskytuje mnoho phishingových útoků, při kterých je nutné být velmi opatrný na co klikneme a jaké údaje sdělíme. U této sociální sítě máme také možnosti různých diskusí u příspěvků skupin, nebo uživatelů. V některých případech se do těchto diskusí zapojí osoba, která se snaží uměle vytvořit konflikt. Takové jednání se nazývá trolling. Také se v těchto diskusích může objevit agresivita a vulgární nadávky, kterým se říká flaming [34].

2.5.2 Instagram

Instagram byl vytvořen v roce 2010 původně jako mobilní aplikace pro Apple, ale po čase byla zpřístupněna i pro Android zařízení. Roku 2012 byla tato sociální síť odkoupena společností Facebook a poté byl umožněn přístup i přes webové stránky.

Instagram funguje na principu sdílení fotografií a krátkých videí u kterých si mohou uživatelé vzájemně projevovat zalíbení pomocí srdíčka, které znamená: „to se mi líbí“, slangově je tento krok nazýván jako „lajkování“. Dále existuje možnost komentování těchto příspěvků, pokud tedy nejsou komentáře vypnuty od uživatele, který obsah sdílí. Příspěvky se na profilu zobrazují, dokud je uživatel nevymaže. Na profilu se také vyskytují fotografie, které se nazývají **příběhy** a jsou přítomny na uživatelském profilu 24 hodin a lze na ně reagovat komentářem, který se zobrazí v soukromé zprávě. Také lze využít možnost živého vysílání, kdy uživatel komunikuje s dalšími uživateli pomocí videa a chatu v reálném čase.

Jsou dvě varianty nastavení profilu uživatele, a to soukromý nebo otevřený. U soukromého profilu nejsou příspěvky viditelné do doby, než uživatel potvrdí žádost o sledování. Naopak, pokud má uživatel otevřený profil, tak na veškeré příspěvky se může podívat kdokoliv, kdo si tento uživatelský profil vyhledá [35]. Obecně je bezpečnější mít založený soukromý profil a korigovat si, kdo může vidět naše příspěvky. Všeobecně je vhodné být obezřetný nad tím, co uživatel zveřejní kvůli jeho bezpečí nejen na sociální síti, ale i v reálném životě. Při komunikaci na sociální síti nikdy nevíme, s kým doopravdy komunikujeme. Jak bylo zmíněno v podkapitole výše, je velmi nebezpečné sdělovat určité informace a to například: jaký vlastníme majetek, kde bydlíme, kam a na jak dlouho jedeme na dovolenou. Dále bychom neměli posílat fotografie, které nechceme, aby byly někdy zveřejněny a mohly by nám, jakkoliv ublížit atd. Na sociálních sítích se velmi často vyskytují praktiky krádeže identity což znamená, že na sociálních sítích existují profily, které nejsou pravé, ale člověk si může stáhnout fotografii z internetu a vydávat se za někoho jiného. Za tímto profilem se může skrývat nebezpečný člověk, který si vytipuje oběť a ta může být obtěžována kyberstalkingem a kybergroomingem, tyto pojmy byly uvedeny a popsány výše. Na Instagramu se také vyskytují různé profily, které ve většině případů zveřejňují diskuse a kompromitující materiály, uživatelé je různě komentují a posílají si je mezi sebou a dalšími sociálními sítěmi, toto počínání je označováno jako jedna z forem kyberšikany. Také u zasílání fotografií bychom měli být obezřetní a nikdy neposílat fotografie, které nechceme, aby byly přítomny veřejně. Ve většině případů takové intimní fotografie vznikají a posílají si je mezi sebou partneři. Na Instagramu je možnost posílání fotografií do soukromých zpráv, které mají po

zobrazení zmizet, ale existuje velké riziko, že si druhý uživatel pořídí záznam obrazu této fotografie. Po rozchodu může dojít k vydírání tzv. sextortion. Tato rizika jsou nejvíce nebezpečná pro děti a dospívající, protože si neuvědomují, co vše se může stát při různém počínání si na sociálních sítích a na koho se v některých případech obrátit. Pomocí rodinného centra mohou mít rodiče dohled nad svým dítětem, a to konkrétně nad tím kolik času na Instagramu stráví, popřípadě tento strávený čas omezit, dále jací uživatelé dítě sledují, a naopak. Pokud dítě některého z uživatelů „nahlásí“, rodičům přijde oznámení. Nahlášení je takzvané oznámení nevhodného obsahu, nebo obtěžování jiným uživatelem [36].

2.5.3 Tik Tok

Tik Tok vznikl roku 2018 a je velmi oblíbený především mezi dětmi a dospívajícími. Tato sociální síť slouží ke sdílení videí s různými efekty a hudbou. Tato videa uživatelé natáčí na různou tématiku. Stejně jako předchozí sociální sítě, které byly zmíněné v předchozích podkapitolách, má Tik Tok jistá rizika.

Objevují se dva způsoby jak influenceři a celkově uživatelé mohou využívat tuto sociální síť k výdělku. První způsob, jak influencer může vydělat jsou reklamy, které vytvoří pro firmy a jejich produkty. Druhý způsob jsou živá vysílání, kdy uživatelé, kteří toto vysílání sledují mohou posílat dary, které mají různou hodnotu uživatelům, kteří živé vysílání realizují. Tyto dary mohou uživatelé posílat poté co si za reálné peníze zakoupí Tik Tok mince. Uživatelé si poté mohou mince, které získají od svých sledujících proměnit za reálné peníze. Tvůrce má padesát procent z výdělku a zbylých padesát procent si bere Tik Tok. Přehled o mincích mají v peněžence, kterou lze najít v nastavení. I když je zakoupení těchto mincí podmíněno dovršením plnoletosti, bohužel tuto podmínku děti a dospívající obchází. Tento nápad o ocenění kreativity tvůrců se na první pohled zdá jako velmi dobrý. Bohužel v některých případech se objevují situace, kdy influenceři využívají pozornosti převážně dětí a dospívajících a o tyto dary přímo žadoní a maskují to takovým způsobem, že se jedná o soutěž. Soutěž spočívá v tom, že kdo pošle nejcennější dary, toho napíší veřejně na tabuli a soutěž vyhraje. Také Tik Tok podporuje toto posílání darů a odesílá upozornění, ve kterém vybízí k poslání těchto darů takovým způsobem, že pokud uživatel pošle nějaký z darů, má možnost získat odznak. Děti a dospívající mají vidinu toho, že se díky poslání daru před známými influencery zviditelní, proto použijí kartu svých rodičů a nakupují mince a následně tyto uživatele podporují. Další rizika jsou spojená s nevhodností sdíleného obsahu například: sexuální videa, kde figurují i děti, nebezpečné výzvy, videa

o sebepoškozování atd. Toto odkazuje na špatnou kontrolu, která by měla probíhat více důkladně. Profil by měli mít uživatelé kvůli jejich bezpečí soukromý a lokaci vypnutou. Rodiče mohou profil svého dítěte kontrolovat přes nastavení funkce family pairing. Pomocí této funkce lze stanovit čas, který může dítě na Tik Toku strávit, určit jaká videa může sledovat a od koho může dostávat zprávy. V Americe se čím dál častěji spekuluje o tom, že je Tik Tok velkou bezpečností hrozbou a je zde riziko zneužití osobních údajů, dokonce je v některých zemích zakázán v pracovních telefonech, protože pochází z Číny a velmi často čelí různým pokutám a obviněním [37].

2.5.4 Snapchat

Snapchat byl spuštěn roku 2011 v Americe původně pro Apple zařízení a po čase také pro Android. Jeho koncept je založen na posílání fotografií a krátkých videí mezi přáteli. Aby si uživatelé mohli mezi sebou posílat fotografie a videa, musí se stát přáteli na Snapchatu. Rozdíl mezi Tik Tok aplikací a Snapchatem je takový, že na Snapchatu si uživatelé posílají videa a fotografie pouze mezi svými přáteli a pokud chtějí, aby bylo jejich video zveřejněno pro všechny uživatele dané platformy, musí být schváleno správci této aplikace, ale tato možnost není momentálně zpřístupněna pro Českou republiku.

Zaslané fotografie nebo video lze přehrát pouze jednou a na určitou dobu, kterou uživatel, který fotografii nebo video posílá, nastaví. Nastavení délky videa a fotografií lze určit od jedné sekundy do deseti sekund, nebo je zde také možnost, že se video či fotka přehraje několikrát za sebou a není to časově omezeno, ale jakmile tuto fotografii, nebo video odklikneme už nelze znovu zobrazit. Dále je možnost si své fotografie a videa ukládat do galerie v aplikaci.

Uživatelé si mohou mezi sebou psát, ale tento chat také mizí, tudíž pokud uživateli píše někdo nevhodné zprávy a vyhrožuje mu, není možné toto počínání žádným způsobem doložit, což je velké nebezpečí této sítě. Toto mizení chatu je závislé na jeho nastavení. Při psaní zpráv mezi dvěma lidmi je automaticky nastaveno, že chat mizí za 24 hodin od zobrazení, ale lze nastavit, že chat zmizí ihned po zobrazení. Existuje možnost, že chat zůstane viditelný a to, pokud si ho jeden z uživatelů průběžně ukládá. U skupinové konverzace se chat smaže po dni od zobrazení všech uživatelů, nebo po týdnu od odeslání zprávy, pokud ji všichni uživatelé nezobrazí. Dále si uživatel může na profil vložit fotografii nebo video, které je přítomné na 24 hodin. Na Snapchatu existuje mapa, kde se zobrazuje poloha uživatelů, což je velmi nebezpečné a uživatelé by v této možnosti sdílení polohy měli

být obezřetní. Mnoho uživatelů o této možnosti sdílení polohy nemají tušení. Bezpečnější nastavení je toto sdílení polohy zamítnout, nebo ho sdíleli pouze s lidmi, se kterými se znají osobně. Při posílání těchto fotografií a videí je také potřeba si uvědomit, že pokud se jedná o materiál, který nechceme, aby viděl i někdo jiný, neměli bychom ho posílat vůbec, protože i když je tato fotografie či video nastaveno na pár sekund, může si uživatel vytvořit snímek obrazovky této fotografie a přeposlat ji dále [38].

2.5.5 BeReal

BeReal patří mezi nejnovější sociální sítě, existuje od roku 2020 a byla vytvořen ve Francii. Má zajímavý koncept, který je založen na tom, že si lidé posílají fotografie, na které mají dvě minuty na pořízení. Tyto fotografie se žádným způsobem neupravují, protože na to uživatelé kvůli časovému limitu nemají čas ani nástroje na rozdíl od ostatních sociálních sítí, kdy uživatelé vidí a zveřejňují dokonalé a upravené fotky. Přidání přátel funguje na stejném principu jako u ostatních sociálních sítí. Sdílení těchto autentických fotografií funguje tak, že každý den v jiném čase přijde výzva na nafocení fotografie. Pokud uživatel tuto výzvu ignoruje a fotografie nesdílí, nevidí obsah ostatních uživatelů. Tato fotografie se pořizuje přední i zadní kamerou a může se zveřejnit buď pouze mezi přáteli, nebo veřejně po dobu 24 hodin.

Tato sociální síť má také svá rizika. Automaticky je zapnutá poloha u příspěvků, které uživatel sdílí. Tato poloha uživatele lze v nastavení vypnout. Někteří uživatelé sdílení polohy berou na lehkou váhu, tudíž nechávají tuto funkci zapnutou, přičemž toto počínání není bezpečné. Vzhledem k tomu, že tato sociální síť žádným způsobem nemoderuje obsah, objevují se různé nevhodné fotografie a neexistuje rodičovská kontrola. Pro dospívající je nebezpečná i z toho důvodu, že jde obsah zveřejnit i mimo přátele, a to může vést k obtěžování, kyberšikaně a dalším rizikům, která jsou spojena se sociálními sítěmi. Vzhledem k tomu, že má uživatel na pořízení fotografie časový limit a nemá mnoho času na rozmyšlenou, může zveřejnit nevhodný obsah (majetek, zázemí firmy), který může někdo zneužít. Dále je uvedeno v podmínkách, že si s pořízeným obsahem může platforma po dobu 30 let dělat co uzná za vhodné, tudíž je velmi riskantní zveřejňovat některý nevhodný obsah, který se může objevit veřejně naprosto kdykoliv a kdekoliv [39].

2.6 Kyberšikana v legislativě

V případě kyberšikany a šikany u dětí vyvstává otázka, zda jsou děti beztrestné. Děti, které ještě nedovršily patnáctý rok života, nejsou odpovědné za trestný čin ani za přestupek. Pokud se ale dopustí trestného činu, má soud pravomoc uložit mu jedno či více opatření např. zákaz styku s určitou osobou či zákaz zdržovat se na určitém místě. V případě dovršení patnáctého roku života se jedinec stává mladistvým, z čehož vyplývá, že se stává odpovědným za přestupky, kterých se dopustí. Pokud jsou dodrženy náležitosti jeho dostatečné mravní a rozumové vyspělosti, stává se také trestě odpovědný z čehož vyplývá, že mu může být uloženo také trestní opatření ve formě obecně prospěšných prací či odnětí svobody. Kyberšikana ani tradiční šikana nejsou samostatně ošetřeny trestním právem – ani v jednom případě se nejedná o trestný čin či přestupek. Nicméně jak šikana, tak kyberšikana, mohou svými projevy naplňovat skutkovou podstatu trestných činů. Nejčastěji se jedná o tyto trestné činy [40].:

- ***Nebezpečné pronásledování -*** §354, trestního zákoníku (Dále jen „TZ“) – jedná se o dlouhodobé a opakované sledování, kontaktování a omezování jedince v obvyklém způsobu života. Nebezpečné pronásledování je charakteristické pro **stalking.**
- ***Pomluva - §***184 TZ, - *„Kdo o jiném sdělí nepravdivý údaj, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu, bude potrestán odnětím svobody až na jeden rok.“*
- ***Šíření pornografie*** - §191 TZ, „*Ten, kdo pořídí, zašle, zveřejní, zprostředkuje, uvede do oběhu nebo jinak naloží s dílem, které zobrazuje pornografické prvky, je projevované násilí nebo zobrazuje pohlavní styk se zvířetem, dopouští se tak trestného činu.*“
- ***Výroba a jiné nakládání s dětskou pornografií*** - § 192 TZ – „*Se dopouští ten, Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, bude potrestán odnětím svobody až na dva roky.“*

- ***Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací -*** § 230 TZ – *„Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci*.“
- ***Vydírání*** - § 175 TZ – *„Kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy nutí, aby něco konal, opominul nebo trpěl, bude potrestán odnětím svobody na šest měsíců až čtyři léta nebo peněžitým trestem.“*
- ***Podvod*** § 209 TZ - „*Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu“* [40].

3 KDE HLEDAT POMOC

Každému z nás se může stát, že se ocitne v situaci, na kterou sám nestačí. Situace, kdy si nevíme rady a potřebujeme pomoct. Existuje celá řada řešení, které nám s naší nelehkou situací může pomoct. Prvním krokem je přiznat si daný problém a o pomoc si říct. Obrátit se můžeme v první řadě na rodiče, učitele ve škole, poradce, školního psychologa, vedoucího v kroužku, prostě jakoukoli dospělou osobu.

Níže budou uvedena místa, kam se může jedinec obrátit v případě, že přijde do jakéhokoli kontaktu s kyberšikanou. Každá ze zmíněných organizací, společností či webových portálů, se specializuje na odbornou pomoc v krizových situacích, které s problematikou kyberšikany ve virtuálním prostředí souvisí.

3.1 Pedagogicko-psychologická poradna (PPP)

Pedagogicko-psychologické poradny se dle vyhlášky č.72/2005 Sb., o poskytování poradenských služeb ve školách a školských poradenských zařízení, podílí na samotném vzdělávacím procesu především v situaci, kdy dochází k narušení a zkomplikování samotného vzdělávacího procesu. Mezi hlavní činnosti PPP patří právě přímá práce s dětmi, žáky a mladistvými. PPP uděluje doporučení, na základě, kterých je upravena a volena vhodná cesta vzdělávání pro konkrétního jedince. Mimo jiné PPP poskytují i kariérní poradenství, ale s ohledem na téma bakalářské práce je nutno zmínit, že se PPP zaměřují i na prevenci rizikového chování u dětí a mládeže a napomáhají v rozvoji pedagogicko-psychologických kompetencí pedagogů. Personální struktura PPP se většinou skládá z psychologů a sociálních pedagogů a v neposlední řadě se na odborných činnostech mnohdy podílí i sociální pracovníci. Jedná se o činnost ambulantní, ale není výjimkou, že pracovníci PPP navštěvují přímo školy nebo školní zařízení [41].

Možnosti pomoci PPP

- Zjistit, jak jsou žáci připraveni na povinnou školní docházku z hlediska pedagogicko-psychologického.
- Vypracovává doporučení a návrhy podpůrných opatření na základě speciální diagnostiky u dětí se speciálními vzdělávacími potřebami.
- Poskytuje speciálně pedagogickou i psychologickou intervenci.

- U žáků se zvýšeným rizikem neúspěšnosti poskytuje poradenské služby. Zároveň tak je přístupná pro rodiče takových dětí, aby jim zprostředkoval poradenské služby, které pro lepší práci s dětmi potřebují.
- PPP spadají pod zařízení spojená se školským poradenstvím. Kompetence tohoto zařízení jsou orientovány primárně na oblast výchovy a vzdělávání. PPP poskytuje psychologické a speciálně pedagogické služby pro děti a žáky u kterých je nutné posoudit školní zralost. Dále se zaměřuje na vzdělávací programy a metodické materiály pro školy.
- Nezaměřuje se jen na děti, ale také na zákonné zástupce žáků, kterým taktéž poskytuje poradenství.
- V neposlední řadě zajišťuje koordinaci školních metodiků a také prevenci v oblasti rizikového chování prostřednictvím metodika prevence [41].

3.2 Středisko výchovné péče (SVP)

Střediska výchovné péče působí primárně jako součást školských zařízení preventivně výchovné péče a školských zařízení pro výkon ústavní výchovy a ochranné výchovy. První SVP byla založena teprve až v roce 1991, kdy zřízení těchto středisek umožnil zákon o předškolních a školních zařízeních. Střediska výchovné péče slouží především pro odstranění příčin nebo důsledků negativních jevů v sociálním vývoji. Také přispívá ke zdravému a správnému rozvoji osobnosti dítěte. Poskytuje tak všestrannou péči nebo preventivní výchovu pro děti a mládež, které vykazují negativní jevy chování, ale pouze v případech, pokud nevykazují takové negativní chování, které je hodno ústavní či ochranné výchovy ve speciálních zařízeních. SVP poskytují své služby jak ambulantní a interní formou, přičemž poskytují taktéž poradenské služby, nejen dětem a mládeži, ale také jejich zákonným zástupcům či pedagogům. Střediska výchovné péče musí spolupracovat i s psychiatrickými odděleními, které poskytuje taktéž poradenské služby, ale již „vyléčeným“ uživatelům. Dalším z cílů SVP je podchytit prvotní varovné signály výskytu negativních jevů ve vývoji jedince. Následně tyto situace zaopatřit a poskytnout jedinci péči, podporu a rady, jak předejít vážným komplikacím, které mohou z negativního chování vzrůst. Důsledky mohou být kriminalita, poruchy psychického rázu, toxikomanie aj. Klienty středisek výchovné péče bývají ve většině případů děti či mládež z dysfunkčních rodin. Funkce střediska je tak ve vztahu k rodině podpůrná a kooperativní. V žádném případě

se nesnaží rodinu či funkce rodiny nahradit, pouze ji koriguje a vede správným směrem. Základem je úzká spolupráce jak mezi rodinou, tak mezi střediskem, rodinou a školským zařízením, které dítě navštěvuje [42].

3.3 E-bezpečí

E-bezpečí je projekt, který je certifikovaný napříč celou republikou. Je zaměřen na **vzdělávání, prevenci, osvětu, intervenci, výzkum a vzdělávání**. Tyto fenomény řeší primárně v souvislosti prostředí, kde se odehrává. Mluvíme tedy o internetovém prostředí. Specializuje se tak především na kybergrooming, sexting, stalking, kyberstalking, rizika sociálních sítí, spamy, online závislosti, zneužití osobních údajů v prostředí elektronických médií apod. E-bezpečí funguje na principu terénní práce, kdy spektrum cílových skupin je velice široké. Pracovníci centra poskytují přednášky či besedy, na kterých prezentují nejrůznější aktuální problémy spojené právě s nebezpečím na internetu. Vše probíhá na základě modelových situacích a skutečných kazuistik. Projekt E-bezpečí je uznávaný a velmi ceněný u Policie ČR i u Ministerstva školství, mládeže a tělovýchovy (MŠMT), Ministerstva vnitra České republiky (MVČR) [43].

3.4 Aplikace „Nenech to být“ (NNTB)

Projekt vznikl z hlavy tří mladíků, kteří se na základní škole setkali s šikanou, z pozice mlčící většiny. Měli pochopitelně, jak už to bývá, strach ozvat se a projevit nesouhlas. Ve svých 17 letech vytvořili mobilní aplikaci „Nenech to být“. Ta umožňovala dětem anonymně poukázat a upozornit na nevhodné až rizikové chování ve škole, či na rizikové chování konkrétního žáka bez strachu postihu. Celý projekt zaštítilo Ministerstvo školství. Pouhé 4 roky od spuštění platformy se zapojilo 1800 škol. Prostřednictvím aplikace zaregistrovali 8000 upozornění na kyberšikanu, sexuální obtěžování, sebepoškozování a jiná trápení. Postupem času vznikla velká poptávka i ze strany firem, proto byla aplikace v roce 2020 upravena tak, aby se mohla využívat nejen v prostředí dětí a mládeže, ale také u dospělých jedinců. V této aplikaci se ve výběru zvolí instituce, do které člověk dochází a poté vyplní oznámení problému. Oznámení se odešle školou pověřeným osobám, a to například metodikovi prevence nebo školnímu psychologovi. Aplikace je volně ke stažení na Google play, nebo App Store [44].

3.5 Linka bezpečí

Linka bezpečí má nepřetržitý provoz a může na ni zavolat kdokoli. Jedinci, kteří se dostanou na základě jakýchkoli okolností do nepříznivé životní situace, stejně tak jako u výše zmíněných se linka bezpečí hodně zaměřuje na prevenci. Také je možné se obrátit na chat této linky, který je k dispozici denně od 9-13 hodin a od 15-19 hodin, nebo odeslat email. Na této webové stránce je také k dispozici rodičovská linka [45].

4 SOFTWARE PRO TVORBU MATERIÁLŮ

Součástí bakalářské práce je tvorba edukačních materiálů, které se zabývají kyberšikanou a prevencí. Pro tuto tvorbu edukačních materiálů byla provedena rešerše programů, s cílem výběru grafických a video editorů.

4.1 Grafické editory

Grafické editory jsou programy, které jsou určeny k tvorbě a úpravě grafického obsahu, konkrétně k tvorbě různých tiskovin nebo grafických znázornění v digitální podobě či k úpravě fotografií. Grafická tvorba lze zhotovit jako dvojrozměrná, která se dělí na vektorovou a rastrovou, nebo trojrozměrná. Každý grafický program je jiný a odlišuje se tím jaké má prostředí, nástroje a funkce. Dále se pak dělí podle toho, pro jakou grafickou úpravu je určen, zda pro vektorovou, nebo rastrovou. V následujících podkapitolách bude vysvětleno, co je to vektorová a rastrová grafika a budou uvedeny některé z programů, které se k těmto druhům grafiky vztahují. Pokud se bude jednat o placené editory, uvedená cena se bude vztahovat ke květnu roku 2023 a kurzu 1€ = 23,75 Kč, 1$ = 21,66 Kč. Možnosti zakoupení software jsou různé, a to konkrétně jednorázový nákup, kdy si uživatel zakoupí licenci, která udává právo na používání programu na neomezenou dobu, nebo na dobu stanovenou licenční smlouvou. Pro uživatele je také k dispozici varianta ročního plánu, kdy uživatel platí za přístup programu po dobu jednoho roku, v některých případech je tato varianta cenově zvýhodněná, nebo lze platit měsíční poplatek.

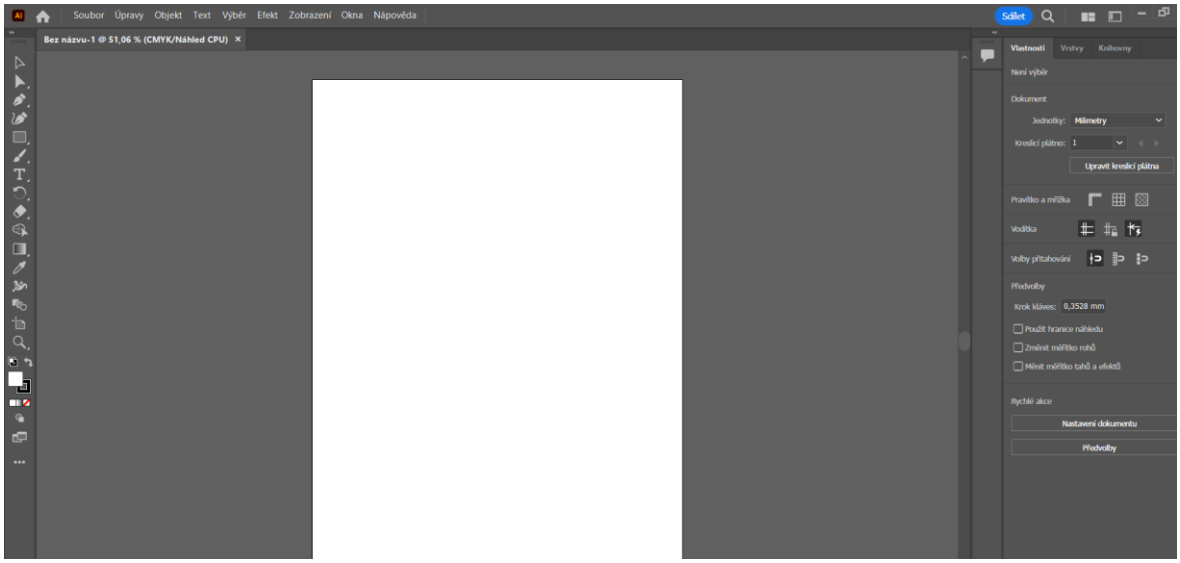
4.1.1 Vektorová grafika

U vektorové grafiky jsou objekty matematicky popsány a jsou využity geometrické útvary. Tyto geometrické útvary jsou přesně definovány pomocí souřadnic počátku, konce a jejich parametrů a je možné popsat jakýkoliv tvar. Díky těmto vlastnostem je vhodná například pro tvorbu animací, ilustrací, logotypů.

U tvorby vektorové grafiky je nesporná výhoda v tom, že při zvětšování a zmenšování objektů neztrácí na kvalitě a také při tvorbě obrázků lze s každým z objektů manipulovat zvlášť a obrázky nejsou tak paměťově velké jako u rastrové grafiky, ale pokud je vytvořen složitější objekt, je tento objekt velmi objemný na operační paměť i na grafiku. Tvorba obrázků je náročnější na čas a dovednosti než u rastrové grafiky. Vektorová grafika není vhodná pro barevné plochy. V některých grafických programech lze zrealizovat vektorovou grafiku, ale také rastrovou [46].

Adobe Illustrator

Adobe Illustrator se řadí mezi profesionální grafické editory a jeho primárním úkolem je zpracovávat a vytvářet vektorovou grafiku. Umožňuje vytvářet obrazce, výseče, průhledné objekty, křivky a také převádět rastrovou grafiku na vektory, ovšem zde je potřeba poznamenat, že čím složitější daný obrázek je, tím nepřesnější vektorizace bude. Tento program je placený a jeho cena je 24,19 € (575 Kč) za měsíc, nebo je možné zakoupení balíčku Adobe Creative Cloud, který stojí po dobu prvního roku 36,29 € (862 Kč) měsíčně, přičemž tato možnost se vztahuje i k níže uvedeným programům od Adobe. V tomto balíčku se vyskytuje dvacet programů, které jsou určeny pro editaci fotografií, grafiky nebo videa, což může být výhodné pro uživatele, kteří využívají více programů od Adobe. Tento program, nebo celý Creative Cloud, je možné vyzkoušet zdarma po dobu sedmi dní a také využít studentskou slevu [47].



Obrázek 1: Prostředí programu Adobe Illustrator

CorelDRAW

CorelDRAW je placený program pro vektorovou grafiku a je součástí balíčku Corel Draw Graphic Suite. Při ročním plánu stojí 808 Kč za měsíc a uživatel při zaplacení licence získá více programů. Tento grafický editor je možné si vyzkoušet zdarma po dobu patnácti dní. Pro tvorbu grafického obsahu je možné v jednom souboru tvořit na více stránkách, různě mezi nimi objekty přesouvat a pracovat s nimi [48].

Inkscape

Tento program pro vektorovou grafiku má značné výhody oproti konkurenci, a to konkrétně především to, že je zdarma. Je snadné se v tomto editoru zorientovat, protože je velmi intuitivní a také obsahuje užitečné nástroje a funkce tudíž je jeho úroveň srovnatelná s editory, které jsou placené [49].

Vectornator

Jedná se o alternativu Illustratoru pro systémy s operačním systémem iOS a macOS. Primárně je tedy určen pro iPady, díky kterým je používání této aplikace velmi interaktivní a jednoduché. Aplikace je zdarma ke stažení a podporuje Apple Pencil, tedy nativní stylus pro iPady, díky kterým je editace obrázků velmi ulehčená, sleduje náklon pera a vytváří realistické zobrazení technik [50].

4.1.2 Rastrová grafika

Rastrová grafika, která je označována také jako bitmapová je tvořena pixely, které jsou charakterizovány barvou, jasem a průhledností. Tyto pixely jsou organizovány do rastru a mají své souřadnice (x,y) pomocí kterých tvoří obraz.

Pro tvorbu rastrové grafiky je k dispozici mnoho barevných filtrů, pomocí kterých lze tvořit zajímavé efekty například: rozostřováni, retuš, smazání některých částí fotografie, přidávání odlesků a odrazů, „rybí oko“, atd. Další nespornou výhodu je velké množství barev, pomocí kterých je možné tvořit různé detaily. Protože vytvořené soubory zahrnují informace o každém pixelu, obsahují velkou datovou náročnost. Velká nevýhoda vzniká při zvětšování vytvořeného obrazu, protože se sníží kvalita a obraz je „rozpixelovaný“. Rastrová grafika je nejvíce vhodná pro obrázky, které je potřeba různými způsoby stínovat, tónovat a také pro různou úpravu a práci s fotografiemi. Nejvíce je využívaná pro tvorbu katalogů, letáků, pohlednic a mnoho dalších [46].

Adobe Photoshop

Jedná se o jeden z nejpoužívanějších programů pro editaci rastrových obrázků. Tento program umožňuje pracovat s vrstvami, vytvářet a upravovat obrazce, retušovat nepovedené fotografie nebo pracovat s maskami, výřezy či průhledností. Jedná se o plně placený program, který stojí 24.19 € (575 Kč), ovšem Adobe nabízí pro studenty sníženou cenu, díky které je možné dosáhnout na celý balíček Adobe Creative Cloudu. Je zde možnost připojit

externí grafický tablet, pomocí kterého je editace značně zjednodušená podobně jako je to u Illustrátoru [51].

Adobe InDesign

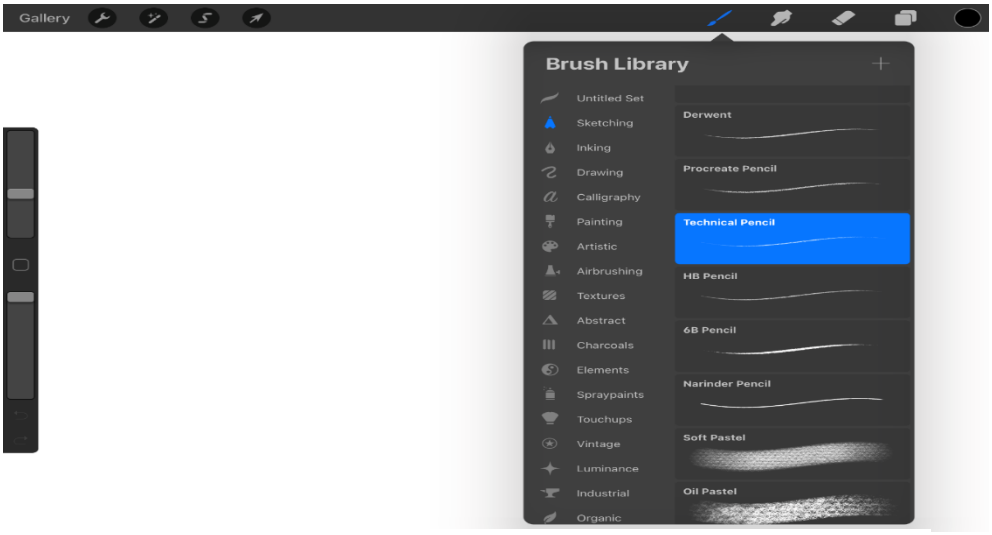
Tento program je placený, stojí 24,19 € (575 Kč) a slouží primárně k sazbě dokumentů a různých brožur. Jedná se o kombinaci Photoshopu a Illustratoru. Je ideální pro tvorbu vícestránkových dokumentů, neboť umožňuje jednoduchou a rychlou správu všech stránek. Může se jednat např. o kalendáře, letáky, časopisy a další podobné tiskoviny [52].

Gimp

Gimp je neplacenou alternativou rastrového editoru. Stejně jako Photoshop, umí i Gimp editovat obrázky, objekty, pracovat s vrstvami, upravovat barevnost či retušovat nedokonalosti na fotografiích. Gimp existuje také jako portable program, tedy není potřeba jej instalovat na pevný disk, ale stačí jej mít umístěný např. na flash disku [53].

Procreate

Tato softwarová aplikace je navržená pro tvorbu ručních ilustrací a je dostupná pouze pro operační systém iOS, a to konkrétně pro iPad či iPad Pro zařízení. Jedná se o placený software, přičemž se neplatí měsíční poplatky, ale pouze jednorázová částka 349 Kč. Stejně jako Photoshop nebo Gimp, umožňuje tento program uživateli vytvářet, upravovat nebo retušovat rastrové obrázky. Je zde však nesporná výhoda oproti stolním aplikacím, a to konkrétně možnost použít Apple Pencil, tedy nativní stylus pro iPady, díky kterým je editace obrázků velmi ulehčená [54].



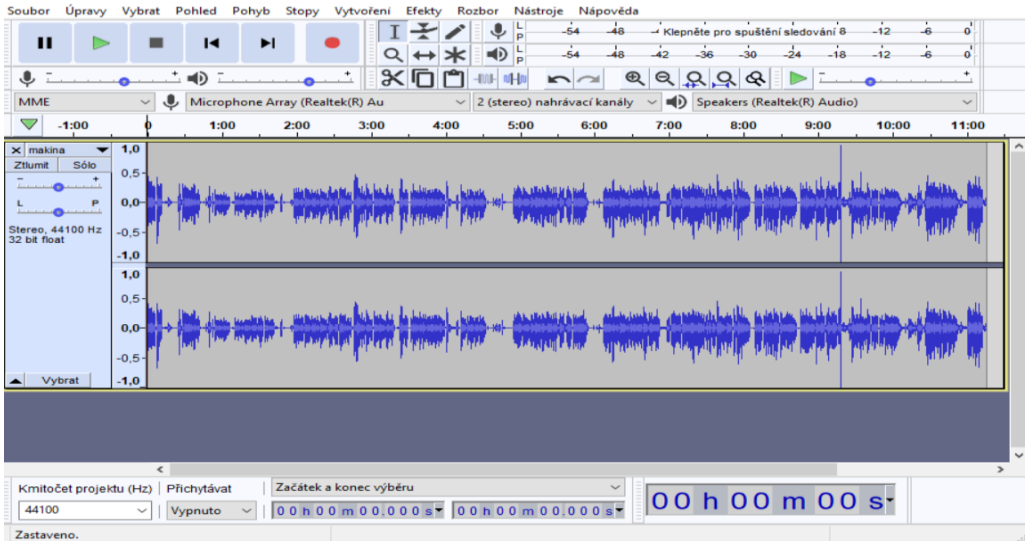
Obrázek 2: Prostředí programu Procreate

4.2 Program pro tvorbu a editaci videa

Programy pro editaci a tvorbu videa můžeme ve všeobecnosti rozdělit na programy pro střih a programy pro video efekty, i když se poslední dobou můžeme setkat s čím dál menším rozdílem mezi těmito dvěma tábory. Samozřejmě se můžeme najít programy placené, tak i s programy neplacené, nicméně pokud se budeme bavit o profesionálním použití, doporučují se spíše ty placené.

4.2.1 Audacity

Tento program slouží pro přímý záznam zvuku a jeho úpravám, jako například změnění rychlosti a přidávání různých efektů. Také je možné převádět různé formáty a exportovat do MP3, WAV a dalších. Mezi jeho hlavní výhody patří to, že je volně ke stažení a k dispozici pro všechny operační systémy. Protože je velmi intuitivní, vyzná se v něm i nový uživatel [55].

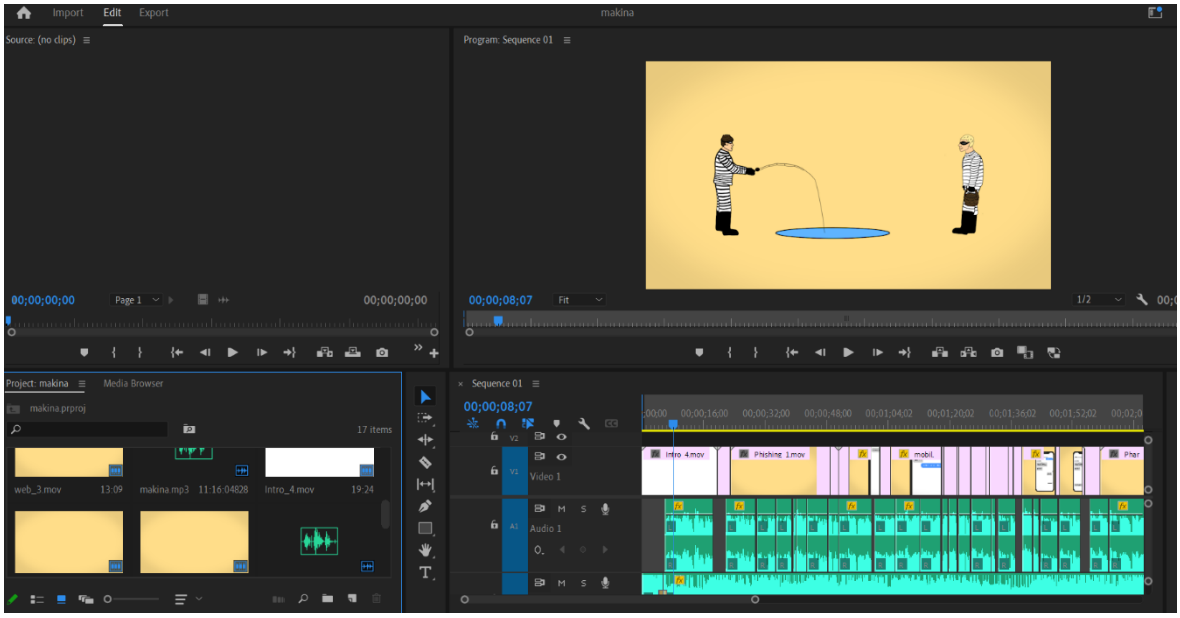


Obrázek 3: Prostředí programu Audacity

4.2.2 Adobe Premiere Pro

Jedná se o profesionální střihový program, který stojí 24,19 € (575 Kč) a umožňuje editaci videa v několika stopách. Pro tvorbu můžeme použít jak videa vytvořená námi, tak také videa, která vytvoříme pomocí interních efektů, tedy například titulkové scény. Je potřeba říct, že se jedná primárně o střihový program, tedy o program, který umožňuje kombinovat několik video i audio stop do sebe. Dále pak umožňuje editovat barevnost daných videí nebo vytvářet různé ořezové masky či aplikovat jednoduché efekty typu rozostření a jiných. Mezi výhody můžeme zařadit to, že pokud se uživatel s programem naučí pracovat, tak je práce

v tomto programu jednoduchá a intuitivní. Jedná se tedy o komplexní program, který umožňuje vytvářet profesionální videa. K nevýhodám může patřit také to, že program může být pro nové uživatele nepřehledný [56].

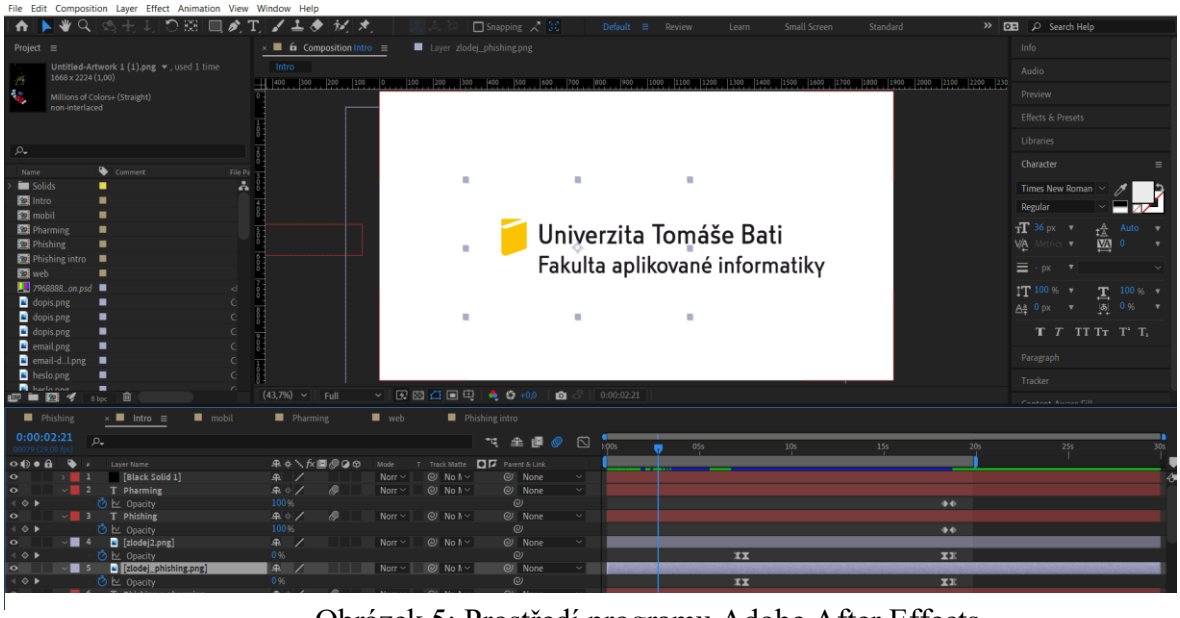


Obrázek 4: Prostředí programu Adobe Premiere Pro

4.2.3 Adobe After Effects

Adobe After Effects je program, který je placený a stojí 24,19 € (575 Kč) je v něm možné vytvářet různorodé animace a efekty. Tyto efekty se následně vyrenderují jako krátké sekvence a v nějakém dalším programu pro editaci, typicky Adobe Premiere Pro, se spojí s hudbou či dalšími audiovizuálními prvky. After Effects samo o sobě umí také pracovat s hudbou a skládat jednotlivé sekvence za sebe, ovšem není to primární úkol tohoto programu. Obvykle se s hudbou pracuje spíše jako se zdrojem dat pro další navazující efekty. Jedná se o program, který ve svém využití nemá téměř konkurenci, protože obsahuje nástroje, díky kterým je vytváření vizuálních efektů poměrně jednoduché. Program je náročný na výpočetní výkon, především na kapacitu RAM paměti.

Premiere Pro je určen k editaci videa, tedy ke zkrácení a spojení video sekvencí, zatímco After Effects slouží primárně k vytváření vizuálních efektů a animací, a to hlavně za pomocí klíčových snímků. Premiere Pro také umí práci s klíčovými snímky, avšak práce s nimi není příliš pohodlná, tudíž je lepší pro tuto práci použít After Effects [57].



Obrázek 5: Prostředí programu Adobe After Effects

4.2.4 Final Cut Pro

Pokud uživatel používá operační systém macOS, je zde varianta střihového programu nativně vytvořeného pro něj. Final Cut Pro je placený program, který je možné zakoupit za jednorázový poplatek 300$ a funguje podle některých uživatelů lépe než třeba Premier Pro, protože není multiplatformní a je zaměřen pouze na macOS [58].

4.2.5 HitFilm Express

Jedná se o obdobu Premiere Pro, ovšem tento program je zcela zdarma a umožňuje používat velkou část nástrojů stejně jako v Premiere Pro. Kombinují se v něm také některé nástroje a fukce z After Effects, např. Motion Tracking, což může některým uživatelům přijít vhod, pokud nechtějí platit měsíční sazbu u Adobe [59].

II. PRAKTICKÁ ČÁST

5 DOTAZNÍKOVÉ ŠETŘENÍ

Součástí bakalářské práce je vyhodnocení dat z výzkumného šetření. Jejímž cílem bylo zjistit povědomí respondentů o problematice, na kterou je práce zaměřena. Součástí vyhodnocení je také samotná interpretace zjištěných výsledků.

5.1 Popis dotazníku a sběr dat

Výzkumná část byla uskutečněna na Základní škole náměstí Míru 83 v Kojetíně se souhlasem ředitele školy. Sběr dat byl realizován pomocí anonymního dotazníkového šetření (viz. příloha I), které se uskutečnilo formou fyzicky vytisknutého dotazníku, protože škola má pouze jednu učebnu, kde jsou přístupné počítače a prostor pro vyplnění dotazníků byl umožněn pouze v hodinách občanské výchovy, v níž nejsou k dispozici počítače.

Položky v dotazníku

- **položky nestrukturované (otevřené) –** respondent není ve svých odpovědích nijak omezen. Má možnost rozepsat se. V dotazníku se jedná konkrétně o položky č. 12-16.
- **položky strukturované (uzavřené) –** Jedná se o takové otázky, kde mají respondenti předem stanovený výčet možností, ze kterých vybírají. Jedná se o položky č. 1-11.

Při sestavování dotazníku byl kladen důraz na dodržení všech náležitostí a zásady, které jsou pro tento druh výzkumného šetření dané.

5.2 Stanovení síle a výzkumných otázek

Výzkum práce byl cílen na informovanost a obecné povědomí studentů základních škol o kyberšikaně a jejich aspektech, ale primárně o bezpečnostních aspektech. Výběr studentů druhého stupně základních škol byl úmyslný. Na základě osobních zkušeností i z dosavadních výzkumů bylo vypozorováno, že právě tato cílová skupina je samotnou kyberšikanou nejvíce ohrožena. Centrum prevence rizikové virtuální komunikace pomocí portálu E–bezpečí uvádí, že kyberšikana nebo šikana má zrod ve škole. V mnoha případech se ukázalo, že kyberagresor a oběť pochází ze stejné školy [43].

5.2.1 Stanovení cílů

Hlavní cíl:

Zjistit povědomí žáků o kyberšikaně a zabezpečení prevence.

Dílčí cíle:

- Zjistit, zda mají žáci základní znalosti o problematice kyberšikany, případně kde se s pojmem setkali.
- Zjistit, zda oni sami přišli do styku s kyberšikanou.
- Zjistit, zda jsou žáci informovaní o možnostech pomoci a řešení.

5.2.2 Výzkumné otázky

Hlavní výzkumná otázka:

- Jaká je informovanost žáků ZŠ v oblasti kyberšikany a následná prevence ve stejné oblasti?

Dílčí výzkumné otázky:

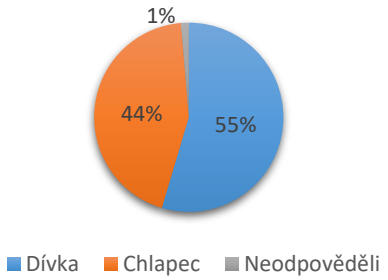
- Mají žáci povědomí o kyberšikaně? Kde se s pojmem setkali?
- Byli žáci v přímém kontaktu s člověkem, který byl účastníkem, nebo obětí kyberšikany?
- Jak si žáci myslí, že je možné vyřešit kyberšikanu?
- Vyskytuje se ve škole, nebo v okolí žáka člověk, nebo společnost, která poskytuje pomoc obětem kyberšikany?

5.3 Analýza a interpretace dat

Z celkového počtu 160 respondentů bylo vyřazeno osm dotazníků. Důvodem k vyřazení bylo to, že v dotazníkovém šetření si hned v úvodu zvolili variantu, že se nechtějí zúčastnit výzkumného šetření. Vzhledem k tomu, že dotazník byl anonymní a dobrovolný, tato volba byla respektována. Ve finále se tedy pracovalo se 152 respondenty.

Otázka č. 1:

První otázka se týkala pohlaví dotazovaných. Z celkového počtu 152 respondentů se výzkumu zúčastnilo 55 % dívek a 44 % chlapců (viz. Obrázek 6). Zbylé jedno procento tvořili dva respondenti, kteří v otázce na pohlaví svou odpověď neuvedli.

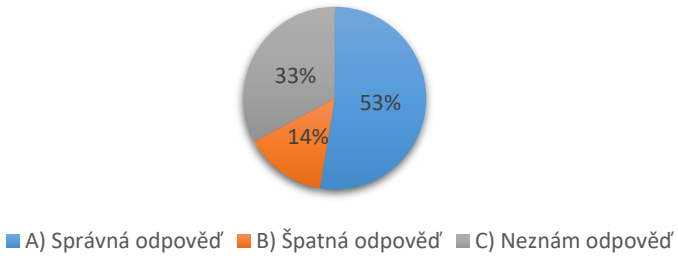


Obrázek 6: Struktura odpovědí na otázku zabývající se pohlavím respondentů

Otázka č. 2:

Vyberte vhodný pojem k této definici: „Jedná se o provokování a napadání uživatelů v diskusních fórech, ale také například v komentářích na sociálních sítích. Toto jednání má povětšinou velice hrubý až vulgární ráz.“

V této otázce byla respondentům předložena definice, která se vztahovala k jednomu z nabízených pojmů. Jejich úkolem bylo k definici přiřadit správný pojem. Na výběr měli ze tří možností, z nichž měli vybrat tu, která koresponduje s definicí. Měli také možnost zvolit čtvrtou variantu odpovědi, v případě že neznají správnou odpověď na otázku. Správně odpovědělo 53 % respondentů. Špatné odpovědi volilo 33 % respondentů a 14 % dotazovaných žáků zvolilo variantu, že neznají odpověď. Rozdíl mezi těmi, kteří znají správnou odpověď a těmi, kteří odpověděli špatně či odpověď naznají, je velice malý. Správnou odpověď uvedlo 80 žáků a zbylých 72 nevědělo nebo odpovědělo špatně. Narážíme tedy na neznalost pojmů pojících se s kyberšikanou. (viz. Obrázek 7).

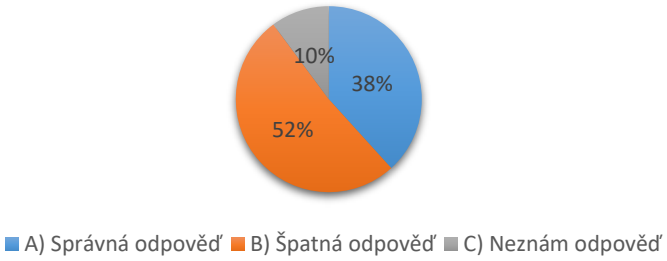


Obrázek 7: Struktura odpovědí na otázku týkající se pojmů flaming a trolling

Otázka č. 3:

Vyberte vhodný pojem k této definici: „Vydírání, ve kterém jsou využita videa a fotografie oběti. Neznámý pachatel vyhrožuje tím, že zveřejní poškozující fotografie a videa oběti, která získal při proniknutí do počítače, e-mailových schránek či účtů do sociálních sítí za účelem poškození osoby. Ve většině případů pachatelé nemají žádné poškozující materiály.“

Stejně jako v předchozí otázce byla předložena definice, která se vztahoval k jednomu z nabízených pojmů. Žáci měli na výběr z několika možností odpovědi. Správně odpovědělo 38 % respondentů, špatnou odpověď zvolilo 52 % respondentů a 10 % žáků neznalo odpověď na otázku (viz. Obrázek 8). Ve většině případů celkem 66 žáků ze 152 nevědělo, jak správně definici přiřadit. A dalších 37 žáků, neznalo odpověď vůbec, lze tedy předpokládat, že problematika tohoto pojmu jim není zcela známá. Pouhých 49 žáků z celkového počtu bylo schopno na otázku odpovědět správně. Ale ani zde není jisté, zda neodpovídali pouze tipem nebo jsou si jistí správností definice.

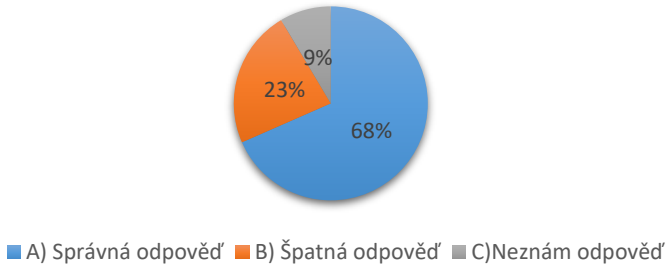


Obrázek 8: Struktura odpovědí na otázku týkající se pojmu Sextortion

Otázka č. 4:

Vyberte vhodný pojem k této definici: „Zneužívání internetu, mobilních telefonů k nebezpečnému pronásledování.“

Ve čtvrté otázce, stejně jako v předchozích dvou, měli respondenti vybrat správný pojem k předem dané definici. Správnou odpověď zvolilo 68 % žáků, což odpovídá 106 dotazovaných respondentů. Zde lze tedy vyvodit, že tento pojem je mezi dotazovanými žáky zažitý a již se s tímto pojmem někde setkali. Špatně na otázku odpovědělo 23 % respondentů z celkového počtu a zbylých 9 % žáků nedokázalo přiřadit správný pojem k definici, proto zvolili variantu, že neznají odpověď na otázku (viz. Obrázek 9).

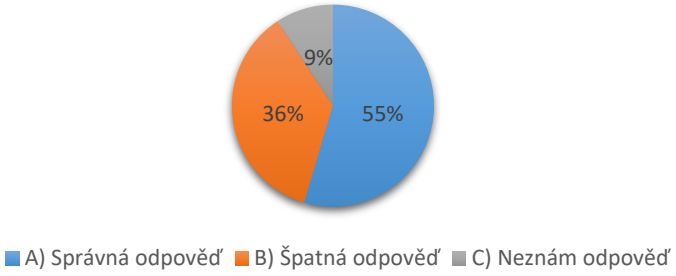


Obrázek 9: Struktura odpovědí na otázku týkající se pojmu Kyberstalking

Otázka č. 5:

Vyberte vhodné pojmenování a definici pro tento obrázek.

V páté otázce byl žákům v dotazníku předložen obrázek, který se vztahoval k jedné definici, která byla zahrnuta mezi nabízenými odpověďmi. V možnostech byla respondentům nabídnuta jedna správná a dvě nesprávné definice. Jejich úkolem bylo přiřadit správnou definici, která by definovala obrázek. Taktéž jako v předchozích otázkách byla pro žáky v nabídce možnost, že neznají odpověď. Správně definici přiřadilo 55 % respondentů, špatně odpovědělo 36 % respondentů a možnost „Neznám odpověď“ zvolilo 9 % z dotazovaných (viz. Obrázek 10).



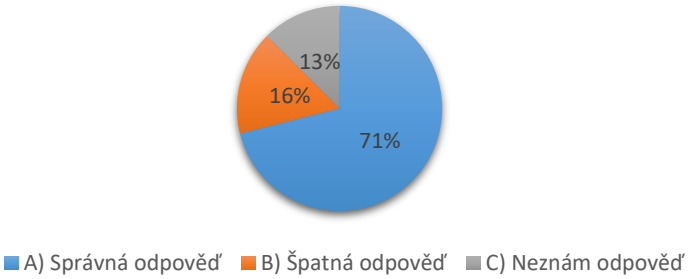
Obrázek 10: Struktura odpovědí na otázku týkající se pojmu Krádež identity

Otázka č. 6:

Vyberte vhodný pojem k této definici: „Elektronické zasílání zpráv, fotografií či videí se sexuálním obsahem. Může být dobrovolné, ale také nedobrovolné.“

V otázce číslo šest měli respondenti opět předepsanou definici a jejich úkolem bylo přiřadit správný nadřazený pojem, který se s definicí pojí. Správnou odpověď zvolilo 71 % dotazovaných, což činilo 108 respondentů. Lze usuzovat, že nápovědou a vodítkem, ke správné odpovědi mohlo žáky vést spojení „sexuální obsah“ v předložené definici. Špatně

odpovědělo 16 % respondentů a možnost, kdy neznali odpověď zvolilo 13 % z celkového počtu dotazovaných (viz. Obrázek 11).

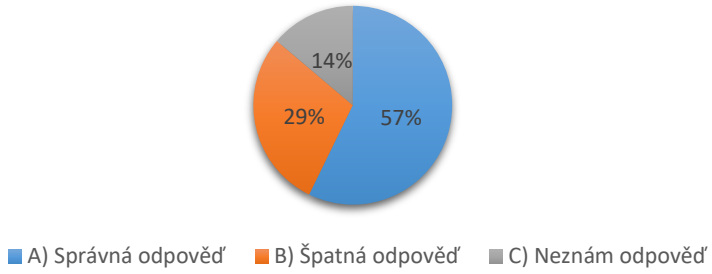


Obrázek 11: Struktura odpovědí na otázku týkající se pojmu Sexting

Otázka č. 7:

Vyberte vhodné pojmenování a definici pro tento obrázek.

Otázka číslo sedm opět obsahovala obrázek, který se vztahoval k jedné z možnosti v odpovědích. Úkolem respondentů bylo přiřadit správné pojmenování a definici k danému obrázku. Opět měli na výběr z několika možností. Správnou variantu zvolilo 57 % respondentů, špatně odpovědělo 29 % a 14 % respondentů neznalo správnou odpověď na otázku (viz. Obrázek 12).



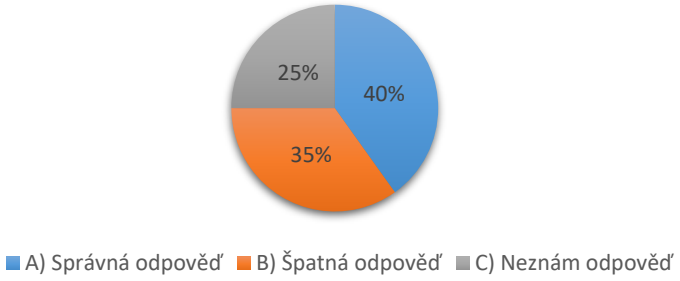
Obrázek 12: Struktura odpovědí na otázku týkající se pojmu Phishing

Otázka č. 8:

Vyberte vhodný pojem k této definici.: „Označuje manipulativní chování, které má přimět uživatele, aby útočníkovi sdělil své osobní údaje na falešných webových stránkách.“

V otázce číslo osm byla žákům předložena definice Pharmingu a jejich úkolem bylo z nabízených možností, zvolit tu správnou. Správně na otázku odpovědělo 40 %, špatně odpovědělo 35 % respondentů. Rozdíl mezi správnými a špatnými odpověďmi tvořilo pouhých 7 respondentů. Lze tedy předpokládat, že problematika výše zmíněného pojmu je

pro žáky novým poznatkem, který je důležitou součástí problematiky, která úzce souvisí s kyberšikanou. Odpověď na otázku neznalo 25 % dotazovaných. Když sečteme počet žáků, kteří odpověděli špatně a ty žáky, kteří uvedli ve svých odpovědích, že neznají odpověď získáme tak 91 respondentů ze 152, kteří neznají význam zmiňovaného pojmu. Tato skutečnost sloužila tedy jako podnět pro utvoření edukačního videa, který by mělo žákům objasnit tento jim neznámý pojem. Video lze má sloužit jako edukační materiál, který lze prezentovat na seminářích připravených pro školy či širokou veřejnost. (viz. Obrázek 13).

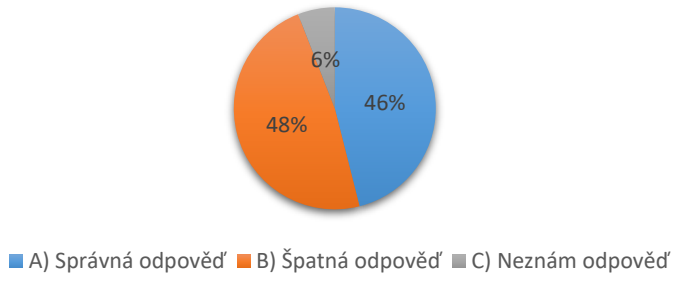


Obrázek 13: Struktura odpovědí na otázku týkající se pojmu Phishing

Otázka č. 9:

Vyberte vhodné pojmenování a definici pro tento obrázek.

V této otázce byl studentům opět předložen obrázek, který zobrazoval situaci kyberšikany. Úkolem respondentů bylo opět přiřadit správnou možnost. Správně odpovědělo 46 % respondentů, špatně odpovědělo 48 % a 6 % neznalo odpověď na otázku. Tato dotazníková položka byla důkazem toho, že problematika není žákům dostatečně známá. Vypovídá o tom fakt, že správně na položku odpovědělo 70 respondentů z celkového počtu dotazovaných. A počet těch, co odpověděli špatně nebo neznali odpověď vůbec, tvoří ve finále více jak polovina dotazovaných a to 82 respondentů. Kyberšikana je základní pojem, na kterém celá bakalářská práce stojí. Proto bylo i v tomto případě vytvořeno edukační video, které se problematikou kyberšikany a vysvětlením pojmu zabývá (viz. Obrázek 14).

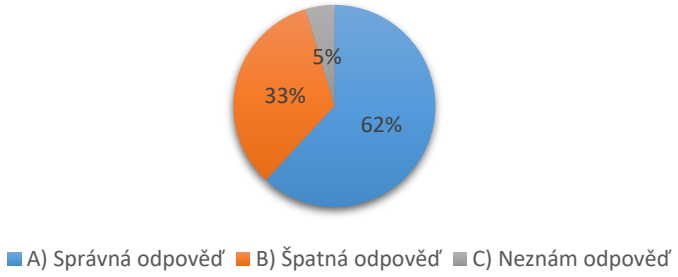


Obrázek 14: Struktura odpovědí na otázku týkající se pojmu Kyberšikana

Otázka č. 10:

Vyberte vhodné pojmenování a definici pro tento obrázek.

Otázka číslo deset opět obsahovala obrázek situace, v tomto případě se jednalo o pojem kybergrooming. Respondenti opět měli na výběr z několika možností, přičemž správná byla opět pouze jedna odpověď. Správnou možnost přiřadilo 62 %, špatně odpovědělo 33 % respondentů a 5 % žáků neznalo odpověď na otázku (viz. Obrázek 15).

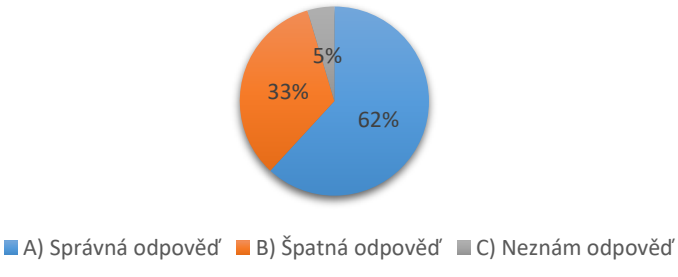


Obrázek 15: Struktura odpovědí na otázku týkající se pojmu Kybergrooming

Otázka č. 11:

Vyberte vhodné pojmenování a definici pro tento obrázek.

Otázka číslo jedenáct obsahovala taktéž obrázkovou situaci, konkrétně se vztahovala k pojmu šikana. Respondenti vybírali z nabízených možností správnou variantu. Správně odpovědělo 94 žáků což tvořilo 62 %. Šikana je pojem, který je hojně diskutované téma, obzvláště u věkové skupiny, kterou tvořili dotazovaní. Předpoklad byl, že procento správných odpovědí bude poněkud vyšší. Chybnou odpověď zvolilo 33 % respondentů a zbylých 5 % respondentů neznalo odpověď na otázku (viz. Obrázek 16).



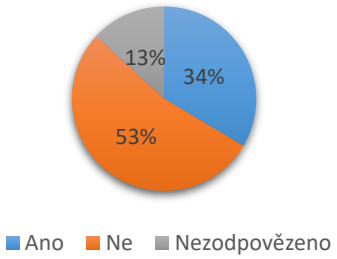
Obrázek 16: Struktura odpovědí na otázku týkající se pojmu Šikana

Otázka č. 12:

Setkal/a ses někdy s kyberšikanou tebe, nebo tvého okolí? Pokud ano, kde?

Otázka č. 12a:

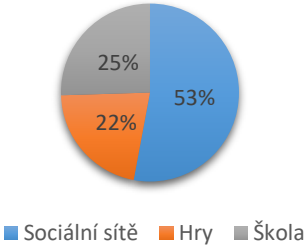
Otázka číslo dvanáct je z důvodu svého charakteru, rozdělena na dvě části. V prvním grafu (12 a) jsou zaznamenány obecné odpovědi respondentů, kdy otázka zjišťovala, zda se respondenti nebo někdo z jejich blízkého okolí s kyberšikanou setkali. V případě, že ano, tak uváděli v odpovědi místa, kde k tomu střetu došlo (viz. 12 b). S kyberšikanou se setkalo 34 % respondentů. Větší procento, konkrétně 53 % respondentů uvedlo, že s kyberšikanou se nesetkali a 13 % dotazovaných na otázku neodpovědělo (viz. Obrázek 17).



Obrázek 17: Struktura odpovědí na otázku týkající se střetu s kyberšikanou

Otázka č. 12b:

Tento graf znázorňuje konkrétní místa, kde se respondenti s kyberšikanou setkali. Vzhledem k různorodým odpovědím, které ale měly společný charakter byly utvořeny kategorie, které obsáhly všechny odpovědi respondentů. Nejčastěji respondenti zmiňovali Facebook, Instagram, TikTok, internet a jiné sociální sítě. Proto byla utvořena kategorie sociální sítě, která všechny tato místa zahrnuje, tuto variantu volilo 53 % dotazovaných. Další samostatná kategorie obsáhla všechny herní portály a služby pro streamování. Variantu „Hry“ zvolilo 22 % respondentů a poslední kategorie byla škola. Z odpovědí respondentů bylo vyvozeno, že tuhle možnost zvolili z toho důvodu, že ke kyberšikaně docházelo přímo na půdě školy, například v době ICT, nebo byl kompromitující materiál spojený s kyberšikanou pořízen ve škole a dále šířen na školních skupinách (viz. Obrázek 18).

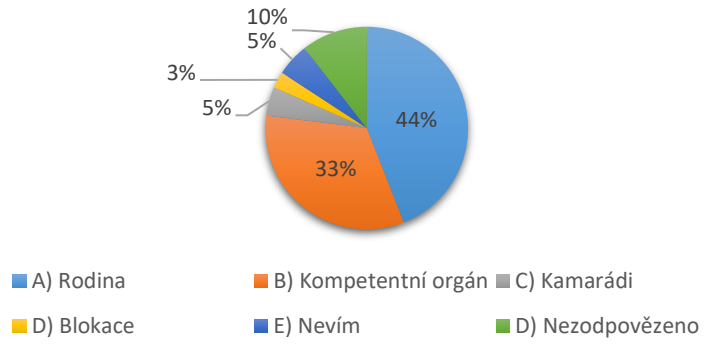


Obrázek 18: Struktura odpovědí na otázku týkající se místa střetu s kyberšikanou

Otázka č. 13:

Kam se se obrátíš, když se staneš obětí nebo budeš svědkem kyberšikany?

V případě otázky číslo třináct se jednalo o otevřenou položku. Respondenti tak měli možnost rozepsat své odpovědi dle svého úsudku bez předložených možností. Opět byly utvořeny kategorie, které obsáhly všechny jednotlivé odpovědi. Do kategorie rodina byli zahrnuti všichni zmínění rodinní příslušníci. Tuto možnost zmínilo ve svých odpovědích nejvíce respondentů, a to 44 %. Další obsáhlejší a nejčastěji zmiňovaná kategorie byl kompetentní orgán. Tato kategorie v sobě ukrývala Linku bezpečí, Policii ČR a učitele. Dále už se jednalo o kategorie méně volené. Někteří respondenti kyberšikanu řeší tak, že nechtěný obsah nebo uživatele zablokují – k této odpovědi se přiklonila 3 % dotazovaných. Někteří respondenti zvolili možnost svěřit se kamarádům, takto odpovědělo 5 % respondentů. Na otázku číslo třináct 16 respondentů neodpovědělo a 8 z dotazovaných uvedlo, že neví, kam a na koho se obrátit v případě střetu s kyberšikanou (viz. Obrázek 19).

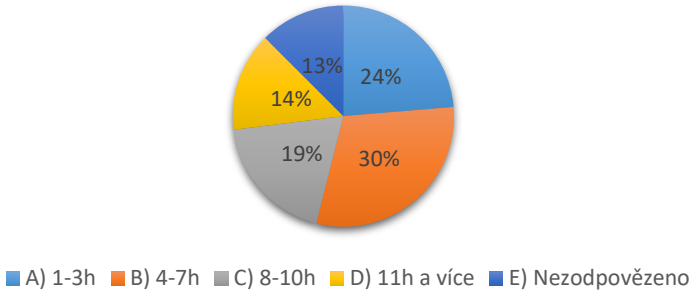


Obrázek 19: Struktura odpovědí na otázku týkající se hledání pomoci

Otázka č. 14:

Kolik času trávíš denně na sociálních sítích a všeobecně na internetu?

Otázka číslo čtrnáct směřovala ke zjištění času, který respondenti tráví na internetu. Výsledky ukazují v celku alarmující čísla. Pouhých 24 % z dotazovaných tráví na internetu něco mezi 1 a 3 hodinami. Nejčastěji zmiňovaný časový úsek byl něco mezi 4 až 7 hod. denně. Obsáhlá kategorie byla také ta, který zahrnovala časový úsek v rozmezí 8 až 10 hod. denně. 14 % respondentů tráví na internetu i více jak 11 hod. denně (viz. Obrázek 20), což je velmi vysoké číslo vzhledem k faktu, že značnou část dne tráví respondenti ve škole. Znamená to, že skoro polovinu dne jsou neustále on-line. Stávají se tak velice ohroženou skupinou z pohledu kyberšikany.

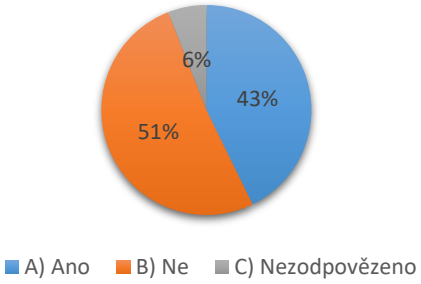


Obrázek 20: Struktura odpovědí na otázku týkající se času stráveného na internetu

Otázka č. 15:

Mají rodiče přehled o tom, co děláš na sociálních sítích?

Položka číslo patnáct směřovala ke zjištění, zda mají rodiče dotazovaných žáků přehled o jejich aktivitách na sociálních sítích a obecně na internetu. U více jak poloviny dotazovaných rodiče nemají přehled o tom, co jejich děti na internetu dělají. U 43 % respondentů rodiče vědí, nebo alespoň tuší co jejich děti na internetu dělají a jak se prezentují. 6 % respondentů na otázku 15 neodpovědělo (viz. Obrázek 21).



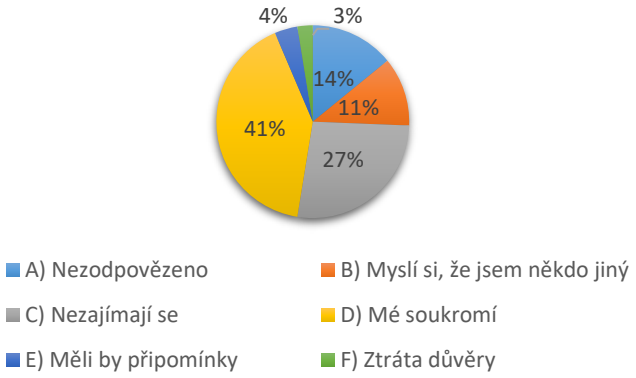
Obrázek 21: Struktura odpovědí na otázku týkající se aktivity na internetu

Otázka č.16:

Pokud jsi v otázce číslo 15 odpověděl/a NE. Napiš, proč nechceš, aby rodiče věděli, co na internetu děláš.

Otázka číslo šestnáct úzce souvisí s předchozí otázkou. Týká se těch respondentů, kteří v otázce patnáct odpověděli NE, tudíž jejich rodiče nemají přehled o jejich aktivitách na sociálních sítích a všeobecně na internetu. Cílem otázky šestnáct bylo zjistit, co je důvodem, proč rodiče o aktivitách svých dětí na internetu neví. Největší procento respondentů uvedlo, že se jedná o jejich soukromí a rodiče nemají právo jim do něj nahlížet. Jednalo se konkrétně o 32 žáků, kteří mají pocit, že kdyby rodiče měli možnost nahlédnout do toho, co na sociálních sítích prezentují, naruší tak jejich soukromí. Dále respondenti hojně uvádí, že rodiče se ani nezajímají o to, co jejich děti na internetu dělají. U 11 % odpovědí

bylo zjištěno, že děti mají strach z toho, že by rodiče zjistili, že se na internetu prezentují jinak, než jací jsou ve skutečnosti. Dále 4 % respondentů uvedlo, že o svých aktivitách rodiče neinformují z důvodu, že si myslí, že by měli nějaké připomínky k tomu, co na sociální sítě přidávají. 14 % respondentů na otázku neodpovědělo. Zbylá 3 % dotazovaných má obavy z toho, že kdyby rodiče věděli, jak se na sítích prezentují, ztratí v ně důvěru (viz. Obrázek 22).



Obrázek 22: Struktura odpovědí na otázku nesdělení aktivit na internetu

Shrnutí

Hlavním cílem výzkumného šetření bylo zjistit povědomí žáků základní školy o kyberšikaně a pojmech s ní souvisejících. Dále bylo úkolem zjistit, zda mají žáci povědomí o možnostech následného řešení problému kyberšikany, pokud se s ní setkají. Na počátku výzkumu byly otázky zaměřeny na teoretická východiska problematiky, kdy bylo zjištěno, že teoretické znalosti pojmů spojené s kyberšikanou mají žáci poměrně v povědomí, ale vyskytovaly se také výsledky, které byly nedostačující. Správné odpovědi mohly být ovlivněny tím, že respondenti měli nabídku možností, ze kterých mohli vybírat. Proto lze usuzovat, že správnost zodpovězených otázek byla ovlivněna vylučovací metodou. Následná hlubší analýza, která se žáků dotýkala osobněji není na dostačující úrovni z hlediska prevence a následného řešení problému spojeného se sociálně patologickým jevem kyberšikany.

V položce, kde se byla otázka zaměřena na to, zda s kyberšikanou někdy přišli do styku, odpovědělo 50 respondentů, že se setkali s kyberšikanou osobně nebo ve svém blízkém okolí. Nejčastěji žáci uváděli střet s kyberšikanou prostřednictvím sociálních sítí. Vzhledem k tomu, že většina z žáků tráví na sociálních sítích a všeobecně na internetu bezmála polovinu dne, je nutností lepší znalost a vědomí toho, jaké nebezpečí jim hrozí.

Cíleně byla v dotazníku obsažena položka, která se respondentů dotazovala na povědomí rodičů o tom, zda mají přehled o aktivitách svých dětí na sociálních sítích. Odpovědi dotazovaných opět poukazují na to, že jsou si vědomi toho, že se na sociálních sítích objevují nevhodné fotografie a rizikové chování, a z toho důvodů s rodiči své počínání na sítích nesdílí. Mají obavy z toho, že by rodiče měli potřebu jejich aktivitu na sítích kontrolovat, či je nějakým způsobem v jejich působení omezovat. Určité procento, konkrétně 21 respondentů, dokonce uvádí fakt, že rodiče nejeví absolutní zájem o to, co jejich děti zveřejňují na svých profilech.

Dále bylo cílem zjistit, zda jsou si vědomi toho kam, případně na koho, se mohou obrátit v případě, že se stanou svědky či přímo obětmi kyberšikany. Z odpovědí lze usuzovat, že konkrétně neví, koho kontaktovat, ale správně uvádějí osoby či složky, které mohou být nápomocny, jako je Policie ČR či rodinní příslušníci. V případě rodiny můžeme říct, že se jedná o první krok k pomoci, ale v žádném případě se nemusí jednat o konečé řešení. Proto byla součástí bakalářské práce vytvořena informační brožura, která má sloužit jako jakýsi průřez problematikou kyberšikany. Dále byl vytvořen informační leták, který obsahuje body, které dětem předesílají, jak se v internetovém prostředí chovat a jak postupovat v případě již vzniklé kyberšikany. Leták obsahuje přímé kontakty na organizace či konkrétní internetové portály, které jsou k přímé pomoci určeny. Pro rodiče byl vytvořený leták, který poukazuje na to, co je důležité u dětí vnímat, jak s nimi komunikovat a také kam se mohou rodiče obrátit v případě problému. Dále byla vytvořena dvě edukační videa – první video poukazuje na podvodné praktiky phishing a pharming, druhé video bylo vytvořeno na téma kyberšikana a její formy, kde jsou řečeny důležité poznatky, které se vztahují k této problematice. Tyto edukační materiály mají sloužit jako první záchytný bod jak přímo pro dítě, tak i pro rodiče a mohou být využity přímo na půdě školy, které je mohou zařadit do svých preventivních programů.

6 TVORBA EDUKAČNÍCH MATERIÁLŮ

Praktickým výstupem bakalářské práce jsou také edukační materiály, které byly realizovány pomocí grafických a video editorů. Jako první byla vytvořena brožura, která se zaměřuje na kyberšikanu. Tato brožura vysvětluje, co je to kyberšikana, jaké jsou její projevy, znaky, typy a formy a jejich objasnění. Dále byly vytvořeny dva letáky, které jsou určeny pro rodiče i děti. Letáky se zaměřují na ukázku různých typů chování na internetu a dávají také praktické tipy, jak by v takových případech měli rodiče se svými dětmi komunikovat.

Byla také vytvořena dvě edukační videa. První edukační video se zabývá phishingem a pharmingem. Toto video bylo vytvořeno na základě nízkého povědomí žáků o této problematice, ale také z důvodu aktuálnosti daného tématu, kdy se tyto podvodné praktiky, které okrádají oběti o důležitá data a peníze, objevují velmi často. Video představuje dva zloděje, jeden ukazuje praktiky phishingu a druhý pharmingu. Zloděj, který představuje phishing stojí u rybníku a loví z něj různá data, přičemž byl tento druh podvodné praktiky ve videu následně vysvětlen. Dále bylo poukázáno na konkrétní případ phishingu, kdy oběť poslala M-platbu, protože si myslela, že pomáhá pouze svému kamarádovi v soutěži a ve finále o své peníze přišla. Druhý zloděj představuje pharming, kdy mu skákají data do košíku. Poté byl opět vysvětlen tento druh praktiky na konkrétním příkladu podvodného e-mailu, kdy oběť vyplnila své údaje od internetového bankovnictví a přišla o své peníze. Bylo poukázáno na to, že je vhodné, aby lidé byli obezřetní.

Druhé edukační video pojednává o kyberšikaně a jejich formách. Toto video bylo vytvořeno jako definice a prevence ohledně kyberšikany a jejich formách. Na rozdíl od prvního videa, které bylo vytvořeno animacemi, na druhém videu je vyobrazena autorka, která hovoří o problematice spojené s kyberšikanou. Konkrétně se video zaměřuje na vysvětlení kyberšikany, jejich projevů, znaků, jaké chování na sociálních sítích a všeobecně na internetu je rizikové a v čem mají být lidé obezřetní, vysvětlení pojmů kybergrooming a krádež identity a stánky na které je možné se obrátit v případě problému.

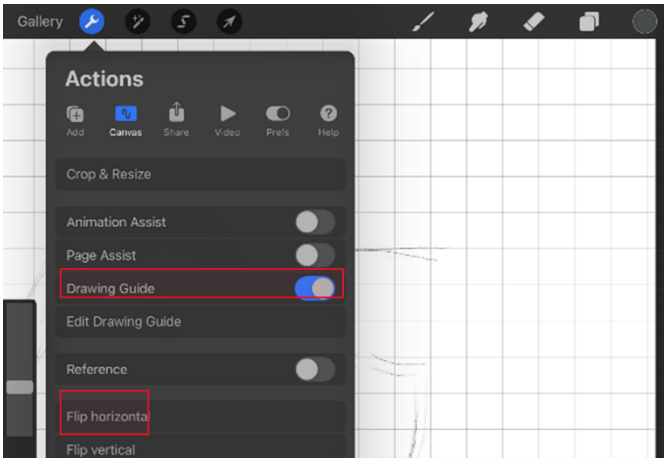
6.1 Grafický obsah

Grafický obsah, a to konkrétně obrázky do dotazníků a videa, letáky a brožura, byly vytvořeny pomocí dvou editorů, a to konkrétně v Procreate a Adobe Illustrator. V Procreate byly realizovány ilustrace a pomocí Illustratoru byly vytvořeny obrázky do videa a také spojen text a ilustrace. Procreate byl vybrán pro realizaci grafiky, protože je jednoduchý na ovládání

a jeho početná nabídka štětců umožňuje vytvářet ilustrace v různých stylech. Dalším důvodem byly pořizovací náklady programu, který je možné pořídit za jednorázový poplatek 349 Kč s doživotní licencí od firmy Apple. Autorka práce vlastní zařízení iPad, pro který je program určen a také stylus tzv. Apple pencil, který na iPadu vytváří pocit skutečného kreslení či psaní na papír s okamžitou odezvou na monitoru zařízení. Apple pencil sleduje náklon pera a vytváří tak realistické zobrazení technik jako je kresba, malba uhlem, akrylovými či olejovými barvami. Ilustrace jsou vytvářeny jako obrazy (bitmapy). Adobe Illustrator byl zvolen z toho důvodu, že se v něm realizují vektorové ilustrace, ale také grafický design obecně. V Illustratoru se běžně vytvářejí loga, ikony, návrhy obalů, design na trička, reklamní design, tiskové produkty a další. Grafika vytvořená v programu Illustrator se může použít v jakékoli velikosti jak v digitálních, tak v tiskových formátech. Výstupem tedy může být např. banner na webové stránky nebo tištěná etiketa na láhev. Grafika je tvořena křivkami, proto je možné ji použít v libovolné velikosti bez ztráty kvality. Tento program umožňuje skvěle kombinovat tvorbu textu spolu s obrázky. Illustrator byl zvolen také z toho důvodu, že v části vytváření videa byl použit software od stejné firmy.

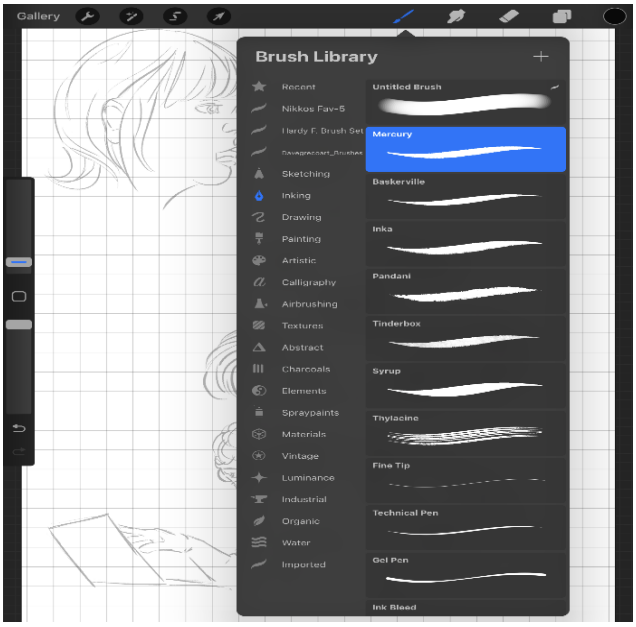
6.1.1 Tvorba ilustrací

Ilustrace byly vytvořeny ve formátu A4 (297 mm x 210 mm) a v barevném režimu CMYK, protože dokument bude zpravidla po vytvoření vytištěn. Pro kreslení byla v panelu Actions (akce) zapnut Drawing guide (průvodce kreslením), neboli navigační mřížka (viz. Obrázek 23), u které lze upravit velikost, její barva a průhlednost. Tato mřížka konkrétně slouží pro kontrolu proporcí ilustrace.



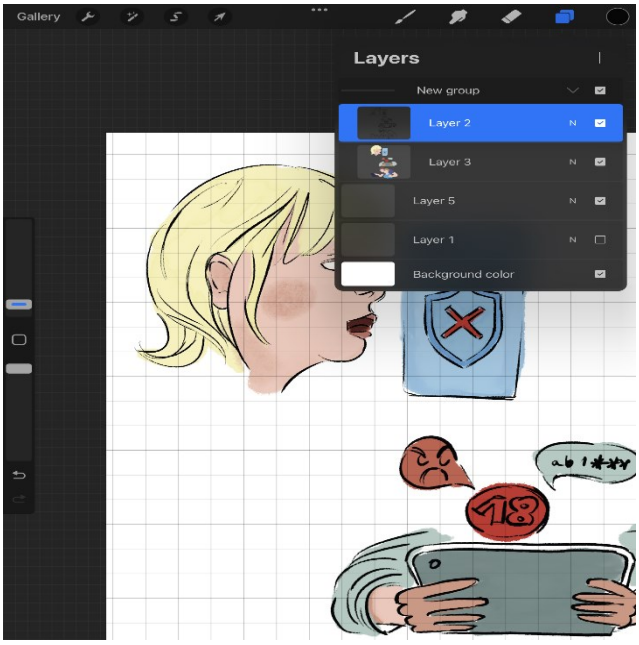
Obrázek 23: Panel akce v programu Procreate

Pod nástrojem Brush Library (Knihovna štětců) se nachází mnoho variant štětců a textur, pomocí kterých je možné vytvořit různorodé ilustrace (viz. Obrázek 24). Štětce lze upravovat pomocí panelu Brush size (velikost štětce) a Brush opacity (průhlednost štětce). Tento nástroj byl pro realizaci obrázků hlavní.



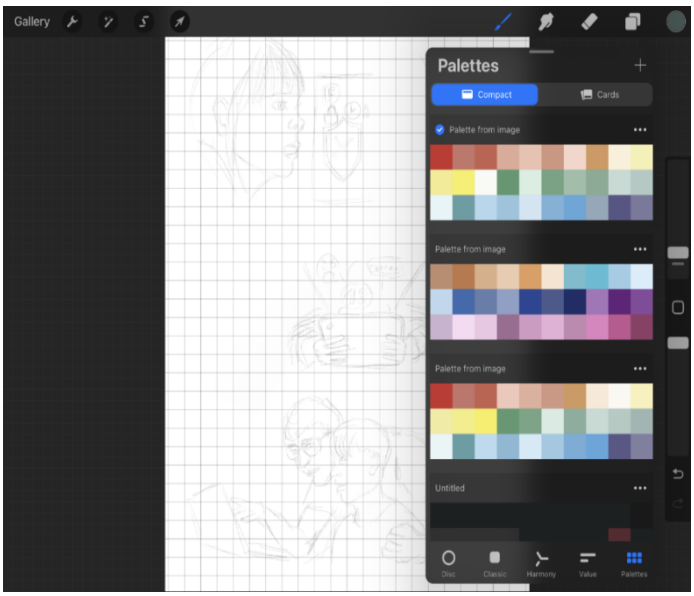
Obrázek 24: Knihovna štětců v programu Procreate

Důležitá část kresby byla práce s vrstvami (layers), pomocí kterých bylo umožněno kreslit překrývající se objekty, aniž by byla změněn objekt, která byla již vytvořen (viz. Obrázek 25). Tento nástroj umožňuje vrstvy přesouvat, upravovat, přebarvovat a mazat jednotlivé prvky. V panelu vrstvy je k dispozici náhled, kde je možné vidět co se ve vrstvě nachází. Název vrstvy se vytváří automaticky číslicemi po sobě. Vrstvy mají několik možností a to konkrétně: přejmenovat, vybrat, kopírovat, vyplňovat barvou, alpha lock (zamknutí obsahu vrstvy), mask (maska vrstvy), cliping mask (ořezová maska), drawing assist (asistent kreslení), reference, merge down (sloučit).



Obrázek 25: Nastavení vrstev v programu Procreate

Barevná paleta (Palettes) zobrazuje barevnou škálu kruhovou nebo čtvercovou (viz. Obrázek 26). Dále je možné volit komplementární barvy, což jsou barvy, které v barevné paletě stojí naproti sobě a pomáhá najít barvy, které se k sobě hodí. Barevné hodnoty je možné upravovat a jsou k dispozici již připravené palety nebo je možné vkládat vlastní palety pomocí vložení obrázku, kde se vyskytují barvy, které chcete použít, a program vytvoří paletu, která disponuje barvami, které se vyskytují na obrázku [60].



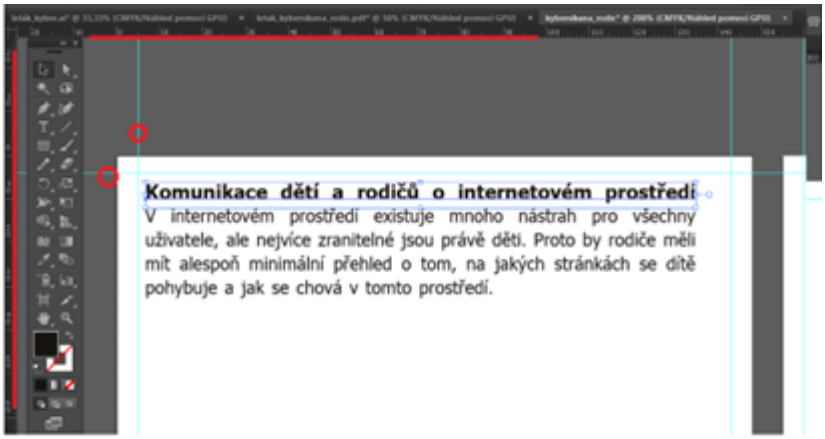
Obrázek 26: Barevná paleta v programu Procreate

Při realizaci ilustrací byl hojně využíván nástroj guma, nejen pro vymazání nepovedených linií, ale především pro změnu intenzity barvy.

Po zhotovení celého obrázku, byla vypnuta background color (barva pozadí) v panelu vrstev, aby bylo pozadí průhledné. Poté byl obrázek uložen v horní části panelu actions (akce) v sekci share (sdílet). Procreate umožňuje uložení obrázku do několika formátů, přičemž v práci byla zvolena možnost uložení jako soubor PNG (Portable Network Graphics).

6.1.2 Tvorba brožury a letáků

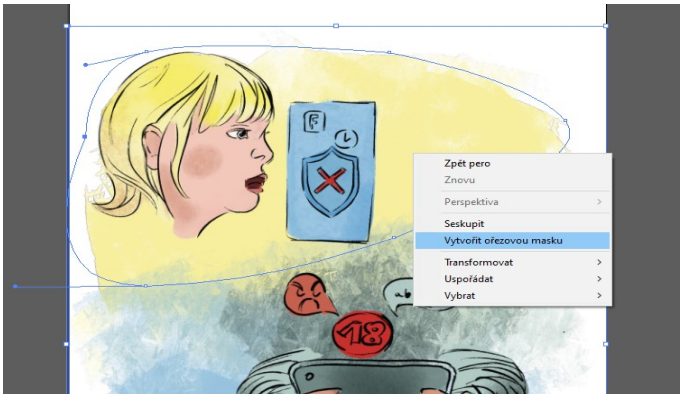
Brožura a letáky byly vytvořeny ve formátu A5 (210 mm x 148 mm) v barevném režimu CMYK s nastavením dvou kreslících pláten, protože dokument bude mít dvě strany. Dále byly vytvořeny vodítka, které sloužily jako pomocné okraje dokumentu (viz. Obrázek 27).



Obrázek 27: Pomocné okraje dokumentu v programu Adobe Illustrator

Důležitým nástrojem pro tvorbu brožury a letáků byl nástroj text a textové pole. Pomocí tohoto nástroje byl postupně vložen text vybrané velikosti a fontu.

Po vložení a úpravě textu byly importovány obrázky, které byly vytvořeny v Procreate. Po importování obrázků byla potřeba si je rozdělit a použít ilustrace odděleně. K ořezání obrázku byla použita maska obrázku, pomocí kotevního bodu a nástroje pero byla vytvořena cesta, která sloužila k vytvoření masky obrázku (viz. Obrázek 28).



Obrázek 28: Tvorba ořezové masky obrázku v programu Adobe Illustrator

Po vytvoření ořezové masky byl obrázek vložen do dokumentu s textem. Takto bylo postupováno i s dalšími ilustracemi.

Při tvorbě brožury a letáků byla použita práce s vrstvami, protože poskytuje snadný způsob, jak vybírat, skrývat, zamykat a měnit atributy vzhledu kresby. V tomto případě se pomocí vrstvy vložily obrázky pod text.

Po finální úpravě textu a obrázků, byl dokument uložen ve formátu programu **ai** pro případné úpravy a následně i ve formátu PDF.

6.1.3 Realizace obrázků do videa

V programu Illustrator byly také vytvořeny obrázky do videa. Realizovány byly v tomto programu, protože bylo zapotřebí tyto obrázky rozpohybovat a k tomu je vhodná vektorová grafika.

Tyto obrázky byly nejprve nakresleny na papír, naskenovány a poté vloženy do Illustratoru. Scan sloužil jako spodní vrstva, podle které se obrázek překresloval na vrstvě nad ní pomocí nástroje pero. Obrys byl obkreslen postupně, každá část těla zvlášť. Po obkreslení a vybarvení jednotlivých částí byly vrstvy seskupeny dohromady. Po dokreslení celého obrázku byl uložen ve formátu **ai** pro případné úpravy a importování do programu Adobe After Effects.

6.2 Edukační videa

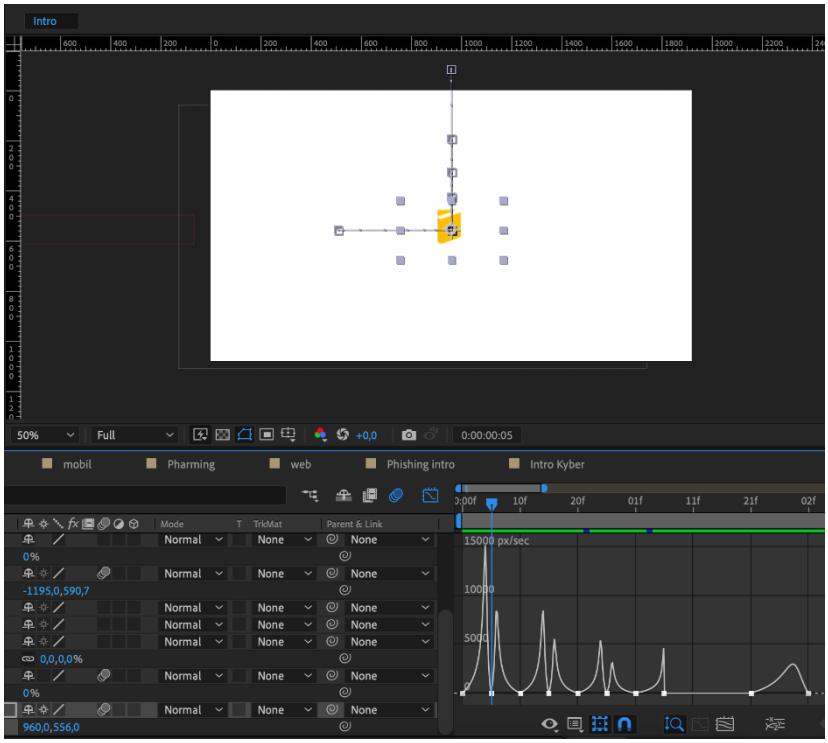
Edukační videa byla vytvořena pomocí dvou video editorů, konkrétně programů od firmy Adobe, konkrétně to jsou After Effects a Premiere Pro. Tyto programy byly vybrány z důvodu autorčiny znalosti programů, dále také pro jejich vzájemnou provázanost, co

se nástrojů a funkcí týče, a v neposlední řadě také pro možnost nahrát si své projekty na Creative Cloud a pracovat na nich odkudkoliv. Tvorba grafického obsahu do videa byla vytvořena v programu Adobe Illustrator. Tyto obrázky byly importovány přímo jako **ai** soubor.

6.2.1 První edukační video

První video, které je tvořeno pouze animacemi, bylo vytvořeno primárně v After Effects. Základem práce v tomto programu je práce s klíčovými snímky, díky kterým se vytváří většina animací. Klíčové snímky fungují na principu uložení pozice a následné práci s nimi. Vytvoření animace probíhá tak, že na počátku pohybu, rotace, či jiného parametru, který budeme upravovat, vytvoříme první klíčový snímek. Následně posuneme animaci do místa, kde chceme mít konec a upravíme daný parametr. Díky tomu se nám vytvoří další klíčový snímek, výplň mezi jednotlivými klíčovými snímky program dopočítá za nás.

Princip skákajícího loga je vytvořen přes klíčové snímky tak, že v první pozici se logo nachází mimo obraz a následně spadne do středu obrazu (viz Obrázek 29). Na celý pohyb je aplikovaný efekt rozmazání, který zakryje pohyb mezi jednotlivými snímky. Kvůli narušení linearity animace bylo potřeba upravit rychlost animace, toho bylo docíleno pomocí nástroje Graph Editor.



Obrázek 29: Úvodní sekvence v programu Adobe After Effects

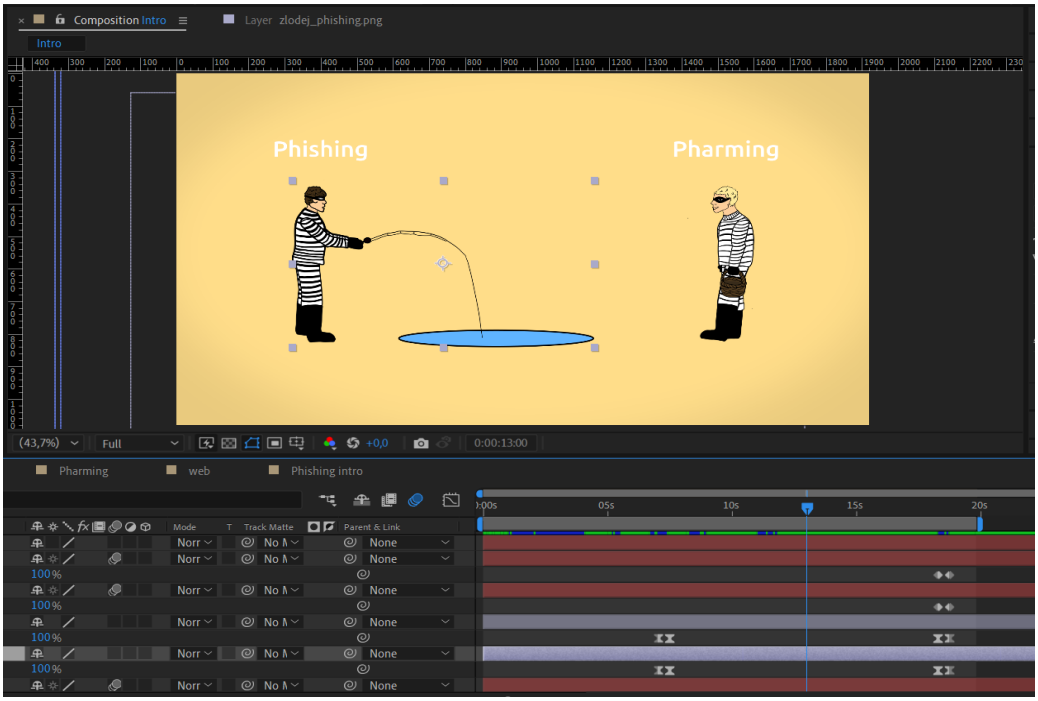
Pro vykreslení další scény byly vytvořeny tři kruhy, které jsou časově od sebe posunuty a pomocí funkce Scale (velikost) a Anchor Point (kotevní bod) upraveny tak, aby se vykreslily z místa loga fakulty. Pro každý kruh byla zvolena jiná barva, jedna z nich je také barva fakulty.

Následovalo vykreslení nápisu Phishing a Pharming, který byl zanimován opět pomocí pozice a následně byl na klíčové snímky aplikován efekt Easy-Ease, který upraví rychlost snímků tak, aby na začátku a na konci animace měly snímky malou rychlost a v průběhu pohybu byly rychlejší. Poté stačilo text skrýt pomocí Opacity a stejným způsobem se objeví dvě ilustrace.

Kromě výše již zmíněných byla pro animaci rybáře použita funkce Parent, která zapříčiní to, že dané spárované objekty se pohybují podle svého „rodiče“. Díky bylo umožněno vytvoření animace rybářského prutu a následné vytahování ulovených hesel z rybníku. Pro plynulou animaci bylo také zapotřebí rozdělit tělo rybáře na několik částí, tedy konkrétně na nohy, trup a ruce, kdy každá část se animovala zvlášť tak, aby co nejlépe kopírovala pohyb lidského těla.

Pro ztvárnění internetového chatu byly použity bubliny textu, které byly předem vytvořeny v Adobe Illustratoru tak, aby byly zachovány proporční náležitosti. Tyto bubliny byly poté importovány do After Effects a pomocí pravítek a vodítek umístěny tak, aby byly rozestupy identické, následně je stačilo zanimovat.

Samotný pohyb druhé postavy byl opět vytvořen přes více objektů, kdy byla zvlášť animovaná každá noha a ruka (viz. Obrázek 30). Po importu objektů položených na zem byla vytvořena trasa pohybu těchto objektů. Tato trasa byla vytvořena mezi prvním a posledním klíčovým snímkem za pomocí nástroje Pero, kterým byly vytvořeny další klíčové snímky a taky upravena celou trajektorii. Následně byla přidána objektu rotace. Takto bylo postupováno u všech tří objektů.



Obrázek 30: Tvorba videa phishing a pharming v programu After Effects

Ukázkový web a všechny navštívené stránky byly vytvořeny v Illustrátoru, kdy jako vzor byl použit vzhled Gmailu a screenshot stránek České spořitelny. Pro kurzor byl použit obrázek stažený ze stránky, kde jsou k dispozici zdarma ikony a malé obrázky [61]. Pro pohyb všech objektů byly opět použity klíčové snímky a rozmazání. Po dokončení videa byl proveden export z After Effects ve formátu MOV (QuickTime), video kodek Animation, z důvodu kvalitního obrazového výstupu.

Po vyrenderování všech sekvencí z After Effects bylo zapotřebí vše spojit dohromady. To bylo realizováno v programu Premiere Pro, kam byly importovány všechny sekvence. Dále bylo také potřeba importovat zvukovou stopu s audiokomentářem. Audiokomentář byl sestříhán tak, aby byly pasáže od sebe odděleny, přičemž se na tyto pasáže poté napasovaly jednotlivé animace. Střih se provádí nástrojem Razor Tool (žiletka). Po upravení komentované pasáže bylo potřeba přidat také zvuk k úvodní scéně s logem. Tento zvuk byl zvolen vzhledem k celkovému dojmu z vykreslení loga. Dále byl také přidán zvukový efekt k přilétajícím textům v prostřihu a také celková podkresová hudba pro celé video.

Tato hudba byla ještě pomocí nástroje Pero upravena tak, aby v pasážích, kde je komentář, byla ztlumená a bylo komentáři rozumět. Po kompletním střihu bylo video označeno pomocí Mark In a Mark Out a daná sekvence byla vyrenderována ve formátu FullHD 30 snímků

za sekundu. Tato snímková frekvence byla použita z toho důvodu, že není výpočetně náročná jako 60 snímků za sekundu, ale zároveň to zachytí plynulejší pohyb než 25 snímků za sekundu.

6.2.2 Druhé edukační video

Pro tvorbu druhého videa bylo třeba sepsat si zevrubný scénář. V tomto scénáři bylo nastíněno, jak by celé video mělo působit díky rozepsání celkových scén nebylo pak následné natáčení tolik složité. Po napsání scénáře byla nachystána scéna na natáčení, přičemž pro samotné natáčení byla použita videokamera, dvě externí světla a externí mikrofon připojený k počítači, kde byl za pomocí aplikace Audacity nahráván zvuk.

Po natočení všech potřebných záběrů byly záběry a zvuková stopa importovány do Premiere Pro. Díky tomu, že kamera nahrává vlastní audio stopu, bylo jednoduché sfázovat externí zvuk a obraz z kamery tak, aby seděl tzv. „na pusu“. Toho bylo docíleno pomocí funkce Synchronize, kdy se vybrala jako zdrojová vrstva záznam externího zvuku a podle něj se vždy jednotlivý záběr automaticky napasoval. Následně bylo potřeba vždy danou scénu sestříhat tak, aby neměla žádné vady v projevu a postupně se takto všechny scény řadily za sebe.

Pro úvodní scénu byla vytvořena obdobná sekvence jako u prvního videa, tj. úvodní video s animovaným logem, pouze se změnil text. Dále se pak v průběhu videa objevují drobné animace, které byly opět vytvořeny v After Effects obdobným způsobem popsaným v předchozím textu této práce. Video je také doplněno jednoduchými grafickými prvky typu bublina, které byly vytvořeny v Illustratoru a pak také přímo v Premiere Pro přes nástroj Obdélník, kterému byl nastaven parametr Okraj na barvu fakulty.

Po sestříhání všech částí následovalo přidání hudby k úvodní sekvenci a přidání zvukových efektů k přechodům textu. Poté byl opět označen úsek videa a bylo zahájeno exportování celé sekvence ve formátu FullHD 30 snímků za sekundu.

7 SEMINÁŘ PREVENCE KYBERŠIKANY

Součástí bakalářské práce je seminář, který je zaměřen na kyberšikanu a její formy. Vzhledem k výsledkům dotazníkového šetření byl tento seminář sestaven pro prevenci a zvýšení povědomí žáků v oblasti kyberšikany.

7.1 Zaměření semináře

K semináři byla vytvořena prezentace, která byla koncipována tak, že na počátku byli účastníci stručně seznámeni s obsahem celého semináře. Před zahájením semináře budou rozdány edukační materiály ve formě brožur a informačních letáčků. Na úvod se ve stručnosti představí přednášející. Posluchačům vysvětlí záměr semináře. Ten byl vytvořen na základě dat získaných z dotazníkového šetření.

Seminář bude zahájen prezentací, která na počátku posluchače stručně seznámí s jejím obsahem.

Časový harmonogram semináře celkem cca 110 min

1. Kyberšikana (její specifika, typy, aktéři …) 15 min
2. Rozdíly a společné znaky kyberšikany a šikany 10 min
3. Formy kyberšikany 15 min
4. Edukační video – Phishing a pharming 5 min
5. Prevence aneb jak kyberšikaně předcházet 10 min
6. Kam se obrátit v případě kyberšikany 10 min
7. Legislativa 10 min
8. Prostor pro diskusi 35 min

Na úvod bude specifikována kyberšikana, její typy, aktéři, dále rozdíly mezi kyberšikanou a klasickou šikanou. Budou vymezeny vztažné pojmy kybergrooming, kyberstalking, krádež identity a další informace z oblasti prevence, diagnostiky či samotného řešení zmíněných problémů. Seminář disponuje praktickými a modelovými situacemi, které jsou zpracovány formou videa, aby byly posluchačům a divákům lépe srozumitelné. Vzhledem z dat získaných z dotazníkového šetření lze vyvodit, že zkoumaný vzorek, není v problematice kyberšikany a bezpečnostních aspektech dosti informovaná. Vzhledem k tomu, že se jedná o problém rapidně narůstající, je osvěta a šíření informací důležitá.

Dále bude seminář věnován vysvětlení kyberšikany z hlediska legislativy. Existují dokumenty, které jsou s prevencí kyberšikany spojeny. Prevence probíhá jak na úrovni státu, tak školy, každé pole působnosti se řídí jinými strategickými dokumenty. Škola je povinna zajistit bezpečnost a ochranu zdraví svých žáků, proto je nezbytně nutné, aby každá škola disponovala opatřeními, která zabrání vzniku sociálně patologických jevů, mezi které právě kyberšikana patří.

Závěr semináře bude věnován prostoru pro volnou diskuzi a dotazy. Dává tak účastníkům prostor pro objasnění toho, co jim není srozumitelné.

Seminář by měl sloužit jak pro žáky základních škol, tak pro jejich pedagogy. Cílem je rozšířit a prohloubit povědomí o problematice kyberšikany. Informační prospekty, které byly v úvodu rozdány si účastníci semináře mohou ponechat. Obsahují nezbytně nutné informace o dané problematice a následném řešení již vzniklého problému.

7.1.1 Brožura a letáky

Brožura byla vytvořena k vysvětlení pojmu kyberšikany a jejich forem. Je v ní vysvětlena kyberšikana jako taková, její projevy, znaky, rozdíl mezi klasickou šikanou a kyberšikanou. Dále byly vysvětleny konkrétní typy a formy kyberšikany, které se mohou v internetovém prostředí objevit (viz. příloha PII).

Dále byly vytvořeny dva letáky – jeden pro děti a druhý pro rodiče. První leták byl vytvořen jako prevence pro děti se základními body, na které si děti mají dávat pozor, čemu se vyvarovat a kam se mohou obrátit v případě problému (viz. příloha PIII). Pro rodiče byl vytvořen leták, který poukazuje na to, co je důležité u dětí vnímat a jak s nimi komunikovat a také kam se mohou rodiče obrátit v případě problému (viz. příloha PIV).

7.1.2 Edukační videa

Edukační videa byla vytvořena z důvodu prevence, ale také proto, že v dnešní době dávají děti většinou přednost videím než psané formě.

První video se zabývá kyberšikanou a je v něm shrnuto vše co je s kyberšikanou spojeno. Konkrétně se toto edukační video zaměřuje na definici kyberšikany, jaké jsou její znaky a v jakých případech je potřeba, aby byly děti obezřetné a na koho se v případě kyberšikany obrátit. V edukačním videu byly také vysvětleny dvě formy kyberšikany, a to konkrétně krádež identity a kybergrooming.

Druhé video je zaměřeno na internetové podvody, konkrétně na phishing a pharming, které se zaměřují na krádež údajů, peněz a také identity. V edukačním videu je vysvětleno, co je to phishing a pharming, konkrétní případy těchto praktik a co se může stát člověku, který není dostatečně pozorný.

ZÁVĚR

Cílem bakalářské práce bylo seznámit čtenáře s problematikou kyberšikany na základních školách, zjistit povědomí žáků v oblasti kyberšikany a zda vědí, kam se obrátit v případě vzniku problému. Dále bylo cílem vytvořit vhodné edukační materiály, které budou sloužit jako pomůcka pro děti, rodiče a pedagogy pro prohloubení informovanosti v dané problematice.

V teoretické části byla definována kyberšikana jako taková a její rozdíly od klasické (školní) šikany. Dále byly popsány nejčastější formy kyberšikany, její projevy, typy a znaky. Také bylo poukázáno, jaké jsou možnosti prevence kyberšikany ze strany školního prostředí. Důležité bylo zmínit sociální sítě, protože v tomto kyberprostoru se většinou kyberšikana odehrává, popsat případná rizika spojené s kyberšikanou, která se mohou objevit a kdo jsou aktéři, kteří tento druh šikany praktikují. Vzhledem k tomu, že některé praktiky v internetovém prostředí jsou trestné, bylo poukázáno na legislativu spjatou s touto problematikou a také bylo zmíněno jaké jsou možnosti pomoci při daném problému, na jaké instituce či internetové stránky se mohou děti či rodiče obrátit.

Praktická část byla zaměřena na realizaci výzkumu na vybrané základní škole. V tomto dotazníkovém šetření bylo hlavním cílem zjistit povědomí žáků o kyberšikaně a pojmech s ní souvisejících a zda ví o možnostech následného řešení problému kyberšikany, pokud se s ní setkají. Bylo zjištěno, že povědomí žáků není dostačující a některé správné odpovědi mohly být ovlivněny tím, že respondenti měli nabídku možností, ze kterých si mohli vybírat, tudíž správnost odpovědí mohla být ovlivněna vylučovací metodou, a právě proto byly vytvořeny edukační materiály, které budou sloužit jako prevence v této oblasti. Následná hlubší analýza, která se studentů dotýkala osobněji není na dostačující úrovni z hlediska prevence. Celkem vysoké procento se s kyberšikanou setkalo osobně, nebo ve svém blízkém okolí. Konkrétně se jednalo o 34 % z dotazovaných. Na otázku zda vědí, kam se obrátit v případě kyberšikany sebe nebo svého okolí, se dá z odpovědí usuzovat, že konkrétně neví, koho kontaktovat. Vzhledem k tomu, že většina z nich tráví na sociálních sítích a všeobecně na internetu bezmála polovinu dne, je nutností lepší znalost a vědomí toho, jaké nebezpečí jim hrozí.

Po vyhodnocení dotazníku byla vytvořena informační brožura, která má sloužit jako jakýsi průřez problematikou kyberšikany. Dále byly vytvořeny dva informační letáky, jeden pro děti a druhý pro rodiče. Leták pro děti obsahuje body, které dětem předesílají, jak

se v internetovém prostředí chovat a jak postupovat v případě již vzniklého problému. Leták obsahuje přímé kontakty na organizace či konkrétní internetové portály, které jsou k pomoci určeny. Leták pro rodiče poukazuje na to, co je důležité při komunikaci mezi dítětem a rodičem, popř. jaké jsou varovné znaky, že je něco v nepořádku. Vytvoření brožury a letáčků bylo náročné především při vymýšlení a kreslení obrázků, které by se hodily k danému tématu.

Dále byly vytvořeny dvě edukační videa. První video je zaměřeno na kyberšikanu a její formy a druhé na ostatní druhy kyberšikany, konkrétně na phishing a pharming. Práce na prvním videu byla o poznání těžší než práce na videu druhém, zejména kvůli náročnosti jeho animací. Nejtěžší pasáží prvního videa bylo vytvořit plynulý pohyb zloděje, který se pohybuje ať už s prutem, nebo po prostoru. V druhém videu bych jako nejtěžší pasáž vybrala samotné natáčení, které zabralo téměř tři hodiny, a to hlavně kvůli velkému objemu textu a absenci předčítajícího zařízení.

Věřím, že tato bakalářská práce a její výstupy najdou své využití jako forma prevence při kyberšikaně a jejich formách.

SEZNAM POUŽITÉ LITERATURY

[1] Kocurová, Marie. *Agresivita a šikanování: studijní text kurzu PC Plzeň*. 1. vyd. Plzeň: Pedagogické centrum Plzeň, 2002. 12 s. ISBN 80-7020-101-0.

[2] KRAUS, Blahoslav, HRONCOVÁ, Jolana a kol., 2010. Sociální patologie. Hradec Králové: Gaudeamus, 325 s. ISBN 978-80-7435-080-1.

[3] ŘÍČAN, Pavel a Pavlína JANOŠOVÁ. Jak na šikanu. Praha: Grada, 2010. Pro rodiče. ISBN 978-80-247-2991-6.

[4] LOVASOVÁ, Lenka. *Šikana*. Praha: Vzdělávací institut ochrany dětí, 2006. ISBN 80-86991-65-2.

[5] BENDL, Stanislav, Lenka KOLLEROVÁ, Kateřina ZÁBRODSKÁ, Jiří KRESSA a Mária DĚDOVÁ. Prevence a řešení šikany ve škole. Praha: ISV, 2003. Pedagogika (ISV). ISBN 80-866-4208-9.

[6] Zákon č. 45/ 2013 Sb. Zákon o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů) In: *Sbírka předpisů ČR* [online]. 2013 [cit. 2022-12-12] Dostupné z: https://www.zakonyprolidi.cz/

[7] BOURCET, Stéphane a Isabelle GRAVILLON. Šikana ve škole, na ulici, doma: jak bránit své dítě--: praktický průvodce pro rodiče, pedagogy a vychovatele. Praha: Albatros, 2006. Albatros Plus. ISBN 8000015528.

[8] MARTÍNEK, Zdeněk. *Agresivita a kriminalita školní mládeže*. Praha: Grada, 2009. Pedagogika (Grada). ISBN 978-80-247-2310-5. – 42

[9] KOLÁŘ, Michal. Bolest šikanování: [cesta k zastavení epidemie šikanování ve školách]. Praha: Portál, 2001. ISBN 80-7178-513-x.

[10] VAŠUTOVÁ, Maria. Proměny šikany ve světě nových médií. Ostrava: Filozofická fakulta Ostravské univerzity v Ostravě, 2010. ISBN 978-80-7368-858-5.

[11] MŠMT. CO DĚLAT, KDYŽ – INTERVENCE PEDAGOGA: Rizikové chování ve školním prostředí – rámcový koncept Příloha č. 7 Kyberšikana. [online]. 2012 [cit. 2022-12-13]. Dostupné z: www.msmt.cz/file/20282_1_1/

[12] *Slovníček pojmů* [online]. Olomouc: Pedagogická fakulta Univerzity Palackého v Olomouc, 2022 [cit. 2022-12-13]. Dostupné z: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/143-slovnicek

[13] ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-80-210-6374-7.

[14] BURDOVÁ, Eva a Jan TRAXLER. *Bezpečně na internetu*. Praha: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK), 2014. ISBN 978-80-904864-9-2.

[15] VANÍČKOVÁ, Eva, Lenka CHUDOMELOVÁ, Jindra POHOŘELÁ a Jana BRANDEJSOVÁ. *Metodika prevence násilí, online násilí a šikany ve školách*. [Praha]: [Fakultní nemocnice v Motole], [2016]. ISBN 978-80-87347-30-0.

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

[17] ROGERS, Vanessa. *Kyberšikana: pracovní materiály pro učitele a žáky i studenty*. Praha: Portál, 2011. ISBN 978-80-7367-984-2.

[18] Kybergrooming a rizikové seznamování v prostředí internetu [online]. Olomouc: Pedagogická fakulta Univerzity Palackého v Olomouc, 2022 [cit. 2022-12-13]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/bud-v-bezpeci/82-bud-v-bezpeci-kybergrooming/file

[19] *Rizikové jevy spojené s komunikací na internetu: Co je flaming* [online]. Olomouc: Pedagogická fakulta Univerzity Palackého v Olomouc, 2022 [cit. 2022-12-13]. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/dalsi-temata/38-35

[20] HOLLÁ, Katarína. Sexting a kyberšikana. Bratislava: IRIS, 2016. ISBN 978-80-8153-061-6.

[21] BLINKA, Lukáš. Online závislosti: jednání jako droga? : online hry, sex a sociální sítě: diagnostika závislosti na internetu: prevence a léčba. Praha: Grada, 2015. Psyché (Grada). ISBN 978-80-247-5311-9.

[22] GILES, David. *Psychologie médií*. Praha: Grada, 2012. Z pohledu psychologie. ISBN 978-80-247-3921-2.

[23] PROCHÁZKA, Roman. *Teorie a praxe poradenské psychologie*. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-247-4451-3.

[24] Cyber-threat-phishing-vs-pharming: Physhing vs Pharming. Fraudwatch.com [online]. [cit. 2023-02-01]. Dostupné z: https://fraudwatch.com/cyber-threat-phishing-vs-pharming/

[25] VÁGNEROVÁ, Kateřina. *Minimalizace šikany: praktické rady pro rodiče*. Vyd. 2. Praha: Portál, 2011. ISBN 978-80-7367-912-5.

[26] KAVALÍR, Aleš, ed. *Kyberšikana a její prevence: příručka pro učitele*. Plzeň: Pro město Plzeň zpracovala společnost Člověk v tísni, pobočka Plzeň, 2009. ISBN 978-80-86961-78-1.

[27] LENHART, Amanda. Cyberbullying. 2007. [on-line]. [cit. 15. 12. 2022]. Dostupné z: http://www.pewinternet.org/2007/06/27/cyberbullying/

[28] KOLÁŘ, Michal. *Nová cesta k léčbě šikany*. Praha: Portál, 2011. ISBN 978-80-7367-871-5.

[29] *Rizikové jevy spojené s online komunikací: Měly by školy řešit kyberšikanu, ke které dochází i mimo výuku?* [online]. 2008 [cit. 2023-01-04]. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/kybersikana/2615-mely-by-skoly-resit-kybersikanu-ke-ktere-dochazi-i-mimo-vyuku-existuje-rada-situaci-kdy-ano

[30] *Kyberšikana ve školním prostředí: Metodický materiál pro pedagogické pracovníky*. Pardubice, 2012. Dostupné také z: https://docplayer.cz/13221096-Kybersikana-ve-skolnim-prostredi-metodicky-material-pro-pedagogicke-pracovniky.html

[31] Zákon č. 561/2004 Sb. *Zákon o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon)* In: *Sbírka předpisů ČR* [online]. 2013 [cit. 2023-01-18] Dostupné z: https://www.zakonyprolidi.cz/

[32] NĚMCOVÁ, Petra. *Školní program proti šikanování a kyberšikanování*. Čáslav, 2021. Krizový plán postupu při zjištění šikany a kyberšikany ve škole. Základní škola Čáslav, příspěvková organizace.

[33] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

[34] Jak se vyvarovat rizik na Facebooku: Facebook. *Vimkamklikam.cz* [online]. 2017 [cit. 2023-02-19]. Dostupné z: https://www.vimkamklikam.cz/rady-a-tipy/jak-se-vyvarovat-rizik-na-facebooku

[35] Zavítejte do historie Instagramu. *Bgram.cz* [online]. [cit. 2023-02-19]. Dostupné z: https://bgram.cz/historie-instagramu/

[36] Děti a rizika sociálních sítí. *Sancedetem.cz* [online]. [cit. 2023-02-19]. Dostupné z: https://sancedetem.cz/deti-rizika-socialnich-siti#rizika-socialnich-siti

[37] Co je Tik Tok a jak funguje? *Digitalninomadstvi.cz* [online]. 2020 [cit. 2023-02-19]. Dostupné z: https://digitalninomadstvi.cz/tiktok/

[38] Snapchat. *E-bezpeci.cz* [online]. 2019 [cit. 2023-02-19]. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/socialni-site/1441-snapchat-uz-neprinasi-revolucni-novinky-pouze-rizika

[39] *Aplikace BeReal* [online]. 2022 [cit. 2023-03-02]. Dostupné z: https://blog.avast.com/cs/aplikace-bereal-ma-skvelou-myslenku.-jak-je-na-tom-ales-ochranou-soukromi

[40] Zákon č. 40/ 2009 Sb. Trestní zákoník In: *Sbírka předpisů ČR* [online]. 2013 [cit. 2022-01-18] Dostupné z: https://www.zakonyprolidi.cz/

[41] Ministerstvo práce a sociálních věcí. Dítě s potřebou bezpečí v oblasti sociálních vztahů (šikana, kyberšikana) - Iniciační fáze – Pedagogicko-psychologická poradna (PPP) [online]. Ministerstvo práce a sociálních věci, c2017-2023 [cit. 2023-01-20]. Dostupné z: http://katalog.pravonadetstvi.cz/mpsv/ciselniky.nsf/i/S069

[42] VOCILKA, Miroslav. Náplň činnosti středisek výchovné péče pro děti a mládež: [metodický materiál]. Vyd. 2. Praha: Tech-market, 1996. ISBN 80-902134-.

[43] Informace o projektu. *E-Bezpečí* [online]. Olomouc: Univerzita Palackého v Olomouci, 2022 [cit. 2023-01-24]. Dostupné z: https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu

[44] Nenech to být. *Nenech to být* [online]. Brno: FaceUp Technology, 2023, 2017 [cit. 2023-01-24]. Dostupné z: https://www.nntb.cz/o-nas

[45] *Linka bezpečí* [online]. Praha: Neziskové občanské sdružení, 1994 [cit. 2023-01-24]. Dostupné z: https://www.linkabezpeci.cz/o-nas

[46] Práce s grafikou a druhy grafických editorů. *Www.maturita.digitalwizard.cz* [online]. [cit. 2023-03-10]. Dostupné z: https://www.maturita.digitalwizard.cz/okruhy/15-prace-s-grafikou-a-druhy-grafickych-editoru/#Rastrova_bitmapova_grafika

[47] Adobe Illustrator. *www.adobe.com* [online]. [cit. 2023-03-13]. Dostupné z: https://www.adobe.com/cz/products/illustrator.html

[48] CorelDRAW. *Www.coreldraw.com* [online]. [cit. 2023-03-13]. Dostupné z: https://www.coreldraw.com/cz/

[49] Inkscape. *Inkscape.org* [online]. [cit. 2023-03-13]. Dostupné z: https://inkscape.org/

[50] Vectornator. *Vectornator.io* [online]. [cit. 2023-03-13]. Dostupné z: https://www.vectornator.io/

[51] Adobe Photoshop. *Adobe.com* [online]. [cit. 2023-03-13]. Dostupné z: https://www.adobe.com/cz/products/photoshop.html

[52] InDesing. *Adobe.com* [online]. [cit. 2023-03-13]. Dostupné z: https://www.adobe.com/cz/products/indesign.html

[53] Gimp. *Gimp.org* [online]. [cit. 2023-03-13]. Dostupné z: https://www.gimp.org/

[54] Procreate. *Procreate.com* [online]. [cit. 2023-03-13]. Dostupné z: https://procreate.com/

[55] Audacity. *Audacityteam.org* [online]. [cit. 2023-04-23]. Dostupné z: https://www.audacityteam.org/

[56] Adobe Premiere Pro. *Adobe.com* [online]. [cit. 2023-03-13]. Dostupné z: https://www.adobe.com/my_en/products/premiere.html

[57] Adobe After Effect. *Adobe.com* [online]. [cit. 2023-03-13]. Dostupné z: https://www.adobe.com/products/aftereffects.html

[58] Final Cut Pro. *Apple.com* [online]. [cit. 2023-03-13]. Dostupné z: https://www.apple.com/final-cut-pro/

[59] HitFilm Express. *Hitfilm-express.en.softonic.com* [online]. [cit. 2023-03-13]. Dostupné z: https://hitfilm-express.en.softonic.com/?ex=DINS-635.2

[60] 18 bezplatných barevných palet. *Artsydee.com* [online]. [cit. 2023-05-08]. Dostupné z: https://www.artsydee.com/color-palettes-for-procreate/

[61] ICONFINDER. *Iconfinder.com* [online]. [cit. 2023-05-19]. Dostupné z: https://www.iconfinder.com/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ICT Informační a komunikační technologie

FCB Facebook

IG Instagram

PPP Pedagogicko – psychologická poradna

TZ Trestní zákoník

SVP Středisko výchovné péče

MŠMT Ministerstvo školství, mládeže a tělovýchovy

MVČR Ministerstvo vnitra České republiky

NNTB Nenech to být (aplikace)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Přílohy na CD

- Elektronická verze dotazník kyberšikana
- Prezentace k semináři: Kyberšikana a její formy
- Elektronická verze brožura kyberšikana
- Elektronická verze leták pro děti
- Elektronická verze leták pro rodiče
- Edukační video: Phishing a pharming
- Edukační video: Kyberšikana a její formy

PŘÍLOHA P I: DOTAZNÍK KYBERŠIKANA

Vážení žáci, mé jméno je Markéta Hovorková a jsem studentkou 3. ročníku oboru Informační technologie v administrativě na Univerzitě Tomáše Bati ve Zlíně. Tento dotazník doplňuje mou bakalářskou práci na téma Bezpečnostní aspekty kyberšikany na základních školách. Analýzou výsledků dotazníku bych ráda zjistila informovanost a základní povědomí žáků o problematice kyberšikany. V každé otázce **je správná pouze jedna z nabízených možností**, pokud si nejste svou odpovědí jistí, zvolte možnost: ***Neznám odpověď*'.** Dotazník je anonymní a veškeré informace budou použity pouze k vypracování bakalářské práce.

Za ochotu a odpovědi Vám předem děkuji.

Markéta Hovorková

Tento dotazník je nepovinný, pokud si nepřejete odpovídat zaškrtněte prosím vedlejší pole. ☐

1. Pohlaví

a) Dívka
b) Chlapec

2. Vyberte vhodný pojem k této definici:

„Jedná se o provokování a napadání uživatelů v diskusních fórech, ale také například v komentářích na sociálních sítích. Toto jednání má povětšinou velice hrubý až vulgární ráz."

a) Flaming a trolling
b) Phishing
c) Pharming
d) Neznám odpověď.

3. Vyberte vhodný pojem k této definici:

„Vydírání, ve kterém jsou využita videa a fotografie oběti. Neznámý pachatel vyhrožuje tím, že zveřejní poškozující fotografie a videa oběti, která získal při proniknutí do počítače, e-mailových schránek či účtů do sociálních sítí za účelem poškození osoby. Ve většině případů pachatelé nemají žádné poškozující materiály."

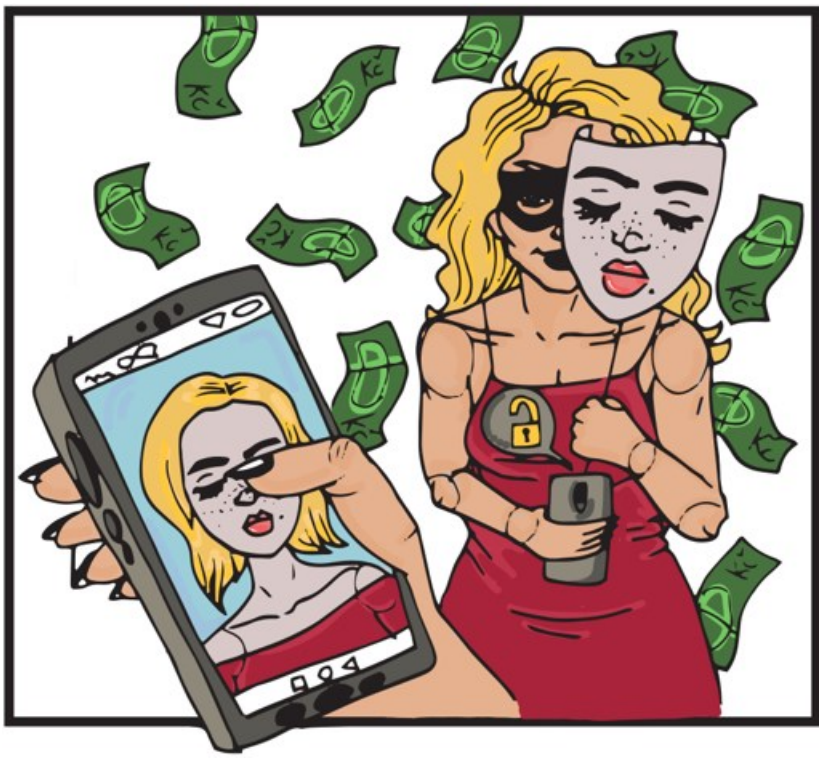
a) Kyberstalking
b) Sextortion
c) Kybergrooming
d) Neznám odpověď.

4. Vyberte vhodný pojem k této definici:

„Zneužívání internetu, mobilních telefonů k nebezpečnému pronásledování.“

a) Kyberstalking
b) Kyberšikana
c) Krádež identity
d) Neznám odpověď.

5. Vyberte vhodné pojmenování a definici pro tento obrázek.



a) Krádež identity –
Odcizení přístupových údajů k e-mailu, uživatelskému účtu na sociálních sítích, v počítačové hře apod. a následné vydávání se útočníka za oběť.
b) Krádež identity –
Zneužívání internetu, mobilních telefonů a komunikačních technologií k nebezpečnému pronásledování.
c) Kybergrooming –
Označuje jednání osoby, která se snaží zmanipulovat vyhlédnutou oběť (nejčastěji pomocí chatu, SMS zpráv, sociálních sítí, herních portálů, skypu) a donutit ji k osobní schůzce. Výsledkem schůzky může být sexuální zneužití, fyzické mučení, nucení k terorismu apod.
d) Neznám odpověď.

6. Vyberte vhodný pojem k této definici:
„Elektronické zasílání zpráv, fotografií či videí se sexuálním obsahem. Může být dobrovolné, ale také nedobrovolné.“

a) Sextortion
b) Sexting
c) Flaming a Trolling
d) Neznám odpověď.

7. Vyberte vhodné pojmenování a definici pro tento obrázek.

a) Pharming –
Označuje manipulativní chování, které má přimět uživatele, aby útočníkovi sdělil své osobní údaje na falešných webových stránkách.
b) Phishing –
Jde o situace, kdy zadávám své osobní údaje za účelem platby (např. platba při online nákupech na ověřených internetových obchodních platformách).
c) Phishing –
Druh nebezpečných komunikačních praktik, zaměřených na krádež citlivých osobních údajů – např. PIN kódu a čísel platebních karet, hesel a údajů k bankovnímu účtu a či další citlivé informace, které by mohly být zneužity.
d) Neznám odpověď.

8. Vyberte vhodný pojem k této definici.:

„Označuje manipulativní chování, které má přimět uživatele, aby útočníkovi sdělil své osobní údaje na falešných webových stránkách.“

a) Kybergrooming
b) Phishing
c) Pharming
d) Neznám odpověď.

9. Vyberte vhodné pojmenování a definici pro tento obrázek.

a) Šikana –
Opakované chování osoby či skupiny s účelem fyzicky či psychicky ublížit osobě, nebo skupině osob, která se nemohou z nejrůznějších důvodů bránit.
b) Kyberšikana –
Opětovné a dlouhodobé obtěžování nevyžádanými esemeskami, e-maily, různými druhy chatu, telefonáty, nechtěnými pozornostmi, případné opakované sledování osoby.

c) Kyberšikana –
Dlouhodobé a také stupňující se užívání psychického napadání proti jedinci nebo skupině jedinců za pomoci internetu (sociální sítě, herní portály).
d) Neznám odpověď.

10. Vyberte vhodné pojmenování a definici pro tento obrázek.

a) Kybergrooming –
Zneužívání internetu, mobilních telefonů k nebezpečnému pronásledování.
b) Kybergrooming –
Označuje jednání osoby, která se snaží zmanipulovat vyhlédnutou oběť (nejčastěji pomocí chatu, SMS zpráv, sociálních sítí, herních portálů, skypu) a donutit ji k osobní schůzce. Výsledkem schůzky může být sexuální zneužití, fyzické mučení, nucení k terorismu apod.
c) Sextortion –
Zneužívání internetu k odeslání falešných SMS zpráv.
d) Neznám odpověď.

11. Vyberte vhodné pojmenování a definici pro tento obrázek.

a) Šikana –
Dlouhodobé a také stupňující se užívání psychického napadání proti jedinci, nebo skupině jedinců za pomoci internetu (sociální sítě, herní portály).
b) Pharming –
Pronásledování, opakované stupňované obtěžování, které může mít různou podobu a intenzitu.
c) Šikana –
Opakované chování osoby či skupiny s účelem fyzicky či psychicky ublížit osobě, nebo skupině osob, která se nemohou z nejrůznějších důvodů bránit.
d) Neznám odpověď.

12. Setkal/a ses někdy s kyberšikanou tebe, nebo tvého okolí? Pokud ano, kde?

13. Kam se se obrátíš, když se staneš obětí, nebo budeš svědkem kyberšikany?

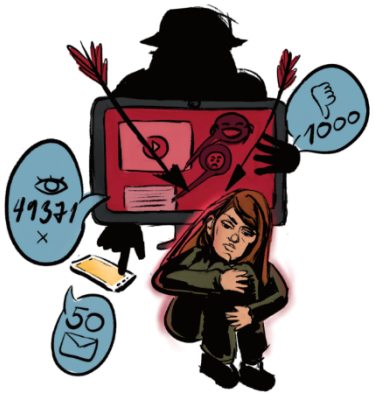
14. Kolik času trávíš denně na sociálních sítích a všeobecně na internetu?

15. Mají rodiče přehled o tom, co děláš na sociálních sítích?

16. Pokud jsi v otázce číslo 15 odpověděl/a NE. Napiš, proč nechceš, aby rodiče věděli, co na internetu děláš.

PŘÍLOHA P II: BROŽURA KYBERŠIKANA A JEJÍ FORMY

Kyberšikana a její formy



Co je to kyberšikana?

Zneužití informačních a komunikačních technologií, zejména pak mobilních telefonů, internetu. Jedná se o činnosti, jež mají někoho záměrně ohrozit, ublížit mu. Podobně jako u šikany tváří v tvář se jedná o úmyslné chování, kdy je oběť napadána útočníkem nebo útočníky zejména psychicky. Povaha a provedení útoků pak určují její závažnost.

Nejčastější projevy kyberšikany:

- Zasílání nevyžádaných, urážlivých, zastrašujících zpráv (SMS,e-mail, chat...)
- Šíření pomluv a lživých informací prostřednictvím sociálních sítí
- Zveřejňování soukromých a intimních fotografií i videí bez souhlasu dotyčného
- Vytváření fiktivních profilů, internetových stránek blogů s lživým, ponižujícím obsahem, vztahujícím se ke konkrétní osobě
- Krádež identity
- Záměrná, cílená provokace v diskusních fórech
- Obtěžování formou nevyžádaných a opakovaných hovorů, zpráv apod.

Kyberšikana nepředstavuje jednotný samostatný jev, nýbrž se jedná o jednu z forem psychické šikany. Na rozdíl od tradiční školní šikany neprobíhá kyberšikana tváří v tvář, kdy se účastníci znají, jsou v přímém osobním kontaktu, znají své nejbližší okolí, přátele či rodinu.
Kyberšikana se odehrává ve virtuálním světě, který zajišťuje agresorovi jistou míru anonymity.
Poskytuje mu tak větší možnosti pro útoky.

Specifické znaky kyberšikany

1. Anonymita

Díky principu virtuálního světa, na němž funguje celý internet, jsou útočníci relativně anonymní. Na sociálních sítích, všeobecně na internetu, vystupují pod falešným profilem, emailovou adresou či telefonním číslem, z čehož vyplývá, že oběť útočníka nemá jak identifikovat. Toto mnohdy vede k posílení odvahy agresora a jeho útoky mohou mít stupňující se charakter. Anonymita na internetu není nikdy stoprocentní.

2. Čas a místo

V případě kyberšikany bohužel nelze předpovídat, kdy útok přijde. Vzhledem ke každodennímu využívání informačních a komunikačních technologií je oběť neustále pod tlakem, kdy ani v domácím prostředí není v bezpečí.
K útoku může dojít ve kteroukoli denní i noční hodinu.

3. Velké publikum a přesah

Velmi kritický dopad na psychiku oběti má veřejná povaha virtuálního světa. Zejména možnost sdílení obsahu. Agresorovi stačí příspěvek publikovat pouze jednou, a právě ono zmíněné velké publikum se dále stará o špinavou práci za útočníka tím, že obsah dál šíří. Rychlost šíření příspěvků na internetu je enormně vysoká, až nekontrolovatelná.

4. Změna charakteru oběti a útočníka

Vzhledem k tomu, že celý útok se odehrává ve virtuálním anonymním prostoru, útočníkem nemusí být jen jedinec fyzicky zdatný, ale zpravidla stačí jen dobrá znalost technologií. Právě anonymita prostředí, ve kterém se vše odehrává, nuluje rozdíly například: věkové, rasové či rozdíly v pohlaví.
Oběti nejsou zpravidla slabší jedinci. Může se jednat také o osoby společensky vysoce postavené.

5. Prakticky neidentifikovatelné následky

Vzhledem k tomu, že násilí v kyberšikaně není pácháno fyzicky, je velmi těžké je dokázat. Absence modřin, oděrků a podlitin ovšem neznamená, že nemá oběť doživotní následky. Ty jsou mnohdy horší než v případě fyzické agrese. Stává se, že oběť se do sebe uzavře. Strach je příčinou toho, že o svých problémech se svým okolím odmítá komunikovat. Obává se reakce okolí. Psychické následky mohou oběti dovést až k myšlenkám na sebevraždu či k samotné sebevraždě.

Rozdíly mezi šikanou a kyberšikanou

Tradiční (školní) šikana	Kyberšikana
Rysy	
Opakování – agresor opakovaně napadá oběť v průběhu času. V případě jednorázového útoku se o šikanu nejedná.	Opakování – v případě kyberšikany stačí jediný „útok", který může mít několik forem. Nejčastější formou bývá zveřejnění obsahu, jež má ponižující charakter. Následné šíření a přeposílání tohoto obsahu se díky veřejné povaze virtuálního prostředí stává opakováním. Tím pádem se agresor jediným aktem může dopustit kyberšikany, která pak trvá už delší čas.
Mocenská nerovnováha – mocenská nerovnováha není jen v oblasti fyzické síly, nýbrž také v psychické oblasti. V tomto případě může psychická a sociální nevyspělost vést k nerovnováze mezi mocí agresora a oběti.	Mocenská nerovnováha – oběť nedokáže obtěžování technologicky zabránit. Nerozhoduje fyzická síla. Agresor zde využívá své technické znalosti.
Přímá	
Fyzická (fyzické násilí, poškozování majetku, krádeže věcí). V tomto případě se jedná o čin, který je vidět, je zřetelné, kdo je aktérem, kdo je v roli oběti či útočníka. Verbální (např. nadávky, urážky, ponižování). Neverbální (např. obscénní gesta).	Fyzická (např. úmyslné pořizování intimních i jiných fotografií, videí oběti a jejich následné umisťování na internet). Oběť ji nemůže předvídat, je nečekaná. Verbální (např. urážlivé, výhružné e-maily či SMS, nebo zprávy na sociálních sítích). Neverbální (např. posílání výhružných nebo obscénních obrázků, nevyžádaná korespondence se sexuálním podtextem).
Nepřímá	
Sociální (např. vylučování někoho ze skupiny). Verbální (např. šíření pomluv a lživých informací).	Sociální (např. vylučování někoho z online skupiny). Verbální (např. zveřejnění soukromé konverzace či informací, šíření pomluv na internetu). Podvádění vydáváním se za někoho jiného, falešné profily, krádež identity.

Typy kyberšikany

Kyberšikana se dělí na dva základní typy. Kyberšikana přímá a kyberšikana v zastoupení.

Kyberšikana přímá

Ze strany agresora dochází k přímým útokům např. v podobě zpráv. Agresor je přímým konatelem protiprávní činnosti.

Formy přímých útoků:

- Posílání SMS, e-mailů, zpráv přes messenger
- Zcizení profilů na sociálních sítích a jejich následné zneužívání
- Šíření osobních, lživých informací, rozesílání intimních fotografií
- Slovní napadání prostřednictvím skupinových chatů při hraní her
- Nabourávání herních či osobních účtů
- Šíření spamů či jiných virů prostřednictvím e-mailu apod.

Nepřímá kyberšikana (kyberšikana v zastoupení)

V případě kyberšikany v zastoupení, využívá agresor k útoku jiné osoby. Tito jedinci ve většině případů netuší, že se stali nástrojem něčí pomsty vůči někomu druhému. Dochází tak k tomu, že agresor je zde pouze jakýmsi prvním impulzem a spouštěčem.
On poskytne prvotní impuls ke vzniku kybernásilí a zbytek pak nevědomky vykonají ostatní účastníci v kyberprostoru.
Jedná se o situace, kdy například agresor disponuje videem s choulostivým obsahem oběti. Poté jej zveřejní na internetu a ostatní uživatelé, kteří obsah zhlédnou a nějakým způsobem ho hanlivě komentují, se taktéž nevědomky dopouštějí kyberšikany. Stává se i to, že útočník si založí falešný profil pod identitou oběti, nebo se dokonce naboural oběti do reálného účtu, a kontaktuje tak blízké a přátele oběti.

Kybergrooming

Jedná se o nepřímou formu kyberšikany. Útočník pod falešnou identitou a falešnou záminkou láká nezletilé oběti na schůzku prostřednictvím ICT za účelem následného sexuálního zneužití.
Útočníci si vybírají oběti, které se vyznačují ekonomicky nízkým statusem, jedince (děti) ze zanedbaných či sociálně slabších rodin, atd. Těmto obětem je nabízena finanční odměna za schůzku, či fotografie a videa s kompromitujícím obsahem sloužícím např. k dětské pornografii.

Scénář kybergroomingu má nepsaná pravila. Útočník se vydává za osoby věkově srovnatelné s obětí. Poté s nezletilou osobou naváže kamarádský vztah a vybuduje v oběti důvěru. Tu si získá na základě sdělení svých problémů, které se ve většině případu velmi ztotožňují s problémy oběti. Následně, po získání kompromitujícího materiálu, se v oběti snaží vzbudit pocit viny, a to především vzhledem k citlivosti informací, jež mu oběť sdělila. U oběti pak dochází k sociální izolaci. Následná schůzka nemusí vždy napoprvé končit útokem, avšak naopak může směřovat k upevnění vztahu s obětí.
Délka kontaktu se odvíjí od schopností a zkušeností agresora.

Formy kyberšikany

Kyberstalking (pronásledování)

Opakované pronásledování oběti pomocí informačních technologií. Agresor (stalker) stupňuje pravidelnost a intenzitu pronásledování, obsah zpráv a vzkazů, taktéž graduje na hrubosti.
V oběti se hromadí obavy a strach nejen o vlastní život,ale i o bezpečí svých blízkých. Nejčastěji se s kyberstalkingem setkáváme u bývalých partnerů.

Harassement (obtěžování)

Obtěžování v kyberprostoru se vyznačuje především opakovaným posíláním nevyžádaných zpráv, telefonátů, emailů apod.

Denigration (ponižování, pomlouvání)

Jedná se o: „Rozšiřování pomluv a lží s cílem poškodit něčí pověst nebo vztahy." Jelikož vše probíhá ve virtuálním prostředí, prostřednictvím moderních technologií a virtuálně v kyberprostoru, je pro oběť velmi těžké se bránit. Ve virtuálním prostředí dochází k šíření informací podstatně rychleji než v reálném životě.

Krádež identity (vydávání se za někoho jiného)

Význam pojmu krádež identity spočívá v tom, že agresor nějakým způsobem získá hesla k účtům profilů a následně se vydává za tu osobu, která je v této situaci obětí. Tak je založen fiktivní profil pod identitou oběti, případně se pracuje s již existujícím účtem z něhož jsou následně kontaktováni přátelé, rodina či blízcí oběti. Tímto způsobem může být velmi silně narušen vztah mezi obětí a jejím blízkým okolím. Lze tak zasílat nenávistné zprávy, zprávy s hanlivým a nevhodným obsahem pod identitou oběti, která je následně očích poškozených vinna. Může se dokonce dopouštět jménem oběti trestné činnosti. Oběti se velmi těžko dokazuje její nevina.

Flaming (flame = hořet)

„Flaming (flame = hořet) je termín označující nepřátelské chování uživatelů na internetu. Obvykle jej doprovází urážky, nadávky, vyhrožování apod. Flaming je obvykle spojen se sociálním prostředím diskusních fór, webového chatu příspěvků, ale může být realizován i prostřednictvím e-mailu." Nejčastěji se s flamingem setkáváme na platformách, kde mohou jedinci veřejně komentovat, vytvářet příspěvky. Zde se flamer = útočník projevuje vulgární až agresivní reakcí na posty (příspěvky), na které má odlišný názor. Reakce nebývají nijak propracované a smysluplné, ale zato jsou plné vulgarismů. Zde je důležité nezaměňovat flamera za trolla. Troll je osoba, která také působí ve veřejných diskuzích s tím rozdílem, že se snaží uměle vytvářet konflikt a vyvolávat negativní diskuse o problematice přímo nesouvisející s příspěvkem.

Sexting

Sexting můžeme definovat jako zasílání zpráv, videí, převážně s intimním obsahem a sexuálním podtextem. Tento fenomén se nejčastěji řeší u dětí a mladistvých. V tomto období není u jedinců ještě plně rozvinut pocit zábran, tudíž si dost dobře neuvědomují možná rizika a následky. Problém se však netýká jen skupiny dětí a mladistvých, ale často tyto materiály vznikají i v partnerských vztazích. Dospělý jedinec si mnohdy nepřipouští, že by mohlo dojít ke zneužití soukromě pořizovaných materiálů. Nejčastěji se tak stává po ozchodu partnerů, kdy se jeden druhému snaží ublížit a pomstít se.
V tomto případě přechází sexting k sextortion.

Happy slapping (veselé fackování)

Jedná se o situace, kdy je neznámý člověk napaden a samotný útok je jedním z útočníků natočen. Natočené video je následně zveřejněno na internetu. Procházka ve své publikaci poradenské psychologie uvádí, že v případě happy slappingu mluvíme o jedné z nejčastější formě kyberšikany.

Outing and trickery (prozrazení a podvádění)

Při prozrazení neboli outingu se jedná o druh kyberšikany, při níž útočník zveřejní fotografie, videozáznamy a informace o oběti, které oběť nikdy nezamýšlela zveřejnit.
Při podvádění (trickery) přesvědčuje útočník oběť, aby mu prozradila tajemství a citlivé informace, které by následně mohl zveřejnit na internetu.

Ostatní formy kyberšikany

Existují další formy kyberšikany, které jsou odlišné tím, že nemají za cíl oběť "pouze" nějakým způsobem poškodit, ale také ji okrást o důležitá data.

Phishing

Je jeden z mnoha druhů napadení v kyberprostoru. Cílem napadení je získat citlivé údaje od uživatele. Tato phishingová napadení je možné odhalit, ovšem uživatel musí být velmi pozorný. Ve většině případů se u phishingových napadení objevují pravopisné chyby, cizí jazyk nebo znaky, jež do zprávy či e-mailu nepatří.

Jednou z možností je, že uživateli přijde zpráva na Facebook od jeho známého (obvykle má tento člověk napadený profil) s prosbou o číslo. Poté, co oběť pošle své telefonní číslo, jí přijde do sms zprávy kód, který útočník zpětně vyžaduje. Pokud tento kód útočníkovi sdělí, může se v měsíčním vyúčtování objevit vyšší částka než obvykle.

Pharming

Stejně jako phishing má pharming stejný cíl. Zmanipulovat oběť tak, aby sdělila své citlivé údaje. Pharming, na rozdíl od phisningu využívá jinou strategii a je těžší jej rozpoznat. Pharmingový útok vypadá tak, že se uživatel ocitne na falešné internetové stránce, aniž by o tom věděl, protože útočník pomocí doménového serveru přepíše IP adresu.

PŘÍLOHA P III: LETÁK PRO DĚTI

Internetové prostředí vlastní mnoho nástrah, proto je důležité, abyste byli opatrní v tom, co zveřejňujete, jaké údaje sdělujete, ale také s kým komunikujete.

Zamyslete se, než něco zveřejníte!

Na sociálních sítích je vhodné chovat se obezřetně v tom, co zveřejňujete. Neměli byste zveřejňovat fotografie svého bydliště a majetku. Také veřejně nepsat, že jste, či budete mimo domov, protože nikdy nevíte, zda některý z útočníků tyto informace a fotografie nevyužije proti Vám.

Buďte opatrní na vše, co posíláte!

Pokud posíláte někomu své fotografie, je potřeba si uvědomit, že mohou být zveřejněny. Nikdy se nenechte přemluvit na odeslání fotografie, kterou nechcete, aby viděli i další lidé. Ačkoli osobě důvěřujete, nikdy nevíte, zda Vaši fotografii nepoužije pro poškození Vaší osoby. Fotografie, které by neměly být zveřejněny, mohou mít dopad na Vaši budoucnost, rodinu nebo práci.

Ověřujte si, s kým si píšete!

Při komunikaci na sociální síti nikdy nevíte, s kým doopravdy komunikujete. Může se jednat o profil, pod nímž se vydává někdo jiný. Proto je důležité, ověřovat si, s kým komunikujete. Osobu si můžete například ověřit tím, že si vyžádáte, aby Vám napsala jakýkoliv text na papír a spolu s ním vyfotila svůj obličej.

Soukromí na sociálních sítích

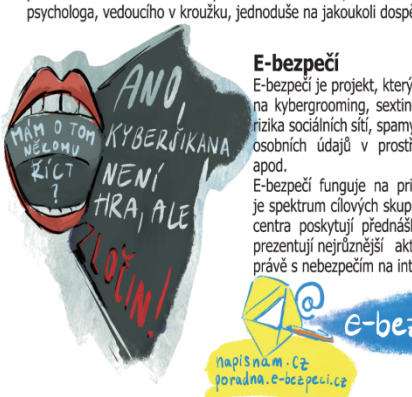
Pokud sdílíte aktuální polohu na sociálních sítích, jste snadno vystopovatelní a zranitelní. Je tedy zapotřebí rozmyslet si, zda sociální sítě potřebují přístup k Vaší aktuální poloze a zda ostatní uživatelé sociálních sítí potřebují vědět, kde se zrovna nacházíte.
Při sdílení aktuální polohy může být ohrožen nejen Váš majetek, ale i Vy. Je taktéž vhodné si promyslet, kdo vidí Vaše fotografie, videa a další informace na Vašem profilu. Je třeba veškerý přístup omezit pouze prostřednictvím soukromého profilu, či omezit viditelnost příspěvků jen pro Vaše přátele, které znáte.

Internetové podvody

V internetovém prostředí se objevuje mnoho podvodů. Není-li člověk pozorný, může být lehce okraden o identitu, peníze i údaje k platebním kartám. Proto buďte obezřetní v tom, na kterých stránkách vyplňujete své osobní údaje. Stránky si raději vždy prověřte.

Na koho se obrátit v případě kyberšikany?

Každému se může stát, že se ocitne v situaci, na niž sám nestačí. Jedná se o situace, kdy si člověk neví rady a potřebuje pomoct. Existuje celá řada řešení, jež Vám s Vaší nelehkou situací mohou pomoci. Prvním krokem je přiznat si daný problém a říct si o pomoc. Obrátit se můžete v první řadě na rodiče, učitele ve škole, poradce, školního psychologa, vedoucího v kroužku, jednoduše na jakoukoli dospělou osobu.



E-bezpečí

E-bezpečí je projekt, který se specializuje především na kybergrooming, sexting, stalking, kyberstalking, rizika sociálních sítí, spamy, online závislosti, zneužití osobních údajů v prostředí elektronických médií apod.
E-bezpečí funguje na principu terénní práce, kdy je spektrum cílových skupin velice široké. Pracovníci centra poskytují přednášky či besedy, na kterých prezentují nejrůznější aktuální problémy spojené právě s nebezpečím na internetu.

Linka bezpečí

Na linku bezpečí se může obrátit kdokoliv, kdo se dostane do nepříznivé životní situace na základě jakýchkoli okolností. Na tuto linku se dovoláte kdykoliv, má nepřetržitý provoz. Pokud Vám je telefonní rozhovor z jakéhokoli důvodu nekomfortní, je možné se obrátit na chat této linky, který je k dispozici
denně od 9 do 13 hodin a od 15 do 19 hodin,
nebo také napsat email, na který dostanete odpověď do tří pracovních dnů.

Aplikace „Nenech to být" (NNTB)

Tato aplikace umožňuje anonymně poukázat a upozornit na nevhodné až rizikové chování ve škole, či na rizikové chování konkrétního žáka bez strachu postihu. V této aplikaci si ve výběru zvolíte školu, do které docházíte a poté vyplníte oznámení Vašeho trápení. Oznámení, které vyplníte, se odešle školou pověřeným osobám, například metodikovi prevence nebo školnímu psychologovi.
Aplikace je volně ke stažení na Google play či App Store.

PŘÍLOHA P IV: LETÁK PRO RODIČE

Komunikace dětí a rodičů o internetovém prostředí

V internetovém prostředí existuje mnoho nástrah pro všechny uživatele, ale nejvíce zranitelné jsou právě děti. Proto by rodiče měli mít alespoň minimální přehled o tom, na jakých stránkách se dítě pohybuje a jak se chová v tomto prostředí.

Komunikace

Nejdůležitější je komunikace mezi dítětem a rodiči. Je zapotřebí, aby dítě vnímalo to, že za rodiči může přijít s jakýmkoliv problémem, aby vědělo, že v nich má oporu za každé situace.

Rizika internetového prostředí

Je nutné, aby rodiče vysvětlili, promluvili a poučili své dítě o nástrahách sociálních sítí, jež se mohou všeobecně na internetu objevovat. Objasnili, jak se má v určitých případech zavhovat, bránit a na koho se v případě problémů obrátit. Dítěti také vysvětlili, co naopak na sociálních sítích dělat nemá, a jaký druh chování některých jedinců nemá podporovat.

Vnímaví rodiče

Při problémech v internetovém prostředí není na první pohled nic vidět. Agrese ve zmiňovaném prostředí není páchána fyzicky, nýbrž psychicky, tudíž je velmi problém rozpoznat. Nevidět modřiny, oděrky ani podlitiny, ovšem neznamená, že se jedná o méně závažnou situaci. Ve většině případech se oběť uzavře do sebe a ze strachu odmítá o čemkoliv komunikovat s okolím. Z tohoto důvodu je třeba, aby byli rodiče co nejvíce obezřetní a byli připraveni svému dítěti pomoci. Rodiče by si měli všímat toho, zda se jejich dítě nechová jinak než obvykle. Například po zobrazení zpráv, příspěvků na sociálních sítích, nebo zdali si v jejich přítomnosti neskrývají telefon.

Internetoví kamarádi

Důležité je, aby dítě nedůvěřovalo každému, kdo mu na internetu napíše. Za profilem, jenž je svým způsobem dítěti sympatický, se může skrývat někdo nebezpečný. Právě proto by bylo vhodné, aby se rodiče svých dětí ptali, s kým jsou v internetovém prostředí v kontaktu.

Rodičovská kontrola

Rodičovská kontrola je součástí většiny sociálních sítí. Na každé z nich však může rodič korigovat jiné aktivity (například čas, jenž dítě na dané sociální síti stráví, apod.). Jednotlivé funkce mnohdy mívají rozdílné názvy.

Organizace, na které se rodič může obrátit

Pokud má rodič pochybnosti o tom, jak má stávající problém řešit, je možné se obrátit na školu, nebo na některé instituce.

Rodičovská linka

Potřebuje-li rodič poradit, nebo vyřešit nějaký problém je rodičovská linka k dispozici od pondělí do pátku.
V pondělí až čtvrtek od deváté hodiny ranní do deváté hodiny večerní, v pátek je tato doba zkrácena o dvě hodiny.
Také je možné využít chat, jenž je k dispozici v neděli od páté hodiny odpolední do deváté. Pokud rodič odešle e-mail, dostane odpověď do tří pracovních dnů.

E – Bezpečí

E-bezpečí je projekt, který se specializuje především na kybergrooming, sexting, stalking, kyberstalking, rizika sociálních sítí, spamy, online závislosti, zneužití osobních údajů v prostředí elektronických médií apod. E-bezpečí funguje na principu terénní práce, kdy je spektrum cílových skupin velice široké. Pracovníci centra poskytují přednášky či besedy, na nichž jsou prezentovány nejrůznější aktuální problémy spojené právě s nebezpečím internetu.