U N I V E R Z I T A P A L A C K É H O
V O L O M O U C I

C Y R I L O M E T O D Ě J S K Á T E O L O G I C K Á
F A K U L T A

Katedra křesťanské výchovy

Sociální pedagogika

Ondřej Gregorek

Program prevence kyberšikany a bezpečnosti na internetu

Bakalářská práce

Vedoucí práce: doc. PhDr. & Mgr. Petra Potměšilová, Ph.D.

2020

Čestné prohlášení:

Prohlašuji, že jsem bakalářský projekt vypracoval samostatně a použil jsem přitom jen uvedené prameny a literaturu.

V ..... dne ..... *Ondřej Gregorek*

Poděkování

Děkuji doc. PhDr. & Mgr. Petře Potměšilové, Ph.D. za odborné vedení bakalářského projektu a cenné rady, které mi pomohly k jeho úspěšnému dokončení. Mé díky patří také mým nejbližším za podporu po dobu psaní tohoto projektu.

Obsah

1. Kyberšikana – obecný úvod a popis fenoménu 7

1.1. Šikana 7
1.2. Definice kyberšikany 8
1.3. Základní znaky kyberšikany 9
1.4. Nejčastější projevy kyberšikany 11
1.5. Prostředky kyberšikany 14
1.6. Příčiny kyberšikany, agresoři a oběti 16
1.7. Prevence a řešení kyberšikany, pomoc obětem 17
1.8. Legislativa 20

2. Bezpečné chování na internetu 21

2.1. Ochrana osobních údajů a soukromí 22
2.2. Hesla 23
2.3. Malware 24
2.4. Spam, phishing 24

3. Návrh programu prevence kyberšikany a bezpečnosti na internetu ... 25

3.1. SWOT analýzy vybraných projektů 25
3.1.1 Internetem Bezpečně 26
3.1.2 E-Bezpečí 28
3.2. Cíle programu 30
3.3. Charakteristika programu 30
3.4. Pokyny k realizaci 31
3.5. Rozpočet programu a personální obsazení 32
3.6. První blok – sociální sítě 33
3.7. Druhý blok – kyberšikana 35
3.4. Třetí blok – kybergrooming 37
3.5. Čtvrtý blok – seznamování a hesla 38
3.6. Pátý blok – závěrečné shrnující aktivity 40

Závěr 42

Seznam literatury 43

Seznam příloh 46

Úvod

Tento bakalářský projekt se zaměřuje na téma prevence kyberšikany a bezpečnosti na internetu dětí a mládeže. Podle posledních průzkumů je tato problematika v současnosti velmi aktuální, s negativními jevy v kyber prostředí se dnes setkává velké množství jedinců (Kopecký, 2014). Internet, počítače či moderní informační a komunikační technologie obecně se staly téměř neodmyslitelnou součástí života obzvláště mladé generace. Ta se díky tomu stále setkává s tímto negativním fenoménem, a to i přesto, že je tomuto tématu věnována velká pozornost, jednak na školách, kde se realizují preventivní programy, přednášky či besedy, tak i přímo v prostředí internetu, kde v současné době existuje několik preventivních programů. I přesto se ukazuje, že je stále třeba důkladná osvěta (Kopecký, Szotkowski, 2019).

Tento projekt se snaží na tuto situaci reagovat, a i když není v jeho možnostech se vyrovnat projektům, na kterých pracuje velké množství kvalifikovaných lidí, snaží se nabídnout určitou formu preventivního programu, který je zaměřen na druhý stupeň základních škol. Program je postaven na tom, aby nabídl ucelený soubor aktivit přímo pedagogovi, který ho může okamžitě realizovat se svou třídou bez potřeby hlubokých znalostí tohoto tématu.

V první části je uveden současný a obecný pohled na tuto problematiku, jsou v ní popsány aktuální poznatky, prezentované v odborné literatuře nebo výzkumech či internetových projektech. Ta má posloužit jako jakýsi základní úvod do dané problematiky pro pedagoga, který bude projekt realizovat a může díky tomu vést jednotlivé aktivity, diskutovat s žáky a odpovídat na jejich dotazy. V další části projektu je představen samotný preventivní program, který je uveden na základě SWOT analýz dvou projektů internetové prevence a bezpečnosti. Jsou zde popsány jeho jednotlivé bloky, jejichž součástí jsou podrobně rozepsané aktivity, které může pedagog se svými žáky v rámci tohoto projektu uskutečnit.

1. Kyberšikana – obecný úvod a popis fenoménu

Internet a moderní technologie se stávají čím dál více nepostradatelnější součástí života lidí a obzvláště mladé generace. V současné době patří šikana a jedna z jejích forem, kyberšikana, která probíhá v online prostředí a za pomoci moderních technologií, k nejvýraznějším sociálně patologickým jevům, se kterým se žáci na školách i v mimo školním prostředí běžně setkávají. Dle výzkumu Kopeckého a Szotkowského (2019, s. 22) se s některou z forem kybernetické agrese setkalo 41,29 % z 27 177 participantů výzkumu, který probíhal během roku 2018. Tomuto fenoménu a jeho prevenci se i v souvislosti s jeho velkým nárůstem věnuje čím dál větší pozornost.

1.1. Šikana

Ještě před tím, než přistoupíme k popisu samotné kyberšikany, je třeba se zastavit u šikany tradiční. K vymezení fenoménu šikany můžeme v různých zdrojích najít větší množství definic. „Šikana je ubližování někomu, kdo se nemůže nebo nedovede bránit. Obyčejně mluvíme o šikaně tehdy, když jde o opakované jednání, ve velmi závažných případech označujeme za šikanu i jednání jednorázové, s hrozbou opakování.“ (Janošová, Říčan, 2010, s. 21)

Šikana se může objevovat mezi dětmi a mládeží ve škole či mimo ni, ale probíhá také mezi dospělými na jejich pracovištích. Martínek (2015, s. 129) popisuje šikanu jako jednání, kdy jeden či více žáků úmyslně a také většinou opakovaně týrá jednoho či více spolužáků a používá k tomu agresi či manipulaci.

Šikanující chování se rozlišuje na dva základní termíny, šikanu a teasing. Samotná šikana se objevuje v různých stupních závažnosti a může být těžké ji od teasingu rozlišit, a to jednak pro samotné aktéry šikany, ať už

to jsou její strůjci či oběti, tak i pro dospělé – učitele či rodiče. Jako teasing se označuje chování, které šikanu zdánlivě připomíná. Například může jít o škádlení dívek chlapci na základní škole (Martínek, 2015, s. 128).

Často také dochází k různému pošťuchování mezi chlapci stejného věku ve třídě, ovšem rivalita, škádlení či soupeření je ve vztazích mezi dětmi či mládeží obvyklé a přirozené, nemusí být tedy nutně bráno negativně. Problémem ale bývá to, že určité chování může být za šikanu bráno například jen ze strany oběti, která ovšem může mít strach se ozvat a na svůj problém upozornit. V této souvislosti ale může být šikana utajena nejen ze strany oběti, ale i ze strany agresora, který, pokud vůbec své chování za šikanu považuje, se snaží své jednání skrýt a může k tomu nutit i svou oběť. Podle posledních výzkumů se se šikanou setkalo 41 % dětí na našich školách, což může znamenat, že pokud se tento fenomén nebude intenzivně řešit, bude se počet agresorů i obětí dále zvětšovat (Martínek, 2015, s. 128). Nárůst šikany je spojován také s tím, že roste informovanost veřejnosti v této oblasti a také že se šikana posunuje k méně nápadným formám (Olweus, 2010 cit. podle Janošová, Kollerová, Zábrodská, Kressa a Dědová, 2016, s. 43).

1.2. Definice kyberšikany

Informační a komunikační technologie, které jsou hlavním dějištěm kyberšikany, se rozvíjí tak závratnou rychlostí, na níž není naše společnost zvyklá a reaguje tak na ni se zpožděním. Devadesát procent své historie tyto technologie absolvovaly během druhé poloviny minulého století (Jirovský, 2007, s. 15).

Kyberšikana jako forma šikany je aktuálním tématem přibližně od začátku našeho tisíciletí, ovšem větší pozornost je tomuto fenoménu věnována jen krátce a její zkoumání je teprve na počátku (Černá, 2013, s. 10). K jejímu rozšíření dochází v souvislosti s velkým rozvojem dostupnosti informačních a komunikačních technologií pro běžné uživatele.

Postupně se počítač s připojením k internetu stal běžnou součástí téměř každé domácnosti. Děti a mladší generace dnes vyrůstají obklopeny těmito technologiemi, ať už tou jsou počítače, chytré telefony, tablety či herní konzole s připojením na internet a je pro ně už nemyslitelné se bez nich v normálním životě obejít (Ševčíková, 2014, s. 38).

Kyberšikana je jedním s nejvážnějších rizik, se kterými se mohou děti během používání těchto technologií setkat. V odborné literatuře existuje mnoho definic tohoto tématu. Černá (2013, s. 7) definuje kyberšikanu jako záměrné agresivní chování, které může být prováděno jednotlivcem i skupinou s využitím elektronických médií vůči jedinci, který se útokům nemůže bránit, dopady tohoto chování mohou být na stejně závažné úrovni nebo i ještě závažnější než tradiční šikana.

„Kyberšikanu definujeme jako zneužití informačních a komunikačních technologií, především mobilních telefonů a internetu, k takovým činnostem, které mají někoho záměrně vyvést z rovnováhy. Jedná se tedy o jednu s forem šikany.“ (Martínek, 2015, s. 171)

1.3. Základní znaky kyberšikany

Dle Černé (2013, s. 41) jsou základními znaky kyberšikany skutečnosti – děje se pomocí elektronických médií, jsou opakované, jsou ze strany útočníka vedeny s agresivním záměrem, mají mocenskou nerovnováhu a jednání agresora je obětí vnímáno jako nepříjemné a agresivní.

Útočník může své jednání provádět opakovaně hlavně díky téměř neomezeným možnostem on-line prostředí. Ty mu umožňují například psát zesměšňující či urážející komentáře na adresu oběti pod její příspěvky či profily na sociálních sítích. Může také opakovaně zveřejňovat fotky či videa ve kterých je oběť, protože má tento materiál uložený ve svém počítači. Jako opakování se dá také označit přehrávání ponižujícího videa,

které je zveřejněno na internetu, což je u kyberšikany větší problém než u šikany tradiční. (Černá, 2013, s. 41)

Součástí kyberšikany je také mocenská nerovnováha, kdy nejde o fyzickou převahu agresora nad obětí, ale spíše o situaci, kdy může agresor oběť šikanovat díky prakticky neomezenému přístupu na internet v jakoukoli dobu. Oběť má sice určité prostředky se proti tomu bránit v rámci možností, které sociální sítě poskytují, například tím, že nahlašuje příspěvky, které vytváří agresor, snaží se zablokovat jeho přístup ke svému účtu či může sociální síť úplně opustit. To ovšem nemusí situaci vyřešit, protože velké množství uživatelů dnes figuruje na více sociálních sítích či webových stránkách, kde ho agresor může vyhledat znovu. Úplné zrušení všech účtů, a s tím i naprosté odpojení se od on-line světa, by dnes bylo pravděpodobně pro drtivou většinu uživatelů nepřijatelným řešením.

Černá (2013, s. 45) dále zmiňuje rozdíl mezi kyberšikanou a on-line obtěžováním. Hlavní součástí kyberšikany je agresivní jednání, které oběť vnímá jako ubližující. O on-line obtěžování jde tedy v případě, kdy oběť jednání nevnímá jako zraňující, může je vnímat jen jako nevinné škádlení či jako neúmyslné jednání. Jako on-line obtěžování bývá označován taky spam – nevyžádaná elektronická pošta, posílaná zpravidla s použitím e-mailových klientů, obvykle s reklamním obsahem (Jirovský, 2007, s. 104).

Jedním z dalších a typických aspektů kyberšikany je anonymita útočníků. Ti nemusí vystupovat pod svým jménem, ale mohou se skrýt za přezdívku, využívat anonymní e-mailovou adresu, v případě komunikace pomocí telefonu si mohou skrývat telefonní číslo. Oběť má tedy obvykle problém zjistit jeho identitu. Anonymita může agresora také motivovat k používání promyšlenějších a intenzivnějších forem útoků. Existují samozřejmě možnosti, jak pachatele vystopovat, ale ne vždy mohou být díky velké anonymitě internetového prostředí použitelné (Martínek, 2015, s. 171).

Ve virtuálním světě také dochází k nepoměru mezi skutečným profilem agresora či oběti v reálném světě a jeho sebeprezentací v on-line prostředí. Martínek (2015, s. 172) mluví o spouštěči kyberšikany, kterým může být jedinec dobře ovládající informační a komunikační technologie, nemusí se nutně jednat o fyzicky zdatného jedince, který by mohl mít převahu nad obětí v případě tradiční šikany. Naopak může jít o žáka, který je sám šikanován ve třídě některými spolužáky a internet je pro něj nástroj, kterým může agresorům šikanu oplatit. Uživatelé se v on-line světě chovají jiným způsobem než v realitě, mohou o sobě uvádět nepravdivé informace, mohou komunikovat jiným způsobem, který by si při jednání tváří v tvář nedovolili.

U kyberšikany také není možné nijak předpokládat čas ani místo útoku, může k němu dojít v kteroukoliv denní dobu a na nejrůznějších místech – sociálních sítích či webových stránkách. Pokud je oběť nějakým způsobem připojená na internet či má založený účet na některé sociální síti, který je dostupný, nemá možnost se před útokem schovat. Útočníkovi také k agresi pomáhá publikum – tedy jiní uživatelé, kteří mohou jakékoli příspěvky, fotografie či videa sdílet dál a tím pádem zhoršují jejich dopad na oběť. Vzhledem k tomu, že kyberšikana má charakter psychického útoku, není její dopad na oběť snadno rozpoznatelný. Oběť může mít strach cokoli oznámit například rodičům či učitelům a může se snažit problém řešit sama (Martínek, 2015, s. 172).

Dle některých výzkumů u kyberšikany nezáleží na pohlaví, dívky a chlapci mají být oběťmi šikany stejně často. (Brown, Demaray a Secord, 2014 cit. podle Kopecký, 2015, s. 13)

1.4. Nejčastější projevy kyberšikany

Podle Martínka (2015, s. 173) existují dva základní typy kyberšikany – nepřímá a přímá. Nepřímá kyberšikana probíhá v zastoupení, kdy

za agresora útok vykoná někdo jiný, může se například nabourat do účtu oběti či si založit účet pod jeho její identitou.

Nepřímá kyberšikana, kdy útok provádí sám agresor, je mnohem častější a má větší množství projevů.

Kybergrooming – Martínek (2015, s. 175) tento projev kyberšikany označuje za nejnebezpečnější. Jde o snahu agresora vytvořit si důvěru u oběti, snaží se ji zkusit přinutit k osobnímu setkání a v krajním případě se pokusí o pohlavní zneužití. Nejčastější obětí bývají děvčata ve věku 9–14 let. Agresor může komunikovat s obětí delší dobu, snažit se z ní vylákat intimní fotografie a následně ji s jejich pomocí vydírat.

Kyberstalking – pronásledování, jde o jednání, které může trvat dlouhodobě, agresor oběti opakovaně posílá nepříjemné nebo přímo výhružné zprávy. K tomu může využít různé prostředky používané ke komunikaci – chaty, e-mail či SMS zprávy. Oběť této agrese často neví, jak se bránit a jakým způsobem nevyžádanou konverzaci ukončit. Tento projev kyberšikany patří k nejčastějším, může mít formu, která se podobá nevinným a lehce obtěžujícím zprávám, až po výhružky, kdy může mít oběť obavu o svou bezpečnost (Burges-Proctor, Patchin a Hindua, 2007 cit. podle Šmahaj, 2014, s. 49). Lehčí forma bývá také označována jako kyberharašení, agresor zprávy posílá například vždy, kdy se oběť připojí a je on-line (Černá, 2013, s. 59).

Flaming – prudká hádka, odehrávající se na diskusních fórech, chatech, pod příspěvky na sociálních sítích či pod články různých internetových médií. Součástí bývají urážky, útočné komentáře nebo vyhrožování, ke kyberšikaně ale dochází v případě, kdy je jednání na straně obětí vnímáno jako ubližující (Černá, 2013, s. 59). K plamenným hádkám tohoto typu dochází v internetovém prostředí poměrně často a nemusí být vždy nutně všemi zúčastněnými stranami vnímány jako kyberšikana.

Pomlouvání – rozesílání nepravdivých informací za účelem někoho poškodit. K uskutečnění tohoto jednání se dají použít různé způsoby, ať už sociální sítě, chat či e-mail. Jako těžší forma se dá označit očerňování, kdy může jít o informace přímo hanlivé. Může jít o zveřejňování upravených fotografií či vytváření webových stránek poškozujících oběti (Nancy Willard, 2007 cit. podle Šmahaj, 2014, s. 48).

Bluejacking – dle Martínka (2015, s. 174) se tímto výrazem označuje rozesílání a zveřejňování dehonestujících nebo zesměšňujících obrázků či nahrávek spolužáků.

Krádež identity – agresor může využít účet oběti (například pokud se oběť zapomene odhlásit ze sociální sítě na počítači, ke kterému mají přístup jiní lidé, typicky třeba ve škole). Agresor poté může rozesílat zprávy nebo přidávat příspěvky, a tím poškodit oběť v očích druhých. Druhou možností je vytvoření falešného profilu oběti a vydávání se za ní (Kowalski a kol., 2008 cit. podle Černá, 2013, s. 57). Agresor v tomto případě může k věrohodnosti použít veřejně dostupné fotografie z pravého profilu, přátelé a známí poté nemusí rozeznat, že se za identitou jim známé osoby vydává někdo jiný, a tím se ji snaží nějak zdiskreditovat či poškodit.

Vyloučení, ostrakizace – Černá (2013, s. 57) uvádí jednání, které není přímou agresí, jde o vyloučení určitého jedince ze skupiny, do které by chtěl patřit (typicky například na Facebooku). Pro oběť to může být velmi nepříjemné, a také se může cítit sociálně vyloučena, protože celou záležitost v on-line prostředí viděla větší skupina lidí.

Happy-slapping – fackování, oběť je fyzicky napadena, vše je natáčeno na video, a poté zveřejněno na internetu (Martínek, 2015, s. 175). Oběť útoku je ještě více ponížena tím, že nahrávku může vidět velké množství lidí. Podle Černé (2013, s. 62) existují i případy, kdy byla oběť místo fackování donucena například ke svlékání a další šíření videa ji dovedlo až k sebevraždě.

1.5. Prostředky kyberšikany

Jako prostředky kyberšikany se označují zařízení a média, pomocí kterých může kyberšikana probíhat. To mohou být hlavně počítače, mobily či tablety s připojením na internet V případě internetových médií jde hlavně o sociální sítě, chaty či e-mail, také internetové hry. Dále může jít také o kyberšikanu pomocí zasílání SMS či MMS zpráv.

Dle výzkumu Kopeckého a Szotkowského (2019, s. 7) využívalo u nás sociální sítě 75 % dotázaných dětí ve věku 13–17 let. U služeb, zaměřených primárně na sdílení videí (např. Youtube) to bylo téměř 56 % dotázaných.

Mezi sociální sítě populární u nás i ve světě se řadí Facebook, který je založen na vytváření vlastního profilu a seznamování se s jinými lidmi či sdílení fotografií. V roce 2018 měla tato sociální síť už 2,5 miliardy uživatelů, což je třetina celé zemské populace (Internetem Bezpečně, 2018).

Hlavním smyslem této sociální sítě je neustálý kontakt s jinými lidmi, který je dnes možný díky mobilnímu internetu dostupnému téměř kdekoli. To vede k situaci, kdy se projevy šikany (zde typicky ubližující komentáře k fotografiím či statusům), rychle šíří v rámci sociální skupiny, do které oběť patří a může vést až k ostrakizaci – vyloučení ze skupiny přátel v rámci sociální sítě i mimo ni (Černá, 2013, s. 65).

Stejný problém může nastat i u sociální sítě Instagram, zaměřené na sdílení fotografií. Podle výzkumu Kopeckého a Szotkowského (2019, s. 9) tuto sociální síť využívá 90 % dětí z dotázaných.

Jako další prostředek kyberšikany bývá uváděno posílání zpráv – instant messaging. Tento způsob internetové komunikace dnes probíhá z části i na sociálních sítích (Ševčíková, 2014, s. 53).

Jako jeden z projevů kyberšikany se zde odehrává například kyberstalking, kdy může být oběť zahlcována obtěžujícím zprávami agresora, který navíc může vystupovat anonymně.

Specifickým prostředkem kyberšikany mohou být on-line interaktivní hry, jejichž součástí může být chat či hlasová forma komunikace s jinými hráči, v jejímž rámci může docházet k nepříjemnému obtěžování, či dokonce vulgárnímu napadání a vyhrožování. I zde může dojít k určitému vyloučení jedince ze skupiny hráčů, které může mít charakter šikany (Černá, 2013, s. 65).

Využívány jsou také služby pro videohovory (typicky aplikace Skype), videohovory lze uskutečňovat i přes sociální sítě, jako je například Facebook. Zde se může odehrávat velmi závažný projev šikany, kybegrooming, který může v extrémním případě vyústit až v sexuální zneužívání.

Jednou z možností kyberšikany je vytváření webových stránek či blogů, určených k zesměšnění či pomlouvání oběti, ať už nepravdivými informacemi či publikováním fotografií a videonahrávek.

V případě kyberšikany s využíváním e-mailových klientů jde o jednu z častých forem kyberšikany zvláště z důvodu velké rozšířenosti tohoto typu komunikace. E-mailový účet dnes vlastní téměř každý, ať už jde o účet osobní, či například účet školní a firemní, který si může agresor lehce vyhledat. Ten může také vystupovat v anonymitě.

Mobilní telefon je aktuálně nepostradatelným komunikačním nástrojem nejen pro děti a mládež, proto i ten může sloužit potencionálnímu agresorovi jako prostředek kyberšikany. Ať už je to posílání obtěžujících či výhružných SMS a MMS zpráv, či neustálé volání v jakoukoliv denní dobu. I zde se útočník může skrýt za anonymitu SIM karet, které jsou jednoduše dostupné v mnoha prodejnách. Pro oběť může být řešením změna telefonního čísla, ovšem může jít o skrytého agresora z jeho okolí, který si i nové telefonní číslo může zjistit (Šmahaj, 2014, s. 50).

1.6. Příčiny kyberšikany, agresoři a oběti

Příčiny kyberšikany mohou být obdobné jako u tradiční šikany nebo se jí mohou podobat v některých znacích. Jednou z častých příčin kyberšikany bývá odplata za tradiční šikanu, která může probíhat například ve školním prostředí. Její oběti se takto mohou snažit oplatit agresorovi jednání, proti kterému se v reálném světě nemohou nebo neumí adekvátně bránit. Jako další příčina toho jednání může být názor agresora, že si to oběť zasloužila, což je podobný případ jako u odplaty, s tím rozdílem, že to nemusí být nutně z důvodu předchozí agrese oběti na agresorovi, ale klidně kvůli nějakému jinému chování. Další možností může být chápání kyberšikany ze strany agresora jako nevinného škádlení či žertu (Hindua, Patchin, 2009 cit. podle Černá, 2013, s. 76).

Agresoři mohou být jedinci, kteří na sebe chtějí upozornit, nemusí být například oblíbení v kolektivu spolužáků a neví, jak jinak na sebe upoutat pozornost. Mohou mít nižší sebevědomí, mohou se snažit o uznání ostatních (Shariff, 2008 cit. podle Kopecký, 2015, s. 23).

Na druhé straně může jít o agresory, kteří mají vysoké sebevědomí i uznání v kolektivu, a právě toho mohou využívat i při šikaně (Sutton, Smith a Swettenham, 1999 cit. podle Kopecký, 2015, s. 23). Důvodem ke kyberšikaně může být také nuda a dostupnost vhodné oběti. Uvádí se také, že agresoři nemusí mít rozvinutou empatii jako ostatní děti, proto s agresivním chováním nepřestávají (Olweus, 1993 cit. podle Černá, 2013, s. 185). Nemusí si tedy uvědomovat následky svého chování.

Oběti kyberšikany jde dle některých výzkumů charakterizovat jako jedince, kteří mohou být více závislí na internetu a necítí se oblíbení v kolektivu (Vandeboshová a Van Cleemputová, 2009 cit, podle Šmahaj, 2014, s. 53). Tím se mohou stát snadným terčem útoku někoho z kolektivu, kdo oběť zná. Dále ale může jít i o situaci, která byla v této práci už zmíněna, kdy se obětí kyberšikany stane agresor šikany tradiční, zde tedy

toto chování slouží jako nástroj pomsty. S tím samozřejmě souvisí anonymita internetového prostředí, kterou může agresor s úspěchem využít.

V České republice není znám případ, kdy by kyberšikana skončila sebevraždou oběti. Existuje ale množství závažných případů, které měly pro oběť nezanedbatelné následky. Například v roce 2008 v Moravské Třebové přerostla tradiční šikana v kyberšikanu, kdy byl třináctiletý chlapec opakovaně napadán slovně i fyzicky svými spolužáky. Nakonec ho svázali izolační páskou k židli, kterou povalili na zem, naznačovali kopání do hlavy a toto celé jednání si natáčeli na mobilní telefon. Známým případem ze zahraničí je také případ kyberšikany dívky z gymnázia v polském Gdańsku, který skončil tragicky. Její spolužáci ve třídě natáčeli záznam, kdy předstírali její znásilnění. Dívka toto ponížení neunesla a spáchala sebevraždu. Policii se podařilo viníky usvědčit hlavně kvůli rekonstrukci videozáznamu smazaného z mobilního telefonu (Krejčí, 2010, s. 36–44).

1.7. Prevence a řešení kyberšikany, pomoc obětem

V oblasti prevence kyberšikany je důležité takové chování či povědomí dětí a mládeže, aby v ideálním případě ke kyberšikaně vůbec nedošlo. K tomuto účelu u nás existuje několik preventivních programů, které se snaží o preventivní informování dětí a mládeže, jejich rodičů i učitelů a odborníků o těchto problémech a tom, jak na ně reagovat a jak je řešit.

Projekt Internetem Bezpečně se prezentuje hlavně pomocí webové stránky internetembezpečně.cz, případně pomocí profilů na sociální síti Facebook či Youtube. Snaží se zvýšit povědomí veřejnosti o rizicích internetu, reaguje na aktuální hrozby a snaží se jejím následkům předcházet. Cílovou skupinou jsou nejen děti a mládež, ale i rodiče, handicapovaní, pedagogové či specialisté prevence. Na webových stránkách lze najít konkrétní témata internetové bezpečnosti – kyberšikanu, sociální sítě,

nebezpečí počítačových virů či kybernetické kriminality. Je zde také sekce pro rodiče či praktické informace, jak chránit svůj počítač a uživatelské účty. Projekt také zveřejňuje aktuální články, které se věnují současným problémům v prostředí bezpečnosti na internetu. Existují zde také materiály pro děti a rodiče, které jsou srozumitelné a přehledné, ale i metodiky pro pedagogy, využitelné během školních preventivních aktivit. V neposlední řadě projekt nabízí přednášky na jednotlivá témata, které jsou dobře využitelné například pro školy v rámci prevence, ale i pro různé organizace, pracující s dětmi či mládeží (Internetem Bezpečně, 2018).

Dalším příkladem projektu zabývajícím se kyberšikanou, je projekt E-Bezpečí, jenž je realizován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého. Má široký realizační tým, ve kterém působí řada pedagogů a odborníků ze samotné univerzity, je financován z veřejných rozpočtů, soukromých zdrojů i vlastních příjmů. Pořádá přednášky a besedy na školách i v jiných organizacích a také realizuje vlastní výzkumná šetření. Specializuje se na kyberšikanu a sexting, kybergrooming, kyberstalking, rizika sociálních sítí, on-line závislosti či zneužití osobních údajů v prostředí internetu. Na svých webových stránkách nabízí velké množství materiálů, metodik a publikací, které mohou využít pedagogové či školy, které chtějí realizovat preventivní program. Dále může nabídnout přednášky na různá témata či výsledky vlastních výzkumů (E-Bezpečí, 2008–2020).

To kromě preventivních programů, které se snaží zvyšovat povědomí o tomto problému a kterým se budeme věnovat později, zahrnuje i chování, které má potenciální kyberšikaně zamezit. Sem se řadí například osobní promluva, díky níž je možnost vyřešit nepochopení, které může ve virtuální realitě nastat. Dle některých výzkumů panuje přesvědčení, že úplná prevence kyberšikany možná není, protože se jí v anonymním internetovém prostředí nedá zcela vyhnout (Černá, 2013, s. 343–348).

Martínek (2015, s. 179) uvádí jako základní pravidla při setkání s kyberšikanou okamžité ukončení komunikace s agresorem, nereagování na jeho další pokusy o kontaktování (chat, e-mail, SMS), dále archivování veškeré komunikace jako zajištění důkazního materiálu a následně podání trestního oznámení na neznámého pachatele na Policii ČR. Poté by se oběť měla pokusit změnit si identitu, ať už profil na sociální síti, změnu e-mailové adresy či telefonního čísla. Důležitou součástí prevence je také promyšlené předávání svých kontaktů jen osobám, které jedinec zná.

Častým problémem obětí kyberšikany bývá ovšem strach cokoli oznámit, ať už z důvodu pomsty či zhoršení útoků agresora či z důvodu studu za situaci, do které se dostal. Pokud je šikanující chování ze strany agresora ve stádiu menší závažnosti, jde například jen o obtěžující konverzaci na chatu či sociální síti, jsou zde možnosti, jak komunikaci s konkrétním uživatelem zablokovat či nahlásit jeho nevhodné příspěvky správcům sociální sítě, chatu či konkrétní webové stránky.

Černá (2013, s. 351–358) tato řešení označuje jako technicky zaměřené strategie a také jako primární způsob ochrany. Další strategií je vyhýbání se či ignorance, jde například o mazání nevhodných zpráv či příspěvků, nenavštěvování určitých stránek či neodpovídání na obtěžující zprávy. Jako disociace se nazývá představa, kdy si jedinec sám oddělí on-line a off-line svět a nebere chování lidí v on-line světě tak vážně. To ovšem jde jen do určité míry závažnosti. Přerámováním se označuje takové chování jedince, který se setkal s obtěžujícím či nevhodným chováním, které se snaží snížit závažnost jednání agresora a svou reakci na něj. Další možností je odplata agresorovi, pomsta za jeho chování, která může ale probíhat i off-line. Oběť se také může pokusit o přímou konfrontaci s agresorem, ať už on-line či off-line, snažit se si s ním vyřešit situaci, zjistit důvod jeho chování. Jinou možností je vyhledání sociální podpory od někoho, kdo může oběti situaci pomoci vyřešit. Toto řešení se jeví jako nejjistější v případě, kdy útok agresora zanechal na oběti nějaké následky a ta neví, jak se zachovat. Může vyhledat pomoc u rodičů, ve školu

u učitelů, případně i kamarádů, další možností je třeba anonymní linka důvěry.

Dle některých výzkumů mají oběti kyberšikany problém se svěřit nějaké autoritě, například rodičům a pokud už se rozhodnou s někým svůj problém sdílet, jsou to často jejich vrstevníci. Oběti mohou mít strach, že jim nebude nikdo věřit nebo že situaci přehání, což může být problém právě v online prostředí, kde nejsou dopady jednoznačně vidět (Černá, 2013, s. 368–370).

Dopady kyberšikany ovšem na obětech mají následky, které se postupně projevují. Můžou to být sociální problémy, oběť se může uzavírat před kolektivem, vyhledávat osamělost. Dále mohou být viditelné problémy v chování, které se dříve neděly (Gradinger, Strohmeier a Speil, 2010 cit. podle Kopecký, 2015, s. 25).

Také se uvádí, že se chování obětí může změnit tak radikálně, že mohou odmítat chodit do školy, mohou být nemocné. Až 8 % obětí kyberšikany také uvažovalo o sebevraždě (Hindua, Patchin, 2010 cit. podle Kopecký, 2015, s. 25).

V této souvislosti je důležitá určitá pozornost autorit, ať už učitelů, tak hlavně i rodičů, kteří by se měli zajímat o aktivity svých dětí na internetu. Samozřejmě je to obtížné zvlášť v dnešní době, kdy tam děti tráví spoustu času a je třeba jim také zachovávat určité soukromí. Určitě by si ale rodiče měli všímat změn v chování svých dětí, které samozřejmě nemusí, ale i mohou mít svůj původ v kyberšikaně.

1.8. Legislativa

Dle Šmahaje (2014, s. 69–70) není v České republice kyberšikana ošetřena přímo v trestním zákoníku. V případě kyberšikany je ovšem možné využít například zákon č. 561/2004 Sb. o předškolním, základním, středním, vyšším odborném a jiném vzdělávání ve znění pozdějších předpisů – řeší

práva a povinnosti školy a studentů a jejich zákonných zástupců. Dále to může být zákon č. 40/1964 Sb., občanský zákoník, §§ 12 a 13 – zákaz natáčení, fotografování a zveřejnění snímků bez souhlasu dotyčné osoby, § 205 – Ohrožování mravnosti, § 217a – Svádění k pohlavnímu styku nebo o zákon č. 359/1999 Sb. – O sociálně-právní ochraně dětí.

2. Bezpečné chování na internetu

Chování v on-line prostředí má na rozdíl od chování v prostředí reálném určitá specifika, spočívající v anonymním prostředí, v absenci fyzického kontaktu, v pocitu, že je možné si dovolit něco, co v běžném reálném světě nejde a že se to do reálného světa nijak nepromítne. Téměř každý uživatel internetu si dnes zvykl na to, že o sobě zveřejňuje určité informace. Problémem ovšem může být to, kdo má k těmto informacím přístup. Mnoho lidí také nedbá na zabezpečení svých zařízení během připojení na internet či neláme si hlavu nad hesly do svých účtů.

V následující tabulce jsou uvedeny jednoduché a základní pokyny k bezpečnému používání internetu (Internetem Bezpečně, 2018).

Zásady bezpečného používání internetu
1. Připojovat se na internet jen z důvěryhodného zdroje. Při připojení na veřejné wifi síti nikdy nezadávat hesla.
2. Udržovat aktualizovaný počítač (operační systém, internetový prohlížeč, antivirový program).
3. Instalovat programy jen z důvěryhodného zdroje.
4. Nastavení automatického zamykání počítače a telefonu při delší nečinnosti.
5. Používání silných a bezpečných hesel – nikomu je nesdělovat, ani nikam nepsat.
6. Kontrola zabezpečení a sdílení na sociálních sítích (Facebook, Instagram)
7. Ověřovat informace, které se objevují na internetu, ve více zdrojích.
8. Číst si podmínky používání služeb a aplikací, nezadávat bezmyšlenkovitě souhlas.
9. Chránit své osobní údaje (adresu, datum narození, telefonní číslo, e-mail, doklady)
10. Neotvírat nedůvěryhodné e-maily, neklikat na odkazy, které se v nich nachází a neotvírat přílohy.

2.1. Ochrana osobních údajů a soukromí

V případě nejvyužívanějších sociálních sítí (např. Facebook) má každý uživatel možnost o sobě sdělit určité informace. Tyto sociální sítě jsou naprogramovány tak, aby toho uživatelé o sobě mohli sdělit co nejvíce a sdíleli to s ostatními uživateli. Mnoho uživatelů poté nepozná, co vše by mělo být soukromé či veřejné, tento problém se také ve velké míře týká dětí a mládeže (Ševčíková, 2014, s. 144). Na sociální síti Facebook uživatelé vystupují obvykle pod svým jménem, případný agresor si tedy může vyhledat profil konkrétního člověka. Problémem jsou tedy veřejné osobní údaje, což jsou informace, pod kterými jde konkrétní osoba jednoznačně identifikovat. Za tyto údaje se považují jméno, příjmení, identifikační údaje

dokladů, pohlaví, datum narození, věk, osobní stav, telefonní číslo či adresa (ManagmentMania, 2011–2016).

Podle některých studií ovšem děti a mládež některé tyto údaje často sdílí v rámci sociálních sítí či internetu i s lidmi, které dobře neznají (Madden a kol., 2013 cit. podle Ševčíková, 2014, s. 151). Se sdílením těchto údajů se zvyšuje riziko krádeže identity, samotných osobních údajů či je možná i kyberšikana. Důležitým krokem k nastavení soukromí je mít okruh přátel v on-line světě stejný jako v realitě. Je tedy důležité zvažovat, koho si do přátel přidávat a jestli bychom to udělali i v reálném světě.

2.2. Hesla

Častým problémem v oblasti zabezpečení účtů bývají hesla. Ať už jde o hesla k účtu osobního počítače, hesla k účtům na různých sociálních sítích a webových stránkách či hesla a zabezpečení internetového bankovnictví. Mnoho uživatelů internetu tomuto důležitému prvku zabezpečení nevěnuje potřebnou pozornost a nevolí si dostatečně silná hesla. Častým argumentem některých lidí bývá, že není v jejich silách si více složitějších hesel zapamatovat.

Jako heslo se označuje řetězec nesnadno uhodnutelných znaků, proto by se neměla používat hesla triviální a snadno uhodnutelná, typickou chybou bývají samostatná slova, jména blízkých osob, domácího mazlíčka, datum narození či jednoduchá posloupnost čísel. Doporučená délka bezpečného hesla je minimálně 8 znaků, kdy doporučeno je znaků 12–14. Heslo by také mělo obsahovat kombinaci číslic, malých a velký písmen a speciálních znaků. Existují programy (passwordcrackery), které jsou určené na prolamování hesel, některé například zkouší různé kombinace znaků a je proti nim tedy účinná co nejsložitější kombinace znaků. Důležité také je nepoužívat jedno heslo pro přihlášení do všech účtů. Doporučuje se vytvořit tři okruhy hesel, jedno pro přihlášení do počítače či telefonu, druhé pro aplikace, e-mail či sociální sítě a třetí do internetových obchodů, fór

nebo her. Hesla by také neměla být nikde napsána, zvláště u počítače nebo do telefonu. Je také třeba mít na paměti, že v případě veřejných wi-fi připojení existuje větší riziko krádeže hesla, proto není rozumné se zde přihlašovat k tak citlivým účtům, jako je například internetové bankovnictví (Internetem Bezpečně, 2018).

2.3. Malware

Anglické slovo Malware znamená škodlivý software, počítačový program, který vnikne do systému za účelem poškození nebo krádeže dat či sledování uživatele. Základními prvky obrany před tímto nebezpečím je instalace antivirového programu, aktualizovaný operační systém a internetový prohlížeč. Důležité je také nestahovat neznámé soubory a aplikace, neotevírat a neodpovídat na neznámé a podezřelé e-maily. Neméně podstatné je také zálohování osobních dat i jinde než na svém počítači, ať už například na externím hard disku či s použitím nějaké online služby (Google Disk, Microsoft Drive). (Internetem Bezpečně, 2018)

2.4. Spam, phishing

Jednou z častých podvodných praktik, se kterou se setkává velké množství uživatelů internetu, je spam. Jde o nevyžádanou poštu, která se může šířit jak e-mailovou komunikací, tak pomocí různých chatů a komunikačních prostředků (např. Facebook messenger). Spammeři mohou získat elektronické adresy, na které poté zasílají nevyžádané zprávy, různým způsobem, často se uživatelé bez rozmyslu pomocí e-mailu registrují na stránky, které slibují různý obsah zdarma, a není na nich jasně ošetřeno, kdo bude mít k adrese přístup (Jirovský, 2007, s. 104).

Spamové e-maily mohou obsahovat škodlivý software – malware. Také se může jednat o podvodné jednání, nazývané phishing, v e-mailu se mohou nacházet odkazy na podvodné stránky, které se snaží z uživatelů vylákat citlivé údaje. Možností, jak se chránit, je několik. Hlavní zásadou je

nezveřejňovat zbytečně e-mailovou adresu, aby nebyla jednoduše dohledatelná potenciálními útočníky. Pokud je to nutné, je rozumné ji zveřejňovat ve formátu jmeno(zavinac)domena.cz. Důležité je také se vyvarovat otevírání příloh neznámých či podezřelých e-mailů, neklikat na odkazy a e-mail nejlépe rovnou smazat (Internetem Bezpečně, 2018).

Časté bývají také e-maily, které se tváří jako zpráva od banky a žádají o zadání přístupových údajů do internetového bankovnictví. Banky o údaje nikdy takovýmto způsobem nežádají, podvodný e-mail se také dá identifikovat podezřelou adresou odesílatele. V případě internetového bankovnictví má zásadní význam tzv. dvoustupňové ověření, kdy je potřeba pro přihlášení také kód, který přijde formou SMS zprávy na zadané telefonní číslo přímo od banky.

3. Návrh programu prevence kyberšikany a bezpečnosti na internetu

Navrhovaný program prevence kyberšikany a bezpečnosti na internetu je zpracován jako soubor aktivit v blocích, které se věnují tématu sociálních sítí, kyberšikany a kybergroomingu a také bezpečnosti na internetu. Je určen pro druhý stupeň základních škol a má sloužit jako program všeobecné primární prevence pro základní orientaci žáků v uvedených tématech.

3.1. SWOT analýzy vybraných projektů

V tomto oddílu praktické části bakalářského projektu jsou uvedeny SWOT analýzy dvou vybraných projektů, které jsou zaměřeny na bezpečné chování a prevenci negativních jevů, probíhajících v internetovém prostředí a prostřednictvím informačních a komunikačních technologií. S přihlédnutím k poznatkům těchto analýz je poté samotný projekt preventivního programu zpracován.

3.1.1 Internetem Bezpečně

O projektu	
➢ Snaží se zvýšit povědomí uživatelů o rizicích internetu ➢ Reaguje na nové hrozby a informuje o nich prostřednictvím svých webových stránek či vzdělávacích akcí	
Silné stránky	**Slabé stránky**
➢ Přehledné a obsáhlé webové stránky ➢ Aktuální informace a články ➢ Materiály a metodiky ➢ Nabídka přednášek	➢ Projekt nemá celostátní dosah ➢ Systematicky nespolupracuje se školami či Ministerstvem školství
Příležitosti	**Hrozby**
➢ Dosah a možnost ovlivnění mladé generace ➢ Možnosti pořádání přednášek prakticky kdekoli	➢ Existence podobných projektů ➢ Závislost na zájmu ze strany organizací či uživatelů

O projektu

Projekt Internetem Bezpečně se snaží hlavně pomocí webových stránek internetembezpečně.cz, případně pomocí profilů na sociálních sítích Facebook či Youtube zvýšit povědomí veřejnosti o rizicích internetu. Na aktuální hrozby reaguje a snaží se jejím následkům předcházet. Cílovou skupinou jsou nejen děti a mládež, ale i rodiče, handicapovaní, pedagogové či specialisté prevence (Internetem Bezpečně, 2018).

Silné stránky

Přehledné a obsáhlé webové stránky – rozčlenění v rámci jednotlivých pod stránek na konkrétní témata internetové bezpečnosti – kyberšikanu, sociální sítě, nebezpečí počítačových virů či kybernetické kriminality. Je zde také sekce pro rodiče či praktické informace, jak chránit svůj počítač či uživatelské účty.

Aktuální informace a články – projekt se věnuje aktuálním problémům v prostředí bezpečnosti na internetu pomocí článků, které zveřejňuje.

Materiály a metodiky – jsou zde také materiály pro děti a rodiče, které jsou srozumitelné a přehledné, ale i metodiky pro pedagogy, využitelné během školních preventivních aktivit.

Nabídky přednášek – projekt nabízí přednášky na jednotlivá témata, které jsou dobře využitelné například pro školy v rámci prevence, ale i pro různé organizace, pracující s dětmi či mládeží.

Slabé stránky

Projekt nemá celostátní dosah – projekty, které jsou uvedeny, probíhaly jen v rámci Karlovarského kraje

Systematicky nespolupracuje se školami či Ministerstvem školství – projekt nemá celostátní dosah i díky tomu, že pravidelně nespolupracuje s konkrétními školami či Ministerstvem školství.

Příležitosti

Dosah a možnost ovlivnění mladé generace – díky aktuálnímu profilu na Facebooku či Youtube je zde možnost dostat se do povědomí mladé generace právě díky tomu, že jsou mezi nimi tyto sociální sítě velmi oblíbené.

Možnosti pořádání přednášek prakticky kdekoliv – nabídky pořádání přednášek na aktuální témata pro školy či organizace kdekoliv u nás.

Hrozby

Existence podobných projektů – projekt je díky konkurenci podobných projektů, které spolu systematicky nespolupracují, odkázán na dostatečný zájem ze strany uživatelů či škol.

Závislost na zájmu ze strany organizací či uživatelů – v případě nezájmu za strany samotných dětí, mládeže či škol a organizací, díky nedostatečné propagaci, se projekt může v krajním případě dostat i do existenčních problémů.

3.1.2 E-Bezpečí

O projektu	
➢ Celorepublikový projekt zaměřený na prevenci, vzdělání a výzkum v oblasti rizikového chování na internetu	
Silné stránky	**Slabé stránky**
➢ Realizován pod Pedagogickou fakultou Univerzity Palackého ➢ Početný realizační tým ➢ Velké množství materiálů či metodik, vlastní výzkum	➢ Webové stránky pro svou rozsáhlost ne zcela atraktivní pro mladší generaci
Příležitosti	**Hrozby**
➢ Možnosti realizace velkého množství projektů či přednášek	➢ Existence podobných projektů

O projektu

Projekt E-Bezpečí je realizován pod Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého. Má široký realizační tým, je financován z veřejných rozpočtů, soukromých zdrojů i vlastních příjmů. Pořádá přednášky a besedy na školách i v jiných organizacích a také realizuje vlastní výzkumná šetření. Specializuje se na kyberšikanu a sexting, kybergrooming, kyberstalking, rizika sociálních

sítí, on-line závislosti či zneužití osobních údajů v prostředí internetu (E-Bezpečí, 2008–2020).

Silné stránky

Realizován pod Pedagogickou fakultou Univerzity Palackého – realizace projektu pod Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého přináší výhody v dostupnosti odborníků, působících v univerzitním prostředí, kteří se na projektu mohou podílet a velkém dosahu aktivit, které mohou využít jméno samotné univerzity.

Početný realizační tým – na projektu spolupracuje velké množství lidí, což může skýtat výhody hlavně ve velkém množství realizovaných přednášek, vypracovaných metodik či publikací, které mohou dopodrobna obsáhnout velké množství aktuálních témat v oblasti rizikového chování na internetu.

Velké množství materiálů či metodik, vlastní výzkum – jak bylo zmíněno výše, díky mnoha zainteresovaným odborníkům projekt na svých webových stránkách nabízí dostatek materiálů, metodik či publikací, které mohou využít pedagogové či školy, kteří chtějí realizovat preventivní program. Dále může nabídnout přednášky na různá témata či výsledky výzkumů, vedených vlastními odborníky.

Příležitosti

Možnosti realizace velkého množství projektů či přednášek – projekt má kapacitu na uskutečňování značného počtu přednášek na školách či v jiných organizacích, které mohou mít zásadní z hlediska povědomí o bezpečném chování v internetovém prostředí vliv na děti, mládež či jiné uživatele informačních technologií.

Hrozby

Existence podobných projektů – i tento projekt může čelit určité konkurenci ze strany podobných projektů, kterých u nás momentálně probíhá celá řada.

3.2. Cíle programu

Cílem programu je zvýšení informovanosti a povědomí žáků druhého stupně v oblasti kyberšikany a bezpečnosti na internetu. Vzhledem k tomu, že kyberšikana patří k základním formám rizikového chování uvedených v Národní strategii primární prevence rizikového chování dětí a mládeže na období 2019–2027 (MŠMT, 2019, s. 6), program a jeho jednotlivé části by měly preventivně působit na schopnosti žáků, předcházet tomuto rizikovému chování, které v rámci pohybu v internetovém prostředí může nastat, případně působit na schopnosti žáků na rizikové situace adekvátně reagovat.

Program je zaměřen také na bezpečné chování na sociálních sítích či na problematiku hesel a bezpečnosti na internetu obecně. Jedním z cílů je nenásilné, zábavné a poučné působení na žáky, které si neklade za úkol je zahltit velkým množstvím informací, ale spíše v nich probudit zájem o tuto problematiku pomocí aktivit či modelových situací. V neposlední řadě jde také o sdílení zkušeností s internetovým prostředím a jeho riziky mezi samotnými spolužáky, kde má pedagog působit jako jakýsi mediátor či průvodce, který se snaží jim pomoci pochopit a vysvětlit danou tematiku.

3.3. Charakteristika programu

Program prevence kyberšikany a bezpečnosti na internetu je koncipován jako program všeobecné primární prevence a je zpracován na základě poznatků, získaných ze SWOT analýz dvou vybraných projektů, tedy projektu Internetem Bezpečně a E-Bezpečí a studiem dalších

podobných projektů a materiálů či metodik, které jsou v jejich rámci nabízeny. Program si neklade za cíl nahradit výše uvedené projekty, které jsou svým rozsahem mnohem obsáhlejší. Jeho hlavní myšlenkou je nabídnout učitelům již zpracovaný soubor aktivit, jenž je připraven k okamžité realizaci a který by měl sloužit jako jakýsi základní úvod do oblasti kyberšikany a bezpečnosti na internetu, díky kterému by žáci, kteří ho absolvují, měli získat elementární povědomí o rizicích, které informační a komunikační technologie skýtají. Na takto získané poznatky mohou dále navázat například další preventivní programy, které budou zaměřeny podrobněji a konkrétněji na vybraný problém. Jedním z cílů programu je také finanční nenáročnost, kdy nejsou potřeba žádné speciální pomůcky.

Součástí programu jsou aktivity, které se snaží danou oblast žákům přiblížit názorným a zábavným způsobem, nesnaží se je zahltit velkým množstvím informací. Aktivity mají formu her nebo diskuzí, jsou využita naučná videa, součástí je i návštěva projekce filmu V síti.

3.4. Pokyny k realizaci

Celý program může uskutečnit jeden pedagog s celou třídou. Ten by měl po prostudování teoretické části tohoto bakalářského projektu získat základní přehled v dané oblasti, s jehož pomocí bude schopen sám připravit jednotlivé aktivity, vést diskuzi s žáky a odpovídat na jejich dotazy.

V oblasti pomůcek pracuje s možnostmi, které jsou k dispozici téměř v každé škole, k jeho realizaci je potřeba tedy hlavně dataprojektor a počítač s připojením na internet a případně školní počítač, tablet či chytrý telefon pro ty žáky, kteří nemají k dispozici svůj přístroj, který je potřeba k některým aktivitám. Dále to jsou jen papíry a běžné psací potřeby.

Program se skládá z pěti bloků, které jsou naplánovány tak, aby jejich časová náročnost byla zhruba dvakrát 45 min a mohly tak být realizovány během vybraných školních hodin.

3.5. Rozpočet programu a personální obsazení

Rozpočet programu se skládá ze mzdy pracovníka, určené samotnou školou, která bude program realizovat, materiálních nákladů potřebných na vypracování aktivit a vstupného na promítání filmu V síti. Předpokládá se, že pomůcky jako dataprojektor, počítač, tablet či jiný přístroj k zapůjčení pro žáky má k dispozici škola a není třeba je pořizovat. To samé může platit i o materiálu, který je potřebný k vypracování aktivit, i ten může případně pedagog využít z prostředků školy.

Níže uvedené náklady jsou spočítány pro vzorovou třídu, která má 25 žáků. Předpokládá se, že uhrazení těchto nákladů bude probíhat z rozpočtu školy, která bude program realizovat.

Materiální náklady (papíry A3 a A4, psací potřeby – tužky, propisky, sady fixů, lepicí páska) – 520,- Kč.

Vstupné na promítání filmu V síti pro školy – 80,- Kč/osoba (pedagog zdarma) – 2000,- Kč pro 25 žáků.

Celkové náklady – 2520,- Kč.

K zajištění financování je možnost využít dotaci v souvislosti s Výzvou na poskytování aktivit v oblasti primární prevence rizikového chování ve školách a školských zařízeních v období 2019–2021 pro rok 2020, zveřejněnou na webových stránkách Ministerstva školství, mládeže a tělovýchovy. Žádost o dotaci předkládá konkrétní škola, ve které bude program realizován.

V souvislosti s touto dotací jsou v podmínkách zveřejněných Ministerstvem školství, mládeže a tělovýchovy určeny minimální kompetence pracovníka, který bude program realizovat. V případě programu všeobecné primární prevence, do které tento projekt spadá, musí pracovník:

- mít dokončené středoškolské vzdělání s maturitou,
- mít absolvován základní kurz primární prevence v rozsahu 40 hodin s minimálním podílem 8 hodin sebezkušenosti,
- mít alespoň započaté další studium (VOŠ, VŠ, jiná specializační studia), které je svým obsahem zaměřeno na práci s lidmi (pedagogika, speciální pedagogika, psychologie, adiktologie, zdravotnictví, sociální práce) – tento bod lze v odůvodněných případech nahradit specifickými znalostmi a dovednostmi z různých oborů (například zástupci záchranného systému, policisté, pracovníci hygienických a lékařských zařízení) či dlouholetou praxí.

3.6. První blok – sociální sítě

Cíl bloku: Žáci by se měli orientovat v oblasti zveřejňování soukromých informací na internetu, měli by si uvědomit, které údaje jsou citlivé a zneužitelné a jak své soukromé údaje chránit na příkladu konkrétní sociální sítě.

Aktivita 1: Co vím o ostatních

Délka aktivity: 30 min

Pomůcky: chytrý telefon (pokud žáci nemají, je potřeba zajistit školní notebook, tablet či telefon), počítač s dataprojektorem, papíry velikosti A4, psací potřeby – propisky, tužky.

Průběh aktivity:

Každý z účastníků dostane čistý papír velikosti A4, který nadepíše svým jménem. Každý poté papír pošle svému sousedovi doprava. Pedagog všem vysvětlí, že pokud nebudou vědět odpověď, mohou využít internet na svém telefonu (tomu, kdo nebude mít k dispozici telefon s internetem, učitel zapůjčí školení tablet). Pedagog poté začne dávat o otázky, může je

postupně promítat dataprojektorem. Každý odpoví na otázku, pokud bude znát odpověď a poté zase pošle papír doprava sousedovi.

Otázky:

1. Oblíbená činnost?
2. Oblíbený film/seriál?
3. V které zemi byl/a naposledy na dovolené?
4. Kolik má sourozenců?
5. Jaký kroužek navštěvuje?
6. Jméno dobrého kamaráda?

Závěrečná diskuze:

Následuje diskuze moderovaná učitelem, ten se ptá každého účastníka, jestli jsou odpovědi pravdivé a jestli si myslí, že je ostatní věděli nebo je našli na internetu. Snaží se s žáky bavit o tom, jaké informace zveřejňují na svých profilech na sociálních sítích a jestli ví o tom, kdo k nim má přístup.

Aktivita 2: Profil na sociální síti

Délka aktivity: 45 min

Pomůcky: počítač s připojením na internet a dataprojektorem, papíry A3, psací potřeby – tužky, pastelky, fixy, lepicí páska či magnety na tabuli k připevnění vytvořených profilů.

Průběh aktivity:

Každý žák dostane papír velikosti A3 a psací potřeby – tužku, pastelky, fixy. Pedagog žákům vysvětlí, že se mají pokusit nakreslit svůj profil na sociální síti, kde mohou zveřejnit informace o sobě: jméno, příjmení, datum narození, bydliště, telefonní číslo, e-mail, libovolné informace o své osobě, svých zálibách, oblíbených filmech, seriálech,

hudebních skupinách, nakreslit svou profilovou fotografii, několik fotografií sebe, případně sebe s kamarády či rodinou, při oblíbené činnosti apod.

Žáci poté své profily nalepí na stěnu či připnou na tabuli a každý si může prohlédnout profil ostatních.

Závěrečná diskuze:

Pedagog se žáky diskutuje na příkladech nakreslených profilů o tom, o kterých informacích si myslí, že by měly být zveřejněny a kdo by k nim měl mít přístup (kamarádi, příbuzní, cizí uživatelé sociální sítě). Pedagog se žáků ptá, jestli ví, jakým způsobem si zabezpečit jednotlivé informace na příkladu sociální sítě Facebook. Na dataprojektoru jim ukáže ukázkový speciálně vytvořený profil na této sociální síti a provede je jednoduchým nastavením soukromí.

Může k tomu využít návod projektu E-Bezpečí: Facebook – Základní zabezpečení a ochrana soukromí, dostupný na webových stránkách projektu na adrese: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1822-facebook-zakladni-zabezpeceni-a-ochrana-soukromi

Dle uvážení může pedagog využít také výukové video na Youtube kanálu – Buď safe on-line: https://www.youtube.com/watch?v=O_1ptzkF-oo

3.7. Druhý blok – kyberšikana

Cíl bloku: Seznámení žáků s fenoménem kyberšikany, jejími jednotlivými formami a možnostmi řešení. Za pomoci aktivit postavených na modelových příbězích si žáci mohou vyzkoušet, jak by v dané chvíli reagovali. Pedagog by je měl poté v závěrečné diskuzi poučit o možnostech, jaké mají, pokud se do podobných situací dostanou sami.

Aktivita 1: A co bys udělal ty?

Délka aktivity: 30 min

Pomůcky: počítač s připojením na internet a diaprojektorem

Průběh aktivity:

Pedagog žákům na úvod vysvětlí, jakým tématem se budou na tomto setkání zabývat, tedy kyberšikanou. Na dataprojektoru jim promítne video z profilu uživatele Nová škola dostupné na serveru Youtube: https://www.youtube.com/watch?v=s_5g2fvsjVs&feature=emb_logo

Po zhlédnutí videa učitel moderuje diskuzi a hromadně se ptá žáků, jak by se v této situaci zachovali, pokud by byli spolužáky dětí na videu, podle možností, které jsou uvedeny na konci:

1. Přidám se
2. Pokusím se to zastavit
3. Odmítnu se zapojit

Podle jejich odpovědí se učitel ptát, jak konkrétně by dále postupovali, jaké by bylo dle nich možné řešení situace z pohledu spolužáka a jaké by bylo možné řešení situace z pohledu dívky, která se stala obětí kyberšikany.

Aktivita 2: Příběhy kyberšikany

Délka aktivity: 40 min

Pomůcky: vytisknuté příběhy (příloha 1), papíry A4, psací potřeby – propiska, tužka.

Pedagog rozdělí žáky na tři skupiny a každé skupině rozdá jeden příběh z Přílohy 1, čistý papír A4 a psací potřeby. Poté jim vysvětlí, že si ho ve skupině mají pozorně přečíst a na papír po diskuzi napsat přesný postup toho, jak by v této situaci měl jedinec dotčený kyberšikanou postupovat. Zástupce skupiny poté přečte nahlas příběh a návrh řešení.

Pedagog jim následně promítne přes dataprojektor základní body řešení kyberšikany (příloha 2). Poté hromadně diskutuje s žáky o tom, jak se jejich řešení podobá řešení doporučovanému.

Pedagog se dále ptá jednotlivých skupin, o který druh kyberšikany, uvedených v příloze 3, se v jejich konkrétním příběhu jedná. Vysvětlí jim, jak jednotlivé druhy kyberšikany vypadají a probíhají. V rámci toho jim může pustit výukové video na Youtube kanálu KPBI – Kraje pro bezpečný internet, dostupné na: https://www.youtube.com/watch?v=AwIm8AfWXO8

3.4. Třetí blok – kybergrooming

Cíl bloku: Žáci by se měli seznámit s nebezpečným fenoménem internetového prostředí – kybergroomingem, pomocí projekce filmu V síti a následné diskuze s pedagogem.

Aktivita 1: Promítání filmu V síti

Délka aktivity: délka filmu 63 min + cesta do kina a zpět

Žáci pod vedením učitele navštíví individuálně domluvenou projekci filmu v Síti ve speciální verzi pro mladší diváky v místním kině.

Aktivita 2: Diskuze o filmu a kybergroomingu

Délka aktivity: 30 min

Pomůcky: počítač s dataprojektorem

Průběh aktivity:

Pedagog vede diskuzi s žáky o shlédnutém filmu za pomoci otázek (příloha 3). Může odpovídat na jejich dotazy, ptát se, zda někdo v jejich okolí neprožil něco podobného. Ptá se jich, jaké řešení by podle nich bylo nejvhodnější, pokud se dostanou do podobné situace, jestli ví, koho v takovém případě kontaktovat (rodiče, učitele, linku důvěry, policii). Může

se také prát na to, jestli by žáci poznali sexuálního predátora a jestli ví, co je v případě sexuálního obtěžování trestné (v jejich případě hlavně věk či požadavky predátora).

3.5. Čtvrtý blok – seznamování a hesla

Cíl bloku: V první části se žáci pomocí aktivity pokusí zamyslet na falešnými profily, které skýtají nebezpečí při seznamování. Seznámí se také s možností ověření pravosti fotografií. V druhé části by žáci měli získat povědomí o bezpečném používání hesel v různých internetových službách, účtech, sociálních sítích či internetovém bankovnictví. Měli by se seznámit s častými chybami při volbě a užívání hesel a zásady bezpečnosti při tvorbě hesla.

Aktivita 1: Seznamování

Délka aktivity: 40 min

Pomůcky: počítač s připojením na internet a dataprojektorem, papíry A4, psací potřeby.

Průběh aktivity:

Pedagog rozdělí žáky na tři nebo čtyři zhruba stejně velké skupiny (podle celkového počtu). Každé skupině rozdá psací potřeby a papír A4. Poté je vyzve, aby zkusili vymyslet a napsat na papír několik bodů, podle kterých by poznali falešný profil nebo jak by se na internetu choval člověk, který se chce seznámit a nemá čisté úmysly.

Následně nechá zástupce každé skupiny přečíst body, které vymysleli. Pomocí dataprojektoru promítne seznam bodů z Přílohy 4. Diskutuje s žáky, jestli se někdy setkali s tím, že by je kontaktoval někdo, kdo by se choval takto podezřele. Ptá se, jak by reagovali.

Poté se žáků zeptá, jestli ví, jakým způsobem se dají ověřit obrázky – profilové fotografie, kterými se mohou prezentovat uživatelé na internetu. Ukáže jim na dataprojektoru příklad vyhledávání pomocí služby Google obrázky, kde se vložením obrázku dá zjistit, jestli nejde o fotografii staženou někde z internetu, což je znakem falešného profilu.

Aktivita 2: Hesla

Délka aktivity: 30 min

Pomůcky: počítač **s** dataprojektorem, papíry, psací potřeby, lepící páska či magnety na tabuli k připevnění papírů.

Průběh aktivity:

Nejprve dá pedagog každému žáku malý kus papíru a psací potřeby a vyzve je, aby se pokusili vymyslet co nejsilnější heslo ke svému účtu a napsali ho na papír. Poté všechny papíry připne či nalepí na tabuli a řekne žákům, aby se pokusili zapamatovat si co nejvíce hesel. Po dvou minutách papíry zakryje či sejme a žáci mají za úkol hesla napsat na papír.

Závěrečná diskuze:

Pedagog vede s žáky diskuzi o tom, kdo si zapamatoval kolik hesel a jakým způsobem by měly být zabezpečené uživatelské účty.

Jestliže používají více hesel pro různé účty, vysvětlí jim principy vícestupňového zabezpečení (zabezpečení pomocí hesla a kódu, který při přihlášení přijde jako SMS zpráva na mobilní telefon – typicky používané u přihlašování do internetového bankovnictví).

K diskuzi učitel využije seznam bezpečnostních standardů při tvorbě hesla (Příloha 4), který může promítnout dataprojektorem. Zeptá se žáků, jestli o alespoň některých těchto standardech slyšeli a jestli je využívají.

Na závěr žákům pustí video z kanálu CZNIC na serveru Youtube, shrnující problematiku hesel:
https://www.youtube.com/watch?v=tTFEbY6S58g

3.6. Pátý blok – závěrečné shrnující aktivity

Cíl bloku: Žáci by si pod vedením pedagoga měli utřídit informace, které během všech částí programu načerpali. Měli by se částečně hromadně a částečně ve skupinách zamyslet nad problémem kyberšikany a bezpečnosti internetu, výstupem by měly být zpracované infoletáky, které mohou být umístěny na viditelném místě na nástěnce ve třídě či ve škole.

Aktivita 1: Infoleták o kyberšikaně

Délka aktivity: 20 min

Pomůcky: papír A3, psací potřeby – fixy, lepicí páska či magnety na tabuli k připevnění papírů, vytištěná příloha 2.

Průběh aktivity:

Na papír A3 se žáci pod vedením pedagoga pokusí hromadně vytvořit infoleták o kyberšikaně, který by mohl být umístěn na nástěnce ve třídě či ve škole. Má jít o základní informace o kyberšikaně, které si zapamatovali, případně mají dovoleno využít internet ve svých zařízeních. Důraz je kladen také na grafické zpracování pomocí fixů. Leták mohou doplnit pravidly při setkání s kyberšikanou (příloha 2), tu mohou případně přepsat a také graficky upravit.

Aktivita 2: Infoletáky o druzích kyberšikany

Délka aktivity: 40 min

Pomůcky: papíry A4, psací potřeby – fixy, tužky, lepicí páska či magnety na tabuli k připevnění papírů, vytištěná příloha 3, rozstřižená na malé papírky podle jednotlivých druhů kyberšikany.

Průběh aktivity:

Pedagog žáky rozdělí do čtyř až pěti skupin (záleží na jeho uvážení a počtu žáků), každé skupině dá papír A4, psací potřeby, fixy. Také každé skupině nechá vylosovat jeden z druhů kyberšikany z rozstřižené přílohy 2. Skupiny mají za úkol vypracovat o daném druhu kyberšikany infoleták, který by mohl být umístěn na nástěnku ve třídě či ve škole. Měl by obsahovat základní informace a graficky zpracován, aby mohl být umístěn spolu s letáky ostatních skupin a letáku z aktivity 1 na nástěnku.

Aktivita 3: Pravidla bezpečného internetu

Délka aktivity: 20 min

Pomůcky: papíry A3, psací potřeby – fixy, lepicí páska či magnety na tabuli k připevnění papírů.

Průběh aktivity:

Pedagog může využít rozdělení do skupiny z předchozí aktivity, každé skupině dá papír A3 a fixy a vyzve ji, aby společně diskutovala nad pravidly bezpečného chování na internetu. Měli by se zamyslet nad tématy, která byla probírána během předchozích setkání a sepsat společně na papír pravidla bezpečného chování, která jsou podle nich důležitá. Papír každé skupiny pedagog poté připevní na tabuli.

Závěrečná diskuze:

Probíhá nad sepsanými pravidly. Pomocí dataprojektoru jim promítne příklad možných pravidel bezpečného internetu (Příloha 5 a Příloha 6). Všichni žáci se poté pokusí s pomocí pedagoga vymyslet vlastní desatero pravidel, které fixy napíší na papír A3 a můžou si ho vyvěsit v rámci své třídy či školy na nástěnku spolu s letáky z předchozích aktivit.

Závěr

Záměrem tohoto bakalářského projektu bylo vytvoření programu prevence kyberšikany a bezpečnosti dětí a mládeže na internetu, který je určen pro druhý stupeň základní školy.

Vzhledem k tomu, že preventivních projektů, které podrobně zpracovávají toto téma, existuje celá řada, nebylo v silách autora je nahradit, ale spíše k nim nabídnout jakousi alternativu, která neklade velké požadavky na personální obsazení, přípravu ani náklady.

V souvislosti s těmito projekty je k dispozici značné množství metodik a materiálů, které mohou pedagogové využít. Neucelenost a nepřehlednost ovšem může působit i odrazujícím dojmem zvláště pro ty, kteří nemají v dané oblasti velký přehled či znalosti.

Projekt je proto vytvořen jako ucelený soubor aktivit, uvedených v jednotlivých tematických blocích, které jsou připraveny k okamžité realizaci a může je vést jediný pedagog bez hluboké znalosti tématu.

Jednou z intencí je také podnítit zájem pedagogů o toto téma a motivovat je k vytváření vlastních programů a aktivit v rámci jejich možností a možností zařízení, ve kterých působí.

Seznam literatury

1. Bezpečně v kyberprostoru – Příběhy pro zamyšlení. 2007–2016. JM školy, portál o školství v Jihomoravském kraji [online]. [cit. 27. 4. 2020]. Dostupné z: http://www.jmskoly.cz/bezpecne_v_prostoru/402738bc-3973-11e1-a4fe-18a905489179
2. CZNIC. In: Youtube [online]. 19. 12. 2016. [cit. 6. 5. 2020]. Dostupné z: https://www.youtube.com/watch?v=tTFEbY6S58g
3. ČERNÁ Alena, 2013. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada. 150 s. Psyché. ISBN 978-80-210-6374-7.
4. E-Bezpečí, 2008–2020. Centrum prevence rizikové virtuální komunikace, Pedagogická fakulta Univerzity Palackého v Olomouci[online]. [cit. 7. 5. 2020]. Dostupné z: https://www.e-bezpeci.cz/
5. Internetem Bezpečně, 2018 [online]. [cit. 20. 4. 2020]. Dostupné z: https://www.internetembezpecne.cz/
6. JANOŠOVÁ Pavlína a Pavel ŘÍČAN, 2010. *Jak na šikanu.* Praha: Grada. 160 s. ISBN 978-80-247-2991-6.
7. JANOŠOVÁ Pavlína, Lenka KOLLEROVÁ, Kateřina ZÁBRODSKÁ, Jiří KRESSA a Mária DĚDOVÁ, 2016. *Psychologie školní šikany*. Praha: Grada. 415 s. Psyché. ISBN 978-80-247-2992-3.
8. JIROVSKÝ Václav, 2007. Kybernetická kriminalita. Praha: GradaPublishing. 288 s. ISBN 978-80-247-1561-2.
9. KOPECKÝ Kamil, 2014.*Výzkum rizikového chování českých dětí v prostředí internetu 2014*. Olomouc: Univerzita Palackého. 20 s.
10. KOPECKÝ Kamil, 2015. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Olomouc: Univerzita Palackého v Olomouci. 169 s. ISBN 978-80-244-4861-9.
11. KOPECKÝ Kamil, 2020. *V síti: Za školou – metodická podpora pro pedagogy*. Olomouc: Univerzita Palackého. 21 s.

12. KOPECKÝ Kamil a René, Szotkowski, 2019. *České děti v kybersvětě (výzkumná zpráva)*. Olomouc: Univerzita Palackého. 32 s.
13. KREJČÍ Veronika, 2010. *Kyberšikana – kybernetická šikana (studie)*. Olomouc: Univerzita Palackého. 72 s. ISBN 978-80-254-7791-5.
14. MARTÍNEK Zdeněk, 2015. *Agresivita a kriminalita školní mládeže*. 2., aktualizované a rozšířené vydání. Praha: Grada. 190 s. ISBN 978-80-247-5309-6.
15. MŠMT, 2019. *Národní strategie primární prevence rizikového chování dětí a mládeže na období 2019–2027*. [online][cit. 10. 5. 2020]. Dostupné z: http://www.msmt.cz/uploads/narodni_strategie_primarni_prevence_2019_27.pdf
16. Nová škola. In: Youtube [online]. 26. 05. 2015 [cit. 27. 4. 2020]. Dostupné z: https://www.youtube.com/watch?v=s_5g2fvsjVs&feature=emb_logo
17. O2 – Chytrá škola. *Bezpečné seznamování online–Metodické náměty na výukové aktivity*. [online]. [cit. 10. 5. 2020]. Dostupné z: https://www.o2chytraskola.cz/data/files/internetove-seznamovani-3cg8vrefc6.pdf
18. O2 – Chytrá škola. *Základy bezpečnosti, tvorba hesla– Metodické náměty pro výukové aktivity*[online]. [cit. 7. 5. 2020]. Dostupné z: https://www.o2chytraskola.cz/data/files/v003-o2-bezpecne-heslo-digital-a4-v06-nahled-ooartx2veh.pdf
19. Osobní údaje, osobní informace, 2011–2016. ManagementMania [online]. [cit. 23. 4. 2020]. Dostupné z: https://managementmania.com/cs/osobni-data-personal-data
20. ŠEVČÍKOVÁ Anna, 2014. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: GradaPublishing. 184 s. ISBN 978-80-210-7527-6.

21. ŠMAHAJ Jan, 2014. *Kyberšikana jako společenský problém: Cyberbullying as a socialproblem*. Olomouc: Univerzita Palackého v Olomouci. 232 s. ISBN 978-80-244-4227-3.
22. ZORMANOVÁ Lucie, 2019. Kyberšikana v České republice a v zahraničí. In: *Metodický portál RVP.CZ* [online]. [cit. 7. 5. 2020]. Dostupné z: https://clanky.rvp.cz/clanek/c/Z/22075/kybersikana-v-ceske-republice-a-v-zahranici.html/

Seznam příloh

Příloha 1: Aktivita Příběhy kyberšikany

Příloha 2: Základní pravidla při setkání s kyberšikanou

Příloha 3: Druhy kyberšikany

Příloha 4: Výběr vhodných oblastí pro diskusi s žáky

Příloha 5: Čeho si na profilech všímat

Příloha 6: Bezpečnostní standardy při tvorbě hesla

Příloha 7: Pravidla bezpečného internetu

Příloha 8: Zásady bezpečného používání internetu

Příloha 1

Aktivita Příběhy kyberšikany

Volně upraveno podle webu jmskoly.cz.

První příběh

Čenda, vysoký, štíhlý teenager, výborný v matice a přírodopisu, se cítí trapně, když se má převlíkat do tělocviku v chlapeckých šatnách, protože nemá tak svalnatou postavu jako jeho spolužáci. Ostatní, urostlí spolužáci atletické postavy si všimli Čendovy stydlivosti a rozhodli se toho zneužít. Vyfotili skrytě na jejich mobilní telefony Čendu v momentě, kdy na sobě neměl tričko a spodky. Tyto obrázky pak kolovaly prostřednictvím mobilních telefonů mezi ostatními studenty. Brzy na to kluci i holky z celé školy si na Čendu ukazovali, hihňali se mu a posmívali se, když šel po školní chodbě. Často zaslechl poznámky na jeho osobu jako: „Tady jde Čenda – ptačí hrudník!“, „Poseroutka!“, „Čenda s kuřecíma nohama!“, „Tyčka!“. Tato slova ho hodně zraňovala a to, jak ho spolužáci vnímali, začalo mít vliv na jeho známky v matice i přírodopisu.

Druhý příběh

Hanka je čtvrťačka a na svůj věk je velmi zběhlá v používání internetu. V pondělí jí přišel email od někoho, kdo se nazýval “stalker@hotmail.com.” V emailu bylo napsáno: „Sleduji tě. Měj se na pozoru.“ Hanka to okamžitě smazala a dál na to nemyslela. V úterý jí přišel další email ze stejné adresy, tentokrát v něm bylo napsáno: „Jsem ti čím dál blíž a zrovna teď tě vidím na počítači, jak si to čteš.“ Hanka se začala strachovat, ale nechtěla to říct svým rodičům, protože se domnívala, že jí zakážou chodit na internet. Ve středu již se strachem objevila další email od „stalker@hotmail.com“. Tentokrát v něm stálo: „Boj se. Tento den může být tvým posledním.“ Vyděšená a znepokojená tím co se děje, se

rozhodla, že až se vrátí ze školy, řekne to svým rodičům. Nebyla schopna se soustředit na žádnou z vyučovacích hodin, kterou měli, kvůli obrovskému strachu z toho, co bylo napsáno v tom posledním emailu: „Dnešek může být tvým posledním.“

Třetí příběh

Linda se zrovna přestěhovala z malé vesnice do města a zapsala se tam do místní střední školy. Protože byla velice hezká, veselé povahy a snadno vycházela s ostatními, lehce získala pozornost mnoha chlapců – fotbalistů. To rozzlobilo školní roztleskávačky. Bára, vedoucí roztleskávačka, má obavu, že Linda jí odláká jejího kluka Filipa, který je kapitánem fotbalového družstva. S pomocí ostatních roztleskávaček se Bára rozhodne vytvořit webovou stránku s názvem: „Nesnášíme Lindu“, kde dívky mohou psát důvody, proč Lindu nesnáší a proč si myslí, že by se měla přestěhovat zpátky na vesnici. Brzy skoro celá škola o těchto stránkách ví a mnozí další začnou psát urážlivé texty o Lindě. Linda se zoufale v novém městě snaží najít přátele, ale nedaří se jí to a začne trpět depresí a nedostatkem zájmu o cokoliv mimo pláč v posteli.

Příloha 2

Základní pravidla při setkání s kyberšikanou (Martínek, 2015, s. 179)

Základní pravidla při setkání s kyberšikanou:
1. Okamžité ukončení komunikace s agresorem
2. Nereagování na jeho další pokusy o kontaktování (chat, e-mail, SMS), zablokování uživatele
3. Archivování veškeré komunikace jako zajištění důkazního materiálu
4. Oznámení kyberšikany někomu, komu důvěřuji a kdo mi s řešením může pomoci (rodiče, učitel)
5. Podání trestního oznámení na neznámého pachatele na Policii ČR (za pomoci dospělé osoby)
6. Změna online identity, ať už profilu na sociální síti, změna e-mailové adresy či telefonního čísla (podle prostředků, kterými kyberšikana probíhala)

Příloha 3

Druhy kyberšikany:
Flaming
Kyberstalking
Ostrakizace, vyloučení
Pomlouvání
Bluejacking
Kybergrooming
Flaming
Krádež identity

Příloha 4

Výběr vhodných oblastí pro diskusi s žáky (Kopecký, 2020, s. 15):

1. Bavíte se na internetu také s neznámými lidmi, které jste mimo internet nikdy osobně neviděli? Třeba když hrajete online hry, surfujete po sociálních sítích atd.?
2. S kým se na internetu bavíte – znáte je z reálného světa? Bavili jste se na internetu někdy s dospělým člověkem, jako si to vyzkoušely naše herečky?
3. Jak to probíhalo?
4. Mají vaši internetoví kamarádi přezdívky, nebo používají spíše klasické jméno a příjmení, ať už reálné, nebo vymyšlené? (Pachatelé ve filmu používají často přezdívky či vymyšlená jména).
5. Mají ve svých profilech svou reálnou fotku? Viděli jste se někdy na webové kameře? A používáte vůbec ke komunikaci webku? A jak to probíhá, co ke komunikaci používáte (třeba Skype nebo jinou aplikaci)?
6. Zažili jste někdy podobné situace, které zachycuje film V síti? Víte o někom, kdo podobnou situaci zažil? Chtěl po vás někdo např., abyste nikomu neřekli, že se spolu bavíte? Chtěl po vás na internetu někdo nějaký nevhodný (neslušný, intimní, citlivý) materiál?
7. Jak byste si ověřili identitu člověka, se kterým se bavíte (např. pomocí reverzního vyhledávání fotografií, emailu apod.)?
8. Existují nějaké nástroje, které to umí? (např. Google Obrázky, TinEye.com apod.).
9. Co byste dělali, kdybyste se dostali do podobných situací? Řekli byste to někomu nebo doufali, že problém zmizí?
10. Znáte nějaké internetové linky, které vám mohou pomoci s vašimi problémy? A raději byste při hledání pomoci telefonovali, nebo spíš psali a chatovali?
11. Co konkrétně byste napsali? Co je důležité uvést?

Příloha 5

Čeho si na profilech všímat (podle projektu O2 – Chytrá škola)

1. Profil je většinou založen krátce (zejména na Facebooku je tato okolnost podezřelá). Tuto skutečnost většinou odůvodňují tím, že jim byl účet někým ukraden a museli si založit nový.
2. V přátelích se vyskytují jen přátelé jednoho pohlaví a věku (například dívky okolo patnácti let).
3. V popiscích jsou dvojsmyslné údaje nebo výzvy, kterými mohou být nabídky na flirt, sex nebo jeho virtuální podobu. Velice časté jsou i výzvy na seznámení v konkrétní věkové hranici: „Hledám kluka 11–12 na pokec.“ Takové selektování děti vůbec nedělají. Pokud se chtějí bavit, je jim jedno s kým, tedy pokud se nepřihlásí někdo věkově srovnatelný s rodiči.
4. Fotografie na profilu jsou dokonalé, vyumělkované a jsou z jedné série. Málokdy na nich uvidíte fotky z běžného života s českým prostředím. Všímejte si, co je na pozadí fotek. Určitě nevěřte fotografii, na které jsou v pozadí např. kulaté kliky, které se u nás nevyskytují.
5. Profil se jmenuje divně. Málokterá slečna by si na internetu dala přezdívku Nymfa007 nebo Nadrzena.karolinka, takové přezdívky si dívky opravdu nedávají. Stejně tak jsou podezřelé profily, které se jmenují Jana Nová, Petra Malá, Katka Spokojená apod. Je dobré si jméno profilu, e-mail nebo další údaj z profilu dohledat na internetu. Můžete se tak dozvědět spousty zajímavých věcí.
6. Kontakt se vyhýbá audiovizuálnímu spojení. Pokud budete chtít zaslat nové fotografie nebo si promluvit na Skypu, vždycky si najde nějakou výmluvu, proč to nejde.
7. U sofistikovaných útočníků jsou prvky manipulace a přesvědčování na takové úrovni, že je velice obtížné i pro specialisty takový profil odhalit. To ale neznamená, že je nejde v případě šetření dohledat a identifikovat.

Příloha 6

Bezpečnostní standardy při tvorbě hesla (podle projektu O2 – Chytrá škola)

Bezpečnostní standardy při tvorbě hesla:
1. **Ideální heslo by mělo být dlouhé minimálně 8 znaků.**
2. **Při tvorbě hesla používejte číslice, velká i malá písmena abecedy a speciální znaky.**
3. **Nikdy nepoužívejte heslo, které lze najít ve slovníku! Rovněž nepoužívejte křestní jména ani příjmení.**
4. **Pro přístup k různým online službám (e-mail, sociální sítě) nepoužívejte stejné heslo.**
5. **Po ukončení práce v prostředí internetu se nezapomeňte odhlásit z účtu, který právě používáte. Zavření prohlížeče vás z účtu neodhlásí!**
6. **Heslo uchovejte v tajnosti, nikomu jej neprozrazujte, ani svému nejlepšímu kamarádovi.**
7. **Důležité účty zabezpečte dvojfázovým (dvojúrovňovým) ověřováním, které kombinuje heslo a kód na mobilním telefonu.**

Příloha 7

Pravidla bezpečného internetu (Byrtusová, 2013 cit. podle Zormanová, 2019)

Pravidla bezpečného internetu

1. **Nedávej nikomu adresu ani telefon. Nevíš, kdo se skrývá za monitorem.**
2. **Neposílej nikomu, koho neznáš, svou fotografii, a už vůbec ne intimní.**
3. **Udržuj hesla k e-mailu i jinam v tajnosti, nesděluj je ani blízkému kamarádovi.**
4. **Nikdy neodpovídej na neslušné, hrubé nebo vulgární maily a vzkazy.**
5. **Nedomlouvej si schůzku na internetu, aniž bys o tom řekl někomu jinému.**
6. **Pokud narazíš na obrázek, video nebo e-mail, který tě šokuje, opusť webovou stránku.**
7. **Svěř se dospělému, pokud tě stránky uvedou do rozpaků nebo vyděsí.**
8. **Nedej šanci virům. Neotvírej přílohu zprávy, která přišla z neznámé adresy.**
9. **Nevěř každé informaci, kterou na internetu získáš.**
10. **Když se s někým nechceš bavit, nebav se.**
11. **Nevhodné příspěvky, komentáře či uživatele vystupující nevhodným způsobem nahlas.**
12. **Uživatele, který nerespektuje pravidla virtuální komunikace, ignoruj nebo zablokuj.**

Příloha 8

Zásady bezpečného používání internetu

1. Připojovat se na internet jen z důvěryhodného zdroje. Při připojení na veřejné wifi síti nikdy nezadávat hesla.
2. Udržovat aktualizovaný počítač (operační systém, internetový prohlížeč, antivirový program).
3. Instalovat programy jen z důvěryhodného zdroje.
4. Nastavení automatického zamykání počítače a telefonu při delší nečinnosti.
5. Používání silných a bezpečných hesel – nikomu je nesdělovat, ani nikam nepsat.
6. Kontrola zabezpečení a sdílení na sociálních sítích (Facebook, ...)
7. Ověřovat informace, které se objevují na internetu, ve více zdrojích.
8. Číst si podmínky používání služeb a aplikací, nezadávat bezmyšlenkovitě souhlas.
9. Chránit své osobní údaje (adresu, datum narození, telefonní číslo, e-mail, doklady).
10. Neotvírat nedůvěryhodné e-maily, neklikat na odkazy a neotvírat přílohy.