Zdravotně
sociální fakulta
Faculty of Health
and Social Sciences

Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

Kyberšikana

Renata Švestková

Ladislav Soldán

Martin Řehka

České Budějovice 2019

KYBERŠIKANA

Renata Švestková, Ladislav Soldán, Martin Řehka

Poděkování:
1. základní škola T. G. Masaryka, Milevsko
Soukromá základní škola a mateřská škola Viva Bambini, České Budějovice
Základní škola a Mateřská škola, Olešník
Základní škola F. L. Čelakovského, Strakonice
Základní škola Pohůrecká, České Budějovice
Základní škola Považská, Strakonice
Bc. Linda Valášková, studentka ZSF JU
Zuzana Straková, Ing. Eva Ježková, Ediční a distribuční činnost ZSF JU

Financováno v rámci projektu MZ ČR s názvem „Prevence kyberšikany a ochrana dětí před on-line hrozbami“ (č. 10/2019/K).

Recenzent:
doc. MgA. Stanislav Suda, Ph.D.

ISBN 978-80-7394-752-1

Obsah

Úvod

Vážení třídní učitelé, školní metodici prevence a Vy všichni, kteří se zamýšlíte nad tím, jak správně postupovat při kyberšikaně.

Prvním krokem, který musíme udělat při řešení kyberšikany, je projevit zájem o ochotu podílet se na řešení dané situace a následně podpořit oběť, aby věděla, že se na Vás může v každém případě spolehnout. Pokud tuto podmínku hned na začátku nesplníte, bude téměř nereálné danou situaci vyřešit.

Tato příručka je sestavena tak, aby byla přehledná a dovedla Vás ke správnému řešení dané situace. V úvodu publikace se dozvíte, že je nutné ověřit si, zda se opravdu jedná o kybernetickou šikanu. Můžete také porovnat, zda se jedná o kombinaci šikany a kyberšikany. Dále se dočtete, jak správně pracovat s dítětem, které se stalo obětí, a naopak které je kybernetickým agresorem. Je důležité si uvědomit, že musíme pracovat s oběma stranami dané situace. Správný postup a řešení kyberšikany si žádá individuální časový plán a je nutné, aby se zapojilo do řešení co nejvíce důvěrných osob, ale zároveň co nejméně osob, které by mohly situaci spíše zhoršit. Řešení kyberšikany vyžaduje týmovou práci všech zúčastněných, a to ve všech ohledech a za každých okolností.

Hlavní věcí, kterou si musíme uvědomit, je to, že když danou situaci začneme řešit, je to již první krok k úspěchu! Když si kybernetická oběť uvědomí, že EXISTUJE osoba, která chce a zároveň dokáže pomoci, pochopit ji a podpořit, je to významný začátek správného řešení kyberšikany. Svým zájmem dokážete zmírnit následky anebo jim zcela zamezit, neboť mohou oběť provázet celý život.

Přejeme Vám, abyste tuto příručku nemuseli nikdy použít a kyberšikanu řešit, a pokud ji řešit budete, věříme, že Vám v rozhodování jak postupovat pomůže právě tato publikace.

Renata Švestková
Ladislav Soldán
Martin Řehka

1 Kyberšikana

Kyberšikanu definujeme jako trýznění, hrozby, obtěžování, ponižování, ztrapňování nebo jiné útoky prostřednictvím internetu, interaktivních a digitálních technologií nebo mobilních telefonů (Krejčí, 2010).

Kyberšikanu popisují Kowalski a Limber (2007) jako elektronickou šikanu prostřednictvím mobilních telefonů (SMS zpráv), e-mailů, rychlých zpráv (Messenger), chatu nebo dalších jiných webových stránek – vysílání škodlivých slov nebo fotografií jednotlivce.

Hlavním cílem při útoku agresorem je zejména ublížit, zesměšnit za použití elektronických komunikačních médií. Je to úmyslné, nepřátelské chování, které se může opakovat, a jednotlivec nebo skupina agresorů ubližuje takovým způsobem, že se oběť nemůže účinně bránit.

Kyberšikana jako taková je zkoumána přibližně od začátku nového tisíciletí, intenzivní pozornost jí tedy začala být věnována nedávno. Kyberšikana je závažný jev, který si zajisté zasluhuje pozornost a adekvátní řešení (Buřičová Kadlecová, 2010).

Prvotním znakem kyberšikany je jednorázové, dlouhodobé či se stupňující a hlavně úmyslné užívání psychického šikanování proti jednotlivci nebo skupině za pomoci nejrůznějších moderních informačních a komunikačních technologií. Útočníkem může být téměř kdokoli, a tak jej nelze jednoznačně identifikovat jako u případů klasické jednotvárné šikany. Agresorem může být i taková osoba, která byla v minulosti obětí šikany. Většinou není pravidlem psychická ani fyzická převaha. Proto z těchto důvodů bývá bohužel také mnohem složitější následné dopadení agresora příslušným orgánem státu. Cílem kyberšikany je ublížit nebo ubližovat někomu nejen fyzicky, ale hlavně po stránce psychic-

ké. Kyberšikana dokonce začíná v mnoha případech jako šikana a končí formou kyberšikany, kde agresor využije různých technologií pro šíření fotek, videí a zastrašení prostřednictvím informačních technologií – internetu či mobilního telefonu (Rogers, 2011).

Jedním z nejdůležitějších znaků kyberšikany je anonymní jednání, agresor má strach, že se někdo dozví jeho identitu. Toto chování je protizákonné a hrozí za ně trest odnětí svobody, to ale neznamená, že pokud agresor jedná na internetu pod cizím jménem nebo nějakým nickem (přezdívkou), nemůžeme najít jeho pravé jméno například pomocí IP adresy. Dnešní doba je již natolik vyspělá, že lze najít opravdu vše a za poměrně krátkou dobu (Černá a kol., 2013).

Formy kyberšikany můžeme v podstatě rozdělit do dvou oblastí:

- První oblastí jsou jednotlivé projevy kyberšikany, tedy konkrétní způsoby, jakými k agresivnímu chování dochází.
- Druhou oblastí pak jsou místa na internetu či v mobilním telefonu, kde ke kyberšikaně dochází, což souvisí s prostředky použitými k její realizaci.

Jedním z nejčastějších důvodů pro kyberšikanu je odplata, oběti tradiční šikany mohou hledat způsob, jak se agresorovi z off-line reality pomstít způsobem, který zajistí anonymitu, čímž znemožní další odplatu ze strany agresora (Buřičová Kadlecová, 2010).

1.1 Rozdíly mezi kyberšikanou a šikanou

Kyberšikana se odehrává ve virtuálním světě. Tak jako se liší virtuální svět od světa reálného, liší se i kyberšikana od klasické šikany. Jak kyberšikana, tak i šikana mají svá specifika (Černá a kol., 2013).

Rozdíly mezi kyberšikanou a šikanou jsou následující:

Agresor
Šikana se odehrává v přímém kontaktu mezi osobami. Naopak při kyberšikaně se útok odehrává většinou anonymně a agresor má od svých

obětí zřejmý odstup. Tento odstup mu mylně zaručuje bezpečí, zejména v tom, že na něj nikdo nemůže přijít. Jelikož agresor nevidí způsobené škody, lehce zapomene na to, co spáchal. Kybernetickým agresorem může být každý, kdo má potřebné znalosti s informačními a komunikačními médii, která jsou všude kolem nás ve velké míře. Kyberagresor tedy může být i fyzicky velmi slabý jedinec, který páchá odplatu za šikanu, se kterou se dříve setkat jako oběť.

Místo a čas

Velmi důležitá odlišnost je to, že kyberšikana se může odvíjet v jakémkoliv čase a v kterémkoliv prostředí. Agresor k útoku používá internetová, komunikační a informační média, k nimž je přístup v dnešní době téměř odkudkoli. Toto zjištění přispívá k psychickému týrání oběti, jelikož útoky mohou přijít kdykoliv a opakovaně, na rozdíl od šikany, která se odehrává například každý den ve stejný čas a na stejném místě. Jako příklad můžeme uvést cestu do školy, přestávky atd.

Oběť

V tomto neskutečném světě nezáleží na věku, pohlaví, síle ani na úspěšnosti útočníka nebo oběti ve společnosti. Původcem kyberšikany může být každý, kdo má potřebné znalosti informačních a komunikačních technologií, tedy i fyzicky slabý jedinec. Z výzkumů vyplývá, že oběti tradiční šikany se často stávají také oběťmi kyberšikany, která je v této souvislosti posunem šikany o krok výše. Výzkumy také uvádějí, že oběti kyberšikany tráví více času na internetu, bývají obvykle málo obeznámeny s riziky spojenými se zneužitím ICT, proto se na internetu chovají méně opatrně.

Ve virtuální neboli internetové realitě nezáleží na pohlaví, věku ani na fyzické síle jedince. Obětí kyberšikany se může stát doslova každý z nás. Nejedná se pouze o specifickou skupinu lidí, ale potkat se s ní můžeme všude.

Obětí kyberšikany se může stát například agresor klasické šikany, role agresora a oběti se vymění a ze školní šikany se stane kyberšikana ve virtuální realitě (kyberprostoru), kde se oběť školní šikany (tedy většinou méně fyzicky zdatná osoba) nebo přihlížející mstí. Dalším příkladem oběti kyberšikany je osoba, která funguje v kolektivu naprosto bez problémů, má přátele, pozitivní postavení v sociální skupině, ale

ve virtuálním světě se stane zranitelnou, agresor nalezne zveřejněné informace o osobě a zneužije je zcela bezdůvodně v její neprospěch. Při šikaně ve škole i na internetu si agresor může vybrat osobu zranitelnou na první pohled. Této skupině obětí se říká pasivní oběti. Jedná se o osoby, které jsou fyzicky méně zdatné, málo asertivní, neoblíbené v kolektivu, nevyhledávají společnost, špatně zapadají do kolektivu a obtížně prosazují své názory, mají strach z komunikace. Poslední skupinu tvoří provokatéři, kteří vyvolávají agresi v agresivním jedinci. Jednou z charakteristik může být hyperaktivní, často až velmi impulzivní chování a také agresivita (Černá a kol., 2013).

Sekundární útočníci

Primární prostředky, které agresor využívá k tomu, aby ublížil oběti, se velmi dobře a jednoduše šíří ve virtuální realitě pomocí různých aplikací, komunikačních prostředků na internetu nebo také mobilním telefonem. Nejčastěji jsou to tedy různé fotografie, videa a zvukové nahrávky. Kyberšikana je specifická tím, že se odehrává před velkým publikem uživatelů sociálních sítí. Útočník nemusí oběť napadat opakovaně, ale bohužel stačí, když si jeden uživatel fotku uloží a pošle nebo ji bude sdílet dál.

Tomuto jevu říkáme sekundární útočníci, mohou to být diváci a šiřitelé. I ti se sekundárně podílejí na kyberšikaně. Toto internetové publikum pak velmi účinně zvyšuje intenzitu kybernetického útoku a zhoršuje tak jeho dopad na oběť.

1.2 Slovník pojmů a kyberslang

V dnešní době je v online komunikaci časté používání zkratek a emotikonů. Ty společně vytvářejí „svůj vlastní jazyk“, který je pro dospělé nesrozumitelný. Může nám ale přitom mnohé napovědět. Uveďme si nejčastější internetové zkratky, se kterými se můžeme setkat. Zkratky vycházejí převážně z angličtiny, uvedeme tedy i český překlad:

Zkratka	Anglický význam	Český překlad
143	I love you	Miluju tě
53X	Sex	Sex
AIR/PIR	Adult in room/Parent in room	Dospělý v místnosti/Rodič v místnosti
ASAP	As soon as possible	Co nejdříve
ASL	Age, sex, location	Věk, pohlaví, bydliště
ASLP	Age, sex, location, picture	Věk, pohlaví, bydliště, fotografie
BFF	Best friend forever	Nejvíc největší kamarád(ka)
BOB	Back off bastard	Nepleť se do toho, haj*le
BRB	Be right back	Hned jsem zpátky
BTW	By the way	Mimochodem
CD9	Code nine, parents around	Kód 9, rodiče se blíží
DIAF	Die in a fire	Zhebni v ohni
DM	Direct message	Přímá zpráva
DMMGH	Don't make me get hostile	Nedělej si ze mě nepřítele
EOM	End of message	Konec zprávy
FOAD	F*ck off and die!	Jdi do p*dele a chcípni!
FYI	For your information	Pro tvou informaci
GAL	Get a life	Vzpamatuj se
GEEZ	Geez(us)	Ježíši!
GNOC	Get naked on camera	Svlékni se před kamerou
IRL	In real life	Ve skutečnosti
KPC	Keeping parents clueless	Udržet rodiče v nevědomosti
LMIRL	Let's meet in real life	Pojď se potkat osobně, „naživo“
LOL	Laughing out loud	Směju se nahlas
NOOB	Newbie	Nováček, člověk bez zkušeností
PAW	Parents are watching	Rodiče se dívají
POS	Parents over shoulder	Rodiče mi koukají přes rameno
ROFL	Rolling on the floor laughing	Válím se smíchy po zemi
SUGARPIC	Suggestive or erotic photo of self	Vlastní lechtivá/erotická fotka
SUP	What's up	Jak to jde
TAW	Teachers are watching	Učitelé se dívají
UMFRIEND	„Intimate“ partners	Důvěrný/intimní partner
ZERG	To gang up on someone	Paktovat/spolčit se s někým

Zdroj: Symantec (2017)

Zkratek je ještě mnohem více a neustále vznikají nové. Význam dalších zkratek je možné nalézt na webu www.zkratky.cz nebo vyhledáním zkratky na Googlu.

Dobré je znát také některé další pojmy, které se v internetové komunikaci používají, např.:

- **BUTTER FACE** – označení pro ženy a dívky, které jsou krásné, až na jejich obličej.
- **BYE FELICIA** – pohrdavé sdělení osobě, které chcete naznačit, že má odejít.
- **NETIQUETTE** – Network etiquette, nepsaná etiketa na dané síti, kterou skupina dodržuje.

1.3 Projevy kyberšikany

Primárně se jedná o sdílené fotky a videa šířící se obrovskou rychlostí na sociálních sítích. Mezi nejznámější řadíme: Instagram, Facebook, Twitter a další sociální sítě, kam se přihlásí miliony uživatelů denně. Tyto stránky využívají ve velké většině mladiství a děti, každý sdílený obsah, informace mohou uživatelé dále předat, poslat dalším osobám. Velký problém je ten, že je kyberšikana těžko zjistitelná rodiči nebo učiteli (Černá a kol., 2013).

Dítě nevykazuje žádné viditelné znaky násilí jako u šikany fyzické. V některých případech si útočník ani nemusí uvědomit, že se jeho chování považuje za kyberšikanu, protože stačí totiž opakovaně, úmyslně a bez rozvážení zasílat a zveřejňovat obsah, který je zveřejněn především bez souhlasu majitele. Útočník si může myslet, že se jedná o pouhý a opakovaný vtip z jeho strany a poškození se může, ale nemusí, opakovat, následky však mohou být velmi razantní (Rogers, 2011).

U kyberšikany je někdy velmi obtížné: *(Kopecký, Szotkowski, 2013)*

a) zajistit rychlou ochranu oběti (odstranit profil jedince, na kterém ke kyberšikaně dochází, zajistit odstranění kybernetických materiálů z internetu, zejména sociálních sítí, a zastavit tak další šíření kyberšikany na internetu);

b) **zajistit dostatečný počet svědků** (u kyberšikany často chybí svědci, publikum sice je značně anonymní a nelze identifikovat, kdo o kyberšikaně má jakékoliv informace);
c) **vystopovat útočníka** (u tradiční fyzické šikany útočníka známe, u kyberšikany však útočník často vystupuje pouze pod přezdívkou, využívá anonymitu – falešné profily a účty na sociálních sítích);
d) **rozpoznat, kdy jde o kyberšikanu a kdy ne** (žáci mezi sebou často nevhodně vtipkují a nerozpoznají hranice kyberšikany, nevědí, jak se s ní vypořádat, koho kontaktovat, jak postupovat, jaké kroky podniknout).

1.4 Typy agresorů

Typy agresorů jsou stupňovány jednotlivě dle závažnosti: *(Kavalír, 2009)*

a) **Vtipálek** – kyberagresor, který na základě nepovedené a neúměrné legrace zakládá a upravuje prostředky (fotky, videa) svých kamarádů či spolužáků, ale neuvědomí si, že to může danému člověku po psychické stránce velmi ublížit.
b) **Neúmyslný kyberagresor** – často má skrytou identitu, působí jako velmi silný jedinec, je to tím, že jedná ve velkém vzteku a bez přemýšlení nad následky. Když je pak tento kyberagresor obviněn, bývá velmi často překvapen, protože si své neprávní jednání ani sám neuvědomuje.
c) **Pomstychtivý andílek** – typ agresora, který má velmi dobré zkušenosti s kyberšikanou, on sám nebo někdo z jeho blízkých se stal obětí kyberšikany, tímto způsobem se člověk mstí a kompenzuje si svůj komplex. Má pocit, že to, co dělá, je účelné a správné.
d) **Sprostá holka** – v nejčastějším případě jde o děvče, které nemá velkou škálu zájmů a koníčků, tímto způsobem si hledá zábavu, důvodem jejího konání (kyberagrese) je získání publika za účelem vysoké popularity mezi vrstevníky. Agresor se od tohoto činu oddálí ve chvíli, kdy začne opadat pozornost a zájem daného publika.
e) **Bažící po moci** – tento typ znázorňuje nejzávažnějšího kyberagresora, jedná se o kyberagresora, který se snaží ovládat oběti prostřednictvím strachu a beznaděje. Kyberagresor dává najevo svoji autori-

tu, sílu a nebojácnost. Velmi často vyžaduje, aby ostatní dělali to, co on sám chce. Potřebuje své publikum s cílem někomu se předvést a dokázat, že je silný.

1.5 Charakteristické rysy kyberšikany

Mezi charakteristické rysy kyberšikany řadíme:

a) **Anonymní chování**
Útočník má skrytou svou pravou identitu pod falešným profilem (nickem). Žádným problémem pro agresora není ani změna identity. Pro oběť je ale nemožné dohledat původ skutečného pachatele, kterého může, ale také nemusí ve skutečnosti znát osobně (Rottová, 2009).

b) **V kterémkoliv čase**
Kyberagresor se především fyzicky nenachází na tomtéž místě jako oběť. Útoky mohou tedy nastat kdykoliv – ve dne či v noci. Na rozdíl od klasické šikany nelze předpokládat, kdy a kde dojde k útoku (např. ve škole, na hřišti nebo doma). Přičemž kyberšikana se může odehrávat v kterýkoli čas a na jakémkoli místě, dokonce i pouze za přítomnosti technologií a skrze internetové připojení (Vágnerová, 2004).

c) **Profil útočníka a oběti**
Ve virtuální realitě nezáleží na tom, kolik je nám let, jaké máme pohlaví, jak jsme fyzicky zdatní a také jaké máme sociální postavení ve skupině (partě či ve třídě), ani na tom, jak moc je útočník nebo oběť ve společnosti úspěšný. Tvůrcem kyberšikany se může stát každý, kdo má znalosti v informačních a komunikačních technologiích, tudíž i fyzicky slabý člověk (Hartlová, Hartl, 2010).

d) **Ve virtuálním prostředí se lidé chovají jinak než ve skutečné realitě**
Kyberagresoři mohou ve virtuální realitě uvádět odlišný věk, jiné pohlaví a povolání s úmyslem ovlivňovat ty jedince, se kterými v danou chvíli komunikují přes internet. Jedinci se ve virtuálním světě chovají méně opatrně než ve světě reálném (jsou odvážnější v různorodé komunikaci – probírají soukromá témata a často komunikují bez zábran a bez domýšlení následků. Velmi často zkoušejí i to, co se v realitě neodváží uskutečnit – nejčastěji vyhrožovat a vydírat jiné

osoby). Ve světě internetu je pak velmi snadné poznat někoho, komunikovat s ním, o čem budu chtít a jak dlouho budu chtít. Z nevydařených reálných vztahů (partnerských či přátelských) si pak jedinec může své neúspěchy kompenzovat právě na internetu. Jedinec se tak začleňuje k rizikové skupině, ze které se ve většině případů stávají oběti kyberšikany (Rottová, 2009).

e) **Pobavení pro široké okolí a velké množství lidí, kteří využívají internet**

Internetový prostor umožňuje přístup velkému množství uživatelů. Ti mohou být pouhými diváky nebo se mohou přidat na stranu agresora. Na základě celosvětové virtuální sítě (např. Facebook) vzniká obrovské publikum, do kterého může patřit kdokoliv, kdo je uživatelem konkrétní internetové stránky. Nástroje kyberšikany, kterými jsou např. fotky, videa, zprávy, lze velmi snadno dále rozesílat mezi další uživatele. Často oběť nemusí být útočníkem ani opakovaně napadána. Stačí, když publikuje v internetovém prostoru citlivé informace nebo jiná média. Ostatní uživatelé internetu se poté postarají o jejich další rozšíření. Takzvané virtuální „publikum" dále umožňuje zvyšovat sílu útoku a zhoršovat jeho následky (Vágnerová, 2004).

f) **Obtížná kontrola a rychlé šíření ve virtuální realitě**

Jednotlivé impulzy kyberšikany šířené prostřednictvím informačních technologií se velmi obtížně monitorují. K odhalení hrozícího nebezpečí je zapotřebí více času. Oběť je vystavena opakovanému tlaku a strachu z hrozby neustále se opakujících útoků ze strany agresora. Nejčastěji se jedná o zasílání urážejících zpráv na sociálních sítích nebo mobilním telefonem formou SMS. Uživatelé, kteří jsou zrovna on-line, mohou k těmto příspěvkům přidávat vlastní komentáře, a tak je dále šířit ve svém profilu svým přátelům. Oběť kyberšikany je tak pod velkým drobnohledem vysokého počtu osob (Rottová, 2009).

g) **Kyberšikana může být způsobena i neúmyslně**

Jako oběť kyberšikany se může v podstatě ocitnout každý, ať už je to úmyslně, či neúmyslně. Výsledkem kybernetické šikany může být to, že nesprávně vyhodnotíme situaci nebo také individuální reakci člověka. Neuvědomíme si, že takovýto „vtip" může způsobit psychickou bolest, která může mít na jednotlivce zdravotní i psychický dopad (Hartlová, Hartl, 2010).

h) Důsledky kyberšikany na oběť není snadné rozeznat

Kybernetická šikana je spojena s psychickým týráním obětí, které není na první pohled jednoduché rozpoznat (na rozdíl od modřin, které jsou typickým znakem klasické šikany). Oběťmi kyberšikany se často stávají osoby, které jsou introvertní, nekomunikují s okolním světem o svých problémech. Oběti pak zůstávají často samy na řešení svých problémů, což ve velké míře vede k nezvládnutí situace jedince (Kolář, 2011).

1.6 Způsoby a typy kyberútoků

Kyberšikana má mnoho způsobů, jak oběti ublížit, většinou se jedná o krádež osobních údajů z počítače, další formou může být zasílání agresivních, urážlivých a obtěžujících e-mailů a SMS (tzv. spam). Mohou obsahovat různé vulgární, výhružné zprávy, vtipy a slogany na určitou osobu s cílem ji zesměšnit a ublížit jí.

Agresor může také vytvářet webové stránky a na nich zveřejňovat urážející obsah týkající se jedné nebo více osob, a to bez ohledu na to, jestli oběť zná. Dítě tyto poskytnuté informace mohou zesměšňovat, přitom si je může denně prohlédnout velké množství uživatelů internetu, velmi častou formou je útok na sociálních komunitních webech či diskusích, neobvyklé není ani to, když útočník sám pořídí fotografii nebo video svým mobilním telefonem a zveřejní soubor na internetu. Je jen otázkou času, kdy se tyto soubory dostanou k dalším uživatelům/osobám internetu, například dalším spolužákům ze třídy nebo třeba rodičům a učitelům. Oběť si pak může připadat méněcenná, jde o narušení osobní svobody člověka. Kyberšikana se odehrává bez přímého kontaktu v kyberprostoru (virtuálním světě), často mimo školní prostředí (Říčan, Janošová, 2010).

Lze rozlišit dva základní typy útoků, a to nepřímé a přímé. Autoři zmiňují, že v případě nepřímých útoků (útok v zastoupení) vykonává kyberšikanu za agresora někdo jiný, často se nevědomě stává komplicem.

Agresor například krade oběti heslo, nabourává se do účtu oběti nebo si zakládá účet pod identitou oběti (Kožíšek, Písecký, 2016).

Nejčastější jsou útoky přímé, kterých je celá řada:

Blogování – je zveřejňování intimních informací nebo pomlouvání prostřednictvím blogu. Informace nemusí být pravdivé (Martínek, 2015).

Bluejacking – tento pojem znamená zasílání nevyžádaných zpráv pomocí funkce Bluetooth ve formě obrázků na mobilní telefon. Přijímající jedinec nemůže zjistit, od koho zpráva pochází (Martínek, 2015).

Catfishing – tímto termínem označujeme situaci, kdy nějaká osoba ukradne dětem či dospělým jejich data, nejčastěji ve formě fotografií, nebo jiné údaje, díky kterým může vytvořit věrohodnou, avšak falešnou identitu na síti. Člověka, který chce záměrně skrývat svou identitu, označujeme právě jako catfish. Útočník prochází jednotlivé profily lidí a hledá veřejně dostupné informace, data a fotografie. V mnoha případech je velmi těžké rozklíčovat motiv takového jednání, nicméně existence více profilů, z nichž některé publikují nevhodné informace, poškozuje dobré jméno a reputaci oběti (Dočekal, Eckertová, 2013).

Cyberstalking – je elektronickou verzí celkem známého stalkingu. Ten označuje dlouhodobé, opakované a často stupňované pronásledování a obtěžování oběti, v případě kyberstalkingu elektronickou formou pomocí moderních technologií. Obsahuje mimo jiné např. výhrůžky, obtěžující zprávy, zahlcování telefonu neustálými zprávami apod. Patří sem ale i monitorování počítače nebo telefonu. Hrozba stalkingu je naplněna v případě, kdy útočník aktivit nenechá ani po důrazném ohrazení se ze strany jeho oběti. Míra nebezpečí spočívá také v reálné možnosti, že kyberstalking přejde z elektronické podoby do reálného prostředí (Dočekal, Eckertová, 2013).

Dissing (event. Trickery) – šikanující jsou často (a bohužel) původně dobrými přáteli svých obětí. V určitou chvíli však útočník zneužije citlivé a přátelsky předané důvěrné informace, které zveřejní, a poškodí tak pověst své oběti, případně jí zničí přátelství s jinými osobami. Kromě informací se může jednat o důvěrně předané fotografie nebo videa. Častým případem je zveřejnění intimních fotografií po ukončení partnerského vztahu, kdy se jeden z partnerů mstí nebo se snaží druhého vydírat a přimět k návratu (Dočekal, Eckertová, 2013).

Exclusion – jedná se o úmyslné, často kruté vyloučení osoby ze sociální skupiny. Dítě může být takto vyčleněno a „vyhozeno“ např. z party

kamarádů, ze skupiny na internetu, z probíhající akce/oslavy. On-line forma může být i mírnější, skupina si domlouvá oslavu/setkání a on-line označují všechny děti, kromě jednoho, které se tím pak cítí vyloučené. Vyloučení může probíhat ale i tím, že např. vzhledem ke slabší sociální vrstvě dítě nemá přístup k technice a internetu, nemá možnost využívat stejné technologické možnosti jako jeho vrstevníci, nemá chytrý telefon a jeho vyloučení je tak dáno pouze tímto faktorem.

Fake profile – stejně jako v bodu níže (Fraping) se jedná o vytváření falešných profilů. Ty jsou vytvářeny za účelem skrytí pravé identity útočníka a obsahují smyšlené nebo zkreslené informace. Záměrem je využít tento profil k útoku na oběť bez odhalení vlastní osoby. Může však probíhat i jinak než vytvořením falešného profilu, útočník může využít jiné zařízení, notebook nebo telefon, aby vše vypadalo, že hrozby odesílá jiná osoba. Útočník má strach z odhalení, proto hledá různé metody pro své vlastní krytí. To ale zároveň značí, že se pravděpodobně bude jednat o někoho, koho oběť dobře zná (Dočekal, Eckertová, 2013).

Fraping – útočník záměrně na sociální síti vytvoří falešnou stránku pod jménem své oběti, která vypadá podobně jako originál, tam pak publikuje soukromé, citlivé, zahanbující nebo nepravdivé informace o své oběti. Tato forma je nebezpečná tím, že napadený má malé šance se bránit, často nemůže na příspěvky reagovat a uvést je na pravou míru, nemůže profil smazat a zveřejněné informace poškozují jeho osobu formou pomluvy. Míra nebezpečnosti je dána také tím, že si druhá strana neuvědomuje závažnost svého chování a považuje je za vtipné a neškodné (Dočekal, Eckertová, 2013).

Happyslapping – v překladu to znamená „veselé fackování". Podstatou je nečekaně fyzicky napadnout mladistvého nebo dospělého jedince, přičemž komplic agresora celou událost nahrává na mobilní telefon nebo na kameru. Poté získané video umístí na internet (nejčastěji na sociální síť), kde je určeno, aby pobavilo publikum. Obětí se může stát prakticky kdokoliv a kdekoliv (Martínek, 2015).

Harassment – neustálá a záměrná forma šikany založená na odesílání vulgárních, urážlivých a obtěžujících zpráv. Je to jedna z nejnebezpečnějších forem šikany, která může mít zásadní dopad na kvalitu života dítěte, v krajních případech končí psychickými poruchami, psychickými

následky v dospělosti nebo pokusy o sebevraždu. Útočníkovy zprávy jsou vždy zlé, zákeřné, napadají úctu a sebevědomí oběti a vyvolávají neustálý pocit strachu. Útočník vyvíjí extrémní úsilí, aby oběť zastrašil, aby způsobil co největší bolest, neustává v nátlaku ani ve frekvenci rozesílání a nedopřeje tak své oběti oddechu od tohoto obtěžování.

Internetové hlasování – agresor na internet umístí urážející otázku, která má za účel zesměšnit nebo zastrašit jedince. Publikum poté hlasuje a zapojuje se tím, že vybírá možnost odpovědi (Martínek, 2015).

Internetové soutěžení – jedná se o to, že jedinec nominuje dalšího jedince, který má za úkol udělat nějakou činnost, natočit se při tom, poté video umístit na sociální síť a nominovat dalšího člověka (Martínek, 2015).

Kyberbullying – zveřejňování choulostivých, lživých informací a obrazových materiálů (fotek, videí) na webových stránkách nebo jejich šíření mobilním telefonem (Martínek, 2015).

Kybergrooming – útočníci vytvářejí se svými oběťmi důvěrné vztahy pomocí moderních komunikačních technologií za jediným záměrem – aby po navázání důvěry vylákali svou oběť k osobnímu setkání, jehož cílem je často sexuální zneužití, manipulace k nelegálním činnostem nebo jiná forma agrese. Nejznámější případem v ČR je kauza Pavla Hovorky z Prahy, který tímto způsobem dokázal vylákat přes 20 chlapců a některé z nich zneužil. Časté jsou také případy, kdy se útočníci pomocí falešných profilů vydávají za celebrity a vyhledávají jejich fanoušky za účelem vylákání oběti na osobní schůzku. Stejně tak se setkáme s falešnými fotografy, kteří chtějí od vytipovaných obětí fotografie, často nahé nebo polonahé, pro smyšlená výběrová řízení. Po získání intimních fotografií se snaží vybrané oběti také pozvat na osobní schůzku, v případě odmítnutí je vydírají s výhrůžkou zveřejnění dříve získaných fotografií. Kybergrooming představuje velké riziko pro děti všech věkových kategorií, stejně tak může ohrozit i dospělé. Ochranu představuje především prevence, dobrá informovanost o této hrozbě mezi rodiči i na školách a mimo jiné také fungující komunikace mezi dítětem a rodičem/učitelem (Dočekal, Eckertová, 2013).

Outing – útočník využívá velké množství veřejných serverů s různým zaměřením, kde publikuje převážně soukromé, ale i jinak citlivé, zahan-

bující nebo nepravdivé informace o své oběti s cílem veřejně ji zesměšnit. Outing může probíhat mnoha způsoby, a vzhledem k tomu, že se v podstatě jedná o únik osobních (často velmi citlivých) informací, pak mohou být dopady na široké škále od nevýznamných až po ty závažné. Co se pocitu soukromí týče, dokonce i čtení soukromých zpráv vašich dětí lze považovat za formu outingu, a dítě tak v tomto případě paradoxně může vnímat formu kyberšikany ze strany svých rodičů, kteří odhalili a přečetli si jeho privátní zprávy (Dočekal, Eckertová, 2013).

Phising – tento název znázorňuje kradení hesel a následné zneužívání osvojeného účtu na sociální síti nebo e-mailu (Martínek, 2015).

Trolling – je forma příspěvku nebo zprávy, kterou útočníci používají se záměrem vyprovokovat dotyčnou osobu (nebo více osob) k dalším reakcím on-line. Útočníci zprávami obtěžují, urážejí ostatní a čekají na jejich reakce. Obvykle je cílem vyvolat v obětech frustraci, vztek a donutit účastníky diskuse k slovním útokům, kterými se samy znemožní. Jedná se o méně nebezpečnou formu kyberšikany, setkáváme se s ní však velmi často (Dočekal, Eckertová, 2013).

1.7 Kde konkrétně se v on-line prostředí můžeme s kyberšikanou setkat

E-mail
Jakmile útočník získá e-mailovou adresu své oběti, nic mu nebrání v odesílání enormního množství obtěžujících zpráv, které často rozesílá z anonymních účtů. Také může e-mailovou adresu zveřejnit na „vhodných" místech internetu, odkud je pak e-mailová schránka bombardována spamy, reklamou a často až stovkami nových e-mailů, o které adresát vůbec nestojí.

Jak se bránit:
Nevyžádané e-maily a slovní útoky přes e-mail jsou spíše obtěžující než nebezpečné (tedy pokud zároveň neobsahují viry). Adresátova schránka je zahlcena, je nutné se v množství nevyžádaných e-mailů dlouze probírat a smazat vše, co je nepotřebné, a to je náročné především časově. V soukromé korespondenci je možné zřídit novou e-mailovou schránku

(např. na freemailu Seznam.cz nebo Gmail.com), tuto adresu pak již nikde nezveřejňovat a používat ji pouze s věrohodnými kontakty. Pokud starou (a napadenou) e-mailovou schránku nebudu vůbec zapínat, pak se útočníkova snaha zcela mine účinkem. Kyberšikana se však netýká pouze soukromých schránek a je-li napadená e-mailová schránka firemní nebo školní, pak je vhodné nasazení filtrů, které budou nevyžádané zprávy automaticky mazat. Nutno ale podotknout, že žádná filtrace nevyžádané pošty nefunguje na 100 procent.

Doporučení:
Nezveřejňujte nikde svou e-mailovou adresu, nepředávejte ji zbytečně nevěrohodným kontaktům a používejte do své schránky silné heslo!

SMS zprávy a obtěžující volání na mobilní telefon
Hnacím motorem mnoha šikanujících je takzvaná textová válka. Ta se nejčastěji odehrává právě formou SMS zpráv, a pokud šikanovaný na zprávy reaguje (ať už jakoukoli formou), tak je to voda na útočníkův mlýn. Útočník často píše z anonymních SIM karet, používá internetové SMS brány, v případě volání pak skrývá číslo pro zamaskování své identity. Oproti e-mailu jsou SMS zprávy mnohonásobně víc obtěžující především proto, že mobilní telefon máme téměř vždy u sebe. Útočníci navíc rádi posílají desítky i stovky zpráv a tím dokážou telefon zcela zahltit a znemožnit tak komunikaci s jinými lidmi. V případě volání si šikanující může dokonce nainstalovat speciální software, který dokáže změnit a zastřít jeho hlas k nepoznání, v jiných případech se záměrně používá „ticho“ v telefonu se snahou psychicky „vydeptat“ volaného. Do obtěžování spadá nejen samotné volání ve formě přijatých hovorů, ale též neustálé a nekonečné prozvánění.

Jak se bránit:
Je dobré si uvědomit, že naše telefonní číslo prostě nemusí vědět úplně každý, a pokud není pro zveřejnění čísla žádný pádný důvod, je lepší nikde je neuvádět. Dejte číslo pouze svým známým, kamarádům nebo lidem, kterým důvěřujete. Samozřejmě i tak nemusí být pro útočníka obtížné se k Vašemu číslu dostat, pokud se tak ale již stane, pokuste se volajícího zablokovat. To můžete udělat i v případě „anonymních volání“, kdy zablokujete přijímání hovorů ze skrytých čísel. Můžete si také nainstalovat program pro nahrávání hovorů, nicméně správně byste ho

bez vědomí volajícího neměli používat. Nezapomeňte, že stejný program může vždy používat i útočník bez Vašeho vědomí.

Doporučení:
Nepředávejte své číslo nikomu zbytečně. V případě, že se stanete terčem útoků, na zprávy ani volání zpět nereagujte. Pokud to nepředstavuje větší problém, pak můžete v případě útoků svoji SIM kartu deaktivovat a pořídit si jiné číslo, které již útočník nebude znát. Nezapomeňte si též zabezpečit svůj telefon heslem, PIN kódem, otiskem prstu nebo jinou formou zabezpečení. Nikdy svůj mobilní telefon nikomu nepůjčujte, do telefonu je totiž také možné instalovat aplikace, které pak budou „špehovat" Vaši komunikaci bez Vašeho vědomí!

Sociální sítě, komunikační programy (Messenger, WhatsApp, Skype apod.)
Mezi nejčastější případy, při kterých dochází ke kyberšikaně na sociálních sítích, patří krádež identity. Špatně zabezpečený profil je snadným terčem pro útočníka, který se do osobního (např. facebookového) profilu může dostat, změnit přístupové heslo a vystupovat tak jako jiná osoba. Původnímu majiteli účtu se již nemusí podařit získat přístup zpět, nebo je tato operace, kterou je nutné nahlásit, velmi zdlouhavá a složitá. Útočník, který profil získal, může za původního majitele veřejně publikovat nepravdivé informace, může přes chat pod falešnou identitou komunikovat s přáteli poškozeného, a navíc také získá přístupy ke všem předešlým komunikacím, příspěvkům a fotografiím (tato soukromá data a komunikaci může navíc zveřejnit). Z výše uvedeného vyplývá, že nabourání účtu jinou osobou je jednou z nejhorších věcí, která se Vám může na sociálních sítích přihodit. Přesto většina uživatelů sociálních sítí zabezpečení svého účtu velmi podceňuje, mají nastavena jednoduchá hesla a praxe přináší téměř každodenně velké množství případů tohoto zneužití. Účet sociální sítě však nemusí být pouze „ukraden", může být i záměrně vytvořen, a to tak, aby se co nejvíce podobal původnímu, originálnímu účtu. Útočník použije veřejně dostupné informace a fotografie k vytvoření falešného účtu, který se pak snaží prezentovat jako „originál". Nebezpečí z toho plynoucí jsou stejná nebo podobná těm, která uvádíme výše. Jiná forma kyberšikany přes sociální sítě je podobná šikaně, kterou jsme uvedli výše u SMS zpráv. Zname-

ná to, že útočník neustále posílá zprávy přes komunikační programy, zahlcuje tak komunikaci a obtěžuje svou vyhlédnutou oběť. Vzhledem k tomu, že sociální sítě používáme z velké části na mobilních zařízeních, je tato forma šikany stejně obtěžující jako u SMS zpráv nebo volání (volat je možné i přes internet pomocí těchto komunikačních programů).

Jak se bránit:

Jednou z nejdůležitějších věcí, o kterou musíme jako uživatelé dbát, je důsledné zabezpečení našich uživatelských účtů. Existují mnohá doporučení, jak sociální sítě zabezpečit, jak si správně nastavit hesla, jak si hesla pamatovat a jak s nimi pracovat. Důležité je také nastavení tzv. dvoufázového ověření, které známe např. z internetového bankovnictví. Pokud si dvoufázové zabezpečení na své sociální síti zapneme, přijde nám před každým přihlášením ještě potvrzení formou SMS. Tím zároveň dokážeme zjistit, zda se nám někdo pokouší z jiného počítače do našeho účtu „nabourat". Stejně jak je uvedeno výše, dbejte i zde o maximální bezpečnost. Do svých sociálních sítí si přidávejte jen ty „přátele", které dobře znáte. Nepřidávejte si pokud možno osoby, které jste nikdy neviděli, a určitě nikdy nepůjčujte nikomu svůj počítač, notebook, telefon nebo tablet, obzvláště ne s aktivním přihlášením na některou ze sociálních sítí. Riziko zneužití je pak velmi vysoké.

Webové stránky, diskusní fóra

Mnozí uživatelé s oblibou komunikují pomocí blogů nebo diskusních fór. V těch je možné publikovat pod svým vlastním jménem, ale často také anonymně. I v těchto případech se můžeme setkat s formou kyberšikany, kdy útočníci, schovaní pod anonymními přezdívkami, napadají diskutující. To je nepříjemné hlavně proto, že diskuse je často veřejně přístupná pro jakéhokoliv uživatele internetu a zveřejnění citlivých informací je pak viditelné pro všechny návštěvníky fóra/blogu. V případě diskusních fór navíc nemá napadený možnost příspěvek smazat a musí o smazání nevhodného příspěvku žádat administrátora stránky. Ten však nemusí reagovat, ať už z důvodu vytížení, nezájmu, nebo je server i administrátor stránky v jiné zemi.

Jak se bránit:

Pokud rádi přispíváte do diskusních fór, nedávejte nikomu záminku k útokům. Pakliže již podobná situace nastane, nepřecházejte do slov-

ního souboje s útočníkem, situaci vyřešte jedním příspěvkem s asertivním přístupem a dál již do diskuse nepřispívejte. Pokud je to možné, pokuste se kontaktovat administrátora stránky a požádejte ho o posouzení situace.

Webkamery

Přestože se webkamery nedají úplně označit jako místo, kde probíhá kyberšikana, dovolíme si je do tohoto seznamu přesto zařadit. Představují totiž značné riziko v ohrožení soukromí uživatele notebooku nebo telefonu. Útočníci se často pokoušejí nepřímo nebo lstivě přinutit svoji oběť k obnažení se před webovou kamerou, použití kamery je velmi jednoduché a přenos pořízeného videa může probíhat při dnešní rychlosti internetu i v reálném čase. Útočníci pak žádají své oběti, aby jim pořízená videa zaslaly, nebo si je dokonce sami nahrávají bez vědomí uživatele. V obou případech pak často pořízení videa využívají k vydírání své oběti a snaží se ji zmanipulovat. Časté jsou případy vylákání na osobní schůzku, nucení k posílání dalších obnažených fotografií pod hrozbou zveřejnění původního videa apod. Tato forma kyberšikany je velmi nebezpečná, protože zasahuje do nejintimnějších oblastí postiženého, výjimkou nejsou pokusy o sebevraždu nebo jiné psychické poruchy.

Jak se bránit:

Webovou kameru používejte jen s věrohodnými kontakty a nikdy, opravdu NIKDY se před kamerou nesvlékejte. Nedělejte to ani pro nejbližší přátele, celosvětové zkušenosti ukazují až nebezpečně vysoký počet podobných zneužití videí nebo fotografií těmi nejbližšími přáteli. Určitým rizikem je i možnost „hacknutí" webové kamery, kdy může útočník nahrávat video, aniž byste o tom vůbec věděli. Pokud kameru nepoužíváte, můžete její čočku přelepit samolepkou nebo jinak. Máte tak jistotu, že i v případě napadení webkamery nedojde k žádné nahrávce, která by se pak dala zneužít.

2 Právo a kyberšikana

Nelegální jednání, která souvisejí s internetem a on-line prostředím, popisuje soubor zákonných norem trestního zákona – zákon č. 40/2009 Sb.

Česká legislativa pojem „kyberšikana" nezná, ale vzhledem k tomu, že je to „jen" elektronická verze klasické šikany, můžeme se opřít o tento pojem. Zákon definuje pojem šikana jako „úmyslné jednání, které je namířeno proti jinému subjektu a které útočí na jeho důstojnost". Rozhodující není ani tak forma jako spíše úmysl, a pokud splňuje znaky vymezené v zákoně, pak se jedná o trestný čin.

Šikana bývá nejčastěji postihována podle ustanovení zákona č. 40/2009 Sb., trestní zákoník (dále jen TZ), a to jako:

- trestný čin omezování osobní svobody;
- trestný čin vydírání;
- trestný čin vzbuzení důvodné obavy;
- trestný čin loupeže;
- trestný čin ublížení na zdraví;
- trestný čin poškozování cizí věci;
- trestný čin znásilnění či pohlavního zneužívání.

Aby byl útočník postižitelný, musí mu být více než 15 let, stejně jako je to u jiných trestných činů. Pokud je útočníkovi v rozmezí 15 až 18 let, je posuzován jako mladistvý. V případě dětí do 15 let věku jsou trestně odpovědní jejich rodiče, dítě však může být postiženo umístěním do

ústavní výchovy nebo mu může být uložen dohled probačního úředníka.

Trestní sazby pro šikanu se liší podle závažnosti, kdy jedno jednání může být kvalifikováno jako více trestných činů.

Pozor! Pokud dochází k šikaně v průběhu vyučování, nese plnou odpovědnost škola! Právně nebo pracovněprávně může být potrestán pedagog či ředitel školy, pokud se prokáže jeho zanedbání, v některých případech může být dokonce přiznán i nárok na odškodné ve věci náhrady škody na věcech, na zdraví nebo v případě psychické újmy.

Přestože kyberšikana (obdobně jako školní šikanování) sice není sama o sobě trestným činem ani přestupkem, mohou její projevy velmi často naplňovat skutkovou podstatu např. těchto trestných činů:

- ublížení na cti, zákon č. 200/1990 Sb., zákon o přestupcích, § 49;
- zákaz natáčení, fotografování a zveřejnění snímků bez souhlasu dotyčné osoby, nařízení EU 2016/679, GDPR;
- nebezpečné pronásledování (v překladu stalking, § 353–354 TZ) – například se jedná o dlouhodobě opakované pokusy kontaktovat všemi dostupnými prostředky (pomocí komunikačních médií) oběť, která proto pociťuje důvodné obavy o život nebo zdraví své či svých blízkých;
- účast na sebevraždě (§ 144 TZ) – nejčastěji se jedná o zaslání SMS oběti s úmyslem vyvolat u ní rozhodnutí k sebevraždě;
- porušení tajemství dopravovaných zpráv (§ 182 TZ) – například „odposlech“ odesílaného e-mailu či SMS zprávy;
- porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183 TZ), např. zveřejnění fotografií, videí, zvukových záznamů z telefonu oběti;
- pomluva (§ 184 TZ) – např. vytvoření webových stránek či různých skupin na sociálních sítích s cílem zesměšnit oběť či více obětí.

V mnoha případech je u kybernetické šikany problém s prokazováním zlého úmyslu pachatele. Přestože je možné na počítači nebo na internetu nalézt stopy nezákonného jednání (např. i ve spolupráci s inter-

netovým poskytovatelem), záleží také na „šikovnosti“ útočníka a jeho schopnosti tyto stopy po sobě zahladit. Někdy je dokonce trest téměř nemožný bez přiznání pachatele, např. u tzv. kybergroomingu (vylákání oběti na osobní schůzku přes internet, detailnější popis – viz dále). Pokud nedojde na osobní schůzce k násilnému činu, nemůže policie nic dělat, a to ani v případech, kdy je incident předem nahlášen a policie je na místě schůzky přítomna. Útočník může tvrdit, že chtěl dítě tímto stylem před podobným nebezpečím jen názorně varovat. Trestná je samozřejmě už jen příprava s úmyslem spáchání závažného činu, nicméně úmysl musí policie prokázat, což je právě velmi obtížné nebo nemožné.

Další riziko může přijít také ze strany rodičů dětí, kteří z nevědomosti umisťují na internet materiály a fotografie, které mohou dětem ublížit. Nejčastějším příkladem je pořizování a umisťování fotografií nahých nebo polonahých dětí na Facebook, Instagram a další sociální sítě, např. z dovolených, z koupání v bazénu apod. Rodiče s úmyslem pochlubit se svými ratolestmi vystavují tyto snímky na sociálních sítích, neuvědomují si ale rizika jejich dalšího zneužití. Toho využívají např. různé skupiny, které si tyto fotografie stahují do svých specializovaných databází a poskytují je za úplatu lidem z celého světa, kteří mají sklony např. k pedofilii. Nikdo si určitě nepřeje, aby fotky jeho dětí putovaly napříč různými pedofilními databázemi, taková situace pak může způsobit i psychickou újmu dítěti, které fotografie později (nebo až v dospělosti) někde na internetu objeví. Případy fotografování a zveřejňování nevhodných snímků ze stran rodičů jsou bohužel v on-line prostředí více než časté.

3 Netolismus – závislost na internetu

Informační a komunikační média procházejí od počátku civilizace vývojem. Poslední vývojovou etapou je digitalizace, která s sebou přináší také internet, počítače s internetem či mobilní telefony (Sak, 2007). Digitalizace může a zcela jistě společnosti přináší mnohé výhody a pozitiva, na druhé straně však stojí také značná rizika. Jedním z možných a velmi častých rizik je vznik závislostí. Setkáváme se dokonce s tvrzeními, která připodobňují závislost na informačních a komunikačních médiích k závislosti na alkoholu s dodatkem, že mohou způsobit značné poruchy vývoje (Spitzer, 2014).

Závislost na internetu je fenoménem moderní doby. Pokud pozorujete, ať už na sobě, či jiných, že trávíte značné množství času hraním on-line her, neustálým kontrolováním Facebooku či jiných sociálních sítí, máte nutkání k on-line nakupování nebo cítíte, že používání moderní techniky Vám narušuje práci, školu nebo fungování rodiny, pak můžete být k závislosti na internetu opravdu velmi blízko. Závislost bývá někdy označována pojmy „netolismus“ nebo „netholismus“ a znamená tedy závislost na virtuálním prostředí, kam koneckonců mohou patřit nejen počítače, ale i tablety, telefony nebo dokonce televizory. Nejrizikovější skupinou, které se ohrožení a závislost nejčastěji týká, jsou pak právě mladí lidí, teenageři nebo dokonce děti. Problémem je, že ať už závislost pociťujeme, nebo ne, stejně jsme v obrovské míře obklopeni moderními technologiemi, které na nás „útočí“ téměř na každém kroku. Mnoho běžných činností se přesunulo do virtuálního prostředí. Chcete si objednat oběd? Stačí si ho vybrat na internetu a oběd Vám přijede až pod nos. Chcete si koupit sekačku nebo třeba boty? Proč chodit do ob-

chodu, když si vše můžete objednat on-line přímo z gauče, který jste si mimochodem také pořídili na internetu. Nemůžete spát a napadlo Vás zahrát si nějakou on-line hru? Můžete se vsadit, že vždy na internetu najdete spoustu lidí, kteří se k Vám v tu chvíli rádi přidají. Internet tedy používáme denně, je těžké se od podobné závislosti oprostit a je v podstatě téměř nemožné se v dnešní době internetu zcela zbavit!

Tyto poruchy vznikají v kyberprostoru, tzn. virtuálním prostoru, do kterého se můžeme dostat pomocí počítačů a počítačových sítí, jež ve spojení s internetem vytvoří on-line prostředí (Divínová, 2005).

Zejména v posledních letech se můžeme setkat také s rozšířením o mobilní telefony a tablety s připojením k internetu, které jsou stále dostupnější také u dětí. Základní závislostí v souvislosti s informačními a komunikačními technologiemi je závislost na internetu. Tato závislost je charakteristická časem stráveným na internetu, který zasahuje reálný život a přináší s sebou časté změny nálad, konflikty a abstinenční příznaky (Jaknainternet.cz, 2018). V těsném závěsu jsou závislosti na mobilních telefonech. Tato závislost je charakteristická neustálou kontrolou telefonního přístroje či neschopností být sám (Kalina, 2008).

S těmito závislostmi velmi úzce souvisí také riziko kyberstalkingu, kybergroomingu či dětská pornografie nebo kyberšikana, na kterou je tato příručka cíleně zaměřena. V případě tvorby závislostí sehrává primární roli rodič. Základem je přesné stanovení hranic, a to již od útlého věku (Spitzer, 2014).

Na druhou stranu, to, že každý den sledujete videa na YouTube, že hodně brouzdáte po internetu a jste často na Facebooku nebo že rádi nakupujete on-line ještě neznamená, že jste na internetu závislí. Problém nastává, když Vám tyto aktivity začnou zasahovat do běžných každodenních činností a narušovat je.

Závislost na internetu není někdy jen o čase, tzn. o tom, kolik hodin denně na internetu strávíme, je také o tom, co na internetu konkrétně děláme. Např. na sociálních sítích nebo u pornografického materiálu jde často o obsah, který se na internetu hledá, než o čas na něm strávený. Samotná závislost pak má výrazný dopad nejen na snížení zbylého času, nutného pro každodenní běžně činnosti, práci, školu, hygienu, ale může s sebou nést dále i poruchy soustředění, fyzickou i psychickou únavu, problematické navazování vztahů, zhoršenou kvalitu komunikace s ostatními, impulzivní jednání apod.

Projevy závislosti na internetu jsou podobné ostatním závislostem, jako je např. závislost na alkoholu. U internetové závislosti hraje velmi důležitou roli ale i zvědavost. Říká se, že zvědavost je jedna z nejsilnějších vlastností, dokonce silnější než lenost, protože jen zvědavost nás kolikrát dokáže zvednout z postele. Na internetu se dozvídáme stále nové a nové věci a zvědavost je stimulována velmi silně. Na sociálních sítích se stále dozvídáme, co je nového, facebooková stránka je v podstatě nekonečná a profilů jsou miliony, teoreticky by se dalo tedy surfovat také donekonečna. Stejně tak internetové hry jako např. World of Warcraft a mnoho dalších mají tu vlastnost, že vlastně nikdy nekončí, příběh vytváří tisíce hráčů z celého světa a hrát se dá doslova navždy, dokud nebudou tyto herní servery vypnuty.

Závislost na internetu je vlastně zvláštním pojmem, protože internet je dnes všude a někdy paradoxně ani nevíme, které služby a aktivity jsou stále „off-line" a které již on-line – objednání jídla přes (internetový) telefon a jeho dovážka, sledování televize, kde ani nevíme, zda jde o internetové či běžné vysílání, kamery na každém rohu a to „zajímavější" nás ještě čeká – chytré parkování ve městech, k internetu připojená lednička, která si sama řekne, co se má nakoupit, chytré hodinky a náramky propojené s Vaším dietním programem, chytré vytápění atd. Čeká nás doba věcí internetu (Internet of Things, IoT), a pokud to jen lehce přeženeme, tak je možné, že svět bude čím dál tím víc on-line než off-line. Rizika závislosti se tak tedy budou bohužel spíše zvyšovat.

Závislost na mobilním telefonu je v dnešní době velmi častá a týká se jak dětí, tak dospělých. Odborným názvem se jí říká nomofobie. Jedná se především o strach, že se člověk ocitne v situaci, kdy u sebe nemá mobilní telefon. Tato fobie má již své místo v Mezinárodní klasifikaci nemocí (MKF). V dnešní době se děti věnují mobilnímu telefonu až několik hodin denně. Dle analýz průměrný uživatel zkontroluje svůj mobil až 150krát denně. Nový pojem, který je spojený se závislostí na mobilním telefonu, se nazývá „Fantomova vibrace", kdy si uživatel mobilního telefonu myslí nebo může i cítit, že jeho telefon vibruje – například že přišlo upozornění či SMS zpráva, i když je mobilní telefon vypnutý (což se stává opravdu minimálně) nebo je v tichém režimu. Tímto syndromem může být postiženo až 90 % uživatelů mobilního telefonu. Člověk závislý na mobilním telefonu má špatný pocit, když není dostupný a neustále kontroluje, jestli mu někdo nevolal, popř. neposlal SMS, v kraj-

ním případě může mít i fyzické potíže – abstinenční příznaky (Veverka, Stavinoha, 2005).

Závislost na mobilním telefonu vzniká velmi často. Pokud jde o pracovní pomůcku, je tato závislost „oprávněná", neboť jde v podstatě o jeden z pracovních nástrojů. Telefon ale často uživatele svádí k dlouhým hovorům, kdy protelefonovaná doba nepřináší časovou úsporu, jakou by telefon měl přinášet. Význam telefonu jako důležitého informačního toku se nedá popřít, je ale třeba připomenout, že někdy mnoho užitečných informací v nadměrném množství přivádí spíše své uživatele do stresových a nepříjemných situací než k prožitku uspokojení (Nešpor, 2011).

Druhy netolismu (Kopecký, 2013)

1. **Závislost na virtuální sexualitě** – velmi časté, nutkavé vyhledávání a následné využití webových stránek s pornografickým obsahem.
2. **Závislost na virtuálních vztazích** – nadměrné věnování se virtuálním vztahům především prostřednictvím on-line komunikace na sociálních sítí a seznamkových webech.
3. **Internetové kompulze** – primárně hraní on-line her, velmi časté nakupování na internetu, sázení přes internet.
4. **Přetížení informacemi** – člověk tráví nadměrné množství času při surfování na internetu nebo při nadměrném vyhledávání v internetových databázích.
5. **Závislost na počítačích** – závislost, která se projevuje nadměrným využíváním osobního či pracovního počítače především k hraní her.

Projevy netolismu

A) Fyzické problémy (Krčmářová, 2012; Netolismus.cz, 2018)

- bolesti krční páteře a zad;
- pálení a slzení očí;
- bolest hlavy;
- bolesti zápěstí a rukou;
- pocity chladných prstů;
- křeče v prstech nebo zápěstí;
- necitlivost v prstech a dlaních;
- mravenčení v nohou.

B) Ztráta kontroly nad časem (Blinka, 2015)

- zvýšení tolerance časové dostupnosti na internetu;
- velmi brzké vstávání či naopak dlouhé ponocování z důvodu potřeby být na internetu.

C) Psychické projevy (Blinka, 2015)

- častý pocit prázdnoty v době, kdy jedinec není on-line u počítače či mobilního telefonu;
- nervozita a neklid, pokud jedinec delší dobu nepoužívá počítač či mobilní telefon;
- přemýšlení o informačních a komunikačních médiích, když je zrovna nepoužívá;
- zatajování možné závislosti na internetu;
- informační a komunikační média používaná jako únik od osobních problémů;
- zvýšená míra agresivity způsobená hraním různých on-line her.

D) Psychosociální projevy (Kopecký, 2013)

- narušené vztahy s rodinou;
- ztráta přátel;
- výměna reálných přátel za „on-line kamarády".

E) Projevy spojené se školní docházkou (Kopecký, 2015)

- méně vykonané práce;
- zanedbávání učení;
- zhoršující se prospěch.

Výše uvedené má pak ve svém výsledku za následek ztrátu sociálních vazeb, zhoršení pracovních vztahů (zhoršení pracovní výkonnosti, hrozba výpovědi z práce), finanční problémy apod. Závislý člověk se dostává do izolace, zhoršují se vztahy s blízkými osobami, dostává se do finančních potíží kvůli platbám např. za on-line hraní nebo za internetové nákupy.

Pokud si závislost na internetu přiznáte, nemusí být úplně optimální ihned se od internetu odpojit, protože hrozí silné abstinenční příznaky. Navíc si tím znemožníte činnosti, které běžně lidé vykonávají, jako jsou čtení e-mailů, internetová telefonie, přehled o počasí apod. Jistou

cestou může být použití specializovaných programů, které hlídají čas strávený na internetu a po určité době ho odpojí. Jsou také schopné zablokovat určité typy stránek buď podle její kategorie, nebo podle konkrétního zadání. Více než vhodné je také vyhledání psychologické péče a konzultace tohoto problému s odborníkem, pomoci může i zvýšení fyzické aktivity, začlenění více sportovních činností do každodenního života apod.

V případě léčby závislostí je postupováno velmi specifickou metodou, která rozpoznává rizikové body u uživatelů (to, co v nich vyvolává nutkání, potřebu utéct do virtuálního světa), a tím závislosti předchází. Důležité je dodat, že omezování či zakazování užívání prostředků není vhodné. Primárně by mělo být cíleno na přípravu plánů postupu v případě rizikových bodů a na rozvoj zdravých sociálních vztahů (Kalina, 2008).

4 Prevence kyberšikany v rodině

Klíčovou roli v prevenci hraje vždy rodina. Hlavní zásadou je otevřená komunikace. Děti ve Vás potřebují vidět oporu, musí vědět, že jste na jejich straně a že situaci s Vámi zvládnou vyřešit. Mějte na paměti, že přímé otázky typu „Někdo tě obtěžuje?“ mohou děti vyděsit a uzavřít tak cestu k řešení. Raději se ptejte opatrně, např. stylem: „Co jsi dnes dělal na tabletu, jak jsi strávil čas na internetu?“ Případně můžete opatrně zmínit některé příklady ohledně bezpečnosti na internetu, ale vyhněte se přímé souvislosti s dítětem nebo jeho přáteli.

Preventivní zásady pro rodinné prostředí můžeme shrnout do těchto bodů:

1. **Nastavte si „on-line“ pravidla.** Domluvte se se svými dětmi, jak budou svou techniku využívat, jaké stránky a aplikace jsou pro ně přístupné, kolik času na internetu stráví a jaké komunikační programy budou používat (včetně toho, jakým jazykem na nich smí mluvit). Přirovnejte tato komunikační pravidla k běžně užívanému chování ve společnosti a veďte své děti k nepsané on-line etiketě. Pravidla, která domluvíte, mohou obsahovat to, že dítě např. nebude půjčovat svůj tablet nikomu cizímu, že nebude komunikovat nebo navazovat vztahy s cizími lidmi (stejně jako to nedělá v běžném životě) a že bude velmi opatrné v tom, co na internetu zveřejní. Nezapomeňte zmínit nutnou diskrétnost i u fotografií, které umí každé zařízení dnes bez problémů pořizovat. Zároveň sami zajistěte (případně s pomocí IT odborníka) co nejpřísnější nastavení internetového soukromí v zařízení Vašeho dítěte. Je velmi důležité také dítěti říci, proč

jsou všechna výše uvedená pravidla důležitá. Odsouhlaste si jasné dodržování těchto pravidel a zmiňte možné důsledky plynoucí z jejich nedodržení. Není na škodu, pokud dětem ukážete i možnosti, jak např. případného „obtěžujícího" zablokovat.

2. **Projevte dítěti svou podporu a sdělte mu, že jste v případě jeho ohrožení připraveni zakročit.** Dopřejte zároveň dětem jejich soukromí a nekontrolujte jim všechny zprávy a aktivitu. Domluvte se, že zakročíte pouze v případě, kdy to bude opravdu nezbytné. Sdělte svým dětem, že o tomto problému s Vámi mohou kdykoliv otevřeně hovořit a že být obětí podobných útoků není žádná ostuda. Obětí se totiž může stát kdokoliv a 100% ochrana neexistuje. Nikdy dětem nevyhrožujte, že jim při porušení pravidel zařízení odeberete. Buďte naopak sami aktivní, ptejte se svých dětí, zda je vše v pořádku, a postupně své děti v tomto ohledu neustále vzdělávejte.
3. **S dětmi však o možné (kyber)šikaně hovořte**, ať už na ni podezření máte, či nikoliv. Preventivní osvěta je v tomto případě více než vhodná a může Vás i Vaše dítě do budoucna ušetřit mnohých trápení.

Nesmíme také zapomenout na opačnou situaci, neboť ne každý rodič je rodičem oběti. Mnoho dětí šikanuje ostatní vrstevníky, přičemž si tyto děti svou činnost neuvědomují, nejsou si vědomy nebezpečí a rizik z toho plynoucích a své konání často považují jen za neškodný vtip. Pokud jste rodič či učitel, nezapomeňte mluvit s dětmi i o této odvrácené straně mince, např. o tom, jak můžeme zdánlivě neškodnými on-line aktivitami dalším ubližovat.

Kyberšikana je problém, který se čím dál více projevuje, což je spojeno právě s extrémním nárůstem dětí, které jsou stále více „on-line". Děti spolu po internetu komunikují, sdílejí zážitky, fotografie i videa, hrají hry, poslouchají hudbu a chytrou techniku používají i pro školní a výukové potřeby. Kyberšikanou ovlivnitelné je tedy v tuto chvíli téměř každé dítě v ČR a jen malé procento, především ze sociálně slabších rodin, přístup k internetu nemá. Vzhledem k oblíbenosti internetu u dětí se dá navíc říci, že riziko ohrožení je 24 hodin denně, 7 dní v týdnu a 365 dní v roce. Není žádným překvapením, že vlivem tohoto rozšíření některé děti tyto prostředky využívají pro šikanování druhých, urážení ostatních je tak pro ně mnohem snazší než v případě těchto výhrůžek tváří v tvář. Mnohé děti navíc ovládají tuto „chytrou techniku" mnohem lépe než je-

jich rodiče a to jim napomáhá v přesvědčení, že u této činnosti nebudou nachytány, a tudíž jim ani nehrozí žádné následky nebo postih. Internet také nemá žádné hranice, děti si běžné píší na cizojazyčných serverech s kamarády z celého světa. A jak je z výše uvedeného zřejmé, nebojí se psát cokoliv, schovány za neviditelnými zdmi virtuálního světa. Pokud píší nevhodné nebo urážlivé příspěvky, mnohdy si bohužel ani neuvědomují, jakou svým jednáním mohou způsobit bolest, škodu nebo jaký psychologický dopad to na ostatní může mít.

5 Technická řešení jako prevence kyberšikany

Uveďme si nyní několik základních technických opatření, která musíme dodržet, abychom předešli útokům nebo pokusům o krádež uživatelských účtů:

1. Silná hesla – jedním z nejzákladnějších pravidel pro IT bezpečnost je mít své zařízení (notebook, tablet, telefon) uzamčené. Počítač nebo telefon – ať už nový, či z druhé ruky – musíte nejprve zabezpečit. Někdy jsou tato zařízení z výroby odemčená, pak stačí notebook nebo telefon zapnout a okamžitě jsme přihlášeni v našem uživatelském účtu. Většina zařízení má možnost uzamčení obrazovky po určité, předem stanovené době (např. 10 minut u notebooku, 30 vteřin u telefonu). Po této době obrazovka ztmavne a zařízení se přepne do režimu spánku. Důležité je myslet na bezpečnost, proto bychom měli mít probuzení přístroje zabezpečené heslem, otiskem prstu, PIN kódem nebo gestem. Ve chvíli, kdy bychom zařízení ztratili nebo by nám bylo odcizeno, je pro útočníka velmi jednoduché uživatelský profil odemknout a získat tak přístup k našim datům, souborům, fotografiím, školním nebo pracovním dokumentům, videím nebo jiným citlivým materiálům. Po spuštění patřičné aplikace pak útočník navíc získá přístup i k e-mailům, k profilům sociální sítě, k veškeré komunikaci, ke kontaktům apod. Z toho zároveň vyplývá, že uzamčený by neměl být pouze samotný přístroj (resp. spořič obrazovky), ale silná hesla musíme mít i do jednotlivých aplikací, do e-mailových schránek, do sociálních sítí atd. Silné (kvalitní) heslo je pak heslo, která má minimálně 8 až 12 znaků, obsahuje malá i velká písmena, číslice a speciální znaky, jako např. hvězdičku (*), lomítko (/), paragraf (§),

procento (%) a další. Při takovémto zabezpečení je šance na prolomení hesla zcela minimální. Oproti tomu hesla typu „123456“, „ahoj“ nebo „password“ nejsou vůbec vhodná, běžně figurují v databázích nejčastějších hesel (ta je možné najít snadno na internetu) a útočníci tato hesla zkoušejí jako první. K prolomení hesla slouží i různé programy, které používají metodu „brute force“ (hrubá síla), což je princip, kdy program využívá výpočetní výkon počítače (nebo několika) a zkouší postupně všechny kombinace čísel a písmen k prolomení hesla. Čas potřebný pro výpočet se však velmi výrazně prodlužuje spolu s tím, kolik znaků heslo obsahuje. Tzn., že pokud splníme výše uvedená pravidla tvorby hesla, trvalo by výpočetnímu algoritmu i několik desítek nebo stovek let (při současném výpočetním výkonu), aby takové heslo prolomil.

Pro každou aplikaci bychom měli mít správně jiné heslo, nedoporučuje se mít jedno heslo pro všechny přístupy. V době, kdy lidé používají značné množství aplikací, je ale problém si tato hesla pamatovat. Existují však programy (password managery), které umějí hesla bezpečně sdružovat, stačí si pak pamatovat pouze jedno heslo. Nejčastější hrozbou je tak tedy uživatel sám, který své internetové bezpečí ohrožuje tím, že má heslo slabé, nebo dokonce své heslo někomu prozradí. Silná hesla do zařízení a aplikací jsou tedy naprosto klíčovým a základním prvkem v IT bezpečnosti.

Dalším důležitým bezpečnostním prvkem pro zabezpečení uživatelských účtů, který je více než vhodné použít pro zabezpečení e-mailových schránek nebo profilů na sociálních sítích, je tzv. dvoufázové ověření. Většina uživatelů internetu tento princip zná již ze svého internetového bankovnictví, kde se tato bezpečnostní vlastnost používá již řadu let. Pokud útočník získá přístup do internetového bankovnictví, není mu pak přihlášení nic platné, pokud nemá přístup i k mobilnímu telefonu (resp. jeho číslu), na který je internetové bankovnictví navázáno. Po každé platbě, kterou v bankovnictví na internetu zadáme, se totiž odešle ověřovací SMS klíč na mobilní telefon. Pokud není platba ověřena, transakce se neprovede. Na stejném principu funguje i přihlašování do většiny sociálních sítí nebo k e-mailových schránkám. Tuto funkci je však třeba vyhledat v nastavení a aktivovat ji. Výhodou je, že i po odcizení přístupových údajů není možné se k účtům přihlásit, protože je vyžádána SMS autorizace. Zkouší-li někdo navíc uhádnout Vaše uživatelské jméno a heslo, může Vám přijít upozornění SMS zprávou

nebo na sekundární e-mail, že se k Vašemu účtu pokouší připojit jiné zařízení. Může to posloužit jako indikátor, že se někdo snaží získat přístup, v některých případech je tedy vhodné zvážit změnu hesla apod.

2. Antivirový program – každé zařízení připojené do internetu je ihned vystaveno riziku útoku. V dnešní době, kdy jsou mnohé procesy zautomatizovány, existuje i celá řada automatických programů (robotů), které se snaží vyhledávat nezabezpečené počítače nebo routery a ty pak napadnout. Existuje mnoho druhů podobných internetových hrozeb, ať už ve formě virů, nebo např. tzv. trojských koňů. Některé škodlivé programy, pokud se do počítače dostanou, se umějí nenápadně implementovat do operačního systému a jsou schopny špehovat a bez vědomí uživatele číst a zaznamenávat jeho stisknuté klávesy, včetně pohybů myši. Těmto programům se říká „keyloggery". Uživatel, který má tento škodlivý program v počítači nainstalován, naťuká heslo např. do své e-mailové schránky, keylogger ho zaznamená a nenápadně odešle útočníkovi. Ten tak snadno získá přístupové údaje k e-mailové schránce.

Podobných hrozeb existuje celá řada a je nutné se proti nim bránit. Proto je více než vhodné mít v počítači nebo telefonu nainstalovaný antivirus, který podobné hrozby hlídá, detekuje a ve chvíli, kdy zjistí virus, znemožní jeho spuštění a uživateli o tom zobrazí informační hlášení. Antivirových programů je na internetu ke stažení velmi mnoho, mezi nejznámější patří v ČR např. Avast, AVG nebo ESET Antivirus. Nicméně ani instalace antiviru neznamená 100% ochranu zařízení. Tvůrci škodlivých programů hledají slabá místa zabezpečení a často takové místo objeví, aniž by je už znaly antivirové programy. Tvůrci antivirů reagují na objevené hrozby velmi rychle, řádově do několika hodin, maximálně dnů. Přesto je třeba vědět, že riziko existuje. Instalace antiviru je však nutná, neboť tato rizika velmi významně snižuje.

3. Aktualizace systému, programů a aplikací – každý operační systém, program nebo aplikace se postupem času vyvíjí a zároveň v sobě obsahuje vývojářské chyby, které se postupně opravují. Stejně tak jsou všechny aplikace ohroženy tím, že v sobě mohou skrývat bezpečnostní díru, kterou může útočník využít pro získání přístupu do počítače. Tyto bezpečnostní chyby jsou vývojáři postupně opravovány („záplatovány"). Je tedy nutné operační systém i aplikace pravidelně aktualizovat,

a pokud program o aktualizaci požádá, je dobré ji z bezpečnostních důvodů neodkládat. Aktualizací by mělo dojít zároveň ke zlepšení funkcionalit daného programu, hlavně ale k jeho dalšímu zabezpečení.

4. Vhodné IT programy pro prevenci a aplikace pro blokování nevhodných stránek – na internetu můžeme nalézt celkem dost programů, které mají za úkol hlídat nebo dokonce blokovat nevhodný obsah. Ve firmách nebo školách je možné tato pravidla aplikovat centrálně, u běžného uživatele se tyto programy instalují přímo na konkrétní zařízení. Programy umějí blokovat stránky s nevhodným obsahem podle jejich tématu, případně podle přesněji zadaných kritérií. Na druhou stranu je třeba zvážit vhodnost nasazení takových programů. Děti, pokud nejsou ještě moc malé, ji mohou vnímat jako omezení svobody, a navíc, jak praxe mnohokrát prokázala, děti jsou vždy schopné najít si cestu k tomu, co hledají. Je až neuvěřitelné, jakou invenci dokážou děti vyvinout ve snaze překonávat veškeré formy této ochrany. Dítě si tedy dříve či později cestu najde, to je nutné vzít v potaz a podle toho se rozhodnout, zda nasazení těchto aplikací proběhne, či nikoliv.

Pokud se však pro nasazení těchto programů rozhodneme, pak nesmíme zapomenout na zamezení jejich odstranění. To se řeší přístupovými právy v profilu zařízení, kdy dítěti nastavíme účet na telefonu nebo notebooku, který bude mít nižší oprávnění, a tudíž nebude mít možnost tyto programy vypnout nebo odinstalovat.

Zvlášť u menších dětí, které používají telefon nebo tablet především na hry, se může jevit jako vhodné spíše nastavení operačního systému tak, aby systém hlídal nevhodné aplikace nebo reklamy. Např. pro operační systém Android existuje systémové nastavení s názvem „Google Play Protect“, které po zapnutí hlídá vhodnost instalovaných aplikací pro děti a vhodnost zobrazovaných reklam, kterými jsou bohužel všechny hry a aplikace velmi zahlceny. Služba tak hlídá, aby se dítěti nezobrazila reklama ukazující násilí, krev nebo jiný škodlivý obsah.

I zde je však třeba zmínit nutnost dohledu rodičů, obzvláště u menších dětí, protože žádná internetová ochrana není dokonalá. Např. videa, která si dítě pouští přes Youtube, nemusejí být úplně vhodná. Děti rády sledují nahrávky z videoher, které jsou komentovány, a popisují, co hráč v danou chvíli dělá. Videa ale často obsahují nevhodný slovník, vulgární výrazy, tyto pro výchovu dítěte nevhodné prvky ale už žádný

automatický systém ohlídat nedokáže. Rodiče tak musí dohlížet pravidelně na aktivitu svých děti na internetu a nepodceňovat tyto internetové hrozby, přestože mohou mít mírnější formu. Pokud dítě rádo komunikuje s ostatními, doporučujeme i zde zvolit adekvátní program. Existují komunikační programy, kde se zaregistruje nejprve rodič, založí v programu účty pro své děti a všechny kontakty, které si děti pak přidávají do svých zařízení, musí být nejprve schváleny rodičem. Podobné možnosti najdeme i pro jiné aplikace. Aktivita a důslednost rodičů je v tomto směru zcela nezbytná.

6 Prevence kyberšikany na základní škole

Tato kapitola je věnována prevenci kyberšikany, která má opodstatněné své místo nejen ve volném čase, ale také ve školním prostředí.

Prevence kyberšikany je obtížná ze dvou hledisek:

1. Přestože není kyberšikana ničím zcela novým, mnoho lidí o ní není informováno a neuvědomuje si, jaké důsledky s sebou může nést. Mnohými bývá internetová šikana podceňována se slovy, že existují další a jiné závažnější formy agrese. Hrozeb je jistě celá řada, ale musíme si přiznat, že kyberšikana představuje velký problém dnešní doby a jejím ignorováním se stane pouze problémem ještě závažnějším.
2. Především ze strany rodičů je třeba převzít zodpovědnost za to, jak dítě technologie dnešní doby využívá, co mu dovolíme a jak na to jako rodiče dohlédneme. Dospělí často tvrdí, že nedokážou udržet „technologický krok" se svými dětmi, mnohdy se snaží odpovědnost přenést na školu, především s poukazem na hodiny výpočetní techniky. Role školy a školní IT edukace je samozřejmě velmi důležitá, nicméně i kdyby škola mohla kontrolovat veškeré on-line aktivity, není v jejích možnostech monitorovat všechny studenty. Nemůže také v této věci za děti přebírat kompletní zodpovědnost. Stejně jako v případě výchovy je tedy nutné, aby škola udělala maximum v rámci školní výuky a aby rodiče zároveň převzali zodpovědnost za on-line chování dětí i ze své strany. V ideálním případě jsou děti náležitě poučeny ve škole, a pokud rizikový případ nastane, nebojí se tento stav bez obav probírat se svými rodiči.

6.1 Rizikové faktory kyberšikany

V oblasti primární prevence kyberšikany lze využít klasifikace rizikových faktorů: (Kopecký, Szotkowski, 2013)

a) **Individuální faktory** – jedná se o pohlaví jedince, temperament, poruchy emocionality a chování, úzkostlivé a depresivní stavy jedince, zvýšenou impulzivitu, deficity v sociálních oblastech, hostilitu nebo agresi, fyzické i psychické násilí, snížené sebevědomí jedince, jeho traumatické a negativní životní události, problémy ve škole, se zákonem.

b) **Rodinné faktory** – sem nejčastěji řadíme dysfunkční rodiny, zhoršené vazby s rodiči, často neuchopené pouto mezi rodičem a dítětem, nedostatek rodičovské kontroly a dohledu, sníženou rodičovskou podporu dítěte, nedostatečný zájem ze strany rodičů, absence pravidel při používání informačních technologií, nesprávnou výchovu, asociální rodiny, nezaměstnanost rodičů či vážné konflikty v rodině.

c) **Vrstevnické vztahy** – v této kategorii jedinec zmiňuje klasickou šikanu, špatné vztahy s vrstevníky spojené s vrstevnickým nátlakem, přítomnost ve skupině s rizikovým chováním, odmítnutí a vyloučení z vrstevnické skupiny, třídy či jiné oblasti.

d) **Školní faktory** – především nepřístupné a nezdravé školní klima, snížené očekávání pedagogů (deformace), špatné školní podmínky a vztahy mezi učitelem a žákem, ne vždy efektivní školní preventivní programy (neúčinné).

e) **Komunita a společenství** – nízká kvalita organizací pro mládež a vrstevníky, ztráta ekonomických a vzdělávacích záležitostí, nedostatečná nabídka volnočasových aktivit pro jedince v daném regionu.

6.2 Primární prevence kyberšikany

Základním prvkem primární prevence je poskytnutí dovedností a vzorců chování, které povedou děti a mládež k vyvarování se takového rizikového chování. Za podstatu je považováno tvoření zdravých mezilidských vztahů ve skupině. Za rizikové chování nebo sociálněpatolo-

gický jev je považováno takové chování jedince, které si s sebou nese zdravotní, sociální a výchovná rizika pro jednotlivce i společnost, čímž je omezen jeho zdravý vývoj (Čech, Zvoníčková, 2017).

Primární prevence v sobě zahrnuje výchovné, vzdělávací, volnočasové, osvětové a poradenské aktivity, zaměřené na širokou veřejnost. Zcela největší pozornost by měla být věnována účelnému využití volného času u dětí a mládeže (Kopecký, Szotkowski, 2013).

Kyberšikanu lze zařadit mezi základní oblasti rizikového chování, konkrétně mezi šikanu a extrémní projevy agrese (Miovský, 2010).

Dle Národní strategie primární prevence rizikového chování dětí a mládeže 2013–2018 se kyberšikana řadí mezi interpersonální agresivní chování (Kopecký, Szotkowski, 2013).

Pokud chceme účinně a efektivně předcházet kyberšikaně nebo také minimalizovat její dopady, je velmi důležitá všeobecná primární prevence v základních školách. Hlavním cílem je předcházet rizikovému chování. Specifickou primární prevenci zaměřenou na kyberšikanu a její další formy lze realizovat ve formě specifické či nespecifické.

Specifickou primární prevenci řadíme do tří úrovní:

1. **Prevence všeobecná** – ta je zaměřena na celou třídu či školu, bez jakéhokoliv rozdílu. Řadíme sem dlouhodobé preventivní programy, interaktivní besedy a projekty. Účinně lze také téma kyberšikany zahrnout do výuky a spojit tak užitečné s prospěšným ve smyslu účinné primární prevence.
2. **Prevence selektivní** – zaměřuje se na osoby, u kterých jsou ve zvýšené míře přítomny rizikové faktory žáka pro vznik a vývoj různých forem rizikového chování, např. děti z vyloučených lokalit, děti s poruchami chování.
3. **Prevence indikovaná** – zaměřená na situace, kdy se v dané třídě či škole již kyberšikana vyskytla či stále vyskytuje.

Nespecifická prevence je pak plánovitě zaměřena na rozvoj zdravého klimatu ve třídě a škole, posilování dobrých vztahů mezi dětmi a učiteli (Kopecký, Szotkowski, 2013).

6.3 Sekundární prevence kyberšikany

Sekundární prevence je zaměřena na osoby, u kterých je zvýšená pravděpodobnost, že se stanou oběťmi trestných činů nebo sociálněpatologického jednání (Kopecký, Szotkowski, 2013).

Jde o prevenci, která má za cíl ovlivňovat skupiny, kde se již rizikové chování (zmíněná šikana či kyberšikana) vyskytlo. Snažíme se účinně zabránit dalšímu obnovení patologického chování, tedy i páchání kyberšikany (Kraus, Hroncová, 2010). Uskutečňují se zde opatření, která minimalizují riziko, aby se problém opakoval.

Do sekundární prevence řadíme včasnou diagnostiku šikany, bezodkladné vyšetření incidentu, různá pedagogická opatření a samozřejmě také výchovné řešení s agresory. Důležitým prvkem sekundární prevence je léčba nemocné skupiny, včetně výchovné práce s iniciátory, ale také oběťmi šikany. Jelikož je kyberšikana úzce spojená se šikanou, je důležité brát v potaz obě tyto možnosti, se kterými se můžeme setkat. Protože chceme zjistit, zda se šikana či kyberšikana ve školním prostředí opravdu objevuje, existuje hned několik způsobů, které nám pomohou odhalit i skrytou šikanu (Bendl, 2001).

Prvním způsobem pro odhalení je pozorování. Je to základní a nejúčinnější metoda, kterou může pedagogický pracovník využít téměř kdekoli a kdykoli. Je nutno se zaměřit na přímé i nepřímé znaky šikanování. Tuto metodu můžeme využívat například při dozoru na chodbách nebo také při hodině počítačové komunikace, kdy pozorujeme žáky, co na počítači dělají. Existují i různé programy, které tuto funkci umožňují. K odhalení šikany je také možné využít dotazníky. Dotazníky žáci vyplní, a poté je důležité, aby s nimi pracovala odpovědná osoba, která má ve škole kompetence pro řešení incidentů šikany a kyberšikany. Ve velkém případě to jsou pedagogové se specializací školního metodika prevence.

Další metodou je sociometrické měření, kterým můžeme zjistit, jaké jsou sociální vztahy ve skupině a jaké je postavení jedinců ve skupinové hierarchii, což nám napomůže i k odhalení šikany ve zkoumané skupině. Zvýšená pozornost ze strany pedagogů by se ve škole měla věnovat i nově příchozím žákům do tříd. Taktéž by žáci z nižších ročníků měli být v jedné části budovy školy a žáci z vyšších ročníků v druhé části.

Škola by měla být postavena tak, aby se v ní vyskytovalo co nejméně skrytých zákoutí, která by komplikovala kontrolu dětí. Taková místa ve škole jsou totiž lákavým místem pro šikanování (Hrabal, 2002).

6.4 Legislativní ukotvení primární prevence na základní škole

Základní škola zajišťuje kooperaci všech činností souvisejících s poradenskou činností vedení školy. Povinností ředitele školy je poradenskou činností pověřit zpravidla školního metodika prevence nebo také výchovného poradce, kteří poté dostatečně spolupracují s dalšími pedagogickými pracovníky školy. Školní metodik prevence má povinnost spolupracovat se školním psychologem, třídním učitelem a taktéž školským poradenským zařízením.

Každá základní škola musí mít vypracovaný přehled institucí – a to zejména pedagogicko-psychologickou poradnu, neziskové organizace, krizová centra, speciálněpedagogické centrum, středisko výchovné péče pro děti a mládež, orgán sociálně-právní ochrany dětí, Policii České republiky, zdravotnická zařízení nacházející se v určitém regionu, na která se může v případě jakýchkoli problémů obrátit a informovat se (MŠMT, 2017).

Seznam všech těchto kontaktů či regionálních partnerů je vhodné veřejně prezentovat na stránkách školy pro veřejnost, zejména pro děti a rodiče, aby je mohli využít (MŠMT, 2017).

K základním strategickým dokumentům, které jsou s prevencí kyberšikany spojeny, patří zejména: *(MŠMT, 2017)*

- zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů;
- zákon č. 563/2004 Sb., o pedagogických pracovnících a o změně některých zákonů, ve znění pozdějších předpisů;
- Metodické doporučení k primární prevenci rizikového chování u dětí a mládeže čj. 21291/2010-28;
- Metodický pokyn ministryně školství, mládeže a tělovýchovy k prevenci a řešení šikany ve školách a školských zařízeních čj. MSMT-21149/2016;

- Strategie prevence kriminality 2016–2020 (definovaná ve víceletých cyklech Usnesením vlády ČR);
- Národní strategie primární prevence rizikového chování dětí a mládeže na období let 2013–2018.

6.5 Systém prevence na základních školách

Základní školy mají povinnost zajistit bezpečnost a ochranu zdraví svých žáků a zároveň vytvořit podmínky pro předcházení vzniku sociálněpatologických jevů. Tato povinnost je podložena školským zákonem (zákon č. 561/2004 Sb., 2012), konkrétně § 29, který se zaměřuje na bezpečnost a ochranu a zdraví v základních školách České republiky (MŠMT, 2017).

Strategické dokumenty školy upravující prevenci rizikového chování žáků: *(MŠMT, 2017)*

1) vnitřní řád školského zařízení, školní řád;
2) školní preventivní strategie;
3) preventivní program školy (dříve minimální preventivní program);
4) krizové plány.

Základní školy poskytují preventivní a poradenské služby v prostředí školního zařízení prostřednictvím tzv. školních poradenských pracovišť, která jsou definována vyhláškou č. 72/2005 Sb., o poskytování poradenských služeb ve školách a školských poradenských zařízeních, ve znění pozdějších předpisů (Kopecký, Szotkowski, 2013).

Poradenské služby jsou zajišťovány výchovným poradcem, školním metodikem prevence, případně školním psychologem / školním speciálním pedagogem a jejich konzultačním týmem složeným z vybraných pedagogů. Cílem školních poradenských pracovišť je především poradenská podpora zejména žáků, rodičů, ale i pedagogů (Ciklová, 2014).

6.6 Prevence kyberšikany na úrovni základní školy

(Kopecký, Szotkowski, 2013)

- Zařadit do školního řádu pravidla používání ICT, internetového připojení a také mobilů žáků během vyučování a o přestávkách.

- Informovat žáky o netiketě a „listině práv na internetu“. O této listině by měli být informování i rodiče nezletilých žáků, např. k nahlédnutí na webových stránkách škol.
- Instalovat a využívat software, který v učebnách vyučujícímu umožňuje informovat se prostřednictvím svého počítače, co právě žák na své počítačové ploše v daný moment dělá. Informovat o tomto opatření žáky a rodiče, systém nezneužívat!
- Učitelé a zaměstnanci školy by měli být vzorem vhodného užívání informačních a komunikačních médií, zejména při využívání mobilního telefonu v přítomnosti žáků.
- Informovat žáky o rizikovém chování na internetu.
- Definovat kompetence v rámci školy a na akcích konaných školou mimo místo, kde se uskutečňuje vzdělávání.
- Začlenit témata spojená s rizikovým chováním na internetu do výuky.
- Vzdělávat pedagogy v tomto směru.
- Podporovat pozitivní využívání technologií, protože ty nezpůsobují pouze negativní dopady, ale mají i pozitivní vliv na žáka. V dnešní době se každý žák ve svém životě – jak osobním, tak profesním – setká s informačními a komunikačními médii a je důležité umět s nimi bezpečně pracovat.

6.7 Prevence kyberšikany na úrovni jednotlivých pedagogů (Kopecký, Szotkowski, 2013)

- Posilovat vzájemnou empatii mezi žáky jednotlivých tříd.
- Pracovat na klimatu třídy, školy.
- Vést žáky k úctě k druhým lidem.
- Nezapomínat poskytovat žákům pozitivní zpětnou vazbu.
- Vytvářet dobré vztahy mezi žáky i kolegy ve školním prostředí.
- Důsledně a včas zasáhnout vůči individuálním projevům agrese.

6.8 Školní program proti šikanování (MŠMT, 2017)

Každá základní škola si vytváří vlastní program proti šikanování, který je součástí preventivního programu školy. Školní program proti šikano-

vání žáků je nejúčinnější způsob, jak nejlépe ochránit žáky před všemi formami šikany. Zahrnuje v sobě metody řešení a opatření zaměřená přímo na nápravu šikanování. Předpokladem fungování školního programu proti šikanování je všeobecná prevence rizikového chování na základní škole.

Vytvoření školního programu proti šikanování je trvalý a dlouhodobý proces. Základní jsou dva znaky, které tento program určují, první je celkový rozměr a druhým znakem je zaměření na specifickou prevenci.

- Pokud škola chce účinně a hlavně efektivně ochránit žáky před šikanováním, zapojí do tohoto procesu všechny pedagogické pracovníky školy.
- Specifická prevence znamená, že se program zabývá pouze řešením šikany, a to prostřednictvím specifické primární prevence a prevence sekundární.

Školní program proti šikanování má 13 hlavních součástí:

1) zmapování situace – analýza a evaluace (zhodnocení), a to před, po zavedení programu a také v jeho průběhu;
2) motivování pedagogů pro změnu situace;
3) společné vzdělávání a supervize všech pedagogů školy;
4) užší realizační tým (zástupce vedení – nejlépe ředitel, zástupci třídních učitelů z 1. a 2. stupně, zástupce družiny, školní metodik prevence, výchovný poradce, školní psycholog atd.);
5) společný postup při řešení šikanování (šest skupin základních scénářů);
6) primární prevence v třídních hodinách;
7) primární prevence ve výuce;
8) primární prevence ve školních i mimoškolních programech mimo vyučování;
9) ochranný režim (demokraticky vytvořený smysluplný školní řád, účinné dohledy učitelů);
10) pravidelná a efektivní spolupráce s rodiči žáků školy (vhodný způsob seznámení s nekompromisním bojem školy proti šikaně, například na webových stránkách, pomocí informativního dopisu a při třídních schůzkách);
11) školní poradenské služby;

12) spolupráce se specializovanými zařízeními;
13) vztahy se školami v okolí (domluva všech ředitelů na spolupráci při řešení šikany, kdy se jí účastní žáci z různých škol v okolí).

6.9 Programy primární prevence realizované ve školách

Hlavním cílem programů primární prevence je oddálit experimentování s návykovými látkami u dětí a mládeže do pozdějšího věku, popřípadě vedení k tomu, aby ztratily o experimentování zájem vůbec (MŠMT, 2017).

Cílem a smyslem preventivních programů by tedy mělo být:
(MŠMT, 2018)

- podpora zdravého životního stylu;
- zvyšování obranných prvků u dětí: protidrogového vědomí, morálky, sebevědomí a zodpovědnosti za své chování a své zdraví;
- prevence ostatních sociálně nežádoucích jevů, které s užíváním omamných látek souvisejí;
- rozvoj osobnosti: cvičení a učení sociálním dovednostem, vytváření pozitivních vztahů;
- naučit účastníky programů kvalitně využívat volný čas;
- v případě potřeby pomoci řešit již vzniklý problém, případně zprostředkovat pomoc v jiném zařízení.

Abychom docílili co největší efektivity programů primární prevence, je nutné je kombinovat s dalšími formami preventivních aktivit (besedy, diskuse, divadelní představení, workshopy apod.). Díky tomu zvýšíme účinnost preventivní intervence (Miovský, 2015).

Jednou z možností je realizace výukového programu. Výukový program je interaktivní výchovně-vzdělávací lekce, jejímž cílem je upevnění, prohloubení a rozšíření učiva všech stupňů škol v souladu se školními vzdělávacími programy (viz tab. 1).

Tabulka 1 – Typologie programů primární prevence	
SKUPINA 1 **Programy zaměřené na rozvoj životních dovedností**	**SKUPINA 2** **Programy zaměřené na intrapersonální rozvoj**
Programy zaměřené na rozhodovací schopnosti	Programy zaměřené na uvědomování si hodnot
Programy zaměřené na zvládání úzkosti a stresu	Programy zaměřené na stanovování cílů
Programy zaměřené na nácvik (rozvoj) sociálních dovedností	Programy zaměřené na budování pozitivního sebehodnocení
Programy zaměřené na nácvik dovedností odolávat tlaku	Programy zaměřené na stanovování norem
	Programy spojené se složením přísahy
	Programy informativní
	Programy vrstevnické
	Programy pro rodiče

Zdroj: Miovský (2015)

Ve vztahu ke kyberšikaně je vhodné zařazovat programy zaměřené na intrapersonální rozvoj:

Programy zaměřené na stanovování norem

Tento typ programu vychází z předpokladu, že mladí lidé mají často mylné představy o rozšířenosti rizikových typů chování a jejich společenské i individuální přijatelnosti. Jejich záměrem je ovlivnit začátek těchto jevů zmírněním představ o očekávaném výskytu a četnosti a o přijatelnosti sledovaných typů rizikového chování. Výsledkem by pak mělo být stanovení pevných norem ve vztahu k rizikovým formám chování (MŠMT, 2005).

Programy informativní

Tyto programy jsou zaměřené na předávání informací o dopadech rizikového chování. Jejich cílem je zvyšovat znalosti cílové skupiny o rizikovém chování (formách kyberšikany), o faktech a mýtech, které jsou s jednotlivými typy rizikového chování spojeny. Pozornost se věnuje negativním, ale i pozitivním dopadům rizikových typů chování tělesného a psychického zdraví i sociálního prostředí jedince. Informace se nejčastěji zaměřují na popis problémového chování, jeho rozdělení a typy,

na příčiny, které vedou k rozvoji rizikových typů chování a na historické a právní souvislosti. Tyto programy mají různé podoby, nejčastěji se realizují: běžná forma výuky, promítání filmů a videopořadů, diskuse, besedy. Sdělování informací by mělo být doplněno diskusí, v jejímž rámci by se pořádající osoba měla snažit doplnit a pozitivním způsobem ovlivnit znalosti o rizikovém chování a o jeho následcích (Miovský, 2015).

Programy vrstevnické (peer programy)
Specifikem tohoto typu programů je zapojení vrstevníků (z angl. peer = vrstevník), kteří vystupují v roli poučeného člověka stejného postavení v oblasti rizikového chování. Peer program poskytuje svým vrstevníkům pravdivé informace o rizikovém chování a umí nabídnout psychosociální podporu ohroženým jedincům ve skupině. Je vnímavý k dění ve skupině a všímá si problémového chování, na které umí upozornit kompetentní osoby (např. školního metodika prevence, školního psychologa, lékaře aj.). Nejedná se však v žádném případě o „donášení", ale díky bezprostřední znalosti skupiny o včasné upozornění na problém (včasná diagnostika), který je možno v jeho zárodku řešit odpovídajícími zásahy v zájmu žáka nebo (třídního) kolektivu (Miovský, 2015).

7 Role rodičů, školy a dětí ve vztahu ke kyberšikaně

Mějte na paměti, že drtivá většina dětí opravdu neřekne svým rodičům, že se staly obětí šikany nebo kyberšikany! Příčin bychom našli celou řadu, např. obavu dítěte ze ztráty přístupu k zařízení a přístupu k internetu, obavu z přehnané reakce rodičů, kteří budou okamžitě jednat a kontaktovat školu nebo rodiče šikanujícího. Některé děti dokonce šikanu nerozpoznají a dávají vinu samy sobě. Jakmile však zpozorujete známky šikany, pak je nutné o celé věci začít mluvit.

7.1 Role rodičů

Pokud máte podezření, že se dítě stalo obětí kyberšikany, zkuste se zaměřit na následující podezřelé chování:

- dítě vykazuje známky nervozity ve chvíli, kdy mu přijde textová/on-line zpráva nebo e-mail;
- pozorujete změny ve využívání chytrých zařízení, dítě se jim vyhýbá, nebo je naopak užívá nadměrně;
- dítě se vyhýbá školní docházce a hledá výmluvy, proč nejít do školy;
- dítě si před vámi více chrání své chytré zařízení nebo se zjevně snaží tajit svou on-line aktivitu;
- děti se odtahují a „vzdalují“ od svých přátel a rodiny;
- objevují se fyzické symptomy, jako jsou poruchy spánku, bolesti břicha a hlavy, úbytek na váze apod.;
- dítě zaostává ve škole nebo se mu výrazně zhoršuje prospěch;
- dítě vykazuje známky frustrace, vzteku, smutku, obzvláště před/po použití svého on-line zařízení;

- dítě si smazalo svůj profil na sociální síti nebo svůj e-mail, přestává používat telefon.

Děti, které kyberšikanu provádějí jiným, vykazují tyto prvky chování:

- rychle přepínají obrazovku nebo vypínají program, vstoupí-li další osoba do místnosti;
- používají zařízení v pozdních večerních nebo i nočních hodinách;
- jsou nervózní nebo se rozčilují v případě, že nemají přístup k technice nebo k internetu;
- vyhýbají se diskusím o tom, co dělají on-line;
- používají více uživatelských účtů nebo používají účty, které nejsou jejich.

V případě, že se dítě stane obětí kyberšikany, tak je nejdůležitější rolí rodiče ujistit svého potomka, že je v naprostém bezpečí a že mu rodina poskytne v této věci plné pochopení a podporu. Rodiče musí svými slovy i činy dítě ubezpečit, že je v zájmu všech tuto situaci vyřešit a že tato záležitost zásadně neovlivní kvalitu života dítěte. Dítě je nutné vyslechnout, věnovat mu pozornost a celá situace nesmí být podceněna! Dítě nesmí mít pocit, že svěřením se rodičům celou situaci ještě zhorší! Je vhodné, pokud rodič v této situaci dále kontaktuje školu pro diskusi tohoto problému; může také kontaktovat rodinu „útočníka" ve snaze najít vhodné a klidné řešení. Dále je možné požádat internetového poskytovatele nebo telefonního operátora o spolupráci při stažení nevhodných on-line příspěvků, případně kvůli některým důkazním materiálům, pokud je to nutné. Účast policie pak může být nutná v případě fyzického napadání nebo při závažných případech kyberšikany.

U role rodičů je však nutné zmínit především jednu zásadní věc. Rodič je v drtivé většině případů tím, kdo dítěti nějakou chytrou technologii (notebook, tablet, telefon) zakoupil. Měl by tedy zároveň dbát na co nejbezpečnější používání této „hračky". Dnešní technologie mají ve většině případů rodičovské zámky a jiné technologie, které umožňují výrazně redukovat rizika plynoucí z užívání těchto prostředků v on-line prostředí. Děti musí být před jejich používáním zároveň důsledně poučeny o správném užívání nového zařízení a také o rizicích, která mohou existovat. Toto je asi nejzásadnější část, která je právě rodiči podceňována, částečně také z důvodu, že rodiče sami neumějí tuto novou

techniku používat, jak jsme již uvedli výše. Poučení však mohou být podobná jako v „off-line“ světě, tzn. nedůvěřovat nikomu, koho neznám, nebavit se s cizími lidmi, nedávat nikomu svoji adresu apod. Příkladů bychom jistě nalezli celou řadu. U velmi malých dětí je vhodná kontrola jejich zařízení, nicméně obecně bychom nikdy neměli špehovat aktivitu dětí na internetu. Ta může být omluvitelná až v případě, že máme silné podezření na ohrožení dítěte. Komunikace, osvěta a případná kontrola s vědomím a souhlasem dětí vytváří vzájemnou důvěru, šmírování tabletu nebo telefonu dětí může naopak vyvolat silnou nedůvěru a uzavření se dítěte v další komunikaci s rodičem. Jak čas plyne, tak je přirozené, že rodiče dávají dětem stále více a více svobody, soukromí a zodpovědnosti, nicméně komunikace mezi rodičem a dítětem v této věci by měla zůstat otevřená. Je vhodné o rizicích mluvit, stejně jako např. o případech z okolí či ze světa, které se staly. Tyto příklady pomohou dětem pochopit rizika, která by si jinak ani nemusely uvědomovat.

Rodiče musí být při nastavování a hlídání pravidel především na začátku důslední, v případě jejich porušení to nemůže rodič nechat jen tak být. Pokud se rodič dostane do obrácené situace a zjistí, že jeho dítě šikanuje jiné, musí mu umět vysvětlit, že jiným tak způsobuje stejnou škodu, bolest a újmu, jako kdyby toto chování prováděl v reálném, nevirtuálním prostředí. Pokud dítě šikanuje jiné, neznamená to automaticky, že je zlé. Jen si nemusí uvědomovat důsledky a dopady svého chování, děti také nemají ještě dostatečně vyvinutou empatii a dělají více chyb. Dítě si však musí odnést za své jednání přiměřený postih, který je závislý na míře škody, např. jak si byl šikanující schopen uvědomit následky svého činu nebo zda byla šikana opakovaná nebo stupňovaná. Rodiče se pak musí více zaměřit na práci se svým dítětem a být na pozoru, aby se situace neopakovala.

7.2 Role školy

Hlavní rolí školy je bezpochyby edukace a školní programy se zaměřením na správné využívání internetu. Studenti musí vědět, že žádná forma šikany není akceptovatelná a že jakékoli obtěžování nebo vyhrožování bude mít pro útočníka vážné následky. Je tedy nutné tyto informace implementovat jak do běžné výuky, tak především v IT předmě-

tech, kde je možné jít více do hloubky. Vhodné je i začlenění do školního řádu, sledování nových potenciálních hrozeb nebo pravidelná účast na školeních s tímto tématem.

Jak již bylo řečeno, žáci si musí být vědomi, že jakákoli forma šikany je nepřípustná. Měli by dostat informaci, že každý takový případ bude důsledně prošetřen a viník náležitě potrestán. Podle závažnosti může jít o udělení snížené známky z chování nebo v krajních případech dokonce vyloučení ze školy. Škola musí být připravena řešit případy šikanování jak s rodiči obětí, tak s rodiči šikanujících a dát všem najevo, že boj s kyberšikanou nepodceňuje. Pokud chce být škola více proaktivní, může vymyslet svoje strategie a programy pro boj se šikanou, zapojit starší studenty, kteří mohou mladším žákům poskytnout svoje zkušenosti a doporučení s používáním telefonů a tabletů. Pokud škola zapojí své vlastní žáky do těchto programů a zapojí je aktivně do řešení a prevence, pak jim projeví důvěru, vytvoří na škole pozitivní klima a výrazně tak sníží rizika kyberšikany na své půdě. Šikana obecně má přímou souvislost se spokojeností a bezpečností ve škole, s příznivým klimatem školy a s přístupem učitelů vůči žákům.

7.3 Role žáka/dítěte

Jednou z nejdůležitějších věcí, která vytváří pocit bezpečí u dětí, je alespoň jeden komunikačně zdravý a důvěryhodný vztah s dospělým (optimálně se svým rodičem). Dítě musí mít jistotu, že může bezpečně mluvit o svých nepříjemných on-line (ale i off-line) zkušenostech a zážitcích. Pokud se setká s mírnější formou šikany, je vhodné poradit se s dospělým na řešení problému, než na něj okamžitě a v afektu reagovat, čímž může dojít k jeho zhoršení nebo eskalaci. Dítě by mělo mít své on-line zařízení zároveň co nejlépe zabezpečené pro případ ztráty/krádeže, musí mít kvalitní hesla do svých účtů a profilů, zařízení nemá půjčovat nebo se na jiných (cizích) zařízeních do svých účtů přihlašovat. Vše výše uvedené výrazně sníží možná rizika. Pokud i tak dojde k ohrožení např. formou výhrůžek, je potřeba ponechat konverzaci jako důkaz a nemazat ji z důvodu studu, obav apod. Pokud rodič nebo škola dokáže ze zařízení vyčíst podstatu hrozby, datum a čas odeslání a další data, může to významně přispět k odhalení útočníka a k zamezení dalších škod. Je

třeba mít na paměti i nebezpečí veřejného odhalení identity útočníka, který se pak sám může stát šikanovaným ze strany spolužáků. Jak jsme již zmínili, za mnohou šikanou nestojí zlé úmysly, ale pouze nedostatečné informace a povědomí o tom, co mohu ostatním způsobit. „Útočník" se pak může dostat do situace, kdy celá věc měla mnohem širší dopad, než předpokládal, sám pak může mít ze svého činu špatné svědomí nebo psychické problémy. Zde je opět namístě mít možnost celou situaci konzultovat s dospělým, kterému dítě věří.

Role žáka má ještě jednu důležitou rovinu. Celá řada dětí se dostane do situace, kdy nejsou obětí ani útočníkem, ale jsou svědky kyberšikany. Svědek takového činu pak neví, jak se správně zachovat, aby neublížil oběti, často se také bojí toho, že pokud útočníka prozradí, sám se pak stane jeho obětí. Dítě navíc často není schopné rozeznat hranici, která je mezi šikanou a běžným popichováním mezi dětmi. Pokud však dítě zjistí, že něco není v pořádku, nemělo by být jen pasivním přihlížejícím. Přehlížením situace totiž v podstatě podporuje chování útočníka. Dítě, které se stalo obětí šikany, často hledá pomoc v prostředí kolem sebe, cítí se bezbranně a hledá záchranu a oporu i mezi svými vrstevníky. Je obrovský rozdíl, jestli svědek události reagovat bude, či nikoliv. Pokud se na to cítí, může se šikanovaného zastat přímo na místě (zde výrazně záleží na dané situaci), případně celou věc řešit s dospělým, rodičem nebo učitelem, kterému důvěřuje. Žák by ale nikdy neměl jít do přímého nebo dokonce ostrého střetu s útočníkem, neměl by mu oplácet stejnou měrou, vysmívat se mu před celou třídou nebo se jinak za šikanovaného mstít.

8 Strategie řešení kyberšikany

Postup, jak se zachovat, pokud dojde ke styku s kyberagresorem, může mít mnoho podob. Velmi důležitá je pomoc rodičů a pedagogů, když rodiče zjistí, že je jejich dítě ohroženo šikanou či kyberšikanou, musí začít situaci řešit, dítě musí vědět, že mu důvěřují a podporují ho. Nejdůležitější je ukončit komunikaci s agresorem, nereagovat a neodpovídat na jeho útoky, rovněž důležité je nesnažit se útok vrátit a zabránit tomu, aby se agresor dostal k dítěti. Pokud jsou k dispozici nějaké důkazy, vše se má uchovat pro pozdější řešení s policií, protože často rodiče berou tento problém na lehkou váhu a nevyhledají pomoc například v pedagogicko-psychologické poradně (Ševčíková a kol., 2014).

8.1 Strategie řešení z pohledu oběti

Před jednorázovou kyberagresí či rozvinutou kyberšikanou neexistuje žádná stoprocentní kyberochrana, dokonce ani to, když kybernetická oběť přestane navštěvovat či využívat internetové nebo sociálně komunikační či mobilní služby, útok nedokáže zastavit. Oběť pouze netuší, že v prostředí internetu dochází k útokům na její osobu. Je potom jen otázkou času, kdy se to oběť dozví od svých přátel či od rodiny. Vyrovnání se s kyberšikanou z pohledu oběti lze rozdělit do dvou základních skupin – reaktivní a preventivní strategie.

Do reaktivní strategie (vyrovnání se oběti s kyberšikanou) řadíme vyhýbání se, to znamená vymazání zpráv z mobilního telefonu nebo sociálních sítí a komunikačních médií, smazání celého účtu, blokace tele-

fonních čísel nebo ignorování útoků. Dále je to přijetí, to znamená, že je kyberšikana vnímána jako součást jedince a bere ji jako součást svého života. Dále je to ospravedlnění, oběť hledá důvody, proč není důležité se kybernetickými útoky zabývat, další možností je „shazování agresora" – nestojí za to, abych se trápil aj., dále vyhledání podpory v okolí, oběť se svěří blízké osobě.

Mezi preventivní strategie patří osobní promluva, to znamená snaha předejít nepochopení způsobenému on-line prostředím, zabezpečení a zvyšování povědomí o kyberšikaně – zabezpečení svých soukromých účtů, omezování zveřejněných informací ke své osobě na sociálních sítích a internetu (Černá et al., 2013).

Vhodný postup pro oběť kyberšikany: *(MŠMT, 2017)*

1. **Důležité je zachovat klid** – nejednat zbytečně rychle, nerozvážně a ukvapeně.
2. **Uschovat si všechny důkazy** – uchovat a uložit si veškeré důkazy kyberšikany (ať už to jsou SMS zprávy, e-mailové zprávy, zprávy z chatu), uložit si webové stránky, fotografie, využít možnost programů na zachycení obrazovky. Na základě těchto důkazů může být proti útočníkovi či útočníkům zahájeno vyšetřování policií.
3. **Ihned ukončit komunikaci s pachatelem** – nijak nekomunikovat s útočníkem, nesnažit se ho žádným způsobem odradit od jeho počínání, nevyhrožovat mu, nemstít se.
4. **Blokovat pachatele a blokovat obsah, který rozšiřuje** – pokusit se zamezit útočníkovi přístup k účtu nebo telefonnímu číslu oběti, a je-li to v dané situaci možné, i k nástroji či službě, skrze niž své útoky realizuje (kontaktovat poskytovatele služby ICT, například sociálních sítí).
5. **Identifikovat pachatele** (pokud to neohrozí oběť a je to v daném případě možné).
6. **Oznámit útok dospělým** (nejlépe dospělému, učiteli, rodiči) – svěřit se blízké osobě, které důvěřujeme. Pro uchování důkazů oslovit někoho, kdo má vyšší ICT gramotnost. Kontaktovat školu a specializované instituce (pedagogicko-psychologickou poradnu, Policii ČR, středisko výchovné péče, intervenční služby specializující se na řešení kyberšikany, psychology apod.).

7. **Nebát se vyhledat pomoc u specialistů** – kontaktovat specializované organizace, poradny, případně Policii ČR.
8. **Žádat konečný verdikt** (v případě řešení situace školou) – po prošetření celého případu trvat na konečném stanovisku všech zapojených a spolupracujících institucí.

8.2 Strategie řešení z pohledu školy

Protože je kyberšikana velmi úzce propojena s tradiční šikanou, která se ve škole běžně vyskytuje, je kyberšikana ve školním prostředí také řešena. Před řešením se však škola často rozhoduje, zda se může, či musí do řešení těchto situací zapojit, či nikoliv. Škola musí řešit všechny případy šikany a kyberšikany, je to její povinnost.

Škola by se kyberšikanou měla zabývat vždy, když se o ní dozví: (MŠMT, 2017)

K nejčastějším argumentům proti řešení kyberšikany školou řadíme:
(Krejčí, 2010)

1. Když kyberšikana probíhá mimo budovu školy (či mimo školní akci), není to problém naší školy.
2. Řešení kyberšikany ve škole vyvolá negativní reklamu a odradí potenciální budoucí žáky a rodiče.
3. Škola nemá žádné nástroje, jak kyberšikanu řešit.
4. Nástroje škola sice má, používá je, ale nefungují na žáky/rodiče.
5. Kyberšikana sama zanedlouho odezní, nemá tedy smysl ji ve školním prostředí nijak řešit.

K nejčastějším argumentům pro řešení kyberšikany školou řadíme:
(Krejčí, 2010)

1. Kyberšikana často doprovází i jiné druhy šikany, které se dějí ve školách. Škola se musí starat o své prostředí a školní klima, musí zajistit práva dětí i zaměstnanců (např. právo na vzdělání, právo na pracovní podmínky atd.).
2. Dle počtu obětí kyberšikany či souvisejících forem kybernetické agrese s ní mají problém téměř všechny základní školy. Škola, která

řeší problémy, jež se v jejím prostředí vyskytují, postupuje správně a zajišťuje si tak dobrou publicitu/reklamu.
3. Škola může postupovat stejně jako při řešení tradiční šikany – kyberšikana s tradiční šikanou souvisí a je s ní velmi často úzce spojena.
4. Pokud nástroje pro řešení kyberšikany ve škole nefungují, je třeba konzultovat individuální problém žáka např. s odbory sociálně-právní ochrany dětí, Policií ČR, specializovanými poradnami a situaci neprodleně řešit.
5. Pokud nebudeme kyberšikanu řešit, dáváme žákům, kteří o kyberšikaně vědí, signál, že mohou kyberšikanu nadále páchat také a nebudou za ni nikdy potrestáni. Tímto způsobem v nich budujeme negativní vzorce chování, které pak mohou předávat svým dětem.

Primárním úkolem školy je identifikace konkrétního případu žáka/žáků. Při řešení různých případů kyberšikany lze využít „Scénáře" * pro obyčejnou počáteční šikanu. Kyberšikana může probíhat v uzavřeném prostředí jak ve škole, tak i doma, proto je důležité chránit oběť nejen ve školním prostředí (Kolář, 2011).

Povinnosti školy

1. Podpořit oběť a zajistit bezpečí

K základním krokům, které by měla škola zajistit, řadíme zejména uklidnění oběti. Škola (učitel, metodik prevence) by měla oběti nejprve nabídnout podporu. Některé reakce mohou být přehnané, jelikož je oběť rozrušená. Ihned poté je důležité zamezit tomu, aby kyberšikana ve školním prostředí dále pokračovala. To znamená co nejdříve odstranit nevhodný obsah z internetu, který byl použit ke kyberšikaně – smazání fotografií, videí nebo zablokování profilu útočníka/agresora. Tento postup je nejlepší provádět s ICT odborníkem, který těmto materiálům rozumí a ví, jak ho z internetu efektivně smazat; popřípadě kontaktovat poskytovatele dané internetové služby.

---

* Metodický pokyn Ministerstva školství, mládeže a tělovýchovy ČR k řešení šikanování ve školách a školských zařízeních, čl. 7.2. Dva scénáře pro každou školu (podrobněji viz metodické doporučení).

2. Zajistit co nejvíce důkazních materiálů

Dalším krokem je zajistit co nejvíce důkazních materiálů, které pak budou nutné k vyšetření celé situace daným subjektem. Předtím, než budou prostředky z on-line služby smazány, je třeba využít funkci snapshot, která dokáže zachytit to, co zrovna vidíme na monitoru počítače či na obrazovce mobilního telefonu. Dále je důležité stáhnout dané internetové stránky do počítače, zajistit seznam žáků, kteří tvořili publikum při kybernetickém útoku, například v určitých skupinách na sociálních sítích. Ideální je uložit i jejich odkazy na osobní profily a pokusit se identifikovat agresora, pokud je to možné.

Pokud se jedná o veřejné diskuse, je získání důkazů mnohem jednodušší, protože přístup do těchto veřejných skupin má každý uživatel dané služby. Bohužel je i velké množství případů, ve kterých agresoři zakládají skupiny uzavřené a soukromé, do kterých není možné bez povolení agresora vstoupit. Vstup do těchto skupin je umožněn pouze pozvaným uživatelům (žákům). V rámci uzavřeného prostředí se poté realizuje kyberšikana. V těchto případech je nutné zvolit variantu kontaktování odborné instituce, např. pracovníky projektu E-bezpečí nebo také v krajní nouzi kriminalisty oddělení informační kriminality Policie ČR, která zajistí potřebný důkazní materiál specifickou cestou, kterou je možné v těchto případech využít. Získaný a uchovaný důkazní materiál bude posléze využit v rámci individuálního vyšetřování policie nebo také při komunikaci s rodiči agresora a oběti. Velmi důležité je však zajistit bezpečí všech svědků – nemělo by být jasné, kdo a jak napomohl k tomu, aby byl důkazní materiál získán.

3. Incident je nutné vždy vyšetřit

Veškeré případy je nutné důkladně prošetřit. Pokud škola není schopna incident sama vyšetřit, může využít podpory externích institucí, které jí poradí další postup. Ve vyšetřování je zahrnuto, kde daný incident probíhal, jak dlouho trval, kdo se do něj zapojil (kteří žáci), jaký dopad měl tento incident na oběť a jakými prostředky škola útok zastavila.

4. Informovat rodiče oběti i agresora

O daném incidentu je nutné informovat jak rodiče oběti, tak i rodiče agresora. V tomto případě je doporučeno využít postupy definované ve scénáři řešení tradiční šikany. Škola by měla poučit rodiče o tom, jaký

bude zvolen postup řešení na úrovni školy, popřípadě o tom, že daný incident/případ nespadá do kompetencí školy a že je možné využít právních služeb. V případě, že incident nespadá do kompetencí školy (může se jednat například o útok mimo vyučování a nemá žádnou návaznost na šikanu, která se odehrává ve škole), mohou rodiče např. zažalovat daného agresora.

5. Zkonzultovat řešení s dalšími institucemi
Jsou případy, ve kterých je vhodné zvolit postup řešení a zejména zvolený postup s dalšími subjekty. Například se jedná o zřizovatele školy, Českou školní inspekci a další. Česká školní inspekce ale není pověřena metodickým vedením (její kompetence jsou jasně vymezeny školským zákonem). V mnoha případech škola totiž nepostupovala správně a žákům např. navrhla sníženou známku z chování v situacích, které jasně a prokazatelně neprobíhaly v době školní výuky ani při aktivitách v rámci školy.

6. Žádat konečný verdikt a informace
Po vyšetření celého incidentu je nutné trvat na konečném verdiktu všech zapojených institucí – ať už se jedná o Policii ČR, orgán sociálně-právní ochrany dětí, pedagogicko-psychologickou poradnu a další subjekty.

7. Zvolit odpovídající opatření
Důležité je, aby škola při trestání individuálních agresorů postupovala v souladu se školním řádem v kombinaci s dalšími strategickými dokumenty školy (např. krizový plán školy, školní preventivní program). Při určení trestu využíváme možnosti, které jsou nabízeny ve scénáři pro řešení tradiční šikany (Kolář, 2011). Pokud je forma kyberšikany méně závažná, doporučuje se využít neformálního řešení. Můžeme zvolit metodu vytvoření sady preventivních materiálů z oblasti rizikového chování na internetu, připravit pro žáky přednášku o důležitosti odpovědného používání moderních komunikačních médií (MŠMT, 2017).

8. Realizovat preventivní opatření
Velmi důležité je, aby se kybernetický incident v budoucnu neopakoval, proto je nutné zajistit preventivní opatření. Jeden z mnoha způsobů

je možný prostřednictvím realizace projektových dnů zaměřených na prevenci, přípravou materiálů na podporu prevence nebo také v rámci výuky využít metodu hraní rolí a také posilování dobrých vztahů mezi žáky. Tyto uvedené kroky umožňují účinně minimalizovat dopad incidentu na oběť, zajistit potrestání agresora a zvýšit šanci, že se incident v budoucnu již nebude opakovat. Tento postup je však pro každého jedince individuální, některé jednotlivé kroky se mohou udělat dříve či později. Je důležitá aktivní spolupráce školy s rodinou oběti i agresora, taktéž i s konkrétní třídou, ve které k incidentu došlo (MŠMT, 2017).

Základní možnosti a limity školy

Každá škola má odpovědnost za děti a žáky. V souladu s ustanovením § 29 zákona č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů, jsou školy a školská zařízení 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 rizikového chování (kyberšikany). Z tohoto důvodu pedagog musí šikanování mezi žáky neprodleně řešit a každé jeho oběti ihned poskytnout pomoc.

Škola či školské zařízení má odpovědnost za děti a žáky v době vyučování a školních akcí, a to podle § 391 zákona č. 262/2006 Sb., zákoník práce a podle Pracovního řádu pro zaměstnance škol a školních zařízení, např. čl. 2 (vyhláška č. 263/2007 Sb., 2007) a odpovídá i za škodu způsobenou žákům v době vykonávání přechodného dohledu, tj. při vyučování a v přímé souvislosti s ním (Kopecký, Szotkowski, 2013).

Při stanovení základních kompetencí při řešení kyberšikany je třeba zjistit, zda jednání souvisí s činností školy, zda se incident týká žáků či zaměstnanců školy a zároveň zda má výrazně negativní dopad do školního klimatu nebo zda takové narušení intenzivně a bezprostředně v tomto případě hrozí (MŠMT, 2017).

Pokud toto narušení hrozí, tak je nutné, aby škola postupovala v těchto bodech: *(MŠMT, 2017)*

- Škola pomůže oběti zajistit veškeré dostupné důkazy.
- Škola postupuje podle krizového plánu, který je stanoven.

- Školský zákon definuje formulaci zvlášť závažného porušení školského zákona, kdy je ředitel školy povinen v uvedeném případě žáka střední školy vyloučit. Jde o hrubé a opakované slovní či fyzické projevy násilí na ostatních žácích nebo také na učitelích školy. V případě žáků, kteří by se dopustili takového zvlášť závažného porušení školského zákona a kteří ještě plní povinnou školní docházku, oznámí ředitel školy incident odboru sociálně-právní ochrany dětí. Ten pak musí případ neprodleně řešit. Současně je v obou případech ředitel povinen nahlásit takové chování také státnímu zastupitelství, které bude postupovat v rámci svých kompetencí a situaci začne řešit dle vlastních postupů.
- V závažnějších případech kyberšikany (jelikož kyberšikana naplňuje skutkovou podstatu trestného činu) škola neprodleně kontaktuje Policii ČR a orgán sociálně-právní ochrany dětí (povinnost).
- Škola informuje všechny zasažené žáky o výsledcích šetření ve škole a udělených trestech agresorům.
- V případě řešení jednotlivých situací lze využít také metodickou pomůcku MŠMT obsahující anonymizované případy a možnosti jejich řešení, které jsou dostupné na internetových stránkách.

Pokud k ohrožení nedojde, není možné, aby škola udělovala kázeňské tresty (snížené známky z chování, jelikož se incident nestal během výuky ani v rámci školní akce, ani v případě, kde učitel dohlíží na žáky – exkurze, kurzy atd.).

To ovšem neznamená, že škola nemusí kyberšikanu řešit alespoň v těchto základních bodech: *(MŠMT, 2017)*

- Zajistit veškeré informace o tom, kterých tříd se incident kyberšikany týká. Ve všech zasažených třídách je nutné provést sociometrii. Sociometrické metody, u nichž je to vyžadováno, musí provádět proškolený pracovník. Dále by škola měla postupovat dle zpracovaného krizového plánu.
- Doporučit rodičům oběti, aby se v případě kyberšikany svého dítěte obrátili na Policii ČR, popřípadě podali žalobu k soudu.
- Doporučit rodičům, aby se v případě kyberšikany svého dítěte obrátili na specializovanou instituci – je několik možností (Linka bezpečí, dětské krizové centrum či pedagogicko-psychologická poradna).

V závažnějších případech rodičům doporučit kontaktovat Policii ČR a rovněž orgán sociálně-právní ochrany dětí.

- Rozhodně informujte (se souhlasem zletilého žáka nebo zákonného zástupce žáka nezletilého) všechny zasažené žáky o postupu při řešení kyberšikany. Sdělte jim, že škola trestat v tomto případě nemůže, a proto byl případ předán policii/soudu. Žáci musí vědět, že za každé nepřiměřené a nezákonné chování přijde trest.

Ohlašovací povinnost školy při výskytu šikany a kyberšikany

Pokud dojde k šikaně či kyberšikaně v průběhu vyučování, s ním souvisejících činností anebo při poskytování školských služeb, má škola povinnost tuto skutečnost oznámit zákonnému zástupci jak žáka, který byl útočníkem (agresorem), tak žáka, který se stal obětí. Tato povinnost vyplývá ze školského zákona (§ 21 odst. 2 školského zákona, podle něhož mají zákonní zástupci dětí a nezletilých žáků právo mj. na informace o průběhu a výsledcích vzdělávání dítěte či žáka a právo vyjadřovat se ke všem rozhodnutím týkajícím se podstatných záležitostí jejich vzdělávání) (MŠMT, 2017).

1. Škola ohlašuje orgánu sociálně-právní ochrany dětí takové situace, které nasvědčují tomu, že dítě je v ohrožení buď proto, že ho ohrožuje jiná osoba, nebo proto, že se ohrožuje svým chováním samo (viz § 6, 7 a 10 zákona č. 359/1999 Sb., o sociálně-právní ochraně dětí, ve znění pozdějších předpisů); v případě šikany se jedná o všechny případy, které škola oznámila policejnímu orgánu nebo státnímu zástupci, a dále případy, které výše uvedeným nebyly oznámeny i navzdory tomu, že se stalo něco závažného, protože nebyl zákonný důvod.
2. Pokud dojde v souvislosti se šikanou k jednání, které by mohlo naplňovat znaky přestupku nebo trestného činu, obrací se škola povinně na Policii ČR. Trestní oznámení je možné podat také na státní zastupitelství. Tuto skutečnost oznámí ředitel školy nebo jiná pověřená osoba jakoukoliv formou (písemně, telefonicky či osobně) na Policii ČR, v ideálním případě přímo specialistovi na problematiku mládeže Služby kriminální policie a vyšetřování těchto činů.
3. V případě závažnějšího stupně šikany či kyberšikany by měl být informován také zřizovatel školy, ve které se incident odehrál (MŠMT, 2017).

8.3 Jak pracovat se žákem, který se stal obětí kyberšikany

Tato kapitola se zabývá tím, jak efektivně pracovat se žákem, který se stal obětí kyberšikany. Tento postup lze využít i pro žáka, který se stal obětí klasické šikany. Je důležité dodržet všechny kroky, aby se žák dokázal s touto negativní zátěží vyrovnat. Ve vážnějších případech je důležité, aby se žákem promluvil odborník, který dle svých postupů dokáže se žákem pracovat, aby se žák neuzavřel a v budoucnu netrpěl traumaty či častou depresivní poruchou, která u těchto obětí není neobvyklá, aby zákonní zástupci (rodiče) spolu se školou spolupracovali a společně se podíleli na úspěšné adaptaci žáka do třídy mezi spolužáky. V tomto případě je velmi důležité poskytnout dítěti podporu a dodržet zcela diskrétnost před ostatními.

Velmi důležitá je podpora

V tomto případě je na prvním místě důležitá podpora postiženého člověka (oběti). Je důležité zdůraznit mu, že udělal velice správnou věc, když útoky kyberšikany ohlásil někomu jinému. Rovněž je důležité, aby s dítětem pracoval odborník, který ví, jak na ně působit. Jsou to školní metodici prevence či výchovní poradci. Také je důležité, aby se o celé situaci dozvěděli rodiče, pokud to nebyli právě oni, za kterými dítě přišlo, že se stalo obětí kybernetického útoku (E-bezpečí.cz, 2018).

Doporučení, jak správně postupovat dál

V některých případech se může stát, že se žák chce agresorovi mstít a oplatit mu kybernetické útoky, se kterými se jako oběť sám setkal. Dítěti je dobré vysvětlit, že se nemá mstít, neposílat odesílateli žádné podobné SMS zprávy či odpovídat na různé konverzace na různých komunikačních serverech. Poraďte dítěti, aby si všechny důkazy uchovalo pro vyšetřování. Aby například nesmazalo zprávu, kterou od agresora obdrželo, taktéž aby si pořídilo snímek obrazovky nebo sdělilo internetovou stránku, kde se objevil případ v internetové komunikaci. Ujistíme se, že dítě rozumí jednoduchým způsobům, jak zabránit tomu, aby k útoku nedošlo znovu. Základem je, aby si změnilo své internetové kontaktní údaje, zablokovalo kontakty, které mu vyhrožovaly, smazalo

či zrušilo si účet na sociální síti, zabezpečilo si svůj osobní profil, aby nebyly jeho údaje veřejné cizím lidem, nebo opustilo chatovací místnost, kde se incident kybernetického útoku odehrál (E-bezpečí.cz, 2018).

Všechny případy kyberšikany je důležité prošetřit a nebrat kybernetické útoky na lehkou váhu

Všechny kybernetické útoky týkající se kyberšikany (šikany) musí být náležitě zaznamenány a prošetřeny patřičným orgánem. V některých závažných případech mohou být některé incidenty považovány za trestný čin. První, čím musíte začít, je posoudit, zda se skutečně jedná o kybernetický útok. Jak již je psáno v předchozím odstavci, je důležité, aby byly všechny důkazy adekvátně uchovány pro případ vyšetření policií. V případně závažných, opakujících se a intenzivních útocích na oběť je důležité na nic nečekat a kyberšikanu okamžitě začít řešit. V případě urážlivého obsahu na internetových stránkách, který je považován za útoky kyberagresorem, lze kontaktovat servisní poskytovatele a policii. V tomto případě příslušné orgány dokážou urážlivý obsah internetu odstranit dříve, než když obsah pouze nahlásíme. Jelikož případů, než se poskytovatelé k nahlášení (tím že pouze klikneme na tlačítko nahlásit na sociálních sítích) obsahu dostanou, je mnoho, je možné, že například urážlivé video, fotografie zůstanou zveřejněné ještě několik hodin či dní. Policie a příslušné orgány mají své postupy, jak se v těchto případech zachovat a obsah co nejdříve stáhnout z internetových stránek. Taktéž je možné, aby servisní poskytovatel internetových stránek zajistil určitá data uživatelů, kteří se na kybernetických útocích podílejí či podíleli (E-bezpečí.cz, 2018).

Snažíme se problém vyřešit tak, aby se nešířil dál

Pokud známe kyberagresora (původce) kyberšikany, požádejte ho o odstranění urážlivého obsahu, pokud ne, obraťte se na poskytovatele internetových stránek. Je možné použít kázeňskou pravomoc, abychom zabránili šíření urážlivého obsahu. Učitelé v České republice bohužel v této oblasti nemají příliš možností (pravomocí). Mohou kybernetickému agresorovi zamezit přístup ke školnímu internetu, ale další možnosti nemají. V některých zemích ale již mají pravomocí v tomto případě mnohem více. Učitelé ve Velké Británii mohou kyberagresorovi zabavit mobilní telefon, který byl k útoku využit. Pokud znáte původce kyberši-

kany, požádejte ho, aby vám řekl, komu zprávu či fotku atd. poslal dál. V tom případě, že nevíme, kdo šíří urážlivý a nelegální obsah, obrátíme se na policii, která sama určí postup (E-bezpečí.cz, 2018).

Po prošetření incidentu kyberšikany s tímto problémem dále pracujte, viníky je třeba za tento čin potrestat

Pokusíme se učinit všechny kroky pro to, aby se tento incident již nikdy neopakoval. Máte před sebou ne zrovna snadný úkol, protože je důležité snažit se změnit postoje žáků a to je práce ne zcela snadná. Chce to vytrvalost, odhodlání a také dostatek času. Je třeba opět se zaměřit na preventivní opatření. U žáků je třeba vybudovat postoj k tomu, aby problém dokázali řešit. Proto je velmi důležitá empatie a podpora (E-bezpečí.cz, 2018).

Jestli chceme žáky potrestat adekvátně, je dobré položit si následující otázky:

- Jaký byl dopad na oběť?
- Byla kyberšikana páchána anonymně?
- Byl urážlivý materiál rozšířen obecně?
- Jak těžké bylo kontrolovat šíření urážejícího obsahu?
- Co bylo hlavním spouštěčem kyberšikany v tomto případě?
- Byl tento případ kybernetického útoku nezáměrný, nebo to byla odplata za šikanu?

Tresty nelze v tomto případě kategorizovat. Při méně závažných incidentech kyberšikany je možné do trestu zahrnout omezení přístupu na internet ve škole nebo úplný zákaz nosit mobilní telefon či jiná komunikační média do školy (E-bezpečí.cz, 2018).

Ukazatele prokazující, že se dítě stalo obětí kyberšikany:

- náhle přestane používat svůj osobní počítač;
- často mění své chování a nálady (několikrát denně);
- před cestou do školy trpí pravidelně bolestmi břicha nebo hlavy, nevolnost;
- je často nervózní nebo nejisté při čtení svých e-mailů nebo SMS zpráv v mobilu;
- nechce nebo se bojí chodit do školy nebo vůbec do společnosti;

- je často rozčilené, expresivní nebo frustrované při odchodu od počítače.

Ukazatele prokazující, že je dítě kybernetickým agresorem (kyberagresorem):

- pravidelně rychle vypíná monitor počítače nebo zavírá programy v počítači, když se rodič nebo učitel přiblíží k počítači;
- tráví u svého počítače dlouhé hodiny hlavně v noci;
- je rozčilené, pokud nemůže nečekaně využít svůj počítač;
- přehnaně a škodolibě se u počítače směje;
- vyhýbá se rozhovorům o tom, co na počítači vlastně tak dlouho dělá;
- používá několik on-line účtů nebo adres, které ani nejsou jeho;
- ve škole mohou být podezřelé smějící se skupinky žáků kolem počítače.

9 Rady a doporučení závěrem

Nejdůležitější prevencí kyberšikany je zdravý selský rozum a opatrnost. Snažte se děti důsledně a opakovaně informovat, kdy stěžejní část by mělo tvořit sdělení, že jakékoliv podezření je vhodné konzultovat s rodiči nebo učitelem. Největším nebezpečím totiž není to, že si dítě povídá s někým cizím, ale fakt, že tuto skutečnost nesdělí nikomu dospělému. Nezapomeňte dětem sdělit, PROČ jim tyto informace předáváte. Pozor také na zákazy, pokud dítěti zakážete internet nebo komunikaci s přáteli z preventivních důvodů, vytváříte tak s dítětem nedůvěryhodný vztah, dítě si přístup k internetu najde i jinak a případné hrozby pak s Vámi nebude konzultovat už vůbec!

Drtivá většina ohrožení našich zařízení nebo internetových napadení spočívá v neznalosti nebo neopatrnosti uživatelů. Lidé se na internetu bohužel příliš zodpovědně nechovají a s ověřováním informací nebo se zabezpečením si hlavu příliš nelámou. Běžné jsou situace, kdy se na internetu (nejčastěji e-mailem nebo na sociálních sítích) hromadně sdílejí informace, které nejsou pravdivé. Uživatel internetu bohužel rád dodržuje pravidlo, že „co je v médiích, to je pravda“, a sdílí tak nesmyslné zprávy a nesmyslná varování, aniž by si je předem ověřil. Dalším a pravděpodobně nejčastějším uživatelským prohřeškem je slabé nebo dokonce žádné heslo do uživatelských účtů. Napadení takového zařízení nebo profilu je pak často jen otázkou času. Uživatelé často ani nezálohují a při napadení zařízení virem může dojít ke ztrátě všech dat, taková ztráta je pak mnohdy nevyčíslitelná (ztráta fotografií, účetních dat, pracovních dokumentů apod.). Závažnější je pak nedůslednost ro-

dičů při dohledu nad aktivitami svých dětí na internetu nebo dokonce nezodpovědnost při zacházení s fotografiemi svých vlastních dětí.

Ve chvíli, kdy máte podezření, že něco není v pořádku, pokuste se citlivě s dítětem o této situaci promluvit. Pokud se podezření potvrdí, zajistěte veškeré důkazy, ať už sami, nebo s pomocí IT odborníka. V tabletu, telefonu nebo počítači uložte všechny texty a veškerou komunikaci, stáhněte fotografie, obrázky i videa. V případě, že nejde text zkopírovat, použijte snímek obrazovky (printscreen). Vše archivujte a uložte bezpečně alespoň na dvě nezávislá úložiště jako zálohu. Všechny tyto získané materiály se Vám mohou hodit pro případné důkazní řízení.

Základní pravidlo při práci s internetem a nahrávání fotografií a videí by se dalo shrnout do věty: VŽDY SI PEČLIVĚ ROZMYSLETE, CO NA INTERNET NAHRAJETE. CO INTERNET SCHVÁTÍ, TO UŽ NENAVRÁTÍ! Je třeba si uvědomit, že nahrání jakýchkoliv dat na internet je v podstatě NEVRATNÝ PROCES. Fotky a příspěvky, které nahrajete do on-line prostředí, už nikdy nedokážete v plné míře smazat. A je nutné o této skutečnosti informovat i děti. Po nahrání se vše začíná ihned archivovat a mnohdy šířit dál jako lavina, každý z nás tak může způsobit naprosto nepředstavitelné škody, přestože původní záměr mohl být jen např. pobavit několik dětí ve třídě, kamarády, známé.

9.1 Desatero bezpečného používání internetu

Jednotlivé kroky, jak se bezpečně pohybovat v prostředí internetu:
(upraveno dle Seznam se bezpečně, 2018)

1. Nezveřejňuj své osobní údaje.
2. Nesdílej odhalené fotky.
3. Bezpečně se odhlašuj.
4. Používej bezpečná hesla.
5. Nepřidávej si osoby do přátel pouze kvůli počtu.
6. Přidávej si pouze osoby, které znáš.
7. Čti pravidla užívání sociálních sítí.
8. Rozlišuj reálný a virtuální život.
9. Nastavuj sdílení na sociálních sítích.
10. Nebuď závislý na sociálních sítích.

9.2 Netiketa

Pojem netiketa je moderní termín, který v sobě skrývá důležitou součást prevence na internetu. Tento pojem by měl znát každý uživatel internetového prostředí. Slovo netiketa se skládá z prvního slova net (= internet) a z druhého slova etiketa. Z toho je zřejmé, že netiketa vymezuje pravidla chování a zásady, které musí znát každý uživatel internetu a hlavně by je měl pečlivě dodržovat, chrání totiž svůj kyberprostor. Je důležité myslet na to, že osoba, se kterou komunikujeme na internetu, je reálná a sami sebe bychom se měli dotázat, zda bychom se opravdu stejně chovali i ve světě reálném. Komunikace na internetu je neosobní a mnoho internetových uživatelů zapomíná na důležitý fakt, že i pachatele (případného agresora) lze na internetu vypátrat a jeho anonymní chování je pouze dočasné (Kavalír, 2009).

Každý uživatel, který se pohybuje v internetovém prostředí, by se měl chovat stejně jako v běžném životě. Měl by dodržovat základní pravidla slušného chování a nejprve si promyslet to, co chce napsat. Není dobré také sdělovat informace, které by v osobním styku neřekl. Uživatel internetu by měl jednat tak, aby se za své chování nemusel ve virtuálním světě stydět. Nevhodné rozšiřování pomluv ubližuje druhým, proto by nikdo neměl šířit tyto zprávy dál. Jak v běžném životě, tak ve virtuální realitě je nutno dodržovat ohleduplnost vůči ostatním lidem. Uživatel internetu musí dodržovat autorská práva, taktéž správce serveru nesmí zneužívat své pozice a nahlížet do zpráv ostatních uživatelů, pokud tedy není napsáno jinak v podmínkách, které musí uživatel přijmout a odsouhlasit, když se na určité stránce chce zaregistrovat (Dočekal, Eckertová, 2013).

Desatero netikety pro uživatele internetu je stanoveno následovně: *(Chování.cz, 2018)*

1. Chovejte se tak, abyste nepoškozovali ostatní uživatele.
2. Neomezujte ostatní při jejich vlastní práci na síti.
3. Nenahlížejte do souborů ostatních uživatelů.
4. Nevyužívejte počítače ke krádežím.
5. Nevyužívejte síť ke zveřejnění falešných údajů, falešného svědectví.
6. Nevyužívejte ani si nekopírujte software, za který jste nezaplatili.

7. Nevyužívejte zdroje ostatních uživatelé bez autorizace.
8. Nepřisvojujte si duševní bohatství ostatních.
9. Uvažujte o společných důsledcích programu, který tvoříte.
10. Používejte počítač s úctou, s respektem a ohleduplně.

9.3 Doporučené odkazy

- Bezpečně on-line (www.bezpecne-online.cz) – stránky pro teenagery, rodiče a učitele s informacemi o bezpečném používání internetu, prevenci a řešení zejména kyberšikany.
- Centrum prevence rizikové virtuální komunikace PdF UPOL (http://prvok.upol.cz) – centrum realizující řadu projektů zaměřených na rizikové chování na internetu.
- Dětské krizové centrum (www.ditekrize.cz) – poradenství a pomoc v krizi.
- E-bezpečí (www.e-bezpeci.cz) – internetový projekt zaměřený na prevenci rizikového chování na internetu.
- Kraje pro bezpečný internet (http://www.kpbi.cz/) – e-learningové lekce pro děti, studenty, rodiče, učitele, sociální pracovníky a další cílové skupiny.
- Poradna e-bezpečí (https://poradna.e-bezpeci.cz/) – poradna pouze písemně zaměřená na prevenci rizikového chování na internetu.
- Poradna MIŠ (www.minimalizacesikany.cz/poradna) – poradna zaměřená na problémy týkající se šikany a také kyberšikany.
- Projekt E-Nebezpečí pro učitele (www.e-nebezpeci.cz) – obsahuje řadu prezentací pro učitele.
- Projekt Internetem bezpečně (www.internetembezpecne.cz) – formou různých vzdělávacích aktivit klade za cíl zvýšit povědomí uživatelů o rizikovém internetovém prostředí.
- Projekt Nebuď oběť! (www.nebudobet.cz) – projekt zaměřený na rizika internetu a různých komunikačních technologií.
- Projekt NNTB „Nenech to být“ (www.nntb.cz) – internetový systém a mobilní aplikace bojující proti šikaně a vylučování z kolektivu na školách po celé České republice.
- Projekt Saferinternet.cz (www.saferinternet.cz) – projet zaměřený na rizika a nebezpečí internetu a komunikačních technologií.

- Server Hoax.cz (www.hoax.cz) – cílem tohoto serveru je informovat uživatele internetu o poplašných, nebezpečných a zbytečných řetězových zprávách, tzv. hoaxech.
- Společenství proti šikaně (www.sikana.org) – stránky občanského sdružení Společenství proti šikaně obsahující mnoho informací a aktualit z oblasti šikany.
- Úřad pro ochranu osobních údajů (www.uoou.cz) – institut zaměřený na ochranu osobních údajů a poradenství.

Použitá a doporučená literatura

1. BENDL, S., 2001. Školní kázeň metody a strategie. Praha: ISV. 267 s. ISBN 80-858660-80-3.
2. BLINKA, L., 2015. Online závislosti: Jednání jako droga?: online hry, sex a sociální stě: diagnostika závislosti na internetu: prevence a léčba. Praha: Grada. 198 s. ISBN 978-80-210-7975-5.
3. BUŘIČOVÁ KADLECOVÁ, J., 2010. Pedagogická intervence u žáků ZŠ. Praha: Wolters Kluwer Česká republika. 332 s. ISBN 978-80-7357-603-5.
4. CIKLOVÁ, K., 2014. Rizikové chování ve škole s vazbou na legislativní úpravu. Praha: Ekonom Press. 160 s. ISBN 978-80-905065-6-5.
5. ČECH, O., ZVONÍČKOVÁ, N., 2017. Nebezpečí kyberšikany: internet jako zbraň? České Budějovice: Theia - krizové centrum o.p.s. 131 s. ISBN 978-80-904854-4-0.
6. ČERNÁ, A. a kol., 2013. Kyberšikana: průvodce novým fenoménem. Praha: Grada, 150 s. Psyché. ISBN 978-80-210-6374-7.
7. Český statistický úřad. Počtem uživatelů internetu jsme přeskočili Evropu. [online] [cit. 2018-08-15]. Dostupné z: https://www.czso.cz/csu/czso/poctem-uzivatelu-internetu-jsme-preskocili-evropu
8. DIVÍNOVÁ, R., 2005. Cybersex – forma internetové komunikace. Praha: Triton. 168 s. EAN EK169109.
9. DOČEKAL, D., ECKERTOVÁ, L., 2013. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. Praha: Computer Press. 224 s. ISBN 978-80-2513-804-5.
10. E-BEZPEČÍ, 2018. E-bezpečí portál. [online] [cit. 2018-08-15]. Dostupné z: https://www.e-bezpeci.cz/index.php/rodice-ucitele-zaci
11. HARTLOVÁ, H., HARTL, P., 2010. Velký psychologický slovník. Praha: Portál. 800 s. ISBN 978-80-7367-686-5.
12. HRABAL, V., 2002. Pedagogicko-psychologická diagnostika žáka. Praha: Karolinum. 199 s. ISBN 8024603195.
13. CHOVÁNÍ, 2018. Chování EU. [online] [cit. 2018-08-15]. Dostupné z: http://www.chovani.eu/netiketa/c56
14. JAK NA INTERNET.CZ. Ochrana dětí na internetu. [online] [cit. 2018-08-15]. Dostupné z: http://www.jaknainternet.cz/page/1700/zavislost-na-internetu/
15. KALINA, K., 2008. Základy klinické adiktologie. Praha: Grada. 392 s.
16. KASPERSKY LAB, 2015. Forms of Cyberbullying. [online] [cit. 2018-08-20]. Dostupné z: https://kids.kaspersky.com/10-forms-of-cyberbullying/

17. KAVALÍR, A., 2009. Kyberšikana a její prevence. Plzeň: Seznam se bezpečně, s. 104. [online] [cit. 2018-08-15]. Dostupné z: https://www.sancedetem.cz/srv/www/content/pub/cs/odborna-knihovna/kybersikana-a-jeji-prevence-prirucka-pro-ucitele-26000.html
18. KOLÁŘ, M., 2011. Nová cesta k léčbě šikany. Praha: Portál. 336 s. ISBN 978-80-7367-871-5.
19. KOPECKÝ, K., 2013. Rizika internetové komunikace v teorii a praxi. Olomouc: Univerzita Palackého v Olomouci. 188 s. ISBN 978-80-244-3571-8.
20. KOPECKÝ, K., 2015. Rizikové formy chování českých a slovenských dětí v prostředí internetu. Olomouc: Univerzita Palackého v Olomouci. 172 s. ISBN 978-80-244-4861-9.
21. KOPECKÝ, K., SZOTKOWSKI, R., 2013. Intervence pedagoga: Rizikové chování ve školním prostředí – rámcový koncept Příloha č. 7. Praha: Ministerstvo školství mládeže a tělovýchovy České republiky, s. 52. [cit. 2018-08-15]. Dostupné z: http://docplayer.cz/3923128-Co-delat-kdyz-intervence-pedagoga-rizikove-chovani-ve-skolnim-prostredi-ramcovy-koncept-priloha-c-7-kybersikana.html
22. KOWALSKI, R. M., LIMBER, S. P., 2007. Electronic bullying among middle school students. Journal Adolesc Health. 41(6), 22–30. Doi: 10.1016/j.jadohealth.2007.08.017.
23. KOŽÍŠEK, M., PÍSECKÝ, V., 2016. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Garada. 176 s. ISBN 978-80-247-5595-3.
24. KRAUS., B., HRONCOVÁ, J., 2010. Sociální patologie 2. vyd. Hradec Králové: Gaudeamus. 50 s. ISBN 9788074350801.
25. KRČMÁŘOVÁ, B., 2012. Děti a online rizika: sborník studií. Praha: Sdružení Linka bezpečí. 178 s. ISBN 978-80-904920-2-8.
26. KREJČÍ, V., 2010. Kyberšikana – kybernetická šikana. Olomouc: Univerzita Palackého v Olomouc, Pedagogická fakulta. 72 s.
27. MARTÍNEK, Z., 2015. Agresivita a kriminalita školní mládeže. Praha: Grada. 192 s. ISBN 978-80-247-5309-6.
28. MIOVSKÝ, M., 2010. Primární prevence rizikového chování ve školství. Praha: Sdružení SCAN. 262 s. ISBN 978-80-87258-47-7.
29. MIOVSKÝ, M., 2015. Návrh doporučení struktury minimálního preventivního programu. Praha: Nakladatelství Lidové noviny. 112 s. ISBN 978-80-87258-74-3.
30. MŠMT ČR, 2005. Věstník ministerstva školství, mládeže a tělovýchovy České republiky. Ročník LXI.
31. MŠMT ČR © 2013–2018. Metodické dokumenty: doporučení a pokyny. [online] [cit. 2018-08-16]. Dostupné z: http://www.msmt.cz/vzdelavani/socialni-programy/metodicke-dokumenty-doporuceni-a-pokyny
32. MŠMT ČR © 2013–2018. Národní strategie primární prevence rizikového chování dětí a mládeže na období 2013–2018. [online] [cit. 2018-08-15]. Dostupné z: http://www.msmt.cz/file/28077

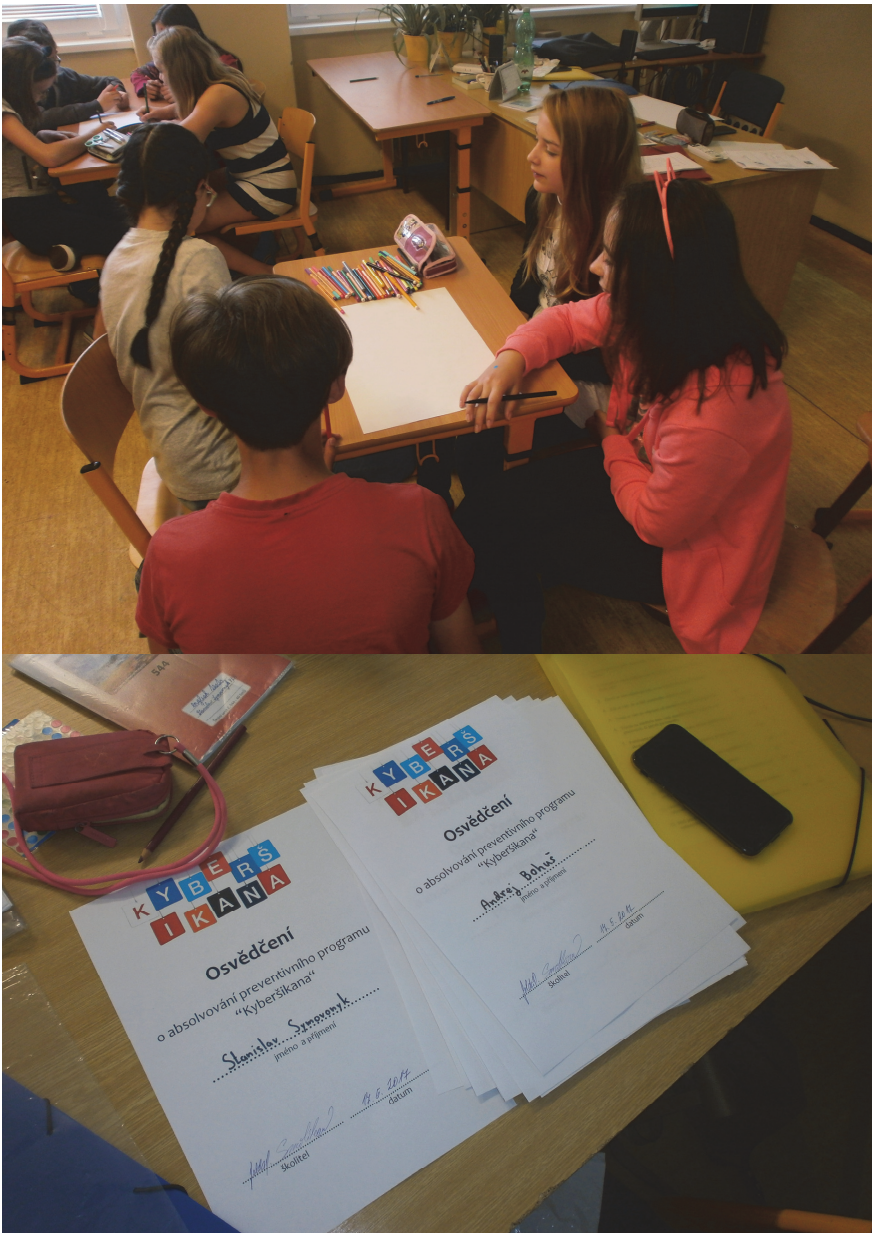
33. NEŠPOR, K., 2011. Návykové chování a závislosti. Praha: Grada. 176 s. ISBN 978802621892.
34. NETOLISMUS – PRŮVODCE ONLINE ZÁVISLOSTMI. [online] [cit. 2018-08-15]. Dostupné z: http://netolismus.cz
35. ROGERS, V., 2011. Kyberšikana: pracovní materiály pro učitele a žáky i studenty. Praha: Portál, 97 s. ISBN 978-80-7367-984-2.
36. ROTTOVÁ, N., 2009. Kyberšikana a její prevence: příručka pro učitele. Plzeň: Člověk v tísni o.p.s. 108 s. ISBN 978-80-86961-78-1.
37. ŘÍČAN, P., JANOŠOVÁ, P., 2010. Jak na šikanu. Praha: Grada. 160 s.
38. SAK, P., 2007. Člověk a vzdělávání v informační společnosti. Praha: Portál. 296 s. ISBN 978-80-7367-230-0.
39. SEZNAM. CZ, a. s., 2018. Seznam se bezpečně. [online] [cit. 2018-08-15]. Dostupné z: https://www.seznamsebezpecne.cz/
40. SPITZER, M., 2014. Digitální demence: jak připravujeme sami sebe a naše děti o rozum. Brno: Host. 344 s. ISBN 978-80-7294-872-7.
41. SYMANTEC, 2017. Cyberbullying: A conversation guide for parents and kids. [online] [cit. 2018-08-26]. Dostupné z: http://now.symassets.com/content/dam/content/en-us/collaterals/ebook/norton-cyberbullying-guide.pdf
42. ŠEVČÍKOVÁ, A. a kol., 2014. Děti a dospívající online: vybraná rizika používání internetu. Praha: Grada, 183 s. Psyché. ISBN 978-80-210-7527-6.
43. ŠIKANA, 2018. Společenství proti šikaně. [online] [cit. 2018-08-15]. Dostupné z: http://www.sikana.org/
44. VÁGNEROVÁ, M., 2004. Psychopatologie pro pomáhající profese. Praha: Portál. 872 s. ISBN 80-7178-802-3.
45. VEVERKA, K., STAVINOHA, R., 2005. Vliv mobilních telefonů na mládež. [online] [cit. 2018-08-15]. Dostupné z: http://www.gyrec.cz/drupal/files/Vaverka.pdf
46. Vyhláška č. 72/2005 Sb., o poskytování poradenských služeb ve školách a školských poradenských zařízeních. In: Sbírka zákonů ČR, částka 20/2005.
47. Vyhláška č. 263/2007 Sb., kterou se stanoví pracovní řád pro zaměstnance škol a školských zařízení zřízených Ministerstvem školství, mládeže a tělovýchovy, krajem, obcí nebo dobrovolným svazkem obcí. In: Sbírka zákonů ČR, částka 86/2007.
48. Zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí. In: Sbírka zákonů ČR, částka 111/1999.
49. Zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon). In: Sbírka zákonů ČR, částka 190/2004.
50. Zákon č. 262/2006 Sb., zákoník práce. In: Sbírka zákonů ČR, částka 84/2006.
51. Zákon č. 40/2009 Sb., trestní zákoník. In: Sbírka zákonů ČR, částka 11/2009.

Přílohová část

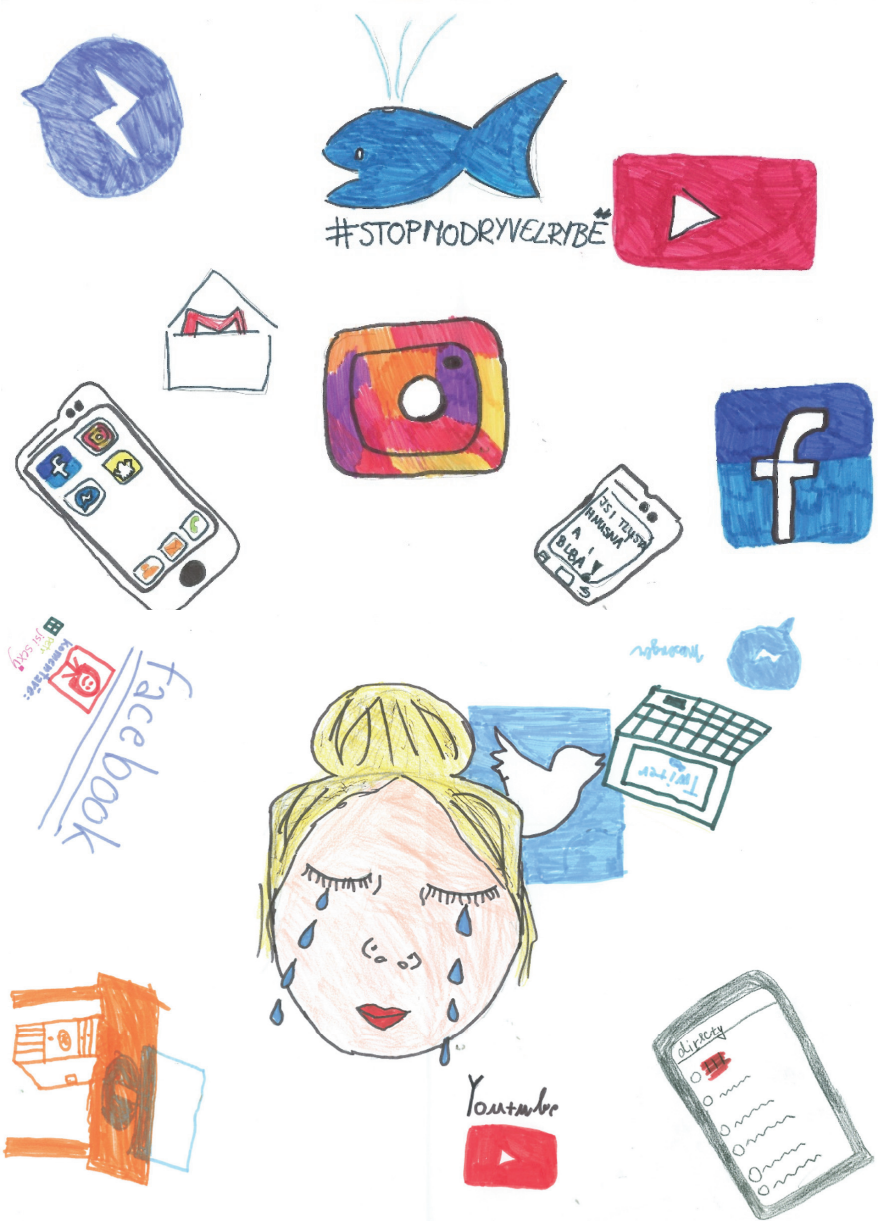
Tato část publikace je věnována výukovému programu projektu OZS/5/4112/2018 Prevence kyberšikany a ochrana dětí před on-line hrozbami, který autoři realizovali v roce 2018 na šesti základních školách v Jihočeském kraji.

Cílem výukového programu je seznámit žáky s rizikem kyberšikany a její prevencí, zmapovat u žáků jejich názor na kyberšikanu a uvést informace týkající se této problematiky na pravou míru. Dalším cílem je zjistit, zda mají sami žáci zkušenosti s kyberšikanou a na základě toho lektor předá žákům informace o správném řešení této problematiky. V poslední části programu lektor ověří znalosti dětí pomocí tvorby myšlenkových map, které děti prezentují v závěru programu.

Výukový program na téma kyberšikana



Myšlenkové mapy – ukázka



Osvědčení pro žáky

OSVĚDČENÍ

O ABSOLVOVÁNÍ PREVENTIVNÍHO PROGRAMU

„Kyberšikana“

.....

jméno a příjmení

....

školitel **datum**

Financováno v rámci projektu MZ ČR s názvem „Prevence kyberšikany a ochrana dětí před on-line hrozbami“ (č.5/18/K).

Poster projektu

PREVENCE KYBERŠIKANY
A OCHRANA DĚTÍ PŘED ON-LINE HROZBAMI

Renata Švestková, Ladislav Soldán, Martin Řehka

Projekt si klade za cíl vysvětlit žákům bezpečné způsoby používání informačních technologií – etiketa na internetu, e-bezpečí a počítačová gramotnost. Naučit je tyto technologie používat tak, aby vedly k podpoře sebeúcty, průbojnosti a budování přátelství.

Děti mají s kyberšikanou bohaté zkušenosti, například na sociálních sítích, herních serverech či hudebních kanálech. Děti, které se s kyberšikanou setkaly, si nesou následky téměř celý svůj život. Nejčastěji to mohou být deprese či neurotická traumata. Není neobvyklé, že některé dlouhodobě kyberšikanované děti tento tlak neunesou a svůj život ukončí...

DESATERO BEZPEČNÉHO POUŽÍVÁNÍ INTERNETU

1. Nezveřejňuj své osobní údaje.
2. Nesdílej odhalené fotky.
3. Bezpečně se odhlašuj.
4. Používej bezpečná hesla.
5. Nepřidávej si osoby do přátel pouze kvůli počtu.
6. Přidávej si pouze osoby, které znáš.
7. Čti pravidla užívání sociálních sítí.
8. Rozlišuj reálný a virtuální život.
9. Nastavuj sdílení na sociálních sítích.
10. Nebuď závislý na sociálních sítích.

Financováno v rámci projektu MZ ČR s názvem „Prevence kyberšikany a ochrana dětí před on-line hrozbami" (č. 5/18/K).

Zdravotně sociální fakulta
Faculty of Health and Social Sciences

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Mgr. Ing. Renata Švestková, Ph. D.; Bc. Ladislav Soldán; Bc. Martin Řehka;
Jihočeská univerzita v Českých Budějovicích, Zdravotně sociální fakulta,
Ústav sociálních a speciálněpedagogických věd
E-mail: svestkor@zsf.jcu.cz

KYBERŠIKANA

Renata Švestková, Ladislav Soldán, Martin Řehka

Vydavatel: Jihočeská univerzita v Českých Budějovicích
Zdravotně sociální fakulta
Sazba a jazyková redakce: Zuzana Straková
Tisk: Typodesign, s. r. o., České Budějovice
1. vydání 2019
82 stran

ISBN 978-80-7394-752-1