Česká zemědělská univerzita v Praze

Institut vzdělávání a poradenství

Katedra celoživotního vzdělávání a podpory studia

Rizikové chování na internetu

Bakalářská práce

Autor: **Tomáš Kučera**

Vedoucí práce: PhDr. Jitka Jirsáková, Ph.D.

2021

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Institut vzdělávání a poradenství

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Tomáš Kučera

Specializace v pedagogice
Poradenství v odborném vzdělávání

Název práce

Rizikové chování na internetu

Název anglicky

Risky Internet Behaviors

Cíle práce

Cílem práce je zjistit povědomí žáků středních odborných škol o projevech rizikového chování, které souvisí s virtuálním prostředím, např. kyberšikana, problematika sociálních sítí, seznamovací aplikace, trolling, haterství, "fake news" atp. a na základě výsledků dotazníkového šetření navrhnout rámec vzdělávacího projektu, který bude zaměřen na prevenci těchto jevů.

Metodika

V teoretické části práce bude provedena rešerše odborné literatury, budou definovány základní pojmy, jako rizikové chování na internetu, prevence, kyberšikana a její projevy apod.

V praktické části práce na základě kvantitativního dotazníkového šetření bude zjišťováno, jaké povědomí a znalosti mají studenti v oblasti rizikového chování na internetu a jak se na internetu projevují. Na základě výsledků tohoto šetření bude vytvořen návrh vzdělávacího projektu, který bude zaměřen na prevenci rizikového chování internetu a zásady bezpečného užívání internetu pro žáky středních odborných škol.

Doporučený rozsah práce

dle pravidel pro psaní bakalářských prací

Klíčová slova

rizikové chování, prevence, kyberšikana, kyberprostor, střední škola, vzdělávací program

---

Doporučené zdroje informací

Adam Alter. Neodolatelné. Vzestup návykových technologií a byznys se závislostí ; Překladatel: Julie Tesla – První vydání – Brno : Host, 2018. – 335 s. ISBN 978-80-757-7460-6

Blinka, Lukáš a kol. Online závislosti: jednání jako droga?: online hry, sex a sociální sítě: diagnostika závislosti na internetu: prevence a léčba. Vydání 1. Praha: Grada, 2015. 198 stran. Psyché. ISBN 978-80-210-7975-5.

Černá, Alena et al. Kyberšikana: průvodce novým fenoménem. Vyd. 1. Praha: Grada, 2013. 150 s. Psyché. ISBN 978-80-210-6374-7.

Kožíšek, Martin a Písecký, Václav. Bezpečně n@ internetu: průvodce chováním ve světě online. První vydání. Praha: Grada Publishing, 2016. 175 stran. ISBN 978-80-247-5595-3.

Ševčíková, Anna a kol. Děti a dospívající online: vybraná rizika používání internetu. Vyd. 1. Praha: Grada, 2014. 183 s. Psyché. ISBN 978-80-210-7527-6.

Předběžný termín obhajoby

2020/21 LS – IVP

Vedoucí práce

PhDr. Jitka Jirsáková, Ph.D.

Garantující pracoviště

Katedra celoživotního vzdělávání a podpory studia

Elektronicky schváleno dne 8. 3. 2021

PhDr. Lucie Smékalová, Ph.D. et Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 8. 3. 2021

Ing. Karel Němejc, Ph.D.

Pověřený ředitel

V Praze dne 22. 03. 2021

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou/závěrečnou práci na téma:

Rizikové chování na internetu

vypracoval/a samostatně a citoval/a jsem všechny informační zdroje, které jsem v práci použil/a a které jsem rovněž uvedl/a na konci práce v seznamu použitých informačních zdrojů.

Jsem si vědom/a, že na moji bakalářskou/závěrečnou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

Jsem si vědom/a, že odevzdáním bakalářské/závěrečné práce souhlasím s jejím zveřejněním podle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Svým podpisem rovněž prohlašuji, že elektronická verze práce je totožná s verzi tištěnou a že s údaji uvedenými v práci bylo nakládáno v souvislosti s GDPR.

V ……. dne ……

…….

(podpis autora práce)

PODĚKOVÁNÍ

Chtěl bych poděkovat vedoucím mé bakalářské práce PhDr. Jitce Jirsákové, Ph.D. a Mgr. Kamile Urban PhD. za skvělou podporu a trpělivost.

Abstrakt

Bakalářská práce na téma **Rizikové chování na internetu** se zaměřuje na problematiku a prevenci kyberšikany a rizikového chování na internetu u žáků středních odborných škol. Cílem práce bylo zjistit, jak se žáci na internetu chovají a jaké mají o problematice povědomí.

Teoretická část práce se zaměřuje na teorii rizikového chování jako takového s následnou návazností na samotnou rizikovost chování na internetu, rozebírá a porovnává tradiční šikanu s kyberšikanou a zároveň se věnuje prevenci těchto jevů.

V rámci praktické části je pomocí kvantitativního dotazníkovému šetření zjišťováno, jak se žáci v praxi na internetu sami chovají a jestli se chovají rizikově nebo naopak dodržují zásady bezpečného užívání internetu. Bylo zjištěno, že žáci mají nedostatek informací v oblasti rizikového chování na internetu, sami se v mnoha případech rizikově chovají a zároveň, že za kyberšikanu považují ve velké většině jen několik konkrétních věcí, jako je třeba slovní agresivita, šíření soukromých zpráv na veřejnosti, shromažďování osobních informací druhých a následné vydírání.

Na základě výsledků z dotazníkového šetření byl vypracován návrh programu, zaměřujícího se na prohloubení informovanosti žáků středních odborných škol v problematice rizikového chování na internetu a kyberšikany, stejně jako na samotnou prevenci těchto jevů.

Klíčová slova:

rizikové chování, prevence, kyberšikana, kyberprostor, střední škola, vzdělávací program

Abstract

The bachelor's thesis on the topic of risky behavior on the Internet focuses on the issue and prevention of cyberbullying and risky behavior on the Internet for students of secondary vocational schools. The aim of the work was to find out how students behave on the Internet and what they are aware of the issue.

The theoretical part of the thesis focuses on the theory of risky behavior as such with a subsequent link to the very risky behavior on the Internet, analyzes and compares traditional bullying with cyberbullying and also deals with the prevention of these phenomena.

In the practical part, a quantitative questionnaire survey is used to determine how students in practice behave on the Internet themselves and whether they behave at risk or, conversely, follow the principles of safe use of the Internet. It was found that students lack information on risky behavior on the Internet, in many cases behave at risk and at the same time that they consider cyberbullying in the vast majority only a few specific things, such as verbal aggression, dissemination of private messages to the public, personal information of others and subsequent blackmail.

Based on the results of the questionnaire survey, a draft program was developed, aimed at deepening the awareness of secondary vocational school students in the issue of risky behavior on the Internet and cyberbullying, as well as the prevention of these phenomena.

Keywords:

risky behavior, prevention, cyberbullying, cyberspace, high school, educational program

OBSAH

ÚVOD

V současné době se internet hojně využívá prakticky ke všemu, k výkonu práce, ke školním povinnostem, a i v rámci domácnosti se internet naprosto běžně užívá. Téma práce je velice aktuální primárně vzhledem k tomu, že je dnes ve velké míře internet využíván zejména adolescenty, kteří se dle výzkumů chovají v kyberprostoru v mnoha případech nezodpovědně, příkladem může být, že o sobě velmi často zveřejňují velké množství informací a ty mohou být následně zneužity. Nejenže adolescenti o sobě sdílejí značné množství osobních informací, zároveň se často stává, že tyto informace i sdělují lidem, které třeba nikdy nepotkali.

Teoretická část se zaměřuje na rozebrání pojmu šikany, její prevenci a následnému porovnání s kyberšikanou, které se práce následně věnuje. V případě je kyberšikany je práce mnohem konkrétnější a zaměřuje se na její dělení, projevy i následnou prevenci, stejně jako na technologie skrze, které se kyberšikana nejčastěji šíří. Ve značné míře se tato část věnuje i rizikovému chování, kde je zaměřeno zejména na jeho definice a dělení a rizikovému chování na internetu. Rizikovému chování na internetu vzhledem k povaze práce je věnováno více prostoru a je tedy rozebrána jeho definice, dělení a také jednotlivé možnosti prevence.

V praktické části jsou vyhodnocena data z dotazníkového šetření a na základě výsledků je pak vytvořen návrh programu prevence, který má za účel zejména žáky dostatečně informovat v problematice rizikového chování na internetu.

Bakalářskou práci na téma **Rizikové chování na internetu** jsem si vybral, protože je třeba, aby se tomuto tématu věnovalo mnohem více než je tomu doposud vzhledem ke stále se zvyšujícímu užívání internetu zejména v případě dospívajících žáků. Pokud budou dospívající žáci dostatečně informováni, předejde se spoustě případů, kdy by mohlo k nějakému rizikovému chování dojít.

TEORETICKÁ ČÁST

1 Cíl a metodika

Cílem práce je zjistit povědomí žáků středních odborných škol o projevech rizikového chování, které souvisí s virtuálním prostředím, např. kyberšikana, problematika sociálních sítí, seznamovací aplikace, trolling, haterství, "fake news" atp. a na základě výsledků dotazníkového šetření navrhnout rámec vzdělávacího projektu, který bude zaměřen na prevenci těchto jevů.

V teoretické části práce bude provedena rešerše odborné literatury, budou definovány základní pojmy, jako rizikové chování na internetu, prevence, kyberšikana a její projevy apod.

V praktické části práce na základě kvantitativního dotazníkového šetření bude zjišťováno, jaké povědomí a znalosti mají žáci v oblasti rizikového chování na internetu a jak se na internetu projevují. Na základě výsledků tohoto šetření bude vytvořen návrh vzdělávacího projektu, který bude zaměřen na prevenci rizikového chování internetu a zásady bezpečného užívání internetu pro žáky středních odborných škol.

2 Rizikové chování

Rizikové chování je takové při, kterém dochází k rizikovým a nebezpečným aktivitám z hledisek sociálních, psychologických ale i zdravotních a fyziologických. Rizikové chování vždy do určité míry ovlivňuje jak okolí, tak i samotného iniciátora. Patří sem např., vandalismus, drogové závislosti a v neposlední řadě šikana (Bendl a kol., 2015).

Rizikové chování je součástí dospívání každého dítěte a vždy při něm dochází k důsledkům, které následně jedince nebo jeho okolí, do určité míry negativně ovlivní. (Dolejš, Orel, 2017).

Rizikové chování lze také označit jako sociálně patologický jev, při kterém dochází ke zvýšenému výskytu výchovných a sociálních rizik jež jsou nebezpečné jako pro jednotlivce tak i jeho okolí a tento jev je pak možné ovlivňovat skrze různé preventivní intervence. Mezi jevy, které jsou zařazeny pod rizikové chování patří (Miovský a kol., 2010):

- Šikana a agresivní chování
- Rizikové chování v rámci dopravy a extrémně nebezpečné sporty
- Poruchy příjmů potravy
- Závislostní chování
- Xenofobní a rasistické chování
- Negativní působení sekt
- Sexuální rizikové chování
- Záškoláctví

Pod rizikové chování můžeme zařadit následující typy chování (Dolejš, Orel, 2017):

1) **Problémové chování** je chování, které je okolím vnímáno jako problémové. Chování překračuje běžné společenské normy (pozdní příchod do školy/práce, neuposlechnutí)
2) **Maladaptivní chování** se dá volně označit taky za nepřizpůsobivé chování, které je společensky nežádoucí, patří sem třeba agresivní chování vůči dalším osobám.

3) **Protispolečenské chování** se projevuje úmyslným poškozováním základů dané společnosti, patří pod něj například demonstrace.
4) **Abnormální chování** je tzv., škodlivé chování. Je rozdílné od běžného morálního a společenského řádu společnosti, ve které se jedinec nachází.
5) **Disociální chování** je krátkodobé, které v určité míře překračuje běžné společenské normy. Ukázkovým příkladem je zde neuposlechnutí, vyrušování ve škole, vzdorovité chování apod., toto chování lze nicméně ovlivnit pedagogickými výchovnými nástroji.
6) **Asociální chování,** sem spadá třeba typické záškoláctví. Asociální chování už vážněji porušuje běžné společenské normy, ale stále nepřekračuje zákon, aby se mohlo stát trestnou činností.
7) **Antisociální chování** je považováno za protispolečenské chování při, které je už zřejmá kriminální činnost, jež může nabývat různorodé vážnosti, zahrnuje šikanu, krádeže a vandalismus.
8) **Delikventní chování** je takové, při kterém dochází ke zjevnému porušování zákonů vymezených státem, patří do něj trestní činnost a fyzické násilí.
9) **Deviantní chování,** lze za něj považovat takové chování, které se vymyká běžným sociálním normám (sexuálně orientované deviantní chování).

2.1 Prevence rizikového chování

Slovo prevence znamená opatření, nebo také včasnou ochranu. Prevence má za úkol zajistit, aby pokud možno nedošlo k rizikovému chování nebo jeho šíření. V rámci prevence jde o vytváření kladného přístupu k zdravému životnímu stylu, zvládání náročných sociálních situací a osvojování si technik k jejich zvládnutí a neposlední řadě o rozvoj pozitivního sociálního chování a psychosociálních dovedností (NUV, 2020).

2.1.1 Specifická primární prevence

Za specifickou primární prevenci považujeme ty aktivity a programy, které se cíleně zaměřují na konkrétní rizikové chování či problematiku. Působí cíleně na informovanost a postoje osob (NICM, 2020).

Specifickou primární prevenci (NUV, 2020) dělíme na:

1) **Všeobecnou prevenci** - se zaměřuje na větší množství osob. Nerozděluje osoby podle toho, jestli mají např. větší sklon propadnout konkrétnímu rizikovému chování a ani podle těchto kritérií neupravuje svůj program. Jde o programy a aktivity kdy má jít o obecné informování o problematice kdy jsou informace předávány většímu množství lidí, nejčastěji to jsou třídy ve školách. Takovéto programy mohou realizovat např. i policisté nebo školní metodik prevence.
2) **Selektivní prevenci** - se zabývá skupinami osob nebo jednotlivci, u kterých se vyskytuje zvýšené riziko k určitému druhu rizikového chování. Skupiny, které jsou náchylnější ke konkrétnímu rizikovému chování lze rozlišit na základě biologických, psychologických ale i sociálních nebo enviromentálních faktorů. V rámci selektivní primární prevence se tak spíše pracuje s menšími skupinami či přímo jednotlivci.
3) **Indikovanou prevenci** - je zaměřena na skupiny či jedince, u kterých je vysoká pravděpodobnost výskytu rizikového chování. Cílem této prevence je zvolit co nejvhodnější program a intervence vzhledem k jedinci a neprodleně je zahájit, aby došlo k zamezení výskytu možného rizikového chování, které se může u indikovaných jedinců s velkou šancí objevit.

2.1.2 Nespecifická primární prevence

Se nezaměřuje na konkrétní problém a rizikové chování ale napomáhají jejich prevenci nepřímo, nezabývá se ničím určitým a zabývá se celkovou problematikou rizikového chování z obecného hlediska (NICM, 2020).

Nespecifická prevence tak napomáhá například vytvářením různých zájmových kroužků, kurzů ať už jde o sport nebo jiné volnočasové aktivity, které se snaží pozitivně ovlivnit rozvoj osobnosti člověka (NUV, 2020).

3 Charakteristika adolescentů a jejich chování na internetu

Adolescence je fáze dospívání, při které dochází k plné pohlavní zralosti a adolescenti mají potřebu patřit do nějaké vrstevnické skupiny, kde naplňují své psychické potřeby a zároveň jim členství ve skupině dodává pocit jistoty, bezpečí a pochopení. Adolescenti v tomto období získávají první vážné zkušenosti v rámci vztahů s opačným pohlavím a formují si vlastní identitu a vytváří si vlastní názor na okolní svět, který je pro ně důležitý. V tomto období si adolescenti snaží co nejvíc užívat života a v mnoha případech nehledí na možná rizika, která svým chováním mohou vyvolat (Dolejš, Orel, 2017).

Adolescenti mají tendence chovat se impulzivně a snaží se co nejvíce poznat svět a sebe samého, provádějí tak často nedomyšlené aktivity, a to jak ve skutečném světě, tak i v kyberprostoru, které jsou ve výsledku pro ně samé i pro jejich okolí rizikové. Často tak realizují rizikové a nebezpečné aktivity jako užívání drog, vandalismus, sexting apod. (Dolejš, Orel, 2017).

Ze studie PEW ze Spojených států amerických z roku 2009, vyšlo najevo, že velké množství dospívajících se na internetu chová nanejvýš rizikově. Nejčastěji dospívající sdílí své jméno, datum narození, adresu školy a bydliště, informace o zájmových aktivitách a v neposlední řadě své vztahy. Na sociálních sítí ze všech dotázaných sdílelo 91 % vlastní fotku, 82 % datum narození, 62 % sdílelo informace o vztazích a celkem 24 % nasdílelo na sociální sítě video, ve kterém figurují. Dalších 53 % z dotázaných uvedlo, že sdílí na internetu svůj email a 20 % pak mobilní číslo. Ze studie následně vyšlo najevo, že starší dospívající mají větší tendenci o sobě na internetu uvádět větší množství osobních informací (Ševčíková Anna, a kolektiv, 2014).

Dle studie bylo zjištěno, že celkem 33 % dotázaných zároveň příliš nezná své přidané kontakty na sociálních sítích a následně celkem 81 % uvedlo, že jejich přidané kontakty vidí na jejich osobním profilu na sociální síti všechno, co sami jako vlastníci profilu na dělají (Ševčíková Anna, a kolektiv, 2014).

V roce 2014 proběhl v České republice výzkum, který mimo jiné zjišťoval, co děti a dospívající na internetu nejčastěji zveřejňují. Výzkumu se zúčastnilo celkem

14 877 dětí ve věku 11 – 14 let a 11 911 dospívajících ve věku 15 – 17 let Nejčastěji je dle výzkumu zveřejňováno jméno a příjmení, tuto informaci o sobě zveřejňuje 77 % z dotázaných, 56 % zveřejňuje fotku obličeje, 56 % e-mail. Z výzkumu zároveň vyšlo najevo, že až 63 % dětí a dospívajících by bez obav zaslali lidem, které nikdy nepotkali své jméno, 44 % e-mail, 39 % fotku obličeje a 38 % dokonce své soukromé telefonní číslo (E-bezpečí, 2014).

4 Šikana a kyberšikana

Teoretická část se dále vzhledem k zaměření bakalářské práce zaměřuje na oblast kyberšikany a zahrnuje další oblasti pojmů, které s rizikovým chováním na internetu úzce souvisí.

Oba termíny - šikana i kyberšikana - jsou spolu vzájemně úzce propojeny. Oběť, která zažívá tradiční šikanu, může s velkou pravděpodobností zažívat právě i kyberšikanu. Pomyslná hranice mezi těmito dvěma pojmy je tak velice úzká a oba termíny vzájemně sdílí množství velice podobných znaků a projevů. V případě šikany se však celá situace odehrává v rámci přímého kontaktu s lidmi, a naopak v rámci kyberšikany zacházíme do oblasti anonymního internetového prostředí (Říčan, 2010).

4.1 Šikana

Šikana je typ agresivního chování, které probíhá za určitých podmínek. Podstatou celé šikany je konkrétní forma agresivního chování (Janošová a kol., 2016).

Šikana probíhá na oběti, která se nedovede nebo nemůže se sama bránit a má stejné postavení jako ostatní v okolí. Typickým příkladem je například škola. Nejdůležitější částí procesu šikany je pak vznik asymetrického mocenského vztahu mezi obětí a agresorem. Tento asymetrický vztah může být způsobený postavením žáků ve třídě. Agresorem je ten, kdo oběť aktivně šikanuje, začíná jí a zároveň jí vede. Typickým příkladem agresora je ten, kdo je tělesně zdatný, oproti oběti. Agresor má tendenci se vyjadřovat hrubě avšak před autoritami se zpravidla tváří nevině, aby vzbudil dojem, že on sám není iniciátorem šikany. Agresorem zároveň bývá osoba, která je horkokrevnější, často se zaplétá do konfliktů a šarvátek s ostatními, takový člověk má tendence porušovat školní řád, kvůli čemuž se dostává do dalších potíží, díky svému chování může obdržet i snížené známky z chování. S chováním se snoubí slabší prospěch agresora ve studiu, neplní své školní povinnosti a není příliš zdatný ve vyučované látce. Agresor nemá při svém konání žádné výčitky svědomí a dělá mu dobře, když vidí, že má nad někým moc. Agresor si šikanou vynahrazuje vlastní nízké sebevědomí nebo nedostatky, kterými naopak jeho oběť trpět nemusí. Může dojít i k závisti např., dobře fungující harmonické rodiny, kterou agresor nemá, a proto šikanuje oběť, která je pravý opak jeho samého. Agresor je často mezi ostatními

neoblíbený a jeho nadřazenost a respekt je vyvolaný pouze skrz strach. Takový člověk rád manipuluje skrz své postavení s ostatními a přiživuje tím celkovou šikanu na své oběti. Zároveň má sklony krutým a zlomyslným činům, agresor často není schopen empatického myšlení a nemá tím pádem potřebu se, jakkoliv ve své šikaně krotit (Říčan, 2010).

Charakteristika oběti agresora se může různit. Prvním příkladem mohou být osoby, které se jeví pro agresora jako „divné“ či „slabé“, patří sem osoby, které jsou plaché, nezačleňují se tolik do kolektivu a spíše sedí stranou od ostatních. Špatně snáší kritiku a mají nízké sebevědomí. Další potenciální obětí agresora je osoba postižená fyzicky či mentálně nebo trpící nemocí, zároveň se agresoři rádi zaměřují na osoby slabší tělesné konstituce, které pro ně už od pohledu nepředstavují riziko, že by se mohly začít bránit nebo by mohli agresorovi po fyzické stránce vzdorovat (Říčan, 2010).

I ve škole však může nastat stav kdy dochází k šikaně ale mezi osobami, které mají rozdílné postavení. Příkladem je pak šikana mezi profesorem a studentem kde mohou být obě strany buď agresorem nebo obětí (Martínek, 2009).

4.2 Dělení šikany

Šikana se dělí na dva základní druhy, a to šikanu přímou a nepřímou. V případě přímé šikany jde o proces, kdy dochází k fyzickému násilí nebo poškozování věcí oběti. Stejně tak se projevuje formou nadávek a vulgarismů. Nejklasičtějším příkladem nepřímé šikany je pak ignorování oběti, vyčleňování jí z kolektivu. Agresorovi v tomto případě jde o to, oběť co nejvíc izolovat od společnosti (Říčan, 2010).

Martínek (2009), následně dělí šikanu ještě na několik dalších druhů:

1) **Fyzická aktivní přímá** je taková, při které dochází k fyzickému násilí vůči oběti.
2) **Fyzická aktivní nepřímá** je šikana, při které agresor využije jinou osobu, aby za něj páchala fyzické násilí na oběti. Sám pak pouze šikaně přihlíží a využívá druhých, aby ubližovali oběti místo něj.

3) **Fyzická pasivní přímá** probíhá v momentě, kdy se agresor pokouší oběti zabránit v jejích úmyslech. Příkladem pak může být třeba krádež psacích pomůcek, aby oběť si oběť při vyučování nemohla psát poznámky.
4) **Fyzická pasivní nepřímá** probíhá při odmítnutí požadavků oběti agresorem ve věcech, které nějakou formou oběť zahrnují. Příkladem může být takové odmítnutí pomoci.
5) **Verbální aktivní přímá**, tento typ šikany bývá jedním z nejběžnějších, zejména pak na školách. Dochází při ní k aktivnímu slovnímu napadání oběti, jejímu zesměšňování a celkově se při ní agresor snaží slovní formou oběti co nejvíce ublížit.
6) **Verbální aktivní nepřímá** je úmyslné rozšiřování drbů a pomluv mezi dalšími lidmi vůči oběti, stejně jako předchozí typ verbální aktivní šikany bývá i tento hojně rozšířen zejména na školách. Oběť se o pomluvách na svou osobu pak dozvídá až v průběhu času. Agresor se snaží kritizovat oběť ve všech směrech, od způsobů jejího chování a vystupování až po takové věci jako je způsob oblékání.
7) **Verbální pasivní přímá** se projevuje ignorováním oběti za všech okolností. Agresor na ni nereaguje, nevnímá ji, když se s ním pokouší navázat kontakt a předstírá, jakoby oběť vůbec neexistovala.
8) **Verbální pasivní nepřímá** šikana se objevuje zejména v případech, kdy jsou šikanováni problémoví žáci. Příkladem pak může být situace, kdy agresor provede něco proti pravidlům a svede své konání právě na onoho problémového žáka, který pak je nespravedlivě potrestán. Agresor se v tomto případě snaží cokoliv svést na problémové žaky, aby nenesli odpovědnost za své vlastní jednání.

4.2 Kyberšikana

Kyberšikana, se může považovat za samostatný fenomén, který nemá nic společného s tradiční šikanou. Opak je však pravdou a kyberšikana je naopak rozšířením tradiční šikany. Ohroženi kyberšikanou jsou v dnešní době obzvlášť

dospívající a děti, kteří mají díky moderním technologiím k internetu takřka stálý přístup (Geisslerová, 2012).

Je třeba zmínit, že kyberšikanou nebývají zasaženi jen děti a dospívající ale i učitelé, ti pak mohou být kyberšikanováni nejen svými vlastními žáky ale i rodiči a v některých případech je agresorem cizí osoba, která si svou oběť zvolila, aniž by se s ní, kdy dostala do styku (Kopecký, Szotkowski, 2016).

Problémem však zůstává absence informovanosti o možných rizicích, která jsou právě s těmito technologiemi úzce propojena. Kyberšikana probíhá prostřednictvím internetu, konkrétně skrz sociální sítě, chatovací aplikace (Whatsapp, Instagram) nebo třeba prostřednictvím mobilních telefonů. Člověk, který má v úmyslu někoho šikanovat prostřednictvím internetu, využívá právě anonymitu, kterou mu internetové prostředí poskytuje, oběť tak ani nemusí mít tušení, kdo přesně ho šikanuje vzhledem k tomu, že útočníci častou využívají falešných jmen a profilů (Geisslerová, 2012).

Za kyberšikanu se nepovažují projevy nesouhlasů, vyjádření opačného názoru nebo vulgarismy v rámci diskuse na účet druhého člověka. Kyberšikana sdílí s šikanou množství obecných rysů a jedním z nejdůležitějších je právě ten, že v obou případech pachatel oběť šikanuje dlouhodobě (Kožíšek, Písecký, 2016).

Nicméně tyto rysy a projevy nabývají především díky internetu o něco jiných měřítek. Kyberšikana je neustále se prohlubující a rozšiřující fenomén, ani dnešní specialisté nedokázali dojít k jednoznačné shodě v rámci její definice což má za následek, že se jednotlivé publikace a odborné články mohou v různých výzkumech a měřeních rozcházet. Priceová a Dalgleish (2010, s. 51), definují kyberšikanu jako: „Kolektivní označení forem šikany prostřednictvím elektronických médií. Stejně jako tradiční šikana zahrnuje i kyberšikana opakované chování a nepoměr sil mezi agresorem a obětí.“

Kyberšikana lze dále dělit na verbální a neverbální, která má zastoupení jak v přímé i nepřímé formě kyberšikany a dále pak na fyzickou v případě přímé kyberšikany a na sociální v případě nepřímé kyberšikany (Černá a kol., 2013).

Za **přímou kyberšikanu** lze považovat tu, kde se agresor aktivně nějakým způsobem projevuje formou útočení na svou oběť s úmyslem jí přímo svými činy ublížit a zesměšnit, aniž by došlo k jakémukoliv fyzickému násilí. Pachatel tak na rozdíl od tradiční šikany nemusí pro ublížení své oběti udělat nic víc než například umístit její intimní fotky na internet nebo jí zasílat výhružné zprávy prostřednictvím komunikačních technologií (Černá a kol., 2013).

Nepřímou kyberšikanu agresor vůči své oběti projevuje i prostým způsobem jako je vyčlenění z kolektivu. Na rozdíl od reálného světa, v rámci kyberšikany je to pak vyloučení z dnes tak populárních komunikačních prostředků jako je například Facebook. Útočník tak velice snadno bez udání jakéhokoliv důvodu svou oběť může opakovaně odebírat z facebookových skupin, aniž by za to byl, jakkoliv potrestán (Černá a kol., 2013).

Tato forma kyberšikany bývá pro oběť daleko více stresující než v případě přímé kyberšikany. Proti této formě kyberšikany má oběť sama jen velice malé možnosti, jak se bránit a jak jí vzdorovat (Říčan, 2010).

Černá a kol., (2013). dále dělí kyberšikanu na:

1) **Fyzická přímá kyberšikana** zahrnuje například nahrávání intimních materiálů o oběti na internet, ať už to jsou fotografie nebo videa.
2) **Verbální přímá kyberšikana** nastává v okamžiku, kdy útočník své oběti posílá nenávistné, vulgární či výhružné zprávy prostřednictvím internetových komunikačních prostředků.
3) **Neverbální přímá kyberšikana** je typ chování, kdy jsou oběti zasílány různé formy výhružných nebo vulgárních obrázků.
4) **Sociální nepřímá kyberšikana** se projevuje neustálým vyčleňováním oběti z kolektivu, v případě internetového prostředí je to pak vyloučení ze skupin na Facebooku apod.

5) **Verbální nepřímá kyberšikana** se projevuje pomlouváním oběti na sociálních sítí za jejími zády, šíření soukromých informací nebo zveřejňování soukromých konverzací s dalšími osobami.
6) **Neverbální nepřímá kyberšikana** je jedna ze stále častěji se objevujících se forem kyberšikany. Pachatel se vydává na internetu za někoho jiného, než je ve skutečnosti a díky této anonymitě má možnost zesměšňovat svou oběť, která si tak myslí, že nenávist vůči ní jde i od dalších osob. Zároveň do této kategorie patří i falešné nahlašování závadného nebo nevhodného obsahu v rámci internetových příspěvků oběti správcům síti a administrátorům (Černá a kol., 2013).

   V případě neverbální nepřímé šikany je velice obtížné agresora najít a usvědčit, internetová anonymita mu zajišťuje takovou formu ochrany, že se nemusí obávat trestu. Tato kyberšikana bývá agresory také používaná nejčastěji (Willard, 2007).

4.2.2 Technologie (prostředky) k šíření kyberšikany

Komunikační technologie můžeme rozdělit na čtyři konkrétní druhy:

a) **Synchronní** jsou takové, kdy spolu lidé komunikují v reálném čase, příkladem může být typický chat nebo hovor skrz dnes velice populární komunikační platformu Discord.

Chat je synchronní komunikační prostředek, který je veřejný, avšak má možnost se stát prostředkem soukromým, v případě, že se přesune do uzavřených skupin, chatovacích místností apod (Willard, 2007).

b) **Asynchronní** jsou ty, kdy osoba odešle zprávu a následně může čekat i v řádu hodin, než dostane od adresáta odpověď. Tato forma komunikace probíhá zejména prostřednictvím E-mailů.

E-mail může být odeslán velkému množství lidí, ale může být odeslán i pouze jednomu člověku (Willard, 2007).

Komunikace prostřednictvím e-mailu je i v dnešní době mezi pachateli kyberšikany velice oblíbená vzhledem k tomu, že je velice obtížné a téměř

nemožné, zjistit skutečnou totožnost majitele e-mailové adresy (Černá a kol., 2013).

Diskusní fóra fungují na principu e-mailové komunikace, osoba umístí na fórum příspěvek a kdokoliv se k tomu může vyjádřit. Odpovědi se tak mohou objevovat v řádu minut ale i hodin a dní. Právě zde se nejčastěji objevuje ostrakizace a flaming (Černá a kol., 2013).

Blogy jsou tzv. mix mezi webovými stránkami a diskusními fóry a jsou tedy označeny za asynchronní veřejné komunikační prostředky. Blogy slouží nejčastěji jako interaktivní deníky nebo články. Vlastník blogu může na takové stránce sdílet krom textových informací i videa, fotky, obrázky i nahrávky (Willard, 2007).

Na blozích může kyberšikana probíhat ve formě flamingu, kdy pachatel chce autora před všemi čtenáři zesměšnit a urazit, nebo kyberšikana můžeme probíhat tím způsobem, kdy vlastník blogu má v úmyslu prostřednictvím svých příspěvků očernit a ztrapnit oběť. V tomto případě je frustrace oběti umocněna tím, že k příspěvek si může přečíst každý kdo na blog zavítá a taktéž má prostor se k příspěvku sám vyjádřit (Černá a kol., 2013).

c) **Soukromé** jsou takové komunikační prostředky kdy, komunikace mezi lidmi probíhá v soukromých/uzavřených skupinách, chatech kam mají přístup jen určití lidé nebo komunikace probíhá čistě mezi dvěma lidmi. Důležité je ovšem zmínit, že žádná komunikace není zcela soukromá, každou zprávu, která je v takovýchto skupinách, chatech a konverzacích zveřejněna, může být dál přeposlána.
d) **Veřejné** prostředky jsou ty, které má možnost si prohlédnout prakticky kdokoliv. Patří k nim např. komentáře a diskuse pod články, příspěvky apod.

4.2.3 Projevy kyberšikany

Kyberšikana zahrnuje množství dalších pojmů, a různé konkrétní druhy a projevy kyberšikany. Formy kyberšikany lze rozdělit do dvou oblastí. První oblastí jsou projevy samotné kyberšikany a druhou oblastí jakou formou jsou tyto projevy realizovány (Černá a kol., 2013).

Mezi nejčastější projevy kyberšikany patří rozesílání obtěžujících, urážlivých nebo výhružných zpráv nebo pořizování fotografií, videozáznamů a následné umísťování na internet s cílem oběť poškodit. Do projevů kyberšikany se řadí i vydírání a posmívání se oběti skrz získaný intimní materiál, obtěžování a pronásledování oběti skrz internet. Do projevů kyberšikany řadíme i např. krádež identity, kdy celá kyberšikana probíhá pod identitou někoho jiného. V neposlední řadě stejně jako u tradiční šikany je součástí kyberšikany pomlouvání oběti, její provokování a očerňování, v tomto případě však prostřednictvím internetových komunikačních prostředků (Kohout, Karchňák, 2016).

V následujících kapitolách budou popsány různé projevy kyberšikany:

1) Phishing by se dal volně přeložit jako tzv. „rybaření“. Pachatel se v tomto případě pokouší od oběti získat např. přihlašovací údaje k e-mailům, účtům apod. nebo citlivé a osobní informace. Pachatel se v tomto případě může i vydávat za někoho jiného, ať už pouze jinou osobu nebo i za přímo za společnost. Cílem celého procesu je následně získané informace zneužít. Míra zneužití údajů může být různá, od utrácení peněz z bankovního účtu oběti po samotné vydírání (Kožíšek, Písecký, 2016).

2) Outing označuje činnost, kdy pachatel záměrně zveřejňuje informace o oběti nebo rovnou zveřejňuje její textové konverzace někomu, komu nebyla původně určena. Oběť si myslí, že pachateli může zcela důvěřovat a prostřednictvím internetových komunikačních prostředků s ním komunikuje a sděluje mu osobní informace. Pachatel v tomto případě může dalším lidem sdílet nejen text ale i fotografie a videa (Černá a kol., 2013).

3) Kyberstalking má mnoho společného s klasickým „Stalkingem“ neboli dlouhodobým a systematickým pronásledováním a obtěžováním oběti (Kožíšek, Písecký, 2016). V případě Kyberstalkingu je to však prostřednictvím informačních technologií kdy pachatel může oběť i vydírat (Willard, 2007), či jí vyhrožovat i fyzickým napadením nebo jí sexuálně obtěžovat zasíláním obscénních zpráv (Černá a kol., 2013).

4) Flaming je možné volně přeložit jako „rozohňování se“. Za flaming se označuje chování pachatele, kdy má v úmyslu svou oběť opakovaně

poškozovat formou výsměchu, nadávek a prudce vyostřených diskusích kdy zachází i k běžnému použití vulgarismů. Pachatel si záměrně např. vyhledává komentáře od oběti u cizích článků a začne se s ní schválně hádat a zesměšňovat jí. Flaming může pachatel provádět jak pod skutečnou, tak pod cizí nebo vymyšlenou identitou (Willard, 2007).

5) Ostrakizace – vyloučení z kolektivu je forma kyberšikany, kdy je oběť vyloučena ze skupin na internetových platformách jako je např. Facebook, ač v konkrétní skupině byla členem. Pachatelovým úmyslem je v tomto případě dát jasně najevo, že o oběť ve skupině nikdo nestojí, a tak jí z těchto skupin odebírá a nedává ani oběti vědět v případě, že se nějaká skupina, o kterou by měla případný zájem, vytváří. Oběť následně zažívá pocit frustrace z důvodu absence naplnění potřeby někam patřit. Nejproblémovějším faktorem v případě ostrakizace je ten, že často vyloučení oběti ze skupiny je svědkem mnohem větší množství lidí než v případě stejné situace v reálném světě (Černá a kol., 2013).

6) Pomlouvání stejně jako v případě tradiční šikany je v kyberšikaně všudypřítomné pomlouvání oběti kdy je cílem jí sociálně poškodit nebo vyloučit. Problémem je v tomto případě fakt, že na internetu se informace šíří mnohem rychleji než v reálném světě, a tak se lživé informace o oběti dostanou mnohem rychleji k většímu množství dalších lidí (Černá a kol., 2013).

7) Harassment považujeme za chování, kdy pachatel neustále zasílá zprávy, které jsou obětí vnímány jako obtěžující a nepříjemné. Zprávy jsou zpravidla zasílány prostřednictvím zpráv na sociálních sítích. Jde o tzv. instant messaging, kdy pachatel oběti okamžitě co se připojí na síť, začne odesílat obtěžující zprávy. V případě harassmentu jde zpravidla o jednosměrnou komunikaci na rozdíl od flamingu protože oběť se snaží komunikaci s pachatelem ukončit a to i formou vulgarismů ve zprávách pachateli. Cílem vulgarismů a agresivního chování oběti je ale učinit přítrž dalšímu obtěžování (Willard, 2007).

8) Sexting

Termín sexting je složený ze slov sex a text, jde tedy o intimní internetovou textovou komunikaci, při které však může docházet mimo jiné i k odesílání fotografií, audio nahrávek či videozáznamů se sexuálním obsahem. Sexting probíhá nejčastěji v rámci milostného vztahu mezi lidmi, bývá nejčastěji zneužit jednou z osob v případě ukončení milostného vztahu. Sexting často provádějí i nezletilé a mladistvé osoby, a proto je považován za vysoce rizikové chování (Kohout, Karchňák, 2016).

Sexting sebou přináší velké množství rizik, které je třeba brát v potaz, mezi příklady možných rizik patří:

1) Možný útočník obdrží explicitní materiál, který může v budoucnu použít jako prostředek k vydírání a zesměšňování oběti.

2) V případě, že útočník zveřejní materiály na sociálních, sítích, blozích nebo třeba skrz e-mailové zprávy, je prakticky nemožné je definitivně smazat vzhledem k tomu, že si je během chvíle, kdy byli na internetu zveřejněny, mohl kdokoliv zkopírovat či stáhnout do svého počítače. Tyto materiály se pak mohou na internetu objevit znovu, i když už byli smazány.

3) V případě, že útočník sdílí sexting na veřejnosti, dopouští se tak z právního hlediska trestního činu.

4) Sexting bývá často použit jako prostředek k vydírání prostřednictvím kybergroomingu (Kohout, Karchňák, 2016).

5 Prevence rizikového chování v kyberprostoru

5.1 Prevence kyberšikany

V případě kyberšikany je nejdůležitější, aby se problematikou zabývala celá společnost, ať už to jsou učitelé nebo rodiče. Kyberšikana je stejně jako tradiční šikana, problém, kterým je třeba se zabývat dřív, než vznikne, vzhledem ke stále rozšiřujícím se digitálním technologiím je třeba se věnovat zejména její prevenci. Tu mohou zajistit právě rodinní příslušníci a školní pracovníci, pokud bude z jejich strany probíhat dostatečná osvěta mladistvých, je možné značně snížit výskyt kyberšikany (Hollá, 2012).

Většina školských zařízení se obzvlášť problematice kyberšikany věnuje až v tom momentu, kdy již probíhá.

Většina škol i organizací se pokouší s již probíhající kyberšikanou bojovat blokací a mazáním závadného materiálu na internetu. Může docházet k zablokování účtů na platformách jako je Facebook, Twitter apod., skutečným problémem je nicméně to, že pokud kyberšikana již nějakou dobu probíhá, blokace a mazání závadného obsahu není nejvhodnějším řešením, vzhledem k tomu, že se již dávno může šířit na jiných internetových platformách ba i prostřednictvím e-mailů a diskusních fór a celá kyberšikana může probíhat jiným způsobem, než probíhala doposud. Blokování a mazání se pak spíš stává zmírněním již probíhající kyberšikany a nelze jí zcela považovat za plnohodnotnou prevenci.

V případě prevence internetové kyberšikany je třeba zajistit dostatečnou informovanost osob, neplatí zde ovšem tzv. „strašení“ internetem kdy osobám hrozíme a vlastně nic nesdělíme, naopak pokud by prevence probíhala touto formou, může mít spíš negativní než pozitivní výsledky.

Možnou formou preventivních programů je prevence zážitková, účastník takového programu prožívá konkrétní příběh, který mu pomáhá se naučit, jak správně v takovém případě jednat, na co si dát pozor a co by neměl dělat a na koho se v případě, že sám něco podobného někdy zažije, se může obrátit s prosbou o pomoc. Tato forma prevence umožňuje účastníkovi si uvědomit, že pokud se zachová určitým způsobem,

např., pošle někomu svou intimní fotografii, může se mu stát, že bude zneužita a veřejně rozšířena. Zážitková forma prevence je tak velice účinná a jednou z nejlepších způsobů prevence kyberšikany.

Další z možných forem prevence kyberšikany jsou mediální kampaně. Kampaň se vysílá prostřednictvím internetu ale i televize a má za účel v krátkých „spotech" sdělit velice stručně a obecně již výše zmíněné možné následky v případě, že se nechováme dle základních pravidel bezpečného pohybu na internetu.

Další možnou formou prevence kyberšikany jsou soutěže. V jejich případě jde o to upozornit veřejnost a účastníky soutěže na konkrétní problematiku rizikového chování a zajišťují účastníkům nové informace v dané problematice a zároveň je učí, jak se bránit a jak postupovat v případě, že se sami dostanou do situace, kdy je někdo „kyberšikanuje".

Poslední formou prevence kyberšikany jsou počítačové hry. V jejich případě jde o pozitivní ovlivnění chování osob a formování jejich osobnosti. Tato forma prevence se nicméně užívá velice zřídka (Kopecký, 2017).

5.2 Fake news

Pojem fake news je označení pro nepravdivé nebo zavádějící informace, nelze však tvrdit, že je tento pojem novým fenoménem. Fake news se dá volně přeložit jako dezinformace, cílem této dezinformace je ovlivnit druhé a zmanipulovat je tak, jak si autor těchto dezinformací přeje. Autor fake news může cílit jak na širokou veřejnost, tak na konkrétní skupiny, např. mladí dospívající. K šíření fake news se používá celá řada komunikačních prostředků, od tisku až po internetové portály. Příkladem společností, které v mnohých případech šíří úmyslně dezinformace jsou třeba bulvární časopisy, noviny a weby. V rámci pojmu fake news je třeba zmínit i termín fáma. Fáma bývá často mylně zaměňována s dezinformací, v případě fámy jde o šíření nepravdivé informace bez vědomí, že je nepravdivá. Lze tedy hovořit o typických drbech, které v mnohých případech neobsahují ani zrnko pravdy. Základním stavebním kamenem fake news je, aby se zakládali alespoň na částečně uvěřitelných a pravdivých informacích. Dezinformaci je třeba následně upravit, aby oslovila buď co největší počet lidí nebo, zaujmula jednu konkrétní skupinu (Vejvodová, Gregor, 2018).

Při čtení fake news si mnoho lidí právě zjištěné informace neověřuje a přijímají je jako fakt. Na vině může být hned několik důvodů. Prvním z nich je lidská lenost, lidé mají tendence nahlížet spíš k emocím než ihned racionálně přemýšlet a uvažovat, jestli právě přečtený příspěvek je pravdivý či nikoliv, obzvlášť pokud na první pohled bez dalšího ověřování působí věrohodně. (Kopecký, 2019).

Druhým důvodem je pak slepá víra v autority. V případě, že si čtenář přečte článek, který působí, že byl napsán např. lékařem a ten v něm doporučuje určitý produkt, ve většině případů lidé přijmou ten fakt, že pokud je to doporučeno lékařem, který se v tom zcela jistě vyzná, je to tedy v pořádku a určitě se jedná o pravdivý článek. Opak může být však pravdou. Šiřitel fake news se může za lékaře pouze vydávat a celý článek vypracoval a článek zaobalil pouze do odborných textů, aby čtenáře ještě více zmátl. Je však třeba zmínit, že ne vždy je šiřitel fake news podvodník nebo osoba, která chce vyvolat paniku nebo jen jistou formu reakcí, šiřitelem může být klidně politik, který je veřejně známý a ten zveřejní dezinformaci o svém politickém odpůrci, aby podkopal jeho postavení. (Kopecký, 2019).

Třetím důvodem, proč si někteří lidé neověřují informace je nízká technická a jazyková dovednost. V tomto případě můžeme zmínit uživatele internetu, kteří s moderními technologiemi neumí zcela pracovat, a proto např. nemusí ani vědět o tom, že jsou další seriózní webové stránky, kde by si o tématu mohli přečíst a informace si ověřit. (Kopecký, 2019).

Posledním důvodem, proč si lidé informace neověřují, může být tzv. Dunning-Krugerův efekt. Tento efekt mimo jiné zmiňuje lidskou nevědomost, kterou si sami neuvědomují. Na webových stránkách tak vidíme osoby, které se vyjadřují k tématu, a přitom o něm vlastně nic neví, skálopevně však budou obhajovat svou pravdu a dále diskutovat i když si sami neuvědomují, že jí nemají, když obhajují pro někoho jiného jasně falešný článek. Takové osoby nemají potřebu si informace dál ověřovat, protože je sami přece již dávno znají (Kopecký, 2019).

5.2.1 Prevence fake news

Nejlepší možností, jak se chránit před fake news je vyhledávat informace z ověřených zdrojů a následně si je ověřit. Je třeba vzít v potaz, že i seriózní

internetový portál se může stát obětí fake news a následně jeho neúmyslným šiřitelem, proto je důležité si informaci ověřit i z jiných zdrojů, je-li totiž informace pravdivá, je prakticky jisté, že se o ní bude zmiňovat více seriózních zdrojů (Hájková, K., Kráčmarová T., Vaněk L., 2021).

5.3 Spaming

Za spam považujeme e-mailové zprávy, které nás obtěžují a zahlcují naší e-mailovou schránku. Nejčastěji to jsou zprávy obsahující nevyžádanou reklamu, falešná oznámení o výhře nějaké částky či produktu nebo jím může být i tzv. řetězový dopis. Společným znakem jakéhokoliv spamu je to, že spamer má v úmyslu rozeslat co nejvíc podobných obtěžujících zpráv. Spameři získávají e-mailové adresy zejména ze sociálních sítí a diskusních fór, není to však pravidlem, v případě, že člověk zadá své údaje do formuláře falešné soutěže, získává spamer nebo jím vytvořený program e-mailovou adresu kam může své spam zprávy zasílat. Nejčastějším důvodem spammingu je neuvážené sdílení své e-mailové adresy na pochybných internetových stránkách (Horák, 2006).

V dnešní době se spam může využívat mnoha způsoby, k rozesílání nevyžádané reklamy ale nejčastěji pak k distribuci virů do počítačů oběti, která klikne na odkaz ve spamové zprávě. Samotná zpráva může vypadat zcela nevinně a stále se jejich podoba zdokonaluje, v některých případech projde i přes anti-spamové zabezpečení, která jsou v dnešní době na stránkách poskytující e-mailové služby samozřejmostí. Taková zpráva se pak tváří, že je naprosto legitimní a často uvádí odesílatele jako skutečnou firmu, a nejen podivnou e-mailovou adresu obsahující směs znaků. Oběť se pak může domnívat, že jde o skutečnou zprávu a ne falešnou, následně klikne na odkaz a do počítače se jí stáhne a nainstaluje virus, který může celé zařízení zablokovat a vydírat oběť. Nejčastěji jde pachateli, který virus vytvořil a rozeslal skrz spamovou zprávu o peníze. V případě, že oběť neodešle konkrétní částku na pachatelův bankovní účet, hrozí smazáním celého systému počítače (Horák, 2006).

5.3.1 Prevence spamu

Pokud je to možné, nikde nezveřejňovat svou emailovou adresu nebo pouze v nezbytně nutné míře, zamezí se tak drtivému množství nevyžádaných zpráv, které

nemusejí být jen otravné ale zároveň i potenciálně nebezpečné. Další možností, jak se proti spamu chránit je uvádět svou emailovou adresu „šifrovaně“ pro stroje. To znamená psát celou emailovou adresu slovně např. jméno(zavináč)seznam(tečka)cz. (Horák, 2006).

5.4 Kybergrooming

„Kybergrooming je psychická manipulace prostřednictvím moderních komunikačních technologií s cílem získat důvěru oběti, vylákat ji na osobní schůzku a zpravidla sexuálně zneužít.“ (Kohout, Karchňák, 2016, s. 49). Oběťmi kybergroomingu jsou zpravidla děti, dospívající a další důvěřivé osoby. Nejčastějšími oběťmi kybergroomingu jsou dospívající dívky, trpící nízkým sebevědomím a pocity osamění, které se pohybují na sociálních sítích a jejich komunikačních prostředcích. Kybergrooming je možné považovat za jakousi přípravu k sexuálnímu zneužití (Jansa a kol., 2017; Kohout, Karchňák, 2016).

Kybergrooming se objevuje primárně na platformách využívající instant messaging, tedy platformy, kdy dochází ke komunikaci v reálném čase, typickým příkladem je facebookový messenger, whatsapp apod (Kohout, Karchňák, 2016).

Kybergroomeři se často vydávají za někoho jiného a svou falešnou identitu upravují dle toho, s kým komunikují. Lidé, kteří takto „loví“ na sociálních sítích jsou schopní si s obětí psát i v řádu celých měsíců, je, aby si získali absolutní důvěru své oběti (Kohout, Karchňák, 2016).

5.4.1 Průběh kybergroomingu

1) Snaha získat si důvěru oběti a navázat s ní úzkou komunikaci.

2) Prohlubování přátelského vztahu, pachatel s obětí aktivně komunikuje, snaží se vzbudit dojem, že mu na ní záleží. Může dojít i k zasílání dárků nebo dokonce peněz.

3) Pachatel se snaží od oběti získat materiál (fotky, videa, informace), které by mohl v budoucnu využít jako prostředek k vydírání.

4) V této fázi se začíná dostavovat emocionální závislost oběti na útočníkovi. Oběť s ním komunikuje na mnohem osobnější úrovni a probírá s ním své problémy i intimní záležitosti.

5) Pachatel se snaží vylákat oběť na osobní schůzku. Častou záminkou pro schůzku je třeba pouhý návrh filmu v kině. Zpravidla se pachatel snaží domluvit konkrétní setkání na místě, které je odlehlejšího charakteru a je tak menší šance na setkání s náhodným kolemjdoucím.

6) V poslední fázi dochází k samotnému sexuálnímu zneužití nebo obtěžování. Pachatel nemusí nutně svou oběť zneužít, může jí však vydírat materiály, které získával během jejich komunikace a hrozit jejich zveřejněním, pokud oběť neudělá, co pachatel chce (Kohout, Karchňák, 2016).

5.4.2 Prevence kybergroomingu

Je třeba si uvědomit, že někdo někde na druhé straně obrazovky nemusí mít dobré úmysly, proto je třeba se chránit. Nejlepším způsobem jak se chránit právě proti kybergroomingu je pak omezit množství osobních informací, které o sobě šíříme na internetu. Mezi informace, které bychom rozhodně neměli nikam veřejně uvádět, patří: Adresa bydliště, adresa školy, hesla k účtům, rodné číslo, číslo mobilního telefonu, intimní fotky a videa (Kohout, Karchňák, 2016).

6 Tvorba vzdělávacího programu

Při tvorbě školního preventivního programu je třeba vzít v potaz, že pro něj má škola pouze omezené finanční, časové a personální prostředky, je proto zapotřebí co nejvíce klást důraz na co nejvyšší efektivitu programu. Program má dopředu jasně definovány cíle a musí být plánován tak aby mohl být řádně realizován (Miovský a kol., 2010).

Program pak musí zabraňovat nebo snižovat riziko výskytu rizikového chování a musí zajistit, aby byli žáci řádně informováni a byli schopni dělat zodpovědná rozhodnutí (Miovský a kol., 2010).

Při obecném plánování tvorby vzdělávacího programu je třeba dbát určitého postupu. Jako první je zapotřebí stanovit celkové pojetí vzdělávání v rámci vzdělávacího programu, následně se zaměřit na to, jakou formou bude celý program probíhat a v neposlední řadě jaký má být profil absolventa programu (Kašparová a kol., 2012).

Předtím než ještě začne být program tvořen, se musí zhodnotit hned několik důležitých faktorů (Miovský a kol., 2010):

1) **Charakteristika školy a její vnitřní zdroje** – zde je zapotřebí mít dostatek informací od třídních učitelů, aby se zjistilo, jestli už se v jejich třídách někdy řešilo nějaké rizikové chování a případně jaké. Zjištěné informace se pak zužitkují při tvorbě samotného obsahu programu.
2) **Vnější zdroje školy pro tvorbu programu –** za vnější zdroje se považují ty, které jsou externí a je potřeba je pro tvorbu a realizaci programu zajistit. Patří sem třeba zajištění informací z různých odborných sociálních sítí, které se věnují danému tématu nebo třeba externí odborníci, kteří pomohou svým výkladem v rámci samotného programu.
3) **Monitoring –** aby se vytvořil dobrý program, je zapotřebí získat zpětnou vazbu od skupiny na, kterou cílíme. V případě žáků je pak žádoucí dotazník kde můžeme zjistit preference na průběh a obsah programu aby pro ně byl zajímavý.

4) **Stanovení cílů –** při tvorbě cílů programu je ideální se řídit metodou SMART čili, že cíl by měl být specifický, měřitelný, akceptovatelný, realistický a jasně časově vymezený. Školní programy prevence se soustředí primárně na krátkodobé cíle, snaží se dosáhnout nějakého okamžitého výsledku po skončení.
5) **Skladba aktivit –** aktivity programu musí být co nejlépe uzpůsobeny dané cílové skupině. Musí začínat brzy, musí být interaktivní a žáci během něj musí získat relevantní informace, které využijí v životě. Program by měl mít různé modelové situace, je prezentován kvalifikovaně a důvěryhodně a zároveň bere v úvahu specifika konkrétní školy.

V rámci tvorby vzdělávacího programu je třeba se školou dohodnout jakým způsobem bude celý program realizován a domluvit se na způsobech výuky a na metodických přístupech. Se školou je třeba domluvit se i na případných dalších aktivitách a činnostech, které budou zapotřebí vykonat, aby byl celý program proveditelný. Příkladem je (v případě, že je to pro program žádoucí) navázat kontakt s partnery, kteří pro program zajistí další obsah nebo materiální zajištění (projektory, promítací plátna nejsou-li k dispozici apod.) (Kašparová a kol., 2012).

Nejdůležitější částí, od které se pak odvíjí plánování celého vzdělávacího programu, a kterou je zároveň zapotřebí provést prvořadě, je stanovit si jasný profil absolventa. Pokud je profil jasně dán, může se následně přejít k plánování realizace vzdělávacího programu tak, aby byla kritéria, která byla stanovena profilem splněna. Při tvorbě profilu se vyjmenují klíčové kompetence, ty se formulují obecně a nemají uvádět žádné dílčí dovednosti a znalosti, které vycházejí z nějaké komplexní kompetence nebo z výsledků výuky konkrétních předmětů (Kašparová a kol., 2012).

PRAKTICKÁ ČÁST

Praktická část bakalářské práce obsahuje vyhodnocení výzkumných otázek a dotazníkové šetření a zahrnuje charakteristiku respondentů a návrh programu prevence.

7 Dotazníkové šetření

7.1 Metoda šetření

Kvantitativní dotazník se soustředí na sběr velkého množství dat oproti kvalitativnímu dotazníku. Dotazník se soustředí na jednoznačný cíl a otázky v dotazníku jsou co nejvíce konkrétní. Otázky jsou jednoznačně formulované, aby nemohlo dojít k jiné interpretaci respondenty. Odpovědi na samotné otázky jsou jasné, nepotřebují dalšího vysvětlování a jsou srozumitelné. Dotazník je objektivní a neprojevuje názory autora dotazníku (Chráska, Kočvarová, 2015).

Jako metoda sběru dat byla vybrána kvantitativní dotazníkové šetření, protože návrh programu prevence je určen pro školní prostředí a je tedy zapotřebí určit, jak se velké množství žáků chová, co zná a co preferují za vzdělávací postupy. Na základě velkého množství dat pak může být vytvořen adekvátní návrh programu prevence pro školy.

Cílem bylo zjistit jaké povědomí a znalosti o rizikovém chování na internetu žáci střední odborné školy mají, jak se sami v internetovém prostředí chovají a v neposlední řadě jakým způsobem získávají informace o rizikovém chování na internetu a jaký způsob dalšího vzdělávání v této oblasti by jim nejvíc vyhovoval.

Pro dotazníkové šetření byly stanoveny tyto výzkumné otázky:

1) Znají žáci pojmy z oblasti rizikového chování a jejich definice?

2) Jak žáci vnímají kyberšikanu?

3) Jak se žáci na internetu chovají?

4) Jak se na internetu chovají žáci, kteří si myslí, že je internet potenciálně nebezpečné místo a jak žáci, kteří si naopak myslí, že je internet relativně bezpečné místo?

Dotazníky byly rozdány mezi žáky střední odborné školy v počtu 130 kusů a vrátilo si jich celkem 104. Dotazník byl anonymní, obsahoval 24 otázek, které byly dále pak rozčleněny do pěti kategorií. První kategorie pokládala otázky obecného charakteru jako pohlaví a věk. Druhá kategorie byla ověřovací a měla za účel ověřit, jaké znalosti v oblasti rizikového chování žáci mají. Třetí kategorie se zaměřovala na povědomí o problematice kyberšikany. Zároveň cílem bylo zjistit, co všechno žáci považují za rizikové chování v rámci kyberšikany a jestli s ní někdy přišli do kontaktu. Čtvrtá kategorie zjišťovala, jak se žáci sami chovají na internetu a poslední pátá kategorie pokládala otázky, jejichž cílem bylo zjistit preference žáků na metody a způsoby dalšího vzdělávání v problematice internetových rizik. Kompletní znění dotazníku je uvedeno v Příloze č. 1.

7.3 Charakteristika respondentů

Dotazníkového šetření se zúčastnilo celkem 104 žáků ze střední odborné školy v Praze, škola si nepřála být jmenována. Většina respondentů byly ženy, muži i ženy byly ve věku 16 – 21 let, v dotazníku byl zastoupen 4., 3., a 2. ročník. V rámci dotazníku odpovídali žáci oboru oční optik, aplikovaná chemie a asistent zubního technika.

7.4 Vyhodnocení dotazníkového šetření

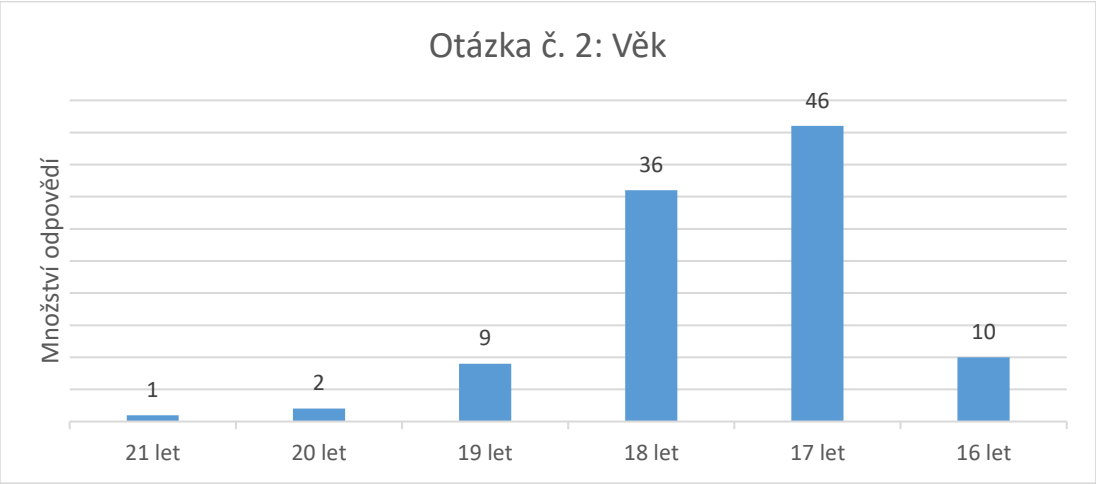
Otázka č. 1: Pohlaví

Na dotazník odpovídalo 66 žen a 38 mužů.

Otázka č. 2: Věk

Nejhojněji byli zastoupeni respondenti ve věku 17 let v počtu 46 (44 %), druhým nejvíce zastoupeným věkem bylo 18 let v počtu 36 (35 %) a následně 16 a 19 let, 10 a 9 osob (10 % a 9 %). Nejméně zastoupenou věkovou kategorií bylo 20 a 21 let, v počtu dvou a jedné osoby (2% a 1%).

Graf 1 Věk



Zdroj: vlastní zpracování

Otázka č. 5: Který z těchto pojmů nedokážete definovat?

V této otázce měli žáci možnost označit všechny nabízené pojmy, které by nedokázali jasně definovat. Z odpovědí bylo zjištěno, že největší množství žáků, celkem 77 (74 %), nedokáže definovat pojem Flaming, 59 (57 %) žáků pak pojem Kybergrooming, 42 (40 %) Outing, 42 (40 %) Harrassment, 14 (13 %) Phishing a 4 (4 %) žáci odpověděli, že nedokážou definovat pojem Sexting Pojem Kyberstalking byl zastoupen pouze jednou odpovědí (1 %). Pojmy Spamming, Fake news a Kyberšikana neoznačil ani jeden z dotazovaných (viz Graf 3).

Graf 2 Definice

Zdroj: vlastní zpracování

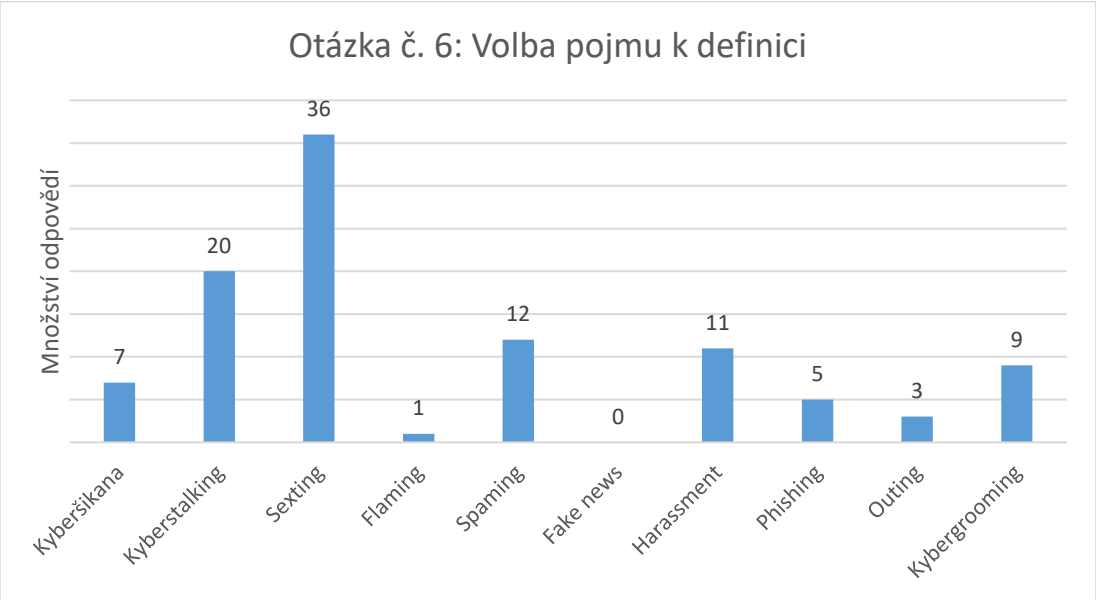
Otázka č. 6: „** je chování, kdy si pachatel na internetu vytipovává oběť, snaží se získat její důvěru, vybudovat s ní blízký vztah a vylákat ji k osobní schůzce. Cílem setkání je oběť zneužít.“**

V rámci této otázky měli žáci za úkol zvolit správný pojem k vypsané definici, v tomto případě pak pojem Kybergrooming. V případě této otázky bylo zjištěno, že ačkoliv u otázky č. 5 odpovědělo 59 (57 %) žáků, že neví co je to Kybergrooming, pouze 9 (9 %) respondentů vybralo tento termín k jeho definici, z čehož vypovídá, že si zbývající respondenti tento pojem zaměňují s pojmem jiným nebo naopak o něm nemají dostatek informací.

Při dalším vyhodnocování dotazníku se došlo k závěru, že nejčastější záměnou u tohoto termínu je termín Sexting, ten zvolilo nejvíce žáků v celkovém počtu 36 (35 %).

Dále pak 20 (19 %) žáků zvolilo termín Kyberstalking, Spamming – 12 (12 %), Harassment – 11 (11 %) , 7 (7 %) žáků zvolilo termín Kyberšikana a v nejmenším zastoupení byly termíny Phishing 5 (5 %), Outing 3 (3 %) a termín Flaming pouze zvolil jeden žák (1 %). Termín Fake news nezvolil nikdo z dotazovaných viz Graf 4.

Graf 3 Definice Kybergrooming



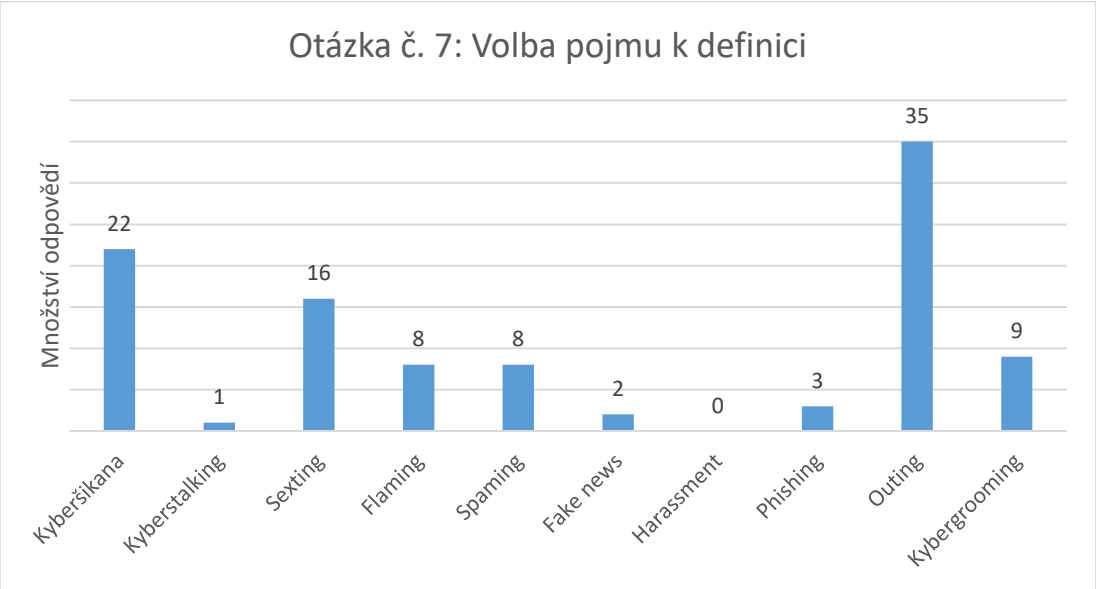
Zdroj: vlastní zpracování

Otázka č. 7: „** je zveřejňování soukromé a osobní komunikace, která proběhla formou textových zpráv nebo třeba emailů.“**

V případě otázky č. 7 měli žáci za úkol zvolit správný pojem k vypsané definici. V tomto případě byl správnou odpovědí pojem Outing. Tuto možnost zvolilo pouze 35 (34 %) žáků a stejně tak jako v předchozí otázce vyplývá, že zbývající žáci, kteří dle otázky č. 5 podle svého mínění dokážou pojem Outing definovat, si ho zaměnili za jiný pojem. 22 (21 %) žáků vybralo pojem Kyberšikana, 16 15 % žáků pojem Sexting, 9 (9 %) žáků vybralo pojem Kybergrooming.

Jak je z Grafu 5 vidět, pojmy Flaming a Spamming byly zastoupeny rovnoměrně celkem v osmi případech (8 %). Nejméně žáků zvolilo pojmy Phishing, 3 (3 %), Fake news 2 (2 %) a Kyberstalking jeden vybral pouze jeden žák (1 %). Harassment k vypsané definici nezvolil ani jeden respondent.

Graf 4 Definice Outing



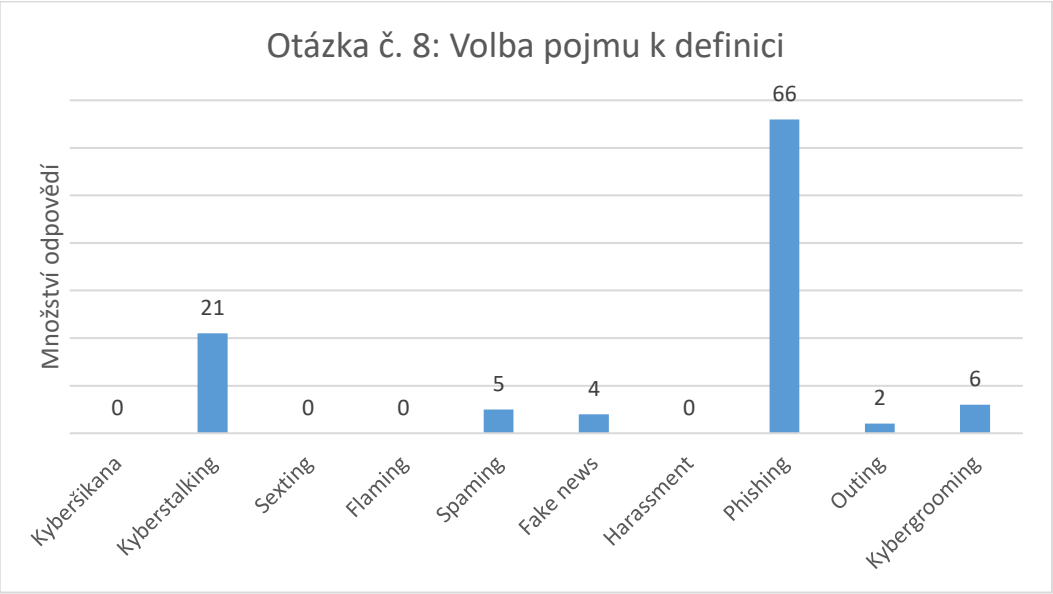
Zdroj: vlastní zpracování

Otázka č. 8: „** je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci.“**

U otázky č. 8 měli žáci vybrat správný termín Phishing, ten správně zvolilo celkem 66 z nich (63 %), jak ukazuje Graf 6 a ze všech otázek zaměřujících se na definice, se v tomto případě odpovědi žáků z více jak většiny shodovaly.

Dalšími zvolenými termíny byly Kyberstalking, ten vybralo 21 žáků (20 %), Kybergrooming – 6 (6 %), Spamming – 5 (5 %), Fake news – 4 (4 %) a jako poslední termín Outing 2 %. Pojmy Kyberšikana, Sexting, Flaming a Harassment nezvolil nikdo z respondentů.

Graf 5 Definice Phishing



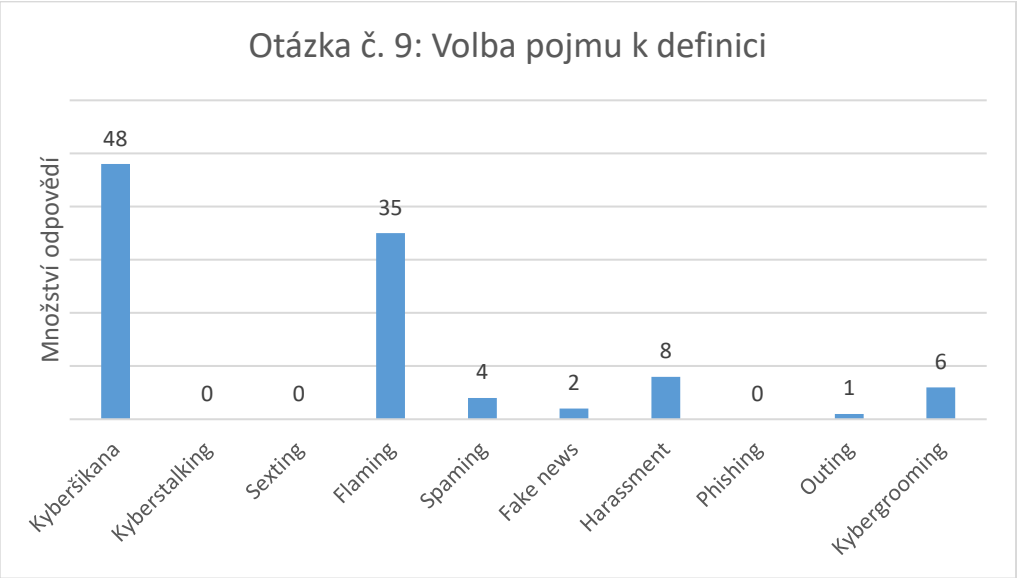
Zdroj: vlastní zpracování

Otázka č. 9: „** je virtuální agresivita, „rozohňování se," vědomě hostilní (nepřátelské) a urážlivé vzkazy na internetu s cílem někoho dehonestovat a rozčílit.“**

V případě otázky č. 9 došlo k nejlepším výsledkům v porovnání s odpověďmi z otázky č.5. Všichni žáci, kteří uvedli v otázce č. 5 (viz. Graf 3), že pojem Flaming dokážou definovat, jej správně zvolili i v otázce č. 9. Z toho vyplývá, že všichni žáci, kteří tento termín zvolili, museli být v rámci tohoto konkrétního pojmu nějakou formou dostatečně informováni.

Flaming zvolilo celkem 35 (34 %) žáků, Kyberšikanu 48 (46 %), Harassment 8 (8 %) žáků, Kybergrooming – 6 (6 %), Spamming – 4 (4 %), Fake news – 2 (2 %) a Outing zvolil jen jeden žák (1 %). Pojmy Kyberstalking, Sexting a Phishing nezvolil nikdo z respondentů (viz Graf 7).

Graf 6 Definice Flaming



Zdroj: vlastní zpracování

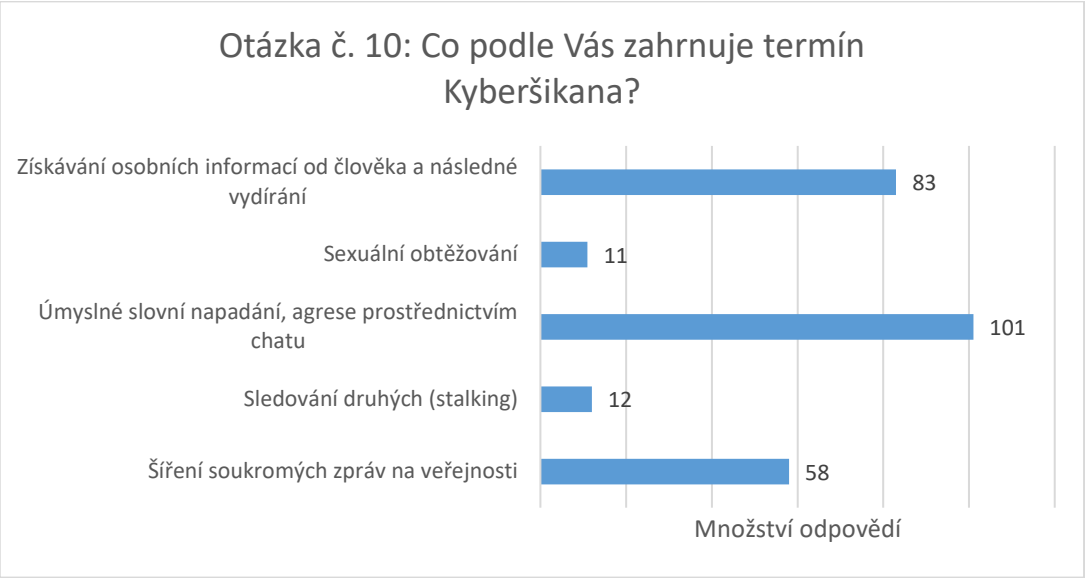
Otázka č. 10: Co podle Vás zahrnuje termín Kyberšikana?

Otázka měla zjistit co všechno dle názoru žáků se řadí pod pojem kyberšikana. Žáci měli možnost vybrat cokoliv z nabízených pěti nabízených možností. Mohli zvolit jednu ale i všechny odpovědi, přičemž v rámci této otázky byly všechny odpovědi správné a všechny jsou považovány za formu kyberšikany.

Nejvíce žáků 101 (97 %) odpovědělo, že do kyberšikany patří *úmyslné slovní napadání, agrese prostřednictvím chatu,* dle 83 (80 %) dotázaných pak *získávání osobních informací od člověka a následné vydíráním,* 58 (56 %) dotázaných soudí, že do kyberšikany patří *šíření soukromých zpráv na veřejnosti,* a pouze překvapivě 12 (12 %) žáků označilo *sledování druhých (stalking)* jako součást kyberšikany stejně jako pouze 11 (11 %) dotázaných se domnívá, že kyberšikana obsahuje *sexuální obtěžování.*

Z toho vyplývá, že žáci jsou nedostatečně informováni v oblasti kyberšikany a nevědí co všechno pojem kyberšikana zahrnuje, neuvědomují si, že kyberšikana není jen o agresivním chováním, zneužívání osobních informacích. V rámci kyberšikany se totiž může vyskytnout i sexuální obtěžování, které se projevuje zasíláním erotických fotografií nebo třeba stalkingem kdy útočník sleduje veškerou aktivitu jedince na internetu, stále ho obtěžuje apod.

Graf 7 Kyberšikana

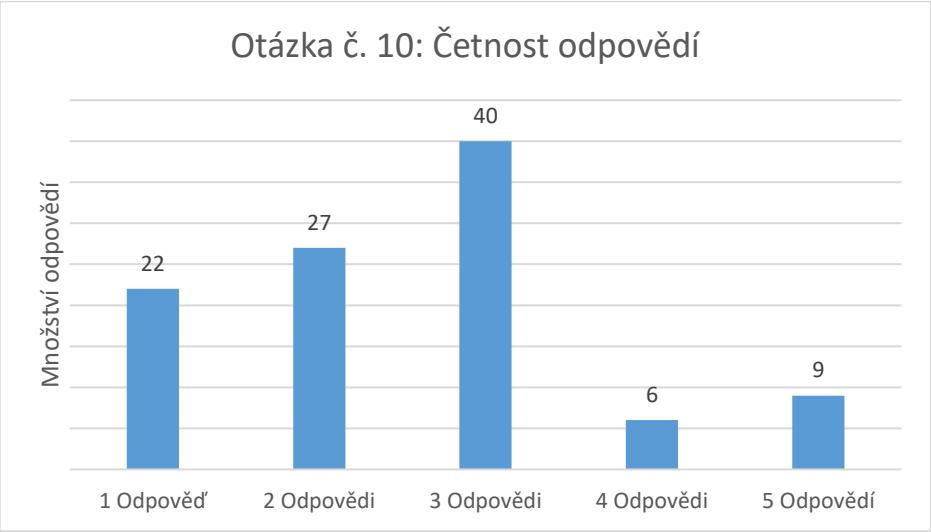


Zdroj: vlastní zpracování

V tomto případě se následně vyhodnocovalo i množství zaškrtnutých odpovědí. Nejčastěji žáci označovali tři odpovědi 40x (38 %), dvě odpovědi se objevily ve 27 případech (26 %) a jedna odpověď pak celkem ve 22 (21 %) případech.

Čtyři možnosti vybralo pouze 6 (6 %) respondentů a všech pět možností vybralo pouze 9 (9 %) dotázaných, z toho vypovídá, že většina žáků nemá dostatek informací o celé problematice a domnívají se tak, že pojem Kyberšikana zahrnuje jen určité pojmy.

Graf 8 Kyberšikana, četnost odpovědí



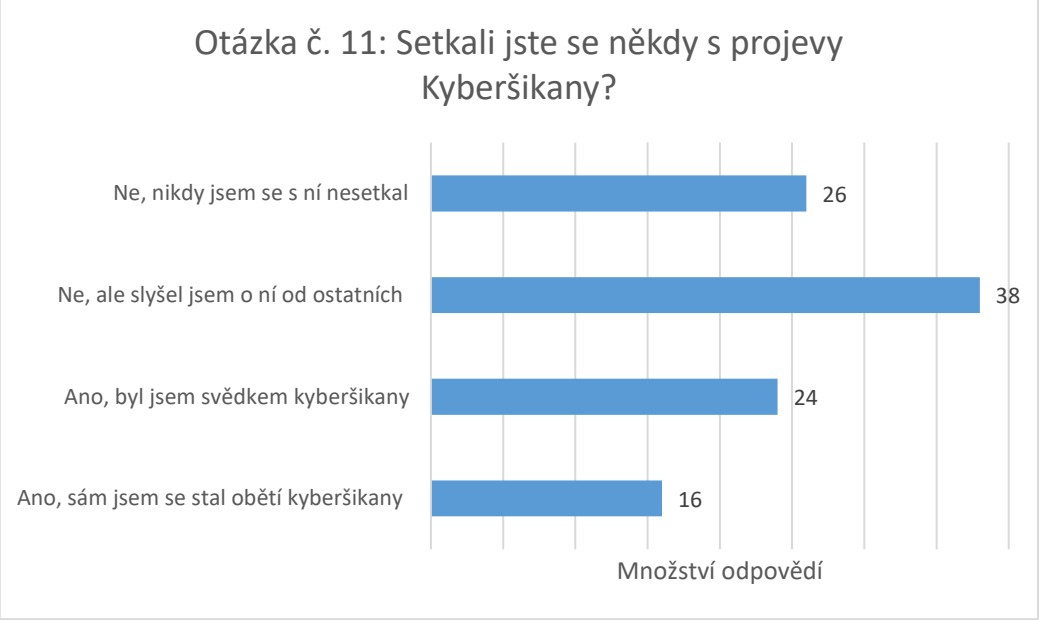
Zdroj: vlastní zpracování

Otázka č. 11: Setkali jste se někdy s projevy Kyberšikany?

Otázka č. 11 měla zjistit, jestli se žáci sami, kdy s Kyberšikanou dostali ať už přímo nebo nepřímo do styku. Bylo zjištěno, že pouze malé množství dotazovaných mělo s Kyberšikanou vlastní zkušenost. 16 (15 %) žáků uvedlo, že byli vystaveni sami kyberšikaně a 24 (23 %) uvedlo, že byli svědkem, když kyberšikanu zažívala druhá osoba.

38 (37 %) žáků zaškrtlo možnost ve, které tvrdí, že s Kyberšikanou nikdy neměli vlastní zkušenost, ale nějakou formou se o ní dozvěděli prostřednictvím dalších lidí a celkem 24 (23 %) respondentů pak uvedlo, že se s Kyberšikanou nikdy nesetkali, ani nepřišli do styku s osobou, která by podobnou zkušenost měla.

Graf 9 Zkušenost s Kyberšikanou



Zdroj: vlastní zpracování

Otázka č. 12: Ohodnoťte dle Vašeho názoru, jaká je bezpečnost internetového prostředí. (1 nejméně bezpečný, 10 maximálně bezpečný)

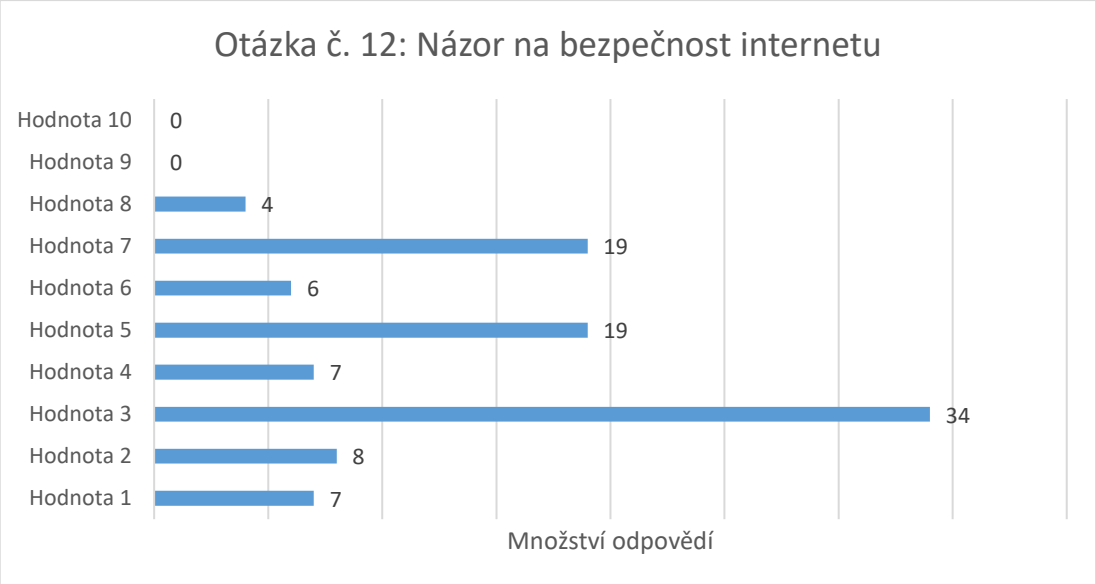
Zde se zjišťovalo, jaký mají respondenti názor na celkovou bezpečnost dnešního internetového prostředí, jestli si myslí, že jsou jejich údaje, které na internetu zveřejní v bezpečí apod.

Žáci kroužkovali možnosti od jedné do deseti, přičemž nižší hodnota znamenala, že se domnívají o nízké bezpečnosti internetu a vyšší hodnota znamenala vyšší domněnku o internetové bezpečnosti, viz Graf 11.

Zajímavé zjištění bylo, že žádný ze 104 respondentů nezakroužkoval hodnoty devět a deset, z toho vyplývá, že se nikdo z nich nedomnívá, že by byl internet zcela bezpečným místem.

Tato otázka byla klíčová pro vyhodnocování 4. výzkumné otázky. Ze 104 respondentů jich 56 (54 %) zakroužkovalo hodnotu 4 a méně, lze tedy usuzovat, že se domnívají, že internet je relativně nebezpečné místo a 29 (28 %) označilo hodnotu 6 a více čili mají na bezpečnost internetu opačný názor. Respondenti, kteří označili hodnotu 5 a měli tedy tak na bezpečnost internetu rozporuplný názor, nebyli pro vyhodnocování 4. výzkumné otázky bráni v potaz.

Graf 10 Názor na bezpečnost internetu

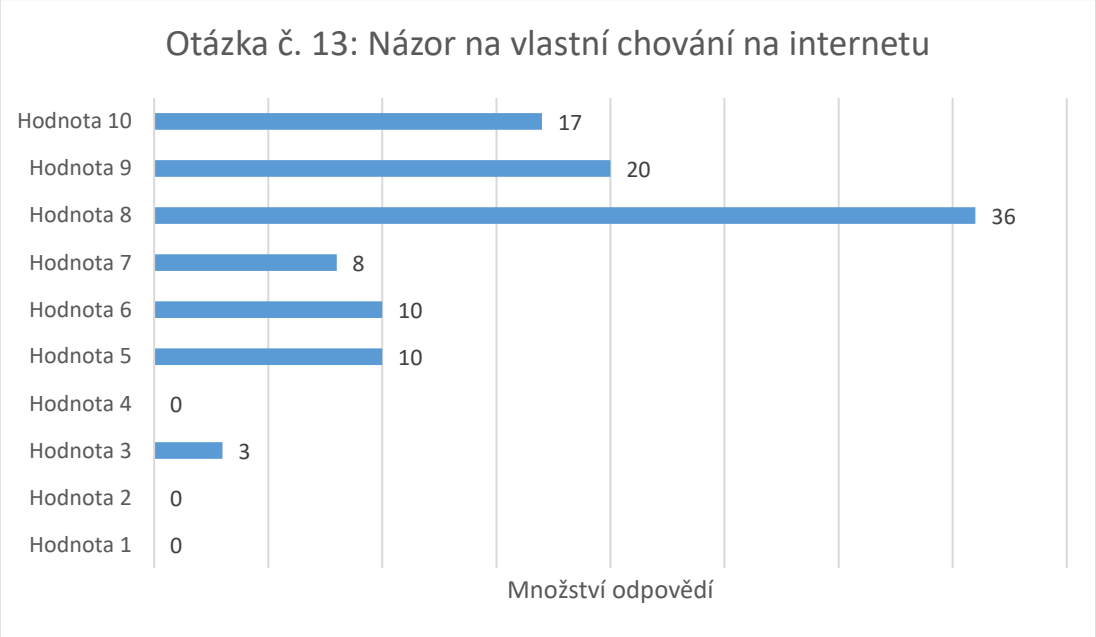


Zdroj: vlastní zpracování

Otázka č. 13: Domníváte se, že se na internetu chováte bezpečně? (1 nechovám se dle zásad bezpečného užívání internetu, 10 naprosto dodržuji zásady bezpečného užívání internetu)

Stejně jako v otázce č. 12 měli žáci zakroužkovat na stupnici od jedné do deseti (viz Graf 12), zdali se dle svého úsudku chovají na internetu v rámci pravidel bezpečného pohybu a užívání internetu. V tomto případě čím vyšší hodnota byla zvolena, tím více se respondent domníval, že se na internetu chová bezpečně, čím nižší hodnotu uvedl, tím více se domnívá, že se naopak na internetu chová rizikově.

Graf 11 Názor na vlastní chování na internetu

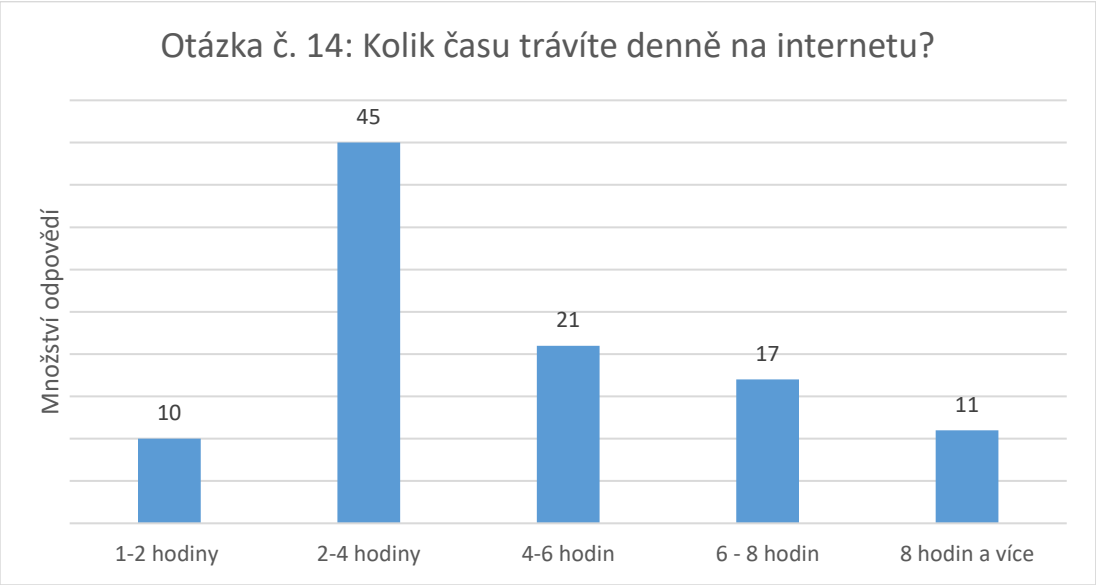


Zdroj: vlastní zpracování

Otázka č. 14: Kolik času trávíte denně na internetu?

Bylo zjištěno, že nejvíce respondentů, celkem 45 (43 %), tráví na internetu denně 2-4 hodiny. Dále pak 21 (20 %) jich uvedlo, že na internetu tráví 4-6 hodin, 17 (16 %) uvedlo, že 6-8 hodin a následně 10 (10 %) respondentů uvedlo, že na internetu tráví pouze 1-2 hodiny. 11 (11 %) respondentů zakroužkovalo možnost 8 hodin a více.

Graf 12 Trávení času na internetu



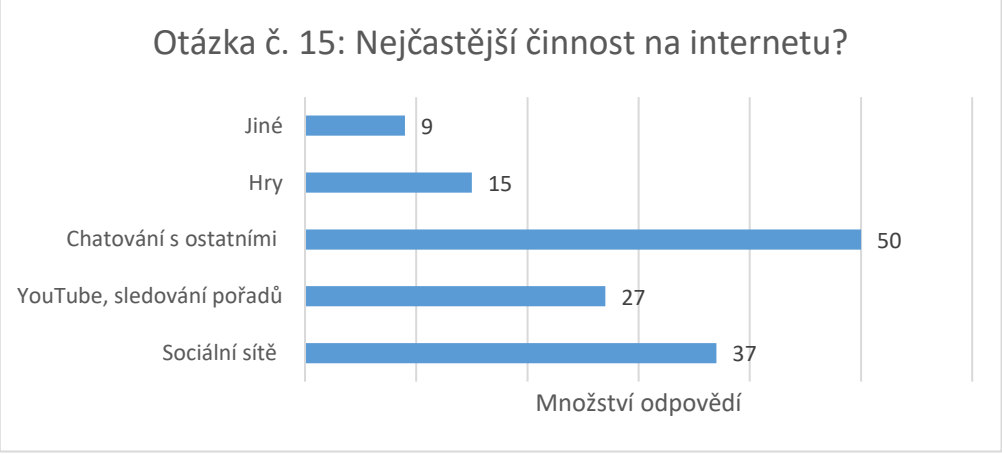
Zdroj: vlastní zpracování

Otázka č. 15: Ve výše uvedené době, co je vaší nejčastější činností?

U otázky č. 15 bylo možné zvolit jednu nebo i více odpovědí**.** Nejvíce respondentů uvedlo (viz Graf 15), že prostřednictvím internetu nejčastěji chatují s ostatními nebo jsou aktivní na sociálních sítích. Značná část respondentů zároveň uvedla, že na internetu tráví volný čas, sledováním seriálů, pořadů apod.

Menší část respondentů pak uvedla, že využívají internet ke hrám a pouze 9 (9 %) ze 104 označilo, že tráví na internetu čas jinak než výše zmíněnými aktivitami.

Graf 13 Nejčastější činnost na internetu



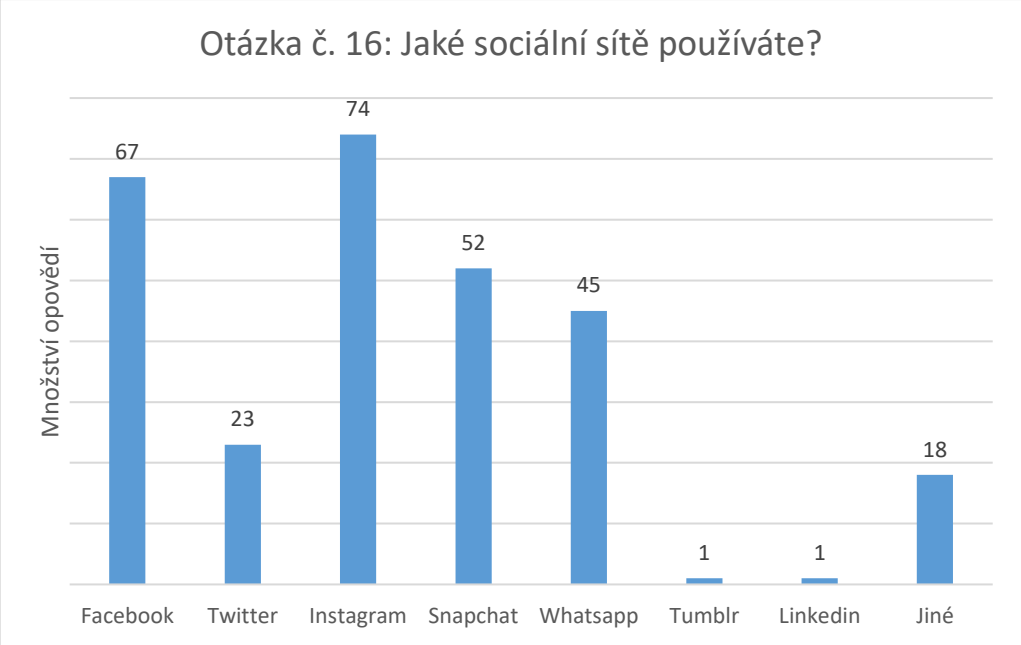
Zdroj: vlastní zpracování

Otázka č. 16: Jaké sociální sítě používáte?

Zde mohli respondenti označit větší množství odpovědí. Nejvíce, celkem 74 (71 %) jich uvedlo, že využívají sociální sítě Instagram, Facebook označilo celkem 67 (64 %) respondentů. 52 (50 %), 45 (43 %) a 23 (22 %) zakroužkovalo možnosti Snapchat, Whatsapp a Twitter. V naprosté menšině, byly sociální sítě Tumblr a Linkedin, ty byly zastoupeny pouze jednou (1 %).

Dalších 18 (17 %) dotázaných uvedlo, že využívá ještě jiné sociální sítě než byly v nabídce.

Graf 14 Sociální sítě



Zdroj: vlastní zpracování

Otázka č. 17: Ověřujete si informace co si na internetu přečtete i z jiných zdrojů?

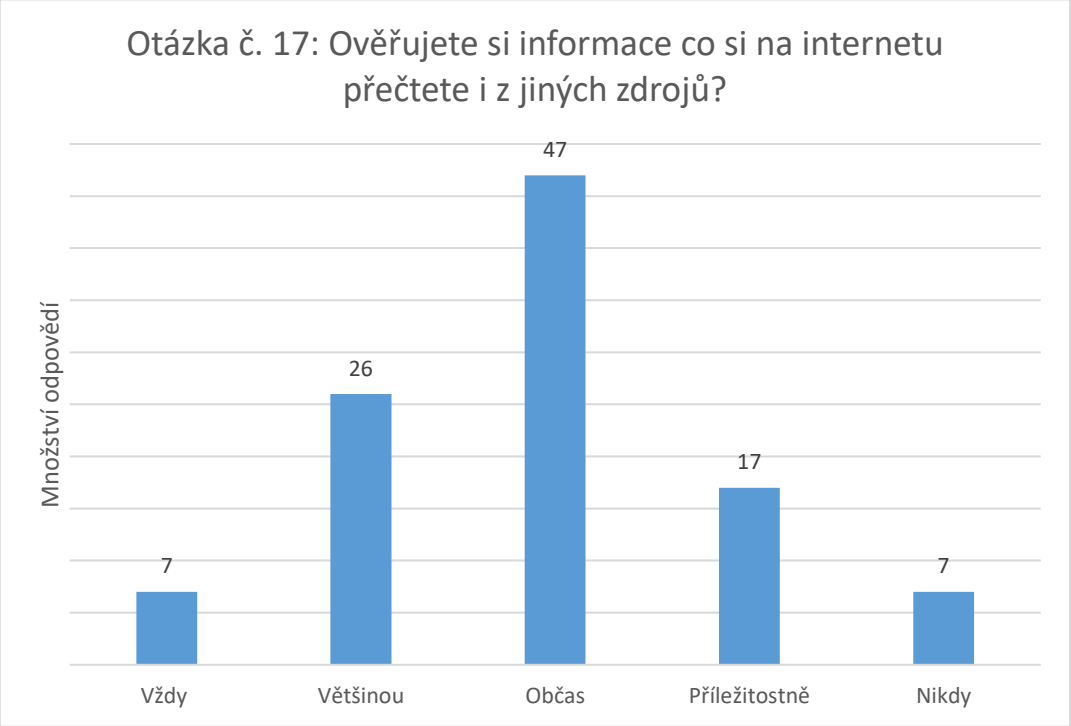
Zde bylo zjišťováno jestli si respondenti ověřují informace, ke kterým se na internetu dostanou nebo jestli zpravidla berou to čeho se dočtou jako hotový fakt.

Bylo zjištěno (viz Graf 16), že více jak polovina dotázaných si ověřuje informace pouze občas nebo ještě méně často. Pouze 26 (25 %) respondentů si většinou informace znovu ověřuje a pouze 7 (7 %) žáků, si právě přečtené informace jde ihned ověřit ještě z jiného zdroje. Z toho vyplývá, že velké množství žáků je náchylných k dezinformacím, fake news apod. a sami se tak mohou stát dalšími šiřiteli.

V rámci vyhodnocení 4. výzkumné otázky bylo zjištěno, že celkem 38 (68 %) osob z původních 56, kteří se domnívají, že internet je relativně nebezpečné místo si informace ověřují pouze občas či ještě méně.

Z 29 osob, které se naopak domnívají, že internet je relativně bezpečný následně 12 (41 %) uvedlo, že si informace ověřují občas či ještě méně.

Graf 15 Ověřování informací



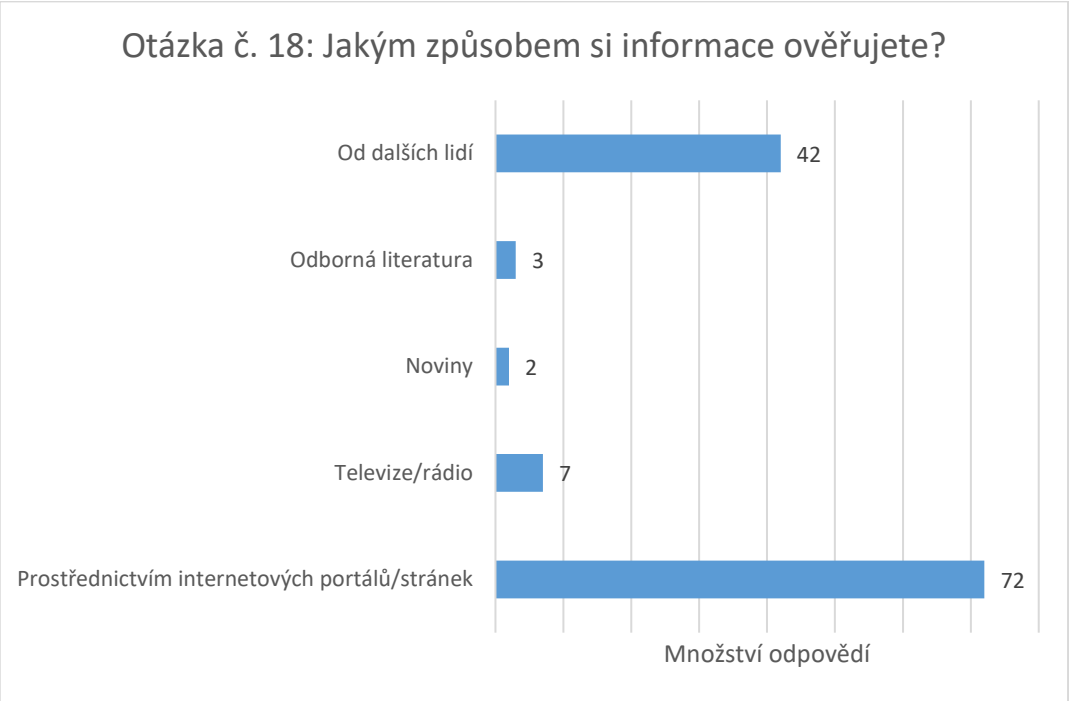
Zdroj: vlastní zpracování

Otázka č. 18 Jakým způsobem si informace ověřujete?

V návaznosti na otázku **č.17** bylo zjišťováno jakým způsobem si respondenti právě zjištěné informace nejčastěji ověřují. Odpovídající měli možnost v rámci této otázky vybrat i více možností.

Drtivá většina odpovídajících 72 (69 %) kroužkovalo možnost internetových stránek a portálů jako místo kde si informace ověřují, znatelná část 42 (40 %) uvedla, že si informace ověřují prostřednictvím dalších lidí a v menšině 7 (7 %),3 (3 %) a pouhých 2 (2 %) hlasů, byly označeny možnosti televize/rádio, odborná literatura a noviny.

Graf 16 Způsob ověřování informací



Zdroj: vlastní zpracování

Otázka č. 19: Byl/a jste někdy požádán/a o zaslání své intimní fotky?

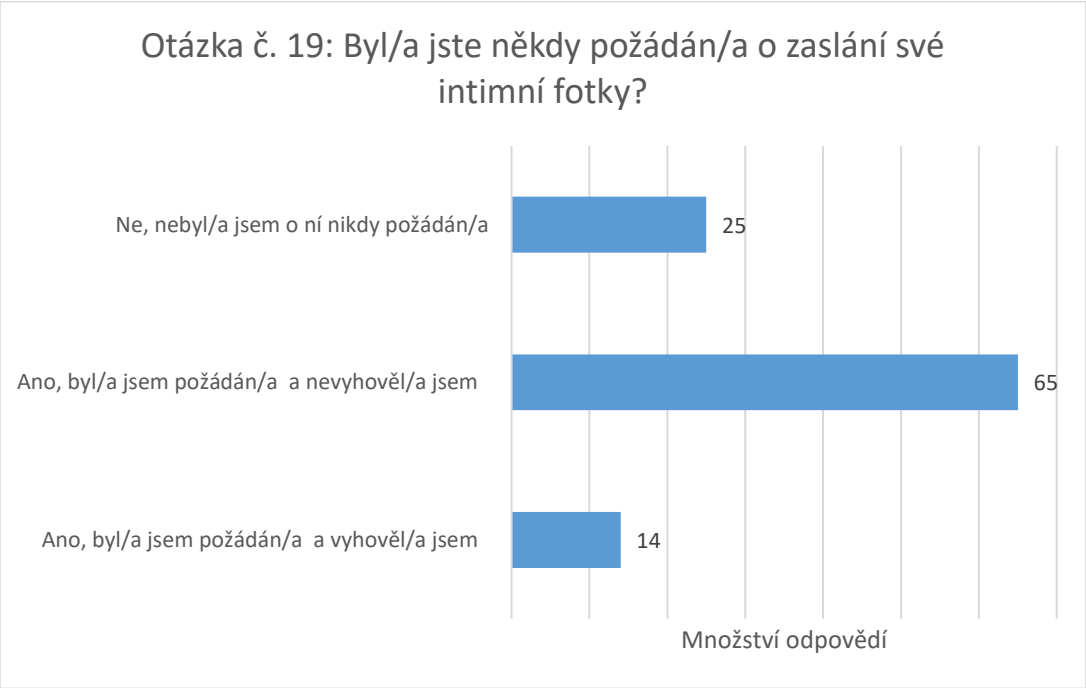
Otázka č. 19 měla zjišťovat jestli respondenti někdy poslali své intimní fotky dalšímu člověku nebo ne.

65 (63 %) dotázaných uvedlo, že byli někdy požádáni o zaslání intimní fotografie ale nevyhověli, 25 (24 %) pak, že o zaslání intmní fotografie nebyli nikdy požádáni a pouze 14 (13 %) osob označilo možnost, kdy byly o zaslání fotografie požádáni, vyhověli a fotku druhému člověku skutečně zaslali.

Pro vyhodnocení výzkumné otázky č. 4 byla využita i tato otázka. Z celkových 56 žáků, kteří uvedli, že se domnívají o relativní nebezpečnosti internetu, 4 (7 %) odeslali někdy intimní fotky druhému člověku.

Ze 29 žáků, kteří se pak naopak domnívají, že internet je relativně bezpečný pak 4 (14 %) z nich zaslali někdy někomu své intimní fotky.

Graf 17 Zaslání intimních fotek



Zdroj: vlastní zpracování

Otázka č. 20: Co sdílíte na internetu za své osobní informace?

Žáci mohli nezvolit žádnou ale i všechny odpovědi. V případě této otázky bylo zjišťováno co všechno o sobě žáci sdílí na internetu, přihlédneme-li k tomu, že v dnešní době se hojně využívají právě sociální sítě kde sdílíme nejen osobní informace ale i případně svou aktivitu a činnosti v reálném světě.

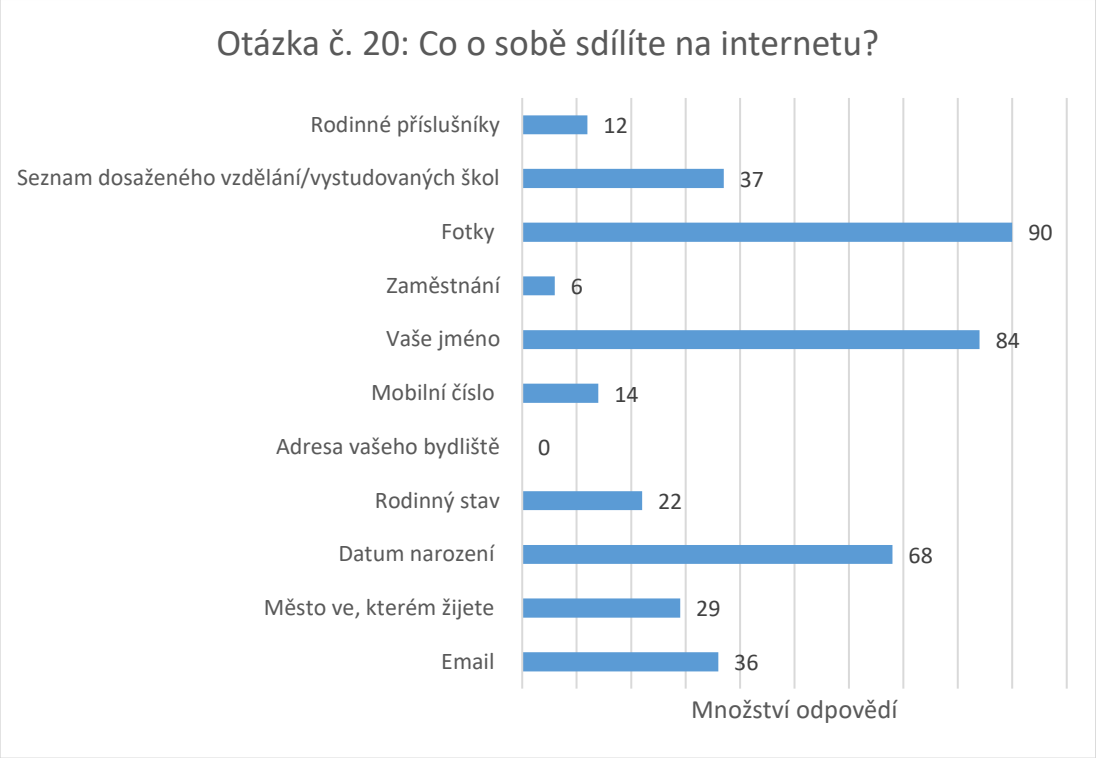
Zjistilo se, že nejčastěji žáci zveřejňují své jméno, datum narození a osobní fotky viz Graf 19.

Pro vyhodnocení výzkumné otázky č. 4 bylo zapotřebí vyhodnotit i 56 a 29 respondentů, přičemž jedni považují internet za relativně bezpečný a druzí nikoliv.

Pro srovnávací část v rámci výzkumné otázky bylo zapotřebí posoudit zda-li o sobě respondenti sdílí tolik informací aby to mohlo být potenciálně rizikové, proto za rizikové chování je považováno pokud o sobě osoba sdílí čtyři a více osobních informací.

Z 56 osob, kteří považují internet za spíše nebezpečné místo jich celkem 28 (50 %) sdílí na internetu čtyři a více osobních informací. Z 29 osob, které jsou opačného názoru pak 14 (48 %) z nich sdílí na internetu čtyři a více osobních informací.

Graf 18 Sdílené informace na internetu



Zdroj: vlastní zpracování

Otázka č. 21: S kolika „přáteli“, které máte přidané na sociálních sítích se znáte osobně?

V tomto případě se zjišťovalo jestli se respondenti skutečně osobně znají se všemi, které mají přidané ve svých „Seznamech přátel“ na sociálních sítích nebo jestli mají v těchto seznamech někoho jen tak volně přidaného aniž by se s ním kdy potkali.

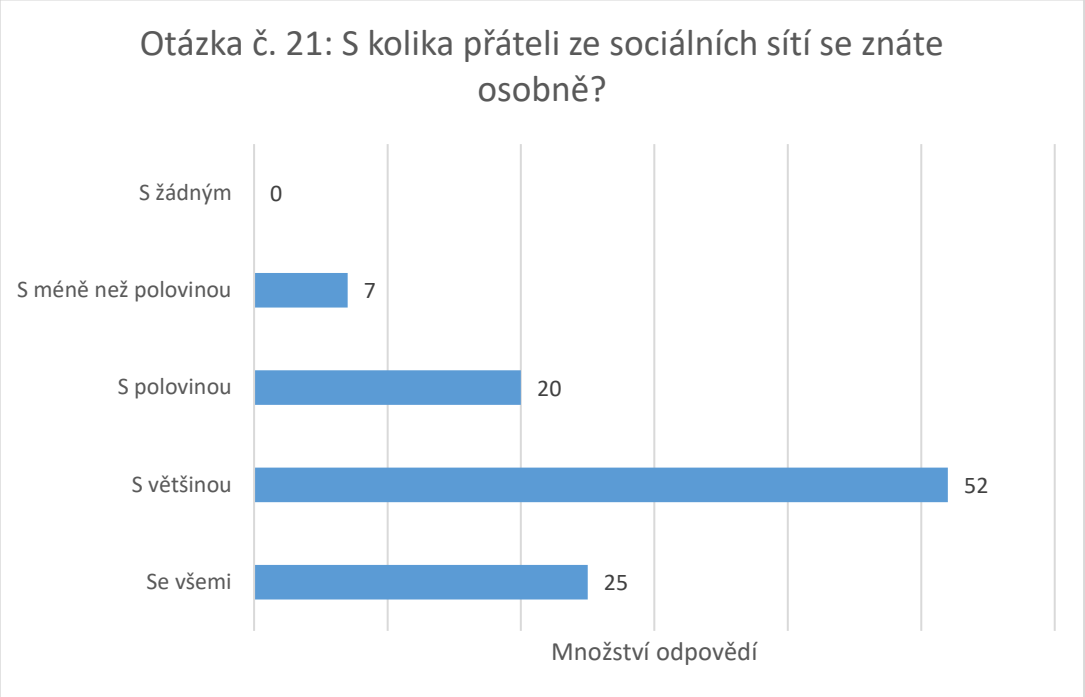
Více jak polovina dotazovaných odpověděla, že se znají buď se všemi 25 (24 %) nebo s většinou 52 (50 %) těchto lidí. Menší množství lidí uvedlo, že se zná s polovinou svých „přátel“ osobně, celkem 20 (19 %) a pouze 7 (7 %) jich uvedlo, že se znají s méně jak s polovinou lidí ze svých seznamů přátel. Nikdo z odpovídajících neoznačil možnost, že se nezná vůbec s nikým koho má ve svém seznamu.

Znalost lidí, které máme přidané na sociálních sítích v osobní rovině je nesmírně důležitá. V tomto případě se pouze menšina žáků vystavuje možnému riziku ze strany cizí osoby, která by mohla po získání dostatečných osobních informací, žáka nějakou formou obtěžovat, vydírat apod.

V rámci této otázky bylo zapotřebí dalšího šetření pro úspěšné vyhodnocení **4.** výzkumné otázky.

Z 56 žáků, kteří hodnotí internet jako spíše nebezpečné místo, se jich 8 (14 %) zná s polovinou či ménším množstvím svých kontaktů ze seznamů přátel osobně. Z 29 žáků, kteří internet hodnotí spíše jako bezpečné prostředí se jich 6 (21 %) zná s polovinou či ménším množstvím svých kontaktů ze seznamů přátel osobně.

Graf 19 S kolika přáteli se znáte osobně



Zdroj: vlastní zpracování

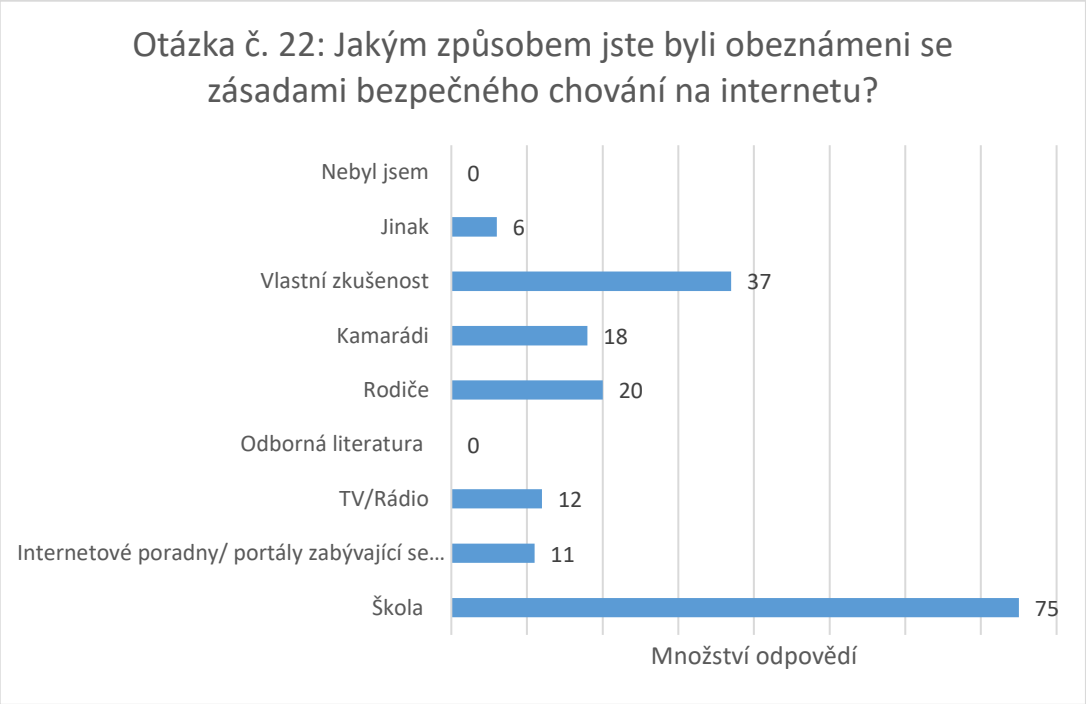
Otázka č. 22: Jakým způsobem jste byli obeznámeni se zásadami bezpečného chování na internetu?

V rámci otázky č. 22 se zjistilo jakým způsobem byli žáci obeznámeni s bezpečným chováním na internetu, stejně jako následující otázky č. **23** a **24,** byla

důležitým zdrojem informací k následné tvorbě návrhu vzdělávacího programu. Žáci mohli (viz Graf 21) zvolit pouze jednu z nabízených možností nebo i více.

Nejvíce jich zvolilo možnost, že byli vzdělávání prostřednictvým školy 75 (72 %) a následně, nejvíce žáků 37 (36 %) tvrdí, že se seznámili se zásadami bezpečného chování na internetu svépomocí, to si lze vysvětlit, že aniž by jim někdo něco v tomto ohledu sděloval, sami od sebe si střeží svou internetovou identitu.

Graf 20 Způsob obeznámenosti s internetem

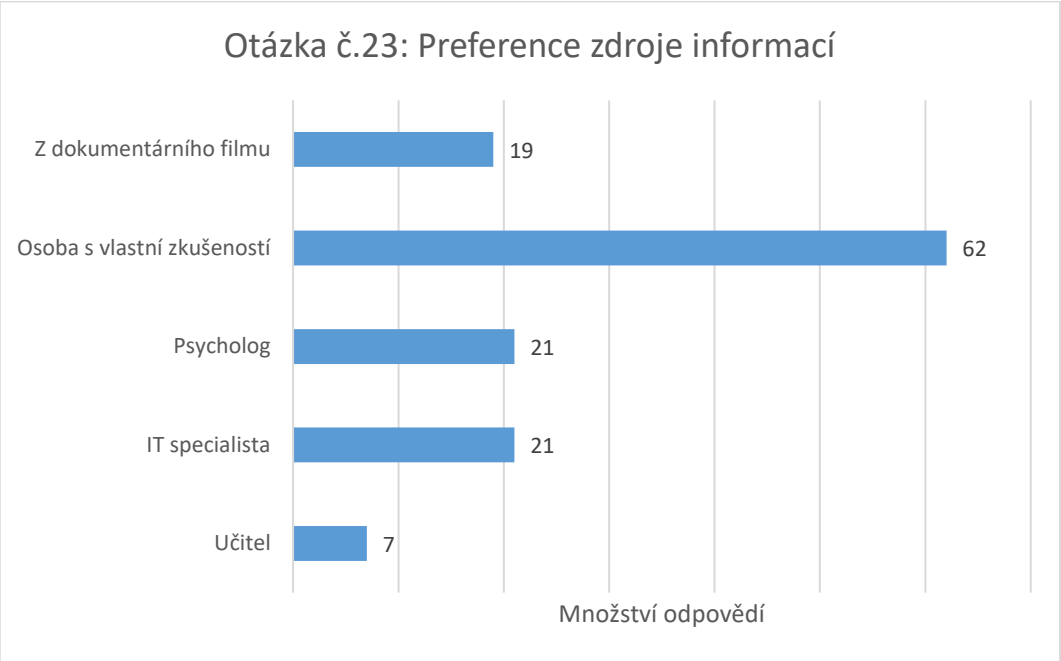


Zdroj: vlastní zpracování

Otázka č. 23: Pakliže byste byl/a účastníkem přednášky či semináře na téma problematiky rizikového chování na internetu, od koho podle vašeho názoru byste získali pro Vás nejpřínosnější informace?

Žáci v případě otázky č. 23 mohli zvolit i více odpovědí. Nejvíce žáků 62 (60 %) uvádělo, že by preferovali aby jim přednášejícího dělal někdo kdo měl s nějakou formou rizikového chování vlastní zkušenost, 21 (20 %) osob by ocenilo jako přednášejícího psychologa nebi IT specialistu. Dalších 19 (18 %) by bylo rádo za nějaký dokumentární film, ze kterého mohou čerpat informace. Nejmenší počet žáků, celkem 7 (7 %) uvedlo, že by preferovali jako přednášejícího učitele.

Graf 21 Preference zdroje informací

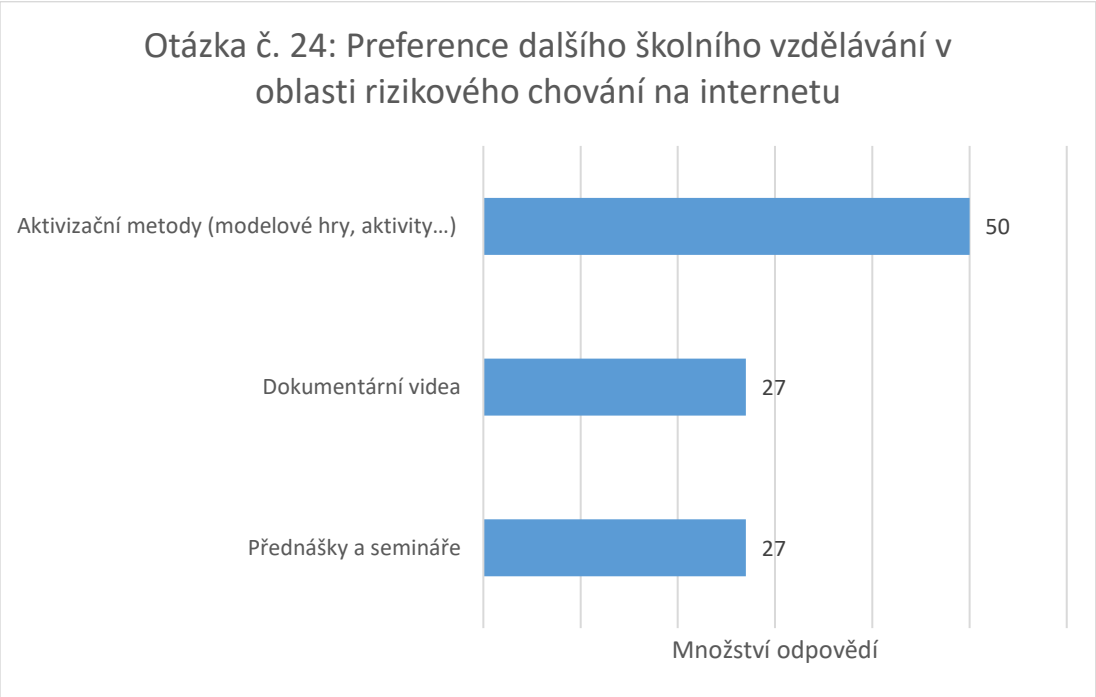


Zdroj: vlastní zpracování

Otázka č. 24: Jaký způsob dalšího vzdělávání ve škole, v oblasti problematiky Rizikového chování na inernetu by Vám nejvíc vyhovoval?

Otázka zjišťovala preferenci dalšího školního vzdělávání v oblasti rizikového chování na internetu. Celkem 50 (48 %) respondentů odpovědělo, že by ocenili různé aktivizační metody na toto téma. 27 (26 %) respondentů pak dále uvedlo, že by naopak preferovali získat informace skrz nějaký vhodný dokumentární snímek a stejné množství 27 (26 %) by ocenilo přednášku či seminář.

Graf 22 Preference dalšího vzdělávání



Zdroj: vlastní zpracování

7.5 Vyhodnocení výzkumných otázek

1) Znají žáci pojmy z rizikového chování a jejich definice?

V případě vyhodnocení této otázky byly brány v potaz výsledky z otázek č. 5,6,7,8 a 9.

V případě samotných otázek, v otázce č. 5 pouze 9 (9 %) žáků odpovědělo správně, v případě otázky č. 6 pak 35 (34 %), v 7. otázce byla úspěšnost nejvyšší a celkem 66 (63 %) odpovědělo správně, v otázce č. 8 pak správně odpovědělo opět pouze 35 (34 %) žáků.

Bylo zjištěno, že ačkoliv se žáci domnívají, že terminologii znají, v mnoha případech přiřazovali špatně pojmy k definicím. Přicházím tedy k domněnce, že si žáci nesprávně vysvětlují některé pojmy, pletou si je a celkově většina z nich nemá dostatek informací, aby správně dokázali tyto pojmy definovat.

2) Jak žáci vnímají kyberšikanu?

Zajímalo mě, jak žáci vnímají kyberšikanu jako takovou, pro vyhodnocení této výzkumné otázky sloužily jako klíčové informační otázky č. 10 a 11. Při průchodu a vyhodnocování samotných dotazníků jsem ale zjistil, že v otázce č. 5, všech 104 žáků uvedlo, že dokážou právě kyberšikanu bez problémů vysvětlit a definovat.

Toto zjištění bylo užitečné při vyhodnocování právě otázky č. 10 kdy měli žáci vybrat jednu nebo více věcí, které spadají pod kyberšikanu a pouze 9 (9 %) žáků vybralo správně všech pět možností.

Nejčastěji podle žáků kyberšikana zahrnuje: šíření soukromých zpráv na veřejnosti, úmyslné slovní napadání, agrese prostřednictvím chatu a získávání osobních informací od člověka a následné vydírání. Naprosté minimum žáků (11 a 12 %) zahrnuli pod kyberšikanu i formy sexuálního obtěžování nebo tzv. Stalking.

Zároveň bylo zjištěno, že celkem 78 (75 %) žáků má nějakou zkušenost s kyberšikanou a 16 (21 %) z oněch 78 (75 %), se stalo obětí kyberšikany.

Opět se tedy dostávám k domněnce, že žáci nemají dostatek informací o kyberšikaně a neví, co všechno zahrnuje.

3) Jak se žáci na internetu chovají?

V rámci této výzkumné otázky mě zajímalo, jak žáci na internetu nejčastěji tráví svůj volný čas, jestli jsou opatrní a hlídají si své osobní informace nebo naopak se chovají rizikově apod. Pro úspěšné vyhodnocení byly využity data z otázek č. 13 – 21.

91 (88 %) žáků označilo, že se na internetu dle svého názoru chová bezpečně.

Drtivá většina žáků tráví na internetu více jak dvě hodiny denně přičemž nejčastěji tuto dobu tráví chatováním s dalšími lidmi nebo třeba užíváním sociálních sítí a sledování online pořadů.

Jakmile se přesuneme k samotným otázkám, jestli se žáci chovají v internetovém prostředí zodpovědně, zjišťujeme, že třeba co se týče ověřování informací, tzn. prevence fake news, je většina žáků 71 (68 %) relativně nedbalá a

informace si ověřují pouze občas nebo ještě méně. V tomto případě se pak chovají rizikově a jsou vystaveni nebezpečí fake news, dezinformací apod.

Při otázce zda-li někdy zaslali žáci někomu svou intimní fotku, vyšlo najevo, že pouze 14 (13 %) z nich někdy někomu podobnou fotku zaslalo.

Při vyhodnocování otázky č. 20 se hledělo na to co o sobě žáci zveřejňují na internetu. V rámci této otázky je třeba přihlédnout i k množství sdílených informací. Jako potenciální riziko bylo považováno, pokud žák sdílí více jak čtyři osobní informace. Těchto žáků bylo 51 (49 %), z toho lze vyvodit, že necelá polovina žáků o sobě sdílí takové množství informací, které může být potenciálně zneužito.

Jako poslední bylo zjišťováno, jestli se žáci znají se všemi lidmi ze seznamů svých přátel na sociálních sítích doopravdy osobně. 77 (74 %) žáků se znají přinejmenším s většinou těchto osob a pouze 27 (26 %) se jich zná pouze s polovinou či méně.

Závěrem k této výzkumné otázce lze říct, že i když se naprostá většina žáků hodnotí jako zodpovědný uživatel internetu, tak se i přesto chovají na internetu alespoň v určitých aspektech rizikově.

4) Jak se na internetu chovají žáci, kteří si myslí, že je internet potenciálně nebezpečné místo a jak žáci, kteří si naopak myslí, že je internet relativně bezpečné místo?

Cílem této otázky bylo zjistit, jestli se žáci, kteří se domnívají, že je internet spíše nebezpečným prostředím chovají přesto rizikově a stejně tak jestli se rizikově chová i druhá skupina, která se naopak domnívá, že je internet spíš bezpečným prostředím. Názor žáků na bezpečnost internetu byl zjištěn z otázky č. 12.

Jako hodnotící kritérium byly použity otázky č. **17, 19, 20** a **21**.

Bylo třeba vzít v potaz jednotlivé otázky, vyhodnotit je a následně vyhodnotit znovu kolikrát se jednotlivci zachovali rizikově. Jako příklad lze uvést, že pokud si žák ověřuje informace pouze příležitostně, zaslal někomu intimní fotku a následně sdílí na sociálních sítích o své osobě čtyři a více informací, pak se chová ve třech případech ze čtyř rizikově.

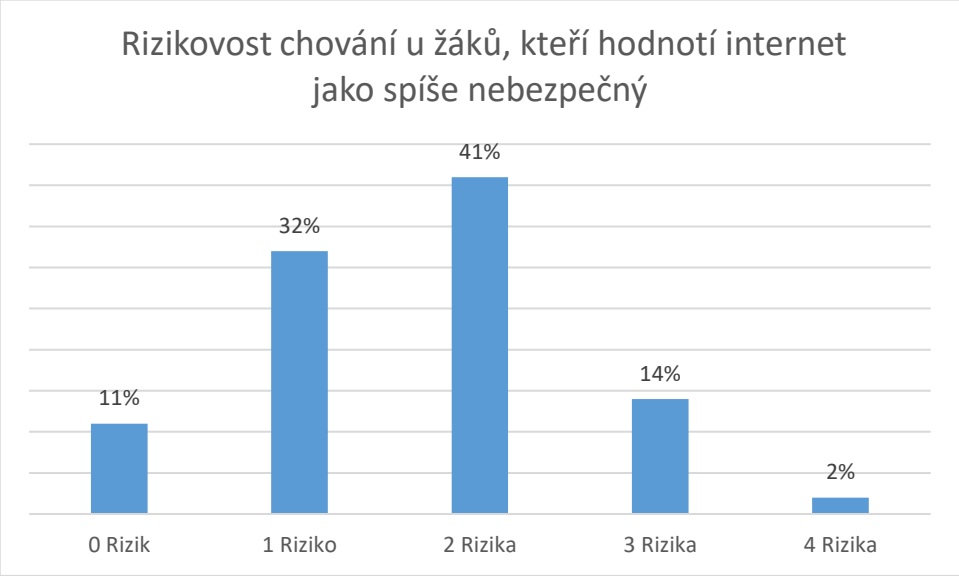
Ze 104 žáků se jich celkem 56 (54 %) domnívalo, že je internet potenciální riziko, 29 (28 %) pak naopak, že je spíše bezpečným místem. Zbývajících 19 (18 %) mělo na tuto věc nevyhraněný názor a nebyli bráni pro vyhodnocování výzkumné otázky v potaz.

Nejprve bude popsána skupina 56 žáků, kteří si myslí, že je internet spíše nebezpečný.

38 (68 %) z nich uvedlo, že si informace ověřují pouze občas či ještě méně, 4 (7 %) někdy někomu poslali svou intimní fotku, 28 (50 %) sdílí na internetu čtyři a více osobních informací a 8 (14 %) žáků se zná s méně než polovinou osob ve svých seznamech přátel na sociálních sítích.

Následně bylo vyhodnoceno, jak často se jednotlivci z této skupiny chovají rizikově. 6 (11 %) osob se nechovalo rizikově ani v jednom případu, v rámci jednoho případu se chovalo rizikově celkem 18 (32 %) osob, v případě dvou případů se rizikově chovalo 23 (41 %) osob a následně ve třech případech se pak 8 (14 %) žáků chová nerozvážně a ve všech čtyřech případech pak pouze jeden žák (2 %).

Graf 23 Rizikovost chování žáků, co hodnotí internet jako nebezpečný



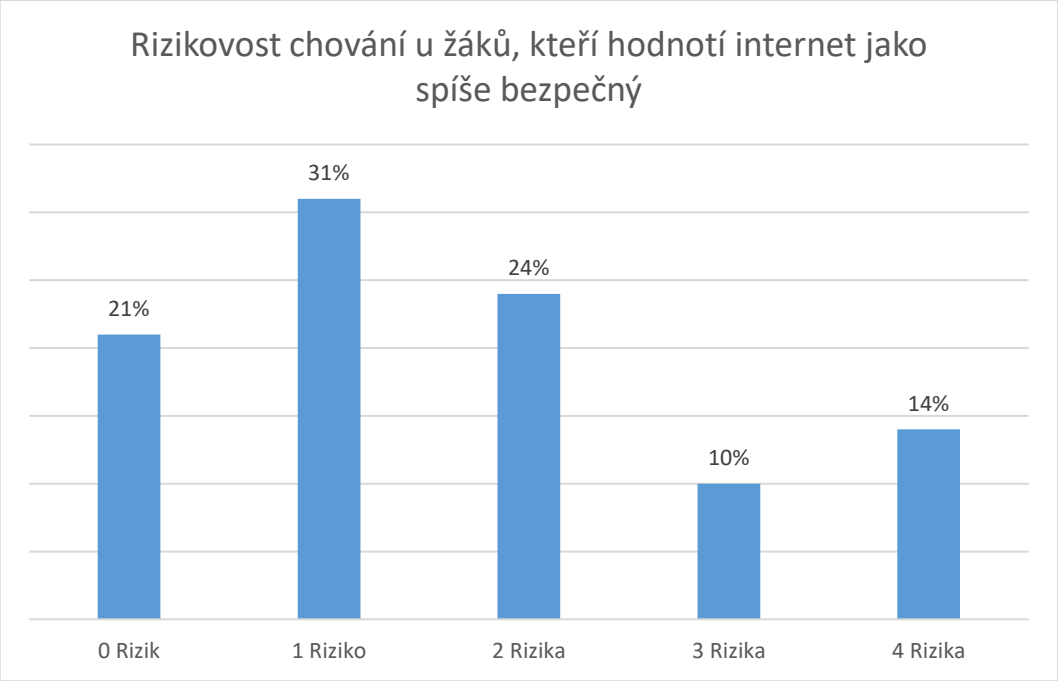
Zdroj: vlastní zpracování

V druhé části bude popsána skupina 29 žáků, kteří si myslí opak a internet je pro ně spíše bezpečný.

Z celkového počtu 29 žáků, kteří hodnotí internet jako bezpečných jich 12 (41 %) uvedlo, že si informace ověřuje pouze občasně nebo ještě méně. 4 (14 %) z 29 žáků někdy někomu poslalo svou intimní fotku, 14 (48 %) sdílí na internetu čtyři a více osobních informací a 6 (21 %) z 29 se zná s polovinou nebo ještě menším množstvím lidí, které mají přidané na sociálních sítích.

Stejně jako u předchozí skupiny i zde bylo vyhodnoceno jak se jednotlivci chovají rizikově. V tomto případě z 29 osob se jich 6 (21 %) nechová rizikově ani v jednom případě, 9 (31 %) pouze v jednom, 7 (24 %) ve dvou případech, 3 (10 %) žáků se chová rizikově ve třech případech a následně 4 (14 %) ve všech čtyřech případech.

Graf 24 Rizikovost chování žáků, co hodnotí internet jako bezpečný



Zdroj: vlastní zpracování

Pokud tedy konečné výsledky obou skupin porovnáme, dostáváme se k zajímavému zjištění.

Původně bylo očekáváno, že žáci, co se na internetu cítí spíše bezpečně, budou více inklinovat k rizikovému chování, protože budou mít pocit, že na internetu jim nic nehrozí, opak byl pravdou. Tito žáci se oproti druhé skupině chovají o mnoho méně rizikově, naopak druhá skupina, kde se očekávalo, že vzhledem k tomu, že internet je pro ně spíš nebezpečné místo, se chová mnohem více rizikově.

8 Návrh vzdělávacího programu

8.1 Představení programu

Z výsledků z dotazníkového šetření a z výzkumných otázek bylo zjištěno, že ačkoliv ne všichni, velké množství žáků má nedostatek informací o rizikovém chování na internetu, problematice sociálních sítí a celkově nemají dostatečné povědomí o zasadách bezpečného užívání internetu. Bylo zjištěno, že relativně velké množství žáků, se zároveň samo chová nějakým způsobem rizikově ať už tím, že o sobě sdílí značné množství soukromých informací, které mohou být dále zneužity, nebo například tím, že informace, které si na internetu přečtou, berou jako fakt, aniž by si tyto informace ověřili ještě z dalšího seriózního zdroje.

V dnešní době, kdy jsou technologie a internet součástí každodenního života, jsem se rozhodl navrhnout program prevence, který bude mít za účel dostatečně informovat žáky o internetových rizicích a měl by jim zároveň sdělit jak se na internetu bezpečně chovat, aby se předešlo věcem jako je třeba zneužití osobních infromací. Velkým bodem programu je zároveň věc kyberšikany. Žáci by měli vědět co všechno kyberšikana zahrnuje a tím pádem, jak jí poznat a jak jí dál řešit.

8.2 Cílová skupina programu

Program je zaměřen na žáky středních odborných škol.

8.3 Cíle programu a profil absolventa

Cílem programu je dostatečně obeznámit středoškolské žáky s problematikou rizikového chování na internetu, internetových rizik a s kyberšikanou a jejich prevencí, aby měli po ukončení programu dostatek informací, aby uměli a zároveň věděli jak internet vůbec používat v rámci záasad bezpečného chování na internetu.

Účastníci jsou na konci vzdělávacího programu:

- schopni jasně definovat co je rizikové chování na internetu, zvládnou uvést i jednotlivé příklady internetových rizik a budou mít povědomí jak těmto rizikům předcházet.
- schopni definovat kyberšikanu a popsat co všechno kyberšikana zahrnuje.

- schopni rozeznat kyberšikanu a budou vědět jak jí dále řešit.
- schopni se v celkové problematice internetových rizik orientovat a aktivně o nich diskutovat.

8.4 Harmonogram programu

Program probíhá v rámci jednoho dne, začíná dopoledne v 8:00 a končí odpoledne v 15:00.

8:00 – 8:30 - Přivítání se s účastníky a jejich následné seznámení s programem.

8:30 – 10:00 – Rizikové chování a rizika internetu, co to je, co zahrnuje, jak mu předcházet. Proč a jak si střežit osobní informace.

9:30 – 9:45 – Pauza v programu.

9:45 – 10:45 – Fake news, dezinformace aneb proč je důležité si informace ověřovat.

10:45 – 11:45 – Kybergrooming a Spam, definice a jak jim předcházet

11:45 – 12:00 - Pauza v programu.

12:00 – 13:30 – Co to je kyberšikana a co všechno zahrnuje.

13:30 – 13:45 – Pauza v programu.

13:45 – 14:00 – Jak se kyberšikana projevuje a jak se jí bránit

14:00 – 15:00 – Prostor pro diskusi a rozdání evaluačních dotazníků

8.5 Rozepsání harmonogramu programu

Díky otázkám č. 22, 23 a 24 se podařilo zjistit jakým způsobem byli dosud žáci v celé věci vzděláváni a jaký způsob dalšího vzdělávání by preferovali. Bylo zjištěno, že žáci většinu informací získávají prostřednictvím školy. Škola by byla i tedy v tomto případě nejvhodnějším prostředníkem kde žákům potřebné informace předat, vzhledem k tomu, že má k dispozici projektory a celkové materiální zajištění pro přednášky, semináře apod.

Na základě výsledků z dotazníků bylo zjištěno, že by většina žáků preferovala hlavně různé aktivizační metody a zbytek žáků by dal přednost spíše seminářům a

dokumentárním snímkům. V případě tvorby tohoto programu je vhodné použít všechny tři varianty.

Celý program by zabral přibližně sedm hodin s přestávkami mezi jednotlivými úseky, program by byl brán jako jakýsi projektový den. Vzhledem k relativní časové náročnosti by pak bylo třeba důkladně probrat organizaci projektu s vedením školy.

V rámci tohoto sedmihodinového úseku by se do hloubky probrala následující jednotlivá témata z oblasti rizikového chování:

- Rizikové chování a rizika na internetu jako celek, co to znamená a co vše pod tyto pojmy spadá a proč je třeba si střežit osobní informace.
- Kyberšikana, co to je, co zahrnuje, jak vypadá samotný průběh a jak se jí bránit.
- Fake news, dezinformace a proč je důležité si infromace ověřovat ze seriozních zdrojů.
- Rizika Spamu při návštěvách nezabezpečených internetových stránek a co je to kybergrooming a jak mu předcházet.

Vzhledem k tomu, že by žáci ve velké většině uvítali jako zdroj informací předání osobní zkušenosti s problematikou od někoho konkrétního, tedy dávají přednost vlastní zkušenosti před uváděním modelových situací a zároveň nepreferují jako přednášejícího vlastního učitele, byl by vhodný aby přednášku řidil externí odborník, který se dané problematice již věnuje. V tomto případě by bylo žádoucí navázat spolupráci a domluvit se s někým z projektu E-bezpečí, který se celou problematikou již několik let úspěšně zabývá a nabízí právě možnosti vzdělávání středoškolských žáků v této problematice.

V první části by se žáci dozvěděli něco o samotném rizikovém chování na internetu, co to vlastně všechno je a jak mu úspěšně předcházet. Dozvěděli by se o problematice fake news a nutnosti ověřování informací vzhledem k tomu, že se v dnešní době ve velkém užívají sociální sítě, kde se právě tyto zprávy šíří. Zjistili by co je to kybergrooming a jak mu předcházet a stejně tak se dozvědí o rizicích spamu a tomu jak se mu co nejlépe bránit. Následně by byla žádoucí jakási modelová hra kdy aniž by přednášející dal žákům předem vědět oč půjde, předvedl jak v praxi vypadá taková internetová komunikace, při které může docházet ke snaze vyloudit z obětí

osobní informace a následně je zneužít. V návaznosti na modelovou hru by bylo podrobně probráno, jak je důležité si osobní informace střežit a bylo by to doplněno tím, jaké jsou možnosti ochrany osobních údajů.

Druhá část programu by se zaměřovala primárně na samotnou kyberšikanu, došlo by k vysvětlení toho co kyberšikana je a co zahrnuje. Žákům by se sdělilo několik případů z praxe a ukázalo by se případným krátkým dokumentárním snímkem či v rámci další modelové hry, jak taková kyberšikana může probíhat. Žáci se dozvědí, jak se kyberšikaně bránit a jak jí dále řešit.

V průběhu celého programu by měli žáci prostor se odborníka na cokoliv zeptat a v samotném závěru se otevře diskuse kolem celé problematiky a žáci budou mít možnost se doptat na všechny další věci, které je zajímají. Po skončení diskuse se žákům rozdají krátké dotazníky díky, kterým získáme nějakou zpětnou vazbu pro případné další zlepšení programu. V dotazníku bude bude trojice následujících otázek:

- **Vyhovoval/a Vám průběh a forma programu?**
  Byla by zde možnost zakroužkovat tyto volby: Ano - Tak napůl - Ne
- **Byl pro Vás program přínosný? Dozvěděli jste se něco nového?**
  Byla by zde možnost zakroužkovat tyto volby: Ano - Tak napůl – Ne
- **Změnili byste na programu něco? Pokud ano, uveďte co.**

Zároveň by součástí programu mělo být i předání informací a kontaktů, externista by sdělil, na koho se v případě dotazů nebo v případě, že sami žáci něco podobného prožívají, obrátit a kam napsat či zavolat. Žáci by tak po absolvování programu měli mít dostatek informací, potřebných k bezpečnému užívání internetu a měli by mít o celé problematice dostatek znalostí, aby byli schopni samostatně diskutovat v rámci tématu a zároveň budou vědět jak případné problematické situace řešit.

9 ZÁVĚR

Bakalářská práce na téma **Rizikové chování na internetu** se zabývala chováním žáků v internetovém prostředí, zjišťovala, jaké vědomosti mají žáci střední školy v oblasti rizikového chování a jaké povědomí mají o problematice kyberšikany. V neposlední řadě se snažila zjistit preference žáků na další vzdělávání v těchto oblastech.

Teoretická část se zabývala samotným pojmem rizikové chování a jeho prevencí, srovnávala tradiční šikanu a kyberšikanu a mimo jiné se zaměřovala i na charakteristiku typického chování adolescenta. Tato část práce se zároveň věnovala rizikovému chování na internetu a jeho prevenci. V největší míře se teorie zaměřovala na samotnou kyberšikanu, její dělení a v neposlední řadě její prevenci.

Praktická část bakalářské práce byla zaměřena na analýzu výsledků, které byly získány prostřednictvím kvantitativního dotazníkového šetření. V úvodu praktické části byly položeny výzkumné otázky, které se zaměřovaly na chování žáků v kyberprostoru, jejich vědomosti v problematice kyberšikany a rizikového chování na internetu. Bylo zjištěno, že velké množství žáků se chová určitým způsobem rizikově a nemají dostatečné povědomí o problematice rizikového chování na internetu a i v oblasti kyberšikany.

Bylo zjištěno, že žáci si často pletou jednotlivé pojmy, nerozumí jim ačkoliv se domnívají, že ano. V rámci praktické části se i vyhodnocovala rizikovost chování na internetu u dvou skupin, přičemž jedna se domnívala, že internet není zcela bezpečné prostředí a skupina druhá měla na internet spíše opačný názor. Zajímavým zjištěním pak bylo, že skupina, která považovala internet jako rizikové prostředí, se sama chovala znatelně více rizikově než druhá skupina. Zajímavé zjištění to bylo z důvodu, že se spíše očekávalo, že druhá skupina, která se na internetu cítí relativně bezpečně bude více náchylná k chybám a k rizikovému chování.

Na základě výsledků zjištěných z dotazníků, byl vypracován návrh vzdělávacího programu, který se zaměřuje především na to, aby dostatečně žáky obeznámil s problematikou rizikového chování a dodal dostatečné množství informací, aby se zabránilo tomu, že se žáci pak můžou zachovat rizikově. Program se

dále soustředil na problematiku kyberšikany a zaměřoval se na to, jak jí poznat, jak se projevuje a jak jí dále lze řešit.

Na závěr bakalářské práce, lze říci, že ačkoliv se internet v dnešní době používá prakticky ke všemu, je zoufale nízká informovanost o internetových rizicích a kyberšikaně mezi dospívajícími žáky kteří bývají těmto jevům vystaveni nejčastěji. Nejlepší prevencí v tomto případě je pak dostatečně žáky informovat už na školách a navázat spolupráci s projekty a odborníky, kteří pomohou se vzděláváním v této oblasti protože ačkoliv si dospívající žáci myslí, že jsou dostatečně obeznámeni s problematikou, není tomu tak a je potřeba právě intenzivnějšího vzdělávání.

SEZNAM POUŽITÝCH ZDROJŮ

MONOTEMATICKÉ PUBLIKACE

1) ALTER, Adam. Neodolatelné. Vzestup návykových technologií a byznys se závislostí ; Překladatel: Julie Tesla - První vydání - Brno : Host, 2018. - 335 s. ISBN 978-80-757-7460-6

2) BENDL, Stanislav, a kol. *Vychovatelství: Učebnice teoretických základů oboru.* 1 vyd. Praha: Grada, 2015, 306s. ISBN 978-80-247-4248-9

3) BLINKA, Lukáš a kol. Online závislosti: jednání jako droga?: online hry, sex a sociální sítě: diagnostika závislosti na internetu: prevence a léčba. Vydání 1. Praha: Grada, 2015. 198 stran. Psyché. ISBN 978-80-210-7975-5.

4) ČERNÁ, Alena., DĚDKOVÁ, Lenka., MACHÁČKOVÁ, Hana., ŠEVČÍKOVÁ, Anna., ŠMAHEL, David., *Kyberšikana: Průvodce novým fenoménem.* 1. Praha: Grada Publishing, 2013, 150 s. ISBN 978-80-247-4577-0

5) DOLEJŠ, Martin a Miroslav OREL. *Rizikové chování u adolescentů a impulzivita jako prediktor tohoto chování*. 1. Olomouc: Univerzita Palackého v Olomouci, 2017, 107 s. ISBN 978-80-244-5252-4.

6) GEISSLEROVÁ, Eli., et al. Mít přehled: „Průvodce informačními a poradenskými službami pro mládež v ČR. 1. Praha: Národní institut dětí a mládeže MŠMT, 2012, 241 s. ISBN 978-80-87449-02-8

7) CHRÁSKA, Miroslav a Kočvarová ILONA. *Kvantitativní metody sběru dat v pedagogických výzkumec*. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta humanitních studií, 2015, 133 s. ISBN 978-80-7454-553-5.

8) JANOŠOVÁ, Pavlína a kol. *Psychologie školní šikany*. 1. Praha: Grada, 2016, 415 s. ISBN 978-80-247-2992-3.

9) KAŠPAROVÁ, Jana a kol. *METODIKA TVORBY ŠKOLNÍCH VZDĚLÁVACÍCH PROGRAMŮ SOŠ a SOU*. 1. Praha: Národní ústav pro vzdělávání, školské poradenské zařízení a zařízení pro další vzdělávání pedagogických pracovníků, 2012, 119 s. ISBN 978-80-87652-05-3.

10) KOHOUT, Roman a Radek KARCHŇÁK. *Bezpečnost v online prostředí*. 1. Karlovy vary: Biblio Karlovy Vary, 2016, 68 s. ISBN 978-80-260-9543-9.

11) KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu*. 1. Praha: Grada Publishing, 2016, 175 s. ISBN 978-80-247-5595-3.

12) MARTÍNEK, Zdeněk. Agresivita a kriminalita školní mládeže. 1. Praha: Grada Publishing, 2012, 152 s. ISBN 978-80-247-2310-5

13) MIOVSKÝ, Michal a kol. *Primární prevence rizikového chování ve školství*. 1. Praha: Sdružení SCAN, 2010, 260 s. ISBN 978-80-87258-47-7.

14) PRICE, Megan a John DALGLEISH. Cyberbullying: Experiences, impacts and coping strategies as described by Australian young people. *Youth Studies Australia*. 2010, , 51-59. ISSN 1038-2569.

15) ŘÍČAN, Pavel. Jak na šikanu. 1. Praha: Grada Publishing, 2010, 160 s. ISBN 978-80-247-2991-6

17) ŠEVČÍKOVÁ, Anna a kol. *Děti a dospívající online: Vybraná rizika používání internetu*. 1. Praha: Grada Publishing, 2014, 183 s. ISBN 978-80-247-5010-1.

18) VEJVODOVÁ, Petra a Miloš GREGOR. *Nejlepší kniha o fake news, dezinformacích a manipulacích!!!*. 1. Brno: CPress, 2018, 142 s. ISBN 978-80-264-1805-4.

19) WILLARD, Nancy E. *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress*. 1. Champaign: Research Press, 2007, 311 s. ISBN 978-0-87822-537-8.

ELEKTRONICKÉ ZDROJE

1) HOLLÁ, Katarína. *KYBERŠIKANA: PREVENCE A INTERVENCE JAKO AKTUÁLNÍ VÝZVA PRO ŠKOLY* [online]. Nitra: Univerzita Konstant'na Filozofa v Nitre, 2012[cit.2021-03-22].Dostupné z: https://www.researchgate.net/profile/KatarinaHolla/publication/279183878_KYBERSIKANA_PREVENCE_A_INTERVENCE_JAKO_AKTUALNI_VYZVA_PRO_SKOLY_CYBERBULLYING_PREVENTION_AND_INTERVENTION_AS_THE_CURRENT_CHALLENGE_FOR_SCHOOLS/links/558d0a9b08ae40781c207407/KYBERSIKANA-PREVENCE-A-

INTERVENCE-JAKO-AKTUALNI-VYZVA-PRO-SKOLY-CYBERBULLYING-PREVENTION-AND-INTERVENTION-AS-THE-CURRENT-CHALLENGE-FOR-SCHOOLS.pdf

2) HORÁK, Vladimír. *Úvod - Co je SPAM a jak se mu bránit* [online]. Praha: Univerzita Karlova,2006 [cit.2021-03-22].Dostupné z: http://uvt1.cuni.cz/email/spam/uvod.html

3) KOPECKÝ, Kamil. *Fake news nejsou žádné "nevhodné názory", ale docela obyčejné lži* [online]. Olomouc: E-bezpečí, 2019 [cit. 2021-03-22]. Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/hoax-fake-news/1612-fake-news-nejsou-zadne-nevhodne-nazory-ale-docela-obycejne-lzi

4) KOPECKÝ, Kamil. Úloha primární prevence aneb Jak informovat o rizikových jevech spojených s internetem. E-Bezpečí, roč. 2, č. 1, s. 27-33. Olomouc: Univerzita Palackého, 2017. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=1235

5) KOPECKÝ, Kamil a René SZOTKOWSKI. *Národní výzkum kyberšikany učitelů 2016 - výzkumná zpráva (základní výsledky)* [online]. Olomouc: Univerzita Palackého v Olomouci, 2016 [cit.2021-03-22]. Dostupné z: https://www.researchgate.net/publication/303987796_Narodni_vyzkum_kybersikany_ucitelu_2016_-_vyzkumna_zprava_kratka_verze

6) Lenhart, A. (2009). Teens and sexting. A Pew Internet & American Life Project Report. Dostupné z: http://ncdsv.org/images/PewInternet_TeensAndSexting_12-2009.pdf

7) *O primární prevenci rizikového chování* [online]. Praha: NUV, 2014 [cit. 2021-03-22]. Dostupné z: http://www.nuv.cz/t/co-je-skolska-primarni-prevence-rizikoveho-chovani

8) *Primární prevence charakteristika* [online]. Praha: NICM [cit. 2021-03-22]. Dostupné z: www.nicm.cz/primarni-prevence-charakteristika

9) VANĚK, L., T. KRÁČMAROVÁ a K. HÁJKOVÁ. *Vakcína proti dezinformacím neexistuje, jaká je tedy jiná prevence?* [online]. Brno:

Fakescape a Medici PRO Očkování, 2021 [cit.2021-03-22].Dostupné z: https://www.fakescape.cz/blog/vakcina-proti-dezinformacim-fake-news

10) *Všeobecná x selektivní x indikovaná školská primární prevence* [online]. Praha: NUV, 2014 [cit. 2021-03-22]. Dostupné z: http://www.nuv.cz/t/co-je-skolska-primarni-prevence-rizikoveho-chovani/vseobecna-x-selektivni-x-indikovana-skolska-primarni-1

11) *Výzkum rizikového chování českých dětí v prostředí internetu 2014* [online]. Olomouc: E-bezpečí, 2014 [cit. 2021-03-29]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/61-vyzkum-rizikoveho-chovani-ceskych-deti-v-prostredi-internetu-2014-prezentace/file

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA č. 1

Dotazník pro žáky

Dotazník se zaměřuje na problematiku rizikového chování na internetu a ukládá si za cíl zjistit jaké povědomí, zkušenosti a znalosti dotázaní v této problematice mají. Dotazník je anonymní a odpovědi z něj budou použity v rámci Bakalářské práce.

1) Pohlaví

a) Muž b) Žena

2) Věk (Doplňte)

3) Ročník, který studujete

a) 1. b) 2. c) 3. d) 4.

4) Studijní obor (Doplňte)

5) Který z těchto pojmů nedokážete definovat. (Možno zvolit i více odpovědí)

a) Kyberšikana b) Kyberstalking c) Sexting e) Flaming f) Spaming g) Fake news

h) Harassment i) Phishing j) Outing k) Kybergrooming

V následujících několika otázkách bude vaším úkolem zvolit správný termín k vypsané definici.

6) „** je chování, kdy si pachatel na internetu vytipovává oběť, snaží se získat její důvěru, vybudovat s ní blízký vztah a vylákat ji k osobní schůzce. Cílem setkání je oběť zneužít.“**

Vyberte správný termín pro tuto definici.

a) Kyberšikana b) Kyberstalking c) Sexting e) Flaming f) Spaming g) Fake news

h) Harassment i) Phishing j) Outing k) Kybergrooming

7) „** je zveřejňování soukromé a osobní komunikace, která proběhla formou textových zpráv nebo třeba emailů.“**

Vyberte správný termín pro tuto definici.

a) Kyberšikana b) Kyberstalking c) Sexting e) Flaming f) Spaming g) Fake news

h) Harassment i) Phishing j) Outing k) Kybergrooming

8) „** je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci.“**

Vyberte správný termín pro tuto definici.

a) Kyberšikana b) Kyberstalking c) Sexting e) Flaming f) Spaming g) Fake news h) Harassment

i) Phishing j) Outing k) Kybergrooming

9) „** je virtuální agresivita, „rozohňování se," vědomě hostilní (nepřátelské) a urážlivé vzkazy na internetu s cílem někoho dehonestovat a rozčílit.“**

Vyberte správný termín pro tuto definici.

a) Kyberšikana b) Kyberstalking c) Sexting e) Flaming f) Spaming g) Fake news

h) Harassment i) Phishing j) Outing k) Kybergrooming

10) Co podle Vás zahrnuje termín Kyberšikana? (Možno zvolit i více odpovědí)

a) Šíření soukromých zpráv na veřejnosti

b) Sledování druhých (stalking)

c) Úmyslné slovní napadání, agrese prostřednictvím chatu

d) Sexuální obtěžování

e) Získávání osobních informací od člověka a následné vydírání

11) Setkali jste se někdy s projevy Kyberšikany?

a) Ano, sám jsem se stal obětí kyberšikany b) Ano, byl jsem svědkem kyberšikany

c) Ne, ale slyšel jsem o ní od ostatních d) Ne, nikdy jsem se s ní nesetkal

12) Ohodnoťte dle Vašeho názoru, jaká je bezpečnost internetového prostředí. (1 nejméně bezpečný, 10 maximálně bezpečný)

1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 – 9 – 10

13) Domníváte se, že se na internetu chováte bezpečně? (1 nechovám se dle zásad bezpečného užívání internetu, 10 naprosto dodržuji zásady bezpečného užívání internetu)

1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 – 9 – 10

14) Kolik času trávíte denně na internetu?

a) 1-2 hodiny b) 2-4 hodiny c) 4-6 hodin d) 6 – 8 hodin e) 8 hodin a více

15) Ve výše uvedené době, co je vaší nejčastější činností?

a) Sociální sítě b) YouTube, sledování pořadů c) Chatování s ostatními d) Hry e) Jiné

16) Jaké sociální sítě používáte? (Možno zvolit i více odpovědí)

a) Facebook b) Twitter c) Instagram d) Snapchat e) Whatsapp f) Tumblr g) Linkedin h) Jiné

17) Ověřujete si informace co si na internetu přečtete i z jiných zdrojů?

a) Vždy b) Většinou c) Občas d) Příležitostně e) Nikdy

18) Jakým způsobem si informace ověřujete? (Možno zvolit i více odpovědí)

a) Prostřednictvím internetových portálů/stránek b) Televize/rádio c) Noviny d) Odborná literatura e) Od dalších lidí

19) Byl/a jste někdy požádán/a o zaslání své intimní fotky?

a) Ano, byl/a jsem požádán/a a vyhověl/a jsem

b) Ano, byl/a jsem požádán/a a nevyhověl/a jsem

c) Ne, nebyl/a jsem o ní nikdy požádán/a

20) Co sdílíte na internetu za své osobní informace? (Možno zvolit i více odpovědí)

a) Email b) Město v, kterém žijete c) Datum narození d) Rodinný stav

e) Adresa vašeho bydliště

f) Mobilní číslo g) Vaše jméno h) Zaměstnání i) Fotky

j) Seznam dosaženého vzdělání / vystudovaných škol k) Rodinné příslušníky

21) S kolika „přáteli“, které máte přidané na sociálních sítích se znáte osobně?

a) Se všemi b) S většinou c) S polovinou d) S méně než polovinou e) S žádným

22) Jakým způsobem jste byli obeznámeni se zásadami bezpečného chování na internetu?

a) Škola b) Internetové poradny / portály zabývající se problematikou

c) TV/Rádio d) Odborná literatura e) Rodiče f) Kamarádi g) Vlastní zkušenost

h) Jinak i) Nebyl jsem

23) Pakliže byste byl/a účastníkem přednášky či semináře na téma problematiky rizikového chování na internetu, od koho podle vašeho názoru byste získali pro Vás nejpřínosnější informace?

a) Učitel b) IT specialista c) Psycholog d) Osoba s vlastní zkušeností

e) Z dokumentárního filmu

24) Jaký způsob dalšího vzdělávání ve škole, v oblasti problematiky Rizikového chování na inernetu by Vám nejvíc vyhovoval?

a) Přednášky a semináře b) Dokumentární videa c) Aktivizační metody (Modelové hry, aktivity…)