Univerzita Hradec Králové
Pedagogická fakulta

DIPLOMOVÁ PRÁCE

2023 **Bc. Marko Čermák**

Univerzita Hradec Králové

Pedagogická fakulta

Katedra aplikované kybernetiky Přírodovědecké fakulty

Rizikové chování studentů středních škol na sociálních sítích

Diplomová práce

Autor:	Bc. Marko Čermák
Studijní program:	N0114A300053 – Učitelství pro střední školy
Studijní obor:	Informatika Základy společenských věd
Vedoucí práce:	RNDr. Petr Coufal, Ph.D.
Oponent práce:	prof. RNDr. Štěpán Hubálovský, Ph.D.

Hradec Králové září 2023

Univerzita Hradec Králové
Pedagogická fakulta

Zadání diplomové práce

Autor:	**Marko Čermák**
Studium:	P20P0455
Studijní program:	N0114A300053 Učitelství pro střední školy
Studijní obor:	Informatika, Základy společenských věd
Název diplomové práce:	**Rizikové chování studentů středních škol na sociálních sítích**
Název diplomové práce AJ:	Risk behavior of high school students on social networks

Cíl, metody, literatura, předpoklady:

Teoretická část diplomové práce se zaměří na seznámení se sociálními sítěmi, jejich riziky a rizikovým chováním studentů. Teoretická část práce bude vycházet z rešerše odborné literatury. Práce bude zaměřena na nejpoužívanější sociální sítě studenty středních škol. Praktická část práce bude spočívat ve vytvoření ucelené sady výukových materiálů pro učitele k využití ve výuce tematického celku ve vybraných předmětech na sš. Empirická část práce bude obsahovat pedagogický výzkum, který bude kvantitativní a realizován formou dotazníkového šetření. Výsledky budou srovnány s podobnými již realizovanými dotazníkovými šetřeními.

KOHOUT, Roman a Radek KARCHŇÁK. Bezpečnost v on-line prostředí. Karlovy Vary: Biblio Karlovy Vary, z.s, 2016, 68 stran : ilustrace (převážně barevné) ; 22 cm. ISBN 978-80-260-9543-9. KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016, 175 stran : ilustrace, portréty ; 24 cm. ISBN 978-80-247-5595-3. PETROWSKI, Thorsten. Bezpečí na internetu pro všechny. Liberec: Dialog, 2014, 242 s. : il. ; 21 cm. ISBN 978-80-7424-066-9. KOPECKÝ, Kamil. UNIVERZITA PALACKÉHO. CENTRUM PREVENCE RIZIKOVÉ VIRTUÁLNÍ KOMUNIKACE. Rizikové formy chování českých a slovenských dětí v prostředí internetu. Olomouc: Univerzita Palackého v Olomouci, 2015, 169 stran : ilustrace (převážně barevné) ; 25 cm. ISBN 978-80-244-4861-9. KRČMÁŘOVÁ, Barbora. Děti a online rizika: sborník studií. Praha: Sdružení Linka bezpečí, 2012, 178 s. ; 21 cm. ISBN 978-80-904920-2-8. PAVLÍČEK, Antonín. VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE. FAKULTA INFORMATIKY A STATISTIKY. Nová média a sociální sítě. Praha: Oeconomica, 2010, 181 s. : il. ; 21 cm. ISBN 978-80-245-1742-1. BLINKA, Lukáš. Online závislosti: jednání jako droga?. Praha: Grada, 2015, 198 stran ; 24 cm. ISBN 978-80-210-7975-5. GREENFIELD, Susan a Radek VANTUCH. Změna myšlení: jak se mění naše mozky pod vlivem digitálních technologií. V Brně: Bizbooks, 2016, 335 stran ; 23 cm. ISBN 978-80-265-0450-4.

Zadávající pracoviště:	Katedra aplikované kybernetiky, Přírodovědecká fakulta
Vedoucí práce:	RNDr. Petr Coufal, Ph.D.
Oponent:	prof. RNDr. Štěpán Hubálovský, Ph.D.

Datum zadání závěrečné práce: 9.4.2019

Prohlášení

Prohlašuji, že jsem diplomovou práci vypracoval samostatně a že jsem v seznamu použité literatury uvedl všechny prameny, z kterých jsem vycházel.

V Hradci Králové dne 22. 11. 2023 Bc. Marko Čermák

Poděkování

Rád bych na tomto místě poděkoval vedoucímu své diplomové práce RNDr. Petru Coufalovi, Ph.D., za odborné vedení, za cenné rady a především za čas, který mi věnoval při řešení dané problematiky. Současně bych chtěl poděkovat všem respondentům, bez nichž by nemohla vzniknout empirická část.
V neposlední řadě bych rád poděkoval své rodině, která mi byla při psaní diplomové práce velkou oporou.

Anotace

ČERMÁK, M. *Rizikové chování studentů středních škol na sociálních sítích.* Hradec Králové, 2023. Diplomová práce na katedře aplikované kybernetiky Přírodovědecké fakulty Univerzity Hradec Králové. Vedoucí diplomové práce RNDr. Petr Coufal, Ph.D. 171 s.

Diplomová práce zkoumá oblast sociálních sítí s důrazem na charakteristiku těchto platforem a souvisejících rizik u studentů středních škol. V rešeršní části se zaměřuje na historii a vlastnosti sociálních sítí a jejich vliv na středoškoláky. Práce se také zabývá shrnutím předchozích výzkumů týkajících se bezpečného internetového chování mladistvých. Praktická část zahrnuje vytvoření výukových materiálů pro pedagogy s cílem integrovat klíčová témata do středoškolských předmětů. Empirický výzkum se opírá o kvantitativní dotazníkové šetření, které zkoumá postoje a chování studentů vůči rizikům sociálních sítí. Získaná data jsou následně porovnávána s dřívějším průzkumem, aby byly odhaleny trendy a změny v rizikovém chování studentů při užívání sociálních sítí.

Klíčová slova

sociální sítě, digitální svět, rizika sociálních sítí, vzdělávání, žáci středních škol, dotazník

Annotation

ČERMÁK, M. *Risk behavior of high school students on social networks.* Hradec Králové, 2023. Diploma Thesis at Faculty of Science University of Hradec Králové. Thesis Supervisor RNDr. Petr Coufal, Ph.D. 171 s.

This thesis explores the field of social networking with an emphasis on the characteristics of these platforms and the associated risks for high school students. The research section focuses on the history and characteristics of social networking sites and their impact on high school students. The thesis also reviews a summary of previous research on safe Internet behavior among adolescents. The practical part involves the development of teaching materials for educators, with the aim of integrating key topics into high school courses. The empirical research is based on a quantitative questionnaire survey that examines students' attitudes and behaviours towards social networking risks. The data collected is then compared with previous research to reveal trends and changes in students' risk-taking behaviour when using social networking sites.

Keywords

social networks, digital world, risks of social media, education, high school students, questionnaire

Obsah

Úvod

V současnosti si málokdo dokáže představit, že by mohl žít bez moderních technologií, jako jsou chytré telefony, počítače a internet. Moderní technologie se začlenily do běžného života zejména díky sociálním sítím, na kterých spolu lidé vzájemně komunikují. Při používání sociálních sítí by si měl každý uživatel být vědom nebezpečí, která mu mohou na těchto platformách hrozit. Zejména středoškoláci, kteří vyrůstali v těsném kontaktu se sociálními sítěmi, by měli být důkladně informováni o hrozbách na internetu. Kvůli tomu se tato diplomová práce zaměřuje především na rizika spojená s používáním sociálních sítí a na to, jak věková kategorie středoškoláků tato rizika vnímá [1].

Tvůrci sociálních sítí vytvořili místo, kde lidé mohou sdílet své myšlenky, pocity, fotografie a videa s ostatními uživateli. Avšak zveřejňování velkého množství osobních informací a možnost neomezené komunikace přináší riziko kyberšikany, kyberstalkingu a kybergroomingu [2, 3].

Tyto jevy byly zmapovány v roce 2020 dokumentárním filmem „*V síti*“, který se dostal do povědomí široké veřejnosti a upozornil na výskyt internetových predátorů [4].

V současnosti se zvyšuje počet zařízení s internetovým připojením, včetně digitálních televizí, herních konzolí, ale i nositelné elektroniky, jako jsou chytré hodinky a náramky. Avšak hlavním faktorem, který pomohl zpřístupnit sociální sítě uživatelům, je především rozvoj chytrých telefonů a dostupnost mobilních dat. Dříve bylo běžné, že se lidé připojovali k internetu pomocí stolních počítačů nebo notebooku, a to pouze z domova nebo z práce. Dnes si téměř každý může nosit internet (sociální sítě) v kapse [1].

Tato diplomová práce se skládá ze tří částí – teoretické, praktické a empirické. V teoretické části jsou definovány základní pojmy týkající se sociálních sítí a jejich rizik. Praktická část obsahuje přípravy na výukové hodiny informačních a komunikačních technologií a společenskovědního vzdělávání zaměřené na bezpečné chování na internetu. Empirická část diplomové práce obsahuje vyhodnocení dotazníkového šetření, jež se zabývá chováním středoškolských studentů na sociálních sítích, časem, který tráví na těchto platformách, a reakcemi mládeže na neznámé profily, sdílený obsah a kyberšikanu. Kombinace teoretických, praktických a empirických složek této diplomové práce přispívá ke komplexnímu pochopení problémů, které představují sociální sítě, a připravuje půdu pro vzdělávací strategie.

Cílem diplomové práce je poskytnout cenné poznatky o rizikovém chování středoškolských studentů na sociálních sítích a nabídnout materiály pro pedagogy, aby mohli v této problematice účinně vzdělávat.

Cíle diplomové práce

- Vytvořit rešerši základních pojmů týkajících se sociálních sítí a jejich rizik.
- Vytvořit přípravu výukových materiálů do hodin informačních a komunikačních technologií a společenskovědního vzdělávání.
- Vytvořit kvantitativní dotazníkové šetření o chování středoškolských studentů na sociálních sítích včetně jeho vyhodnocení a srovnání s obdobným průzkumem.

1 Sociální sítě

Pojem sociální síť pochází ze sociologie a byl poprvé použit sociálním antropologem J. A. Barnesem v roce 1954 v jeho publikaci „Class and Committees in Norwegian Island Parish“. Barnes se zabýval studiem sociálních vztahů mezi norskými rybáři a na základě svého pozorování definoval společnost jako množinu bodů, z nichž jsou některé propojeny vzájemnými vztahy, což nazval sociální sítí [5].

Současná sociologie chápe pojem sociální síť jako soubor sociálních subjektů, které mezi sebou vytvářejí uzly vzájemných vztahů. Toto sociologické vymezení sociální sítě se svojí podstatou příliš neliší od internetové sociální sítě, kterou známe dnes. Jak sociologické, tak internetové pojetí se zaměřuje na mezilidské vztahy, především pak jejich propojování a vytváření [5].

Dnes se pojmem sociální síť označuje internetová služba, která umožňuje vytvoření veřejných, soukromých a firemních profilů. Uživatelé se mohou jejich prostřednictvím propojovat s ostatními a sdílet různý obsah, jako jsou fotografie, videa anebo texty. Sociální sítě také umožňují sdílení obsahu mezi uživateli různých fór a skupin, což usnadňuje koordinaci událostí a společných projektů. Tyto sítě se používají hlavně k rychlé komunikaci na velké vzdálenosti [2, 3, 5].

1.1 Historie internetových sociálních sítí

V roce 1978 vznikl systém BBS (Bulletin Board System), který jako první umožňoval posílat textové zprávy. Psaní přes tento systém bylo velmi pomalé, protože v systému mohl být přihlášen vždy jen jeden uživatel. V roce 1988 finský student Jarkko Oikarinen tento problém vyřešil pomocí prvního IRC (Internet Relay Chat), který se jmenoval OuluBox. Tato aplikace poprvé umožnila uživatelům komunikovat mezi sebou v reálném čase, což dalo základ pro současné chatovací aplikace [5, 6].

V roce 1997 vznikla sociální síť SixDegrees.com, která jako první umožňovala uživateli vytvářet si seznamy přátel a přidávat si do nich ostatní účty z této platformy. Uživatelé si tak mohli prohlížet profily ostatních a chatovat s nimi. Na platformě SixDegrees.com bylo registrováno přes milion účtů. Provoz této sociální sítě byl v roce 2001 ukončen kvůli finančním problémům. Zakladatel projektu Andrew Weinreich tvrdí, že „SixDegrees předběhla svou dobu“ [5, 6].

V roce 2003 vznikla sociální síť Myspace, která byla vytvořena za pouhých 10 dní. Tento projekt se stal první veřejně známou sociální sítí a poskytl uživateli možnosti vytvářet si profil a propojovat ho s přáteli. V roce 2006 měl Myspace přes 100 milionů registrovaných uživatelů [6].

V roce 2004 založil Mark Zuckerberg společnost Facebook, která se později stala největší sociální sítí na světě s více než dvěma miliardami aktivních uživatelů. Zuckerberg investoval svůj finanční zisk do koupě konkurenčních sociálních sítí, například Instagram pořídil za 1 miliardu dolarů v roce 2012 a WhatsApp za 16 miliard dolarů v roce 2014 [6, 7, 8].

V roce 2014 byla založena sociální síť Musical.ly, která byla o čtyři roky později koupena čínskou společností ByteDance. Tato firma následně spojila Musical.ly se svou aplikací Douyin a vytvořila tak sociální síť TikTok, která se stala konkurenceschopnou sociálním sítím Marka Zuckerberga [9].

1.2 Vlastnosti sociálních sítí

Sociální sítě jsou charakterizovány interaktivitou, což znamená, že uživatelé mohou aktivně vytvářet a sdílet obsah, zapojit se do komunikace a reagovat na podněty ostatních. Interaktivita umožňuje uživatelům vytřídit si obsah podle svých představ, což zvyšuje atraktivitu sociální sítě a čas, který na ní uživatelé tráví [1, 5].

Pro sociální sítě je také běžná velká svoboda projevu, což znamená, že uživatelé mohou veřejně vyjadřovat své názory. Svoboda projevu ale může být zneužita k šíření falešných zpráv a to může vést k vyvolávání zmatku ve společnosti [2, 10].

Navzdory rozmachu dezinformačních praktik se sociální sítě snaží zajistit transparentnost. Umožňují uživatelům snadno nalézt relevantní a aktuální informace týkající se jak místních událostí, tak i globálních témat. Dostupnost sociálních sítí a jejich obsahu je také zásadní pro udržení aktuálnosti, protože uživatelé mohou opakovaně procházet obsah vytvořený jinými uživateli z různých částí světa [5].

Další výhodou většiny sociálních sítí je, že poskytují své služby zdarma nebo za velmi nízký poplatek. Uživatelé proto mohou používat sociální sítě bez vysokých finančních nákladů. Měli by si však být vědomi toho, že výměnou za bezplatné služby poskytují platformám o sobě informace, jež využívají sociální sítě při zobrazování reklamy, která jim generuje zisk [11].

Negativní vlastností sociálních sítí je, že mohou u některých uživatelů vyvolat pocit nedostatečnosti. Ten zpravidla vychází z toho, že lidé na sociálních sítích sdílí přikrášlené zážitky ze svého života a fotografie upravené pomocí některého ze softwaru. Upravené příspěvky jsou následně prezentovány jako obraz reality a to může především u mladistvých vzbudit pocit méněcennosti nebo jiné psychické problémy [12].

Další nevýhodou používání sociálních sítí je ztráta vlastního soukromí, ke které dochází při nadměrném sdílení osobních informací. Takto veřejně sdílené informace pak mohou být zneužity proti jejich autorovi formou kyberšikany, kybergroomingu, kyberstalkingu a jiných kybernetických útoků [1, 3].

1.3 Vliv sociálních sítí na dospívání mládeže

Mládež se občas v dospívání potýká s pocitem osamělosti a hledá své místo ve společnosti. Proto využívá různé způsoby, jak být v kontaktu se svými vrstevníky. Mezi ně může patřit například i používání sociálních sítí. Dospívající si vytváří sociální vztahy podle své vlastní volby, na rozdíl od rodinných vztahů, které nemohou ovlivnit. Současně si během tohoto období vytváří i sociální vztahy, které jsou nejvíce ovlivněny sociokulturním prostředím. Mladistvý během dospívání nechce být kontrolovaný a chce se osamostatnit. To je jedním z důvodů, proč používá sociální sítě, na kterých není pod kontrolou rodičů nebo jiných rodinných příslušníků. Pocitově mu komunikace na sociálních sítích poskytuje více soukromí než komunikace v domácím prostředí. Používání těchto internetových nástrojů nahrazuje setkávání se, například na sportovištích nebo na diskotékách. Ačkoliv se tyto prostory na první pohled zdají být odlišné, plní ve vývoji mladistvého stejnou úlohu, a to poskytovat otevřený a zvenčí nekontrolovaný způsob komunikace, během které může uživatel sdílet své pocity, problémy, starosti, ale také radosti se svými vrstevníky [10, 13, 14].

Zdravý vývoj jedince zahrnuje rozvíjení a upevňování vlastní osobnosti. Mladý člověk získává zpětnou vazbu o tom, „kým je“, především od lidí ze svého okolí, s nimiž komunikuje a konfrontuje své názory. Zpětná vazba od vrstevníků na sociálních sítích pomáhá dospívajícímu formovat jeho názor o sobě samém a o svém „já“. Jedinec si na sociálních sítích svobodně volí, které informace o sobě bude sdílet, to mu umožňuje učit se, jak zacházet se svojí individuální svobodou a jak přijímat odpovědnost [10, 13, 14].

Mladý člověk chce v dospívání cítit, že je okolím vnímán. Tato potřeba se na sociálních sítích může projevovat například tak, že dospívající zvýší četnost sdílení svých příspěvků se záměrem na sebe upozornit. Když jsou jeho aktivita nebo názor oceněny kladnou reakcí ostatních uživatelů, cítí se šťastný. Problém je v tom, že o pozornost na sociálních sítích bojuje většina jejich uživatelů. To může vést k tomu, že se jedinec stane více kontroverzním, aby na sebe upoutal zájem ostatních. Hodnota pozornosti na sociálních sítích je subjektivní a někteří uživatelé ji nepovažují za důležitou, takže o ni nebojují. To, jak moc je pro jedince důležitá zpětná vazba na sociálních sítích, závisí na osobnosti člověka. Silné osobnosti zpětnou vazbu na sociálních sítích nepotřebují, zatímco u lidí s nízkou sebeúctou může nedostatečná pozornost vést k soutěžení a porovnávání se s ostatními [10, 12, 14].

Současní dospívající se k sociálním sítím staví více otevřeně než dospělí. Mladí lidé jsou zvyklí používat tyto platformy pro komunikaci s okolím a pro propagaci sebe samých, zatímco dospělí k nim přistupují s větším skepticismem. Rozdíl mezi nimi na sociálních sítích spočívá v tom, že mladí lidé vyrůstali spolu s vývojem těchto platforem, zatímco většina dospělých se teprve učí tyto platformy používat, včetně většiny funkcí, které sítě nabízejí [10].

1.4 Příklady sociálních sítí

Sociální sítě jsou internetové platformy, které umožňují uživatelům vytvářet a sdílet obsah s ostatními uživateli. Mezi nejznámější patří Facebook, Instagram, Twitter nebo TikTok. Tyto sítě slouží k propojování lidí s podobnými zájmy, umožňují komunikaci mezi uživateli, sdílení fotografií, videí a dalšího obsahu [12].

1.4.1 Facebook

Facebook je sociální síť patřící společnosti Meta Platforms. Tuto platformu vytvořil v roce 2004 student Harvardu Mark Zuckerberg. Původně se Facebook nazýval TheFacebook.com. Pojmenování TheFacebook bylo inspirováno stejnojmenným letákem, který se rozdával studentům Harvardu v prvním ročníku. Tento leták, stejně tak jako Facebook, vznikl za účelem rychlejšího a snadnějšího seznámení studentů mezi sebou. Marku Zuckerbergovi s vytvářením Facebooku pomáhali jeho spolubydlící – Andrew McCollum, Dustin Moskovitz, Chris Hughes a Eduard Saverin [3, 5, 6].

Původně měl Facebook sloužit výhradně studentům Harvardu, aby na něm mohli sdílet informace a vzájemně komunikovat. V dnešní době se stal celosvětovým fenoménem a používají ho více než dvě miliardy uživatelů [6].

Obrázek 1 Logo sociální sítě Facebook [15].

Facebook během svého vývoje okopíroval některé koncepty konkurenčních platforem. Aktuální verze Facebooku nabízí uživatelům, oproti starším verzím této sociální sítě, větší spektrum aplikací, které zvětšily paletu uživatelských možností. Kromě psaní a sdílení příspěvků může současný uživatel na této platformě například prodávat zboží, streamovat videa nebo navazovat nové kontakty pomocí seznamovací funkce „seznamka“ [15].

Nedílnou součástí dnešního Facebooku je Messenger. Messenger je chatovací aplikace, přes kterou spolu mohou uživatelé Facebooku vzájemně komunikovat. Funkce chatování byla původně dostupná pouze v prostředí aplikace Facebooku, nicméně později byla vytvořena tato samostatná aplikace, která v současné době nabízí rozšiřující funkce k běžnému chatování. Těmi jsou skupinové chaty, telefonáty a videohovory i možnost sdílet fotografie a videa [16].

V roce 2019 byl natočen film „*The Social Network*“, který se zaměřil na příběh vzniku Facebooku a na řešení mnoha problémů, s nimiž se tato sociální síť na začátku musela potýkat. Film se soustředí na konflikty s bratry Winklevossovými, kteří obvinili Marka Zuckerberga z krádeže svého nápadu na webovou stránku HarvardConnection, již měl Zuckerberg použít jako inspiraci pro vytvoření Facebooku [17].

1.4.2 Instagram

Instagram vznikl v roce 2010 a původně sloužil ke sdílení fotografií mezi uživateli. V dnešní době se používá jako nástroj k chatování a zároveň se zde může uživatel setkat s různými typy krátkých videí – stories, reels... Instagram se od tehdejších gigantů na poli sociálních sítí jako Twitter, Facebook lišil tím, že umožňoval sdílet pouze fotografie s krátkým textem. Tento text zpravidla obsahoval hashtag (#), pomocí kterého mohli jiní uživatelé danou fotografii vyhledat. Používání hashtagů na Instagramu vydrželo až do současnosti. Instagram, stejně jako Facebook, aktuálně patří společnosti Meta Platforms Marka Zuckerberga, který Instagram v roce 2012 odkoupil za jednu miliardu dolarů [3, 7].

Obrázek 2 Logo sociální sítě Instagram [18]

Instagram se inspiroval sociální sítí Snapchat a umožnil svým uživatelům sdílet i tzv. instastories (sdílení příběhů). Stories je příspěvek (fotografie či krátké video) o maximální délce 60 sekund, který je ostatním uživatelům zpřístupněn pouze na dobu 24 hodin a pak zmizí [18, 19].

Další funkce, kterou by mohl Instagram do své aplikace implementovat, je placené členství, díky kterému by měli populární tvůrci možnost sdílet prémiový obsah se svými fanoušky. Ti si budou muset zaplatit členství, aby se jim prémiový obsah zpřístupnil. Podobnou funkci v současnosti nabízí weby Patreon nebo Onlyfans. Na těchto a jim podobných platformách sdílí tvůrci svůj prémiový obsah pro fanoušky, kteří jsou za něj ochotni zaplatit. Implementování této funkce na Instagramu by mohlo vypadat tak, že profily budou mít možnost tvorby speciálního obsahu pro své sledovatele, tento obsah by byl přístupný jen těm sledujícím, kteří zaplatili předplatné, ostatním by se nezobrazoval [20].

1.4.3 TikTok

Tato sociální síť vznikla v roce 2014 pod názvem Musical.ly a v roce 2018 ji koupila společnost ByteDance, která vlastnila obdobnou aplikaci Douyin. Po nákupu sociální sítě Musical.ly došlo k sjednocení těchto dvou aplikací a k vytvoření jednotné s názvem TikTok. Změna vlastníka a názvu však zásadně neovlivnila uživatelsky snadné rozhraní ani obsah, který se na této sociální síti vyskytuje [9].

Obrázek 3 Logo sociální sítě TikTok [21]

Sociální síť TikTok nabízí uživateli obsah ve formě krátkých videí, která trvají maximálně 3 minuty, proto by se mohlo zdát, že zde uživatel nestráví příliš mnoho času, ale opak je často pravdou. Hlavním důvodem je kvalitní algoritmus, jenž je navržen tak, aby uživateli nabízel pro něj zajímavé příspěvky, které si získají jeho pozornost [21].

Aplikace TikTok byla v roce 2019 jednou z nejstahovanějších sociálních sítí mezi teenagery a v současnosti je k dispozici ve 150 zemích a v 75 jazycích, včetně češtiny. TikTok má i své webové rozhraní, většina uživatelů však používá k návštěvě této sociální sítě výhradně mobilní aplikaci [21, 22].

1.4.4 BeReal

BeReal je sociální síť, kterou založili francouzští podnikatelé Alexis Barreyat a Kévin Perrea v prosinci roku 2019. Tato síť se od ostatních liší tím, že je zaměřená na pravdivost a autenticitu. Její tvůrci si kladou za cíl umožnit uživatelům sdílet opravdové momenty ze svého života, bez toho, aby se snažili vypadat lépe nebo dokonale. V tomto ohledu je BeReal odlišný od jiných sociálních sítí, kde se uživatelé často snaží ukazovat ve vysněném světle [23].

Obrázek 4 Logo sociální sítě BeReal [24]

BeReal pošle uživateli náhodně během dne notifikaci s výzvou, aby pořídil fotografie z přední a zadní kamery. Ty jsou pak sdíleny na zdi příspěvků pro přátele a mohou být také zveřejněny pro všechny uživatele na síti. Veřejné příspěvky se zobrazují v záložce „global“. Aplikace vyžaduje, aby uživatel reagoval na notifikaci do 2 minut. Pokud tak neučiní, může stále vytvořit příspěvek. Avšak ostatní uživatelé uvidí, že byl vytvořen později [24].

1.4.5 Twitter

Twitter byl založen v roce 2006 a odlišuje se od ostatních sociálních sítí tím, že podporuje pouze krátké a úderné příspěvky známé jako tweety. Tyto tweety jsou v současnosti omezené na 280 znaků a mohou obsahovat text, obrázky, GIFy, videa a odkazy na další obsah. Díky tomu se Twitter stal velmi populárním způsobem sdílení novinek, myšlenek a názorů a stal se také důležitým nástrojem pro společenskou komunikaci a politickou diskusi. Současný Twitter má přes 400 milionů uživatelů. První tweet zveřejnil jeho zakladatel Jack Dorsey dne 21. března 2006 a zněl: „just setting up my twttr“. Tuto větu lze přeložit jako „právě si nastavuji svůj Twitter“ [5, 25].

Obrázek 5 Logo sociální sítě Twitter [25]

V roce 2021 koupil Twitter americký miliardář Elon Musk. Podle zpráv z médií byla pořizovací cena Twitteru odhadována na 44 miliard dolarů. Tato koupě se stala jednou z největších akvizic v historii Twitteru a přinesla značnou pozornost médií a veřejnosti [26].

Během psaní diplomové práce (dne 24. 7. 2023) došlo k přejmenování platformy. V rámci tohoto procesu změnila platforma své jméno na „X“. Přesto však diplomová práce nadále používá původní označení Twitter [27].

1.4.6 LinkedIn

Sociální síť LinkedIn se odlišuje od ostatních sociálních sítí tím, že umožňuje propojování uživatelů na základě jejich povolání. Tato platforma byla vytvořena za účelem sdílení profesního života, zprostředkování komunikace mezi uživateli konkrétní profese a sdílení jejich nápadů. Toho často využívají personalisté a headhunteři, kteří zde hledají pracovníka na konkrétní pracovní pozici. LinkedIn používá 500 milionů uživatelů z celého světa [5, 28].

Obrázek 6 Logo sociální sítě LinkedIn [28]

1.4.7 Snapchat

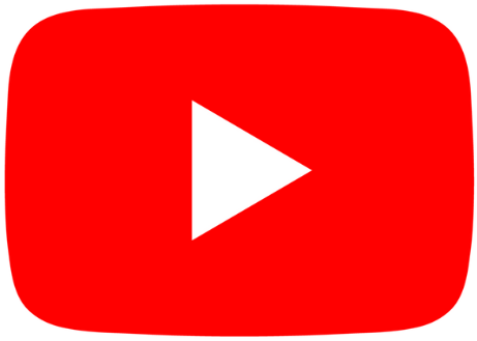
Sociální síť Snapchat vznikla v roce 2011 a původně se jmenovala Picaboo. Podstata Snapchatu je v tzv. „snapech“, což jsou fotografie nebo krátká videa, které může uživatel posílat komukoliv ze svého seznamu přátel – jednotlivci, skupině, všem. „Snap“ se jim zobrazí na krátkou dobu (10 sekund). Poté, co si adresát příspěvek zobrazí, už ho znovu neotevře. Kromě posílání a přijímání „snapů“ nabízí tato sociální síť také řadu dalších funkcí, například možnost chatovat s přáteli, používat filtry k vylepšení fotografií a videí, „discover“ k procházení obsahu ostatních uživatelů. Další funkcí je „memories“, ta umožňuje uživatelům ukládat si své „snapy“ a vytvářet sbírky oblíbeného obsahu [3, 19].

Obrázek 7 Logo sociální sítě Snapchat [19]

Od roku 2021 má aplikace více než 360 milionů aktivních uživatelů a je oblíbená zejména mezi mladšími uživateli [29].

1.4.8 YouTube

Sociální síť YouTube vytvořili Chad Hurley, Steve Chen a Jawed Karim v roce 2005. Měla původně sloužit jako platforma, na které by uživatelé sdíleli krátká videa pro své přátele a rodinu, avšak v současné době se jedná o sociální síť, na níž různí tvůrci tvoří obsah pro své fanoušky. Historicky prvním přidaným příspěvkem je video přímo od jednoho ze zakladatelů s názvem „Me at the ZOO“. Má pouze 18 vteřin a bylo nahráno 23. dubna 2005. Od té doby ho vidělo více než 225 milionů lidí. V roce 2006 společnost Google odkoupila platformu YouTube za 1,65 miliardy dolarů. V současnosti ji používá přes 2 miliardy uživatelů z více než 90 zemí a každou minutu nahrají uživatelé nová videa v rozsahu 500 hodin [5, 30].



Obrázek 8 Logo sociální sítě YouTube [30]

1.4.9 WhatsApp

Sociální síť WhatsApp založili v roce 2009 bývalí zaměstnanci společnosti Yahoo Brian Acton a Jan Koum. Název WhatsApp pochází z anglického výrazu „what´s up“ – co se děje. Je to jazyková hříčka se slovy „up“ a „app“ (tj. zkratka pro slovo application – aplikace), která se vyslovují podobně. Tato sociální síť umožňuje zdarma posílat textové zprávy, fotografie, videa a další multimediální obsah pomocí mobilního rozhraní. V roce 2014 koupila WhatsApp společnost Facebook za 12 miliard dolarů a v roce 2016 dosáhla tato sociální síť jedné miliardy uživatelů. Aplikace WhatsApp se stala oblíbenou platformou pro zasílání zpráv díky své jednoduchosti a bezpečnosti [8, 31].

Obrázek 9 Logo sociální sítě WhatsApp [31]

2 Charakteristika rizik na sociálních sítích

Tato kapitola se zabývá nejčastějšími riziky, která hrozí uživatelům sociálních sítí, především dětem a mladistvým. Je však důležité si uvědomit, že zmíněná rizika se netýkají pouze dětí a teenagerů. Všichni uživatelé sociálních sítí by měli být obezřetní ohledně informací, které o sobě na těchto platformách sdílejí. Zveřejněné příspěvky na sociálních sítích si může kdokoliv archivovat a tento obsah následně zneužít. Zejména děti a mladiství by měli být informováni o tom, jak se správně chovat na sociálních sítích, protože za internetovými profily se může skrývat kdokoliv – ať už kamarád, nebo hacker či predátor, který může mít nekalé úmysly. Mezi základní rizika, kterým se lidé na sociálních sítích vystavují, patří například ztráta anonymity a soukromí, kyberšikana, kybergrooming, kyberstalking, sexting, fake news, phishing a vishing [3, 12].

2.1 Závislost na sociálních sítích

V široké veřejnosti se často probírá problematika závislosti dospívajících na sociálních sítích. Někteří jedinci na nich tráví téměř veškerý svůj volný čas, to může mít negativní vliv na jejich psychický vývoj a může to zapříčinit i asociální chování, zhoršení studijních výsledků nebo citové ochladnutí [1, 12, 13].

K závislosti může přispět i způsob, jakým vývojáři danou síť vytvořili. Uživateli se s pomocí algoritmu zobrazuje cílený obsah snažící se ho zaujmout, dále zde má mnoho pozitivních stimulů, které ho motivují trávit na síti svůj čas. Jedním ze způsobů, kterými vývojáři manipulují s lidmi na sociálních sítích, je zpřístupnění pouze tlačítka „to se mi líbí“ pro rychlou pozitivní zpětnou vazbu na síti, přitom tlačítko „to se mi nelíbí“ chybí. Lidé se díky tomu setkávají s větším množstvím pozitivních reakcí u svých příspěvků, jejich počet je však ovlivněn dostupností a časovou nenáročností tvorby této pozitivní zpětné vazby. Naopak autorovi negativní zpětné vazby nezbývá nic jiného než svůj názor napsat do komentářů. Proto někteří uživatelé posílají pouze kladná hodnocení příspěvkům, které se jim líbí, a na ostatní nereagují [15, 18, 21].

Závislost současných teenagerů na sociálních sítích, tedy čas, který jim věnují, můžeme porovnávat s tím, jak mladí lidé trávili čas dříve – tj. například při sledování televize nebo při venkovních aktivitách. Hlavními důvody, proč dospívající používají sociální sítě, jsou sociální vazby s ostatními uživateli (kamarády), zábava a chatování. Díky tomu, že mládež na sociálních sítích tráví čas především vzájemnou komunikací, mohlo by se jejich samotné používání považovat za společenské. Pokud se na závislost na sociálních sítích budeme dívat touto perspektivou, dalo by se o ní hovořit jako o závislosti na kamarádech [1, 13].

2.2 Ztráta anonymity a soukromí

Riziko ztráty a zneužití osobních údajů na internetu se zvyšuje při častém používání sociálních sítí. Všichni lidé by si měli důkladně promyslet, které informace o sobě na internetu sdělují. Člověk se vystavuje velkému riziku, pokud má svůj profil (například na Instagramu nebo TikToku) v režimu „veřejný“. V ten moment je jeho soukromí nechráněné a všichni ostatní uživatelé mají přístup k obsahu profilu (fotografie, videa…) a k osobním údajům, které jsou na tomto profilu zveřejněny. Problematika soukromí však plně nezávisí na uživateli. V některých případech sociální sítě vyžadují při registraci osobní údaje. Z toho vyplývá, že pokud chce uživatel danou sít používat, nevyhne se sdílení těchto dat [1, 18, 21].

Problematika ztráty anonymity a soukromí je velmi častým fenoménem, který se týká dětí a mládeže. Ukazatelem zmíněného rizika může být slabé zabezpečení sociálních sítí a profilů mladistvých. Sdílení citlivých údajů může vést k jejich odcizení a následnému zneužití. Osobní údaje nemusejí být vždy zneužity za účelem finančního zisku. Velmi často jsou totiž tato rizika spojena s kyberšikanou, pokusy o fyzický kontakt, krádeží identit a dalšími [12].

2.3 Kyberšikana

Za kyberšikanu se považuje opakované a systematické napadání jedince nebo skupiny pomocí moderních technologií, například prostřednictvím sociálních sítí, internetu, počítače, fotografií nebo chytrého telefonu. Na rozdíl od klasické šikany u kyberšikany oběť nemusí znát totožnost útočníka, což vede k jeho problematickému vypátrání. Dále je kyberšikana nebezpečnější v tom, že útočník může oběť napadnout na dálku, nečekaně, za pomoci svého mobilního telefonu. To představuje problém kvůli nemožnosti útěku před útoky [2, 3, 12, 32].

Během kyberšikany sice nehrozí fyzické napadení, ale oběť je vystavena jiné formě útoku. Jedná se především o vyhrožování, zveřejňování fotografií, nahrávek anebo videí, zastrašování, vydírání, krádež identity, napodobování účtu oběti a další [3, 12, 32].

Oběti kyberšikany se doporučuje, aby si útočníka na daných sociálních sítích zablokovala a jeho profil nahlásila. Tím ale nezamezí tomu, aby si agresor založil nový účet a v kyberšikaně pokračoval. Než si oběť útočníka zablokuje, měla by udělat archivaci důkazního materiálu, do kterého spadá veškerá komunikace s agresorem. Kyberšikana neprobíhá pouze pomocí sociálních sítí, ale i pomocí e-mailu nebo SMS zpráv [3, 12, 32].

2.4 Kybergrooming

Grooming v širším slova smyslu označuje více druhů manipulativního chování. Při kybergroomingu se útočník za pomoci moderních technologií snaží získat důvěru své oběti a následně se s ní setkat v reálném světě [2, 3, 10, 32].

Útočník vzbuzuje důvěru u své oběti na základě svého profilu a během chatování využívá volně dostupné informace, které jeho cíl o sobě na internetu sdílí, tím se snaží navodit pocit, že se zajímá o stejná témata. Kybergroomer si většinou vytvoří více falešných účtů, které zvyšují důvěryhodnost hlavního falešného profilu, například sdílením skupinových fotografií, vzájemným označováním a komentováním příspěvků nebo pouze věrohodným počtem přátel. Díky tomu působí falešný profil uvěřitelněji [2, 3, 10, 32].

Při chatování se snaží predátor vzbudit ve své oběti dojem, že mu na ní záleží. Toto chování zpravidla doprovází nabídky různých odměn. Nejtypičtějšími jsou například finanční dary nebo pomoc s domácím úkolem, koupě počítačové hry a další. Odměny vedou k získání větší důvěry, oběť má pocit, že na ní groomerovi opravdu záleží. Často se mu začne svěřovat se svými problémy a trápeními. Tím se jejich vztah výrazně upevní. Predátor důvěry následně zneužije k osobnímu setkání nebo k získání specifického obsahu, jako jsou například osobní údaje nebo intimní fotografie. Na základě těchto informací je oběť dále vydírána [3, 10, 32].

Standardním cílem kybergroomera je dostat svoji oběť, nejčastěji dítě, na osobní schůzku, která většinou probíhá na odlehlých místech. Zde má dítě malou šanci, že se dovolá pomoci. Toho chce útočník zneužít a v takovéto situaci svou oběť fyzicky napadnout nebo sexuálně zneužít. Oběť tuto skutečnost ve většině případů zatají a nechá si ji pro sebe kvůli studu. Nejčastěji se jedná o děti ve věku 11-17 let, dívky i chlapci jsou zneužíváni v podobném počtu případů. Ochranou před těmito incidenty může být zajištění dostatečné prevence a vytvoření důvěry mezi dětmi, rodiči a učiteli [2, 3, 10, 32].

Pokud je kybergroomer pečlivý, je jeho odhalení velmi náročné. Uživatel internetu by v případě podezření, že je v kontaktu s falešným profilem, měl zkontrolovat datum založení jeho účtu, datum nahrání profilových fotografií, původ profilové fotografie, dále zda okruh jeho přátel na sociálních sítích netvoří podezřele identická skupina lidí (například pouze dívky okolo šestnácti let). Pokud má uživatel sociální sítě stále pochybnosti, může poprosit možného útočníka o fotografii jeho tváře spolu s něčím netypickým, například s papírem s datem a nápisem „TATO DYPLOMOVÁ PRÁCE SI ZASOUŽÍ ÁČKO“. Gramatická chyba v textu je úmyslně proto, aby uživatel omezil riziko, že kybergroomer podobnou fotku najde na internetu. Dalším způsobem ověření toho, že si uživatel píše s „pravým profilem“, může být videochat. Avšak pozor, jak specifickou fotografii (se vzkazem), tak videochat lze s pomocí moderních technologií upravit, aby vypadaly věrohodně [3, 32, 33].

2.5 Kyberstalking

Kyberstalking je forma obtěžování na internetu, která zahrnuje opakované snahy navázat nežádoucí komunikaci s obětí za účelem upoutání její pozornosti. Tento typ obtěžování má různé podoby, například nevyžádané zprávy, sledování online aktivity nebo vyhrožování. Je spojován s kyberšikanou a může mít pro oběť vážné následky. Kromě emocionálního utrpení může kyberstalking vést i k fyzickým újmám, zejména pokud se stalker přesune do offline světa. Je klíčové, aby lidé byli o rizicích kyberstalkingu informováni a přijímali preventivní opatření k ochraně sebe samých. Patří sem obezřetnost při sdílení osobních informací online a používání nastavení ochrany soukromí k ovládání toho, kdo vidí jejich informace [3, 10, 12].

Existuje mnoho různých metod, které kyberstalker může k obtěžování své oběti použít. Patří mezi ně zasílání výhružných nebo obtěžujících zpráv, online šíření pomluv nebo nepravdivých informací o objektu svého zájmu, dále zveřejňování trapných nebo osobních informací, pokusy o kontaktování prostřednictvím více online účtů nebo platforem. Někteří kybernetičtí pronásledovatelé mohou také používat sledovací software či jiné nástroje ke sledování online aktivit oběti nebo se mohou pokoušet získat přístup k jejím osobním účtům a zařízením bez jejího svolení. V některých případech může kyberstalker své chování vystupňovat a přidat i offline výhrůžky nebo zastrašování, například zanecháváním zastrašujících vzkazů či telefonátů [3, 10, 12].

Oběti kyberstalkingu mohou bojovat s řadou negativních důsledků, včetně strachu, úzkosti, deprese a potíží se spánkem. Mohou také pociťovat ztrátu kontroly nad svým online prostředím a nedostatek soukromí. Je proto důležité, aby podnikly kroky na svou ochranu a vyhledaly pomoc. To může zahrnovat zablokování účtů stalkera, změnu jejich online návyků a vyhledání podpory u přátel, rodiny nebo odborníka na duševní zdraví. V závažných případech je nutné zapojit orgány činné v trestním řízení [3, 10, 12].

2.6 Sexting

Sexting je forma rizikového jednání, při kterém dochází k posílání intimního obsahu pomocí fotografií, videí, audionahrávek nebo psaného textu. Je to specifický druh chování, který sdílejí především teenageři. V romantickém vztahu dvou lidí může být posílání erotického obsahu považováno za formu experimentu, zpestření všedního dne a u některých párů i za normální věc [2, 3, 12, 32, 34].

Pokud člověk posílá erotický obsah bez nátlaku a z vlastní vůle, je toto chování označováno jako dobrovolný sexting. Dospívající během dobrovolného sextingu uspokojují svou sexuální zvědavost nebo ho využívají k přilákání objektu svého zájmu, protože chtějí získat pozornost. Opakem dobrovolného sextingu je sexting nedobrovolný, který probíhá pod nátlakem – tj. při obtěžování, psychickém nebo fyzickém vyhrožování. [2, 3, 32, 34].

Sexting se dělí na dva základní typy: self-sexting a peer-sexting. Během self-sextingu uživatel distribuuje sexuální obsah, kde je vyobrazen on sám. Fotografie, které sdílí, jsou jeho a sám si je dobrovolně nafotil. Oproti tomu při peer-sextingu uživatel sdílí erotický materiál, ve kterém se on sám nevyskytuje, např. fotografie, videa a erotické GIFy, které mohou pocházet z internetu [34].

Sexting s sebou nese riziko toho, že se erotický materiál dostane k uživatelům, pro které nebyl určen. Útočník, jenž má k erotickému dokumentu přístup, může následně osobu na něm zachycenou vydírat za účelem zisku finančních prostředků, dalšího erotického obsahu nebo osobního setkání [2, 3, 32, 34].

2.7 Phishing

Phishing je typ kybernetického útoku, při kterém se útočník vydává za důvěryhodnou osobu, aby od oběti získal citlivé informace, například údaje o kreditní kartě nebo internetovém bankovnictví. Toho se často dosahuje pomocí podvodných e-mailů, které se tváří jako poslané z legitimního zdroje, ale ve skutečnosti obsahují odkazy na falešné webové stránky [2, 3, 35].

Ty jsou identifikovatelné pomocí drobných odchylek v názvu domény. Například pravá webová doména společnosti Alza.cz má adresu: https://www.alza.cz. Podvodníci však chtěli v listopadu 2022 zneužít nepozornosti lidí a vytvořili falešný web https://alza-cz.pro, díky kterému zjistili čísla platebních karet obětí a následně jim odcizili z účtů finanční prostředky [36].

Jednu z forem phishingového útoku zažil i známý youtuber Adam Jícha, který e-mailem obdržel nabídku spolupráce. Útočník po něm chtěl, aby vytvořil reklamu na softwarový produkt, jenž byl ke stažení na falešné webové adrese. Když si Adam Jícha nainstaloval nebezpečný software z falešné stránky, byly mu odcizeny všechny přihlašovací údaje a soubory, které měl uložené ve svém počítači, včetně fotografie občanského průkazu. Pro ochranu před těmito útoky je důležité být obezřetný při otevírání e-mailů nebo klikání na odkazy z neznámých zdrojů a ověřovat pravost webových stránek před tím, než jsou zadány citlivé údaje [37].

2.8 Vishing

Výraz vishing vznikl kombinací anglického slova „voice“ (hlas) a výrazu phishing, což je specifický kybernetický útok (viz 2.7). Vishing je metoda, při které se útočník snaží z oběti vylákat citlivé informace, nejčastěji k platební kartě nebo internetovému bankovnictví. Na rozdíl od phishingu, při kterém útok zpravidla probíhá pomocí e-mailové zprávy, během vishingu útočník s obětí telefonuje. Má předem připravený „callscript“ (průběh hovoru) tak, aby z oběti vylákal veškeré důležité informace. Doporučením, jak se proti vishingu bránit, je během podezřelých nebo naléhavých telefonátů z banky zavěsit a vzápětí kontaktovat banku prostřednictvím jejího oficiálního čísla nebo kontaktovat svého osobního bankéře. Útočníci totiž mohou používat software, který telefon zmate, a v příchozích kontaktech se zobrazí číslo nebo název banky [3, 38].

3 Pravidla bezpečného chování na sociálních sítích

Internet se stal nedílnou součástí našeho každodenního života a nabízí nekonečné možnosti komunikace, vzdělávání a zábavy. Představuje však také řadu rizik, včetně kyberšikany, krádeží identit nebo sdílení nevhodného obsahu. Aby se jim uživatelé vyhnuli a mohli co nejlépe využívat výhod online světa, je zapotřebí dodržovat zásady bezpečného chování. Tato kapitola poskytne přehled zásad bezpečného chování na internetu. Jejich dodržováním mohou jednotlivci chránit sebe i ostatní před riziky a plně využívat možnosti, které internet nabízí [1, 3, 12].

3.1 Zabezpečení počítače a mobilu

V moderní době je zabezpečení počítačů a mobilních zařízení naprosto klíčové. Mezi základní zásady, které mohou přispět ke zvýšení bezpečnosti zařízení a online účtů, patří nastavení silného hesla, které by mělo být dlouhé, jedinečné a složité, neobsahující žádné osobní údaje. Doporučená je také kombinace velkých a malých písmen, znaků a číslic. Také je nevhodné používat stejné heslo na více účtech, protože to zvyšuje riziko, že pokud dojde k napadení jednoho z účtů, mohou útočníci získat přístup k ostatním účtům pomocí stejného hesla [2, 12, 35].

K zesílení ochrany se používá dvoufaktorové ověřování (2FA). Tento typ zabezpečení poskytuje dostatečnou ochranu tím, že vyžaduje, aby uživatelé při přihlašování k účtu zadali nejen heslo, ale také kód, který je zaslán prostřednictvím SMS zprávy, aplikace nebo e-mailu. Dochází tak k zabránění neoprávněnému přístupu i přes odhalení hesla [12].

Dále je pro správné zabezpečení zařízení nutné hlídat aktualizace operačního systému a aplikací. Aktualizace opravuje chyby a slabá místa, která by mohla být zneužita útočníky k proniknutí do systému a odcizení citlivých dat. Bez pravidelných aktualizací jsou zařízení zranitelná a mohou být snadným cílem útočníků, kteří využívají bezpečnostních chyb ve starších verzích softwaru [39].

Mezi další způsoby, jak zabezpečit počítač či mobil, patří antivirový software, který chrání před malwarem a viry. Dokáže totiž odhalit a odstranit hrozby dříve, než stihne dojít k poškození zařízení či odcizení osobních údajů. [2, 35].

3.2 Uživatelská obezřetnost

Některým rizikům může uživatel předcházet svojí obezřetností například tak, že si bude kontrolovat, na které odkazy kliká. Při prozkoumávání neznámých odkazů se často stává, že uživatel najde podvodnou stránku, jejímž cílem je odcizit citlivé informace nebo stáhnout uživateli do počítače malware (nebezpečný software). Proto je důležité před kliknutím na odkaz ověřit jeho pravost a dávat pozor při obdržení takových odkazů od neznámých zdrojů [3, 35, 36].

3.3 Kontrola sdíleného obsahu

Na sociálních sítích mají lidé příležitost zveřejňovat téměř jakýkoliv obsah. Každý by si ale měl dávat pozor na to, jestli jím zveřejněný příspěvek neobsahuje informace, které by ho mohly poškodit [2, 32, 35].

Mezi ty, jež by se neměly sdílet na sociálních sítích, patří nejen intimní fotografie, ale i osobní údaje – jméno, příjmení, adresa, e-mail, telefonní číslo, adresa školy, přístupové údaje k internetovému bankovnictví, hesla aj. Jako pomůcka pro určení bezpečnostního rizika při sdílení příspěvku může posloužit například otázka: „Chtěl bych nosit tričko, na kterém by byl vytištěn daný příspěvek, a co by si o takovém tričku myslelo moje okolí, přátelé a rodiče?“ Tato pomůcka může být aplikována na všechny příspěvky, především na takzvané „stories“ – dočasné příspěvky, které po uplynutí určité doby zmizí. Uživatelé mylně nabývají dojmu, že je tato forma příspěvku bezpečná, protože je časově omezená. Avšak kdokoliv a kdykoliv (po dobu zveřejnění) si může udělat jeho kopii, např. kopii obrazovky, záznam obrazovky. Těmito způsoby se z dočasného příspěvku může velice jednoduše stát trvalý. Nebezpečí pořízení screenshotu nebo záznamu obrazovky nehrozí pouze u sdílení příspěvku, ale i během samotné komunikace mezi uživateli [1, 12].

Při sdílení by měl uživatel vzít na vědomí, že nese odpovědnost za jeho obsah. Je dobré se řídit pravidlem, že pokud si není uživatel jistý, má-li nějaký příspěvek zveřejňovat, je lepší ho nesdílet [1, 12].

3.4 Nastavení soukromí na sociálních sítích

Správné nastavení účtu na sociálních sítích je dobrou prevencí, jak předcházet možným rizikům. Toto nastavení ovlivňuje viditelnost údajů a příspěvků uživatele na konkrétní platformě. Uživatel má zpravidla na výběr mezi veřejným a soukromým profilem. Veřejný profil se vyznačuje tím, že mu mohou ostatní uživatelé psát zprávy nebo komentovat příspěvky, které jsou rovněž veřejné (přístupné všem). Oproti tomu soukromý, neveřejný profil je uzamčený a jeho majitel dostává notifikace o tom, že ho jiný uživatel chce sledovat. Majitel se pak může rozhodnout, jestli danému uživateli profil zpřístupní, nebo ne. Teprve po zpřístupnění se uživateli zobrazí příspěvky soukromého profilu a má možnost komentovat příspěvky a psát soukromě zprávy [12, 18, 35].

Další způsob nastavení soukromí je založen na principech blacklistu a whitelistu. Blacklistovým způsobem zablokuje uživatel konkrétní účet útočníka, tomu se následně nezobrazí uživatelův účet, takže ztratí přístup k příspěvkům a možnosti korespondence s uživatelem. Tento způsob blokace může agresor na sociálních sítích obejít založením nového profilu. Whitelistový způsob je bezpečnější a od blacklistového se liší tím, že si uživatel vybírá konkrétní účty, kterým zpřístupní příspěvky a možnost psaní zpráv [40].

3.5 Nepsat si s cizími lidmi

Na sociálních sítích je běžné, že spolu konverzují lidé, kteří se vzájemně neznají. Z bezpečnostního hlediska je však lepší komunikaci s neznámým účtem na internetu vůbec nenavazovat a daný účet si zablokovat. Toto opatření je důležité proto, aby se uživatelé chránili před možným nebezpečím, které může nastat při navázání kontaktu s neznámými lidmi. Je třeba si uvědomit, že i když se tyto osoby mohou zdát příjemné a neškodné, mohou mít skryté úmysly, jako je například získání osobních údajů nebo jiných citlivých informací. Je proto důležité, aby uživatelé byli opatrní a chránili si svá data. Mezi osobní údaje patří například adresa nebo telefonní číslo. K jejich ochraně slouží používání bezpečnostních opatření, jako jsou například silná hesla a aktivní ochrana soukromí na sociálních sítích, jež zamezí pokusům o komunikaci neznámých účtů. Pokud se mladistvý uživatel rozhodne komunikovat s cizími lidmi na internetu, je důležité, aby k takové konverzaci přistupoval s rozvahou a zodpovědností. Měl by zvážit, zda je opravdu nutné sdílet osobní informace s neznámými uživateli, a pokud ano, měl by je sdílet jen v omezené míře. V takovém případě by na to měl upozornit dospělou osobu, aby eliminoval případná rizika [1, 10, 32].

3.6 Říct si o pomoc

Pro správnou ochranu před kybernetickými útoky je důležité, aby se lidé nebáli říci si o pomoc. Mladistvý se může obrátit na rodiče nebo jinou dospělou osobu, které důvěřuje, když má podezření, že se stal obětí kybernetického útoku. Stejně tak může dospívající hledat podporu u svých kamarádů, kteří by mohli mít podobné zkušenosti, a při řešení této situace následovat jejich ověřené bezpečnostní postupy. Učitelé jsou také cennými zdroji informací a pomoci. Mladiství je mohou informovat o tom, co se stalo, a společně s nimi hledat řešení. Učitelé také mohou iniciovat případná opatření na škole, aby zvýšili prevenci kybernetických útoků a povědomí o nich [3, 32].

3.7 Vzdělávat se

Vzdělávání o kybernetických útocích je klíčové pro prevenci a ochranu před neustále se vyvíjejícími riziky digitálního světa. Informovaný uživatel je schopný rozpoznat podezřelé aktivity a vyvodit opatření pro svou bezpečnost. Díky tomu zásadně sníží pravděpodobnost úspěšnosti útoku a ochrání svoje osobní údaje a digitální identitu. Uživatel, který se seznámí s moderními postupy kybernetické bezpečnosti, by si měl také osvojit správné návyky pro bezpečné používání sociálních sítí, které mu pomohou chránit se před potenciálními útoky. Mezi tyto návyky patří používání silných a jedinečných hesel, povědomí o phishingových útocích, znalost moderních způsobů zabezpečení zařízení a pravidelná aktualizace softwaru. Vzdělání umožňuje zlepšit odolnost vůči kybernetickým hrozbám a zabezpečit digitální prostředí uživatele [2, 32, 39].

4 Výzkumy zaměřené na online rizika u mladistvých

Tato kapitola diplomové práce se zaměřuje na výsledky výzkumů, které se zabývaly chováním českých dětí na internetu. Jsou zde prezentovány výsledky různých studií, jež se v České republice věnovaly tématům, jakými jsou využívání sociálních sítí, přístup k nevhodnému obsahu na internetu a kyberšikana. Tyto studie poskytují informace o tom, jak děti využívají internet a jakým způsobem se na něm mohou setkat s různými nebezpečími [34, 41, 42, 43, 44].

4.1 EU KIDS ONLINE IV (2017-2018)

Výzkum EU KIDS ONLINE IV se zabýval online aktivitami dětí a dospívajících na internetu a riziky, která jim hrozí. Sběr dat probíhal pomocí dotazníkového šetření v období od října 2017 do února 2018 na 89 základních a středních školách. Celkem se ho zúčastnilo 2 825 respondentů ve věku 9-17 let (z toho 51 % chlapců a 49 % dívek), kteří buď pravidelně, nebo příležitostně používají internet. Věkové rozložení účastníků bylo následující: 25 % dětí ve věku 9-10 let, 24 % ve věku 11-12 let, 21 % ve věku 13-14 let a 30 % ve věku 15-17 let [41].

Získávání dat, jak je již uvedeno výše, probíhalo během vyučování pomocí online dotazníku. Před každým dotazováním byly vyžadovány písemné souhlasy zákonných zástupců a celý projekt byl schválen etickou komisí pro výzkum Masarykovy univerzity. Dotazníky byly anonymní, aby byla zajištěna ochrana soukromí účastníků [41].

4.1.1 Výsledky výzkumu

V první části výzkumu byly položeny otázky ohledně četnosti, s jakou děti a dospívající ve věku 9-17 let používají internet nebo jsou online, a ohledně zařízení používaného pro připojení. Bylo zjištěno, že 84 % z nich se připojuje k internetu pomocí mobilního zařízení a 45 % pomocí notebooku nebo stolního počítače. Denně se na internet připojuje pomocí mobilního zařízení 85 % dívek a 82 % chlapců. To je více než přes notebook nebo počítač, přes který se připojuje 32 % dívek a 57 % chlapců. U nejmladších účastníků výzkumu ve věku 9-10 let bylo pozorováno mírně nižší používání internetu, přičemž 13 % z nich se na mobilním zařízení téměř nikdy nepřipojuje a 5 % vůbec nikdy [41].

Další otázky výzkumu se zaměřily na rozdíly v čase stráveném na internetu dětmi a dospívajícími během školních dnů a víkendů. Během školních dnů se 35 % z nich připojuje k internetu na 4 a více hodin denně, zatímco 9 % na 7 a více hodin. Během víkendů se na internet připojuje 51 % z nich na 4 a více hodin denně a 22 % respondentů uvádí, že se na internet připojuje na 7 a více hodin. V této oblasti si chlapci i dívky udržují podobné množství času stráveného na internetu [41].

Dále byly zkoumány aktivity, kterým se děti a dospívající ve věku 9-17 let věnují při používání internetu na mobilních zařízeních nebo počítačích. Největší podíl z nich (75 %) denně tráví čas sledováním online videí, dále komunikací s rodinou nebo kamarády (73 %), poslechem hudby (72 %), používáním sociálních sítí 70 %) a využíváním internetu pro školní práci (65 %). Zajímavostí je, že zkoumaný vzorek respondentů téměř vůbec, nebo dokonce nikdy nehledal zprávy na internetu [41].

Pokud jde o počítačovou gramotnost, téměř všichni účastníci výzkumu (91 %) umí odstranit uživatele ze svého seznamu kontaktů, 88 % z nich ví, které informace by neměli sdílet na internetu, a 83 % umí uložit fotografii nebo obrázek z internetu. Zajímavým zjištěním je, že 75 % dětí a dospívajících umí upravit nastavení soukromí, 66 % z nich umí vybrat vhodná klíčová slova pro vyhledávání na internetu a 53 % umí ověřit pravdivost informací z internetu (přičemž chlapci mají ve zvládání ověřování pravdivosti internetu mírnou převahu o 14 % nad dívkami) [41].

Další část výzkumu zjišťovala, jestli se dotazovaní v posledním roce setkali na internetu s něčím, co je obtěžovalo, nebo je nějakým způsobem rozrušilo. Celkem 36 % respondentů odpovědělo, že ano. Dívky uváděly vyšší procento obtěžování (40 %) než chlapci (31 %) a mezi dospívajícími ve věku 15–17 let odpověděla pozitivně polovina dotázaných. Denně se s nevhodným obsahem na internetu setkávají 2 % dotázaných [41].

Výzkum se dále zabýval tím, komu se respondenti svěřují, když se setkají se závadným obsahem na internetu. Nejčastěji o tomto problému hovoří se svými vrstevníky (57 %), rodiči (28 %) a sourozenci (13 %). Značné procento (25 %) nesdílí své negativní zkušenosti z internetu s nikým a pouze 1 % vyhledá odbornou pomoc. Nejběžnějšími způsoby, jak dotázaní řeší závadný obsah na internetu, jsou zavření okna prohlížeče nebo blokování útočníka (obojí 35 %) [41].

Výzkum také odhalil, že v roce 2018 bylo obětí agrese na internetu až 25 % dětí a dospívajících. Z toho 19 % útoků bylo osobní povahy a 15 % se uskutečnilo prostřednictvím internetu nebo mobilních telefonů. 11 % respondentů se dopustilo útoků tváří v tvář a 8 % útočilo online. Chlapci ve věku 13–17 let byli nejčastějšími agresory (26 %), zatímco dívky uvádějí, že na internetu útočí spíše vzácněji (11 %) [41].

Formy online agrese, kterým byli respondenti vystaveni, zahrnovaly nehezké a nepříjemné zprávy (82 %) a vyhrožování (39 %). Většina obětí (79 %) pociťovala nějakou formu nepříjemných prožitků, zatímco pouze 21 % nevnímalo toto setkání jako něco, co by je emocionálně zasáhlo. Tyto situace mají největší následky na věkovou kategorii dospívajících (17–19 let), kdy u 13 % z nich přetrvávaly nepříjemné pocity až několik měsíců. U dívek nepříjemný pocit přetrvával déle než u chlapců [41].

V souvislosti se sexuálním obsahem na internetu se ukázalo, že až 12 procent respondentů se s ním setkává každý den nebo téměř každý den. U věkové kategorie 15–17 let to bylo dokonce 25 %. Nejčastěji se s ním setkávají na mobilních zařízeních nebo noteboocích (30 %). Překvapivě 80 % dětí a dospívajících nebylo sexuálním obsahem nijak rozrušeno a 41 % z nich bylo rádo, že ho vidělo (dívek 11 %, chlapců 60 %). Dívky vnímaly zprávy se sexuálním obsahem více negativně než chlapci. Se sextingem, tedy přijímáním zpráv se sexuálním obsahem ve formě slov, obrázků nebo videí, má zkušenost 35 % dětí a dospívajících ve věku 11–17 let. Nejvíce takových zpráv si vyměňují dospívající ve věku 15–17 let [41].

Dále téměř polovina (49 %) účastníků výzkumu ve věku 9–17 let uvedla, že byla na internetu někdy v kontaktu s neznámou osobou. U věkové kategorie 9–10 let to bylo 16 %, zatímco u věkové kategorie 15–17 let to bylo 77 %. S neznámou osobou se 23 % dotázaných setkalo osobně, z toho 78 % hodnotilo setkání pozitivně. Nejčastěji se setkali s lidmi ve svém věku (67 %), ale u 7 % případů šlo o schůzku s dospělou osobou [41].

Děti a dospívající ve věku 11–17 let na internetu přicházejí do styku s obsahem nebo diskusemi, které zahrnují nenávistné zprávy napadající určité skupiny nebo jednotlivce (26 %), kruté nebo násilné obrázky, fotografie nebo videa (18 %), ukázky fyzického poškozování nebo sebepoškozování (17 %), informace o užívání drog (17 %) a způsoby spáchání sebevraždy (11 %) [41].

Během výzkumu 21 % respondentů uvedlo, že jejich zařízení (mobilní telefony, tablety, počítače) bylo někdy napadeno virem. 9 % se setkalo s neoprávněným použitím svého hesla, 7 % uvedlo, že jejich osobní údaje byly zneužity způsobem, který se jim nelíbil, a 7 % z nich trpělo nedostatkem spánku nebo jídla kvůli internetu [41].

4.2 České děti v kybersvětě (2019)

Tento výzkum byl proveden ve spolupráci mezi Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci a společností O2 Czech Republic. Pro sběr dat byl použit anonymní online dotazník, který byl distribuován do základních škol v celé České republice. Celkem se do výzkumu zapojilo 27 177 dětí ve věku 7-17 let, přičemž reprezentativní vzorek se zaměřoval na věkovou skupinu 11-17 let, z nichž 49,83 % byli chlapci [42].

Cílem výzkumu bylo zkoumat otázky spojené s tím, jak respondenti využívají internet, mobilní telefony a jak často se setkávají s kybernetickou agresí. Sběr dat probíhal v období od 1. února 2019 do 1. května 2019 a vyhodnocení dat bylo provedeno pomocí statistického softwaru Statistica [42].

4.2.1 Výsledky výzkumu

Výzkumné otázky se zaměřily na dětmi nejčastěji navštěvované webové stránky na internetu. Respondenti byli rozděleni do dvou věkových skupin: do 13 let a od 13 let. Děti mladší 13 let nejčastěji navštěvují sociální sítě (51,75 %), webové stránky pro sdílení videí, jako YouTube nebo Stream (41,10 %), online encyklopedie (30,32 %) a herní stránky (29,52 %). Nejméně často dotazovaní do 13 let navštěvují stránky s pornografií (2,84 %), darknetové stránky (2,08 %) nebo stránky s násilným obsahem (1,37 %). Respondenti starší 13 let navštěvují častěji sociální sítě (75,61 %), platformy YouTube nebo Stream (55,91 %), online encyklopedie (39,23 %), e-shopy, bazary a aukční servery (28,58 %). Stránky s pornografií navštěvuje 18,08 % z nich, nejméně se navštěvují darknetové stránky (4,07 %) a stránky s násilným obsahem (3,75 %). Sociální sítě, kterými jsou například Facebook, Instagram nebo YouTube, navštěvuje nejvíce dospívajících ve věku 17 let (80,15 %) a návštěvnost postupně klesá spolu s věkem dětí. Aplikace TikTok má mezi českými dětmi také poměrně vysokou návštěvnost (28,48 %), zejména mezi dětmi ve věku 11-12 let [42].

Výzkum se dále zabýval tím, jakým způsobem používají děti mobilní zařízení. Více než polovina z nich (59,1 %) má trvalý přístup k internetu přes mobilní data a není tak omezena na připojení k Wi-Fi. Mezi nejčastější aktivity, ke kterým děti využívají mobilní telefony, patří telefonování (72,49 %), psaní a odesílání zpráv přes online aplikace (66,39 %), sledování videí na YouTube (65,42 %), psaní a odesílání SMS/MMS zpráv (54,22 %), fotografování (51,66 %) a hraní her (49,52 %) [42].

V rámci výzkumu se sledovala také kybernetická agrese v online prostředí. Zjistilo se, že téměř polovina dotazovaných (41,29 %) zažila kybernetickou agresi během posledního roku. Nejčastěji šlo o slovní útoky prostřednictvím internetu nebo mobilních telefonů (27,17 %), prolomení a napadení online účtů na sociálních sítích nebo e-mailu (12,64 %) a šíření zesměšňujících nebo trapných fotografií (12,25 %). Méně časté byly případy šíření intimních fotografií dětí (3,38 %), zesměšňujících nebo ponižujících zvukových záznamů dětí (3,82 %) a zneužívání online účtů k obtěžování přátel dětí (4,97 %). Nejčastějšími platformami, na kterých docházelo ke kybernetické agresi, byly Facebook (56,41 %), Facebook Messenger (42,67 %) a Instagram (31,65 %). Nejméně se respondenti setkali s agresí na Pinterestu (1,31 %), v online hrách (0,94 %) nebo na Discordu (0,60 %). Většina těchto agresí trvala méně než týden (60,02 %) nebo 1-2 týdny (13,80 %), ale některé případy trvaly i déle než rok (6,76 %). Nejčastěji byli agresory spolužáci ze stejné třídy (29,40 %), bývalí kamarádi (16,40 %), žáci z jiné školy (14,43 %) nebo spolužáci ze stejné školy, ale z jiné třídy (12,66 %). Chlapci (34,68 %) byli častěji pachateli agresí než dívky (21,49 %), přičemž v některých případech nebyl pachatel identifikován (21,06 %) [42].

Mezi další rizikové situace, s kterými se děti setkávají, patří nedodání objednaného a zaplaceného zboží z internetu (13,34 %) a krádež virtuálních postav v online hrách (10,45 %). Poslední otázka výzkumu se týkala osobních schůzek s cizími lidmi z internetu, přičemž 26,77 % dětí uvedlo, že bylo pozváno někým cizím na osobní setkání, 70 % z pozvaných se tohoto setkání zúčastnilo [42].

4.3 Sexting u českých dětí (2020)

Tento výzkum se zaměřoval na fenomén sextingu, což je elektronické šíření obsahu se sexuální tematikou pomocí internetu a mobilních telefonů. Patří sem především textové zprávy, fotografie a videa. Cílem studie bylo analyzovat rozšíření sextingu mezi českými dospívajícími ve věku 11–17 let a zhodnotit souvislosti s různými faktory [34].

Sběr dat probíhal od 1. srpna 2018 do 1. srpna 2019 na základních a středních školách v České republice prostřednictvím anonymního elektronického dotazníkového šetření využívajícího specializovaný systém E-Bezpečí. Do výzkumu byli zapojeni žáci ve věku 11–17 let. Celkem se studie zúčastnilo 5 675 respondentů, jejichž průměrný věk činil 14,20 let. Z tohoto počtu 51,75 % tvořili chlapci a 48,25 % dívky [34].

4.3.1 Výsledky výzkumu

V rámci tohoto výzkumu byl zkoumán sexting ve třech základních formách: textové zprávy, fotografie a videa. Tyto formy byly dále rozděleny do tří kategorií: odesílání intimního materiálu jiné osobě (přes soukromou komunikaci), přijímání intimního materiálu a sdílení intimního materiálu (veřejně nebo ve skupině s dalšími uživateli, kteří mohou daný materiál dále šířit) [34].

Z výsledků výzkumu vyplývá, že sexting ve formě textových zpráv provozuje 25,92 % českých dospívajících, přičemž 54,81 % z nich jsou chlapci a 45,19 % dívky. Z těchto respondentů pravidelně rozesílá intimní zprávy 16 % a příležitostně je rozesílá více než 83 % z nich. Tato forma sextingu je považována za méně rizikovou než zasílání fotografií a videí [34].

Se zasíláním vlastních intimních fotografií má zkušenost 15,68 % českých účastníků výzkumu, přičemž 51,82 % jsou dívky a 48,18 % chlapci. Z nich pravidelně zasílá fotografie 26 % a příležitostně 74 %. Tento druh sextingu je považován za vysoce rizikový, protože může vést k online i offline agresi, jako je vydírání nebo vyhrožování [34].

Dalším zkoumaným aspektem bylo zasílání vlastních intimních videí. Přibližně 5,9 % českých dospívajících rozesílá svá vlastní videa, přičemž 63,96 % z nich jsou chlapci a 36,04 % dívky [34].

Z výzkumu vyplývá, že chlapci odesílají provokativní erotické textové zprávy a videa častěji než dívky. Nicméně obě pohlaví vykazují stejnou míru ochoty k odesílání intimního materiálu v podobě textu, fotografie nebo videa, ta se zvyšuje s věkem, zejména u respondentů ve věku 15–17 let. Zajímavé je, že respondenti, kteří se účastnili sexuální výchovy nebo byli o tématu poučeni, projevují větší ochotu k odesílání intimních materiálů. Stejnou ochotu vykazují dotazovaní, kteří se zúčastnili besed o nebezpečích internetu, ve srovnání s těmi, kteří se neúčastnili. Děti, kterým rodiče omezují čas strávený online projevují menší ochotu k odesílání intimního materiálu [34].

Zároveň bylo zjištěno, že účastníci výzkumu, kteří komunikují na internetu s neznámými lidmi, projevují větší ochotu k odesílání intimního materiálu v podobě textu, fotografie nebo videa. Nejčastěji se sexting provozuje pomocí sociálních sítí Facebook (66,74 %), Facebook Messenger (54,23 %) a Snapchat (47,97 %), zatímco nejméně se využívají sociální sítě LinkedIn (2,96 %) a Pinterest (3,07 %). Dotázaní také uvedli, že v případě zneužití jejich intimní fotografie nebo videa by se nejčastěji svěřili rodičům (39,67 %) nebo kamarádům (28,39 %). 33,59 % dětí uvedlo, že by se s touto situací nikomu nesvěřilo [34].

Výzkum ukázal, že necelá polovina respondentů (48,84 %) má negativní zkušenosti s internetovým nebo mobilním ponižováním, urážením nebo zesměšňováním, z toho 50,9 % dětí bylo obětí takových forem agresivního jednání. Dokonce 40,32 % účastníků výzkumu zažilo vyhrožování nebo zastrašování prostřednictvím internetu nebo mobilního telefonu. Pachateli těchto agresivních činů jsou nejčastěji bývalí partneři (29,28 %), bývalí kamarádi (28,60 %) nebo neznámí útočníci (29,28 %) [34].

4.4 Riziková komunikace a seznamování českých dětí v kyberprostoru (2021)

V rámci tohoto výzkumu byly zkoumány projevy rizikové online komunikace u českých dětí. Dětem byly zadány otázky směřující k získávání údajů o tom, jaké informace o sobě sdělují online, jakým způsobem komunikují v online prostředí, jaké metody používají při seznamování. Pro sběr dat byl použit kvantitativní výzkumný dotazník prostřednictvím nástroje Google Forms. Tento anonymní dotazník byl distribuován po celé České republice ve spolupráci s krajskými a městskými koordinátory a manažery prevence rizikového chování. Před samotným dotazníkovým šetřením proběhla pilotní studie, která zahrnovala rozhovory a konzultace s odborníky. Sběr dat probíhal v období od 1. srpna 2018 do 1. srpna 2019 a dotazníkové odpovědi byly následně zpracovány a analyzovány pomocí statistického softwaru Statistica 12. Celkem se dotazníkového šetření zúčastnilo 5 675 žáků základních a středních škol z celé České republiky ve věku mezi 11 až 17 lety. Z tohoto počtu bylo 51,75 % chlapců a 48,25 % dívek [43].

4.4.1 Výsledky výzkumu

Z výzkumu vyplývá, že více než polovina dospívajících (50,50 %) komunikuje s cizími lidmi na internetu. Mnoho z nich vyhledává především kamarády opačného pohlaví. Celkem 13,75 % respondentů by si do svých přátel přidalo zcela neznámou osobu, z toho 17,22 % chlapců a 10,3 % dívek. Setkání s neznámou osobou z internetu by 50,62 % dotazovaných odmítlo. Avšak 17,77 % respondentů bylo ochotno se na setkání vydat a 30,85 % by bylo v tomto ohledu neutrální. Chlapci (23,47 %) vykazovali větší ochotu k setkání než dívky (12,05 %). Z výzkumu je patrné, že chlapci vykazují větší ochotu k rizikové online komunikaci než dívky, přičemž tato ochota se zvyšuje s věkem. Studie se rovněž zaměřovala na souvislost mezi účastí dětí na besedách o nebezpečích internetu a ochotou k rizikové online komunikaci. Bylo zjištěno, že ti, kteří se besed účastnili, projevují větší ochotu k těmto rizikovým aktivitám. Naopak ti, jimž rodiče omezují nejen dobu strávenou na internetu, ale i přístup k některým webovým stránkám, vykazují menší ochotu k těmto aktivitám [43].

Výzkum odhalil, že 22,57 % dotazovaných jejich internetový kamarád požádal, aby jejich online komunikace zůstala tajná. Co se týče osobních setkání, 31,06 % respondentů bylo požádáno o schůzku. Ze všech dotazovaných by 58,56 % informovalo své rodiče o plánované schůzce, 28,04 % z nich by to sdělilo svému kamarádovi nebo sourozenci a 10,56 % by o tom nikomu neřeklo [43].

Další část výzkumu se zaměřila na vnímání rizik spojených s online komunikací a osobními setkáními. 38,63 % respondentů považuje online komunikaci s neznámými lidmi na internetu za rizikovou, zatímco 36,75 % ji považuje za bezpečnou. Zároveň 71,21 % účastníků výzkumu vnímá osobní setkání s cizí osobou z internetu za rizikové. Mezi nejčastěji uvedené důvody, proč setkání může být nebezpečné, patří skutečnost, že dotyčná osoba se může vydávat za někoho jiného, může je zneužít, okrást nebo jim ublížit [43].

Chlapci a dívky, kteří participovali na tomto výzkumu, na internetu také sdílí některé své osobní údaje. Nejčastěji jsou to jméno a příjmení (89,55 %), fotografie obličeje (66,98 %), e-mailová adresa (65,06 %) a telefonní číslo (29,43 %). Nejméně sdílejí své heslo k e-mailové adrese (3,07 %), rodné číslo (1,53 %) nebo PIN kreditní karty (0,60 %). Fotografie obličeje je považována za nejrizikovější osobní údaj. I přesto 33 % dotazovaných nevnímá zveřejňování fotografií obličeje jako rizikové. Se žádostí o citlivé údaje se setkalo 31,37 % respondentů. Dále například 18 % účastníků výzkumu vyhovělo žádosti o zaslání fotografie obličeje cizí osobě na internetu a 16,27 % dospívajících bylo požádáno o intimní fotografie, z nich 21,42 % takovou žádost splnilo [43].

Důležitým tématem výzkumu bylo ověření, zda by mladiství dokázali rozpoznat falešný profil na sociálních sítích nebo podezřelou online komunikaci s dospělou osobou. 56,9 % z nich uvedlo, že by podezřelou online komunikaci odhalilo, zejména díky neodbytným otázkám týkajícím se osobních údajů a požadavkům

na zaslání běžných nebo intimních fotografií. 12,6 % dotazovaných přiznalo, že by tuto komunikaci nedokázalo rozpoznat. Celkem 36,78 % dospívajících tvrdí, že by rozpoznalo online komunikaci s dospělou osobou, zatímco 19,19 % by ji nerozpoznalo. Téměř polovina respondentů (49,78 %) neověřuje identitu svých internetových přátel v kyberprostoru [43].

Výsledky výzkumu ukázaly, že chlapci vykazují větší schopnost rozpoznat podezřelou komunikaci, komunikaci s dospělou osobou a falešné profily na sociálních sítích než dívky. Schopnost rozpoznání také roste s věkem jedince. Více těchto schopností měly děti, které se zúčastnily besed o nebezpečích na internetu. Zatímco respondenti, jimž rodiče omezují čas strávený na internetu nebo přístup k určitým internetovým stránkám, vykazovali menší schopnost rozpoznání podezřelé komunikace a falešných profilů. Větší schopnost rozpoznat tato rizika měli ti, které běžně komunikují s neznámými lidmi na internetu [43].

Nejčastěji využívanými internetovými aplikacemi a sociálními sítěmi jsou YouTube (90 %), Facebook (87,4 %) a Instagram (50,75 %). Většina dospívajících má počítač umístěný ve svém vlastním pokoji (více než 57 %), zatímco 20 % z nich sdílí pokoj se sourozencem a 12,09 % má počítač v obývacím pokoji. Zároveň většina z nich (61,89 %) sdělila, že nemá stanovené omezení času stráveného na internetu ze strany svých rodičů [43].

Pokud jde o vzdělávání v oblasti rizikového chování na internetu, 80 % dětí se zúčastnilo preventivních besed zaměřených na rizika spojená s internetem. Ve školách se také vyučuje sexuální výchova, které se zúčastnilo 50,22 %. 73,9 % dospívajících bylo někým o sexu poučeno, nejčastěji od kamarádů (39,91 %), učitelů (33,39 %) nebo rodičů (32,74 %) [43].

4.5 Online svět v dětských domovech (2022)

Tento výzkum se zaměřoval na rizikové situace v souvislosti s internetem, kterým čelí děti v dětských domovech. Cílem bylo získat informace o jejich přístupu k internetu, o jejich zkušenostech a o tématech, kterým se pracovníci dětských domovů věnují ve vztahu k online světu. Výzkum probíhal prostřednictvím elektronického dotazníku [44].

Celkem se výzkumu zúčastnilo 166 pracovníků dětských domovů ze všech krajů České republiky. Z toho 25,3 % respondentů byly ženy a 74,7 % muži. Věkový rozptyl pracovníků byl mezi 22 a 70 lety, s průměrným věkem 45,66 let. Většina z nich měla ukončené vysokoškolské vzdělání (70,48 %) nebo středoškolské vzdělání s maturitou (25,51 %) [44].

Druhou zkoumanou skupinu tvořilo 197 klientů (dětí žijících v dětských domovech). Z nich 54,31 % byly dívky a 45,69 % chlapci. Věk dotazovaných byl ve věkovém rozmezí od 9 do 25 let. Z toho většina (79,69 %) byla mladších 18 let [45].

Výzkum probíhal ve spolupráci se Safer Internet Centrum ČR a Pedagogickou fakultou Univerzity Palackého v Olomouci, konkrétně s jejím Centrem prevence rizikové virtuální komunikace. Sběr dat probíhal od května do října 2021 [44].

4.5.1 Výsledky výzkumu

V první části výzkumu se zkoumaly obecné informace o využívání internetu v dětských domovech, o nejčastěji navštěvovaném online obsahu a o opatřeních pro zabezpečení internetu [44].

Na základě dotazníků bylo zjištěno, že téměř všechny dětské domovy (99,39 %) mají přístup k internetu. Téměř 83,13 % jejich pracovníků omezuje klientům přístup k internetu. Z tohoto počtu mělo 78,92 % klientů přístup k internetu omezený na předem stanovený čas, 13,25 % mělo neomezený přístup a 7,23 % z nich mělo přístup k internetu až po splnění povinností. Většina pracovníků dětských domovů reguluje čas strávený na internetu nezávisle na věku klientů (63,86 %), přičemž zbylá procenta se řídí jejich věkem. Nejčastěji klienti tráví na internetu 2-3 hodiny v pracovní dny a nejvíce 3-4 hodiny v sobotu a 2-4 hodiny v neděli. Omezení přístupu na internet se obvykle uplatňuje ve večerních hodinách, konkrétně v pondělí až čtvrtek mezi 20. a 21. hodinou a v pátek a sobotu mezi 21. a 22. hodinou. Nejčastěji klienti používají internet ve svém vlastním pokoji (40,36 %), přičemž 31,33 % z nich sdílí pokoj s někým dalším [44].

Pokud jde o bezpečnostní opatření, 46,99 % pracovníků omezuje internetový obsah, dalších 22,29 % neomezuje obsah, ale má ústní dohodu s klienty. 8,43 % pracovníků neprovádí kontrolu obsahu, ani nemá s klienty žádnou ústní dohodu. Většina dětských domovů používá různé formy kontroly obsahu, včetně ústní dohody s důkladnou kontrolou (36,75 %), ústní dohody bez důkladné kontroly (30,12 %), nastavení konkrétních služeb (21,69 %), softwarových řešení (17,47 %) a hardwarových řešení (12,65 %). Většina pracovníků dětských domovů (63,86 %) také nastavuje „dětský“ režim pro filtrování obsahu na internetových stránkách [44].

Většina klientů (80,71 %) vlastní mobilní telefon, ostatní si půjčují telefony od kamarádů nebo vychovatelů. Téměř polovina z klientů (50,25 %) má přístup na internet pomocí mobilních dat a není tedy odkázána na Wi-Fi. Zajímavým zjištěním bylo, že 17,26 % klientů získává kredit nebo data pro své telefony od neznámých lidí na internetu. 2 % klientů získala kredit výměnou za své fotografie nebo videa, včetně snímků zobrazujících jejich nahotu [44].

Mezi nejčastější aktivity klientů na internetu patří psaní a odesílání zpráv přes online aplikace (55,84 %), sledování videí na YouTube (52,28 %), telefonování (48,73 %), fotografování (42,13 %) a hodnocení obsahu na sociálních sítích (41,12 %). Mezi oblíbené aktivity také patří hraní her (41,12 %). Mezi nejčastěji hrané hry patří Minecraft (45,22 %) a Roblox (39,49 %) [44].

Další část výzkumu se zaměřovala na identifikaci rizikových forem komunikace u klientů. Podle zjištěných informací se nejčastěji jednalo o následující situace: slovní ublížení prostřednictvím internetu nebo mobilních telefonů (48,19 %), šíření ponižujících a zesměšňujících fotografií (29,52 %), vyhrožování a zastrašování pomocí internetu nebo mobilních zařízení (22,29 %), neoprávněný přístup nebo prolomení hesla do online účtu – například k sociálním sítím (21,69 %) a šíření intimních fotografií (17,47 %). Pouze 8,43 % klientů zažilo online podvody v rámci inzerátů, nákupů nebo aukcí. Zajímavým zjištěním je, že 27,11 % pracovníků a klientů uvedlo, že se v dětském domově s žádnou z výše uvedených situací dosud nesetkali [44].

Většina těchto útoků trvala kratší dobu než týden (36,75 %), 22,29 % útoků trvalo 1 až 2 týdny a 9,64 % útoků trvalo 3 až 5 týdnů. Nejčastěji dochází k útokům prostřednictvím sociálních sítí, přičemž Facebook (62,92 %), Instagram (32,58 %), Facebook Messenger (32,58 %), YouTube (15,73 %) a TikTok (13,48 %) jsou hlavními platformami, na kterých se tyto útoky vyskytují. Nejčastěji na děti útočili jejich bývalí kamarádi (15,73 %) a spolužáci ze stejné třídy (14,61 %) [44].

Z celkového počtu dotázaných, kteří se setkali s nějakým typem online útoku, se 37,08 % rozhodlo o tom nikomu neříkat. Menší část z nich o problému informovala své rodiče (26,97 %) nebo vychovatele v dětském domově (15,73 %) a pouze minimum dospívajících oznámilo situaci Policii ČR (2,25 %) nebo zavolalo linku bezpečí (2,25 %) [44].

Předmětem výzkumu také bylo, jak klienti dětských domovů komunikují s lidmi, které neznají, prostřednictvím internetu. Většina z nich (64,47 %) striktně odmítla komunikovat s neznámými osobami na internetu, zatímco ostatní běžně navazují konverzaci s neznámými lidmi. Děti si často na internetu hledají nové kamarády a 62 % z nich uvedlo, že si přidalo neznámou osobu z internetu mezi své přátele na sociálních sítích. Pokud by je někdo na sociální síti oslovil s žádostí o přidání mezi přátele, 62,94 % z nich by s tímto požadavkem souhlasilo a přidalo by si danou osobu mezi své přátele. 18,27 % dotazovaných klientů uvedlo, že neznámá osoba, kterou si přidali mezi přátele, je požádala o udržování jejich přátelství v tajnosti. Přesto by se většina z nich (63,96 %) odmítla setkat s někým, koho znají pouze přes internet. Jen 14,21 % by na takovou schůzku šlo. Pokud by šlo o osobní setkání, nejčastěji by se respondenti svěřili vychovatelům z dětského domova (64,47 %), rodičům (30,96 %) nebo kamarádům či sourozencům (17,77 %). Nicméně 11,17 % mladistvých by o setkání nikomu neřeklo [44].

Další část výzkumu se zaměřovala na sexualitu dospívajících v dětských domovech. Většina z nich (77,66 %) uvedla, že byla poučena o sexu. Nejčastěji tuto informaci získali od vychovatele v dětském domově (45,18 %), matky (31,47 %), otce (13,20 %), učitele (27,92 %), kamaráda nebo kamarádky (22,34 %) nebo si sami na internetu našli informace (15,23 %). Pouze malé procento uvedlo, že je o sexu poučil někdo dospělý na internetu (1,02 %) nebo dědeček (1,52 %), případně získali informace z časopisu (2,03 %) [44].

V některých dětských domovech se vyskytuje fenomén sextingu, tedy posílání intimních zpráv a fotografií. Podle výzkumu se 7,11 % dětí přiznalo, že se tomuto chování věnuje pravidelně, zatímco 12,18 % dětí to zkusilo jen jednou. Většina klientů (70,56 %) však nikdy nic podobného nezasílala. Ti, kteří provozují sexting, nejčastěji posílají zprávy a fotografie svým bývalým (39,47 %) nebo současným (26,32 %) partnerům. Někteří z nich také provozují sexting s osobami, které znají pouze z internetu (18,41 %) [44].

Poslední část výzkumu se zaměřovala na realizaci preventivních opatření v dětských domovech. Nejčastěji se prevence provádí formou rozhovoru mezi vychovatelem a klientem (89,16 %). Další formy prevence zahrnují zhlédnutí preventivně zaměřených filmů (57,23 %) a přednášky (47,59 %). Pouze 0,6 % pracovníků uvedlo, že se prevencí nezabývá a přenechává tento úkol škole nebo jiné instituci. Mezi nejčastěji řešená témata patří komunikace s neznámými lidmi (89,16 %), ochrana osobních údajů (86,75 %), seznamování se v online prostředí (84,34 %), agrese na internetu (76,51 %) a sexting, včetně sexuality a pornografie (72,29 %). Méně často se s dětmi probírá problematika autorských práv (16,06 %) a negativního vlivu sekt (19,28 %). Pouze 1,81 % pracovníků uvedlo, že s klienty neřeší vůbec žádná témata [44].

5 Přípravy do výuky informačních a komunikačních technologií a základů společenských věd

S rostoucím významem digitálních technologií se stává stále důležitější, aby lidé byli obeznámeni s riziky a bezpečnostními opatřeními při používání digitálních zařízení a služeb. Proto je nutné poučit žáky o základech digitální bezpečnosti a poskytnout jim nástroje a dovednosti, které jim umožní chránit jejich osobní údaje a komunikovat bezpečně na internetu [10].

V této kapitole jsou popsány přípravy do výuky ze vzdělávacích oblastí Člověk a společnost a Informační a komunikační technologie, které mohou posloužit jako inspirace pro výuku výše zmíněné problematiky. Jednotlivé přípravy si dávají za cíl rozšířit žákovy znalosti a dovednosti v oblasti bezpečné komunikace v digitálním světě. Tyto přípravy jsou tematicky tvořeny v souladu s rámcově vzdělávacím programem pro obchodní akademie (obor vzdělávání 63–41–M/02) z roku 2020 [45].

5.1 Rámcově vzdělávací program

Rámcově vzdělávací program je klíčovým prvkem moderního vzdělávacího systému. Jedná se o plán vzdělávání, který stanovuje cíle, obsah a metodiku výuky pro daný obor nebo stupeň vzdělání. Jeho cílem je zajistit, aby studenti získali potřebné znalosti, dovednosti a kompetence v souladu s požadavky společnosti a trhu práce. Rámcově vzdělávací program také umožňuje flexibilitu a přizpůsobení vzdělávacího procesu měnícím se potřebám a vývoji oboru. V současné době je tato koncepce používána v mnoha zemích jako základ pro tvorbu školních osnov a pro hodnocení vzdělávacích výsledků [45].

5.1.1 Rámcově vzdělávací program – Vzdělávací oblast: Informační a komunikační technologie

Podle rámcově vzdělávacího programu pro obchodní akademie rozvíjí vzdělávací oblast Informační a komunikační technologie znalosti získané v základním vzdělávání. Žáci se učí informatickému myšlení a zdokonalují své porozumění principům digitálních technologií. Studium informatiky jim umožňuje se seznámit s pojmy, nástroji a metodami tohoto oboru, který se zaměřuje na efektivní a automatizované zpracování informací. V informatice se žáci učí analyzovat a porovnávat různá řešení problémů a svá řešení postupně vylepšovat. Žáci se dále učí navrhovat informační systémy pro konkrétní účely a získávat, zpracovávat a zabezpečovat data. Získané postupy a postoje pomáhají žákům lépe porozumět digitálním technologiím. V informatice je kladen důraz na aktivní přístup žáků k řešení praktických problémů [45].

5.1.2 Rámcově vzdělávací program – Vzdělávací oblast: Společenskovědní vzdělávání

Podle rámcově vzdělávacího programu pro obchodní akademie rozvíjí vzdělávací oblast Společenskovědní vzdělávání společenskovědní znalosti získané v základním vzdělávání. Tato oblast pomáhá žákům kriticky reflektovat společenskou skutečnost a rozvíjet myšlenkové operace, praktické dovednosti a vědomí vlastní identity. Zahrnuje také historické vědomí a uchování tradičních hodnot, občanské vzdělání a respekt k základním principům demokracie. Tato oblast připravuje žáky na odpovědný občanský život v souladu s principy udržitelného rozvoje a podporuje vědomí neopakovatelnosti a jedinečnosti života a úcty k výtvorům lidského ducha [45].

5.2 Přehled jednotlivých příprav

Jednotlivé přípravy jsou uvedeny v příloze (viz Příloha B) diplomové práce.

5.2.1 Informační a komunikační technologie: První hodina

První hodina informačních a komunikačních technologií dodržuje rámcově vzdělávací program pro obchodní akademie (obor vzdělávání 63–41–M/02) a konkrétně vychází ze vzdělávacího obsahu práce v lokální síti, elektronická komunikace, komunikační a přenosové možnosti Internetu. Rámcově vzdělávací program zde uvádí téma e-mailu, chatu, messengeru, videokonference…

Tabulka 1 Informační a komunikační technologie: První hodina

Škola	63–41–M/02 Obchodní akademie
Předmět	Informační a komunikační technologie
Vzdělávací obsah	Práce v lokální síti, elektronická komunikace, komunikační a přenosové možnosti Internetu
Průřezové téma	Mediální výchova
Téma vyučovací hodiny	Bezpečné digitální prostředí
Cíle hodiny	Žák vyjmenuje alespoň 5 platforem, které v digitálním světě slouží ke komunikaci mezi uživateli.
	Žák rozpozná alespoň 3 platformy, které v digitálním světě slouží ke komunikaci mezi uživateli, podle loga.
	Žák definuje výhody a nevýhody alespoň 1 této komunikační platformy z digitálního světa.

Během hodiny žáci získají znalosti o vlastnostech digitálního světa. Učitel jim na začátku hodiny pomáhá vést diskusi o důležitosti vzdělání v oblasti bezpečnosti v digitálním prostředí. Dále žáci pracují ve skupinách, kde vyhledávají informace o konkrétních sociálních sítích a ztvárňují je graficky na flipchartový papír. V závěru vyučovací hodiny se provádí rekapitulace, v rámci které učitel shrnuje důležité informace a žáci zhodnocují svou dosavadní práci ve skupinách. Celá hodina je strukturovaná a zahrnuje aktivizační prvky.

Průběh hodiny

Tato hodina je navržena tak, aby byla co nejvíce atraktivní a interaktivní pro žáky. Na začátku hodiny učitel třídu zklidní a získá si její pozornost, následně vytváří příjemnou atmosféru a prostřednictvím ice-breakingu se snaží naladit žáky na téma hodiny. Poté se opakuje látka minulé hodiny pomocí hry, která žáky aktivizuje. Díky tomu si připomenou důležité informace z minulé hodiny a vyučující si tak zkontroluje, co si pamatují.

Dále jsou žáci seznámeni s průběhem hodiny a motivováni pomocí diskuse o důležitosti vzdělání v oblasti bezpečnosti v digitálním světě. Tímto způsobem se v nich vyvolá vnitřní motivace, aby pro ně téma hodiny bylo více poutavé.

Po motivaci následuje expozice, během které učitel předává základní teoretické znalosti o vlastnostech digitálního světa. Zde žáci získávají nové informace a osvojují si základní poznatky k tématu sociální sítě.

Poté následuje skupinová práce, která umožňuje žákům uplatnit jejich znalosti a dovednosti v praxi. Třída je rozdělena do skupin, ve kterých žáci vyhledávají informace o konkrétních sociálních sítích a graficky tato data ztvárňují na flipchartový papír. Aktivita podporuje týmovou spolupráci, výměnu informací a rozvoj komunikačních dovedností.

Na konci hodiny jsou rekapitulovány důležité informace z hodiny, včetně jejího průběhu. Rovněž se získává zpětná vazba od žáků. Ta je důležitá, protože díky ní se dá zhodnotit, zda hodina splnila svůj cíl a zda žáci získali potřebné znalosti a dovednosti.

Celkově tato hodina kombinuje různé prvky, jako je interakce, aktivní účast žáků, opakování minulého učiva, motivace, diskuse a skupinová práce. Věřím, že takový přístup zajišťuje efektivní výuku a zároveň motivuje žáky ke kritickému myšlení, spolupráci a získávání nových dovedností.

5.2.2 Informační a komunikační technologie: Druhá hodina

Druhá hodina informační a komunikační technologie dodržuje rámcově vzdělávací program pro obchodní akademie (obor vzdělávání 63–41–M/02) a konkrétně vychází ze vzdělávacího obsahu práce v lokální síti, elektronická komunikace, komunikační a přenosové možnosti Internetu. Rámcově vzdělávací program zde uvádí téma e-mailu, chatu, messengeru, videokonference…

Tabulka 2 Informační a komunikační technologie: Druhá hodina

Škola	63–41–M/02 Obchodní akademie
Předmět	Informační a komunikační technologie
Vzdělávací obsah	Práce v lokální síti, elektronická komunikace, komunikační a přenosové možnosti Internetu
Průřezové téma	Mediální výchova
Téma vyučovací hodiny	Bezpečná práce s hesly, zabezpečení zařízení a dat
Cíle hodiny	Žák vyjmenuje alespoň 3 pravidla pro bezpečnou práci s hesly.
	Žák vyjmenuje alespoň 2 pravidla pro zabezpečení zařízení.
	Žák vyjmenuje alespoň 2 pravidla pro zabezpečení dat.

Během hodiny žáci získají znalosti o práci s hesly a bezpečnostními opatřeními v digitálním prostředí. Na začátku hodiny prezentují žáci produkt své skupinové práce z minulé hodiny. Jedná se o flipchartový papír obsahující informace o konkrétní sociální síti. Poté učitel prezentuje žákům základní pravidla pro bezpečnou práci s hesly. Žáci pak pracují samostatně na tvorbě vlastních bezpečných hesel. Hodina se uzavírá rekapitulací, hodnocením žáků a získáním zpětné vazby. Celá hodina je strukturovaná a zahrnuje aktivizační prvky.

Průběh hodiny

Tato hodina byla vytvořena tak, aby byla co nejvíce přitažlivá a interaktivní pro žáky. Na začátku hodiny učitel třídu uklidní a získá si její pozornost, následně vytváří příjemnou atmosféru a prostřednictvím ice-breakingu se snaží naladit žáky na téma hodiny. Poté probíhá opakování minulé hodiny, během kterého žáci prezentují produkt své skupinové práce z minulé hodiny. Jedná se o flipchartový papír obsahující informace o konkrétní sociální síti. Vyučující po skončení prezentace provede hodnocení skupinových prací a umožní žákům vyjádřit názory na jejich práci ve skupině. Tím se podporuje jejich reflexe a sebereflexe.

Během následné diskuse získává učitel povědomí o stávajících znalostech třídy týkajících se bezpečného zacházení s hesly. Tím získá přehled o úrovni znalostí ve třídě. Poté prezentuje žákům základní pravidla pro bezpečné zacházení s hesly a ukazuje jim postupy pro vytvoření bezpečného hesla. Třída si osvojuje teoretické znalosti o práci s hesly.

Během aplikace žáci tvoří svá vlastní hesla podle představených pravidel. Učitel jim při tomto procesu asistuje. Žáci tak získávají praktické dovednosti. Následně si třída zkontroluje bezpečnost svých hesel pomocí nástroje https://www.passwordmonster.com/ .

Hodina končí fixací, během které učitel shrnuje řečené informace, a následnou rekapitulací nově získaných informací a průběhu hodiny. Rovněž se získává zpětná vazba od žáků. Ta je důležitá, protože díky ní se dá zhodnotit, zda hodina splnila svůj cíl a zda žáci získali potřebné znalosti a dovednosti.

Věřím, že prostřednictvím této strukturované a interaktivní výukové hodiny mají žáci možnost získat klíčové znalosti a dovednosti týkající se bezpečného zacházení s hesly. V rámci této hodiny proběhne diskuse, expozice, aplikace, fixace, reflexe a rekapitulace, to podporuje efektivní formu učení a zároveň motivuje žáky k aktivnímu přístupu ke vzdělávání.

5.2.3 Informační a komunikační technologie: Třetí hodina

Třetí hodina informačních a komunikačních technologií dodržuje rámcově vzdělávací program pro obchodní akademie (obor vzdělávání 63–41–M/02) a konkrétně vychází ze vzdělávacího obsahu práce v lokální síti, elektronická komunikace, komunikační a přenosové možnosti Internetu. Rámcově vzdělávací program zde uvádí téma e-mailu, chatu, messengeru, videokonference…

Tabulka 3 Informační a komunikační technologie: Třetí hodina

Škola	63–41–M/02 Obchodní akademie
Předmět	Informační a komunikační technologie
Vzdělávací obsah	Práce v lokální síti, elektronická komunikace, komunikační a přenosové možnosti Internetu
Průřezové téma	Mediální výchova
Téma vyučovací hodiny	Způsoby útoků na sociálních sítích – cíle a metody útočníků
Cíle hodiny	Žák vyjmenuje alespoň 3 způsoby útoků na počítačová zařízení.
	Žák vyjmenuje alespoň 3 sociotechnické metody útočníků.
	Žák vyjmenuje alespoň 3 způsoby, jak se proti sociotechnickým metodám útoku bránit.

Během hodiny se žáci seznámí s teoretickými znalostmi o rizicích digitálního světa, včetně kyberšikany, sextingu, phishingu, vishingu a kybergroomingu. Výklad učitel doplňuje o videa a diskusi, při které se žáci aktivně zapojují do průběhu hodiny. Na konci hodiny probíhají fixace a rekapitulace, při kterých se učitel zaměřuje na zopakování klíčových informací a zhodnocení práce žáků. Celá hodina je strukturovaná a zahrnuje aktivizační prvky.

Průběh hodiny

Tato hodina je navržena tak, aby se žáci seznámili s riziky digitálního světa a získali základní teoretické znalosti o kyberšikaně, sextingu, phishingu, vishingu a kybergroomingu. Na začátku hodiny učitel třídu zklidní a získá si její pozornost, následně vytváří příjemnou atmosféru a prostřednictvím ice-breakingu se snaží naladit žáky na téma hodiny.

Následuje opakování minulé vyučovací hodiny, které umožní žákům osvěžit si znalosti předchozího tématu. Pokud některý z žáků na minulé hodině chyběl, získá nyní alespoň stručný vhled do problematiky bezpečného používání hesel.

Dále jsou žáci seznámeni s průběhem hodiny a vyučující se v nich snaží vyvolat vnitřní motivaci k tématu hodiny. Do diskuse o způsobech útoků v digitálním světě se třída aktivně zapojuje, vyjadřuje své názory a zkušenosti. Následně učitel vede výklad s prvky diskuse o různých tématech, jako je kyberšikana, sexting, phishing, vishing a kybergrooming. Při výkladu některých témat jsou také použita videa, která názorně prezentují konkrétní rizika a problémy.

Hodina končí fixací, během které učitel shrnuje řečené informace, a následnou rekapitulací důležitých informací z hodiny a jejího průběhu. Rovněž je získávána zpětná vazba od žáků. Ta je důležitá, protože díky ní se dá zhodnotit, zda hodina splnila svůj cíl a zda žáci získali potřebné znalosti a dovednosti.

Celkově tato hodina kombinuje různé prvky, jako je opakování minulého učiva, motivace, diskuse, výklad s prvky diskuse, videa, fixace a rekapitulace. Věřím, že takový přístup umožňuje žákům získat základní znalosti o rizicích digitálního světa a aktivně se zapojit do vzdělávacího procesu. Tato hodina je strukturovaná a interaktivní, což přispívá k efektivnímu vzdělávání a rozvoji kritického myšlení žáků v oblasti digitální bezpečnosti.

5.2.4 Společenskovědní vzdělávání: První hodina

První hodina společenskovědního vzdělávání dodržuje rámcově vzdělávací program pro obchodní akademie (obor vzdělávání 63–41–M/02) a konkrétně vychází ze vzdělávacího obsahu člověk jako občan. Rámcově vzdělávací program zde uvádí téma masových médií a jejich funkce, do kterého komunikace prostřednictvím sociální sítě jistě patří.

Tabulka 4 Společenskovědní vzdělávání: První hodina

Škola	63–41–M/02 Obchodní akademie
Předmět	Společenskovědní vzdělávání
Vzdělávací obsah	Člověk jako občan
Průřezové téma	Mediální výchova
Téma vyučovací hodiny	Bezpečná komunikace na sociálních sítích
Cíle hodiny	Žák vyjmenuje 3 rizika, která hrozí při komunikaci na sociálních sítích.
	Žák definuje a vysvětlí 1 riziko, které se vyskytuje při komunikaci na internetu.
	Žák identifikuje alespoň 1 rizikové chování na sociálních sítích na základě příběhu.

Během hodiny se žáci seznámí s teoretickými znalostmi o bezpečné komunikaci na sociálních sítích. Poté následuje skupinová práce, kdy žáci ve skupinách vyhledávají informace o konkrétním riziku a ztvární je na flipchartový papír. V závěru vyučovací hodiny se provádí rekapitulace, při níž učitel shrnuje důležité informace a žáci zhodnocují svou dosavadní práci ve skupinách. Celá hodina je strukturovaná a zahrnuje aktivizační prvky.

Průběh hodiny

Tématem hodiny je bezpečnost při komunikaci prostřednictvím sociálních sítí a hodina se podrobněji zabývá konkrétními riziky spojenými s tímto tématem. Na začátku hodiny učitel třídu zklidní a získá si její pozornost, následně vytváří příjemnou atmosféru a prostřednictvím ice-breakingu se snaží naladit žáky na téma hodiny.

Opakování minulé hodiny probíhá prostřednictvím metody deset slov. Během této aktivity si žák připraví větu přesně o deseti slovech týkající se tématu probíraného v předchozí hodině. Žáci následně mají příležitost sdílet své věty se zbytkem třídy. Tato aktivita umožňuje žákům aktivně se zapojit a připomenout si důležité informace. Tím se podporuje jejich sebevědomí a zároveň se upevňují jejich dosavadní znalosti a dovednosti.

K vytvoření vnitřní motivace u žáků je použit demonstrativní příběh „O Elišce“, který rovněž slouží jako podnět pro nadcházející diskusi. Ta umožňuje žákům prezentovat své dosavadní znalosti a zkušenosti.

Expozice zajišťuje předání teoretických znalostí o hrozbách při komunikaci na sociálních sítích a internetu. Třída získává tyto informace od vyučujícího a ptá se na případné nejasnosti, což posiluje její schopnost porozumět tématu.

Poté následuje skupinová práce, ta umožňuje žákům uplatnit jejich znalosti a dovednosti v praxi. Žáci jsou rozděleni do skupin, ve kterých vyhledávají informace o konkrétním riziku vyskytujícím se na sociálních sítích a graficky tato data ztvárňují na flipchartový papír. Tato aktivita podporuje týmovou spolupráci, výměnu informací a rozvoj komunikačních dovedností.

Na konci hodiny jsou rekapitulovány důležité informace z hodiny, včetně jejího průběhu. Rovněž se získává zpětná vazba od žáků. Ta je důležitá, protože díky ní se dá zhodnotit, zda hodina splnila svůj cíl a zda žáci získali potřebné znalosti a dovednosti.

Celkově tato hodina poskytuje žákům možnost aktivně se zapojit, diskutovat a získat nové znalosti v oblasti bezpečnosti na sociálních sítích. Věřím, že takový přístup zajišťuje efektivní výuku a zároveň motivuje žáky ke kritickému myšlení, spolupráci a získávání nových dovedností v digitálním světě.

5.2.5 Společenskovědní vzdělávání: Druhá hodina

Druhá hodina společenskovědního vzdělávání dodržuje rámcově vzdělávací program pro obchodní akademie (obor vzdělávání 63–41–M/02) a konkrétně vychází ze vzdělávacího obsahu člověk jako občan. Rámcově vzdělávací program zde uvádí téma masových médií a jejich funkce, do kterého komunikace prostřednictvím sociální sítě jistě patří.

Tabulka 5 Společenskovědní vzdělávání: Druhá hodina

Škola	63–41–M/02 Obchodní akademie
Předmět	Společenskovědní vzdělávání
Vzdělávací obsah	Člověk jako občan
Průřezové téma	Mediální výchova
Téma vyučovací hodiny	Konkrétními rizika při komunikaci na sociálních sítích
Cíle hodiny	Žák umí prezentovat před diváky (spolužáky).
	Žák vyjmenuje alespoň 3 zásady, jak bezpečně komunikovat na sociálních sítích.
	Žák uvede rizika sociálních sítí a doloží je alespoň jedním příkladem. Uvede také možnosti, jak těmto rizikům předcházet.

Během hodiny se žáci seznámí s teoretickými znalostmi o bezpečné komunikaci na sociálních sítích. Na začátku hodiny prezentují žáci produkt své skupinové práce z minulé hodiny. Jedná se o flipchartový papír obsahující informace o konkrétních rizicích na sociálních sítích. Poté jsou žáci seznámeni s pravidly pro přípravu divadelní hry a rozděleni do skupin, ve kterých pracují na přípravě vlastního divadelního vystoupení, a nakonec prezentují své hry před třídou. Hodina končí rekapitulací klíčových informací, hodnocením žáků a získáním zpětné vazby. Celá hodina je strukturovaná a zahrnuje aktivizační prvky.

Průběh hodiny:

Tato hodina je navržena tak, aby podporovala kreativitu, spolupráci a komunikaci mezi žáky. Na začátku hodiny učitel třídu zklidní a získá si její pozornost, následně vytváří příjemnou atmosféru a prostřednictvím ice-breakingu se snaží naladit žáky na téma hodiny.

Následuje seznámení žáků s průběhem hodiny, které jim umožňuje získat přehled o časovém plánu a cílech hodiny. Vyučující zároveň vytváří u žáků vnitřní motivaci k tématu hodiny. Dalším cílem motivace je podpořit žáky, aby se cítili sebevědomě a neobávali se vystupovat před svými spolužáky.

Poté probíhá opakování minulé hodiny, během kterého žáci prezentují produkt své skupinové práce z předchozí hodiny. Jedná se o flipchartový papír obsahující informace o konkrétním riziku na sociální síti. Vyučující po skončení prezentace provede hodnocení skupinových prací a umožní žákům vyjádřit názory na jejich práci ve skupině. Tím se podporuje jejich reflexe a sebereflexe.

Poté je třída seznámena s pravidly pro přípravu divadelních her a rozdělena do skupin pomocí sáčku s barevnými víčky. Každá skupina připravuje vlastní divadelní hru. Vyučující kontroluje práci skupin a podporuje třídu v její práci.

Následuje aktivita, při níž skupiny předvádějí své divadelní hry před třídou. Učitel chválí žáky za jejich práci a uvádí další možnosti zpracování tématu. Tím se podporuje sebevědomí žáků a jejich schopnost prezentovat svou práci.

Hodina končí fixací, během které učitel shrnuje řečené informace, a následnou rekapitulací důležitých informací z hodiny, včetně jejího průběhu. Do rekapitulace a hodnocení hodiny se zapojují i žáci. Díky tomu se dá zhodnotit, zda hodina splnila svůj cíl a zda si žáci osvojili potřebné znalosti a dovednosti.

Věřím, že tato interaktivní a kreativní hodina umožňuje žákům rozvíjet dovednosti v oblasti herectví a současně podporuje jejich týmovou spolupráci a komunikaci. Je zde prostor pro prezentaci, reflexi a sebereflexi, což přispívá ke kvalitnímu učení a rozvoji žáků.

5.2.6 Společenskovědní vzdělávání: Třetí hodina

Třetí hodina společenskovědního vzdělávání dodržuje rámcově vzdělávací program pro obchodní akademie (obor vzdělávání 63–41–M/02) a konkrétně vychází ze vzdělávacího obsahu člověk jako občan. Rámcově vzdělávací program zde uvádí téma masových médií a jejich funkce, do kterého komunikace prostřednictvím sociální sítě jistě patří.

Tabulka 6 Společenskovědní vzdělávání: Třetí hodina

Škola	63–41–M/02 Obchodní akademie
Předmět	Společenskovědní vzdělávání
Vzdělávací obsah	Člověk jako občan
Průřezové téma	Mediální výchova
Téma vyučovací hodiny	Zásady bezpečné komunikace na sociálních sítích
Cíle hodiny	Žák vytvoří desatero zásad, jak správně komunikovat na sociálních sítích.
	Žák zdůvodní alespoň 3 zásady bezpečné komunikace na sociálních sítích.
	Žák vyjmenuje alespoň 5 zásad bezpečné komunikace na internetu.

Během hodiny se žáci seznámí se zásadami bezpečné komunikace na sociálních sítích a zopakují si dosavadní znalosti. Opakování probíhá pomocí kvízové hry Kahoot, při které si žáci připomenou důležité informace z minulých hodin. Následně pak žáci samostatně tvoří svá vlastní desatera pro bezpečnou komunikaci na internetu. Ta jsou pak zkontrolována pomocí aktivity na způsob hry Bingo. Hodina končí rekapitulací klíčových informací, hodnocením žáků a získáním jejich zpětné vazby. Celá hodina je strukturovaná a zahrnuje aktivizační prvky.

Průběh hodiny:

Hodina by měla být interaktivní a atraktivní pro žáky. Na začátku hodiny učitel třídu zklidní a získá si její pozornost, následně vytváří příjemnou atmosféru a prostřednictvím ice-breakingu se snaží naladit žáky na téma hodiny.

Následuje opakování minulé hodiny, během něhož učitel připomíná průběh předchozí vyučovací hodiny a témata, která byla divadelně inscenována. Žáci se zapojí do krátké aktivity ve dvojicích, v níž společně vymýšlejí odpovědi na otázky, které se týkají rizik na sociálních sítích. Práce ve dvojicích umožňuje žákům aktivně se podílet na opakování a připomenout si důležité informace z minulých hodin. Zároveň se tímto přístupem rozvíjí vzájemná komunikace žáků.

Poté je třída seznámena s průběhem hodiny. Kvízová hra Kahoot slouží k opakování klíčových znalostí týkajících se bezpečné komunikace na sociálních sítích, práce s hesly, zabezpečení zařízení a dat. Učitel moderuje hru a komentuje odpovědi třídy. Žák si zároveň takto ověří své dosavadní znalosti. Po kvízu vyučující opakuje klíčové znalosti, které zazněly během hry. Třída se aktivně podílí na opakování a ptá se na případné nejasnosti.

Následuje samostatná práce, během níž žáci vytvářejí vlastní desatero bezpečné komunikace na sociálních sítích. Vyučující jim při tomto procesu asistuje a kontroluje průběh aktivity. Žáci si zapisují své desatero, které je zároveň záznamem jejich práce.

Poté učitel prezentuje vlastní desatero a třída si kontroluje, zda to její obsahuje stejná pravidla, podobně jako u hry Bingo. Učitel komentuje odpovědi třídy a v případě, že se u žáka objeví smysluplná pravidla, která ve svém desateru vyučující nemá, žáka pochválí. Během fixace učitel opakuje nejčastěji zmiňovaná pravidla a žáci se aktivně podílejí na rekapitulaci a komentování jednotlivých pravidel.

Na konci hodiny jsou rekapitulovány důležité informace z hodiny, včetně jejího průběhu. Do závěrečného shrnutí a hodnocení hodiny se zapojují i žáci.

Věřím, že tato interaktivní hodina umožňuje žákům efektivně si zopakovat a zapamatovat důležité znalosti z oblasti bezpečné komunikace na sociálních sítích. Žáci se aktivně zapojují, získávají zpětnou vazbu a pracují samostatně, což přispívá k jejich vzdělávacímu procesu.

5.3 Reflexe

Celková reflexe průběhu připravených hodin je velmi pozitivní, nicméně si uvědomuji, že tato skutečnost může být ovlivněna tím, že všechny přípravy byly realizovány na škole, kde již osm měsíců učím a se žáky mám vybudovaný dobrý vztah.

U většiny hodin se mi podařilo dodržet plánovaný průběh hodiny. Mám pocit, že žáci během vyučovacích hodin získali dostatečné množství informací. Tím myslím, že bych do plánovaných hodin žádná další témata nepřidával, ani je neubíral. Hodiny byly po informačně vzdělávací stránce na dobré úrovni. Cíle hodin byly nastaveny adekvátně a podařilo se jich vždy dosáhnout alespoň u poloviny žáků.

Během realizace všech příprav byla v hodinách přátelská atmosféra. Velký vliv na hodinu mělo i zvolené téma. Bylo vidět, že žáky bezpečná komunikace v digitálním světě zajímá a že oceňují využitelnost těchto hodin v praxi. V průběhu hodin se mi opakovaně stávalo, že žáci sdíleli svoje osobní zkušenosti. Z této skutečnosti jsem měl dobrý pocit, především kvůli tomu, že mnozí žáci byli překvapeni, že se některý ze spolužáků dostal do podobné situace jako oni. Myslím si, že toto sdílení pomohlo prolomit pomyslnou bariéru ve třídách. To, podle mého názoru, povede k menšímu strachu říci si o pomoc u svých vrstevníků. Zároveň mě sdílené příběhy žáků utvrdily v tom, že mnou zvolené téma je pro žáky aktuální a důležité.

Žáci se aktivně zapojovali během všech hodin a jejich výstupy z jednotlivých aktivit byly smysluplně kreativní. Žáky kreativní činnosti, kterými byly příprava plakátu a desatera, hraní divadelní hry, ale i diskuse, bavily. Především však žáci ocenili aktivity, při kterých mohli tvořit na papír. Myslím si, že to bylo zapříčiněno tím, že na škole nevyučujeme žádný cíleně umělecky zaměřený předmět.

Za možné riziko, které jsem si při tvorbě těchto příprav neuvědomil, považuji sdílení zkušeností žáků. I přesto, že ho v rámci celkové reflexe považuji za kladné. Měl jsem v jeho průběhu značné obavy, že se některý ze žáků stal obětí útoku v digitálním světě a tato zkušenost v něm zanechala psychické problémy a sdílení podobného příběhu mu způsobí negativní emoce. Jsem rád, že taková situace v žádné třídě nenastala, nicméně při realizaci těchto příprav bych doporučil značnou opatrnost.

5.3.1 Informační a komunikační technologie: První hodina

Tato příprava byla realizována v první polovině roku 2023 na střední škole s maturitním oborem během hodiny informační a komunikační technologie v půlené třídě. Na hodině bylo 14 žáků.

Samotná příprava do hodiny byla retrospektivně upravena na základě realizované praxe. Původní verze obsahovala etapu, během které žáci prezentovali svoje vytvořené plakáty ještě během této hodiny. To se z časových důvodů nestihlo, a tak žáci prezentovali své výtvory na začátku příští hodiny. Myslím si, že kdybych místo flipchartového papíru použil papír o rozměrech A4, žáci by stihli zadané plakáty vytvořit, a dokonce je i odprezentovat. Nicméně se zároveň domnívám, že zmenšení formátu pracovní plochy by snížilo čitelnost plakátů a zároveň by to vzalo žákům prostor se dostatečně vyjádřit.

Začátek hodiny i naladění atmosféry proběhly úspěšně. Žáci vědí, že i když na jejich škole působím jako učitel, jsem stále studentem vysoké školy. Během ice-breakingu jsem je proto seznámil s tím, že tato hodina vznikla v rámci mé diplomové práce, která je zaměřená na bezpečnou komunikaci v digitálním světě. Během opakování (hra kufr) dávali všichni žáci pozor, nicméně se u prvního pojmu stalo, že ostatní žáci ze třídy napovídali. Pochválil jsem je a upozornil jsem je, že si jednotlivé pojmy spolu ještě projdeme. Poprosil jsem je také o to, aby dali prostor dobrovolníkům, kteří se přihlásili, a opakovali si s nimi pouze v duchu. Protože žáci byli touto aktivitou nadšeni, slíbil jsem jim, že pokud bude vhodná příležitost a ve třídě bude stále přátelská nálada, v budoucnu si ještě kufr na začátku hodiny zahrajeme.

Motivační fázi považuji za úspěšnou. Diskuse, která byla součástí motivační fáze, se však samostatně zúčastnili pouze čtyři žáci. Zbylé žáky jsem zapojil do diskuse tím, že jsem je vyvolal. Chtěl jsem do diskuse zapojit co nejvíce žáků z důvodu aktivizace. Ta se projevila během výkladu, při němž jsem pokládal žákům otevřené otázky, na které už samostatně odpovídali.

Klíčovou aktivitou byla tvorba plakátů o konkrétních sociálních sítích. Při rozdělování žáků do skupin podle toho, které sociální sítě používají, jsem zohlednil i jejich vzájemné vztahy. Žáci byli rozděleni do čtyř dvojic a dvou trojic. Všechny skupiny porozuměly zadání a pracovaly samostatně. Při obcházení skupin jsem se snažil žáky motivovat, aby nešetřili místem na flipchartovém papíru a aby plakát udělali dobře čitelný. Zároveň jsem skupinám připomínal, že je poté čeká i prezentace dané sociální sítě.

Obrázek 10 Žáci při tvorbě plakátů o konkrétních sociálních sítích během hodiny informačních a komunikačních technologií

Na hodině se mi líbila její atmosféra, během které nevznikl žádný konflikt. Zároveň jsem měl dobrý pocit z toho, že žáky tvorba plakátů bavila. Po formální stránce byla hodina plynulá a jednotlivé fáze hodiny na sebe přirozeně navazovaly. Zároveň jsem rád, že se mi podařilo naplnit cíle hodiny.

5.3.2 Informační a komunikační technologie: Druhá hodina

Tato příprava byla realizována v první polovině roku 2023 na střední škole s maturitním oborem během hodiny informační a komunikační technologie v půlené třídě. Na hodině bylo přítomno 15 žáků.

Začátek hodiny i naladění atmosféry proběhly úspěšně. Během ice-breakingu jsem žáky proto seznámil s tím, že tato hodina vznikla v rámci mé diplomové práce, která je zaměřená na bezpečnou komunikaci v digitálním světě.

Během motivace jsem zopakoval informace, které byly řečeny na minulé hodině. Byl jsem spokojen, že si žáci tyto poznatky pamatovali. Opakování probíhalo velmi plynule, nicméně si myslím, že je to zapříčiněné tématem, které je žákům blízké, a zároveň věřím, že žáci mají již poměrně dost zkušeností s populárními sociálními sítěmi.

V první části hodiny žáci ve skupinách prezentovali své vytvořené plakáty o různých sociálních sítích. Během prezentace se žáci střídali při představování jednotlivých flipchartů. Prezentace žáků se mně líbila a místy mě i pobavila. Většina

skupin prezentovala plakát a konkrétní sociální síť velmi seriózně, nicméně objevily se i skupinky, jež do své prezentace vložily i prvky recese, které však byly přijatelné. Když jsem si chtěl fotografovat jejich prezentaci, překvapilo mě, jak se někteří z nich styděli. Respektoval jsem jejich rozhodnutí a nefotografoval jsem je během prezentace. Nicméně jeden ze žáků využil této příležitosti a nabídl se, že se nechá vyfotografovat namísto svých spolužáků. Podle mého názoru tato situace ještě více posílila přátelskou atmosféru ve třídě.

Druhá část hodiny se věnovala práci s hesly. Během fáze diskuse (získávání zpětné vazby o dosavadních znalostech žáků) mě překvapilo, že žáci mají široké znalosti o správném používaní hesel, avšak ne všichni tyto znalosti aplikují do praxe. Není překvapivé, že žáky více bavila fáze aplikace, během které vymýšleli svá vlastní hesla, jež následně testovali na webu https://www.passwordmonster.com, než expozice, při které se dozvěděli teoretická pravidla o správném používání hesel. Aktivita, během které žáci vymýšleli hesla, se mi ze začátku velmi líbila, žáci tvořili hesla, která byla zpravidla algoritmická, a tedy odvoditelná. Po chvilce však začali někteří žáci mezi sebou soupeřit, kdo vymyslí komplikovanější heslo na dešifrování, avšak nebrali už v potaz nutnost nějak si dané heslo odvodit či zapamatovat.

Obrázek *11* Žáci během prezentace vlastních plakátů o konkrétních sociálních sítích během hodiny informačních a komunikačních technologií

Během opakování nevznikla žádná nestandardní situace. Žáci aktivně a smysluplně odpovídali na otázky k tématu hodiny. Na hodině se mi líbila její atmosféra, během které nevznikl žádný konflikt. Zároveň jsem měl dobrý pocit z nadšení některých žáků z tématu bezpečná práce s hesly. Po formální stránce byla hodina tematicky plynulá a jednotlivé fáze hodiny na sebe přirozeně navazovaly. Zároveň jsem rád, že se mi podařilo naplnit cíle hodiny.

5.3.3 Informační a komunikační technologie: Třetí hodina

Tato příprava byla realizována v první polovině roku 2023 na střední škole s maturitním oborem během hodiny informační a komunikační technologie v půlené třídě. Na hodině bylo přítomno 15 žáků.

Začátek hodiny i naladění atmosféry proběhly úspěšně. Žáci byli také informováni o tom, že hodina je součástí mé diplomové práce. Opakování minulé hodiny probíhalo tak, že jsem žákům pokládal otázky související s předchozí hodinou a žáci na ně odpovídali. Touto metodou opakování jsem si, podle mého názoru, ještě více získal pozornost žáků.

Hlavní náplní této hodiny bylo seznámení žáků s konkrétními způsoby kybernetických útoků. K tomu byla využita metoda výkladu s prvky diskuse. Výklad některých témat jsem doplnil o video, které s tématem souviselo a názorně demonstrovalo danou problematiku. Videa byla vhodně zvolena, byla dostatečně krátká a zároveň výstižná. V průběhu výkladu a pouštění videí byl ve třídě klid. Během diskuse žáci vzájemně sdíleli své vlastní zkušenosti s online hrozbami a současně spolu sdíleli různé postupy, které mohou pomoci při řešení těchto situací nebo při jejich prevenci. To se mi velmi líbilo.

Většinu žáků nejvíce oslovilo video o kybergroomingu. Je to hrané video z českého prostředí inspirované skutečnou událostí. Až budu příště učit další hodinu s podporou této přípravy, opět budu prezentovat jednotlivé hrozby v stejném pořadí. Pořadí jednotlivých rizik mi připadá smysluplné, především díky tomu, že poslední hrozbou je kybergrooming, jehož výklad je doplněn o velmi realistické video, které svým zpracováním pomohlo zdůraznit důležitost tématu této hodiny.

V hodině se mi podařilo vytvořit atmosféru založenou na dvou pocitech: bezpečí a ohroženosti. V žácích jsem vyvolal pocit ohrožení, že případná neznalost způsobů sociotechnických metod útočníků v digitálním světě může negativně ovlivnit jejich život. A zároveň jsem vytvořil bezpečný prostor pro komunikaci na toto téma. Po formální stránce byl dodržen plánovaný průběh hodiny. Zároveň jsem rád, že se mi podařilo naplnit cíle hodiny.

5.3.4 Společenskovědní vzdělávání: První hodina

Tato příprava byla realizována v první polovině roku 2023 na střední škole s maturitním oborem během hodiny společenskovědního základu v celé třídě. Na hodině bylo přítomno 27 žáků.

Začátek hodiny a navození atmosféry byly zdařilé. Během ice-breakingu jsem proto žáky seznámil s faktem, že tato hodina vznikla v rámci mé diplomové práce, která je zaměřená na bezpečnou komunikaci v digitálním světě.

Během opakovací metody „deset slov“ žáci vytvořili smysluplné věty přesně o deseti slovech, které se týkaly učiva minulé hodiny, následně tyto věty sdíleli se spolužákem v lavici. Čtyři žáci se dobrovolně přihlásili, že přednesou své věty před zbytkem třídy.

Použití příběhu „O Elišce“ v motivační fázi považuji za vhodně zvolené, žáci dávali pozor a aktivně se účastnili následné diskuse. Z diskuse vzešlo mnoho různých názorů, takže jsem musel improvizovat a příběh obohatit o detaily. Myslím si, že v praxi je dobré v podobných situacích improvizovat z důvodu, že někteří žáci rádi slovíčkaří a prostor pro improvizaci učiteli dává možnost obrátit žáky správným směrem. Někteří žáci hledali v příběhu kličky a snažili se rizikové chování Elišky zlehčit, což bylo opakem toho, čeho jsem se snažil docílit. Chtěl jsem, aby si žáci uvědomili zodpovědnost za své chování v digitálním světě, a to se mi povedlo.

Aktivita, při které žáci tvořili ve skupinách plakáty na témata sdílení osobních údajů, kyberšikana, phishingové a vishingové útoky, sexting, probíhala v přátelské atmosféře. Třída byla rozdělena do čtyř skupin a každá skupina zpracovávala jedno téma. Ze začátku jsem si myslel, že skupiny jsou poměrně velké, nicméně v praxi se ukázalo, že počet žáků je ideální. Ve skupině si žáci rozdělili role a každý člen se aktivně podílel na výstupu skupiny. Někteří se zaměřili na tvorbu plakátu, jiní hledali potřebné informace a ostatní si připravovali projev k prezentaci.

Obrázek *12* Žáci při tvorbě plakátů o konkrétních rizicích sociálních sítí během hodiny společenskovědního vzdělávání

tak, jak byla připravena, a podařilo se mi naplnit cíl hodiny alespoň u poloviny žáků.

5.3.5 Společenskovědní vzdělávání: Druhá hodina

Tato příprava byla realizována v první polovině roku 2023 na střední škole s maturitním oborem během hodiny společenskovědního vzdělávání v celé třídě. Na hodině bylo přítomno 29 žáků.

Na začátku hodiny se mi podařilo vytvořit příjemnou atmosféru. Během ice-breakingu jsem žáky informoval, že tato hodina vznikla v rámci mé diplomové práce, která se zaměřuje na bezpečnou komunikaci v digitálním světě.

V první části hodiny žáci ve skupinách prezentovali své vytvořené plakáty o rizicích na sociálních sítích. Během prezentace se žáci střídali při představování jednotlivých flipchartů. V průběhu prezentací se žáci spontánně začali ptát prezentující skupiny na informace, které je k tématu zajímaly. To se mi velmi líbilo.

Když jsem se zeptal žáků, zda si je můžu fotografovat v průběhu prezentace, všechny skupiny mi oznámily, že by jim to bylo nepříjemné. To jsem respektoval.

Obrázek *13* Plakáty konkrétních rizik sociálních sítí vytvořené žáky během hodiny společenskovědního vzdělávání

Žáci se poté rozdělili do skupin podle vlastního výběru, vzniklo pět skupin po čtyřech žácích a tři skupiny po třech žácích. Každá skupina dostala zadánu odlišnou divadelní hru. Zadané hry vznikly s pomocí umělé inteligence od společnosti OpenAI. Poté, co umělá inteligence vymyslela jednotlivá představení, upravil jsem je ještě tak, aby byla gramaticky a pedagogicky použitelná ve výuce. Žáci byli s touto skutečností seznámeni. Měli zadáno, aby divadelní hry upravili podle sebe, mohli změnit děj, jména či dialogy s podmínkou, že dodrží téma bezpečná komunikace v digitálním světě a upravená verze hry nebude obsahovat vulgarismy ani žádné druhy zesměšňování.

Během příprav svých výstupů pracovaly skupiny zodpovědně a nesnažily se vyučovací hodinu sabotovat. Dále se mi líbila empatie při rozdělování rolí v divadelních hrách. Pokud byl žák stydlivý, spolužáci ho nenutili k vystoupení během divadelní inscenace.

Při realizaci krátkého divadelního vystoupení vzniklo několik vtipných momentů, které podpořily již tak dobrou atmosféru ve třídě. Líbilo se mi, že většina skupin využila volnost, kterou tato metoda nabízela, a za stanovený čas vymyslela i provizorní rekvizity. Během jednotlivých vystoupení se smáli žáci jak v pozici herců, tak diváků, nicméně nikdy se nejednalo o posmívání. Z hodiny si odnáším osobní motivaci k většímu zapojení podobných inscenačních metod do výuky.

Na hodině se mi líbila její tvořivá atmosféra, během které nevznikl žádný konflikt, a zároveň se mi líbila práce žáků ve skupinách. Po formální stránce proběhla hodina tak, jak byla připravena, a podařilo se mi naplnit cíl hodiny alespoň u poloviny žáků.

5.3.6 Společenskovědní vzdělávání: Třetí hodina

Tato příprava byla realizována v první polovině roku 2023 na střední škole s maturitním oborem během hodiny společenskovědního vzdělávání v celé třídě. Na hodině bylo přítomno 26 žáků.

Začátek hodiny i naladění atmosféry proběhly úspěšně. Žáci věděli, že jsem stále studentem vysoké školy, i když na škole působím jako učitel. Během ice-breakingu jsem je proto seznámil s tím, že tato hodina vznikla v rámci mé diplomové práce, která je zaměřená na bezpečnou komunikaci v digitálním světě.

Během opakování minulé hodiny jsem připomenul divadelní hry, které žáci hráli. Zároveň jsem chtěl po žácích, aby připomněli klíčové zápletky svých vystoupení a ponaučení, která z nich měla vyplynout.

Abych se ještě více ujistil o úrovni znalostí žáků, zahrál jsem si s nimi Kahoot na téma bezpečná komunikace v digitálním světě. Během Kahootu se cyklicky opakovaly fáze ruchu a ticha. Ruch nastal vždy, když se objevila správná odpověď a žákům se zobrazil žebříček prvních pěti hráčů, oproti tomu ticho zavládlo v okamžicích, kdy žáci odpovídali na otázky. Žákům se Kahoot líbil a měl jsem radost, že se většina z nich snažila až do konce.

Obrázek *14* Žáci přihlašující se do aplikace Kahoot během hodiny společenskovědního vzdělávání

Poté žáci pracovali na své samostatné práci, během které si měli připravit vlastní desatero pro bezpečnou komunikaci v digitálním světě. Žáci měli desatero tvořit samostatně, nicméně občas jsem zahlédl, že se radí se spolužákem. Na to jsem zpravidla nereagoval. Tito žáci spolu komunikovali potichu a nerušili své spolužáky. Během práce na desateru jsem chtěl v žácích rozvinout samostatné a kritické myšlení, což se mi, myslím, podařilo.

Během kontroly vytvořeného desatera pomocí hry Bingo vznikl ve třídě mírný ruch, nicméně nepůsobil zásadně rušivě. Žáci s unikátní odpovědí dostali prostor říci své pravidlo a následně ho obhájit. Všichni žáci takto prezentovali smysluplné nápady, a tak jsem je za to pochválil. Některé z nápadů se sice neshodovaly s mým desaterem, ale shodovaly se s desaterem ostatních spolužáků.

Na hodině jsem se přesvědčil o tom, že žáci umí pracovat samostatně. Během hodiny byla příjemná atmosféra a žáci se aktivně podíleli na jejím průběhu. Po formální stránce proběhla hodina tak, jak byla připravena, a podařilo se mi naplnit cíl hodiny alespoň u poloviny žáků.

6 Výzkum

6.1 Výzkumný problém

Rozvoj internetu a široké využívání sociálních sítí změnily způsob komunikace mezi lidmi a ovlivnily jedince všech věkových skupin. Zejména pak děti a dospívající, kteří vyrůstali v kontaktu s digitálními technologiemi a používají tyto platformy jako prostředek pro navazování kontaktů s vrstevníky, pro sebevyjádření a trávení volného času. Vedle četných výhod a možností, které online svět nabízí, však existuje i řada rizik a nebezpečí, která je třeba důkladně prozkoumat a pochopit [1].

Prostřednictvím tohoto výzkumu se diplomová práce snaží rozšířit stávající soubor poznatků o rizicích a nebezpečích, kterým mladiství ve věku 15 až 20 let čelí na internetu a sociálních sítích. Pochopením příčin, které k těmto rizikům přispívají, může pomoci vyvinout strategie, jež dospívajícím usnadní bezpečný a zodpovědný pohyb v digitálním prostředí. Navíc mohou být výsledky výzkumu využity jako cenný pedagogický materiál pro učitele na středních školách.

6.2 Cíle výzkumu

Hlavním cílem výzkumu je prozkoumat a analyzovat chování mladistvých ve věku 15–20 let na internetu a sociálních sítích.

6.3 Metodologie výzkumu

Výzkum bude kvantitativní. Sběr dat bude realizován formou nestandardizovaného dotazníkového šetření vlastní konstrukce (viz příloha A)., Otázky dotazníkového šetření budou zjišťovat, jak mladiství používají sociální sítě, jak se chovají při sdílení informací na těchto platformách a s kterými online riziky se setkávají. Vyhodnocení výzkumu bude provedeno formou popisné statistiky s následnou diskusí. Výsledky výzkumu pomohou odhalit vzájemné souvislosti a získat tak cenné poznatky o online rizicích, kterým děti a dospívající čelí.

6.4 Realizace výzkumu a jeho vyhodnocení

Během výzkumu byla realizována dvě dotazníková šetření se stejnými otázkami. Obě šetření probíhala v období od září 2021 do června 2023 pomocí platformy Google Forms. První dotazníkové šetření bylo zadáno osobně autorem diplomové práce v různých ročnících Obchodní akademie a Jazykové školy Pardubice a zúčastnilo se ho celkem 205 respondentů. Druhé dotazníkové šetření bylo sdíleno na platformě Facebook (v komunitách hráčů počítačových her) a zúčastnilo se ho 764 respondentů. Celkem se dotazníkových šetření zúčastnilo 969 studentů. Obě šetření probíhala anonymně. Vzorek respondentů byl tříděn dle pohlaví.

Charakteristika zkoumaného vzorku

Tabulka 7 První dotazníkové šetření – Osobní sběr dat

První dotazníkové šetření								
Věk	15-16 let		17–18 let		19–20 let		Celkem	
Pohlaví							205	100 %
Chlapci	47	22,93 %	34	16,58 %	6	2,93 %	87	42,44 %
Dívky	54	26,34 %	61	29,76 %	3	1,46 %	118	57,56 %

Z dotazovaného vzorku patří 101 respondentů (49,27 %) do věkové kategorie 15-16 let, 95 respondentů (46,34 %) do věkové kategorie 17–18 let a 9 respondentů (4,39 %) do věkové kategorie 19-20 let.

Tabulka 8 Druhé dotazníkové šetření – Online sběr dat

Druhé dotazníkové šetření								
Věk	15-16 let		17–18 let		19–20 let		Celkem	
Pohlaví							764	100 %
Chlapci	163	21,34 %	172	22,51 %	139	18,19 %	474	62,04 %
Dívky	151	19,77 %	68	8,90 %	71	9,29 %	290	37,96 %

Z dotazovaného vzorku patří 314 respondentů (41,11 %) do věkové kategorie 15-16 let, 240 respondentů (31,41 %) do věkové kategorie 17–18 let a 210 respondentů (27,48 %) do věkové kategorie 19-20 let.

Tabulka 9 Souhrn obou šetření

Souhrn obou šetření								
Věk	15-16 let		17–18 let		19–20 let		Celkem	
Pohlaví							969	100 %
Chlapci	210	21,67 %	206	21,26 %	145	14,96 %	561	57,89 %
Dívky	205	21,16 %	129	13,31 %	74	7,64 %	408	42,11 %

Celkem bylo dotazovaných 969 respondentů. Z toho patří 415 respondentů (42,83 %) do věkové kategorie 15-16 let, 335 respondentů (34,57 %) do věkové kategorie 17–18 let a 219 respondentů (22,60 %) do věkové kategorie 19-20 let.

Otázka č. 3: Víte, co jsou to sociální sítě?

Tabulka 10 Víte, co jsou to sociální sítě?

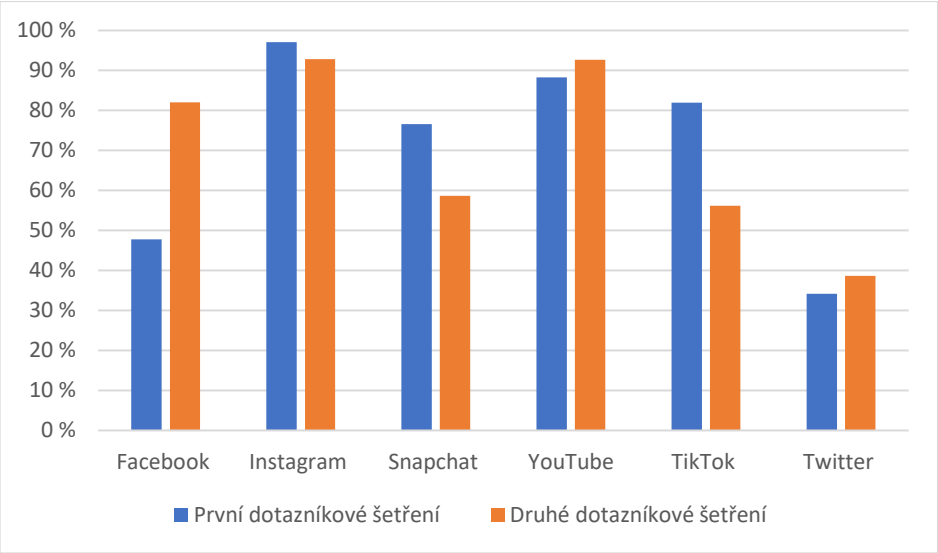
	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano	204	99,51 %	758	99,21 %	962	99,28 %
Ne	1	0,49 %	6	0,79 %	7	0,72 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %

Z podrobnějšího prozkoumání dotazníků od respondentů, kteří odpověděli „ne“, vyplývá, že touto odpovědí chtěli vyjádřit svůj nezájem o sociální sítě nebo zdůraznit, že je nepoužívají – což je případ dívky ve věku 19-20 let z druhého dotazníkového šetření. V případě jednoho z chlapců ve věku 15-16 let lze ze zbytku vyplněného dotazníku usuzovat, že zjevně ví, co jsou to sociální sítě, a může se tak jednat o chybu. Minimálně jeden další respondent (chlapec ve věku 17-18 let) patrně dotazník vyplnil neupřímně vzhledem k jeho odpovědi „prodej drog“ na otázku číslo č. 8. Na základě výzkumu nelze jednoznačně prohlásit, že úplně všichni respondenti ve věku 15-20 let znají sociální sítě, drtivá většina je ale zná.

Otázka č. 4: Které sociální sítě používáte?

Tabulka 11 Které sociální sítě používáte?

	První dotazníkové šetření		Druhé dotazníkové šetření		Sjednocené šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Facebook	98	47,80 %	627	82,07 %	725	74,82 %
Instagram	199	97,07 %	709	92,80 %	908	93,70 %
Snapchat	157	76,59 %	448	58,64 %	605	62,44 %
YouTube	181	88,29 %	708	92,67 %	889	91,74 %
TikTok	168	81,95 %	429	56,15 %	597	61,61 %
Twitter	70	34,15 %	295	38,61 %	365	37,67 %



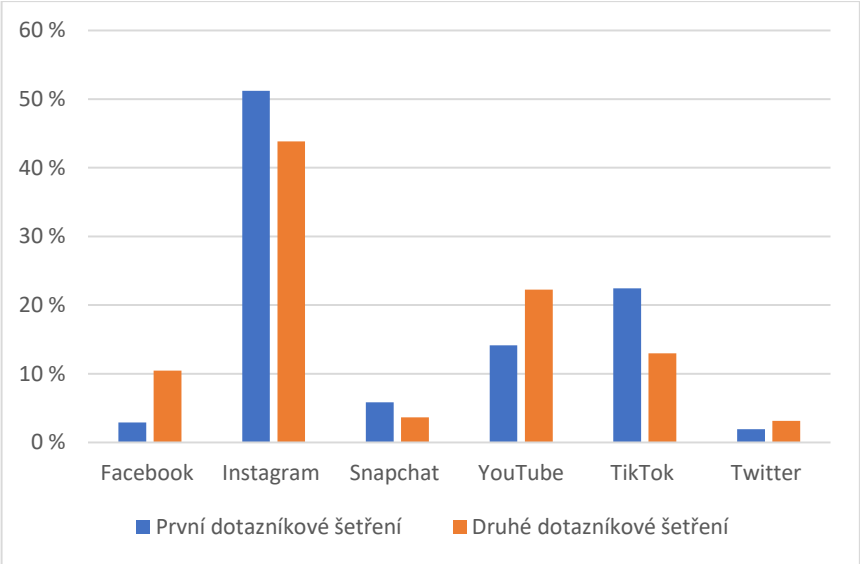
Graf 1 Které sociální sítě používáte?

Otázka je zaměřena na prostý výčet používaných sociálních sítí, to znamená, že respondenti nerozlišovali jejich subjektivní oblíbenost. Relativně vysoký rozdíl v míře používání Facebooku ve výsledcích výzkumů je dán rozdílnými vzorky respondentů, kdy druhé šetření probíhalo převážně prostřednictvím této sociální sítě. Nejvíce používané sociální sítě jsou Instagram (908 respondentů z 969) a YouTube (889 respondentů z 969). Nejméně se používá Twitter (365 respondentů z 969).

Otázka č. 5: Kterou sociální síť používáte nejčastěji?

Tabulka 12 Kterou sociální síť používáte nejčastěji?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Facebook	6	2,93 %	80	10,47 %	86	8,87 %
Instagram	105	51,22 %	335	43,85 %	440	45,41 %
Snapchat	12	5,85 %	28	3,66 %	40	4,13 %
YouTube	29	14,15 %	170	22,25 %	199	20,54 %
TikTok	46	22,44 %	99	12,96 %	145	14,96 %
Twitter	4	1,95 %	24	3,14 %	28	2,89 %
Ostatní	3	1,46 %	28	3,67 %	31	3,20 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %



Graf 2 Kterou sociální síť používáte nejčastěji?

Povaha otázky umožňovala vybrat právě jednu odpověď. Kromě zde uvedených šesti možností byly na výběr ještě sociální sítě Discord, Twitch, Reddit, případně „jiné“. Tyto však měly pouze zanedbatelný počet odpovědí, a proto nejsou v grafu zastoupeny. Nejčastěji používanou sítí je Instagram (440 respondentů z 969). Zajímavé je sledovat pozvolný vzestup TikToku. Tento fakt je dobře patrný při porovnání s výzkumem v rámci bakalářské práce Veroniky Jordánové [46], který byl uskutečněn v roce 2019 a kde o TikToku ještě není ani zmínka, protože se v Evropě začal masově šířit až na přelomu let 2019 a 2020 [47].

Otázka č. 6: Používáte telefon/tablet k připojení na sociální sítě?

Tabulka 13 Používáte telefon/tablet k připojení na sociální sítě?

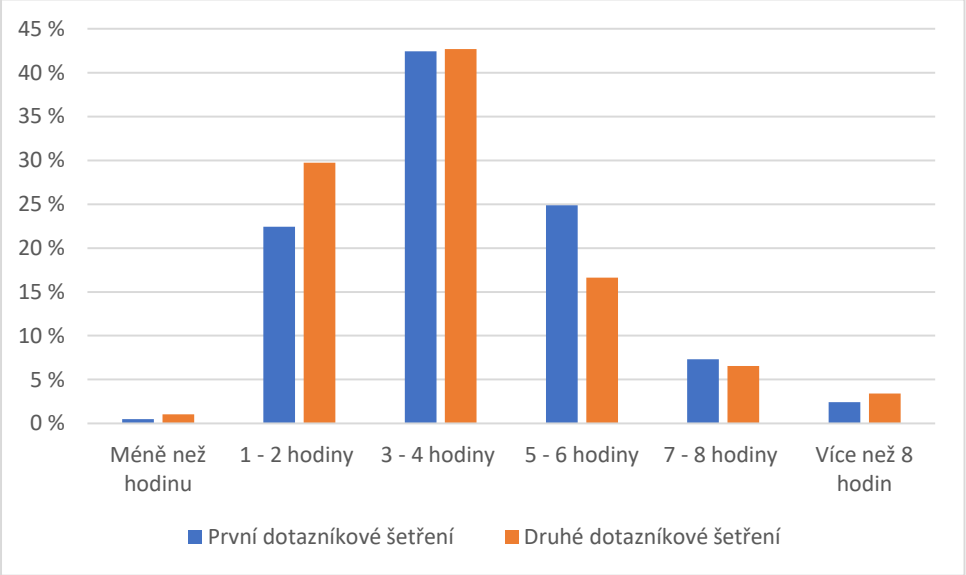
	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano	205	100,00 %	759	99,35 %	964	99,48 %
Ne	0	0,00 %	5	0,65 %	5	0,52 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %

Otázka měla za cíl zjistit, zda mladí lidé mají téměř neomezený přístup k sociálním sítím. Téměř všichni oslovení, konkrétně 99,48 % z nich, používají telefon nebo tablet k připojení na tyto platformy.

Otázka č. 7: Kolik hodin přibližně denně strávíte na sociálních sítích?

Tabulka 14 Kolik hodin přibližně denně strávíte na sociálních sítích?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Méně než hodinu	1	0,49 %	8	1,05 %	9	0,93 %
1–2 hodiny	46	22,44 %	227	29,72 %	273	28,17 %
3–4 hodiny	87	42,44 %	326	42,67 %	413	42,62 %
5–6 hodiny	51	24,88 %	127	16,62 %	178	18,37 %
7–8 hodiny	15	7,31 %	50	6,54 %	65	6,71 %
Více než 8 hodin	5	2,44 %	26	3,40 %	31	3,20 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %



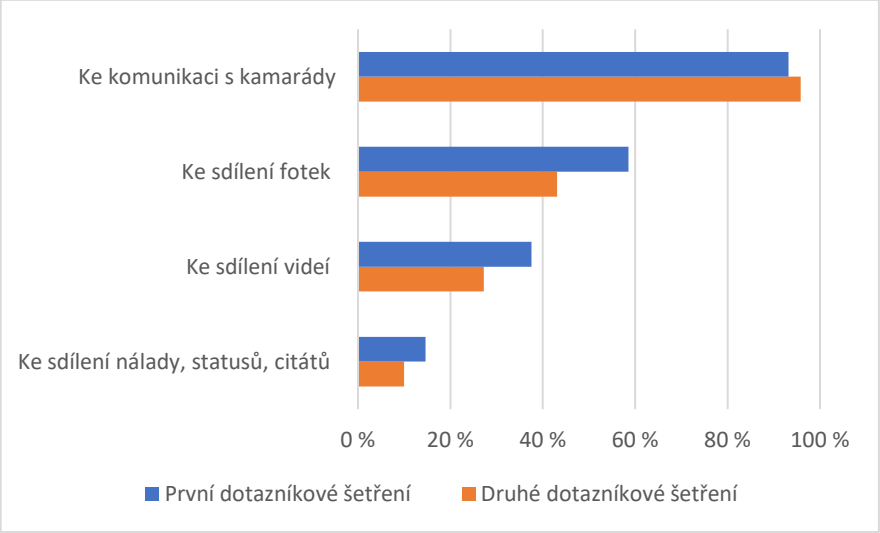
Graf 3 Kolik hodin přibližně denně strávíte na sociálních sítích?

Ačkoliv nelze bez dalšího výzkumu a statistické analýzy učinit jednoznačný závěr, že s přibývajícím časem stráveným na sociálních sítích se zvyšuje pravděpodobnost rizikového chování, studie provedené na podobném vzorku respondentů ukazují na zvyšující se riziko internalizujících poruch chování, jako jsou deprese a úzkosti [48]. Z tohoto pohledu jsou poměrně závažná dvě zjištění. Za prvé, že v průměru okolo jedné čtvrtiny respondentů tráví na sociálních sítích více než 5 hodin denně, a za druhé, že odpověď s nejvyšší četností je 3-4 hodiny denně, tu vybralo 87 respondentů prvního dotazníku, resp. 326 druhého. Naprosté minimum respondentů pak na sociálních sítích tráví méně času než hodinu denně.

Otázka č. 8: K čemu sociální sítě používáte?

Tabulka 15 K čemu sociální sítě používáte?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ke komunikaci s kamarády	191	93,17 %	732	95,81 %	923	95,25 %
Ke sdílení fotek	120	58,54 %	329	43,06 %	449	46,34 %
Ke sdílení videí	77	37,56 %	208	27,23 %	285	29,41 %
Ke sdílení nálady, statusů, citátů	30	14,63 %	76	9,95 %	106	10,94 %



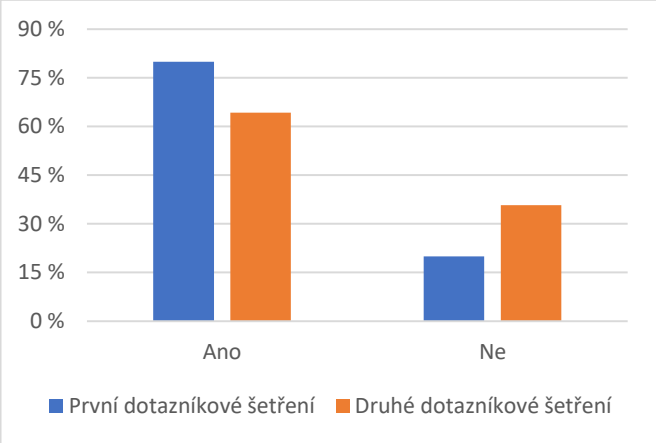
Graf 4 K čemu sociální sítě používáte?

Tato otázka umožňovala výběr z vícero připravených odpovědí, přičemž respondenti mohli zároveň zadat i svou vlastní odpověď. Této možnosti využila pouze menšina dotázaných, proto nejsou jejich odpovědi reprezentovány v grafech výše. Zatímco nabízené možnosti se kromě komunikace s přáteli zaměřovaly spíše na tvorbu a sdílení obsahu, většina vlastních odpovědí respondentů souvisela naopak s konzumací obsahu, např. sledování videí, memů, fotek apod. Několik starších respondentů zmínilo použití za účelem výdělečné činnosti, jednou z odpovědí byl „marketing“ a druhou „správa Instagramové stránky“. Drtivá většina (923 respondentů z 969) používá sociální sítě ke komunikaci s kamarády, což je konzistentní s výzkumem Veroniky Jordánové [46].

Otázka č. 9: Pokud používáte Facebook/Instagram/Snapchat, využíváte možnosti stories? Zveřejněné fotky či videa, které po 24 hodinách „zmizí“.

Tabulka 16 Pokud používáte Facebook/Instagram/Snapchat, využíváte možnosti stories? Zveřejněné fotky či videa, které po 24 hodinách „zmizí“.

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano	164	80,00 %	491	64,27 %	655	67,60 %
Ne	41	20,00 %	273	35,73 %	314	32,40 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %



Graf 5 Pokud používáte Facebook/Instagram/Snapchat, využíváte možnosti stories? Zveřejněné fotky či videa, které po 24 hodinách „zmizí“.

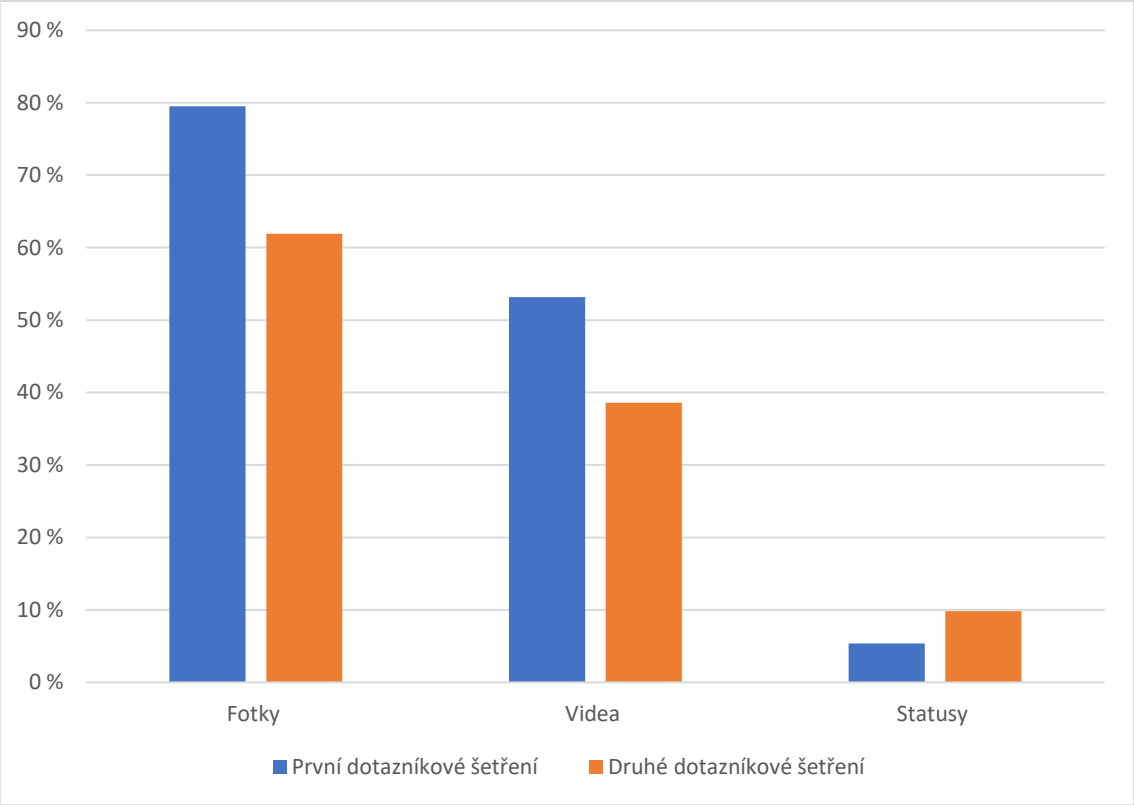
Sociální sítě umožňují různé způsoby sdílení médií, které mají různý potenciál pro případné rizikové chování. Instagram stories umožňuje zveřejnění fotek, videí a jiného obsahu na 24 hodin širokému okruhu sledujících i nesledujících profilů, přičemž dosah lze upravovat a omezovat pomocí nastavení soukromí. Snapchat nabízí podobnou funkcionalitu, ovšem jeho podstata tkví převážně ve sdílení krátkodobého obsahu, který po zobrazení zmizí. Dle studie [49] uveřejněné v International Journal of Environmental Research and Public Health jsou uživatelé Snapchatu v porovnání s ostatními sociálními sítěmi nejčastěji vystaveni kyberšikaně.

Z výsledků obou dotazníkových šetření vyplývá, že neexistuje žádný zjevný meziskupinový trend ve využívání této funkcionality. Nedá se tedy učinit závěr, že by např. mladší respondenti využívali stories více než starší. Z dat je ovšem patrné, že napříč všemi skupinami respondentů sdílejí stories více dívky než chlapci, a to v průměru o 23,17 procentního bodu v případě prvního dotazníkového šetření (66,66 % vs. 89,83 %) a 24,25 procentního bodu v případě druhého šetření (55,06 % vs. 79,31 %).

Otázka č. 10: Jaký obsah sdílíte ve stories?

Tabulka 17 Jaký obsah sdílíte ve stories?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Fotky	163	99,39 %	473	96,33 %	636	97,10 %
Videa	109	66,46 %	295	60,08 %	404	61,68 %
Statusy	11	5,70 %	75	15,27 %	86	13,13 %



Graf 6 Jaký obsah sdílíte ve stories?

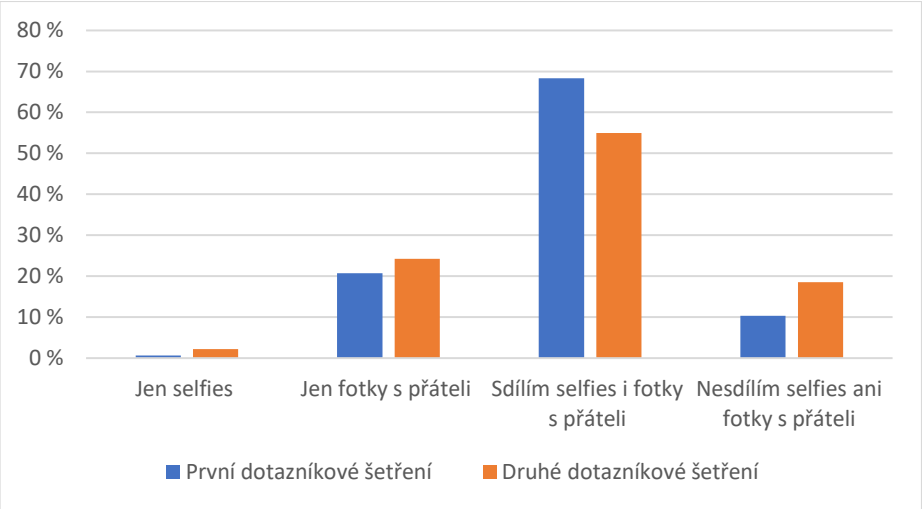
Otázka byla položena pouze respondentům, kteří na předchozí otázku odpověděli kladně. Výsledky odpovědí na tuto otázku jsou konzistentní s výsledky otázky č. 8, kdy pořadí sdílených médií je shodné v posloupnosti fotky, videa a statusy. Sdílený obsah také odpovídá oblíbenosti jednotlivých sociálních sítí, mezi kterými převládají zejména ty, jejichž smyslem je sdílení vizuálního obsahu. To ukazuje na vnitřní konzistenci dat získaných při dotazníkovém šetření.

Respondenti měli jako u jiných otázek možnost zadání své vlastní odpovědi, v té se objevovaly zejména tzv. memes, ale také hudba, kresby, politika a jiné.

Otázka č. 11: Sdílíte ve stories své selfies nebo fotky s přáteli?

Tabulka 18 Sdílíte ve stories své selfies nebo fotky s přáteli?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Jen selfies	1	0,61 %	11	2,24 %	12	1,83 %
Jen fotky s přáteli	34	20,73 %	119	24,24 %	153	23,36 %
Sdílím selfies i fotky s přáteli	112	68,29 %	270	54,99 %	382	58,32 %
Nesdílím selfies ani fotky s přáteli	17	10,37 %	91	18,53 %	108	16,49 %
Celkem	164	100,00 %	491	100,00 %	655	100,00 %



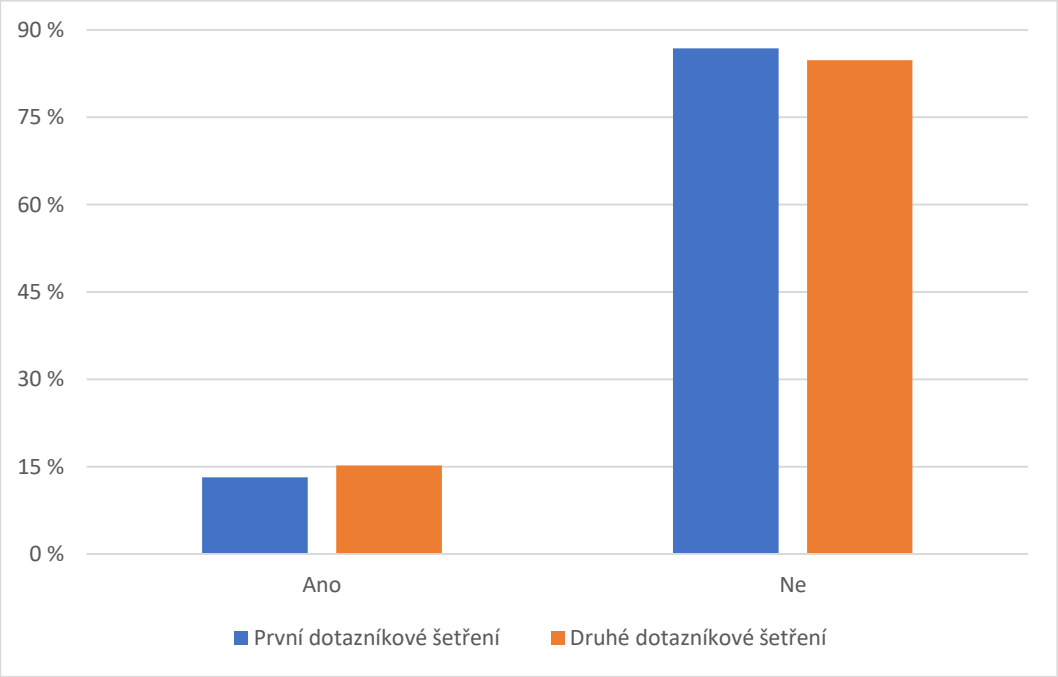
Graf 7 Sdílíte ve stories své selfies nebo fotky s přáteli?

Otázka byla položena pouze těm respondentům, kteří pozitivně odpověděli na otázku č. 10. V prvním šetření odpovědělo celkem 71,71 % ze všech dotázaných, že sdílí své fotografie ve stories, zatímco ve druhém šetření takto odpovědělo 52,36 % ze všech dotázaných. Pokud sloučíme odpovědi všech respondentů z obou šetření, zjistíme, že celkově 56,45 % dotázaných sdílí své snímky ve stories. Přitom podobně jako u jiných otázek na sdílení obsahu i zde je poměrně značný rozdíl mezi chlapci a dívkami, kdy dívky mnohem častěji odpovídají, že sdílí jak selfie, tak fotky s přáteli. Chlapci častěji odpovídali, že sdílí pouze fotky s přáteli.

Otázka č. 12: Sdílíte své konkrétní informace? Bydliště, školu, kterou navštěvujete, svoji rodinu.

Tabulka 19 Sdílíte své konkrétní informace? Bydliště, školu, kterou navštěvujete, svoji rodinu.

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano	27	13,17 %	116	15,18 %	143	14,76 %
Ne	178	86,83 %	648	84,82 %	826	85,24 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %



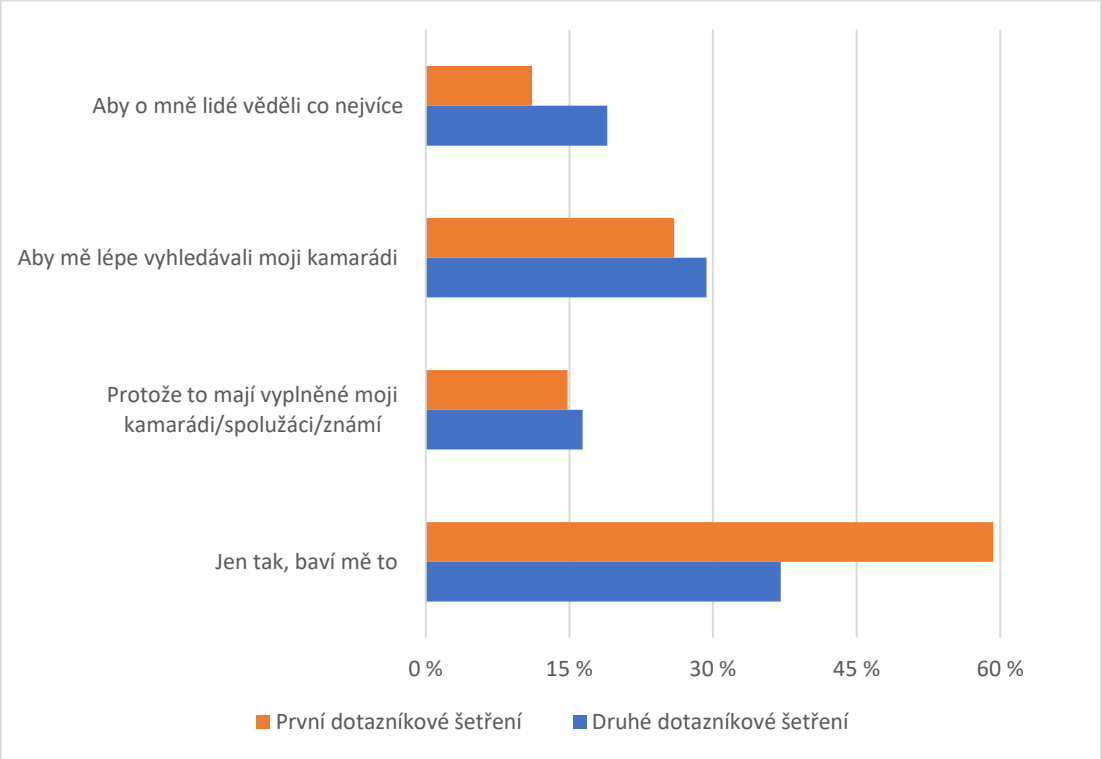
Graf 8 Sdílíte své konkrétní informace? Bydliště, školu, kterou navštěvujete, svoji rodinu.

V této části se dotazník zaměřuje již na šetření konkrétního případu rizikového chování, kterým je sdílení osobních informací na sociálních sítích. Překvapující je fakt, že trend sdílení osobních informací je spíše stoupající směrem ke starším respondentům, kteří by měli být spíše schopni vyhodnotit dopady svého chování na internetu. Důvody sdílení osobních informací jsou předmětem následující otázky.

Otázka č. 13: Proč sdílíte své konkrétní informace?

Tabulka 20 Proč sdílíte své konkrétní informace?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Aby o mně lidé věděli co nejvíce	3	11,11 %	22	18,97 %	25	17,48 %
Aby mě lépe vyhledávali moji kamarádi	7	25,93 %	34	29,31 %	41	28,67 %
Protože to mají vypl-něné moji kamarádi/ spolužáci/ známí	4	14,81 %	19	16,38 %	23	16,08 %
Jen tak, baví mě to	16	59,26 %	43	37,07 %	59	41,26 %



Graf

Graf 9 Proč sdílíte své konkrétní informace?

Otázka byla položena pouze respondentům, kteří kladně odpověděli na předchozí otázku č. 12. Z toho důvodu je soubor respondentů, zejména v prvním šetření, relativně omezený, a tudíž prezentovaná data mohou být zkreslena. Dále bylo v rámci otázky umožněno, aby účastníci označili více než jednu správnou odpověď nebo napsali vlastní odpověď. Nejčastější odpověď „jen tak, baví mě to“ naznačuje jistou lehkovážnost související s dotazovaným chováním.

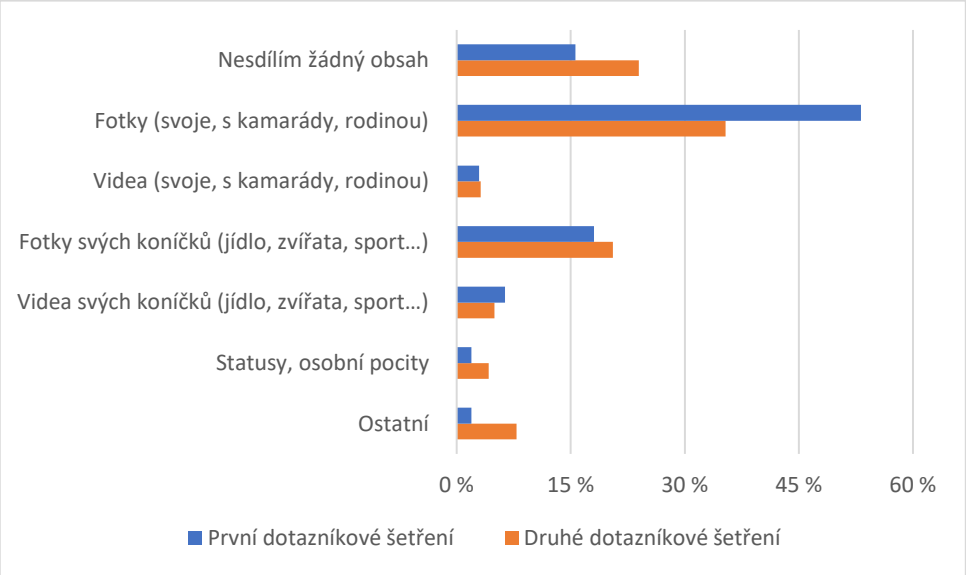
Otázka č. 14: Jaký obsah sdílíte na sociálních sítích?

V rámci této otevřené otázky nebyly respondentům nabídnuty žádné připravené možnosti, a proto je její grafické zobrazení nebo statistické vyhodnocení obtížné. Při detailnějším prozkoumání odpovědí jde o různé konkrétní příklady obsahu s četností zhruba podobnou jako v odpovědi na otázku č. 11, tzn. respondenti často zmiňují sdílení fotek s nějakým konkrétnějším tématem. U chlapců jsou častými odpověďmi sportovní aktivity, sport obecně, fotbal, florbal, hokej, případně jiné volnočasové záliby. Častou odpovědí je i „nic“ nebo „žádný“. U dívek je častou odpovědí „fotky s přáteli“, což odpovídá vysoké četnosti této odpovědi v otázce č. 11. Kromě toho jsou častou odpovědí fotky a videa zvířat, osobní život, případně cestování a zážitky.

Otázka č. 15: Jaký obsah nejvíce sdílíte na sociálních sítích?

Tabulka 21 Jaký obsah nejvíce sdílíte na sociálních sítích?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Nesdílím žádný obsah	32	15,61 %	183	23,96 %	215	22,19 %
Fotky (svoje, s kamarády, rodinou)	109	53,17 %	270	35,34 %	379	39,11 %
Videa (svoje, s kamarády, rodinou)	6	2,93 %	24	3,14 %	30	3,10 %
Fotky svých koníčků (jídlo, zvířata, sport…)	37	18,05 %	157	20,55 %	194	20,02 %
Videa svých koníčků (jídlo, zvířata, sport…)	13	6,34 %	38	4,97 %	51	5,26 %
Statusy, osobní pocity	4	1,95 %	32	4,19 %	36	3,72 %
Ostatní	4	1,95 %	60	7,85 %	64	6,60 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %



Graf 10 Jaký obsah nejvíce sdílíte na sociálních sítích?

Druh i četnost odpovědí ve své podstatě odpovídají odpovědím na otázky č. 8 a č. 10, kdy respondenti nejčastěji sdílejí své fotografie, fotky s kamarády nebo fotky aktivity či koníčků. Konzistentně se zmíněnými otázkami určité procento dotázaných nesdílí žádný obsah.

Otázka č. 16: Označujete své přátele na fotkách/ve videích?

Tabulka 22 Označujete své přátele na fotkách/ve videích?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano	165	80,49 %	497	65,05 %	662	68,32 %
Ne	40	19,51 %	267	34,95 %	307	31,68 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %

Otázka č. 17: Víte, jak si ochránit své soukromí na sociálních sítích?

Tabulka 23 Víte, jak si ochránit své soukromí na sociálních sítích?

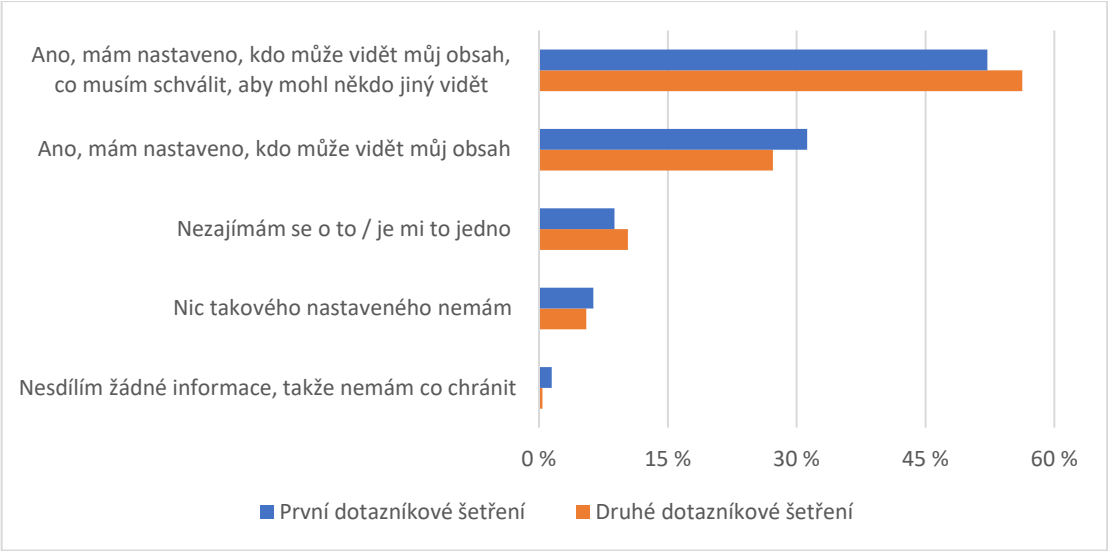
	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano	198	96,59 %	740	96,86 %	938	96,80 %
Ne	7	3,41 %	24	3,14 %	31	3,20 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %

Drtivá většina dotázaných, 96,59 % v případě prvního dotazníkového šetření, resp. 96,86 % v případě druhého, odpověděla na tuto otázku kladně ve smyslu, že mají přehled o tom, jak si chránit svoje soukromí na internetu. Jak lze ale usuzovat z odpovědí na předchozí i následující otázky, zejména č. 12, 18, 20, 22 a 25, část respondentů takové znalosti buď nemá, nebo se je rozhodli v některých případech neaplikovat. V rámci šetření se tak může jednat o kognitivní zkreslení, konkrétně o tzv. tendenci souhlasit, která je např. v článku *Improving social media measurement in surveys* [50] zmiňována jako poměrně značná limitace dotazníkových šetření v oblasti sociální sítí.

Otázka č. 18: Chráníte si soukromí na sociálních sítích pomocí nastavení?

Tabulka 24 Chráníte si soukromí na sociálních sítích pomocí nastavení?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano, mám nastaveno, kdo může vidět můj obsah, co musím schválit, aby mohl někdo jiný vidět	107	52,20 %	430	56,28 %	537	55,42 %
Ano, mám nastaveno, kdo může vidět můj obsah	64	31,22 %	208	27,23 %	272	28,07 %
Nezajímám se o to/Je mi to jedno	18	8,78 %	79	10,34 %	97	10,01 %
Nic takového nastaveného nemám	13	6,34 %	42	5,50 %	55	5,67 %
Nesdílím žádné informace, takže nemám co chránit	3	1,46 %	3	0,39 %	6	0,62 %
Ostatní	0	0,00 %	2	0,26 %	2	0,21 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %



Graf 11 Chráníte si soukromí na sociálních sítích pomocí nastavení?

Jak již bylo řečeno u výsledků předchozí otázky, přestože většina dotázaných tvrdí, že ví, jak si chránit své soukromí na sociálních sítích, poměrně velká část k tomu nevyužívá ten nejzákladnější dostupný nástroj, kterým je nastavení soukromí. 16,58 % respondentů z prvního šetření nemá žádné specifické nastavení soukromí nebo se o takové nastavení nezajímá, v případě druhého šetření se jedná o 16,49 %.

Je zde tedy poměrně značný rozpor mezi teorií a praxí při ochraně svého soukromí na internetu. Zatímco v prvním šetření 96,59 % respondentů odpovědělo, že ví, jak chránit své soukromí na sociálních sítích (otázka č. 17), z této otázky vyplývá, že pouze 83,42 % si chrání své soukromí pomocí nastavení. Oproti tomu v druhém šetření pouze 65,05 % odpovědělo kladně na otázku č. 17, avšak 83,51 % z nich si chrání své soukromí pomocí nastavení.

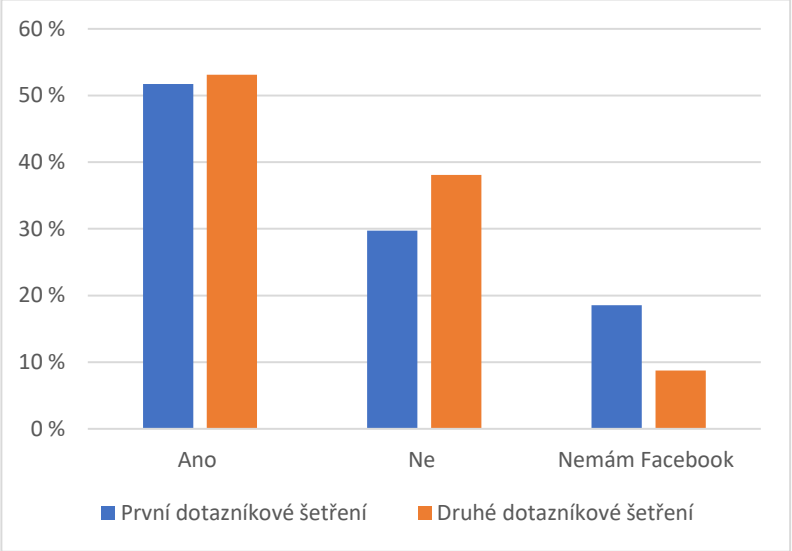
Otázka č. 19: Kolik máte na Facebooku přátel?

Otázka byla položena jako otevřená bez rozsahů, takže respondenti mohli zadat jakoukoliv hodnotu či komentář. Zhruba 63 % dotázaných odpovědělo buď přesnou, nebo přibližnou číselnou hodnotou, často například formou „okolo 100“. Z takto získaných hodnot vychází průměrně 146 přátel na respondenta. V zbývajících relevantních odpovědích cca 18 % respondentů uvedlo, že buď nemají, nebo nepoužívají Facebook, a cca 13 % respondentů odpovědělo, že neví, kolik mají přátel.

Otázka č. 20: Znáte všechny tyto lidi osobně? (Facebook přátelé)

Tabulka 25 Znáte všechny tyto lidi osobně? (Facebook přátelé)

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano	106	51,71 %	406	53,14 %	512	52,84 %
Ne	61	29,75 %	291	38,09 %	352	36,32 %
Nemám Facebook	38	18,54 %	67	8,77 %	105	10,84 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %



Graf 12 Znáte všechny tyto lidi osobně? (Facebook přátelé)

Po odhlédnutí od respondentů nemajících Facebook, kteří pro vyhodnocení následujícího dotazu nejsou podstatní, bylo zjištěno, že 29,75 %, resp. 38,09 % dotázaných nezná osobně všechny své přátele na Facebooku. Pokud má dotazovaná osoba pouze jednoho „neznámého“ přítele, je zařazena do uvedené skupiny, což komplikuje posouzení rizika. Tito „neznámí“ přátelé mají přístup ke sdílenému obsahu, a proto by respondenti měli přemýšlet o tom, koho přijímají za přátele a jaké informace jim poskytují.

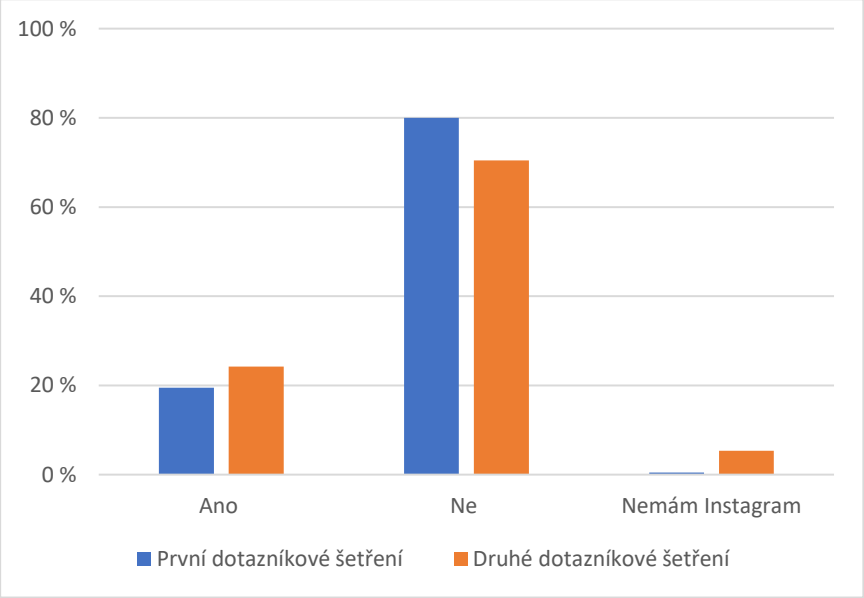
Otázka č. 21: Kolik máte sledujících na Instagramu?

Oproti předchozí otázce č. 19 zde respondenti odpovídali mnohem přesněji a celých 97,57 % uvedlo číselnou hodnotu. Minimum dotázaných pak uvedlo, že buď neví, nebo Instagram nepoužívá. Průměrný počet sledujících je 545, přičemž zajímavá byla odpověď dívky ve věku 17-18 let, která uvedla, že na veřejném profilu má přes 1000 sledujících, ale na soukromém jich má pouze 60.

Otázka č. 22: Znáte všechny tyto lidi osobně? (Instagram sledující)

Tabulka 26 Znáte všechny tyto lidi osobně? (Instagram sledující)

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano	40	19,51 %	185	24,21 %	225	23,22 %
Ne	164	80,00 %	538	70,42 %	702	72,45 %
Nemám Instagram	1	0,49 %	41	5,37 %	42	4,33 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %



Graf 13 Znáte všechny tyto lidi osobně? (Instagram sledující)

Na rozdíl od Facebooku, kde hlavní podstatou je komunikace a sdílení obsahu s přáteli, podstatou Instagramu je být mnohem otevřenější a není tedy překvapením, že výsledky jsou mnohem více ve prospěch neznámých sledujících. Při konkrétním porovnání s výsledky otázky č. 20 se jedná o rozdíl 50,25 p. b. (29,75 % vs. 80,00 %) v případě prvního dotazníkového šetření a celých 32,33 p. b. (38,09 % vs. 70,42 %) v případě druhého šetření. Uživatelé Instagramu mají možnost skrytí či blokace nechtěných sledujících a mohou si také přepnout svůj účet do soukromého režimu, kdy je mohou sledovat pouze předem schválení uživatelé, lze tak podobně jako u přátel na Facebooku řídit, kdo se dostane ke zveřejněnému obsahu. Dosah profilu je potom ovšem nižší.

Otázka č. 23: Myslíte si, že se na sociálních sítích může člověk stát závislým?

Tabulka 27 Myslíte si, že se na sociálních sítích může člověk stát závislým?

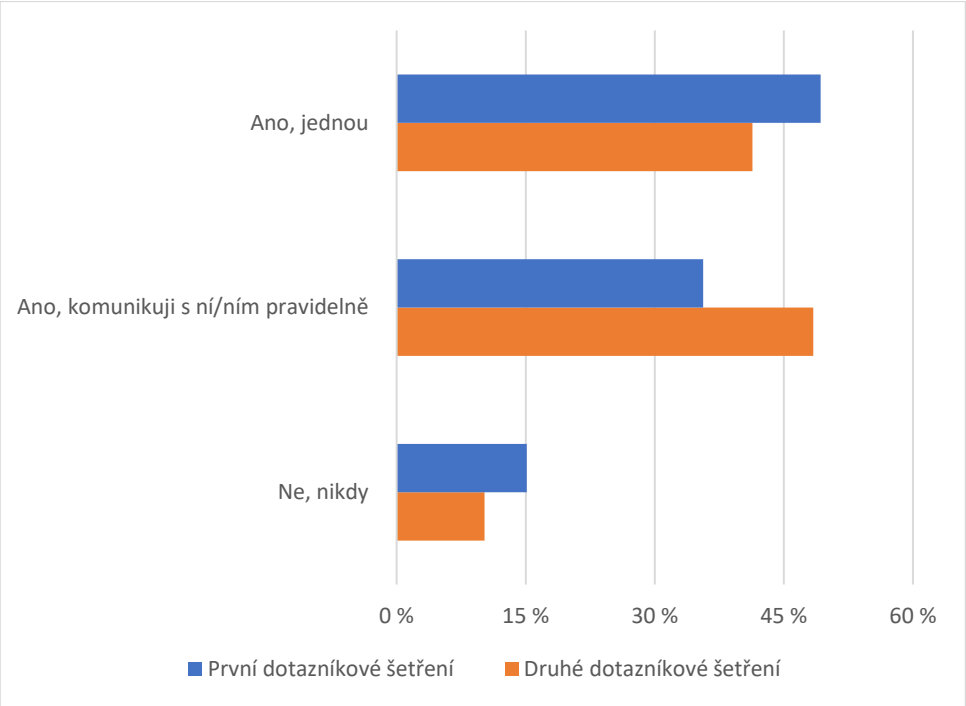
	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano	202	98,54 %	740	96,86 %	942	97,21 %
Ne	3	1,46 %	24	3,14 %	27	2,79 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %

Pouze 1,46 % dotázaných v rámci prvního šetření a 3,14 % dotázaných v rámci druhého šetření si myslí, že není možné stát se závislým na sociálních sítích, což je méně než v dotazníku Veroniky Jordánové [46], kde byl výsledek 10 %. Jelikož její výzkum byl proveden v roce 2019, je možné, že osvěta v tomto směru posunula znalost mezi mládeží a dospívajícími. Skutečnost, že v souvislosti s používáním sociálních sítí může vznikat závislost, je totiž poměrně dobře prokázaná, např. v systematickém přehledu uveřejněném v roce 2022 v časopise Frontiers of Psychiatry [51].

Otázka č. 24: Komunikovali jste někdy s člověkem, kterého jste nikdy neviděli v reálném světě?

Tabulka 28 Komunikovali jste někdy s člověkem, kterého jste nikdy neviděli v reálném světě?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano, jednou	101	49,27 %	316	41,36 %	417	43,03 %
Ano, komunikuji s ní/ním pravidelně	73	35,61 %	370	48,43 %	443	45,72 %
Ne, nikdy	31	15,12 %	78	10,21 %	109	11,25 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %



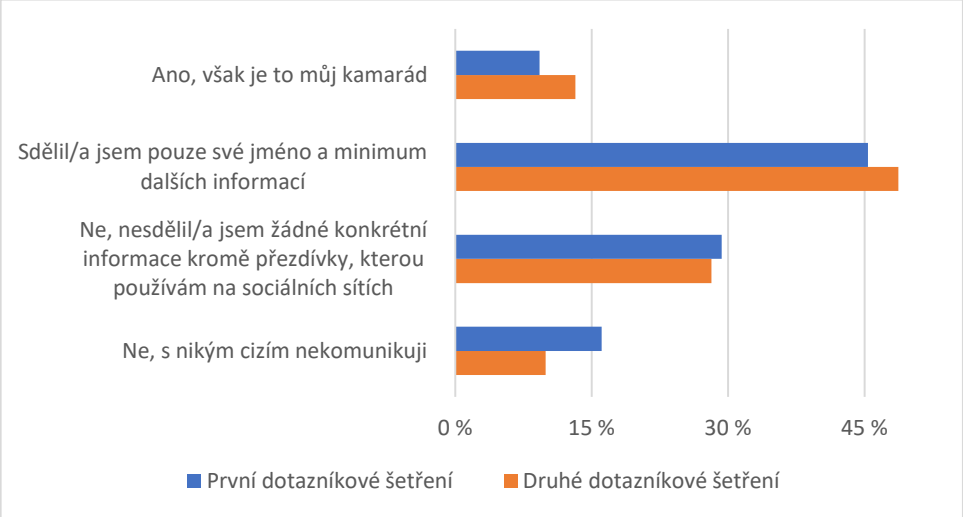
Graf 14 Komunikovali jste někdy s člověkem, kterého jste nikdy neviděli v reálném světě?

Výsledky nejsou překvapením a přímo vyplývají z odpovědí na otázku č. 20 a 22, kdy zejména v prostředí aplikace Instagram může často docházet ke komunikaci s neznámými lidmi pomocí komentářů nebo přímých zpráv. Pouze 15,12 %, resp. 10,21 % dotázaných nikdy nekomunikovalo s neznámým člověkem na internetu. Za zmínku stojí poměrně podstatný rozdíl v četnosti takové komunikace, kdy v rámci prvního dotazníku odpovědělo 35,61 % dotázaných, že pravidelně komunikují s člověkem, kterého neznají v reálném životě, zatímco v rámci druhého šetření je to 48,43 %. Rozdíl 12,82 procentního bodu lze vysvětlit složením dotazovaného vzorku, protože druhé šetření bylo provedeno v komunitách hráčů počítačových her, kde je mnohem větší předpoklad, že bude docházet k takovéto komunikaci.

Otázka č. 25: Sdělujete tomuto neznámému člověku své osobní údaje (věk, bydliště, školu, do které chodíte, informace o rodině…)?

Tabulka 29 Sdělujete tomuto neznámému člověku své osobní údaje (věk, bydliště, školu, do které chodíte, informace o rodině…)?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano, však je to můj kamarád	19	9,27 %	101	13,22 %	120	12,38 %
Sdělil/a jsem pouze své jméno a minimum dalších informací	93	45,36 %	372	48,69 %	465	47,99 %
Ne, nesdělil/a jsem žádné konkrétní informace kromě přezdívky, kterou používám na sociálních sítích	60	29,27 %	215	28,14 %	275	28,38 %
Ne, s nikým cizím nekomunikuji	33	16,10 %	76	9,95 %	109	11,25 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %



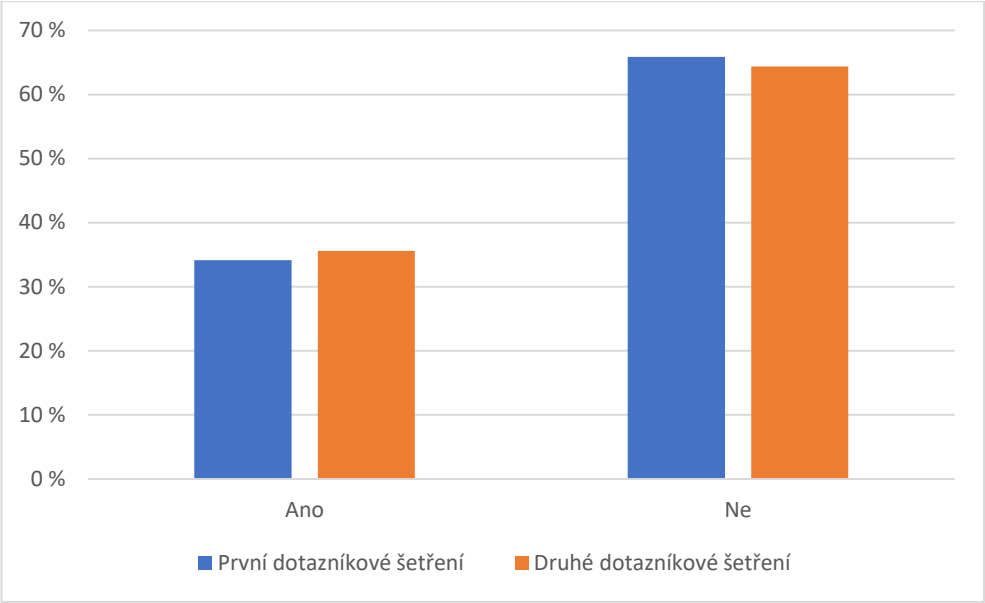
Graf 15 Sdělujete tomuto neznámému člověku své osobní údaje (věk, bydliště, školu, do které chodíte, informace o rodině…)?

Podobně jako na předchozí otázku i zde odpovědělo 16,10 %, resp. 9,95 %, že s nikým cizím nekomunikují, což potvrzuje vnitřní konzistenci výzkumu. Zároveň si většina respondentů, 90,73 %, resp. 87,62 %, uvědomuje, že není bezpečné sdílet větší množství osobních informací s neznámými lidmi, což je pozitivní. Často ovšem může docházet k sdělení více informací, než si dotyčný uvědomuje, nebo může dojít ke sdělení takové informace, která umožní člověku se zlými úmysly vyhledání dalších informací. Celkem 585 (60,37 %) ze všech dotazovaných uvedlo, že neznámé osobě sdělili minimálně své jméno, což ji potom jednoduchým vyhledáváním může zavést k jejich facebookovému nebo instagramovému profilu, kde je dle míry zabezpečení k dispozici množství dalších informací. Je nutné si uvědomit, že každý člověk svým působením na internetu zanechává tzv. digitální stopu, která je do jisté míry nesmazatelná, a ti nejmladší uživatelé internetu a sociálních sítí by měli být vzděláváni v její aktivní správě.

Otázka č. 26: Zažili jste někdy Vy nebo někdo ve Vašem okolí kyberšikanu? (šikana, která probíhá na internetu, na sociálních sítích pomocí komentářů, sdílení Vašich fotek, zesměšňování apod.)

Tabulka 30 Zažili jste někdy Vy nebo někdo ve Vašem okolí kyberšikanu? (šikana, která probíhá na internetu, na sociálních sítích pomocí komentářů, sdílení Vašich fotek, zesměšňování apod.)

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano	70	34,15 %	272	35,60 %	342	35,29 %
Ne	135	65,85 %	492	64,40 %	627	64,71 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %



Graf 16 Zažili jste někdy Vy nebo někdo ve Vašem okolí kyberšikanu? (šikana, která probíhá na internetu, na sociálních sítích pomocí komentářů, sdílení Vašich fotek, zesměšňování apod.)

Celkem 35,29 % dotázaných odpovědělo, že se někdy setkali s kyberšikanou, což je bohužel velmi vysoký poměr, přesto je to stále zhruba o 11 % méně, než ukazují srovnatelné průzkumy provedené v USA [52]. Při srovnání se studií uveřejněnou v porovnávané bakalářské práci od Veroniky Jordánové [46] je to ovšem znatelný pokles, jelikož výsledky z roku 2019 ukázaly pozitivní odpověď v 81 % případů.

Otázka č. 27: Jak tato kyberšikana probíhala? Prosím popište.

Otázka byla položena pouze respondentům, kteří na předchozí otázku odpověděli kladně, a povaha otázky byla z principu otevřená. Četnost odpovědí je 70 v prvním šetření, resp. 272 ve druhém a ze získaných dat vyplývá, že dívky se s kyberšikanou setkávají o cca 43 % častěji než chlapci.

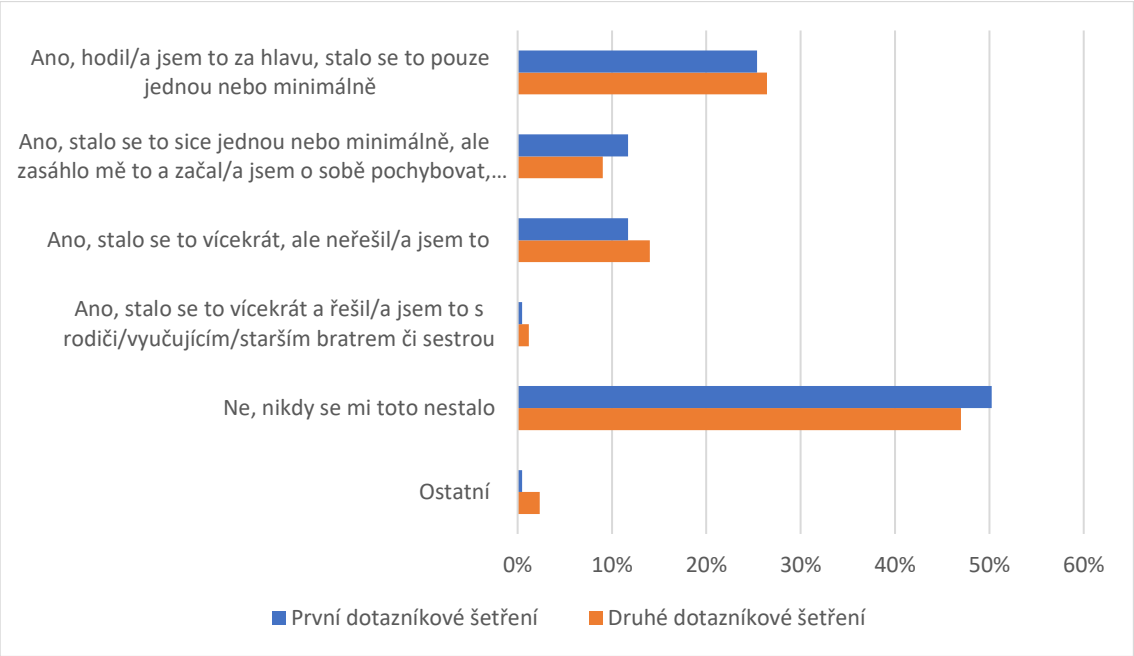
Chlapci často zmiňují zesměšňování a nadávky, zneužívání soukromých fotek či vydírání za pomoci pořízeného videa. Jeden z respondentů, chlapec ve věku 17-18, dostával kromě jiného návody na sebevraždu, z kontextu vyplývá, že to bylo v rámci hraní online hry. Další chlapec zmínil velmi nebezpečné vydávání se za jinou osobu pomocí vytváření falešných účtů.

Dívky obdobně zmiňují nadávky, výhrůžky a zesměšňování. U starších dívek se objevilo několik příkladů zneužití intimních fotek k zesměšnění či vydírání, které podle kontextu dalších odpovědí byly řešeny i policií. Obecně velká část kyberšikany dle respondentů probíhala za pomoci vizuálního obsahu (nevhodných fotek nebo videí).

Otázka č. 28: Zažili jste někdy zesměšnění na sociální síti? Někdo nelichotivě okomentoval Vaši fotku, status, cokoli. A jak jste se s tím vypořádali?

Tabulka 31 Zažili jste někdy zesměšnění na sociální síti? Někdo nelichotivě okomentoval Vaši fotku, status, cokoli. A jak jste se s tím vypořádali?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano, hodil/a jsem to za hlavu, stalo se to pouze jednou nebo minimálně	52	25,36 %	202	26,44 %	254	26,21 %
Ano, stalo se to sice jednou nebo minimálně, ale zasáhlo mě to a začal/a jsem o sobě pochybovat, mrzelo mě to	24	11,71 %	69	9,03 %	93	9,60 %
Ano, stalo se to vícekrát, ale neřešil/a jsem to	24	11,71 %	107	14,00 %	131	13,52 %
Ano, stalo se to vícekrát a řešil/a jsem to s rodiči/ vyučujícím/ starším bratrem či sestrou	1	0,49 %	9	1,18 %	10	1,03 %
Ne, nikdy se mi toto nestalo	103	50,24 %	359	46,99 %	462	47,68 %
Ostatní	1	0,49 %	18	2,36 %	19	1,96 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %



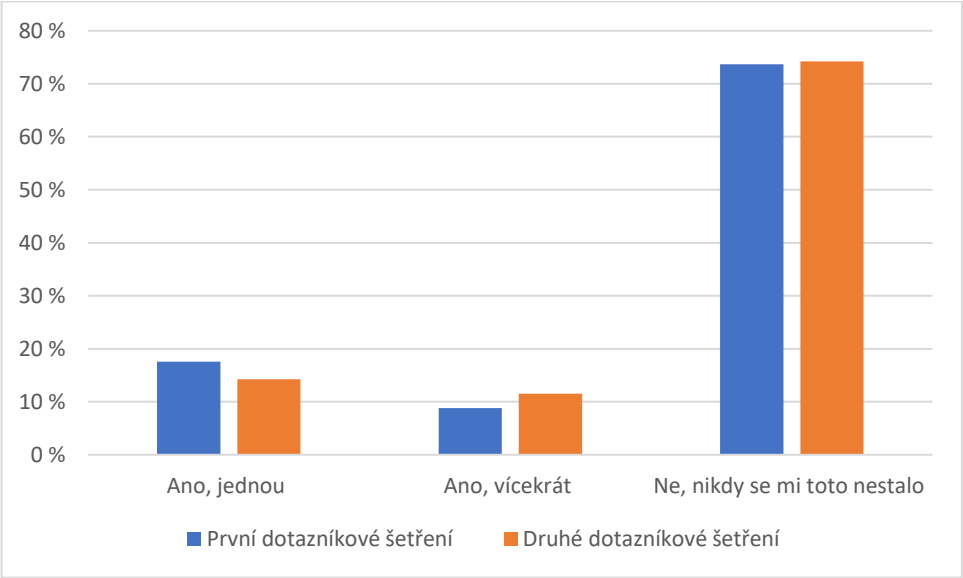
Graf 17 Zažili jste někdy zesměšnění na sociální síti? Někdo nelichotivě okomentoval Vaši fotku, status, cokoli. A jak jste se s tím vypořádali?

Přestože pouze 35,29 % všech respondentů odpovědělo na otázku č. 26, že se nějakým způsobem setkali s kyberšikanou, zde 49,27 %, resp. 50,65 % dotázaných uvádí, že zažili zesměšňování na internetu. Kyberšikana, do které patří i urážky, vyhrožování, pomluvy, obtěžování a právě i zesměšňování, je totiž nejčastější formou útoku na internetu a sociálních sítích. Dle výsledku šetření si tedy část mladistvých plně neuvědomuje všechny projevy šikany a doporučení a další edukace by se tedy mohly ubírat tímto směrem. S tím souvisí i fakt, že pouze minimum dotázaných takové situace řešilo s někým dospělým.

Otázka č. 29: Stalo se Vám někdy, že na Vás cíleně na internetu útočil jeden člověk/skupina lidí? Např. zesměšňující fotky, nepříjemné zprávy apod.

Tabulka 32 Stalo se Vám někdy, že na Vás cíleně na internetu útočil jeden člověk/skupina lidí? Např. zesměšňující fotky, nepříjemné zprávy apod.

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano, jednou	36	17,56 %	109	14,27 %	145	14,96 %
Ano, vícekrát	18	8,78 %	88	11,52 %	106	10,94 %
Ne, nikdy se mi toto nestalo	151	73,66 %	567	74,21 %	718	74,10 %
Celkem	205	100,00 %	764	100,00 %	969	100,00 %



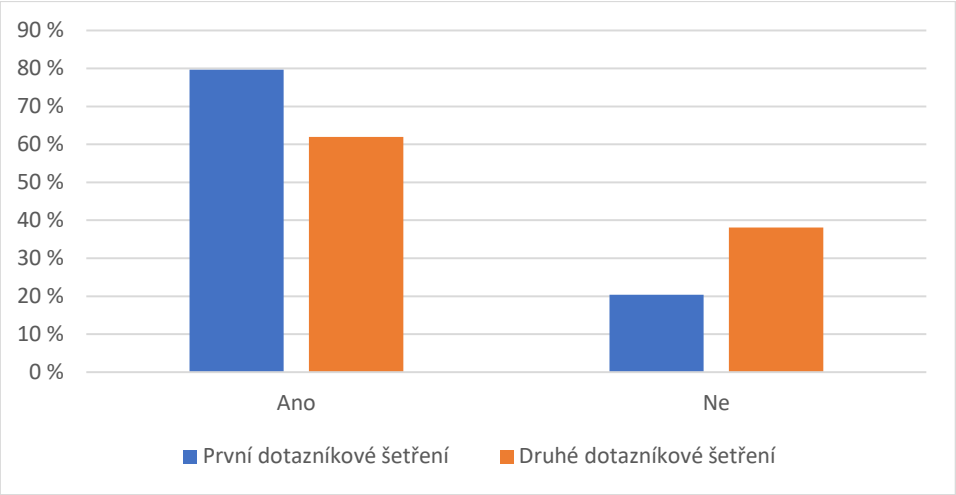
Graf 18 Stalo se Vám někdy, že na Vás cíleně na internetu útočil jeden člověk/skupina lidí? Např. zesměšňující fotky, nepříjemné zprávy apod.

Celkem 74,10 % dotázaných se nikdy nesetkalo s tím, že by se stali obětí cíleného útoku na internetu, který by byl ve své podstatě horší než mírné formy zesměšňování. Průměr respondentů z obou šetření, kteří se právě jednou setkali s cíleným útokem, je 14,96 % a zbývajících 10,94 % se tedy stalo obětí opakované kyberšikany. Tyto výsledky odpovídají výzkumu Veroniky Jordánové [46], ve kterém se 11,70 % dotázaných stalo obětí jednorázového útoku a 11,70 % opakovaného útoku. Proto zde není možné vysledovat žádný silný rostoucí trend.

Otázka č. 30: Zesměšňoval Vás na internetu někdo, koho znáte/jste znali z reálného života?

Tabulka 33 Zesměšňoval Vás na internetu někdo, koho znáte/jste znali z reálného života?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano	43	79,63 %	122	61,93 %	165	65,74 %
Ne	11	20,37 %	75	38,07 %	86	34,26 %
Celkem	54	100,00 %	197	100,00 %	251	100,00 %



Graf 19 Zesměšňoval Vás na internetu někdo, koho znáte/jste znali z reálného života?

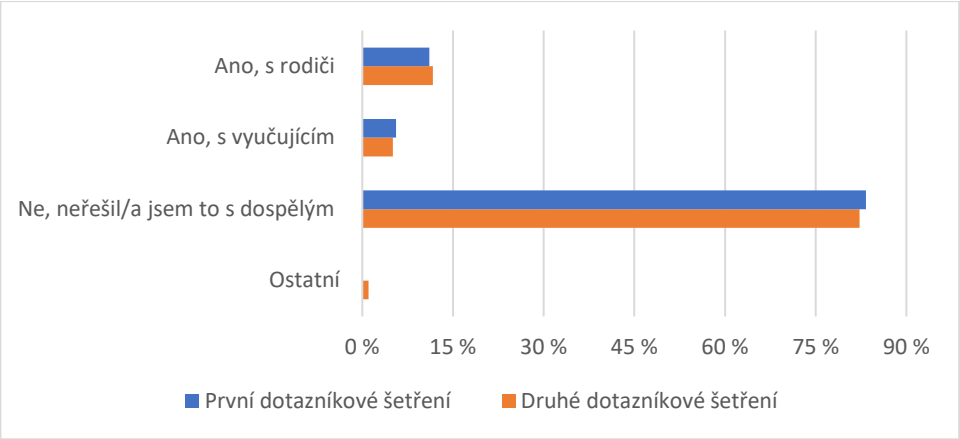
Vyhodnocení této otázky je zajímavé zejména v porovnání s otázkou č. 24, výsledky musí být vyhodnoceny v kontextu mírně rozdílného statistického výběru respondentů. První šetření bylo provedeno osobně ve třídách a druhé šetření online zejména ve facebookových skupinách hráčů počítačových her. Respondenti z druhého výběru se o něco častěji baví s lidmi, které osobně neznají, a proto v jejich případě dochází častěji k zesměšňování od těchto osob.

Otázka byla zároveň položena pouze těm, kteří na otázku č. 29 odpověděli kladně. To v případě prvního dotazníku zapříčinilo snížení četnosti odpovědí na 54, čímž se mírně snižuje vypovídací hodnota oproti druhému šetření, kde četnost byla 197. Pro obě šetření nicméně platí, že se mladiství častěji setkávají se zesměšňováním ze strany lidí, které osobně znají.

Otázka č. 31: Řešili jste tuto věc s někým dospělým?

Tabulka 34 Řešili jste tuto věc s někým dospělým?

	První dotazníkové šetření		Druhé dotazníkové šetření		Souhrn obou šetření	
Odpověď	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**	**Počet hlasů**	**Počet procent**
Ano, s rodiči	6	11,11 %	23	11,67 %	29	11,55 %
Ano, s vyučujícím	3	5,56 %	10	5,08 %	13	5,18 %
Ne, neře-šil/a jsem to s dospělým	45	83,33 %	162	82,23 %	207	82,47 %
Ostatní	0	0,00 %	2	1,02 %	2	0,80 %
Celkem	54	100,00 %	197	100,00 %	251	100,00 %



Graf 20 Řešili jste tuto věc s někým dospělým?

Pouze minimum dotázaných, 16,67 %, resp. 17,77 %, takovou situaci řešilo s někým dospělým. Z toho lze učinit závěr, že ačkoliv se mládež s různou formou kyberšikany setkává poměrně často (viz předchozí výzkumné otázky), snaží se ji buď ignorovat, nebo řešit sama, než aby ji řešila s někým dospělým. Rodiče a učitelé tedy často ani nemusí vědět, že k ní dochází. Z výsledků dále vyplývá, že když už se mladiství rozhodnout šikanu řešit, je to častěji s rodiči než s vyučujícím.

Dva dotázaní z druhého výzkumného šetření uvedli, že tuto situaci řešili s policií.

Otázka č. 32: Jak jste tuto věc řešili?

Tato otázka byla zadána jako otevřená. Četnost odpovědí v případě prvního dotazníku byla 50 a v případě druhého 147. Zhruba polovina dotázaných v rámci obou šetření odpověděla, že danou situaci neřešili nijak, ignorovali ji nebo jim byla jedno. V případech, kdy se dle kontextu dotazníku jednalo o kyberšikanu ze strany osoby, kterou konkrétní respondent osobně neznal, bylo často uvedeným řešením použití některého z nástrojů pro zabezpečení účtu na konkrétní sociální síti, tedy např. nastavení soukromého profilu, nahlášení účtu, blokace apod. Část respondentů se o dané situaci radila s přáteli a několik se jich obrátilo na policii.

Otázka č. 33: Co byste doporučil tomu, kdo je šikanován? Prosím vypište.

Doporučení reflektují různé přístupy k řešení šikany již zjištěné v rámci šetření. Někteří radí okamžitě řešit s dospělými, někteří radí ignorovat nebo řešit pomocí vhodných nástrojů na sociální síti (blokace/nahlášení). Chlapec ve věku 15-16 let správně podotýká, že záleží na míře šikany, které bude odpovídat i vhodné řešení. Dívka ve věku 17-18 radí svěřit se osobě, které lze důvěřovat, což může být například kamarádka, vyučující nebo rodič, ale hlavně řešit šikanu co nejdříve a nenechat ji zajít příliš daleko. Další dívka ve stejném věku doporučuje zabezpečit si sociální sítě a udržovat si důvěryhodný kruh přátel, protože šikana je často spojena s anonymitou sociálních sítí.

6.5 Srovnání výzkumu

V roce 2019 proběhlo kvantitativní dotazníkové šetření (výzkum) v rámci bakalářské práce: „*Sociální sítě a jejich bezpečnost z pohledu mladistvých*“, jehož autorkou byla Veronika Jordánová [46].

Šetření bylo provedeno ve třídách druhého stupně základní školy v Přerově, a to díky spolupráci s paní Mgr. Markétou Krajňakovou, Ph.D. Celkem bylo odesláno 45 dotazníků, z nichž všech 45 bylo úspěšně vyplněno. Zároveň byla na další školy s žádostí o vyplnění odeslaná online verze stejného dotazníku, což zvýšilo celkový počet respondentů na 94 (54 dívek a 40 chlapců) [46].

Výzkum byl vybrán proto, že časový odstup tří let umožňuje poměrně zajímavé srovnání. Jelikož prostor internetu a sociálních sítí je velmi dynamický, porovnání se starším výzkumem by nemuselo přinést relevantní výsledky. Šetření je také poměrně jednoduše opakovatelné se stejnými, či podobnými otázkami a lze tak ověřit reliabilitu původního výzkumu. Zároveň si jsou věkové skupiny respondentů z obou výzkumů poměrně blízké.

6.5.1 Shodnost a rozdíly ve výsledcích výzkumů

Otázka č. 3: Víte, co jsou to sociální sítě?

Většina respondentů v obou výzkumných šetřeních odpověděla, že ví, co jsou to sociální sítě. Konkrétně ve srovnávaném šetření na otázku odpovědělo kladně 97,87 % oslovených jednotlivců, zatímco v aktuálním šetření spojeném s touto diplomovou prací kladně odpovědělo 99,28 % všech zúčastněných.

Otázka č. 4: Které sociální sítě používáte?

První tři místa v obou porovnávaných šetřeních obsadily platformy YouTube, Facebook a Instagram, ovšem jejich pořadí se mírně liší podle sledovaných skupin. Oproti roku 2019 zaznamenává Facebook mírný pokles popularity, zatímco Instagram zaznamenává její mírný nárůst. Z výsledků je patrná rostoucí obliba TikToku, který ve srovnávaném výzkumu není zmíněn, protože v roce 2019 teprve pomalu získával na popularitě.

Otázka č. 5: Kterou sociální síť používáte nejčastěji?

V kontrastu k předchozímu srovnávanému průzkumu, kde byla soutěž o oblíbenost různých sociálních sítí mnohem vyváženější, lze po třech letech pozorovat, že mezi mladými lidmi dominuje Instagram jako jednoznačně nejoblíbenější platforma. Stále ho následují platformy YouTube a Facebook.

Otázka č. 6: Používáte telefon/tablet k připojení na sociální sítě?

Většina zúčastněných respondentů obou šetření na tuto otázku reagovala kladně. Ve srovnávaném dotazníku takto odpovědělo 95,75 % respondentů, zatímco aktuální šetření, které je součástí této diplomové práce, uvádí navýšení tohoto trendu na 99,48 % respondentů.

Otázka č. 7: Kolik hodin přibližně denně strávíte na sociálních sítích?

Jelikož byly účastníkům daných šetření prezentovány mírně odlišné možnosti, nelze odpovědi přesně srovnávat. Zatímco v případě porovnávaného výzkumu mohli respondenti vybírat z variant 0 hodin, 1-3 hodiny, 4-5 hodin a více, ve výzkumu předkládaném v této diplomové práci byly nabídnuty varianty méně než hodinu, 1-2 hodiny, 3-4 hodiny, 5-6 hodin, 7-8 hodin a více než 8 hodin. Toto rozdílné členění přispívá k přesnosti získaných dat, avšak žádná z těchto variant přesně nekoresponduje s odpovídajícími kategoriemi ve srovnávaném výzkumu.

Otázka č. 8: K čemu sociální sítě používáte?

V obou šetřeních převažuje skupina respondentů využívajících sociální média hlavně pro komunikaci s přáteli, konkrétně ve srovnávaném šetření je to 93,62 % a v tom současném 95,25 % ze všech dotázaných. Podobně bylo na druhém místě uvedeno sdílení fotografií.

Otázka č. 9: Pokud používáte Facebook/Instagram/Snapchat, využíváte možnosti stories? Zveřejněné fotky či videa, které po 24 hodinách „zmizí".

V porovnávaném průzkumu kladně odpovědělo 59,57 % dotázaných. Zjištění z průzkumu prováděného v rámci této diplomové práce ukazuje, že 67,60 % všech respondentů využívá stories. To naznačuje nárůst oblíbenosti této funkce mezi lety 2019 a 2023.

Otázka č. 10: Jaký obsah sdílíte ve stories?

V rámci této diplomové práce byla otázka položena pouze účastníkům, kteří na předchozí dotaz odpověděli kladně. V kontrastu s tím ve srovnávaném výzkumu byla otázka položena všem účastníkům. Pro účely porovnání je nezbytné vyčistit výsledky prvního výzkumu o 40,43 % respondentů, kteří uvedli, že nevyužívají žádné sdílení obsahu. Po této korekci zjišťujeme, že ve srovnávaném výzkumu představuje podíl 100 % pro fotografie a 58,93 % pro videa. Průzkum této diplomové práce zjistil, že fotografie (97,10 %) a videa (41,69 %) ve stories sdílí v současné době méně uživatelů než před třemi lety. Velký pokles nastal v oblibě sdílení videí, rozdíl činí 17,24 procentního bodu.

Otázka č. 11: Sdílíte ve stories své selfies nebo fotky s přáteli?

Otázka byla v obou pracích položena jiným způsobem a obsahovala jiné možnosti, proto nelze kladné odpovědi přímo srovnávat. Relevantní je pouze negativní odpověď „ne“ ze srovnávaného dotazníku, která koresponduje s odpovědí „nesdílím selfie ani fotky s přáteli“. Zatímco ve srovnávaném průzkumu takto odpovědělo 41,49 % účastníků, v dotazníkovém šetření této diplomové práce se tímto způsobem vyjádřilo pouze 16,47 % ze všech respondentů.

Otázka č. 12: Sdílíte své konkrétní informace? Bydliště, školu, kterou navštěvujete, svoji rodinu.

V tomto konkrétním případě jsou výsledky téměř shodné. Ve srovnávaném průzkumu odpovědělo negativně 82,98 % respondentů, zatímco v průzkumu prováděném v rámci této diplomové práce bylo takových odpovědí 85,24 %. Rozdíl mezi těmito dvěma hodnotami činí pouhých 2,26 procentních bodů.

Otázka č. 13: Proč sdílíte své konkrétní informace?

Podobně jako u otázky č. 10 je i zde důležité před srovnáním upravit výsledky a vyřadit nepodstatné odpovědi. Po této korekci se ukázalo, že ve srovnávaném výzkumu 31,58 % oslovených zvolilo možnost „jen tak, baví mě to“, což je nižší číslo než výsledek z průzkumu provedeného v rámci této diplomové práce (41,26 % ze všech dotázaných).

V rámci analýzy získaných výsledků je důležité zdůraznit, že porovnávané vzorky jsou v obou výzkumech již poměrně malé, 38 respondentů v porovnávaném průzkumu a 143 respondentů v průzkumech diplomové práce. To zapříčiňuje, že relevance srovnání se snižuje. I přesto se poměry výsledků vzájemně podobají.

Otázka č. 14: Jaký obsah sdílíte na sociálních sítích?

Tato otázka nebyla ve srovnávaném šetření položena.

Otázka č. 15: Jaký obsah nejvíce sdílíte na sociálních sítích?

Získané pořadí odpovědí je podobné v obou výzkumech. Nejčastěji jsou sdíleny vlastní fotografie nebo fotografie s přáteli, dále následují snímky spojené s osobními zálibami, videa, statusy a další obsah. V rámci obou průzkumů této diplomové práce uvedlo 22,19 % respondentů, že nesdílí žádný obsah, což je o 16,87 procentního bodu více než ve výsledcích porovnávaného průzkumu.

Otázka č. 16: Označujete své přátele na fotkách/ve videích?

Na tuto otázku odpovědělo kladně 62,77 % respondentů srovnávaného průzkumu. V kontrastu k tomu v prvním šetření provedeném v rámci této diplomové práce stejně odpovědělo 80,49 % a v druhém šetření 65,05 % dotázaných.

Otázka č. 17: Víte, jak si ochránit své soukromí na sociálních sítích?

Z výsledků průzkumu z roku 2019 vyplynulo, že 92,55 % respondentů má povědomí o tom, jak zabezpečit své soukromí na sociálních sítích. V rámci této diplomové práce na stejnou otázku odpovědělo kladně 96,80 % ze všech dotázaných, zatímco pouze 3,20 % respondentů uvedlo, že tuto problematiku neovládá.

Otázka č. 18: Chráníte si soukromí na sociálních sítích pomocí nastavení?

Při porovnání výsledků diplomové práce s výzkumem provedeným v roce 2019 je patrný pozitivní trend ve využívání nastavení soukromí k ochraně na sociálních sítích. Zatímco ve srovnávaném výzkumu 23,40 % mladistvých odpovědělo, že nemá žádná nastavení nebo se o takové nastavení nezajímají, v aktuálním výzkumu takto reagovalo pouze 16,30 %, což je rozdíl 7,1 procentního bodu.

Otázka č. 19: Kolik máte na Facebooku přátel?

Ve srovnávaném výzkumu byla položena otázka: „Kolik máte na Facebooku/Instagramu přátel?“, která byla v rámci této diplomové práce rozdělena na dvě samostatné otázky kvůli rozdílné povaze těchto sociálních sítí. To znamená, že výsledky jsou bohatší na informace, avšak zároveň se stávají méně porovnatelnými s výzkumem z roku 2019. Kromě toho v aktuálním výzkumu bylo na tuto otázku odpovídáno formou otevřených odpovědí, zatímco ve srovnávaném výzkumu dotazovaní vybírali z předem připravených možností.

Otázka č. 20: Znáte všechny tyto lidi osobně? (Facebook přátelé)

Ve srovnávaném výzkumu kladně odpovědělo 47,87 % účastníků, zatímco 52,13 % vybralo zápornou odpověď. Tento výsledek se neshoduje ani s jedním z obou průzkumů provedených v rámci této diplomové práce, konkrétně u obou otázek týkajících se Facebooku a Instagramu. Kombinací výsledků z otázek č. 20 a 22 by vzniklo číslo, které by pro výzkum nemělo přílišnou relevanci a z něhož by nebylo možné odvodit spolehlivé závěry.

Otázka č. 21: Kolik máte sledujících na Instagramu?

Tato otázka nebyla ve srovnávaném výzkumu samostatně položena.

Otázka č. 22: Znáte všechny tyto lidi osobně? (Instagram sledující)

Viz srovnání otázky č. 20.

Otázka č. 23: Myslíte si, že se na sociálních sítích může člověk stát závislým?

Srovnání bylo provedeno v rámci předchozí kapitoly 6.4 Realizace výzkumu a jeho vyhodnocení.

Otázka č. 24: Komunikovali jste někdy s člověkem, kterého jste nikdy neviděli v reálném světě?

V rámci výzkumu této diplomové práce pouze 11,25 % ze všech dotázaných nikdy nekomunikovalo s člověkem, kterého neznali z reálného světa. Naopak ve srovnávaném průzkumu takovou odpověď vybralo 25,53 % respondentů, což představuje rozdíl 14,28 procentního bodu. Lze tedy sledovat trend, který je pochopitelný se vzrůstající oblibou sociálních sítí. Četnost odpovědí o jednorázové komunikaci s neznámým člověkem je zhruba srovnatelná, rozdíl se tedy přesunul ve prospěch opakované komunikace.

Otázka č. 25: Sdělujete tomuto neznámému člověku své osobní údaje (věk, bydliště, školu, do které chodíte, informace o rodině, ...)?

Z porovnání odpovědí na předchozí otázku jasně vyplývá nárůst tendence komunikovat s neznámými osobami. Avšak u této konkrétní otázky je zjevný stagnující trend týkající se sdílení osobních údajů mezi mladými lidmi a neznámými jednotlivci. Podle průzkumu z roku 2019 se tímto způsobem chovalo 11,70 % dotázaných, kdežto v aktuálním výzkumu spojeném s touto diplomovou prací to bylo 12,38 % z celkového počtu respondentů. Rozdíl mezi těmito výsledky činí pouze 0,68 procentního bodu. V rámci průzkumu prováděného v souvislosti s diplomovou prací se projevilo, že současná mládež je častěji než v minulosti ochotná sdílet své méně osobní informace. Tento směr je v kontrastu s dobou před třemi lety, kdy mladí lidé nevykazovali sklon k navazování komunikace s neznámými uživateli internetu.

Otázka č. 26: Zažili jste někdy Vy nebo někdo ve Vašem okolí kyberšikanu? (šikana, která probíhá na internetu, na sociálních sítích pomocí komentářů, sdílení Vašich fotek, zesměšňování apod.)

Srovnání bylo provedeno v rámci předchozí kapitoly 6.4 Realizace výzkumu a jeho vyhodnocení.

Otázka č. 27: Jak tato kyberšikana probíhala? Prosím popište.

Oba průzkumy zadaly tuto otázku ve formě otevřeného dotazu. Jejich výsledky jednoznačně ukazují, že tendence v oblasti kyberšikany zahrnující využívání zesměšňujícího vizuálního obsahu (fotografií a videí) nadále přetrvává. V rámci obou zkoumaných výzkumů, ať už v průzkumu z roku 2019, či v aktuálním výzkumu spojeném s touto diplomovou prací, se vyskytli mladiství, kteří byli vystaveni kyberšikaně nejen formou urážek, ponižování, vyhrožování a pomluv, nýbrž se také setkali s metodou vytváření falešných profilů, které se za oběti vydávaly.

Současně lze v obou dotazníkových šetřeních identifikovat mimořádné formy kyberšikany. V průzkumu z roku 2019 jeden z respondentů zmínil, že kyberšikana dospěla až k znásilnění, zatímco v současném výzkumu byla zaznamenána odpověď, kdy se jedinec setkal s útočníkem, který ho naváděl k sebevraždě.

Otázka č. 28: Zažili jste někdy zesměšnění na sociální síti? Někdo nelichotivě okomentoval Vaši fotku, status, cokoli. A jak jste se s tím vypořádali?

Porovnáním lze zaznamenat nepříznivý směr vývoje četnosti trendu zesměšňování na sociálních sítích. Zatímco ve srovnávaném průzkumu se s akty zesměšňování nikdy nesetkalo 60,64 % účastníků, v rámci šetření prezentovaného v této diplomové práci to platilo pouze pro 47,68 % ze všech dotázaných.

Otázka č. 29: Stalo se Vám někdy, že na Vás cíleně na internetu útočil jeden člověk/skupina lidí? Např: zesměšňující fotky, nepříjemné zprávy apod.

Srovnání bylo provedeno v rámci předchozí kapitoly 6.2 Prezentace výsledků.

Otázka č. 30: Zesměšňoval Vás na internetu někdo, koho znáte/jste znali z reálného života?

V porovnávaném průzkumu uvedlo 19,15 % dotázaných, že zažili online zesměšňování na internetu od osob, které znali ze svého reálného života. Z toho vyplývá zajímavý kontrast mezi oběma studiemi. V rámci výzkumu této diplomové práce, konkrétně v otázce č. 24, bylo zjištěno, že mladí jedinci na sociálních sítích častěji komunikují s lidmi, se kterými se setkávají pouze online. Navzdory tomu 17,03 % ze všech respondentů uvedlo, že se na internetu setkali se zesměšňováním od osob, s nimiž se znají i mimo online svět.

Otázka č. 31: Řešili jste tuto věc s někým dospělým?

Ve srovnávaném šetření byla otázka opět položena všem respondentům, proto je pro porovnání třeba výsledky očistit o odpovědi „nikdy se mi to nestalo“. Získané výsledky pak představují následující hodnoty: 61,54 % respondentů tuto situaci nesdílelo s žádným dospělým, 30,77 % zvolilo řešení s rodiči a 7,69 % se obrátilo na svého učitele. Vzhledem k nízké četnosti odpovědí (celkem 25 respondentů) však není možné s vysokou mírou spolehlivosti tvrdit, že existuje záporný trend, který by naznačoval, že dospívající se stále méně obrací na dospělé osoby při řešení situací kyberšikany.

Otázka č. 32: Jak jste tuto věc řešili?

Ve srovnávaném šetření byla otázka opět položena všem respondentům, proto je pro porovnání třeba výsledky očistit o odpovědi „nikdy jsem nic takového neřešil“. Z předpřipravených odpovědí nejvíce dotázaných, kteří tuto situaci zažili, zvolilo možnosti: toho člověka jsem znal/a osobně a vyříkali jsme si to (27,27 %), tento člověk to přestal dělat sám od sebe (27,27 %). Vzhledem k nízké četnosti odpovědí (celkem 22 respondentů) však není možné s vysokou mírou spolehlivosti tvrdit, že existuje záporný trend, který by naznačoval ignorování daného problému.

Z výzkumného šetření z roku 2019 vyplývá, že žádný z respondentů, který zažil zesměšňování na internetu, v takové situaci nevyužil některého z nástrojů pro zabezpečení účtu na konkrétní platformě (např. nastavení soukromého profilu, nahlášení účtu, blokace…).

Otázka č. 33: Co byste doporučil tomu, kdo je šikanován? Prosím vypište.

Tato otázka byla jak ve srovnávaném šetření z roku 2019, tak i v aktuálním výzkumu položena formou otevřené otázky. Odpovědi se příliš nelišily od aktuálního výzkumu. Jedním z rozdílů je, že ve srovnávaném dotazníku žádný z respondentů nedoporučoval tuto situaci ignorovat, avšak vzhledem k počtu respondentů (14) není možné na tomto základu vytvořit důvěryhodný závěr.

6.6 Závěry výzkumu

Tato diplomová práce se snaží pomocí vlastního výzkumu rozšířit dosavadní poznatky o rizicích, kterým čelí mladí a dospívající v prostoru internetu, zejména pak při používání sociálních sítí, které v poslední dekádě zásadně změnily způsob komunikace. Přestože některé druhy online interakcí jsou v dnešní době důležité a sociální média mohou hrát významnou roli v budování mezilidských vztahů, přinesl vzestup sociálních sítí i řadu nebezpečí a negativních jevů. Výzkum provedený v rámci empirické části práce měl za cíl sebrat kvalitní data, jejichž vyhodnocením by se mohl získat cenný pedagogický materiál pro učitele na středních školách. Provedení dvou dotazníkových šetření, jednoho ve třídách konkrétní střední školy a druhého online, a porovnání výsledků měly zajistit reprezentativní vzorek respondentů.

Pomocí srovnání výsledků z obou dotazníkových šetření s dřívějším výzkumem provedeným v rámci bakalářské práce Veroniky Jordánové [46] mohla tato diplomová práce validovat kvalitu obou výzkumů a zároveň vysledovat trendy ve stále se měnícím digitálním prostředí. Srovnávaný výzkum proběhl v roce 2019 pomocí dotazníkového šetření provedeného jak osobně, tak pomocí online dotazníku.

Z výsledků výzkumu této diplomové práce vyplývá, že téměř všechny děti a mladiství ve věku 15-20 let mají telefon nebo tablet, vědí, co jsou to sociální sítě, a v drtivé většině je také používají. Výčet používaných sociálních sítí ukazuje široký záběr respondentů, přičemž více než polovina z nich aktivně využívá všechny uvedené sociální sítě, tedy Facebook, Instagram, Snapchat, YouTube a TikTok, s výjimkou Twitteru. Pokud si ale mladiství měli vybrat pouze jednu síť, na které tráví nejvíce času, zvítězil rozhodně Instagram. Zajímavým trendem při porovnání se zmíněným starším výzkumem je vzestup TikToku během posledních tří let. Zásadní je zjištění, že okolo jedné čtvrtiny mladistvých tráví na sociálních sítích více než 5 hodin denně a většina mladistvých mezi 3 a 4 hodinami denně.

Z pohledu cílů diplomové práce bylo zajímavé zjištění, že téměř všichni respondenti tvrdí, že vědí, jak si na sociálních sítích ochránit své soukromí. Z odpovědí na následující dotazy je však patrné, že část mladistvých buď přeceňuje své vědomosti v této oblasti, nebo se rozhodla je neaplikovat na své chování na sociálních sítích. V porovnání se starším výzkumem je nicméně vidět pozitivní trend ve využití nastavení soukromí k ochraně na sociálních sítích. Druhá polovina výzkumu byla věnována převážně průzkumu zkušeností s kyberšikanou, se kterou se setkala zhruba třetina respondentů, což je mnohem méně, než ukázal srovnávaný výzkum. Z dat také vyplývá, že kyberšikana nejčastěji měla podobu zesměšňování, nadávek a výhrůžek a dívky se s ní setkaly častěji než chlapci.

Pro minimalizaci rizik na sociálních sítích lze doporučit pokračování ve vzdělávání dětí, mládeže, ale i rodičů a pedagogů v bezpečném používání sociálních sítí. Každý uživatel internetu vytváří tzv. digitální stopu, která roste s počtem sdílených osobních i zdánlivě nevinných informací, které poté může zneužít cizí osoba se zlými úmysly. Mladiství by se tedy měli zaměřit na možnosti nastavení soukromí a vždy se zamyslet nad tím, s kým jaké informace sdílí, a to zejména v prostředí oblíbeného Instagramu.

Na druhou stranu je třeba si uvědomit, že nebezpečí sociálních sítí není ani zdaleka spojeno pouze s neznámými osobami, protože z výsledku výzkumu vyplývá, že děti a mládež se častěji s kyberšikanou setkávají ze strany osob, které znají. Ačkoliv předchozí doporučení je částečně platné i v takových případech, důležitější je budování důvěry jak s pedagogy, tak rodiči, jelikož drtivá většina mladistvých svou zkušenost s kyberšikanou neřešila s nikým dospělým.

Dle mého názoru mohou zákazy a monitorování užívání sociálních sítí ze strany rodičů nebo pedagogů vést ke ztrátě důvěry u mladistvých. Naopak je třeba otevřeně a bez předsudků diskutovat o užívání sociálních sítí, o nebezpečích, kterým se na nich děti a mladiství mohou vystavovat, a obecně zvyšovat digitální gramotnost.

Sestavení dotazníku bylo do určité míry limitováno výzkumem provedeným v původní bakalářské práci [46]. Jelikož jedním z cílů bylo obě šetření porovnat, nemohlo dojít k přílišnému odklonu od formulace dotazu, případně nabízených odpovědí. Tam, kde byly nabídnuty jiné odpovědi, např. v otázce č. 7, bylo znemožněno přímé porovnání prací.

V rámci výzkumu této diplomové práce byla provedena dvě šetření za jiných podmínek. První dotazníkové šetření bylo zadané osobně a druhé online. Výsledky obou ovšem byly obdobné, a tedy vypovídající. Počet respondentů byl dostatečný pro získání kvalitních výsledků ve většině případů, výjimku tvoří některé podmíněné otázky, kde se četnost dotázaných snižuje.

Výzkumy využívající sběru dat na sociálních sítích se obecně provádějí pomocí kvantitativních metod a hrozí jim tedy limitace možným kognitivním zkreslením, jako např. u otázky číslo 14, kde mohlo dojít k takzvané „tendenci souhlasit“ [50], protože odpovědi nejsou konzistentní s odpověďmi na další otázku.

Jednou z očividných limitací je také chápání kyberšikany, kdy v rámci jedné otázky se s kyberšikanou setkala jen třetina respondentů, ale v následující otázce se více než polovina setkala se zesměšněním na sociálních sítích, což je rozhodně součást kyberšikany. Pro výsledky práce by bylo také zajímavé zjistit, proč většina mladistvých neřeší šikanu s dospělou osobou. Takto vznikají pouhé domněnky, které ale nelze zahrnout do závěrů práce. Nezbývá tedy než doporučit tuto oblast podrobit dalšímu výzkumu.

7 Závěr

Diplomová práce se zaměřuje na vliv sociálních sítí a jejich rizik na studenty středních škol. V úvodu jsou stanoveny tři cíle pro tuto práci. První z cílů se zabýval teoretickým zpracováním tématu sociálních sítí a jejich hrozeb.

- Vytvořit rešerši základních pojmů týkajících se sociálních sítí a jejich rizik.

V teoretické části byla provedena literární rešerše, která charakterizovala důležité pojmy týkající se sociálních sítí, jejich historie a vlastností. Zároveň je zde zmíněný jejich vliv na dospívajícího jedince. Celá první kapitola je zakončena popisem jednotlivých, v současnosti nejpopulárnějších, sociálních sítí. V druhé kapitole teoretické práce jsou shrnuta nejčastější rizika současné doby, jako jsou kyberšikana, kybergrooming, sexting a jiné rizikové jevy, které s sebou používání sociálních sítí nese a které představují značná nebezpečí pro jejich uživatele. V další kapitole jsou shrnuta základní pravidla pro bezpečné používání těchto internetových platforem, mezi něž patří například zabezpečení počítačového či mobilního zařízení, uživatelská obezřetnost, kontrola sdíleného obsahu, správné nastavení sociálních sítí atd. V poslední kapitole, která se věnuje rešeršní části, jsou prezentovány výsledky pěti relevantních výzkumů, které se zabývaly tématem bezpečnosti na sociálních sítích a internetu u dětí a mladistvých.

Další cíl práce byl připravit vzdělávací materiál pro výuku této problematiky.

- Vytvořit přípravu výukových materiálů do hodin informačních a komunikačních technologií a společenskovědního vzdělávání.

Praktická část této diplomové práce zahrnuje přehled jednotlivých příprav (3 přípravy do vyučovací hodiny informačních a komunikačních technologií a 3 přípravy do vyučovací hodiny společenskovědního vzdělávání). Ke každé přípravě je v práci uvedená reflexe z aplikace těchto pedagogických materiálů. Samotné přípravy do hodin jsou uvedeny v rámci přílohy diplomové práce z důvodu jejich velkého rozsahu.

Posledním stanoveným cílem této práce byla realizace vlastního výzkumu.

- Vytvořit kvantitativní dotazníkové šetření o chování středoškolských studentů na sociálních sítích včetně jeho vyhodnocení a srovnání s obdobným průzkumem.

V rámci empirické části práce jsou uvedena dvě dotazníková šetření, kterých se celkem zúčastnilo 969 respondentů ve věku od 15 do 20 let. První šetření bylo zadáváno osobně studentům Obchodní akademie a Jazykové školy Pardubice a zúčastnilo se ho celkem 205 respondentů. Druhé dotazníkové šetření bylo sdíleno na platformě Facebook (v komunitách hráčů počítačových her) a zúčastnilo se ho 764 respondentů. Výsledky dotazníkových šetření jsou prezentovány v rámci této diplomové práce a zároveň byly podrobeny srovnání s podobným výzkumem realizovaným v roce 2019. Závěr této části obsahuje stručné shrnutí výsledků.

Všechny stanovené cíle diplomové práce se podařilo splnit.

Přínos této práce je v několika oblastech. První oblastí je rešeršní část sociálních sítí a rizik spojených s jejich užíváním spolu s pravidly pro bezpečnou komunikaci. Zde jsou zahrnuty rozbory studií, které zkoumaly tuto problematiku. Velkým přínosem práce jsou vytvořené výukové materiály pro výuku informačních a komunikačních technologií a společenskovědního vzdělávání, které jsou zaměřené na problematiku používání sociálních sítí a jsou ověřeny ve výuce. Dalším z přínosů je výzkum, který zjistil aktuální trendy v chování mladistvých na sociálních sítích. To může být inspirací školám, které mohou pořádat besedy, projektové dny a jiné aktivity zaměřené na bezpečné používání těchto platforem.

Seznam použité literatury

[1] ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu.* Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-210-7527-6.

[2] KOHOUT, Roman, Radek KARCHŇÁK. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978-80-260-9543-9.

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

[4] *V síti* [film]. Režie Barbora CHALUPOVÁ, Vít KLUSÁK. Česko: Vít Klusák, Filip Remunda, 2020.

[5] PAVLÍČEK, Antonín. *Nová média a sociální sítě*. Praha: Oeconomica, 2010. ISBN 978-80-245-1742-1.

[6] ŠVARCOVÁ, Alžběta. *Než přišel Facebook. Stručný průvodce historií sociálních sítí. Internet pro všechny* [online]. (21.12.2017) [cit. 2023-05-07]. Dostupné z: http://www.internetprovsechny.cz/nez-prisel-facebook-strucny-pruvodce-historii-socialnich-siti/

[7] SEDLÁK, Jan. *Proč Facebook zaplatil miliardu dolarů za Instagram*. E15 [online]. (11.04.2012) [cit. 2023-05-07]. Dostupné z: https://www.e15.cz/byznys/technologie-a-media/proc-facebook-zaplatil-miliardu-dolaru-za-instagram-758751

[8] KUŽNÍK, Jan. *Facebook koupil populární aplikaci WhatsApp za 16 miliard dolarů*. Idnes [online]. (19.02.2014) [cit. 2023-05-07]. Dostupné z: https://www.idnes.cz/mobil/aplikace/facebook-koupil-popularni-aplikaci-whatsapp-za-16-miliard-dolaru.A140219_235912_aplikace_kuz

[9] TIDY, Joe, Sophia SMITH GALER. *TikTok: The story of a social media giant*. BBC [online]. (05.08.2020) [cit. 2023-05-07]. Dostupné z: https://www.bbc.com/news/technology-53640724

[10] KRČMÁŘOVÁ, Barbora. *Děti a online rizika: sborník studií.* Praha: Sdružení Linka bezpečí, 2012. ISBN 978-80-904920-2-8.

[11] WOLF, Karel. *Jak vlastně Facebook vydělává peníze?*. Itbiz [online]. (13.03.2010) [cit. 2023-05-07]. Dostupné z: https://www.itbiz.cz/jak-vlastne-facebook-vydelava-penize

[12] DOČEKAL, Daniel, Jan MÜLLER, Anastázie HARRIS, Luboš HEGER. *Dítě v síti: manuál pro rodiče a učitele, kteří chtějí rozumět digitálnímu světu mladé generace*. Praha: Mladá fronta, 2019. Flowee. ISBN 978-80-204-5145-3.

[13] BLINKA, Lukáš. *Online závislosti: jednání jako droga?: online hry, sex a sociální sítě : diagnostika závislosti na internetu : prevence a léčba*. Praha: Grada, 2015. Psyché (Grada). ISBN 978-80-210-7975-5.

[14] GREENFIELD, Susan. *Změna myšlení: jak se mění naše mozky pod vlivem digitálních technologií.* Brno: BizBooks, 2016. ISBN 978-80-265-0450-4.

[15] Meta Platforms, Inc. *Facebook* [software]. 31.07.2023 [cit. 2023-08-08]. Dostupné z: https://play.google.com/store/apps/details?id=com.facebook.katana

[16] Meta Platforms, Inc. *Messenger* [software]. 02.08.2023 [cit. 2023-08-08]. Dostupné z: https://play.google.com/store/search?q=messenger&c=apps

[17] *The Social network* [česky Sociální síť] [film]. Režie David FINCHER. USA, 2010.

[18] Instagram. *Instagram* [software]. 31.07.2023 [cit. 2023-08-08]. Dostupné z: https://play.google.com/store/apps/details?id=com.instagram.android

[19] Snap Inc. *Snapchat* [software]. 02.08.2023 [cit. 2023-08-08]. Dostupné z: https://play.google.com/store/apps/details?id=com.snapchat.android

[20] HORYNA, Jan. *Instagram chce rovněž nabídnout placené členství pro přístup k exkluzivním Stories: To ale není vše, co se chystá.* Techarena [online]. (01.07.2021) [cit. 2023-05-07]. Dostupné z: https://www.techarena.cz/instagram-chce-rovnez-nabidnout-placene-clenstvi-pro-pristup-k-exkluzivnim-stories/n-4635/

[21] TikTok Pte. Ltd. *TikTok* [software]. 05.08.2023 [cit. 2023-08-08]. Dostupné z: https://play.google.com/store/apps/details?id=com.zhiliaoapp.musically

[22] JONES, Katie. *Ranked: The World's Most Downloaded Apps. Visual Capitalist* [online]. (25.01.2020) [cit. 2023-05-07]. Dostupné z: https://www.visualcapitalist.com/ranked-most-downloaded-apps/

[23] KONOPÁSKOVÁ, Michaela. *Aplikace BeReal vás vrátí do reality. V čem je její kouzlo?*. [online]. (11.05.2022) [cit. 2023-05-07]. Dostupné z: https://clickbait.cz/2022/05/11/aplikace-bereal-vas-vrati-do-reality-v-cem-je-jeji-kouzlo/

[24] BeReal. *BeReal* [software]. 22.07.2023 [cit. 2023-08-08]. Dostupné z: https://play.google.com/store/apps/details?id=com.bereal.ft

[25] Twitter, Inc. *Twitter* [software]. 22.06.2023 [cit. 2023-07-07]. Dostupné z: https://play.google.com/store/apps/details?id=com.twitter.android

[26] CONGER, Kate, Lauren HIRSCH. *Elon Musk Completes $44 Billion Deal to Own Twitter.* The New York Times [online]. (27.10.2022) [cit. 2023-05-07]. Dostupné z: https://www.nytimes.com/2022/10/27/technology/elon-musk-twitter-deal-complete.html

[27] MAC, Ryan, Tiffany HSU. *From Twitter to X: Elon Musk Begins Erasing an Iconic Internet Brand.* The New York Times [online]. (24.07.2023) [cit. 2023-08-08]. Dostupné z: https://www.nytimes.com/2023/07/24/technology/twitter-x-elon-musk.html

[28] LinkedIn. *LinkedIn* [software]. 02.08.2023 [cit. 2023-08-08]. Dostupné z: https://play.google.com/store/apps/details?id=com.linkedin.android

[29] SHEPHERD. Jack. *24 Essential Snapchat Statistics You Need to Know in 2023.* The Social Shepherd [online]. (26.07.2023) [cit. 2023-08-08]. Dostupné z: https://thesocialshepherd.com/blog/snapchat-statistics

[30] Google LLC*. Youtube* [software]. 04.08.2023 [cit. 2023-08-08]. Dostupné z: https://play.google.com/store/apps/details?id=com.google.android.youtube

[31] WhatsApp LLC*. WhatsApp* [software]. 03.08.2023 [cit. 2023-08-08]. Dostupné z: https://play.google.com/store/apps/details?id=com.whatsapp

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

[33] Buď safe online, 2020, *Selassie a Jirka Král – FAKE profily | Buď safe online na Slovensku,* YouTube video. [cit. 2023-05-07]. Dostupné z: https://www.youtube.com/watch?v=TtKuWmsCp6M

[34] SZOTKOWSKI, René. *Sexting u českých dětí*. Olomouc: Univerzita Palackého v Olomouci, 2020. ISBN 978-80-244-5793-2. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/odborne-studie/144-sexting-u-ceskych-deti-2020-szotkowski-kopecky-dobesova/file

[35] PETROWSKI, Thorsten. *Bezpečí na internetu: pro všechny*. Liberec: Dialog, 2014. Tajemství (Dialog). ISBN 978-80-7424-066-9.

[36] *Varování před podvodným webem*. Alza [online]. (10.11.2022) [cit. 2023-05-07]. Dostupné z: https://www.alza.cz/varovani-pred-podvodnym-webem

[37] RTHWLDN, 2019, *Co se stalo? / Sebrali mi YouTube účet,* YouTube video. [cit. 2023-05-07]. Dostupné z: https://www.youtube.com/watch?v=oYp1Y7Nma9M

[38] Jirka vysvětluje věci, 2023, *Jak podvodníci využívají psychologii,* YouTube video. [cit. 2023-05-07]. Dostupné z: https://www.youtube.com/watch?v=xYTrb-U0Dps

[39] MATĚJÍČEK, Pavel. *Proč je důležité aktualizovat*. Edu [online]. [cit. 2023-08-08] Dostupné z: https://www.edu.cz/proc-je-dulezite-aktualizovat/

[40] *What's the Difference Between Blacklisting, Whitelisting & Greylisting?.* Packetlabs [online]. (12. 08. 2022) [cit. 2023-08-08] Dostupné z: https://www.packetlabs.net/posts/blacklisting-whitelisting-greylisting/

[41] BEDROŠOVÁ, Marie, Renata HLAVOVÁ, Hana MACHÁČKOVÁ, Lenka DĚDKOVÁ, David ŠMAHEL. (2018). *České děti a dospívající na internetu: Zpráva z výzkumu na základních a středních školách. Projekt EU Kids Online IV – Česká republika.* Brno: Masarykova univerzita. Dostupné z: https://irtis.muni.cz/media/3115505/eu_kids_online_report.pdf

[42] KOPECKÝ, Kamil, René SZOTKOWSKI. *České děti v kybersvětě. Jak se chovají online a co jim hrozí?.* Olomouc: Univerzita Palackého, 2019. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/117-ceske-deti-v-kybersvete/file

[43] KOPECKÝ, Kamil, René SZOTKOWSKI, Pavla DOBEŠOVÁ. *Riziková komunikace a seznamování českých dětí v kyberprostoru*. Olomouc: Univerzita Palackého v Olomouci, 2021. ISBN 978-80-244-5914-1. Dostupné z: https://doivup.upol.cz/pdfs/doi/9900/04/3400.pdf

[44] KOPECKÝ, Kamil, René SZOTKOWSKI. *Online svět v dětských domovech – Výzkumná zpráva.* Olomouc: Pedagogická fakulta Univerzity Palackého, 2022. Dostupné z: https://e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/153-online-svet-v-detskych-domovech-2022-vyzkumna-zprava/file

[45] MŠMT. (2020). *Rámcový vzdělávací program pro obor vzdělání 63–41 – M/02 Obchodní akademie.* Praha: MŠMT. Dostupné z: https://www.edu.cz/wp-content/uploads/2020/08/63-41-M02_Obchodni_akademie_2020_zari_rev.pdf

[46] JORDÁNOVÁ, Veronika. *Sociální sítě a jejich bezpečnost z pohledu mladistvých* [online]. Zlín, 2019 [cit. 2023-08-05]. Dostupné z: https://theses.cz/id/gjdbtc/. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce Ing. Lukáš Králík.

[47] ZENG, Jing, Chrystal ABIDIN, Mike SCHÄFER. *Research perspectives on TikTok and its legacy apps: introduction*. International Journal of Communication. 2021, 15, 3161–3172. ISSN 1932-8036. Dostupné z: https://www.researchgate.net/publication/354157316 Research perspectives on TikTok and its legacy apps introduction

[48] RIEHM, Kira, Kenneth FEDER, Kayla TORMOHLEN, et al. *Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth*. *JAMA Psychiatry.* 2019, 76 (12), 1266–1273. Dostupné z: https://jamanetwork.com/journals/jamapsychiatry/fullarticle/2749480

[49] BOZZOLA, Elena, Spina GIULIA, Rino AGOSTINIANI, Sarah BARNI, Rocco RUSSO, Elena SCARPATO, Antonio DI MAURO, Antonella Vita DI STEFANO, Cinthia CARUSO, Giovanni CORSELLO, Annamaria STAIANO. *The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks*. Int J Environ Res Public Health. 2022 Aug 12, 19 (16): 9960. Dostupné z: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9407706/

[50] KURU, Ozan, Josh PASEK. *Improving social media measurement in surveys: Avoiding acquiescence bias in Facebook research*. Computers in Human Behavior. 2016, 57, 82–92. ISSN 0747-5632. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S0747563215302788.

[51] PELLEGRINO, Alfonso, Alessandro STASI, Veera BHATIASEVI. *Research trends in social media addiction and problematic social media use: A bibliometric analysis*. Frontiers in Psychiatry. 2022, 13. ISSN 1664-0640. Dostupné z: https://www.frontiersin.org/articles/10.3389/fpsyt.2022.1017506/full

[52] VOGELS, Emily. *Teens and Cyberbullying 2022* [online]. Pew Reseatch Center. 15.12.2022. [cit. 7. 5. 2023]. Dostupné z: https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam příloh

Příloha A: Dotazník

Bezpečnost na sociálních sítích

Dobrý den,

tímto Vás chci poprosit o vyplnění dotazníku níže. Dotazník Vám zabere pár minut a je součástí mé diplomové práce. Dotazník obsahuje 33 otázek, které jsou zaměřené na sociální sítě a jejich bezpečnost z pohledu mladistvých.

Dotazník je anonymní. U každé otázky vyberte alespoň jednu odpověď.

Pohlaví *

- Muž
- Žena

Kolik je Vám let? *

- < 12
- 13-14
- 15-16
- 17-18
- 19-20
- > 21

Víte, co jsou to sociální sítě? *

- Ano
- Ne

Které sociální sítě používáte? *

- [ ] Nepoužívám sociální sítě
- [ ] Facebook
- [ ] Instagram
- [ ] Snapchat
- [ ] YouTube
- [ ] TikTok
- [ ] Twitter
- [ ] Jiná…

Kterou sociální síť používáte nejčastěji? *

- ( ) Nepoužívám sociální sítě
- ( ) Facebook
- ( ) Instagram
- ( ) Snapchat
- ( ) YouTube
- ( ) TikTok
- ( ) Twitter
- ( ) Jiná…

Používáte telefon/tablet k připojení na sociální sítě? *

- ( ) Ano
- ( ) Ne

Kolik hodin přibližně denně strávíte na sociálních sítích? *

- ○ Méně než hodinu
- ○ 1 - 2
- ○ 3 - 4
- ○ 5 - 6
- ○ 7 - 8
- ○ Více něž 8 hodin

K čemu sociální sítě používáte? *

- ☐ Ke komunikaci s kamarády (chat, messenger, direkt message, aj.)
- ☐ Ke sdílení fotek
- ☐ Ke sdílení videí
- ☐ Ke sdílení nálady, statusů, citátů
- ☐ Jiná…

Pokud používáte Facebook/Instagram/Snapchat, využíváte možnosti stories? Zveřejněné fotky * či videa, které po 24 hodinách „zmizí".

- ○ Ano
- ○ Ne

Jaký obsah sdílíte ve stories? *

- ☐ Fotky
- ☐ Videa
- ☐ Statusy
- ☐ Jiná…

Sdílíte ve stories své selfies nebo fotky s přáteli? *

- ( ) Jen selfies
- ( ) Jen fotky s přáteli
- ( ) Sdílím selfies i fotky s přáteli
- ( ) Nesdílím selfies ani fotky s přáteli

Sdílíte své konkrétní informace? Bydliště, školu, kterou navštěvujete, svoji rodinu. *

- ( ) Ano
- ( ) Ne

Proč sdílíte své konkrétní informace? *

- [ ] Aby o mně lidé věděli co nejvíce
- [ ] Aby mě lépe vyhledávali moji kamarádi
- [ ] Protože to mají vyplněné moji kamarádi/spolužáci/známí
- [ ] Jen tak, baví mě to
- [ ] Jiná…

Jaký obsah sdílíte na sociálních sítích? *

Text stručné odpovědi

Jaký obsah nejvíce sdílíte na sociálních sítích? *

- ○ Nesdílím žádný obsah
- ○ Fotky (svoje, s kamarády, rodinou)
- ○ Videa (svoje, s kamarády, rodinou)
- ○ Fotky svých koníčků (jídlo, zvířata, sport…)
- ○ Videa svých koníčků (jídlo, zvířata, sport…)
- ○ Statusy, osobní pocity
- ○ Jiná…

Označujete své přátele na fotkách/ve videích? *

- ○ Ano
- ○ Ne

Víte, jak si ochránit své soukromí na sociálních sítích? *

- ○ Ano
- ○ Ne

Chráníte si soukromí na sociálních sítích pomocí nastavení? *

- ○ Ano, mám nastaveno, kdo může vidět můj obsah, co musím schválit, aby mohl někdo jiný vidět
- ○ Ano, mám nastaveno, kdo může vidět můj obsah
- ○ Nezajímám se o to/Je mi to jedno
- ○ Nic takového nastaveného nemám
- ○ Jiná…

Kolik máte na Facebooku přátel? *

Text stručné odpovědi

Znáte všechny tyto lidi osobně? (Facebook sledující) *

- Ano
- Ne
- Nemám Facebook

Kolik máte sledujících na Instagramu? *

Text stručné odpovědi

Znáte všechny tyto lidi osobně? (IG sledovatelé) *

- Ano
- Ne
- Nemám Instagram

Myslíte si, že se na sociálních sítích může člověk stát závislým? *

- Ano
- Ne

Komunikovali jste někdy s člověkem, kterého jste nikdy neviděli v reálném světě? *

- Ano, jednou
- Ano, komunikuji s ní / ním pravidelně
- Ne, nikdy

Sdělujete tomuto neznámému člověku své osobní údaje (věk, bydliště, školu, do které chodíte, informace o rodině…)? *

- ◯ Ano, však je to můj kamarád
- ◯ Sdělil/a jsem pouze své jméno a minimum dalších informací
- ◯ Ne, nesdělil/a jsem žádné konkrétní informace kromě přezdívky, kterou používám na sociálních sítích
- ◯ Ne, s nikým cizím nekomunikuji

Zažili jste někdy Vy nebo někdo ve Vašem okolí kyberšikanu? (šikana, která probíhá na internetu, na sociálních sítích pomocí komentářů, sdílení Vašich fotek, zesměšňování apod.) *

- ◯ Ano
- ◯ Ne

Jak tato kyberšikana probíhala? Prosím popište. *

Text dlouhé odpovědi

Zažili jste někdy zesměšnění na sociální síti? Někdo nelichotivě okomentoval Vaši fotku, status, cokoli. A jak jste se s tím vypořádali? *

- ◯ Ano, hodil/a jsem to za hlavu, stalo se to pouze jednou nebo minimálně
- ◯ Ano, stalo se to sice jednou nebo minimálně, ale zasáhlo mě to a začal/a jsem o sobě pochybovat, mrzel…
- ◯ Ano, stalo se to vícekrát, ale neřešil/a jsem to
- ◯ Ano, stalo se to vícekrát a řešil/a jsem to s rodiči/vyučujícím/starším bratrem či sestrou
- ◯ Ne, nikdy se mi toto nestalo
- ◯ Jiná…

Stalo se Vám někdy, že na Vás cíleně na internetu útočil jeden člověk/skupina lidí? Např. zesměšňující fotky, nepříjemné zprávy, apod. *

- Ano, jednou
- Ano, vícekrát
- Ne, nikdy se mi toto nestalo

Zesměšňoval Vás na internetu někdo, koho znáte/jste znali z reálného života? *

- Ano
- Ne

Řešili jste tuto věc s někým dospělým? *

- Ano, s rodiči
- Ano, s vyučujícím
- Ne, neřešil/a jsem to s dospělým
- Jiná...

Jak jste tuto věc řešili? *

Text stručné odpovědi

Co byste doporučil tomu, kdo je šikanován? Prosím vypište. *

Text stručné odpovědi

Příloha B: Edukační materiály pro výuku bezpečného používání sociálních sítí

Informační a komunikační technologie: První hodina

Příprava na výuku

Škola: 63–41 – M/02 Obchodní akademie	Třída: První ročník
Předmět: Informační a komunikační technologie	Tematický okruh: Práce v lokální síti, elektronická komunikace, komunikační a přenosové možnosti Internetu
Počet žáků: 16	Průřezové téma: Mediální výchova
Cíle hodiny: Žák vyjmenuje alespoň 5 platforem, které v digitálním světě slouží ke komunikaci mezi uživateli. Žák rozpozná alespoň 3 platformy, které v digitálním světě slouží ke komunikaci mezi uživateli, podle loga. Žák definuje výhody a nevýhody alespoň 1 této komunikační platformy z digitálního světa.	
Téma vyučovací hodiny: Bezpečné digitální prostředí	

Rozvíjené klíčové kompetence:

- Kompetence k učení: Žák najde potřebné informace
- Kompetence k učení: Žák vyhledává informace na internetu
- Kompetence k učení: Žák si své závěry ověřuje vždy v několika pramenech
- Kompetence k řešení problémů: Žák definuje, čemu konkrétně nerozumí a co mu dělá problém
- Kompetence komunikativní: Žák vyjadřuje své názory, slovem i písmem – kultivovanou formou
- Kompetence sociální a personální: Žák přijímá zodpovědnost za své chování, názory a postoje
- Kompetence sociální a personální: Žák se umí začlenit do skupiny a v té spolupracovat
- Kompetence sociální a personální: Žák respektuje práci ostatních
- Kompetence občanská: Žák organizuje spolupráci
- Kompetence k podnikavosti: Žák se ztotožňuje s cíli, které mu stanovil někdo jiný
- Kompetence k podnikavosti: Žák pojmenuje, jakými disponuje schopnostmi, znalostmi a dovednostmi

Pomůcky:

- Počítač a projektor
- Prezentace (Příloha)
- Flipchartový papír a psací potřeby
- Hra: Kufr (Prezentace + Příloha)
- Kartička se zadáním pro skupinovou práci (Příloha)

Metody:

- Slovní metoda – Vysvětlování, práce s textem, diskuse, prezentování vlastní tvorby
- Názorně demonstrační metoda – Instruktáž
- Praktická metoda – Vytváření dovedností, produkční metoda (tvorba plakátu)

Organizační formy:

- Hromadná (frontální) výuka
- Skupinová (kooperativní) výuka

Rozvržení výuky (časový harmonogram - 45 minut):

Časová orientace	**Průběh**	**Poznámky k rozboru**
1	Začátek hodiny – Zklidnění žáků, získání pozornosti	
2	Naladění atmosféry (Ice-breaking)	Slide 1
4	Opakování minulé hodiny	Slide 2
10	Seznámení žáků s průběhem dnešní hodiny	Slide 3
12	Motivace – Proč je důležité učit se o bezpečnosti v digitálním světě?	Slide 4
15	Expozice – Vlastnosti digitálního světa	Slide 5–7
25	Aktivita – Skupinová práce – Rozdělení do skupin	Slide 8
28	Aktivita – Skupinová práce – Tvorba plakátu, zápis do TK	Slide 9
40	Rekapitulace průběhu dnešní hodiny a slovní hodnocení žáků	Slide 10
43	Příprava na průběh příští hodiny	Slide 11
45	Konec hodiny – Rozloučení se s žáky	Slide 12

Průběh hodiny:

1 - Začátek hodiny – Zklidnění žáků, získání pozornosti

Učitel – Postaví se před třídu a čeká, než se žáci ztiší a postaví. Následně pozdraví žáky.

Žák – Ztiší se a svým postavením dá najevo, že vnímá přítomnost učitele a začátek hodiny.

2 - Naladění atmosféry - Ice-breaking (Slide 1)

Učitel – Vytváří příjemnou atmosféru – Okomentuje počasí; zeptá se na náladu žáků…

Během ice-breakingu se učitel přihlásí do počítače a spustí prezentaci.

Žák – Koncentruje se a komunikuje s učitelem.

4 - Opakování minulé hodiny (Slide 2)

Učitel – Opakuje látku pomocí hry „Kufr“. Vybere dva žáky, jeden z nich napovídá pojmy promítnuté v prezentaci, druhý se je snaží uhádnout. Učitel, poté co žák uhádne všechny pojmy, ještě jednou zopakuje klíčové znalosti z minulé hodiny (Příloha: Kufr – Internet).

Žák – Formuluje a rozpoznává pojmy. Pociťuje úspěch, uklidní se, připomíná si znalosti, které už zná. Pokud žák chyběl na předchozí hodině, dozví se nyní důležité informace z minulé hodiny.

10 - Seznámení žáků s průběhem dnešní hodiny (Slide 3)

Učitel – Seznámí žáky s průběhem dnešní hodiny, řekne číslo, téma, cíl a průběh hodiny.

Žák – Seznámí se s harmonogramem dnešní hodiny.

12 - Motivace a diskuse – Proč je důležité učit se o bezpečnosti v digitálním světě? (Slide 4)

Učitel – Motivuje žáky pomocí diskuse na téma: „Proč je důležité učit se o bezpečnosti v digitálním světě?“ Během diskuse se snaží vyvolat vnitřní motivaci v žácích k tématu hodiny. Učitel nápady žáků chválí.

Žák – Aktivně se zapojuje do diskuse. Žák si samostatně vymyslí důvody, proč by se měl o téma bezpečnosti v digitálním světě zajímat.

15 – Expozice – Žáci si osvojují nové poznatky pod vedením učitele (Slide 5–7)

Učitel – Předává základní teoretické znalosti o vlastnostech digitálního světa.

Žák – Osvojuje si základní teoretické poznatky učiva.

25 - Aktivita – Skupinová práce – Rozdělení do skupin (Slide 8)

Učitel – Seznámí žáky s cílem skupinové práce. Poté rozdělí žáky do skupin podle toho, které sociální sítě používají.

Žák – Rozdělí se do skupin, vyslechne instrukce a začne pracovat na skupinové práci.

Skupinová práce – Žáci mají ve skupině vyhledat informace o konkrétní sociální síti a následně tyto informace graficky ztvárnit na flipchartový papír.

28 – Aktivita – Skupinová práce, zápis do TK (Slide 9)

Učitel – Během aktivity kontroluje její průběh a napomáhá žákům. Zapíše do třídní knihy.

Žák – Pracuje ve skupině, získává informace, ztvárňuje informace na flipchartový papír.

40 - Rekapitulace průběhu dnešní hodiny a slovní hodnocení žáků (Slide 10)

Učitel – Připomene etapy dnešní hodiny, zopakuje důležité informace, zhodnotí práci žáků, získává jejich zpětnou vazbu.

Žák – Aktivně se podílí na rekapitulaci dnešní hodiny a předává zpětnou vazbu učiteli.

43 – Příprava na průběh příští hodiny (Slide 11)

Učitel – Seznámí žáky s tématem příští hodiny.

Žák – Je seznámen s průběhem příští hodiny.

45 – Konec hodiny – Rozloučení se s žáky (Slide 12)

Učitel – Rozloučí se s žáky, ti se zvoněním mohou opouštět učebnu.

Žák – Uklidí si svůj pracovní prostor a se zvoněním opouští učebnu.

Příloha:

Kufr – Internet

1. Internet
2. World Wide Web
3. Prohlížeč
4. Server
5. E-mail
6. Hacker
7. Firewall
8. Malware
9. Sociální sítě
10. Cloud

Kartička se zadáním pro skupinovou práci

1. **Facebook**
   - Historie a vznik
   - Charakteristika a funkce
   - Výhody a nevýhody
   - Příklady použití

2. **Instagram**
   - Historie a vznik
   - Charakteristika a funkce
   - Výhody a nevýhody
   - Příklady použití

3. **TikTok**
   - Historie a vznik
   - Charakteristika a funkce
   - Výhody a nevýhody
   - Příklady použití

4. **Twitter**
   - Historie a vznik
   - Charakteristika a funkce
   - Výhody a nevýhody
   - Příklady použití

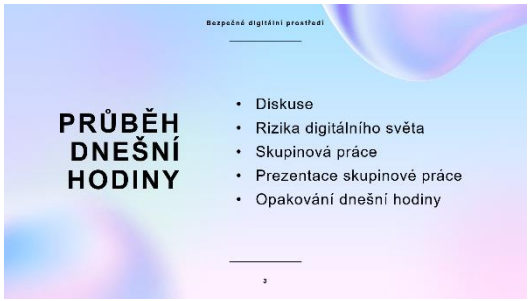
5. **Snapchat**
    - Historie a vznik
    - Charakteristika a funkce
    - Výhody a nevýhody
    - Příklady použití

6. **YouTube**
    - Historie a vznik
    - Charakteristika a funkce
    - Výhody a nevýhody
    - Příklady použit

Prezentace

Slide 1

Slide 2



Slide 3

Slide 4

Slide 5

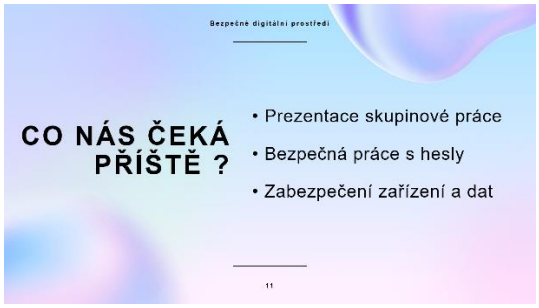
Slide 6

Slide 7

Slide 8

Slide 9

Slide 10



Slide 11

Slide 12

Slide 13

Informační a komunikační technologie: Druhá hodina

Příprava na výuku

Škola: 63–41 – M/02 Obchodní akademie	Třída: První ročník
Předmět: Informační a komunikační technologie	Tematický okruh: Práce v lokální síti, elektronická komunikace, komunikační a přenosové možnosti Internetu
Počet žáků: 16	Průřezové téma: Mediální výchova
Cíle hodiny: Žák vyjmenuje alespoň 3 pravidla pro bezpečnou práci s hesly. Žák vyjmenuje alespoň 2 pravidla pro zabezpečení zařízení. Žák vyjmenuje alespoň 2 pravidla pro zabezpečení dat.	
Téma vyučovací hodiny: Bezpečná práce s hesly, zabezpečení zařízení a dat	

Rozvíjené klíčové kompetence:

- Kompetence k učení: Žák najde potřebné informace
- Kompetence k učení: Žák vyhledává informace na internetu
- Kompetence k učení: Žák si své závěry ověřuje vždy v několika pramenech
- Kompetence k řešení problémů: Žák definuje, čemu konkrétně nerozumí a co mu dělá problém
- Kompetence sociální a personální: Žák přijímá zodpovědnost za své chování, názory a postoje
- Kompetence sociální a personální: Žák respektuje práci ostatních
- Kompetence občanská: Žák srozumitelně předkládá získané informace
- Kompetence k podnikavosti: Žák se ztotožňuje s cíli, které mu stanovil někdo jiný
- Kompetence k podnikavosti: Žák pojmenuje, jakými disponuje schopnostmi, znalostmi a dovednostmi

Pomůcky:

- Počítač a projektor
- Prezentace (Příloha)

Metody:

- Slovní metoda – Vysvětlování, práce s textem
- Názorně demonstrační metoda – Instruktáž
- Samostatná práce žáků – Prezentace

Organizační formy:

- Hromadná (frontální) výuka
- Skupinová (kooperativní) výuka
- Samostatná práce

Rozvržení výuky (časový harmonogram - 45 minut):

Časová orientace	Průběh	Poznámky k rozboru
1	Začátek hodiny – Zklidnění žáků, získání pozornosti	
2	Přihlášení se do počítačů	
3	Naladění atmosféry (Ice-breaking)	Slide 1
5	Opakování minulé hodiny (+ Motivace)	Slide 2
8	Seznámení žáků s průběhem dnešní hodiny	Slide 3
10	Aplikace a fixace – Prezentace skupinových prací (plakátů)	Slide 4-10
22	Fixace – Zhodnocení skupinové práce žáků	Slide 4-10
25	Diskuse – Získání zpětné vazby o dosavadních znalostech žáků	Slide 11
28	Expozice – Práce s hesly	Slide 12-13
33	Aplikace – Tvorba hesla, zápis do TK	Slide 14
40	Fixace – Zopakování řečených a klíčových informací z hodiny	Slide 12-13
42	Rekapitulace průběhu dnešní hodiny a slovní hodnocení žáků	Slide 15
44	Příprava na průběh příští hodiny	Slide 16
45	Konec hodiny – Rozloučení se s žáky	Slide 17

Průběh hodiny:

1 - Začátek hodiny – Zklidnění žáků, získání pozornosti

Učitel – Postaví se před třídu a čeká, než se žáci ztiší a postaví. Následně pozdraví žáky.

Žák – Ztiší se a svým postavením dá najevo, že vnímá přítomnost učitele a začátek hodiny.

2 - Přihlášení se do počítačů

Učitel – Přihlásí se do počítače. Řeší případné problémy s funkčností počítačů.

Žák – Přihlásí se do počítače.

3 - Naladění atmosféry - Ice-breaking (Slide 1)

Učitel – Vytváří příjemnou atmosféru – Okomentuje počasí; zeptá se na náladu žáků… Během ice-breakingu učitel spustí prezentaci.

Žák – Uklidní se a komunikuje s učitelem.

5 - Opakování minulé hodiny + Motivace (Slide 2)

Učitel – Opakuje téma minulé hodiny pomocí otázek položených žákům, kteří byli na minulé hodině přítomni. Během opakování učitel motivuje žáky tím, že připomene jejich odpovědi z minulé hodiny na otázku: „Proč je důležité učit se o bezpečnosti v digitálním světě?“

Žák – Pociťuje úspěch, uklidní se, připomíná si znalosti, které už zná. Pokud žák chyběl na předchozí hodině, dozví se nyní důležité informace z minulé hodiny.

8 - Seznámení žáků s průběhem dnešní hodiny (Slide 3)

Učitel – Seznámí žáky s průběhem dnešní hodiny, řekne číslo, téma, cíl a průběh hodiny.

Žák – Seznámí se s harmonogramem dnešní hodiny a uvědomuje si užitečnost tématu.

10 – Aplikace – Prezentace skupinových prací - plakátů (Slide 4-10)

Učitel – Moderuje prezentaci jednotlivých skupin, doplňuje případné chybějící informace.

Žák – Prezentuje skupinovou práci, zapisuje si informace prezentované jinými skupinami.

22 – Fixace – Zhodnocení skupinové práce žáků (Slide 4-10)

Učitel – Systematizuje řečené informace. Nechá žáky samostatně zhodnotit jejich dosavadní práci ve skupině, kterou také okomentuje.

Žák – Aktivně se podílí na rekapitulaci informací a realisticky ohodnotí svou práci ve skupině.

25 – Diskuse – Získání zpětné vazby o dosavadních znalostech žáků (Slide 11)

Učitel – Získává zpětnou vazbu o dosavadních znalostech žáků na téma bezpečná práce s hesly, zabezpečení zařízení a dat. Pokládá žákům otázky:

- Jaká znáte pravidla pro používání hesel?
- Co jsou to biometrická hesla?
- Co je to dvoufázové ověření?

Žák – Aktivně se zapojuje do diskuse a sdílí své dosavadní zkušenosti z práce s hesly.

28 - Expozice – Práce s hesly (Slide 12–13)

Učitel – Seznámí žáky s pravidly pro bezpečné zacházení s hesly a ukáže jim postupy pro vytvoření bezpečného hesla. Tímto postupem je „algoritmizované“ heslo. Při tomto postupu si žák vymyslí libovolnou větu, například: „Mám rád vanilkovou zmrzlinu“, a tuto větu následně upraví, například tak, že bude postupně psát počáteční písmena jednotlivých slov s tím, že u každého dalšího slova přidá jedno písmeno a současně použije místo mezery symbol čísla nebo speciální znak. Zároveň v hesle náhodně použije velká písmena. Vytvořené heslo může vypadat například takto: m4Ra#vAN9zmRz!.

Žák – Získá teoretické znalosti o zacházení s hesly.

33 - Aplikace – Tvorba hesla, zápis do TK (Slide 14)

Učitel – Seznámí žáky s nástrojem pro generování hesel: https://www.eset.com/cz/generator-hesel/ a napomáhá jim při tvorbě vlastních hesel. Zapíše do třídní knihy.

Žák – Tvoří vlastní heslo podle řečených pravidel. Bezpečnost svého hesla zkontroluje pomocí nástroje na webu: https://www.passwordmonster.com/ .

40 – Fixace – Zopakování řečených a klíčových informací z hodiny (Slide 12–13)

Učitel – Sumarizuje řečené informace.

Žák – Doplňuje si svůj zápis o chybějící informace.

42 - Rekapitulace průběhu dnešní hodiny a slovní hodnocení žáků (Slide 15)

Učitel – Připomene etapy dnešní hodiny, zopakuje důležité informace, zhodnotí práci žáků, získává jejich zpětnou vazbu.

Žák – Aktivně se podílí na rekapitulaci dnešní hodiny a předává zpětnou vazbu učiteli.

44 - Příprava na průběh příští hodiny (Slide 16)

Učitel – Seznamuje žáky s tématem příští hodiny.

Žák – Je seznámen s průběhem příští hodiny a odhlašuje se z počítače.

45 – Konec hodiny – Rozloučení se s žáky (Slide 17)

Učitel – Rozloučí se s žáky, ti se zvoněním mohou opouštět učebnu.

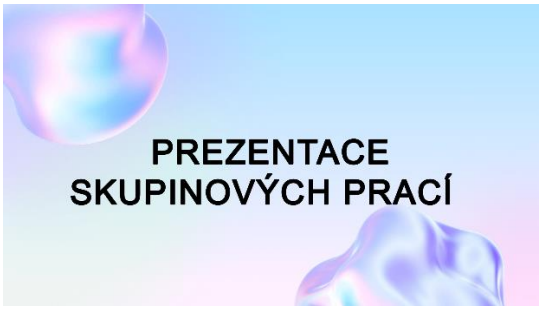
Žák – Uklidí si svůj pracovní prostor a se zvoněním opouští učebnu.

Prezentace

Slide 1

Slide 2

Slide 3



Slide 4

Slide 5

Slide 6

Slide 7

Slide 8

Slide 9

Slide 10

Slide 11

Slide 12

Slide 13

Slide 14

Slide 15

Slide 16

Slide 17

Slide 18

Informační a komunikační technologie: Třetí hodina

Příprava na výuku

Škola: 63–41 – M/02 Obchodní akademie	Třída: První ročník
Předmět: Informační a komunikační technologie	Tematický okruh: Práce v lokální síti, elektronická komunikace, komunikační a přenosové možnosti Internetu
Počet žáků: 16	Průřezové téma: Mediální výchova
Cíle hodiny: Žák vyjmenuje alespoň 3 způsoby útoků na počítačová zařízení. Žák vyjmenuje alespoň 3 sociotechnické metody útočníků. Žák vyjmenuje alespoň 3 způsoby, jak se proti sociotechnickým metodám útoku bránit.	
Téma vyučovací hodiny: Způsoby útoků na sociálních sítích – cíle a metody útočníků	

Rozvíjené klíčové kompetence:

- Kompetence k učení: Žák najde potřebné informace
- Kompetence k řešení problémů: Žák definuje, čemu konkrétně nerozumí a co mu dělá problém
- Kompetence komunikativní: Žák vyjadřuje své názory, slovem i písmem – kultivovanou formou
- Kompetence sociální a personální: Žák přijímá zodpovědnost za své chování, názory a postoje
- Kompetence sociální a personální: Žák respektuje práci ostatních
- Kompetence občanská: Žák srozumitelně předkládá získané informace
- Kompetence k podnikavosti: Žák pojmenuje, jakými disponuje schopnostmi, znalostmi a dovednostmi

Pomůcky:

- Počítač a projektor
- Prezentace (Příloha)

Metody:

- Slovní metoda – Vysvětlování, práce s videem, diskuse
- Názorně demonstrační metoda – Instruktáž

Organizační formy:

- Hromadná (frontální) výuka

Rozvržení výuky (časový harmonogram - 45 minut):

Časová orientace	Průběh	Poznámky k rozboru
1	Začátek hodiny – Zklidnění žáků, získání pozornosti	
2	Naladění atmosféry (Ice-breaking), zápis do TK	Slide 1
3	Opakování minulé hodiny	Slide 2
6	Seznámení žáků s průběhem dnešní hodiny (+ Motivace)	Slide 3
9	Diskuse – Způsoby útoků v digitálním světě	Slide 4
13	Expozice – Cíle a sociotechnické metody útočníků	Slide 5
17	Výklad s prvky diskuse – Kyberšikana	Slide 6
20	Výklad s prvky diskuse – Sexting	Slide 7
23	Video: Phishing a vishing	Slide 8
25	Výklad s prvky diskuse – Phishing a vishing	Slide 9
28	Video: Kybergrooming	Slide 10
34	Výklad s prvky diskuse – Kybergrooming	Slide 11
37	Fixace – Zopakování řečených a klíčových informací z hodiny	Slide 12
41	Rekapitulace průběhu dnešní hodiny a slovní hodnocení žáků	Slide 13
43	Příprava na průběh příští hodiny	Slide 14
45	Konec hodiny – Rozloučení se s žáky	Slide 15

Průběh hodiny:

1 - Začátek hodiny – Zklidnění žáků, získání pozornosti

Učitel – Postaví se před třídu a čeká, než se žáci ztiší a postaví. Následně pozdraví žáky.

Žák – Ztiší se a svým postavením dá najevo, že vnímá přítomnost učitele a začátek hodiny.

2 - Naladění atmosféry (Ice-breaking), zápis do TK (Slide 1)

Učitel – Vytváří příjemnou atmosféru – Okomentuje počasí; zeptá se na náladu žáků… Během ice-breakingu se učitel přihlásí do počítače a spustí prezentaci. Zapíše do třídní knihy.

Žák – Koncentruje se a komunikuje s učitelem.

3 - Opakování minulé hodiny (Slide 2)

Učitel – Opakuje téma minulé hodiny pomocí otázek pokládaných žákům, kteří byli na minulé hodině přítomni.

Žák – Aktivně se účastní rekapitulace minulé hodiny. Pociťuje úspěch, uklidní se, připomíná si znalosti, které už zná. Pokud žák chyběl na předchozí hodině, dozví se nyní důležité informace z minulé hodiny.

6 - Seznámení žáků s průběhem dnešní hodiny - Motivace (Slide 3)

Učitel – Seznámí žáky s průběhem dnešní hodiny, řekne číslo, téma, cíl a průběh hodiny. Během toho také motivuje žáky, snaží se v nich vyvolat vnitřní motivaci k tématu hodiny.

Žák – Seznámí se s harmonogramem dnešní hodiny a uvědomuje si užitečnost tématu.

9 – Diskuse – Způsoby útoků v digitálním světě (Slide 4)

Učitel – Vede diskusi na téma rizika v digitálním světě.

Žák – Aktivně se účastní diskuse na téma rizika v digitálním světě.

13 - Expozice – Cíle a sociotechnické metody útočníků (Slide 5)

Učitel – Předává základní teoretické znalosti o způsobech útoků na počítačové zařízení a o cílech a sociotechnických metodách útočníků.

Žák – Dává pozor a zapisuje si tyto základní teoretické poznatky.

17 - Výklad s prvky diskuse – Kyberšikana (Slide 6)

Učitel – Vede výklad na téma kyberšikana, během kterého využívá aktivizační prvky, aby zapojil žáky do procesu vzdělávání.

Žák – Získává nové informace a aktivně se účastní průběhu hodiny.

20 - Výklad s prvky diskuse – Sexting (Slide 7)

Učitel – Vede výklad na téma sexting, během kterého využívá aktivizační prvky, aby zapojil žáky do procesu vzdělávání.

Žák – Získává nové informace a aktivně se účastní průběhu hodiny.

23 – Video: Phishing a vishing (Slide 8)

Učitel – Pustí video, které názornou formou prezentuje rizika phishingu.

Žák – Pomocí videa se seznámí s problematikou phishingu.

Video – https://www.youtube.com/watch?v=00hpRjfbM0A

25 - Výklad s prvky diskuse – Phishing a vishing (Slide 9)

Učitel – Vede výklad na téma phishing a vishing, během kterého využívá aktivizační prvky, aby zapojil žáky do procesu vzdělávání.

Žák – Získává nové informace a aktivně se účastní průběhu hodiny.

28 – Video: Kybergrooming (Slide 10)

Učitel – Pustí video, které názornou formou prezentuje rizika kybergroomingu.

Žák – Pomocí videa se seznámí s problematikou kybergroomingu.

Video – https://www.youtube.com/watch?v=fcLoLnhkLIE

34 - Výklad s prvky diskuse – Kybergrooming (Slide 11)

Učitel – Vede výklad na téma kybergrooming, během kterého využívá aktivizační prvky, aby zapojil žáky do procesu vzdělávání.

Žák – Získává nové informace a aktivně se účastní průběhu hodiny.

37 – Fixace – Zopakování řečených a klíčových informací z hodiny (Slide 12)

Učitel – Sumarizuje řečené informace.

Žák – Doplňuje si svůj zápis o chybějící informace.

41 - Rekapitulace průběhu dnešní hodiny a slovní hodnocení žáků (Slide 13)

Učitel – Připomene etapy dnešní hodiny, zopakuje důležité informace, zhodnotí práci žáků, získává jejich zpětnou vazbu.

Žák – Aktivně se podílí na rekapitulaci dnešní hodiny a předává zpětnou vazbu učiteli.

43 - Příprava na průběh příští hodiny (Slide 14)

Učitel – Seznamuje žáky s tématem příští hodiny.

Žák – Je seznámen s průběhem příští hodiny a odhlašuje se z počítače.

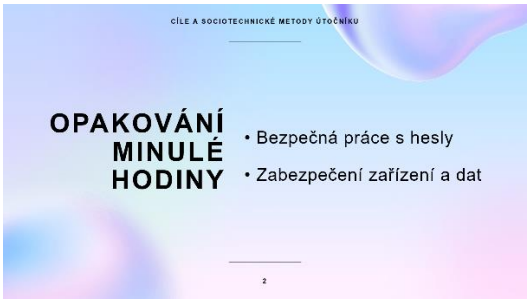
45 – Konec hodiny – Rozloučení se s žáky (Slide 15)

Učitel – Rozloučí se s žáky, ti se zvoněním mohou opouštět učebnu.

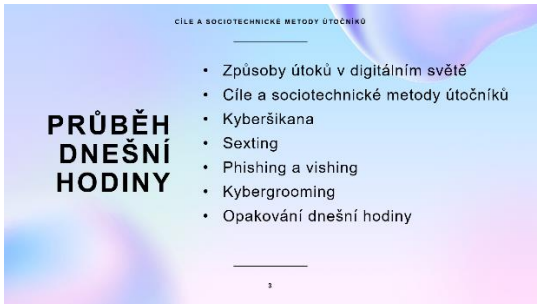
Žák – Uklidí si svůj pracovní prostor a se zvoněním opouští učebnu.

Prezentace

Slide 1



Slide 2

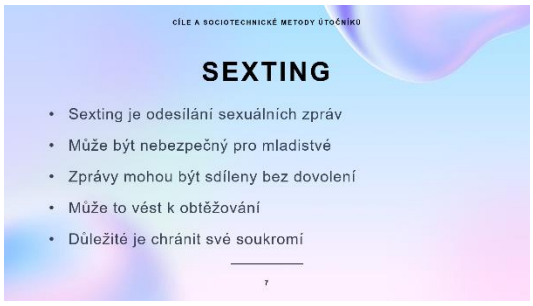


Slide 3

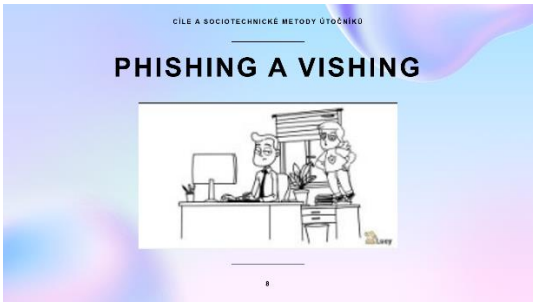
Slide 4

Slide 5

Slide 6



Slide 7



Slide 8

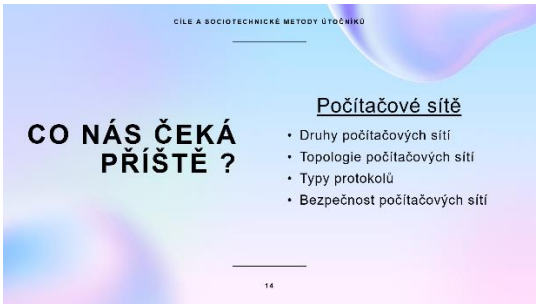
Slide 9

Slide 10

Slide 11

Slide 12

Slide 13



Slide 14

Slide 15

Slide 16

Společenskovědní vzdělávání: První hodina

Příprava na výuku

Škola: 63–41 – M/02 Obchodní akademie	Třída: Druhý ročník
Předmět: Společenskovědní vzdělávání	Tematický okruh: Člověk jako občan
Počet žáků: 30	Průřezové téma: Mediální výchova
Cíle hodiny: Žák vyjmenuje 3 rizika, která hrozí při komunikaci na sociálních sítích. Žák definuje a vysvětlí 1 riziko, které se vyskytuje při komunikaci na internetu. Žák identifikuje alespoň 1 rizikové chování na sociálních sítích na základě příběhu.	
Téma vyučovací hodiny: Bezpečná komunikace na sociálních sítích	

Rozvíjené klíčové kompetence:

- Kompetence k učení: Žák najde potřebné informace
- Kompetence k učení: Žák vyhledává informace na internetu
- Kompetence k učení: Žák si své závěry ověřuje vždy v několika pramenech
- Kompetence k řešení problémů: Žák definuje, čemu konkrétně nerozumí a co mu dělá problém
- Kompetence komunikativní: Žák vyjadřuje své názory, slovem i písmem – kultivovanou formou
- Kompetence sociální a personální: Žák přijímá zodpovědnost za své chování, názory a postoje
- Kompetence sociální a personální: Žák se umí začlenit do skupiny a v té spolupracovat
- Kompetence sociální a personální: Žák respektuje práci ostatních
- Kompetence občanská: Žák srozumitelně předkládá získané informace
- Kompetence občanská: Žák organizuje spolupráci
- Kompetence k podnikavosti: Žák se ztotožňuje s cíli, které mu stanovil někdo jiný
- Kompetence k podnikavosti: Žák pojmenuje, jakými disponuje schopnostmi, znalostmi a dovednostmi

Pomůcky:

- Počítač a projektor
- Prezentace (Příloha)
- Připravený (motivační) příběh (Příloha)
- Kartička se zadáním pro skupinovou práci (Příloha)
- Flipchartový papír a psací potřeby

Metody:

- Slovní metoda – Práce s textem, diskuse, deset slov, prezentování vlastní tvorby
- Názorně demonstrační metoda – Instruktáž
- Praktická metoda – Vytváření dovedností, produkční metoda (tvorba plakátu)

Organizační formy:

- Hromadná (frontální) výuka
- Skupinová (kooperativní) výuka

Rozvržení výuky (časový harmonogram - 45 minut):

Časová orientace	**Průběh**	**Poznámky k rozboru**
1	Začátek hodiny – Zklidnění žáků, získání pozornosti	
2	Naladění atmosféry (Ice-breaking)	Slide 1
4	Opakování minulé hodiny – Deset slov	Slide 2–3
10	Seznámení žáků s průběhem dnešní hodiny	Slide 4
12	Motivace – Komunikace na sociálních sítích	Slide 5
14	Diskuse – Téma: Bezpečná komunikace na sociálních sítích	Slide 6
18	Expozice – Žáci si osvojují nové poznatky pod vedením učitele	Slide 7
23	Aktivita – Skupinová práce – Rozdělení do skupin	Slide 8-9
25	Aktivita – Skupinová práce – Tvorba plakátu, zápis do TK	Slide 9
38	Rekapitulace průběhu dnešní hodiny a slovní hodnocení žáků	Slide 10
43	Příprava na průběh příští hodiny	Slide 11
45	Konec hodiny – Rozloučení se s žáky	Slide 12

Průběh hodiny:

1 - Začátek hodiny – Zklidnění žáků, získání pozornosti

Učitel – Postaví se před třídu a čeká, než se žáci ztiší a postaví. Následně pozdraví žáky.

Žák – Ztiší se a svým postavením dá najevo, že vnímá přítomnost učitele a začátek hodiny.

2 - Naladění atmosféry - Ice-breaking (Slide 1)

Učitel – Vytváří příjemnou atmosféru – Okomentuje počasí; zeptá se na náladu žáků… Během ice-breakingu se učitel přihlásí do počítače a spustí prezentaci.

Žák – Koncentruje se a komunikuje s učitelem.

4 - Opakování minulé hodiny (Slide 2–3)

Učitel – Opakuje látku pomocí metody deset slov. Žák si během této metody připraví větu přesně o deseti slovech. Tato věta má obsahovat alespoň jednu novou informaci z minulé hodiny. Věty následně žák sdílí se svými spolužáky. Učitel poté, co žáci řeknou příslušné informace, ještě jednou zopakuje klíčové znalosti z minulé hodiny.

Žák – Pociťuje úspěch, uklidní se, připomíná si znalosti, které už zná. Pokud žák chyběl na předchozí hodině, dozví se nyní důležité informace z minulé hodiny.

10 - Seznámení žáků s průběhem dnešní hodiny (Slide 4)

Učitel – Seznámí žáky s průběhem dnešní hodiny, řekne číslo, téma, cíl a průběh hodiny.

Žák – Seznámí se s harmonogramem dnešní hodiny a uvědomuje si užitečnost tématu.

12 - Motivace – Komunikace na sociálních sítích (Slide 5)

Učitel – Motivuje žáky, snaží se v žácích vyvolat vnitřní motivaci k tématu hodiny. Učitel k tomu používá otevřené otázky a na závěr vypráví žákům příběh, na kterém demonstruje důležitost bezpečnosti na sociálních sítích (Příloha: Příběh „O Elišce“).

Žák – Dává pozor, získává informace pro nadcházející diskusi.

14 – Diskuse – Téma: Rizika při komunikaci na sociálních sítích (Slide 6)

Učitel – Vede diskusi na téma „Bezpečná komunikace na sociálních sítích“ s cílem zjistit dosavadní znalosti žáků (Příloha: Diskusní otázky).

Žák – Aktivně se účastní diskuse a prezentuje své dosavadní znalosti a zkušenosti.

18 - Expozice – Žáci si osvojují nové poznatky pod vedením učitele (Slide 7)

Učitel – Předává základní teoretické znalosti o bezpečnostních rizicích při komunikaci na sociálních sítích a internetu.

Žák – Dává pozor a zapisuje si základní teoretické poznatky.

23 - Aktivita – Skupinová práce – Rozdělení do skupin (Slide 8-9)

Učitel – Seznámí žáky s cílem skupinové práce a poté je rozdělí do skupin pomocí sáčku s barevnými víčky.

Žák – Vytvoří skupiny, vyslechne instrukce a začne pracovat na skupinové práci.

Skupinová práce – Žáci si vylosují kartičku se zadáním skupinové práce, během které mají vyhledat informace o konkrétním riziku při komunikaci na sociálních sítích a následně tyto informace graficky ztvárnit na flipchartový papír (Příloha: Kartička se zadáním pro skupinovou práci).

25 – Aktivita – Skupinová práce – Tvorba plakátu, zápis do TK (Slide 9)

Učitel – Kontroluje průběh skupinové práce a napomáhá žákům. Zapíše do třídní knihy.

Žák – Pracuje ve skupině, získává informace, ztvárňuje informace na flipchartový papír.

38 - Rekapitulace průběhu dnešní hodiny a slovní hodnocení žáků (Slide 10)

Učitel – Připomene etapy dnešní hodiny, zopakuje důležité informace dnešní hodiny. Nechá žáky samostatně zhodnotit jejich dosavadní práci ve skupině, kterou také okomentuje.

Žák – Aktivně se podílí na rekapitulaci dnešní hodiny a předává zpětnou vazbu učiteli.

43 - Příprava na průběh příští hodiny (Slide 11)

Učitel – Seznámí žáky s tématem příští hodiny.

Žák – Je seznámen s průběhem příští hodiny.

45 – Konec hodiny – Rozloučení se s žáky (Slide 12)

Učitel – Rozloučí se s žáky, ti se zvoněním mohou opouštět učebnu.

Žák – Uklidí si svůj pracovní prostor a se zvoněním opouští učebnu.

Příloha:

Příběh „O Elišce“

Venku zuřila zima a Eliška (hrdinka našeho příběhu) se nudila. Zatoužila po něčem zajímavém, a tak se rozhodla, že prozkoumá sociální sítě. Vyhledávala novinky o svých přátelích, ale brzy zjistila, že se u nich nic zajímavého neděje. Rozhodla se tedy, že prozkoumá internetová fóra a online komunity. Hledala, hledala a najednou narazila na komunitu, ve které se lidé svěřovali se svými zájmy a koníčky. Byla nadšená, protože zde byla spousta lidí, kteří sdíleli její zájmy. Eliška se rozhodla přidat se do této komunity a začít komunikovat s ostatními členy. Zpočátku to bylo skvělé. Eliška se přes internet seznámila s lidmi, kteří sdíleli její zájmy, a dokonce se s nimi sblížila. Avšak brzy začala porušovat pravidla bezpečného chování na internetu. Začala sdílet své osobní údaje a fotografie, aniž by přemýšlela o následcích. Neuvědomila si, že by je mohli někteří uživatelé zneužít a že se tak vystavuje nebezpečí. Když se jednoho dne přihlásila na svůj e-mail, zjistila, že byla obětí kybernetického útoku. Útočníci získali přístup k jejímu účtu. Eliška byla vyděšená a snažila se tuto situaci řešit, ale bylo již pozdě. Útočníci využili přístupu k jejímu účtu a začali posílat Eliščiným přátelům nevyžádané zprávy s viry.

Diskusní otázky

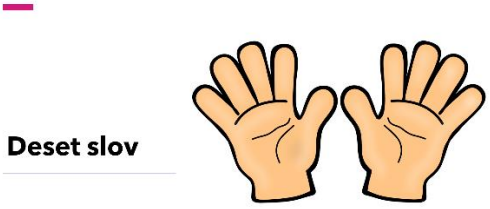
1. Čím ohrozila Eliška svoji bezpečnost na internetu?
2. Jak se cítila poté, co jí útočníci ukradli účet? Jak byste se cítili vy?
3. K čemu použili útočníci Eliščin účet?
4. Jak může komunikace na sociálních sítích ovlivnit náš reálný život?
5. Jaká jsou rizika při sdílení osobních údajů a fotografií na sociálních sítích?
6. Jaké jsou různé druhy kybernetických útoků a jak se před nimi můžeme chránit?

Kartička se zadáním pro skupinovou práci

1. **Sdílení osobních údajů** – Riziko zneužití osobních údajů, jako jsou jméno, bydliště, telefonní číslo, e-mailová adresa a další citlivé informace.
   Definujte dané riziko. Uveďte, jak k němu dochází a jak se proti němu bránit.
2. **Kyberšikana** – Riziko šikany a obtěžování prostřednictvím internetu, jako jsou například urážky, pomluvy a výhrůžky.
   Definujte dané riziko. Uveďte, jak k němu dochází a jak se proti němu bránit.
3. **Phishingové a vishingové útoky** – Riziko podvodů, které mají za cíl získat citlivé informace, jako jsou hesla nebo bankovní údaje.
   Definujte dané riziko. Uveďte, jak k němu dochází a jak se proti němu bránit.
4. **Sexting** – Riziko sdílení intimních fotografií nebo videí prostřednictvím internetu. Definujte dané riziko. Uveďte, jak k němu dochází a jak se proti němu bránit.

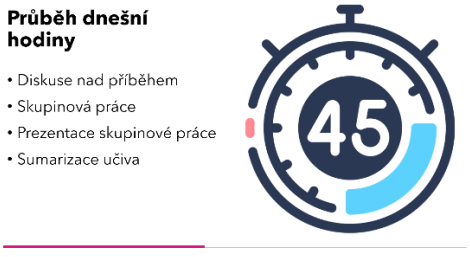
Prezentace

Slide 1



Slide 2

Slide 3



Slide 4

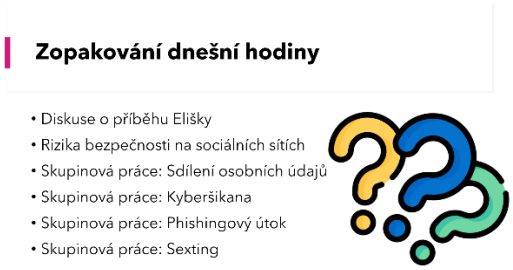
Slide 5

Slide 6

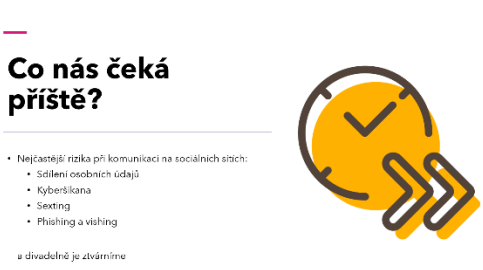
Slide 7

Slide 8

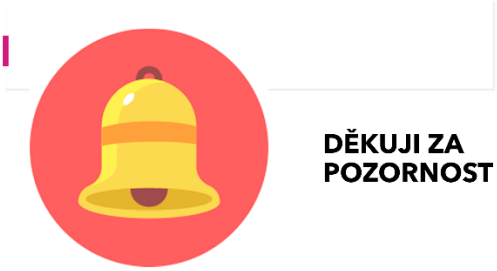
Slide 9



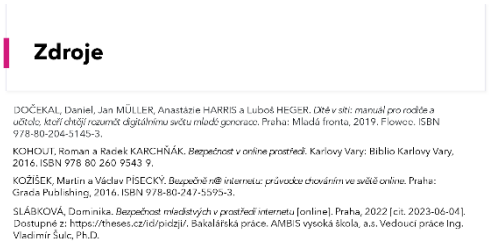
Slide 10



Slide 11



Slide 12



Zdroje

DOČEKAL, Daniel, Jan MÜLLER, Anastázie HARRIS a Luboš HEGER. *Oté v síti: manuál pro rodiče a učitele, kteří chtějí rozumět digitálnímu světu mladé generace*. Praha: Mladá fronta, 2019. Flowee. ISBN 978-80-204-5145-3.

KOHOUT, Roman a Radek KARCHŇÁK. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978 80 260 9543 9.

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

SLÁBKOVÁ, Dominika. *Bezpečnost mladistvých v prostředí internetu* [online]. Praha, 2022 [cit. 2023-06-04]. Dostupné z: https://theses.cz/id/pidzji/. Bakalářská práce. AMBIS vysoká škola, a.s. Vedoucí práce Ing. Vladimír Šulc, Ph.D.

Slide 13

Společenskovědní vzdělávání: Druhá hodina

Příprava na výuku

Škola: 63–41 – M/02 Obchodní akademie	Třída: Druhý ročník
Předmět: Společenskovědní vzdělávání	Tematický okruh: Člověk jako občan
Počet žáků: 30	Průřezové téma: Mediální výchova
Cíle hodiny: Žák umí prezentovat před diváky (spolužáky). Žák vyjmenuje alespoň 3 zásady, jak bezpečně komunikovat na sociálních sítích. Žák uvede rizika sociálních sítí a doloží je alespoň jedním příkladem. Uvede také možnosti, jak těmto rizikům předcházet.	
Téma vyučovací hodiny: Konkrétními rizika při komunikaci na sociálních sítích	

Rozvíjené klíčové kompetence:

- Kompetence k učení: Žák identifikuje důležité informace
- Kompetence k řešení problémů: Žák definuje, čemu konkrétně nerozumí a co mu dělá problém
- Kompetence komunikativní: Žák vyjadřuje své názory, slovem i písmem – kultivovanou formou
- Kompetence sociální a personální: Žák přijímá zodpovědnost za své chování, názory a postoje
- Kompetence sociální a personální: Žák se umí začlenit do skupiny a v té spolupracovat
- Kompetence sociální a personální: Žák respektuje práci ostatních
- Kompetence občanská: Žák organizuje spolupráci
- Kompetence k podnikavosti: Žák se ztotožňuje s cíli, které mu stanovil někdo jiný
- Kompetence k podnikavosti: Žák pojmenuje, jakými disponuje schopnostmi, znalostmi a dovednostmi

Pomůcky:

- Scénáře krátkých divadelních her (Příloha)
- Sáček s barevnými víčky

Metody:

- Slovní metoda – Vysvětlování, práce s textem, diskuse
- Názorně demonstrační metoda – Divadelní hra
- Praktická metoda – Divadelní hra

Organizační formy:

- Hromadná (frontální) výuka
- Skupinová (kooperativní) výuka

Rozvržení výuky (časový harmonogram - 45 minut):

Časová orientace	Průběh	Poznámky k rozboru
1	Začátek hodiny – Zklidnění žáků, získání pozornosti	
2	Naladění atmosféry (Ice-breaking)	
4	Seznámení žáků s průběhem dnešní hodiny (+ Motivace)	
8	Opakování minulé hodiny – Aplikace a fixace – Prezentace skupinových prací (plakátů)	
18	Fixace – Zhodnocení skupinové práce žáků	
22	Aktivita – Seznámení žáků s průběhem divadelních her	
24	Aktivita – Skupinová práce – Příprava divadelní hry, zápis do TK	
32	Aktivita – Skupinová práce – Skupiny předvádí své divadelní hry	
40	Fixace – Zopakování řečených a klíčových informací z hodiny	
42	Rekapitulace průběhu dnešní hodiny a slovní hodnocení žáků	
44	Příprava na průběh příští hodiny	
45	Konec hodiny – Rozloučení se s žáky	

Průběh hodiny:

1 - Začátek hodiny – Zklidnění žáků, získání pozornosti

Učitel – Postaví se před třídu a čeká, než se žáci ztiší a postaví. Následně pozdraví žáky.

Žák – Ztiší se a svým postavením dá najevo, že vnímá přítomnost učitele a začátek hodiny.

2 - Naladění atmosféry (Ice-breaking)

Učitel – Vytváří příjemnou atmosféru – Okomentuje počasí; zeptá se na náladu žáků…

Žák – Koncentruje se a komunikuje s učitelem.

4 - Seznámení žáků s průběhem dnešní hodiny (+ Motivace)

Učitel – Seznámí žáky s průběhem dnešní hodiny, řekne číslo, téma, cíl a průběh hodiny. Během toho také motivuje žáky, snaží se v nich vyvolat vnitřní motivaci k tématu hodiny.

Žák – Seznámí se s harmonogramem dnešní hodiny a získá dostatečné sebevědomí.

8 - Opakování minulé hodiny – Aplikace a fixace – Prezentace skupinových prací (plakátů)

Učitel – Moderuje prezentaci jednotlivých skupin, doplňuje případné chybějící informace.

Žák – Prezentuje skupinovou práci, zapisuje si informace prezentované jinými skupinami.

18 - Fixace – Zhodnocení skupinové práce žáků

Učitel – Systematizuje řečené informace. Nechá žáky samostatně zhodnotit jejich dosavadní práci ve skupině, kterou také okomentuje.

Žák – Aktivně se podílí na rekapitulaci informací a realisticky ohodnotí svou práci ve skupině.

22 - Aktivita – Seznámení žáků s průběhem divadelních her

Učitel – Seznámí žáky s pravidly pro přípravu divadelní hry a rozdělí žáky do skupin pomocí sáčku s barevnými víčky (Příloha: Divadelní hra 1-8).

Žák – Poslouchá pokyny a zeptá se na nejasnosti.

24 - Aktivita – Skupinová práce – Příprava divadelní hry, zápis do TK

Učitel – Kontroluje práci skupin a napomáhá žákům. Zapíše do třídní knihy.

Žák – Připravuje a upravuje své krátké divadelní vystoupení.

32 - Aktivita – Skupinová práce – Skupiny předvádí své divadelní hry

Učitel – Chválí žáky a šetrně, v krajní situaci, sděluje případnou kritiku.

Žák – Ztvárňuje vylosovanou a upravenou divadelní hru, podporuje spolužáky při jejich divadelním vystoupení.

40 - Fixace – Zopakování řečených a klíčových informací z hodiny

Učitel – Sumarizuje řečené informace.

Žák – Píše si stručný zápis z hodiny.

42 - Rekapitulace průběhu dnešní hodiny a slovní hodnocení žáků

Učitel – Připomene etapy dnešní hodiny, zopakuje důležité informace, zhodnotí práci žáků, získává jejich zpětnou vazbu.

Žák – Aktivně se podílí na rekapitulaci dnešní hodiny a předává zpětnou vazbu učiteli.

44 - Příprava na průběh příští hodiny

Učitel – Seznamuje žáky s tématem příští hodiny.

Žák – Je seznámen s průběhem příští hodiny.

45 – Konec hodiny – Rozloučení se s žáky

Učitel – Rozloučí se s žáky, ti se zvoněním mohou opouštět učebnu.

Žák – Uklidí si svůj pracovní prostor a se zvoněním opouští učebnu.

Příloha:

Divadelní hra 1: Zastavte online zloděje!

Postavy: Anna - 18 let, středoškolská studentka

Tomáš - 23letý IT technik

Hackula - záhadný internetový zloděj

(Anna sedí u počítače a začne volat Tomášovi)

- *Anna: Tomáši, musím ti něco důležitého říct!*
  - *Tomáš: Co se stalo, Aničko? Vypadáš rozrušeně.*
- *Anna: Ukradli mi všechna moje hesla a přihlašovací údaje! A co víc, vykradli mi bankovní účet.*
  - *Tomáš: To je hrůza! Jak se ti to mohlo stát?*
- *Anna: Myslím si, že jsem nedodržovala bezpečnostní opatření při používání sociálních sítí. Měla jsem veřejný profil a sdílela jsem tam spoustu osobních informací, které útočník mohl zneužít.*
  - *Tomáš: Je to možné. Bezpečná komunikace na sociálních sítích je důležitá.*
- *Anna: Teď si to uvědomuji. Bohužel jsem se musela přesvědčit na vlastní kůži.*
  - *Tomáš: Je mi líto, že sis neuvědomovala význam bezpečného online chování dříve. Doufám, že se z toho poučíš a už se ti nic podobného nestane.*
- *Anna: Určitě! Teď si vážím ochrany svých osobních údajů a dodržování bezpečné komunikace na internetu. Získala jsem důležitou lekci.*

(Do scény vstupuje Hackula, záhadný internetový zloděj.)

- *Hackula (pokřikuje): Ha ha ha! Ukradl jsem tvoje heslo! A připrav se, ukradnu ti všechno!*

Divadelní hra 2: Žádost o přátelství

Postavy: Erik – 16 let, středoškolský student

Jiří – 16 let, středoškolský student, Erikův kamarád a spolužák

Klára – nová dívka ze stejného ročníku, ale z druhé třídy

(Dvě postavy, Erik a Jiří, se potkávají ve školní kantýně.)

- *Erik: Hele, Jirko, mám novou hru na mobilu! A víš co? Klára, ta nová holka z druhé třídy, mi poslala žádost o přátelství na sociální síti. Podívej, jaké příspěvky má na svém profilu.*
  - *Jiří: Hmm, to bych si raději dával pozor. Takovéto sdílení osobních údajů a fotek na internetu může být nebezpečné.*
- *Erik: Ale všichni to přece dělají. Nemůžeme být jediní, kdo neukazuje svůj život na sociálních sítích.*
  - *Jiří: Ano, to je pravda, ale musíme si uvědomit, že to, co jednou skončí na internetu, tam zůstane navždy. A to může mít negativní dopad na náš život v budoucnosti.*
- *Erik: Nějak mi to nedochází.*
  - *Jiří: Představ si, že jednou se rozhodneš sdílet své osobní údaje a fotky. Nemůžeš si být jistý, kdo se na ně podívá. Musíme být obezřetní a pamatovat na to, že bezpečnost je na prvním místě.*
- *Erik: Myslíš, že bych se měl vzdát sociálních sítí?*
  - *Jiří: Ne, to ne. Sociální sítě mají své pozitivní stránky, ale musíme být chytří a chránit své soukromí. Dávejme si pozor na to, co sdílíme a komu důvěřujeme online.*
- *Erik: Jirko, máš pravdu. Budu opatrný a dám si pozor na to, co sdílím na internetu. Děkuju, že jsi mi otevřel oči.*
  - *Jiří: Není zač. Jsme tu přece pro sebe, abychom se navzájem chránili.*

Divadelní hra 3: Upravené fotografie

Postavy: *Nina - 15 let, středoškolská studentka*

Jan - 16 let, středoškolský student

Lukáš - 17 let, středoškolský student, kamarád Niny a Jana

(Jan potká Ninu na chodbě školy poté, co jí včera vulgárně okomentoval fotky na internetu.)

- *Nina: Ahoj, Honzo. Proč mi píšeš vulgární komentáře k fotkám? Nechápu, proč se takhle chováš. Nikdy jsem ti nic neudělala.*
  - *Jan: Co kecáš! Ty a tvoje kamarádky se chováte, jako by vám sociální sítě patřily. Myslíte si, že máte právo všechny hodnotit a posuzovat. To už se mi fakt nelíbí.*
- *Nina: Nechápu. Co jsem udělala špatně?*
  - *Jan: To není jen o tobě, ale o celé vaší partě. Prostě už mě nebaví, jak se na mě díváte s posměchem. Mám pocit, že si ze mě děláte legraci.*
- *Nina: Tobě vadí to, jak jsme ti upravili fotky?*
  - *Jan: Jo! Všichni se mi kvůli té fotomontáži smějí a dávají mi hrozné přezdívky.*
- *Nina: Aha.*

(Na scénu přichází Lukáš.)

- *Lukáš: Čau, co se tady děje? Důležitý záležitosti na sociálních sítích?*
  - *Jan: Čus, Lukáši. Hele, Nina a její kamarádky mi upravily fotky a teď se mi všichni na internetu vysmívají.*
- *Lukáš: To nezní moc dobře. Ale víš, Honzo, to neznamená, že se máš k Nině chovat vulgárně. Chápeš, že každý na internetu má právo na respekt a slušné zacházení?*
  - *Jan: Ale ona se taky chovala neslušně, když si dělaly legraci z mého vzhledu.*
- *Lukáš: Jasně. Nina takové věci neměla dělat. Ale Honzo, důležité je mít na paměti, že existují jiné způsoby, jak se bránit, než psát vulgární komentáře k Nininým fotkám.*
- *Nina: Ne, kluci, je to moje chyba. Bylo to myšleno jako vtip, nenapadlo mě, že ti to, Honzo, ublíží. Promiň, hnedka to smažu.*
  - *Jan: Víš, fakt mě to vytočilo, nicméně jsem se nezachoval nejlíp. Ty komentáře taky smažu.*

Divadelní hra 4: Falešný účet

Postavy: Tereza - 16 let, středoškolská studentka

Lukáš - 17 let, středoškolský student

Superadmin - tajný superhrdina se zaměřením na sociální sítě a internet

(Otevřená scéna, Tereza a Lukáš se potkají ve školní kantýně.)

- *Tereza: Ahoj, Lukáši, jak se máš?*
  - *Lukáš: Čau, Terko! Hele, včera jsem zjistil, že se za mě na internetu někdo vydává.*
- *Tereza: To zní hrozně. Musíš být obezřetný. To by mohla být kyberšikana!*
  - *Lukáš: No jo, ale co mám dělat?*

(Superadmin přichází na scénu.)

- *Superadmin: Slyšel jsem, že potřebujete pomoc s bezpečností na sociálních sítích. Mám tady pár rad navíc.*
- *Tereza: Ano, prosím! Tady Lukáš s nimi má problém. Co byste mu doporučil?*
- *Superadmin: Je důležité si uvědomit, že ne všichni lidé na internetu jsou ti, za které se vydávají. Nikdy nevěř neznámým osobám na internetu a nesdílej s nimi své osobní informace. Celkově je nejlepší, když se vyvaruješ konverzací s lidmi, které osobně neznáš.*
  - *Lukáš: To zní rozumně. Musím si dobře rozmyslet, komu věřit a s kým komunikovat online.*
- *Superadmin: Správně! A když jsi ve veřejných diskuzích, buď zdvořilý a respektuj ostatní. Nenech se vyprovokovat a nepropadni nenávisti na internetu. Buďme vzájemně ohleduplní.*
  - *Lukáš: Dobře, ale co mám udělat s tím falešným účtem?*
- *Superadmin: Nejdříve si ulož důkazy, že se za tebe někdo vydává, a pak zkus jeho účet nahlásit. Kdyby to nepomohlo, zkus kontaktovat někoho dospělého, ten ti jistě pomůže.*
- *Tereza: To jsou výborné rady! Díky, že jste přišel, pane Superadmine.*
- *Superadmin: Rád jsem pomohl. Pamatujte si, že internet je mocný nástroj, ale s ním přichází i zodpovědnost. Užijte si ho a používejte ho bezpečně!*

Divadelní hra 5: Fotohavárie na síti

Postavy: Aleš – 16 let, středoškolský student

Eliška – 16 let, kamarádka Aleše a Petry

Petra – 16 let, Alešova přítelkyně

(Scéna: Aleš, Eliška a Petra se setkávají na autobusové zastávce.)

- *Aleš: Ahoj, Eliško! Jak se dnes máš?*
- *Eliška: Čau, lidi! Jsem v pohodě. A co vy?*
- *Aleš: Hm, no... Říkal jsem Pétě, že bych chtěl její fotku, na které bude jen v tangách.*
- *Eliška: Cože?! Aleši, opravdu si myslíš, že je to rozumný nápad?*
- *Petra: Ano, musím se připojit k Elišce. Sexting může mít nepříjemné následky.*
- *Aleš: Ale proč? Vždyť tohle dělají všichni.*
- *Eliška: Aleši, i když něco dělá hodně lidí, neznamená to automaticky, že je to bezpečné. Musíš si uvědomit, že taková fotka může skončit v nesprávných rukou.*

(Časový skok.)

- *Aleš a Petra: Eliško, musíš nám pomoct!*
- *Petra: Někdo posílá moji fotku v tangách všem po škole!*
- *Eliška: Cože?! To je hrozné. Jak se to mohlo stát?*
- *Aleš: Nejsem si jistý. Nevím, jak se to vlastně stalo.*
- *Eliška: Aleši, měli jste si dávat pozor. A Petro, vůbec nechápu, proč si mu takovou fotku posílala.*
- *Petra: To teď neřeš, musíme začít rychle jednat.*
- *Eliška: Souhlasím. Měli bychom se poradit s dospělými, jako je náš učitel informatiky nebo vedení školy. Společně můžeme najít způsob, jak zvládnout tuto situaci.*
- *Petra: Ano, potřebujeme pomoc. Musíme zastavit šíření této fotky.*

Divadelní hra 6: Fotohavárie na síti

Postavy: Karel – 18 let, začíná randit s Monikou

Monika – 17 let, opatrná dívka, která si chrání své soukromí na internetu

Veronika – 16 let, náhodná kolemjdoucí

(Karel a Monika sedí spolu v parku a povídají si.)

- *Karel: Hele, řekni mi, pošleš mi nějakou fotku? Ne nutně nahou, jen nějakou tvou.*
  - *Monika: Ne. Nikdy neposílám své fotky ostatním lidem.*

(Karel ukazuje Monice fotku na svém telefonu.)

- *Karel: Tohle vypadá jako fotka tvého těla. Nejsi to ty?*
  - *Monika: To nemůže být moje fotka.*

(Karel si čte textové zprávy na obrazovce.)

- *Karel: Taky používáš tuhle přezdívku.*
  - *Monika: To neznamená, že jsem na té nahé fotce já.*

(Veronika vstoupí na scénu.)

- ❖ *Veronika: Promiňte, že vás přerušuji. Ale to jsem já na té fotce.*
  - *Monika: Co tu děláte?*
- ❖ *Veronika: Udělala jsem chybu a poslala ji špatné osobě.*
- *Karel: Co se stalo?*
- ❖ *Veronika: Omylem jsem klikla na špatné jméno v seznamu kontaktů.*
  - *Monika: Vidíš a to je jeden z důvodů, proč své fotky nikomu neposílám.*

Divadelní hra 7: Soutěž na Facebooku

Postavy:Oskar – 18 let, středoškolský student

Jakub – 17 let, středoškolský student

Hana – 16 let, středoškolská studentka

Sabina – 17 let, středoškolská studentka

(Oskar, Jakub, Hana a Sabina se potkají v knihovně.)

- *Oskar: Čau, všichni! Jak se máte?*
  - *Jakub: Ahoj, Oskare! Právě jsme se tady potkali a začali diskutovat o internetové bezpečnosti.*
    - ❖ *Hana: Víte co, lidi? Na Instagramu jsem viděla super soutěž. Přemýšlím, že bych se do ní zapojila.*
      - ➢ *Sabina: Počkej, Hani! Na internetu musíš být opatrná. Některé soutěže mohou být podvod.*
        - ❖ *Hana: Ale co se může stát? Jenom musím vyplnit jméno, adresu a telefonní číslo.*
          - *Jakub: To může být rizikové. Tímto způsobem mohou podvodníci získat tvé osobní údaje.*
            - ❖ *Oskar: Kuba má pravdu. To, co popisuješ, zní jako phishingový útok. Musíš být obezřetná a chránit si své údaje.*
              - ❖ *Hana: Takže bych to neměla dělat?*
                - ❖ *Sabina: Správně. Musíš si dávat pozor. Používej pouze oficiální a ověřené webové stránky pro soutěže a ujisti se, že tvé osobní údaje zůstanou v bezpečí.*

(Hana přemýšlí.)

- ❖ *Hana: Díky všem za radu. Budu opatrná a zajistím, že ochrana mých osobních údajů bude na prvním místě.*

Divadelní hra 8: Prevence je lepší než léčba

Postavy: Roman – 32 let, učitel a vedoucí kroužku informatiky

Barbora – 16 let, středoškolská studenta

Dominika – 15 let, středoškolská studentka

Adam – 15 let, středoškolský student

(Roman, Barbora, Dominika a Adam se setkají na kroužku informatiky.)

- *Roman: Ahoj, všichni! Přemýšlel jsem o tom, jak vás seznámit se správným chováním na internetu. Myslím, že divadelní představení by bylo skvělým způsobem, jak to všechno vysvětlit.*
- *Barbora: Skvělý nápad! Už se nemůžu dočkat, až začneme!*
- *Dominika: Je důležité si uvědomit, že na internetu musíme být opatrní. S phishingem jsem se už setkala.*
- *Adam: Phishing? To zní jako ryba! To se mně snad nestane.*
- *Roman: Phishing je nebezpečný útok, při kterém se snaží zloději získat naše citlivé informace, například hesla. Nikdy nesmíte klikat na podezřelé odkazy nebo sdělovat citlivé informace neznámým lidem.*
- *Barbora: Ale to se přece může stát každému, ne?*
- *Dominika: Ano, ale můžeme se chránit. A víš, že existuje i vishing?*
- *Adam: Vish... co? To zní ještě divněji než phishing!*
- *Roman: Ano, vishing je podobný útok, ale používá se k němu telefon. Zloději se snaží získat informace prostřednictvím klamavých telefonátů.*
- *Dominika: Musíme být opatrní i při telefonování!*
- *Barbora: To je jako zloděj, který tě chce okrást, ale místo okna použije telefon!*
- *Adam: No já většinou telefonuji jen s kamarády, takže mi to nehrozí.*
- *Roman: Ale i ty bys měl být opatrný. Neměj důvěru k neznámým lidem a nezveřejňuj osobní informace na sociálních sítích.*
- *Dominika: A měj silná hesla a pravidelně je měň!*
- *Adam: Hmm, asi bych se měl trochu polepšit...*
- *Roman: Správně! Prevence je vždycky lepší než léčba. Pokud dodržujete pravidla bezpečného chování na internetu, vyhnete se mnoha problémům.*

Společenskovědní vzdělávání: Třetí hodina

Příprava na výuku

Škola: 63–41–M/02 Obchodní akademie	Třída: Druhý ročník
Předmět: Společenskovědní vzdělávání	Tematický okruh: Člověk jako občan
Počet žáků: 30	Průřezové téma: Mediální výchova
Cíle hodiny: Žák vytvoří desatero zásad, jak správně komunikovat na sociálních sítích. Žák zdůvodní alespoň 3 zásady bezpečné komunikace na sociálních sítích. Žák vyjmenuje alespoň 5 zásad bezpečné komunikace na internetu.	
Téma vyučovací hodiny: Zásady bezpečné komunikace na sociálních sítích	

Rozvíjené klíčové kompetence:

- Kompetence k učení: Žák najde potřebné informace
- Kompetence k řešení problémů: Žák definuje, čemu konkrétně nerozumí a co mu dělá problém
- Kompetence komunikativní: Žák vyjadřuje své názory, slovem i písmem – kultivovanou formou
- Kompetence sociální a personální: Žák přijímá zodpovědnost za své chování, názory a postoje
- Kompetence sociální a personální: Žák respektuje práci ostatních
- Kompetence občanská: Žák srozumitelně předkládá získané informace
- Kompetence k podnikavosti: Žák se ztotožňuje s cíli, které mu stanovil někdo jiný
- Kompetence k podnikavosti: Žák pojmenuje, jakými disponuje schopnostmi, znalostmi a dovednostmi

Pomůcky:

- Počítač a projektor
- Prezentace (Příloha)
- Papír a psací potřeby
- Připravený Kahoot (Příloha)

Metody:

- Slovní metoda – Vysvětlování, práce s textem, diskuse
- Názorně demonstrační metoda – Instruktáž
- Praktická metoda – Výtvarná metoda

Organizační formy:

- Hromadná (frontální) výuka
- Skupinová (kooperativní) výuka
- Samostatná práce

Rozvržení výuky (časový harmonogram - 45 minut):

Časová orientace	Průběh	Poznámky k rozboru
1	Začátek hodiny – Zklidnění žáků, získání pozornosti	
2	Naladění atmosféry (Ice-breaking)	Slide 1
4	Opakování minulé hodiny – Práce ve dvojicích	Slide 2-3
10	Seznámení žáků s průběhem dnešní hodiny (+ Motivace)	Slide 4
12	Aktivita – Kvíz – Kahoot	Slide 5
26	Opakování klíčových informací z aktivity Kahoot	Slide 6
30	Aktivita – Samostatná práce, zápis do TK	Slide 7-8
34	Kontrola vytvořených desater – BINGO	Slide 9
39	Fixace – Zopakování řečených a klíčových informací z hodiny	Slide 9
41	Rekapitulace průběhu dnešní hodiny a slovní hodnocení žáků	Slide 10
44	Příprava na průběh příští hodiny	Slide 11
45	Konec hodiny – Rozloučení se s žáky	Slide 12

Průběh hodiny:

1 - Začátek hodiny – Zklidnění žáků, získání pozornosti

Učitel – Postaví se před třídu a čeká, než se žáci ztiší a postaví. Následně pozdraví žáky.

Žák – Ztiší se a svým postavením dá najevo, že vnímá přítomnost učitele a začátek hodiny.

2 - Naladění atmosféry - Ice-breaking (Slide 1)

Učitel – Vytváří příjemnou atmosféru – Okomentuje počasí; zeptá se na náladu žáků… Během ice-breakingu se učitel přihlásí do počítače a spustí prezentaci.

Žák – Koncentruje se a komunikuje s učitelem.

4 - Opakování minulé hodiny (Slide 2-3)

Učitel – Připomene průběh minulé vyučovací hodiny – divadelní hry. Poté opakuje téma minulých hodin pomocí krátké aktivity ve dvojicích. Rozdělí žáky do dvojic podle zasedacího pořádku. Každá dvojice dostane otázky (Příloha: Opakování minulé hodiny – Otázky) zaměřené na témata z minulých hodin. Žáci ve dvojici společně vymyslí krátkou odpověď. Dvojice pak dostanou prostor sdělit své odpovědi nahlas.

Žák – Aktivně se účastní rekapitulace minulé hodiny ve dvojici. Pociťuje úspěch, uklidní se, připomíná si znalosti, které už zná. Pokud žák chyběl na předchozí hodině, dozví se nyní důležité informace z minulé hodiny.

10 - Seznámení žáků s průběhem dnešní hodiny (+ Motivace)

Učitel – Seznámí žáky s průběhem dnešní hodiny, řekne číslo, téma, cíl a průběh hodiny. Také motivuje žáky, snaží se v nich vyvolat vnitřní motivaci k tématu hodiny.

Žák – Seznámí se s harmonogramem dnešní hodiny a uvědomuje si užitečnost tématu.

12 - Aktivita – Kvíz – Kahoot (Slide 5)

Učitel – Moderuje kvízovou hru (Příloha: Kvíz – Kahoot) a komentuje odpovědi žáků.

Žák – Aktivizuje se, dává učiteli zpětnou vazbu o svých znalostech.

Aktivita – Cílem této aktivity je zopakovat a zafixovat důležité znalosti týkající se bezpečné komunikace na sociálních sítích, včetně práce s hesly, zabezpečení zařízení a dat.

26 - Opakování klíčových informací z aktivity Kahoot (Slide 6)

Učitel – Opakuje klíčové znalosti, které zazněly během kvízové hry Kahoot.

Žák – Aktivně se podílí na opakování klíčových znalostí, které zazněly během kvízové hry Kahoot, a na případné nejasnosti se zeptá učitele.

30 - Aktivita – Samostatná práce, zápis do TK (Slide 7-8)

Učitel – Seznámí žáky se zadáním samostatné práce. Během aktivity kontroluje její průběh a napomáhá žákům. Zapíše do třídní knihy.

Žák – Poslouchá instrukce samostatné práce a případně se zeptá na nesrovnalosti. Poté samostatně vytvoří vlastní desatero bezpečné komunikace na sociálních sítích.

Samostatná práce – Žák tvoří vlastní desatero bezpečné komunikace na sociálních sítích.

34 - Kontrola vytvořených desater (Slide 9) - BINGO

Učitel – Prezentuje vlastní desatero a žáci si zaznamenávají, která pravidla mají stejná. Pokud žák bude mít napsané ve svém desateru jiné pravidlo, než řekne učitel, sdělí ho nahlas. Pokud bude žákovo pravidlo smysluplné, učitel ho pochválí.

Žák – Kontroluje si svoji samostatnou práci a na případné nejasnosti se zeptá učitele.

39 - Fixace – Zopakování řečených a klíčových informací z hodiny (Slide 9)

Učitel – Rekapituluje nejčastější pravidla, která žáci zmínili ve svém desateru, a ta komentuje.

Žák – Aktivně se podílí na rekapitulaci a komentování jednotlivých pravidel.

41 - Rekapitulace průběhu dnešní hodiny a slovní hodnocení žáků (Slide 10)

Učitel – Připomene etapy dnešní hodiny, zopakuje důležité informace, zhodnotí práci žáků, získává jejich zpětnou vazbu.

Žák – Aktivně se podílí na rekapitulaci dnešní hodiny a předává zpětnou vazbu učiteli.

44 - Příprava na průběh příští hodiny (Slide 11)

Učitel – Seznamuje žáky s tématem příští hodiny.

Žák – Je seznámen s průběhem příští hodiny.

45 – Konec hodiny – Rozloučení se s žáky (Slide 12)

Učitel – Rozloučí se s žáky, ti se zvoněním mohou opouštět učebnu.

Žák – Uklidí si svůj pracovní prostor a se zvoněním opouští učebnu.

Příloha:

Opakování minulé hodiny – Otázky

1. Co si představíte pod pojmem „bezpečná komunikace na internetu“?
2. Jaká existují rizika při komunikaci na internetu?
3. Jak si zkontrolujete, že osoba, se kterou na internetu komunikujete, je ta, za niž se vydává?
4. Jaké jsou nejčastější formy kyberšikany a jak se jí můžete bránit?
5. Co je to phishing a jaká jsou jeho rizika?
6. Co je to sexting a jaká jsou jeho rizika?
7. Jaké jsou nejlepší způsoby ochrany své online identity a soukromí?

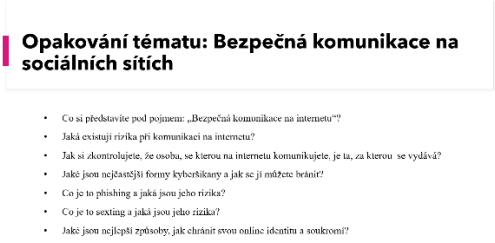
Kvíz – Kahoot

https://create.kahoot.it/share/bezpecnost-na-internetu/56a25da6-f872-4ce9-a15f-db4dd803b537

Prezentace

Slide 1

Slide 2



Slide 3

Slide 4

Slide 5

Slide 6

Slide 7

Slide 8

Kontrola DESATERA - BINGO

- Používám unikátní a silná hesla, chráním si své účty.
- Používám aktualizovaný operační systém, software a antivirus (na počítači i mobilu).
- K novým informacím přistupuji skepticky a ověřuji si jejich pravost z několika zdrojů.
- Na internetu navštěvuji pouze důvěryhodné webové stránky.
- Dávám si pozor na to, co na internetu sdílím, nesdílím osobní údaje.
- Na sociálních sítích mám bezpečně nastavené soukromí.
- Nekomunikuji s neznámými uživateli.
- Neotevírám podezřelé odkazy a přílohy.
- Pokud jsem se stal obětí kybernetického útoku, nebojím se říci si o pomoc.
- Vzdělávám se o kybernetických rizicích.

Slide 9

Zopakování dnešní hodiny

- Kahoot
- Tvorba vlastního desatera

Slide 10

Co nás čeká příště?

- Vzestup mezinárodní spolupráce
- Otevření hranic a migrace
- Globalizace ekonomiky a obchodu
- Kultura a kulturní diverzita
- Globální výzvy a řešení

Slide 11

DĚKUJI ZA POZORNOST

Slide 12

Zdroje

DOČEKAL, Daniel, Jan MÜLLER, Anastázie HARRIS a Luboš HEGER. *Dítě v síti: manuál pro rodiče a učitele, kteří chtějí rozumět digitálnímu světu mladé generace*. Praha: Mladá fronta, 2019. Flowee. ISBN 978-80-204-5145-3.

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

SLÁBKOVÁ, Dominika. *Bezpečnost mladistvých v prostředí internetu* [online]. Praha, 2022 [cit. 2023 06 04]. Dostupné z: https://theses.cz/id/pidpji/. Bakalářská práce. AMBIS vysoká škola, a.s. Vedoucí práce Ing. Vladimír Šulc, Ph.D.

Slide 13