Univerzita Hradec Králové
Pedagogická fakulta
Ústav sociálních studií

Prevalence rizikové komunikace v online prostředí u studentů vysokých škol

Bakalářská práce

Autor: Tereza Ťopková
Studijní program: B7507 Specializace v pedagogice
Studijní obor: Sociální patologie a prevence
Vedoucí práce: Mgr. Lucie Křivánková, Ph.D.
Oponent práce: PhDr. Jindra Vondroušová, Ph.D.

Hradec Králové 2023

Univerzita Hradec Králové
Pedagogická fakulta

Zadání bakalářské práce

Autor:	**Tereza Ťopková**
Studium:	P20P0105
Studijní program:	B7507 Specializace v pedagogice
Studijní obor:	Sociální patologie a prevence
Název bakalářské práce:	**Prevalence rizikové komunikace v online prostředí u studentů vysokých škol**
Název bakalářské práce AJ:	The Prevalence of Risk Communication in Cyberspace Among University Students

Cíl, metody, literatura, předpoklady:

Bakalářská práce se zabývá problematikou rizikové komunikace v online prostředí u studentů vysokých škol. Cílem je blíže popsat formy rizikové komunikace a zjistit jakou zkušenost s touto problematikou mají studenti VŠ. V teoretické části se zabývá komunikací, online prostředím a sociálními sítěmi, skrze které je riziková komunikace provozována. Definuje konkrétní formy této komunikace, kterými jsou zejména kybergrooming, sexting, phishing, kyberšikana a další.
V praktické části se nachází výzkumné šetření orientované na studenty vysokých škol a jejich zkušenosti a vztah k rizikové komunikaci v online prostředí, které je realizováno kvantitativní výzkumnou metodou, konkrétně online dotazníkem.

ECKERTOVÁ, Lenka a DOČEKAL, Daniel. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče.* Brno: Computer Press, 2013. 224 s. ISBN 978-80-251-3804-5.

GAVORA, Peter. *Úvod do pedagogického výzkumu*. Překlad Vladimír Jůva a Vendula Hlavatá. 2., rozš. české vyd. Brno: Paido, 2010. 261 s. ISBN 978-80-7315-185-0.

KOPECKÝ, Kamil a kol. *Rizikové formy chování českých a slovenských dětí v prostředí internetu.* Olomouc: Univerzita Palackého v Olomouci, 2015. 169 s. ISBN 978-80-244-4861-9.

KOŽÍŠEK, Martin a PÍSECKÝ, Václav. *Bezpečně n@ internetu: průvodce chováním ve světě online.* Praha: Grada Publishing, 2016. 175 s. ISBN 978-80-247-5595-3.

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

Zadávající pracoviště:	Ústav sociálních studií, Pedagogická fakulta
Vedoucí práce:	Mgr. Lucie Křivánková, Ph.D.
Oponent:	PhDr. Jindra Vondroušová, Ph.D.

Datum zadání závěrečné práce: 1.2.2022

Prohlášení

Prohlašuji, že jsem bakalářskou práci Prevalence rizikové komunikace v online prostředí u studentů vysokých škol vypracovala pod vedením vedoucí práce Mgr. Lucie Křivánkové, Ph.D. samostatně a uvedla jsem všechny použité prameny a literaturu.

V Hradci Králové dne 6. 12. 2023

_____

Tereza Ťopková

Poděkování

Ráda bych tímto poděkovala Mgr. Lucii Křivánkové, Ph.D. za odborné vedení bakalářské práce, cenné rady, vstřícný přístup, ochotu i trpělivost. Velké díky zároveň patří respondentům, jelikož bez jejich participace by nebylo možné práci napsat. Dále bych chtěla poděkovat mému nejbližšímu okolí za jejich podporu během celého studia.

Anotace

ŤOPKOVÁ, Tereza. *Prevalence rizikové komunikace v online prostředí u studentů vysokých škol*. Hradec Králové: Pedagogická fakulta Univerzity Hradec Králové, 2023. 51 s. Bakalářská práce.

Bakalářská práce se zaměřuje na rizikovou komunikaci v online prostředí u studentů vysokých škol. Cílem této práce je blíže popsat formy rizikové komunikace a zjistit jakou zkušenost s touto problematikou mají studenti VŠ. V teoretické části je práce zaměřena na komunikaci, online prostředí a sociální sítě, skrze které je riziková komunikace nejčastěji provozována. Zabývá se také charakteristickými rysy vysokoškolských studentů z pohledu vývojové psychologie a také specifik dnešních studentů vysokých škol za pomocí charakteristik generace Z. Dále definuje konkrétní formy rizikové komunikace, kterými jsou zejména kybergrooming, sexting, phishing, kyberšikana a další. V praktické části se následně nachází výzkumné šetření orientované na studenty vysokých škol, jejich zkušenosti a vztah k rizikové komunikaci v online prostředí, které je realizováno kvantitativní výzkumnou metodou, konkrétně online dotazníkem.

Klíčová slova: riziková komunikace, studenti vysokých škol, online prostředí, sociální sítě

Annotation

ŤOPKOVÁ, Tereza. *The Prevalence of Risk Communication in Cyberspace Among University Students*. Hradec Králové: Faculty of Education, University of Hradec Králové, 2023. 51 pp. Bachelor Thesis.

The bachelor thesis focuses on the problematics of risk communication in cyberspace among university students. The aim of this thesis is to closely describe the forms of risk communication and find out what experiences do the university students have with said communication. In the theoretical part the thesis is focused on communication, cyberspace a social network sites through which is the risk communication most often realized. The thesis deals with the characteristics of university students from the developmental psychology point of view and with the specifics of generation Z. Defines specific forms of risk communication which are cybergrooming, sexting, phishing, cybelbullying and other. In the empirical part the research inquiry is found, which targets university students, their experience and relation towards risk communication in cyberspace. Research inquiry is realized through a quantitative research method, specifically an online survey.

Key words: risk communication, university students, cyberspace, social network sites

Prohlášení

Prohlašuji, že bakalářská práce je v souladu s rektorským výnosem č. 13/2022 (Řád pro nakládání s bakalářskými, diplomovými, rigorózními, disertačními a habilitačními pracemi na UHK).

Datum: ……. Podpis studenta: ……..

Obsah

Úvod

Tato bakalářská práce se zabývá problematikou rizikové komunikace v online prostředí, kdy v praktické části této práce je zaměřena na studenty vysokých škol a na to, zdali vůbec, a případně tedy jaké, zkušenosti mají právě s rizikovou komunikaci na internetu oni samotní.

Cílem práce je dále přiblížit problematiku rizikové komunikace a definovat její konkrétní druhy, kterými může být provozována. Výzkumné šetření v návaznosti na to přibližuje, jaké zkušenosti mají studenti vysokých škol s rizikovou komunikací v online prostředí. Výzkumné šetření mapuje nejen současné období, tedy dobu, kdy respondenti studují vysokou školu, ale dává možnost nahlédnout do zkušeností respondentů i retrospektivně, jelikož dotazníkové šetření se zabývalo i obdobím, kdy byli dotazovaní ještě žáky základní, potažmo studenty střední školy.

Tato bakalářská práce je rozdělena do tří hlavních kapitol, kdy první dvě jsou zaměřené spíše teoreticky k ukotvení pojmů, které jsou stěžejními pro tuto práci. První kapitola se zabývá bližším definováním cílové skupiny vysokoškoláků, se kterou se následně pracuje v praktické části práce, specifiky jejich pohybu po internetu a komunikace v něm, zejména pak v kontextu sociálních sítí. Navazující kapitola je teoreticky zaměřena na přiblížení konkrétních druhů rizikové komunikace, se kterými se běžně mohou uživatelé internetu setkat a které jsou následně zkoumány v empirické části práce.

Třetí kapitola je věnována samotnému výzkumnému šetření, které bylo podkladem pro empirickou část této práce. V této kapitole jsou blíže definovány metody užité ke sběru dat, nachází se zde také intepretace a podstata výzkumného problému, výzkumného cíle a dílčích hypotéz, jež byly stanoveny právě na základě výzkumného problému. Následuje analýza výsledků dotazníkového šetření a shrnutí informací z něho získaných.

Toto téma bylo pro bakalářskou práci zvoleno hned z několika důvodů. Online prostředí v dnešní době již obklopuje téměř bez výjimek každého z nás a je téměř nemožné se mu, a tedy i jeho nástrahám, vyhnout. Jednou z mnohých nástrah může být právě riziková komunikace, kterou mohou provozovat lidé vědomě (bez ohledu na to, zda si v plné míře uvědomují právě její rizika či nikoli) nebo nevědomě tím, že se stanou objektem něčí rizikové komunikace. Dalším důvodem bylo i čím dál častější osobní setkávání s tímto druhem internetové komunikace, a to jak již bylo výše zmíněno, ať už

jako aktivní provozovatel této komunikace nebo zprostředkovaně – objekt nebezpečných praktik jiných osob či subjektů.

1 Současní vysokoškolští studenti a online prostředí

Online prostředí a studium na vysoké škole v dnešní době už od sebe nelze jen tak oddělit, jelikož právě používání internetu se stalo nedílnou součástí každodenního života většiny světové populace, a tak ani u vysokoškolských studentů v České republice nemůžeme hledat výjimku. Pobyt v online prostředí je pro vysokoškoláky otázkou nejen odreagování, ale dnes již také studia, práce a velké spousty dalších povinností.

Současní vysokoškoláci, čímž je míněna zejména generace lidí, kteří studují v současné době na vysokých školách v bezprostřední návaznosti na studium střední školy. Tato generace lidí je považována za tzv. „digitální domorodce". Tento termín zpopularizoval americký autor Marc Prensky, když v roce 2001 publikoval odborný článek s názvem *Digital Natives, Digital Immigrants*, kde označuje za digitální domorodce osoby, které se v digitálním světě pohybují téměř od narození a digitálním jazykem se dorozumívají jako rodilí mluvčí. Za ty by se sice dle Prenského (2001, online) daly považovat lidé narození již v posledních pár dekádách 20. století, tedy i generace Y, tzv. mileniálové. Podle již zmíněné charakteristiky „narození do digitálního světa" se vším všudy ale lépe zapadá, zejména tedy v našich podmínkách, generace narozená až po roce 1995, tedy generace označována písmenem „Z". Generace Z bude blíže specifikovaná v následující podkapitole.

Digitální domorodci jsou dle Helsperové (2008, online) dále charakterističtí těmito třemi způsoby chování v online prostředí:

1. Jsou schopni pohotově se vyhnout e-rizikům, jelikož se v online prostředí velmi dobře orientují, a ví, jak v něm bez problémů manévrovat.
2. Online rizikům se předem nevyhýbají, sami jsou totiž schopni používat techniku internetového predátora, ale začnou jednat teprve až se s nějakým rizikem setkají tváří v tvář.
3. Používají tzv. „pštrosí taktiku", což znamená že před případnými nelibými obsahy, které jsou směřovány přímo na jejich osobu, obrazně strčí hlavu do písku tak, že nehodící se obsah rychle odstraní a dále se chovají, jako že k žádnému ohrožení nedošlo, respektive v budoucnu ani nemůže dojít.

Blinka (2015, s. 94) uvádí, že v období dospívání se může internet stát *„spolehlivým a vždy přístupným prostředkem ke zvládání emoční přecitlivělosti a lability"* a je také obdobím s jednou z nejvyšších prevalencí internetové závislosti.

Aktivity v online prostředí, které bývají v tomto věku spojovány s nadměrným užíváním internetu či až se vznikem závislosti, jsou dále konkrétně zejména sledování videí, hraní online her a nadměrné užívaní sociálních sítí, potažmo chatovacích místností (Durkéé a kol., 2012, Kuss a kol., 2013 in Blinka 2015).

Výše zmíněné přílišné užívání internetu a případné závislostní chování na něm by z hlediska vývoje jedinců mohlo souviset s nesplněním nějaké, případně i více ze základních vývojových potřeb a úkolů. Těmito dle Blinky (2015) jsou:

Identita

Experimentování v období dospívání je pro mladé lidi velmi atraktivní a prostředí internetu jim toto bezvýhradně umožňuje. To platí zejména pak v otázce hledání své identity. Internet dává lidem možnost vytvořit si naprosto libovolný obraz o sobě samých, ať už jde třeba o prezentaci svého ideálního já na sociálních sítích, v chatovacích místnostech nebo například při hraní online her.

Socializace

Vytvářeních jakýchsi sociálních dovedností je jedním z dalších důležitých potřeb a úkolů jedince z hlediska jeho správného vývoje. Tyto sociální dovednosti následně umožňují jedincům vytváření blízkých vztahů s vrstevníky, které se časem mohou vyvinout v první romantické prožitky. Jedinci, kteří naopak vykazují známky nadměrného užívání internetu mají pak s naplněním této vývojové potřeby problémy, jelikož následně nemají dostatečné schopnosti k navázání kvalitních mezilidských vztahů.

Sexualita

Stejně tak umožňuje online prostředí dospívajícím experimentovat se svou sexualitou. To se pojí pak zejména na atributy již zmíněné v oblasti experimentování s vlastní identitou, ale také i k oblasti výše zmíněné potřebu socializace. Ta v kontextu sexuality umožňuje dospívajícím experimentovat při komunikaci na sociálních sítích, nebo při hraní online her, ale také v případech sledování stránek a vyhledávání obsahu se sexuálním nebo pornografickým podtextem.

Oblast sexuality a experimentování se v dnešní době poměrně úzce váže k online prostředí. Dalo by se totiž konstatovat, že celý tento proces je vlastně touto cestou

mnohem jednodušší než v reálném světě. Formování sexuální identity nám z období adolescence, kdy se ozývají sexuální touhy, hledají se jakékoli peprné informace a vyvíjí se sexuální hodnoty, může plynule pokračovat i do mladé dospělosti, jak uvádí Ambrožová (2020).

1.1 Specifika vysokoškolských studentů

Na současné studenty vysokých škol můžeme nahlížet z několika hledisek. V této kapitole budou blíže rozebrány konkrétně dvě hlediska, kdy prvé z nich bude, jakým způsobem jsou vnímáni z pohledu vývojové psychologie a druhým hlediskem budou specifika generace, do které tyto osoby, současní vysokoškolští studenti, spadají.

Z hlediska vývojové psychologie je poměrně složité obecně studenty vysokých škol zařadit do jedné konkrétní vývojové skupiny. Dle mého názoru se zkrátka v této etapě života vzájemně prolínají období adolescence a zároveň období mladé dospělosti. To lze však vycítit i z definic různých autorů, kteří k tomu také nemají jasně vyhraněný postoj.

Například Marie Vágnerová (2000, s. 253), která ohraničuje období adolescence věkem od 15 do 20 let konstatuje, že ačkoli toto období z jeho konce ohraničuje *„dovršení přípravného profesního období“*, myšleno zřejmě jako absolvování střední školy či učiliště, po kterém by měl následovat vstup do zaměstnání. Právě skupina vysokoškoláků je tohoto výjimkou, jelikož ve své profesní přípravě pokračují mnohdy ještě několik let po dovršení 20. roku života. Adolescence je také období, které by mělo být ukončeno tím, že se člověk stane ekonomicky samostatným a nezávislým, kdy opět určitá část vysokoškolských studentů tento atribut splňuje, a tedy spíše následně spadají minimálně podle tohoto znaku do skupiny mladých dospělých. Ovšem naopak někteří vysokoškoláci nemají po dobu studia, ať už je bakalářské, magisterské, popřípadě doktorandské, potřebu se ekonomicky osamostatnit. Zůstávají tak například i po celou dobu studia v bezpečí domova u rodičů, případně jim je alespoň ze strany rodičů finančně vypomáháno, tak že plnou ekonomickou samostatnost zatím v závislosti na vlastní existenci řešit nemusí. (Vágnerová, 2000)

Dále i dle Říčana (2006) je konec období adolescence velmi složité jednoznačně určit. To je dáno zejména tím, že toto období není ohraničeno nějakým zásadním mezníkem v biologickém či sociálním vývoji člověka, ale že je tato hranice zkrátka velmi individuální. Říčan proto u vysokoškoláků obrazně přidává tři roky navíc k hranici

„běžného“ ohraničení adolescence, jelikož díky tomu, že si takzvaně prodlužují svou žákovskou roli, adolescenci si tím prodlužují.

Dle Vágnerové (2000) je možným hlavním důvodem nesourodosti v otázce dospívání ten fakt, že role vysokoškoláka nepřichází také automaticky ruku v ruce se statusem dospělého. Z toho důvodu může být pak na vysokoškoláky nahlíženo jako na adolescenty a ne jako na plnohodnotné dospělé.

Dle výše zmíněných autorů, by se ale vysokoškolští studenti nejpozději v druhé polovině třetí dekády svého života měly zapojit do polnohodnotného života mladých dospělých a období adolescence už by mělo být (samozřejmě až na výjimky) zcela překonané.

Generace Z je specifická skupina osob, která se narodila v letech 1995-2010.Tedy alespoň na tomto časovém rozmezí se shoduje většina literatury a často bývá jinak označována například jako již zmínění digitální domorodci, Gen Z, iGens, Post-Millenials, Gen Next, Gen Tech, Rainbow Generation, nebo Generace Me (Závodná a Falch, 2022). Dále pak Jones a Shao (2011) pracují s označením Net Generation. To je odvozené od moderních technologií obklopující tuto generaci téměř od narození a toto označení se dále pojí také s termínem digitální domorodci.

V neposlední řadě je důležité zmínit označení někdy možná až s trochou hanlivého podtextu „*generace sněhových vloček*“ a tomuto označení se této generaci dostálo jak pro svou jedinečnost, ale právě i pro svou křehkost, snadnou zranitelnost a celkovou neurotičnost (Hnilica, 2018, s. 255). Závodná (2022, s. 10) dokonce sněhové vločky popisuje jako *„plačtivé, arogantní, přecitlivělé děti“*. To vše může být způsobeno vlivem hyperprotektivních rodičů, „*neustále nad dítětem vznášejících se rodičů*“, tzv „*helicopter parents*“, ale i učitelů, tedy zejména zástupců generace mileniálů, generace Y (srov. s Harper 2017; Marano 2008; In: Hnilica 2018, s. 255; a Heldal a Stiklestad, 2022, s 218).

1.2 Online prostředí a komunikace v něm

Komunikace v online prostředí je pro uživatele internetu velmi atraktivní, ať už se jedná o jakoukoli věkovou skupinu. Dle mého názoru její potenciálně největší výhodou může být možnost vystupovat naprosto anonymně, což je pro řadu lidí velice lákavé, nebýt alespoň na malou chvíli sám sebou, ale být někým jiným, nebo třeba i „nikým“.

Dle Ambrožové (2020) může při tomto druhu komunikace člověk zapojovat svou fantazii, domýšlet si jak ten druhý člověk, se kterým interaguje, vypadá, dává možnost

komunikovat hned s několika lidmi naráz, a to jak ve skupinové formě například v jednom chatu, tak i jednotlivě s několika navzájem nepropojenými lidmi v samostatných chatech zároveň. Další charakteristikou online komunikace také je, jak se vlastně před pár lety naplno prokázalo, že dokáže uspokojit naši potřebu sdružovat se, i když by to třeba fyzicky nebylo možné.

Krom výše zmíněných zdánlivých výhod se k internetové komunikaci a celkově k online prostředí váže i nemálo negativních jevů. Jak definuje Mareš (2013), jedná se o tzv. „internetový paradox“, který vedle sebe staví prvotní myšlenku informačních a komunikačních technologií, být cenným přínosem pro lidstvo a fakt, že dnes s sebou kyberprostor přináší i nejrůznější závislosti a rizikové jevy. Nejprve optimistický předpoklad internetu jako svobodného a bezpečného místa a postupem času pesimisticky vyhlížející realita, kdy je svět internetem namísto spojování, naopak rozdělován.

Konkrétními riziky by pak dle Kopeckého (2007) mělo být zejména nedostatečné ověřování si informací přebíraných z internetu, závislostní chování a neblahý dopad na fyzickou kondici, prokrastinace na PC, problémy s komunikací v reálném světě, nepřipravenost řešit konfliktní situace z důvodu nedostatečného rozvoje sociální inteligence a například rizika, která vyplývají z rizikové komunikace online.

Hulanová (2012) pak Kopeckého charakteristiku doplňuje o omezení percepce s následkem neschopnosti empatie, anonymitu a zneužívání cizí identity, nereálné vnímání stráveného času online, tzv „sociální mnohočetnost“. Ta je dána navazováním extrémního množství kontaktů, monitorováním a archivací veškeré online interakce, frustrací uživatele v případě, že se objeví technické problémy a disinhibicí uživatelů v kyberprostoru, neboli opadnutím zábran v porovnání s reálným světem.

V oblasti online prostředí a komunikace v něm existují dva sobě navzájem podobné fenomény, kterými jsou tzv. „digital gap“ a „communication gap“. Digital gap neboli digitální propast, která spočívá v neporozumění chování digitálních domorodců, staršími, nebo ne tak zběhlými lidmi v digitálním prostředí, tedy digitálními přistěhovalci. Communication gap, tedy komunikační propast, která zapříčiňuje nejrůznější bariéry pro efektivní komunikaci mezi dvěma lidmi, nejčastěji odlišných generací, jiného jazyka nebo s rozdíly v rodinném či edukačním prostředí. (srov Ambrožová, 2020 a Dyikuk 2019, online)

Phubbing

Ignorování konverzace „in real life“ a namísto toho upřednostňování telefonu. Dle Ambrožové (2020) jsou vysokoškoláci tímto jevem nejohroženější skupinou. To je myšleno tak, že jsou nejvíce náchylní se ubírat k tomuto druhu negativního chování. K „phubování“ může docházet jak ve škole, tak v rodině či partnerských vztazích a takovéto chování je bráno jako velmi nezdvořilé vůči osobám proti kterým je namířeno a dá se řadit až do internetové závislosti. Tzv Phubber, tedy osoba, která záměrně ignoruje druhého člověka, tzv phubeeho, tím, že neustále hledí do svého mobilního telefonu, místo toho aby participovala na společné konverzaci a tím narušuje vlastně veškerou snahu o komunikaci na něj mířenou.

Tele-cocooning

Tento termín úzce souvisí s výše zmíněným phubbingem, jelikož osoby, které provozují phubbing mají tendenci si vytvářet nějaký svůj vlastní svět ve virtuálním prostředí a namísto komunikování tzv face to face v reálném světě se ubírají ke způsobu komunikace s druhou osobou bez potřeby jakéhokoli fyzického kontaktu s ní. Jde tedy vlastně o jakousi intimní interakci člověka s technologií. (Kobayashi, Boase, 2014 in Ambrožová, 2020)

1.3 Sociální sítě

Termínem sociální síť, nebo také sociální média, jak uvádí Kopecký a Mikulcová (2020), nebo někdy zkratkou SNS, z anglického „social network site“, se dle Boydové a Ellisonové (2007) rozumí webová služba, která má za cíl lidem umožnit zejména 3 věci. Zaprvé si její uživatelé na SNS mohou vytvořit veřejný nebo polo-veřejný účet, zadruhé si v rámci té dané sociální sítě mohou vytvořit seznam z dalších uživatelů, se kterými jsou ve spojení a zatřetí jim daný systém také umožňuje si procházet a prohlížet výše zmíněný seznam, spolu se seznamy ostatních uživatelů registrovaných na dané sociální síti.

Sociální sítě ovšem neslouží jen k výše zmíněným aktivitám a rozhodně neslouží primárně pouze jednotlivcům k vytváření si osobních účtů, ale samozřejmě umožňují vytvářet i profily firemní, diskuzní fóra či prezentace a zejména dnes je jejich neodmyslitelnou a z mého pohledu i nejvýznamnější součástí, samozřejmě spolu

s komunikací, možnost sdílení fotografií, videí a dalších jiných obsahů, jak mimo jiné zmiňují i Kožíšek s Píseckým (2016).

Ševčíková (2014) pak za přednosti sociálních sítí považuje zejména již zmíněnou komunikaci uživatelů, spolu s možností sebeprezentace každého jedince.

Dle Kopeckého a Mikulcové (2020) je sociální sítí internetová služba, která slouží nejen k vzájemnému propojování uživatelů SS, ale zejména pak k navazování a udržování vztahů a kontaktů napříč celým světem. Pomocí vytvořených uživatelských profilů se následně osoby mohou na internetu prezentovat, sdílet nejrůznější příspěvky, ať už ve formě fotografií, videí, či textu a takovéto příspěvky ostatních uživatelů následně komentovat nebo hodnotit dle libosti, ovšem v rámci uživatelských pravidel každé takové platformy.

Dále například dle Černé (2013) je nejvýznamnějším znakem sociálních sítí pak možnost být v kontaktu s druhými lidmi a být v obraze, co právě tito lidé, v podstatě reálném čase, dělají.

Ve spojitosti s nadměrným trávením volného času v online prostředí, respektive konkrétněji na sociálních sítích byl zaveden pojem odvozený přímo od jedné z největších sociálních sítí světa, a to „facebooková deprese“. O té se dá dle Okeeffeové a Clarke-Pearsonové (2011, online) hovořit v případech, že uživatelé tráví přespříliš času právě na sociálních sítích, až se u nich projeví symptomy klasické deprese. Ambrožová (2020) termín doplňuje tím, že je sice odvozen od jedné konkrétní sociální sítě, ale lze chápat daleko šířeji v kontextu ostatních sociálních sítí. Deprese se může rozvinout z důvodu neustálého porovnávání našeho „obyčejného“ života s tím zdánlivě perfektním, jak ho vyobrazují na SS ostatní uživatelé. Kvůli tomu se člověk může cítit frustrovaný, až méněcenný, obzvláště pokud neoplývá určitou psychickou resiliencí, či dostatečnou mírou kritického myšlení.

Mimo jiné, například Dulovics (2021) uvádí, že navazování kontaktu s neznámými osobami a například účast v rizikových online skupinách, které mohou podporovat nějaké patologické chování a také neuvážené rozesílání obrazových materiálů a informací patří mezi základní oblasti rozdělení online rizikového chování, ohrožující vlastní osobu a dále pak různé formy kyberšikany spolu s šířením nevhodných obsahů, kterými mohou například být poplašné, zavádějící či nesnášenlivé.

K nejvýznamnějším a bezpochyby i nejpoužívanějším mezinárodním sociálním sítím pak konkrétně patří zejména Facebook, Instagram, WhatsApp, Facebook

Messenger, Twitter, Snapchat a TikTok, ale to je ovšem jen výčet těch pár z mého pohledu opravdu nejvyužívanějších.

Co se českých sociálních sítí týče, tak za zmínku dle mého názoru stojí, dnes již neexistující, Lidé.cz, což byla dle autorů Kožíška a Píseckého (2016) *„největší česká seznamovací síť“*, jejíž počátky se datují až k roku 1997, tedy do doby, kdy u českých uživatelů nebyly ještě tak hojně využívané mezinárodní sociální sítě. V dobách největší slávy tuto českou sociální síť využívaly stovky tisíc lidí. Jak mimochodem uvádí David Slížek (2014), tak konkrétně roku 2014, kdy se její koncepce proměnila vyloženě na seznamku, existovalo na této síti na 280 000 profilů a denně tuto již koncepčně seznamku používalo zhruba 100 000 reálných uživatelů, což v českém měřítku nebylo rozhodně málo. Ovšem nejenom změna koncepce, ale zejména dokumentární film V síti Víta Klusáka, zapříčinil roku 2020 definitivní konec této české sociální sítě, jelikož se ukázalo, že je výživným podhoubím právě pro takové kyber predátory, na které byl zaměřen zmíněný dokument. Tuto sociální síť jsem se rozhodla blíže popsat z toho důvodu, že byla podkladem právě dokumentárního snímku V Síti, kdy jeho shlédnutí mne přimělo zaměřit svou bakalářskou práci právě na problematiku rizikové komunikace v prostředí internetu.

2 Riziková komunikace v online prostředí a její konkrétní formy

Mezi bezpečnou a rizikovou komunikací v online prostředí je dle Kopeckého (2021) velmi tenká hranice, což vyplývá již z podstaty kyberprostředí a psychologie samotné. Ohroženi překročením této hranice jsou pak zejména nezkušení dospělí lidé či děti, které zatím nemají dostatečné povědomí o zásadách bezpečného pohybu po internetu. Rizikovou komunikaci v online prostředí můžeme chápat tedy jako jakoukoli interakci mezi internetovými uživateli, která by mohla ať už skrze posílání textových zpráv, fotografií, obrázků, videí či jiných obsahů ublížit buďto příjemci takového materiálu, jejímu odesílateli, nebo i třetí straně, tedy někomu ne přímo zúčastněnému.

K rizikové komunikaci na internetu se velmi úzce váže pojem sociální inženýrství. To ovšem, jak by se dle názvu mohlo zdát, není jakási společensky prospěšná aktivita, provozována skrze internet, zpravidla vysokoškolsky vzdělaným člověkem s inženýrským titulem, ale jedná se o souhrnný název pro manipulativní chování v prostředí internetu, kdy člověk vědomě a záměrně manipuluje lidmi a informacemi s vidinou osobního prospěchu. Toho zkouší nejčastěji dosáhnout rozesíláním podvodných e-mailů, vydáváním se za někoho jiného a sází tak zejména na chybný úsudek své oběti. Tento termín je nejčastěji spojován s internetovými podvody, kdy například právě skrze e-mailovou korespondenci přijde zpráva, která na první pohled vypadá jako od konkrétní banky a ve zprávě je požadováno po adresátovi vyplnění osobních údajů. Příjemce následně na základě chybného úsudku sdělí sociálním inženýrům, kteří si na něj podvod připravili, cenné osobní údaje. Ovšem do sociálního inženýrství lze díky jeho charakteristice také zahrnout takzvané „kybergroomery“, kteří cílí pak zejména na mladší populaci, která bývá častokrát velmi důvěřivá a nezkušená, a tak jsou tito jedinci schopni naprosto cizím lidem, kteří se vydávají za někoho jiného, věkově, ale třeba i zájmy dítěti blízkého, sdělit velmi osobní informace. (Dočekal, Eckertová, 2013)

Sociální inženýrství má také své specifické fáze, které jsou i výše zmiňovanému kybergroomingu v některých ohledech velmi podobné. To platí tedy zejména pokud se jedná o útoky na předem vytipované oběti a nejde o tzv „rozhození sítí“, tedy útoky náhodné, ve většině případů realizované skrze e-mailovou korespondenci ve formě tzv „spamů“.

Celkem se dají vytipované útoky rozčlenit do 6 fází:

1. Nejdříve přichází, jak sám název napovídá, „tipování“ - v této fázi jde zejména o zaměření se na určitou skupinu osob, ať už může být kritériem pro tipování věk oběti, pohlaví, zájmy nebo místo bydliště.
2. Druhá v pořadí přichází fáze „vytvoření si důvěryhodného profilu“, který bude mít za cíl vzbudit v obětech dojem, že se jedná o skutečného člověka, svými zájmy, věkem, pohlavím, či bydlištěm, velmi podobného vytipované oběti či skupině obětí.
3. Následuje fáze, kdy si sociální inženýři vyberou svou oběť pečlivě podle jejího věku, jak uvádí Kožíšek a Písecký (2016), kdy si striktně vymezí konkrétní věkovou hranici, jakou může být např. 10-11 let. V případě, že by se jednalo o opravdové dětí, které by se chtěly seznámit s novými lidmi skrze internet, by se takto explicitně vyjádřená věková hranice zřejmě neobjevila ,a tak toto může být jeden z faktorů, kterým může být takový sociální inženýr s falešným profilem, zaměřující se na „lovení“ dětí, snadněji rozpoznatelný od opravdových profilů.
4. V další fázi, kdy již kontaktovali svou oběť se podvodníci budou snažit co nejvíce se přizpůsobit mluvě vytipované oběti a mít podobné zájmy, jaké si u ní zjistili v rámci fáze 1.
5. Předposledním stupněm je přitvrzení, jež spočívá v umění sociálního inženýra vycítit, že je oběť ochotna komunikovat i o ožehavých tématech, a tak na tyto následně sociální inženýr komunikaci úmyslně směřuje.
6. Posledním stadiem je „nabídka schůzky“, ale ta je zdaleka nejcharakterističtější pro již zmíněný kybergrooming, jako dílčí formu sociálního inženýrství. (Kožíšek, Písecký, 2016)

2.1 Kyberšikana

S rozmachem informačních a komunikačních technologií, se začala přesouvat „tradiční“ šikana z prostředí fyzického do toho virtuálního. Tak vznikla nová forma šikany – kyberšikana. V odborné literatuře se ale můžeme setkat také s názvy jako online obtěžování, elektronická agrese, online šikana, e-šikanování nebo internetové či digitální šikanování a mnoho dalšími označeními, ovšem nejrozšířenějším a celosvětově nejhojněji využívaným termínem je právě kyberšikana, jak uvádí Hollá (2016).

Hinduja a Patchin (2006) cyberbullying, jak se nazývá kyberšikana v angličtině, definují jako „*úmyslné a opakované ubližování prostřednictvím elektronického textu, provozované zejména skrze internet či mobilní telefon*“. Obecněji by se dalo říci, že se jedná o šikanu provozovanou prostřednictvím informačních a komunikačních technologií.

Kyberšikana je charakteristická zejména anonymitou agresora, také smazává nepoměr sil mezi oběma stranami, jelikož kyberagresor již oproti původci obyčejné „tradiční“ šikany nemusí oplývat nějakou významnou fyzickou převahou, ale tato převaha může být nahrazena právě technickou zdatností. Tato forma šikany může mít podobu verbálních útoků, neoprávněného šíření fotografií, videí, či audio nahrávek, ztrapňování, výhrůžek, zastrašování, vydírání, nebo třeba krádeže identity. Od klasické šikany se dále liší tím, že může být neustálá, obzvlášť v dnešní době, kdy si většina lidí neumí představit svůj den bez mobilního telefonu a i při práci či studiu se častokrát již bez informačních a komunikačních technologií také neobejdeme. Podobně jako u tradiční šikany, je také jednou z důležitých charakteristik dlouhodobost. Ta je ovšem v případě kyberšikany velmi těžce definovatelná, jelikož nemusí spočívat přímo v tom, že jeden kyberagresor dlouhodobě, systematicky, úmyslně šikanuje svou oběť skrze IKT, ale může být dána tím, že někdo přidá či rozešle jednorázově nějaký pro oběť citlivý obsah a ten se pak následně naprosto nekontrolovatelně šíří internetem, kdy je téměř nemožné zajistit jeho definitivní odstranění, jelikož si ho do doby stažení z internetu mohl kdokoli uložit a kdykoli ho může opět zneužít, či šířit dál. (Kožíšek, Písecký, 2016)

Dle Hroncové et al (2020) se kyberšikana od šikany klasické může odlišovat tím, že v případě kyberšikany oběť pachatele na rozdíl od šikany tradiční znát nemusí, což může být dané zejména již zmíněnou anonymitou a dalším rozdílem je, že kyberšikana na rozdíl od šikany normální může probíhat naprosto všude tam, kde dostupné internetové připojení a tedy oběť je v neustálém stresu z toho, kdy přijde další atak.

Smith, del Barrio a Torkunaga (2013) dále pak vidí rozdíl také v rozložení sil, co se týče původce a oběti šikany, potažmo kyberšikany, jelikož při šikaně elektronické nemusí mít pachatel nějakou výraznou zejména fyzickou, ale i psychickou převahu nad obětí, jelikož při kyberšikaně je převaha dána schopností využití informačních a komunikačních technologií.

Z důvodu komplexnosti této problematiky a nesnadnosti jejího finálního a ustáleného definování se ovšem u některých autorů můžeme setkat se zajímavým pohledem na celý fenomén kyberšikany, a to takovým, že někteří autoři pod tento

celosvětově rozšířený problém zahrnují i další formy rizikové komunikace, které budou v této práci dále rozebrány, a to sexting, happy slapping, kybergrooming, nesnášenlivost na internetu a také nevyžádanou poštu (Hulanová, 2012; Hudecová a Kurčíková. 2014; In Hollá 2016).

2.2 Kybergrooming

Kybergroomingem se dle Kopeckého (2010, online) rozumí jednání internetových uživatelů, které má za cíl vybudovat falešnou důvěru a tím vylákat svou oběť na osobní schůzku. Pokud kybergroomer ovšem uspěje může schůzka vyústit v sexuální zneužití oběti, fyzické napadení, či zneužití k výrobě pornografie, zejména tedy té dětské a dalšímu (Kopecký a kol, 2015, online).

Jak jsem již v jedné z předchozích kapitol zmínila, sociální inženýrství a kybergrooming toho mají dosti společného, ale přesto je důležité zdůraznit, že se nejedná o jedno a totéž. Sociální inženýrství je spíše jakýmsi souborem strategií a technik, jak sice manipulovat protistranou, získat od ní osobní údaje a jiné citlivé obsahy, ale na rozdíl od kybergroomingu, v případě sociálního inženýrství není primárním cílem internetové aktivity sexuální zneužití oběti. Kybergroomer tedy pak pouze využívá jednotlivých technik sociálního inženýrství jejichž výsledkem má být dostatečné zmanipulování oběti na to, aby svolila k osobní schůzce, na které by pak mělo dojít k sexuálnímu zneužití, což je právě primárním cílem aktivity kybergroomera. (Kopecký a kol, 2015, online)

Kybergrooming má podobně jako sociální inženýrství také své specifické etapy a ty Kopecký, Szotkowski a Dobešová (2021) rozdělil takto:

Příprava na kontakt s obětí

V této fázi si dá kybergroomer práci zaprvé s vyhledáním oběti například na nejrůznějších diskuzních fórech, jež jsou orientovány zejména na děti, nebo své oběti vyhledává na sociálních sítích, kde si mohou vytřídit uživatele dle preferovaného věku, pohlaví, místa bydliště atd. Zadruhé si v této fázi predátor vytváří věrohodný falešný profil, který slouží zejména jako pojistka pro nesnadnější dohledání jeho opravdové identity a také si fiktivní identitu volí z toho důvod, aby byl pro svou cílovou skupinu zejména věkově atraktivnější, než by tomu bylo při používání jeho pravé identity. Zatřetí

si může v této počáteční fázi vypomoci tzv. falešnou autoritou, která následně dodává informacím, které bude se svými oběťmi sdílet, na věrohodnosti.

Kontaktování oběti

Tato fáze spočívá v samotném oslovení oběti, zejména skrze nějakou sociální síť, chatovací službu, nebo video chat a zpravidla se oslovení oběti děje tzv. nedopatřením, jelikož konverzace začíná často slovy *„ahoj, omylem jsem si tě přidal do přátel, …“* A poté přistupuje útočník k etapě třetí.

Budování a prohlubování vztahu

Podstatou této etapy je ta vůbec nejesenciálnější složka kybergroomingu a tou je manipulace. Útočník si volí, jakou manipulativní techniku zrovna použije, vzhledem k osobnosti oběti, nebo přímo jeho momentálního osobního rozpoložení. Nejčastěji se kybergroomeři schylují k tzv „efektu zrcadlení“, jehož principem je snaha napodobit svou oběť, a tak se jí zalíbit. Snaží se mít podobné koníčky, jako oběť, podobné problémy nebo názory, s cílem prolomit pomyslné ledy v nastolené konverzaci a působit jako spřízněná duše. Následně se snaží pozitivně zapůsobit na svou oběť a získat si její sympatie, získat od ní co nejvíce osobních informací, aby mohl začít s tzv. profilací oběti. Ta spočívá v zálohování veškerých získaných informací, které mu oběť buď sama sdělila, nebo byly na internetu volně dostupné/dohledatelné. Touto aktivitou si predátor pak zejména připravuje půdu k pozdějšímu vydírání oběti, ale také si každou svou oběť profiluje z toho důvodu, aby se mu to zkrátka nepletlo a aby zůstával po celou dobu konverzace v obraze.

Krom manipulace může útočník přistupovat k oběti za použití techniky nazývané „vábení a uplácení“, kdy jeho kýženým cílem je dostat z oběti informace o místu bydliště, o telefonním čísle a dalších, a tyto údaje se snaží z oběti vylákat pod záminkou zaslání různých darů, kreditu, či dnes již spíše mobilních dat, k čemuž právě zejména tyto dva zmíněné údaje potřebuje. Nejde však jen o to dostat z oběti její telefonní číslo či místo bydliště, útočník se pomocí techniky uplácení může snažit získat fotografie své oběti a to zejména pak ty intimní, které by mohl následně využít k praktikám jako je vydírání či vyhrožování a dalším nebezpečným důsledkům spojených se zasíláním sexuálních obsahů, tedy sextingem.

Příprava na osobní schůzku a její realizace

Dle Kopeckého dělení jde o poslední fázi kybergroomingu, kdy útočník, který stále skrývá svou pravou identitu pokračuje ve své manipulaci, tentokrát v podobě „izolace oběti od okolí“. Tímto krokem získává absolutní důvěru oběti a zajišťuje si tak její mlčenlivost. Izolací se rozumí navázání tak důvěrného pouta, které je postaveno na nejrůznějších vzájemně si sdělených tajemstvích, zejména tedy těch intimních, je v tom případě, že se útočník pokusí začít vydírat svou oběť těmito materiály, jeho oběť natolik paralyzovaná/zahnaná do kouta, že se již nemůže efektivně a racionálně bránit.

Vyvrcholením této fáze kybergroomingové manipulace je pak osobní setkání oběti s útočníkem, které se v těch pozitivních případech může proměnit v nevinnou schůzku, ale také může skončit dle těch nejčernějších scénářů třeba fyzickým útokem či sexuálním napadením, nebo také přinucením oběti k výrobě pornografie, provozování prostituce, opakovaným zneužíváním nebo až smrtí. Pokud ovšem oběť zažije nějaký traumatizující zážitek při osobním setkání s kybergroomerem následky mohou být obrovské a fatální dopad má celá taková zkušenost zejména na psychiku oběti.

2.3 Sexting

Další formou rizikové komunikace, na kterou se zaměřuje tato bakalářská práce je sexting. Döringová (2014) tento termín charakterizuje jako vyměňování osobních intimních obsahů vlastní výroby skrze mobilní telefon či přes internet. Tento termín charakterizuje zasílání, přeposílání či sdílení vlastních či cizích intimně laděných zpráv, videí a fotografií skrze moderní komunikační technologie. Jde jak o umisťování sexuálně laděného obsahu na internet samotný, tedy například v rámci svého vlastního profilu na některé ze sociálních sítí, ale také odesílání takového obsahu soukromě jiným uživatelům. (Eckertová, Dočekal, 2013)

Jak uvádí Kopecký (2021a, online), tak zejména v případě provozování tohoto druhu rizikové online komunikace, se aktéři vystavují enormnímu riziku zneužití jejich intimních materiálů v kyber světě. Problémem pak je zejména to, že tyto materiály sdílejí s ostatními lidmi zcela dobrovolně a vědomě, v rámci seznamování nebo partnerských vztahů a nepřipouští si to, že v případě rozpadu těchto vztahů se mohou takové materiály stál prostředkem vydírání nebo vyhrožování v nejrůznějších podobách, které budou dále v textu konkretizovány a přiblíženy. Tento způsob internetové interakce je akademickým diskurzem vnímán jako vysoce rizikový, a nejohroženější skupinou jsou dospívající lidé,

zejména dívky. Dle zjištění Döringové (2014) je ale sexting přeci jen rozšířenější mezi dospělými, respektive mladými dospělými než mezi mládeží.

Hollá (2016) dělí sexting na aktivní a pasivní, podle toho, zdali se jeho aktéři aktivním způsobem zapojují do zasílání a sdílení ať už vlastních či cizích erotických materiálů, nebo tyto materiály po někom vyžadují, a nebo v druhém případě se do této rizikové aktivity zapojují pasivně, tedy nepřímo, tak, že pouze přijímají takovéto materiály, bez toho aniž by je po někom vyžadovali nebo tuto aktivitu sami iniciovali.

Kybersex

Kybersex je dle mého názoru takovým pomyslně vyšším stupínkem sextingu. Divínová (2005) kybersex totiž popisuje jako online vyměňování si sugestivních či explicitně erotických zpráv a sexuálních fantazií, které je zpravidla doprovázeno masturbací zúčastněných osob. Jako většina aktivit na internetu má kybersex ovšem jak svá pozitiva, tak i negativa. Za pozitivum by se dle mého názoru dal považovat ten fakt, že dává člověku možnost experimentovat se svou sexualitou a určitým způsobem růst po této osobnostní stránce. Na stranu druhou se na takové aktivitě dá snadno získat závislost, což muže mít naopak velmi negativní dopad na sociální a zejména pak partnerský život jedince, jelikož je možné, že najednou přestane mít zájem o to, intimně se sbližovat buďto se svým stávajícím partnerem či dalšími osobami v budoucnu v reálném světě.

2.4 Phishing

„Rhybaření“, takto by se dala do češtiny přeložit nechvalně známá, podvodná technika užívána v elektronické komunikaci, neboli phishing. Její podstatou je zasílání nevyžádaných zpráv zejména prostřednictvím e-mailové komunikace, SMS zpráv, ale dnes také velmi rozšířených zpráv na sociálních sítích, které se často tváří, jako neškodné zprávy od našich internetových přátel a obsahují nebezpečný odkaz, který příjemce přesměruje na pravě vypadající stránky nějaké známé instituce nebo internetové platformy s cílem vylákat z příjemce citlivé osobní údaje.

Jak zmiňují Eckertová a Dočekal (2013), tak těmi nejčastějšími se myslí údaje důležité pro přístup k uživatelským účtům na sociálních sítích, ale také například k internetovému bankovnictví. Phishing je důmyslnou aktivitou již zmíněných sociálních inženýrů, kteří se snaží takovéto informace vylákat ze svých obětí za pomocí nejrůznějších manipulačních technik a lákavých slovních obratů, které ovšem nejsou

vždy prosty pravopisných a dalších jazykových chyb, což může být právě jedním z ukazatelů, že daná zpráva může být právě pokusem o phishingový útok Cílem této podvodné techniky, nejčastěji využívané již zmíněnými sociálními inženýry, je vylákat z příjemce této zprávy citlivé osobní údaje, zejména přístupy k uživatelským účtům na sociálních sítích, ale také například k internetovému bankovnictví. (Kožíšek, Písecký, 2016)

Důležité je dle mého názoru alespoň zmínit další dvě praktiky spadající pod phishing, kterými jsou vishing a pharming, ačkoli tyto se zpravidla neodehrávají buďto online nebo se nešíří nějakým druhem internetové komunikace.

Vishing

Tento druh rizikové komunikace vznikl spojením slov voice, tedy hlas, a phishing a nejenom svým názvem je tato technika phishingu podobná, ale podobá se mu právě svou podstatou, jelikož při jejím použití jde také o získání a zneužití citlivých osobních údajů, to vše ale skrze využití fingovaného telefonátu. Citlivé informace tedy útočník z oběti vymámí za použití svého hlasu a nejčastěji vydáváním se za osobu z nějaké veřejné či státní instituce. Útočníci se mnohdy představují jako zaměstnanci banky, nebo příslušníci PČR a za použití legendy o napadení bankovního účtu oběti naléhají na sdělení zejména přístupů k internetovému bankovnictví nebo citlivých údajů o platební kartě. (Vodafone, 2023, online)

Pharming

Tato podvodná technika je zjednodušeně takovým phishingem bez návnady, jelikož v technice pharmingu zkrátka zchází ten element svádění, manipulace, který je pro phishing esenciální. Pharming je totiž charakteristický přesměrováním na právě vypadající stránku, kterou běžně používáme, za rozdílu že tato je ve skutečnosti falešná a jako pravá se bohužel jen velmi obstojně tváří, takže při nedostatečné obezřetnosti může tak oběť vyplnit například přihlašovací údaje do internetového bankovnictví na velmi zdařilé a téměř nerozpoznatelné falešné stránce. (Kohout a Karchňák, 2016)

Spear phishing

V otázce, na koho je spear phishing cílený, jde o přesný opak klasického phishingu, jelikož ten je typický rozesíláním velkého množství e-mailů na náhodné adresy, kdežto

v případě spear phishingu se cíli na konkrétní osoby, často na konkrétní pozici nebo rovnou určitého vysoce postaveného manažera konkrétní firmy. Fakt, že tato praktika cílí na konkrétní e-mailové účty a schovává se za účty opravdu používané například v dané firmě, z ní dělá těžko zachytitelnou pro tzv. antiphishingový filtr, takže není zařazena do spamu, ale mezi normální příchozí poštu a tím i těžko rozpoznatelnou pro jejího příjemce, například bez gramatických chyb. Zpráva podobně jako klasický phishingový e-mail obsahuje škodlivý odkaz, který ale pak zjednodušeně řečeno parazituje přímo v počítači a shromažďuje více spíše citlivé informace, které jsou předmětem duševního vlastnictví a ne jen „obyčejné osobní údaje“. (Čermák, 2012, online)

2.5 Hating

Nenávistné projevy v online prostředí, neboli hating, jak jej definuje Kopecký a Mikulcová (2020), je neustále rozrůstající se fenomén, který je například spolu s kyberšikanou či kybergroomingem dalším projevem agrese v prostředí internetu. Tento jev je charakteristický přidáváním nenávistných obsahů skrze sociální sítě, zejména v sekcích komentářů, diskuzí anebo přímo v soukromých chatech atd. Nejčastěji je hating namířen proti nejrůznějším skupinám osob či menšinám, z řad etnických, náboženských či sexuálních, ale to není podmínkou, jelikož objektem nenávistného projevu se může na internetu stát téměř kdokoli bez ohledu na to, zdali je příslušníkem některé ze zmíněných skupin či menšin. Tento jev je opět velmi úzce propojen s již výše zmíněnou disinhibicí osob v online prostoru, vlivem které lidé ztrácejí zábrany, jelikož nabývají dojmu, že mohou vystupovat zcela anonymně.

Tento typ rizikové online komunikace je dále úzce spojován s problematikou hoaxů a dezinformací, které mohou být výtvorem tzv. internetových trollů, což jsou dle Kopeckého (2011) uživatelé internetu, kteří záměrně narušují veřejné diskuze nebo chaty vkládáním nevhodného a kontroverzního obsahu s úmyslem takovou konverzaci ještě více emocionálně vyhrotit, za účelem vlastního pobavení nebo naprostého znehodnocení dané, do té doby třeba i věcné, diskuze.

Jak uvádí Waqas, Salminen, Jung, Almerekhi a Jansen (2019, online), k problematice hatingu se neodmyslitelně pojí následující pojmy:

- **Online firestorms** – online bouře, nebo lépe spíše online přestřelky, jsou pobuřující formy internetových diskuzí, které se většinou odehrávají v rámci diskuzních fórem mezi soupeřícími skupinkami.

- **Online hatespeech** – doslovně tedy nenávistné projevy, v tomto případě ale na rozdíl od „obyčejného“ hatingu, již klasifikovány jako tresný čin, který definuje §356 trestního zákoníku – „podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod“.
- **Online toxicity** – online toxicita je druh rizikové komunikace v prostředí internetu, která spočívá v komentování příspěvků na sociálních sítích za účelem odradit další potencionální přispěvatele, komentující, od participování v rozjeté diskuzi, z toho důvodu, že je velká pravděpodobnost, že budou právě těmi komentujícími, kteří se toxicky vůči druhým vyjadřují, přede všemi zesměšněni.

2.6 Další druhy online rizikové komunikace

Oba níže zmíněné druhy rizikové komunikace, potažmo rizikového chování na internetu se dají dle Dvořákové (2020, online) zahrnout do oblasti tzv. nekonsenzuální pornografie, nebo také tzv. „*image-based sexual abuse*“, což znamená v překladu „sexuální zneužívání na základě obrazového materiálu“ a jedná se často právě o kombinaci výše popsaných druhů rizikové komunikace, jelikož obsahují ať už prvky kyberšikany, phishingu, sextingu nebo třeba kybergroomingu.

Revenge porn

Takzvanou „porno-pomstou“ se rozumí druh kyberšikany, která vychází z materiálů vytvořených k provozování sextingu, kdy dochází k nekontrolovanému šíření vlastních sexuálních materiálů konkrétní osoby, ovšem bez jejího souhlasu za účelem jí ublížit, ponížit nebo poškodit pověst daného člověka. Oběťmi takového činu se nejčastěji stávají dívky, potažmo ženy a naopak šiřiteli těchto obsahů jsou zejména jejich bývalí partneři, jelikož nejčastěji se k takovýmto činům schylují osoby po nezvládnutých rozchodech, nebo revenge porn může být v některých případech i součástí stalkingu. Tento rizikový jev je o to závažnější, jelikož šiřitelé si neberou servítky se zveřejněním detailních osobních informací o dané osobě, jako jsou jméno, či bydliště. Ovšem ne vždy jsou všechny informace pojící se k porno pomstě pravdivé, šiřitelé jsou totiž schopni připojovat i údaje naprosto smyšlené za účelem ještě více poškodit danou osobu. Jelikož jsou ale sociální sítě často správně vyhodnotit škodlivý obsah, tak příspěvky jako revenge porn ze svých sítí úspěšně odstraňují, což ale vede k šíření takových obsahů soukromými

zprávami, e-maily nebo třeba skrze speciální webové, či rovnou porno stránky. (E-Bezpečí, 2021, online)

Sama mohu potvrdit, že při pouhém zadání do internetového vyhledávače sousloví „revenge porn“, prohlížeč mezi pár odbornými články nabídnul hned několik odkazů se zadaným termínem přímo na pornostránky, kde jak se domnívám, byla nasdílena právě taková kompromitující videa.

Sextortion

Termín složený z anglických slov „sex“ a „extortion“, neboli vydírání, je spojením zejména phishingu a kybergroomingu, kdy je často předem vytipovaná oběť nucena pod pohrůžkou zveřejnění erotických materiálů, které mohou být často i smyšlené, vytvářet a zasílat nejen čím dál explicitnější erotické fotografie či videa, ale může být také manipulována k osobnímu setkání, což může vyústit až v sexuální zneužití. Jedná se vlastně o přesný příklad praktik zobrazených v dokumentárním filmu V Síti, jak zmiňuje Dvořáková (2020).

Kopecký (2021b, online) pak dělí tuto praktiku podle druhu osob, na které je zaměřená následovně:

- Na konkrétní osobu – zpravidla začíná oslovením na sociálních sítích od neznámé osoby, nejčastěji ženy, která postupně se svou obětí buduje vztah, podobně jako klasický kybergroomer. Tato osoba z oběti pak začne lákat fotografie, mimojiné i intimního charakteru, nebo manipuluje ke komunikaci přes webkameru následně se snahou získat intimní záběry, případně přímo masturbaci. Celý takový průběh konverzace si ovšem pachatel/ka nahrává a připravuje si tak půdu k pozdějšímu vydírání.
- Na osobu náhodnou, pomocí zasílání e-mailového spamu – nejčastěji se v sekci spamu v elektronické poště objeví zpráva o tom, že *„neznámý hacker pronikl do počítače, získal přístup ke všem našim složkám a také webkameře, už mnoho měsíců nás nahrává a získal naše intimní záběry a pokud nezaplatíme, všechny tyto materiály zveřejní a poškodí naši pověst“*. Tato taktika je tedy postavená na strachu z toho, že se nám opravdu někdo naboural do počítače, což ovšem vůbec nemusí být pravda a jedná se o pouhou manipulaci.

3 Zkušenosti studentů vysokých škol s online rizikovou komunikací

V této kapitole se nachází nejprve přiblížení metodologických východisek, pomocí kterých bylo koncipováno výzkumné šetření. Následně se zde nachází popis a přiblížení charakteristik výzkumného souboru a samotná analýza výsledků realizovaného výzkumného šetření. Závěr této kapitoly je věnován shrnutí výsledků získaných dotazníkovým šetřením.

3.1 Metodologická východiska

Pro účely výzkumného šetření byl nejdříve stanoven výzkumný problém, který zněl: Jaké zkušenosti mají studenti VŠ s rizikovou komunikací v online prostředí? Výzkumný problém dle Gavory (2010) udává základní orientaci výzkumu. Může být formulován otázkou, ale i větou oznamovací, přičemž ona věta oznamovací by se následně měla dát přeformulovat případně i do tvaru tázacího. Odpovědí na otázku formulovanou výzkumným problémem by pak měl být výsledek výzkumu.

V návaznosti na stanovený výzkumný problém byl definován výzkumný cíl práce. Ten určuje, čeho by se mělo výzkumným šetřením dosáhnout (Reichel, 2009 in Knytl, Křívánková, 2022). Výzkumný cíl stanovený pro tuto práci zněl: Zjistit, zdali se dotázaní vysokoškolští studenti v různých etapách svého života setkali v online prostředí s konkrétními zkoumanými formami rizikové komunikace, zdali tyto konkrétní formy internetové komunikace sami provozují, v minulosti provozovali, nebo zda se stali objektem některé z forem rizikové komunikace, kterými se bakalářská práce zabývá.

Jak uvádí Gavora (2010, s. 63) „*hypotéza je vědecký předpoklad*“, který je vyvozen z vědecké teorie. Nutností pro tento předpoklad je, že se musí opírat o poznatky, které jsou zatím o zkoumaném jevu známy nebo musí vycházet z praktických zkušeností autora výzkumu. Hlavní funkcí stanovených hypotéz je dále vyvrátit či potvrdit daný předpoklad, který byl hypotézou formulovaný. Pro výzkumné šetření, které bylo podkladem empirické části této bakalářské práce byly stanoveny následující **hypotézy**:

- **H1**: Obětmi manipulativní internetové komunikace jsou alespoň dvakrát častěji mladší uživatelé internetu
- **H2:** Více než pětina dotázaných se setkala na vlastní kůži s phishingem.

- **H3:** Ochota jít na osobní schůzku s neznámým člověkem z internetu s věkem respondentů roste.
- **H4:** Dotázané ženy se staly obětí kyberšikany více jak čtyřikrát častěji než muži.
- **H5**: Více než polovina dotázaných se setkala s nenávistnými projevy na internetu.
- **H6**: Prevalence provozování sextingu s přibývajícím věkem respondentů stoupá minimálně o 10 %.

Podložení hypotéz

H1: Obětmi manipulativní internetové komunikace jsou alespoň dvakrát častěji mladší uživatelé internetu.

Ke stanovení této hypotézy vedl výrok K. Kopeckého (2009), který uvádí, že manipulativní online komunikací jsou nejvíce ohroženy zejména žáci ZŠ. V jejich věku jim totiž schází určitý stupeň mediální gramotnosti na to, aby dokázali kriticky uvažovat nad některými jim adresovanými informacemi. Tím pádem se online manipulátorem nechají přesvědčit podstatně snadněji oproti ostatním, mediálně gramotnějším, uživatelům internetu.

H2: Více než pětina dotázaných se setkala na vlastní kůži s phishingem.

Tato hypotéza vychází z poznatků zabezpečovací firmy Avast, která v roce 2020 uvedla, že na 24 % Čechů a Češek se ve svém životě setkalo s podivně vypadajícím e-mailem či zprávou od někoho známého s urgentní výzvou pro zadání osobních údajů po kliknutí na zaslaný internetový odkaz.

H3: Ochota jít na osobní schůzku s neznámým člověkem z internetu s věkem respondentů roste.

Tato hypotéza byla stanovena na základě výzkumů K. Kopeckého 2011, kdy ochotu jít na osobní schůzku s neznámou osobou z internetu, projevilo 39,09 % dotázaných dětí ve věku 11-17, a i v roce 2015 by bylo schopné přistoupit na takovou schůzku 40,22 % dětí stejného věku. Kdežto z výzkumu z roku 2013, který byl zaměřen výhradně na studenty PdF UPOL, by již bylo ochotných jít na schůzku s člověkem, kterého poznali na internetu 55,71 % dotázaných. To může být sice podmíněné tím, že poznávání nových lidí, i skrze internet, jde ruku v ruce se studiem vysoké školy a také se s postupem vývoje a také tím, že se využívání informačních a komunikačních technologií stává součásti

běžné mezilidské interakce v dospělosti. To všem nemění nic na tom, že takovéto schůzky by neměly být stále vnímány jako potencionálně rizikové.

H4: Dotázané ženy se staly obětí kyberšikany více jak čtyřikrát častěji než muži.

Tato hypotéza byla stanovena na základě výzkumu J. Šmahaje (2014) „Kyberšikana jako společenský problém", který se ve své empirické části zabývá zejména popisem a analýzou možných souvislostí mezi vybranými duševními stavy, procesy aosobnostními charakteristikami zejména pak obětí kyberšikany se zaměřením jak na žáky 2. stupně ZŠ, středních škol a gymnázií, ale také na studenty škol vysokých. A z otázky *„zjistit, zda jsou u obětí kyberšikany rozdíly z pohledu pohlaví a věku*, vyplývá, že *„častějšími oběťmi kyberšikany jsou ženy (v poměru 4 : 1), v průměrném věku 22,53 let*".

H5: Více než polovina dotázaných se setkala s nenávistnými projevy na internetu.

Hypotéza č. 6 byla stanovena na základě výzkumu z roku 2020 EU Kids Online, kde na 59 % dotázaných dětí ve věku od 11 do 17 let uvedlo, že se v posledních 12 měsících setkalo na internetu s nenávistnými nebo ponižujícími zprávami či komentáři. Smutnou zajímavostí je dle mého názoru také ten fakt, že z 10 evropských zemí, které byly do výzkumu zapojeny, se s touto formou rizikové komunikace naše děti setkávali napříč zúčastněnými zeměmi nejvíce.

H6: Prevalence provozování sextingu s přibývajícím věkem respondentů stoupá minimálně o 10 %.

Hypotéza č. 4 se opírá opět o výzkumy z let 2011, 2013 a 2015 Kamila Kopeckého, kdy v prvním zmíněném výzkumu se přiznalo 9,15 % dětí k nahrání svého intimně laděného videa či fotografie na internet a 10,44 % odeslalo takovýto materiál někomu jinému. Ve výzkumu z roku 2015 pak byly bilance takové, že stejný obsah na internet přidalo jen 7,41 % dětí, ale poslalo ho 12,14 % respondentů ve věku od 11 do 17 let. Oproti tomu stojí výzkumy vysokoškolských studentů PdF UPOL z roku 2013, kdy 12,42 % dotázaných uvedlo, že svá intimně laděná videa a fotografie přidává na internet a 23,28 % pak odesílá takovéto materiály skrze internetové služby jiným lidem. A například v roce 2016 dle průzkumu magazínu Studenta již intimně laděnou fotgrafii či video odeslalo někomu jinému téměř 32 % dotázaných vysokoškoláků.

Stanovené hypotézy byly následně ověřovány pomocí jednotlivých položek výzkumného šetření, jež bylo realizováno online dotazníkem. Ten byl šířen skrze sociální

sítě a sběr dat probíhal během měsíce března roku 2023. Dotazník se skládal z celkem tří sekcí, kdy první z nich obsahovala otázky demografického charakteru. Následovala sekce zaměřená na zkoumání zkušeností s jednotlivými druhy rizikové komunikace v online prostředí. Položky v této sekci dotazníku měly výčtový charakter, které jsou dle Chrásky (2016) charakteristické možností volby několika odpovědí najednou. Třetí sekce dotazníkového šetření se skládala z uzavřených a polouzavřených otázek, které měly za cíl doplnit zjištěné informace z předchozí sekce.

3.2 Výzkumný soubor

V této podkapitole budou přiblíženy zejména demografické údaje charakterizující výzkumný soubor, který se do výzkumného šetření zapojil. V online dotazníkovém šetření na tyto demografické údaje byly zaměřeny celkem tři otázky, kdy první se týkala věku dotázaných, jelikož šetření bylo určené konkrétní věkové kategorii, která odpovídá charakteristikám současných vysokoškolských studentů. Následovala otázka zaměřená na pohlaví respondentů, které měla spíše informativní charakter a poslední položkou první sekce dotazníkového šetření byla otázka zaměřující se na studovanou vysokou školu, jelikož toto bylo dalším atributem pro participaci ve výzkumném šetření.

Tabulka 1 *Věkové zastoupení výzkumného souboru*

Věk	Počet	Procenta
18-20	48	16,1 %
21-23	194	64,9 %
24-27	56	18,7 %
33	1	0,3 %
Celkem	299	100 %

Dotazníkového šetření se zúčastnilo celkem 299 osob, kdy nejvíce respondentů bylo ve věkové kategorii 21-23 let. Celkem byla tato věková kategorie reprezentována 194 lidmi. Nejméně byla zastoupena věková kategorie 18-20 let, a to celkem 48 respondenty a dále věková kategorie 24-27 let, reprezentována 56 respondenty. Samostatně pak stojí respondent, který uvedl do políčka „věk“ číslo 33, což se výrazně vymyká věkové hranici, která byla pro toto dotazníkové šetření vymezena, a to věkem od

19 do 26 let. Z toho důvodu byl tento jedinec vyřazen z celkového počtu respondentů. K tomu se přistoupilo z toho důvodu, že by se dalo pochybovat o jeho zkušenostech s dále v dotazníku zkoumanými jevy. Následně je totiž mapována zkušenost s online rizikovou komunikací již na základní škole a přeci jen v době, kdy byl tento respondent žákem ZŠ, by se dalo pochybovat o celkové dostupnosti online připojení, a tedy i zkušeností s rizikovou komunikaci v online prostředí. Po vyřazení tohoto jednoho respondenta se snížil celkový počet respondentů na **298.**

Tabulka 2 *Pohlaví respondentů*

Pohlaví	Počet	Procenta
Žena	244	81,9 %
Muž	53	17,8 %
Jiné	1	0,3 %
Celkem	298	100 %

Dotazníkového šetření k bakalářské práci se zúčastnilo celkem 299 osob, kdy následně jedna z důvodu velkého věkového rozdílu byla vyřazena. Z celkového počtu 298 respondentů se pak jednalo konkrétně o 244 žen, 53 mužů a jedna osoba využila možnosti vyplnit kolonku „jiné“, ovšem ne zcela relevantním způsobem, kdy uvedla pohlaví „cedník“. Z toho důvodu byl tento respondent z celkového počtu také vyřazen, pro možnou nedůvěryhodnost jeho odpovědí**.** Konečný počet respondentů, z jejichž odpovědí výzkumné šetření vychází se tedy rovná **297.**

Další položkou v dotazníkovém šetření byla otázka na studovanou vysokou školu. Z této položky vyplynulo, že nejvíce, konkrétně 151 respondentů, bylo studenty Univerzity Hradec Králové, druhá nejčastěji zmiňovaná byla Univerzita Karlova a to konkrétně 20 respondenty a na 3 místě v četnosti zastoupení se umístila Vysoká škola ekonomická s 13 respondenty. Dále se pak objevovali respondenti již spíše v řádech jednotek z dalších univerzit a vysokých škol v ČR a jeden respondent z Žilinské univerzity na Slovensku.

3.3 Analýza a interpretace výsledků

V této podkapitole budou podrobněji rozebrány výsledky druhé části dotazníkového šetření, která již nebyla zaměřena na demografické složení respondentů, ale právě na samotnou prevalenci rizikové komunikace v online prostředí studentů

vysokých škol. Nejprve půjde o zkušenosti respondentů s rizikovou komunikací online v jednotlivých etapách jejich života. Pro lepší vybavení si a následné zařazení zkušeností respondentů byly tyto životní etapy rozděleny do tří stupňů v kontextu dosavadní školní docházky. Jednalo se tedy o období základní, střední a vysoké školy.

Nutno dodat, že následující výsledky šetření porovnávají počty odpovědí neboli zkušeností respondentů s daným jevem, nikoli počty respondentů samotných.

Otázka č. 1 a 2 se zaměřuje na manipulativní chování jako takové, se kterým je možné setkat se při internetové komunikaci. **H1 se nepřijímá,** jelikož v ani jedné ze zkoumaných položek nedominuje počet souhlasných odpovědí za období základní školy, kdy právě tito žáci jsou tedy v kontextu školní docházky těmi nejmladšími uživateli internetu. U tohoto souboru otázek dominuje období střední školy. Tabulka obsahuje pouze odpovědi respondentů, kteří zaškrtli alespoň jednu z možností „ZŠ, SŠ, VŠ". Pro lepší orientaci v tabulce se v ní nenachází počet ani procentuální zastoupení respondentů, kteří se s jevem nikdy nesetkali, ale tento údaj se nachází v poznámce pod tabulkou. Tabulka tudíž vychází z odpovědí ze zbývajícího počtu 203 (68,4 %) a 109 (36,7 %) respondentů.

Tabulka 3 *Manipulativní chování skrze internetovou komunikaci*

Konkretizace otázky	ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
Snaha vylákat z Vás osobní informace/intimní materiály	121	40,7 %	153	51,5 %	53	17,8 %
Snaha vylákat Vás na osobní schůzku	58	53,2 %	74	67,9 %	29	26,6 %

Pozn.: V prvním případě označilo možnost „nikdy" 94 respondentů (31,6 %), v druhém jich tuto možnost označilo 188 (63,3 %).

Následovaly otázky č. 3 a 4, které se vztahovaly ke konkrétní podobě manipulativní komunikace v prostředí internetu, a to k prevalenci phishingu. První z otázek se vztahovala k **hypotéze č. 2, která se tímto přijímá,** jelikož s phishingem se z celkového vzorku respondentů nesetkalo pouze 32 respondentů (10,8 %) a zbývajících 265 respondentů (89,2 %) nějakou osobní zkušenost s tímto jevem v určité zkoumané etapě mělo.

Tabulka 4 *Obdržení phishingové zprávy*

Otázka č. 3: Obdrželi jste někdy podvodný (phishingový) e-mail nebo zprávu na soc. síti?					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
146	49,2 %	233	78,5 %	187	63 %

Pozn.: Možnost „nikdy“ označilo v tomto případě 32 respondentů (10,8 %).

Následovala otázka, která zkoumala, zdali se dotázaní stali obětí tohoto druhu manipulativní internetové komunikace, tak že se internetovým útočníkům opravdu podařilo odcizit osobní údaje respondentů tohoto výzkumného šetření. V tomto případě již nebyla prevalence souhlasných odpovědí zdaleka tak vysoká jako u předchozí otázky, jelikož obětí se z celkového počtu respondentů stalo pouze 38 respondentů (12,8 %).

Tabulka 5 *Oběti phishingu*

Otázka č. 4: Stali jste se obětí phishingu? (zcizení osobních údajů vlivem podvodných e-mailů/zpráv)					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
12	4 %	21	7,1 %	15	5,1 %

Pozn.: Možnost „nikdy“ označilo v tomto případě 259 respondentů (87,2 %).

K těmto dvěma otázkám zaměřeným na phishing se dále vztahuje doplňující otázka z 3. sekce dotazníkového šetření „Skrze jakou komunikaci se nejčastěji setkáváte s podvodnými zprávami?“. Z výsledků této položky vyplývá, že nejčastěji se s těmito zprávami respondenti setkávají ve zprávách na sociálních sítích, kdy tuto možnost označilo celkem 159 respondentů (53,5 %). Dále pak skrze e-mailovou komunikaci, tu označilo 116 dotázaných (39,1 %). Chatovací místnosti označilo 8 respondentů (2,7 %) a jiné platformy 5 dotázaných (1,7 %)

Tabulka 6 *Nejčastější forma setkání s podvodnou zprávou*

Skrze jakou komunikaci se nejčastěji setkáváte s podvodnými zprávami		
E-maily	116	39,1 %
Zprávy na sociálních sítích	159	53,5 %
Chatovací místnosti	8	2,7 %
Jiná (internetové bazary, SMS zprávy, …)	5	1,7 %

Nikdy jsem se s ničím takovým nesetkal/a	9	3 %
Celkem	297	100 %

Soubor následujících čtyř otázek se dále věnuje problematice kybergroomingu, kdy v první z nich bylo cílem zmapovat, zdali byli respondenti pozváni na osobní schůzku s neznámým člověkem z internetu v některém ze zkoumaných období a souhlasně odpovědělo celkem 152 dotázaných (51,2 %).

Tabulka 7 *Pozvání na osobní schůzku s neznámým člověkem z internetu*

Otázka č. 5: Byli jste někdy pozváni na osobní schůzku s neznámým člověkem, kterého jste potkali na internetu?					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
64	21,5 %	111	37,4 %	67	22,6 %

Pozn.: Možnost „nikdy“ označilo v tomto případě 145 respondentů (48,8 %).

Následující otázka měla za cíl v návaznosti na předcházející otázku zjistit, zdali respondenti a neznámí uživatelé internetu uskutečnili společnou schůzku. V tomto případě potvrdilo celkem 123 respondentů (41,4 %), že se opravdu s neznámým člověkem z internetu osobně setkali.

Tabulka 8 *Setkání s neznámým člověkem z internetu*

Otázka č. 6: Setkali jste se s neznámým člověkem, kterého jste poznali na internetu?					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
15	5,1 %	86	29 %	65	21,9 %

Pozn: Možnost „nikdy“ označilo v tomto případě 174 respondentů (58,6 %).

Položka č. 7 se vztahuje **k H3, která se tímto nepřijímá**, jelikož ačkoli je v následující tabulce vidět nárůst odpovědí respondentů v období střední školy oproti škole základní, tak tato vzrůstající tendence nepřetrvává do období vysoké školy a naopak opět mírně klesá. Tabulka čítá odpovědi od celkem 119 respondentů (40,1 %), kteří tedy byli ochotni se s neznámým člověkem z internetu setkat, bez ohledu na to, zdali k setkání nakonec opravdu došlo či nikoli.

Tabulka 9 *Ochota setkat se s neznámým člověkem z internetu*

Otázka č. 7: Byli jste ochotni se s takovým člověkem setkat, i když k setkání samotnému nakonec nemuselo dojít?					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
18	6,1 %	82	27,6 %	59	19,9 %

Pozn.: Možnost „nikdy“ označilo v tomto případě 178 respondentů (59,9 %).

Následující položka v dotazníkovém šetření měla spíše doplňující charakter k výše položeným otázkám, jelikož mířila na vlastní iniciativu dotázaných se s neznámým člověkem setkat. Celkem se za iniciátora osobní schůzky považuje 74 dotázaných (24,9 %).

Tabulka 10 *Respondenti v roli iniciátorů schůzky*

Otázka č. 8: Byli jste někdy Vy iniciátorem osobní schůzky s neznámým člověkem z internetu?					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
14	4,7 %	45	15,2 %	34	11,4 %

Pozn.: Možnost „nikdy“ označilo v tomto případě 223 respondentů (75,1 %).

Následující série čtyř otázek se zabývá problematikou kyberšikany, kdy první z nich zkoumá vlastní zkušenost s rolí oběti. Tato položka se vztahuje k **H4**, **která se tímto přijímá,** jelikož z celkového počtu 66 respondentů (22,2 %), kteří se stali obětí kyberšikany, bylo 53 žen (17,8 %), což je právě více než čtyřnásobek oproti mužům, kterých bylo pouze 13 (4,4 %). Jelikož se tato hypotéza vztahuje k pohlaví respondentů, kteří se stali obětí kyberšikany, tak na ZŠ to bylo konkrétně 37 žen, v období SŠ 20 žen a na vysoké škole 6 žen.

Tabulka 11 *Oběti kyberšikany*

Otázka č. 9: Stali jste se obětí kyberšikany?					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
48	16,2 %	22	7,4 %	6	2 %

Pozn.: Možnost „nikdy“ označilo v tomto případě 231 respondentů (77,8 %).

V případě této otázky bylo dále zjištěno, že celkem 148 dotázaných (49,8 %) má ve svém okolí osobu, která se v některé ze zkoumaných etap stala obětí kyberšikany.

Tabulka 12 *Známí respondentů obětí kyberšikany*

Otázka č. 10: Znáte ve svém okolí někoho, kdo se stal v některém ze zkoumaných období obětí kyberšikany? (stal se jí na ZŠ, SŠ, nebo VŠ?)					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
112	37,7 %	78	26,3 %	12	4 %

Pozn.: Možnost „nikdy“ označilo v tomto případě 149 respondentů (50,2 %).

K otázce výše se následně vztahovala doplňující otázka z třetí sekce dotazníkového šetření ve znění „Pokud víte o někom z Vašeho okolí, kdo se stal obětí kyberšikany, jakého pohlaví byl?“. Z výsledků této položky vyplývá, že ve 113 případech se jednalo o ženu (38 %), v 21 případech se jednalo o muže (7,1 %) a 3 případech se zřejmě oběť neidentifikovala ani jako muž, ani jako žena, a proto dotázaní zvolili možnost jiné (1 %)

Tabulka 13 *Pohlaví obětí kyberšikany z okolí respondentů*

Pokud víte o někom z Vašeho okolí, kdo se stal obětí kyberšikany, jakého pohlaví byl?		
Žena	113	38 %
Muž	21	7,1 %
Jiné	3	1 %
Nikoho takového neznám	160	53,9 %
Celkem	297	100 %

Dále byla problematika kyberšikany zkoumána ještě otázkou č. 11, z jejíchž výsledků vyplývá, že roli agresora si na vlastní kůži vyzkoušelo 22 respondentů (7,4 %). Zajímavé je také na této položce ten fakt, 13 žen a 9 mužů mělo zkušenost s kyberšikanováním někoho jiného. Pozoruhodné je také to, že 7 žen a 5 mužů z těchto, co měli zkušenost s rolí agresora, bylo zároveň i někdy ve svém životě obětí kyberšikany, což je vlastně více než polovina u obou pohlaví.

Tabulka 14 *Respondenti v roli agresora*

Otázka č. 11: Šikanovali jste Vy někdy někoho v kyberprostředí?					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
12	4 %	21	7,1 %	15	5,1 %

Pozn.: Možnost „nikdy“ označilo v tomto případě 275 respondentů (92,6 %).

Následující soubor tří otázek se dále věnoval problematice hatingu, tedy projevům nenávisti online. Položka č. 12. dotazníkového šetření měla za cíl zmapovat, jestli se vůbec dotázaní s jevem jako takovým v prostředí internetu setkali. Na základě této otázky bylo zjištěno, že s hatingem se v některém ze zkoumaných období setkala naprostá většina respondentů, konkrétně 276, což odpovídá 92,3 % z celkem 297 dotázaných.
H5 vztahující se k této položce se tímto přijímá, jelikož všechna zkoumaná období přesahují nadpoloviční zkušenost s daným jevem.

Tabulka 15 *Setkání s nenávistným projevem na internetu*

Otázka č. 12: Setkali jste se s nenávistnými projevy na internetu? (příspěvky na soc. sítích, komentáře pod příspěvky, online diskuze,...)					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
180	60,6 %	254	85,5 %	214	72,1 %

Pozn.: Možnost „nikdy“ označilo v tomto případě 21 respondentů (7,1 %).

Následující položka zjišťovala, zdali se dotázaní stali objektem hatingu v prostředí internetu, na což souhlasně odpovědělo 94 respondentů (31,6 %).

Tabulka 16 *Respondenti objektem nenávistného komentáře*

Otázka č. 13: Byl někdy nenávistný projev ve veřejném prostoru na internetu namířen proti Vám?					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
54	18,2 %	52	17,5 %	30	10,1 %

Pozn.: Možnost „nikdy“ označilo v tomto případě 203 respondentů (68,4 %).

Cílem položky č. 14 bylo dále zjistit, zdali respondenti někdy zaujali roli tzv. „hatera“ a projevili se tak vůči někomu či něčemu na internetu nenávistně. S touto pozicí mělo osobní zkušenost jen pouhý zlomek dotázaných, konkrétně 45 respondentů (15,2 %).

Tabulka 17 *Vlastní projev nenávisti online*

Otázka č. 14: Projevili jste se někdy nenávistně ve veřejném prostou na internetu?					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
29	9,8 %	18	6,1 %	17	5,7 %

Pozn. 1: Možnost „nikdy“ označilo v tomto případě 252 respondentů (84,8 %).

K doplnění zkušeností s problematikou hatingu byly v třetí sekci dotazníkového šetření položeny dvě doplňující otázky č 3 a 4, které zněly: „Jak často se setkáváte s nenávistnými projevy na internetu?“ a „Projevujete se nenávistně ve veřejném prostoru na internetu?“

Tabulka 18 *Frekvence setkávání se a vlastní projevy hatingu v současnosti*

	Doplňující otázka č. 3		Doplňující otázka č. 4	
Vůbec	7	2,4 %	267	89,9 %
Velmi zřídka	56	18,9 %	29	9,8 %
Několikrát do měsíce	98	32,9 %	0	0 %
Několikrát do týdne	77	25,9 %	1	0,3 %
Denně	59	19,9 %	0	0 %
Celkem	297	100 %	297	100 %

Poslední skupina otázek se zaměřovala na zkušenost respondentů s rizikovým jevem zvaným sexting. Z výsledků položky č. 15 vyplynulo, že sexting alespoň v některé ze zkoumaných etap provozovala nadpoloviční většina dotázaných, konkrétně 168 respondentů (56,6 %). K této položce se také vztahovala **H6, která se tímto nepřijímá**, jelikož navzdory tomu, že mezi prvními dvěma zkoumanými etapami byl opravdu nárůst vyšší minimálně o 10 % (jednalo se dokonce o téměř 30% nárůst), tak bohužel mezi druhou a třetí etapou se toto nepotvrdilo a nárůst minimálně o 10 % se nekonal. Naopak v období VŠ klesla hodnota na 29,6 % oproti zkušenostem respondentů ze střední školy, která dosahovala 41,4 %

Tabulka 19 *Provozování sextingu*

Otázka č. 15: Provozovali jste někdy sexting? (zasílání vlastních sexuálně laděných obsahů - fotek, videí, text. zpráv)					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
32	10,8 %	123	41,4 %	88	29,6 %

Pozn.: Možnost „nikdy“ označilo v tomto případě 129 respondentů (43,4 %).

K otázce výše se dále vztahovala poslední doplňující otázka z třetí sekce dotazníkového šetření, která zněla: „Jakým způsobem nejčastěji provozujete sexting?“ Výsledky této položky ukazují, že 149 respondentů (50,2 %) současných vysokoškoláků

v době, kdy bylo šetření realizováno sexting neprovozovalo a největší zastoupení měly odpovědi „intimně laděné textové zprávy“, které označilo na 105 respondentů (35,3 %) a fotografie, které označilo 37 dotázaných (12,5 %). Ve zbývajících 6 případech se pak vždy v zastoupení jednoho respondenta objevovaly odpovědi jako „všechno“, „intimné správy, fotky a videá“, „whatsapp“, „vyzkoušeno pouze jednou“, „videa“ nebo „Tak s lidmi, které osobně znám si občas posíláme yiff“.

Poslední zmíněný termín je označením jak pro zasílání textových zpráv, tak ale například i obrázků s furry tématikou, které také obsahují sexuální podtext, jakožto i samotná zkratka „yiff“, která pochází z anglického spojení „Young Incredibly Fuckable Furry“.

Tabulka 20 *Způsoby provozování sextingu v současnosti*

„Jakým způsobem nejčastěji provozujete sexting?“		
Intimně laděné textové zprávy	105	35,3 %
Fotografie	37	12,5 %
Videa	1	0,3
Jiné	5	1,7
Nikdy jsem sexting neprovozoval/a	149	50,2 %
Celkem	297	100 %

Poslední položkou, která zkoumala prevalenci rizikové komunikace v různých etapách života respondentů, v tomto případě konkrétně sextingu, byla otázka č. 16. Z té vyplynulo, že na 190 respondentů (64 %) obdrželo v některé ze zkoumaných etap nekonsensuální intimně laděný obsah skrze internetovou komunikaci. Zajímavostí by mohlo být, že naprostou většinu, konkrétně 172 z těchto 190 respondentů, tvořily ženy (90,5 %).

Tabulka 21 *Nekonsensuální obdržení intimní zprávy*

Otázka č. 16: Obdrželi jste bez Vašeho souhlasu intimně laděnou zprávu, video či fotografii?					
ZŠ	ZŠ (%)	SŠ	SŠ (%)	VŠ	VŠ (%)
94	31,6 %	160	53,9 %	83	27,9 %

Pozn.: Možnost „nikdy“ označilo v tomto případě 107 respondentů (36 %).

3.4 Shrnutí výsledků

Z mého pohledu je velmi zajímavé zjištění, že v 11 z celkových 16 položek, které byly zaměřeny na zjišťování prevalence rizikové komunikace v různých etapách života respondentů, se stalo nejrizikovějším obdobím období střední školy. To by podle mého názoru mohlo být znakem toho, že prevence, která by se týkala ohrožení v kyberprostředí, by měla být zaměřena jak zejména na žáky základních škol, tak ale i na studenty škol středních, na které by se rozhodně v tomto ohledu nemělo zapomínat. Jak je z výsledků tohoto výzkumného šetření zřejmé, online rizikovou komunikací jsou nejčastěji ohroženi právě studenti středních škol. To ale může být dáno i tou skutečností, že období střední školy je z pohledu rizikového chování jako celku, pravděpodobně nejrizikovějším, jelikož studenti jsou v tomto věku nejvíce ohroženi rozvojem syndromu rizikového chování v dospívání.

Dále u položek, které měly za cíl sledovat i zastoupení respondentů dle pohlaví, dominovaly ženy. V položce č. 9 byly více než čtyřikrát častěji obětí kyberšikany než muži nebo v naprosté většině se staly objektem rizikové online komunikace, co se poslední položky týče.

3 hypotézy z 6 přijaty vlivem výsledků dotazníkového šetření nebyly. Jednalo se konkrétně o H1, H3 a H6. První z těchto hypotéz se věnovala zkušenostem s manipulativním chováním jako takovým a nepodařilo se potvrdit, že by s tímto druhem online rizikové komunikace měly největší zkušenosti dotázaní z doby, kdy navštěvovali základní školu. Druhá hypotéza z nepřijatých se orientovala na ochotu setkat se s neznámým člověkem z internetu. V této hypotéze bylo cíleno na předpoklad, že nejvíce ochotni by měli být studenti v období vysoké školy, jelikož již dosáhli dospělosti a na případná rizika takovéto schůzky by měli být schopni eliminovat, a tudíž být schopni bez obav se tohoto setkání zúčastnit. Třetí hypotéza která nebyla přijata, byla H6, jež cílila podobně jako H3 na ten předpoklad, že opět nejvíce zkušeností budou mít se zkoumaným jevem respondenti z období vysoké školy. Zkušenost sice z období ZŠ do období SŠ měla vzrůstající tendenci, ta už ale bohužel nepokračovala do posledního zkoumaného období, a tudíž ani tato hypotéza nemohla být přijata. Hypotézy č. 2, 4 a 5 přijaty byly, což bylo milým překvapením.

Závěr

Tato práce se zaměřila na prevalenci rizikové komunikace v online prostředí u studentů vysokých škol. Poznatky vyvozuje z realizovaného výzkumného šetření, které bylo distribuováno cílové skupině pomocí sociálních sítí ve formě online dotazníku.

Na začátku práce bylo definováno, kdo je považován za studenta vysoké školy. Je to tedy někdo, kdo své vysokoškolské studium započal bezprostředně po dokončení středoškolského vzdělání. Dále je specifikováno, že tito studenti jsou narozeni po roce 1995, tudíž patří do generace Z. Z hlediska vývojové psychologie nebylo přesné ukotvení studenta vysoké školy možné, jelikož ani literatura na tyto osoby nemá jednotné stanovisko. Tato skupina osob totiž bilancuje mezi obdobím adolescence a mladé dospělosti.

Následně byl nastíněn vztah studentů vysokých škol k online prostředí a zejména pak sociálním sítím. Jelikož je cílová skupina označována za digitální domorodce, online prostředí a pohyb v něm je tudíž součástí jejich každodenního života.

Dále byly představeny a definovány různé druhy rizikové komunikace v online prostředí. Mezi definovanými byla například kyberšikana kybergrooming, sexting. Dalšími zmíněnými druhy rizikové komunikace byly kromě dalších i phishing nebo hating.

Praktická část práce byla zaměřena na zkušenosti vysokoškolských studentů s rizikovou komunikací v online prostředí. Tyto zkušenosti byly mapovány pomocí výzkumného šetření realizovaného skrz online dotazník, ke kterému měli respondenti přístup na vybraných sociálních sítích. Dotazník vyplnilo celkem 299 respondentů. Z tohoto počtu byli 2 dotazovaní vyřazeni z důvodu nesplnění věkové hranice stanovené pro účely této práce a z důvodu nerelevantnosti uvedeného pohlaví. Celkově se dotazníkového šetření zúčastnilo na 244 žen a 53 mužů z nejrůznějších vysokých škol v ČR, kdy největší zastoupení měla právě Univerzita Hradec Králové s celkem 151 vyplněnými dotazníky.

Hlavním cílem práce bylo zjistit jaké zkušenosti mají studenti vysokých škol s rizikovou komunikací v online prostředí, což se dle mého názoru podařilo. Pomocí dotazníkového šetření se ukázalo, že nejvíce zkušeností mají s rizikovou komunikací současní studenti vysokých škol z období studia na střední škole. Toto období totiž dominovalo v 11 z celkových 16 položek, které byly zaměřeny na zkoumání zkušeností v různých etapách života respondentů se zkoumanými rizikovými jevy. Dle těchto

výsledků by se tedy mohlo jednat o nejrizikovější období v životě dotázaných. Tento výsledek mě osobně poněkud překvapil, jelikož jsem žila v domnění, že vlivem útlého věku a nezkušeností s prostředím internetu jako takového bude nejrizikovějším obdobím základní škola.

Seznam použitých zdrojů

Tištěné zdroje

AMBROŽOVÁ, Petra. *Nové formy školního podvádění a vyrušování v kontextu digitálního vzdělávání*. Červený Kostelec: Pavel Mervart, 2020. 229 s. ISBN 978-80-7465-451-0.

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

ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Psyché (Grada). Praha: Grada, 2013. 152 s. ISBN 978-80-210-6374-7.

DIVÍNOVÁ, Radana. *Cybersex: forma internetové komunikace*. Praha: Triton, 2005. 168 s. ISBN 80-7254-636-8.

DULOVICS, Mário, GALKOVÁ, Lucia a ZOŠÁKOVÁ, Karina. *Vybrané virtuálne ohrozenia stredoškolskej mládeže vo voľnom čase*. Banská Bystrica : BELIANUM. ISBN 978-80-557-1905-4.

ECKERTOVÁ, Lenka a DOČEKAL, Daniel. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče*. 1. vyd. Brno: Computer Press, 2013. 224 s. ISBN 978-80-251-3804-5.

GAVORA, Peter. *Úvod do pedagogického výzkumu*. Překlad Vladimír Jůva a Vendula Hlavatá. 2., rozš. české vyd. Brno: Paido, 2010. 261 s. ISBN 978-80-7315-185-0.

HELDAL, Frode a STIKLESTAD, Trond. Sněhové vločky – týmové učení jako nástroj; nejste lepší než vaše skupina. In: ZÁVODNÁ, Lucie Sára, a FALCH, Torberg, ed. *Výuka generace sněhových vloček: nové metody a výzvy: sborník příspěvků z kulatého stolu*. Praha: Vysoká škola ekonomická v Praze, Nakladatelství Oeconomica, 2022. s. 117–134. ISBN 978-80-245-2452-8.

HELSPER, Ellen, Johanna. *Digital Natives and ostrich tactics? The possible implications of labelling young people as digital experts* [online]. 2008 [cit. 2023-01-13]. Available from:

https://www.researchgate.net/publication/41185477_Digital_Natives_and_ostrich_tactics_The_possible_implications_of_labelling_young_people_as_digital_experts.

HNILICA, Karel, ed. *Stereotypy a legitimizace sociální stratifikace*. Praha: Univerzita Karlova, Pedagogická fakulta, 2018. 331 s. ISBN 978-80-7290-996-4.

HOLLÁ, K. 2016. *Sexting a kyberšikana*. Bratislava: IRIS. 166 s. ISBN 978-80-8153-061-6.

CHRÁSKA, Miroslav. *Metody pedagogického výzkumu: základy kvantitativního výzkumu.* 2., aktualizované vydání. Pedagogika (Grada). Praha: Grada, 2016. 254 s. ISBN 978-80-247-5326-3.

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

KOPECKÝ, Kamil. *Moderní trendy v elektronické komunikaci.* Olomouc: Hanex, 2007. 98 s. ISBN 978-80-85783-78-0.

KOPECKÝ, Kamil a kol. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. 1. vydání. Olomouc: Univerzita Palackého v Olomouci, 2015. 169 stran. ISBN 978-80-244-4861-9.

KOPECKÝ, Kamil. *Rizikové chování studentů Pedagogické fakulty Univerzity Palackého v prostředí internetu*. 1. vyd. Olomouc: Univerzita Palackého v Olomouci, 2013. 110 s. ISBN 978-80-244-3858-0.

KOPECKÝ, Kamil a MIKULCOVÁ, Klára. *Aktuální problémy mediální výchovy a mediální gramotnost žáků 2. stupně ZŠ*. 1. vydání. Olomouc: Univerzita Palackého v Olomouci, 2020. 119 stran. ISBN 978-80-244-5900-4.

KOPECKÝ, Kamil; SZOTKOWSKI, René a DOBEŠOVÁ, Pavla. *Riziková komunikace a seznamování českých dětí v kyberprostoru*. Olomouc: Univerzita Palackého v Olomouci, 2021. 111 s. ISBN 978-80-244-5914-1.

MAREŠ, Jiří. *Pedagogická psychologie*. Praha: Portál, 2013. 98 s. ISBN 978-80-262-0174-8.

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

ŠMAHAJ, Jan. *Kyberšikana jako společenský problém: Cyberbullying as a social problem.* Olomouc: Univerzita Palackého v Olomouci, 2014. 234 s. ISBN 978-80-244-4227-3.

ZÁVODNÁ, Lucie, Sára. Je generace sněhových vloček citlivější? Výzkum nové generace studentů. In*:* ZÁVODNÁ, Lucie Sára a FALCH, Torberg (ed.). *Výuka generace sněhových vloček: nové metody a výzvy: sborník příspěvků z kulatého stolu*. Praha: Vysoká škola ekonomická v Praze, nakladatelství Oeconomica, 2022. s. 9–24. ISBN 978-80-245-2452-8.

ZÁVODNÁ, Lucie Sára a FALCH, Torberg (ed.). *Výuka generace sněhových vloček: nové metody a výzvy: sborník příspěvků z kulatého stolu*. Praha: Vysoká škola ekonomická v Praze, nakladatelství Oeconomica, 2022. 185 s. ISBN 978-80-245-2452-8.

Elektronické zdroje

AVAST. Téměř čtvrtina Čechů se setkala s phishingovým útokem. In: Avast. Software s.r.o.. *Avast* [online]. 2020 [cit. 2023-02-22]. Dostupné z: https://press.avast.com/cs-cz/temer-ctvrtina-cechu-se-setkala-s-phishingovym-utokem

BOYD, Danah, M. and ELLISON, Nicole, B. Social Network Sites: Definition, History, and Scholarship, *Journal of Computer-Mediated Communication* [online]. 2007, vol. 13, no. 1, pp. 210–230 [cit. 2023-02-22]. Available from: https://doi.org/10.1111/j.1083-6101.2007.00393.x.

ČERMÁK, Miroslav. Spear phishing je cílený phishing, kterému se lze jen těžko bránit. In: Miroslav Čermák. *Clever and smart* [online]. 2012. [cit. 2023-02-15]. Dostupné z: https://www.cleverandsmart.cz/spear-phishing-je-cileny-phishing-kteremu-se-lze-jen-tezko-branit/.

DÖRING, Nicola. Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting? In: *Cyberpsychology Journal of Psychosocial Research on Cyberspace* [online]. 2014, vol. 8, no. 1 [cit. 2023-02-15]. Available from:

https://www.researchgate.net/publication/272852535_Consensual_sexting_among_adolescents_Risk_prevention_through_abstinence_education_or_safer_sexting.

DVOŘÁKOVÁ, Michaela. Revenge porn a deepfakes: Ochrana soukromí v éře moderních technologií. *Revue pro právo a technologie* [online]. Brno Masarykova univerzita, 2020, roč. 11, č. 22, s. 51–89. [cit. 2023-02-22]. ISSN: 1805-2797. Dostupné z: https://journals.muni.cz/revue/article/view/13416/pdf.

DYIKUK, Justine, J. The Digital Age: Bridging the Communication Gap Between Digital Natives and Digital Immigrants. *Sumerianz Journal of Social Science* [online]. 2019, vol. 2, no. 1, pp. 13–19 [cit. 2023-02-22]. Available from: https://www.sumerianz.com/?ic=journal-home&info=archive-detail&journal=28&month=01-2019&issue=1&volume=2.

E-BEZPEČÍ. Revenge porn (porno-pomsta). In: *YouTube* [online video]. 16. 11. 2021 [cit. 2023-02-15]. https://www.youtube.com/watch?v=joK4pVU1xkQ&t=233s.

HINDUJA, Sameer, PATCHIN, Justin, W. Bullies Move beyond the Schoolyard: A Preliminary Look at Cyberbullying. In: *Youth Violence and Juvenile Justice* [online]. 2006, vol. 4, pp. 148-169 [cit. 2023-02-22]. Available from: https://doi.org/10.1177/1541204006286288.

https://doi.org/10.1177/1541204006286288 [online]. 2006 [cit. 2023-02-22].

HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech.* [online]. Praha, 2012.145 s. [cit. 2023-02-22].
Dostupné z: https://dspace.cuni.cz/bitstream/handle/20.500.11956/44778/RPTX_2011_1_11210_0_369503_0_120488.pdf?sequence=1. Rigorózní práce. Univerzita Karlova v Praze. Filozofická fakulta. Vedoucí práce Prof. PhDr. Šulová Lenka, CSc.

JONES, Chris and SHAO, Binhui. The Net Generation and Digital Natives: Implications for Higher Education. In: ResearchGate. *ResearchGate* [online]. 2011 [cit. 2023-02-22]. Available from https://www.researchgate.net/publication/277243597_The_Net_Generation_and_Digital_Natives_Implications_for_Higher_Education.

KNYTL, Martin a KŘIVÁNKOVÁ, Lucie. Typografie & odborný text: průvodce pro zpracování nejen závěrečných prací. Druhé, aktualiz. a rozš. vyd. Hradec Králové: Gaudeamus, 2022. 286 s. ISBN 978-80-7435-875-3.

KOPECKÝ, Kamil. Poradna projektu E-Bezpečí pro oběti kybernetické kriminality zaznamenala za 1. čtvrtletí roku 2021 ve srovnání s předchozím rokem téměř čtyřicetiprocentní nárůst počtu případů. Dominantní jsou pak případy spojené se zneužitím intimního obsahu. In: Centrum prevence rizikové virtuální komunikace, Pedagogická fakulta Univerzity Palackého v Olomouci. E-*Bezpečí* [online]. Olomouc: Univerzita palackého v Olomouci, 2021a [cit. 2023-02-22]. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=2186.

KOPECKÝ, Kamil. Co je sextortion. In: Centrum prevence rizikové virtuální komunikace, Pedagogická fakulta Univerzity Palackého v Olomouci. E-*Bezpečí* [online]. Olomouc: Univerzita palackého v Olomouci, 2021b [cit. 2023-02-22]. Dostupné z: https://www.e-bezpeci.cz/index.php/71-trivium/2421-co-je-sextortion.

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

O´KEEFFE, Gwen, Schuring and CLARKE-PEARSON, Kathleen. The Impact of Social Media on Children, Adolescents, and Families. *American Academy of Pediatrics* [online]. 2011, vol. 127, no. 4 [cit. 2023-01-13]. Available from: https://publications.aap.org/pediatrics/article/127/4/800/65133/The-Impact-of-Social-Media-on-Children-Adolescents?autologincheck=redirected.

PRENSKY, Marc. *Digital Natives, Digital- Immigrants* [online]. *2001* [cit. 2023-01-13]. Available from: https://webcitation.org/5eBDYI5Uw.

SLÍŽEK, David. Seznam.cz upravuje nové Lide.cz a bezděčně stvořil vlastní Messenger. In: INTERNET INFO. *Lupa.cz* [online]. 2014 [cit. 2023-02-22]. Dostupné z: https://www.lupa.cz/clanky/seznam-cz-upravuje-nove-lide-cz-a-bezdecne-stvoril-vlastni-messenger/.

SMITH, Peter, K., del BARRIO, Cristina, TOKUNAGA, Robert. Definitions of bullying and cyberbullying: How useful are the terms?. In: ResearchGate. *ResearchGate* [online]. 2013 [cit. 2023-02-22]. Available from: https://www.researchgate.net/publication/301924784_Definitions_of_bullying_and_cyberbullying_How_useful_are_the_terms.

ŠMAHEL, D., MACHÁČKOVÁ, H., MASCHERONI, G., DĚDKOVÁ, L., STARKSRUD E., ÓLAFSSON, K., LIVINGSTONE, S., and HASEBRINK, U. EU *Kids Online 2020: Survey results from 19 countries*. *EU Kids Online* [online]. 2020 [cit. 2023-02-22]. Available from: https://doi.org/10.21953/lse.47fdeqj01ofo.

VODAFONE. Jak poznám podvodné hovory (vishing)? In: Vodafone Czech Republic a.s. *Vodafone* [online]. 2023 [cit. 2023-10-30]. Dostupné z: https://www.vodafone.cz/pece/muj-ucet-cislo/bezpecnost/vishing-podvodne-hovory/.

WAQAS, Ahmed, SALAMINEN, Joni, JUNG, Soon-gyo, ALMEREKHI, Hind and JANSEN, Bernard J. Mapping online hate: A scientometric analysis on research trends and hotspots in research on online hate. In: *Plos one* [online]. 2019 [cit. 2023-02-30]. Available from: https://doi.org/10.1371/journal.pone.0222194.

Seznam tabulek

Přílohy

Příloha A: **Dotazník**

Dobrý den,

jmenuji se Tereza Ťopková a jsem studentkou 3. ročníku oboru Sociální patologie a prevence na Univerzitě Hradec Králové. Tímto bych Vás chtěla požádat o vyplnění následujícího krátkého dotazníkového šetření, jehož výsledky budou využity v rámci mé bakalářské práce. Dotazník je určen pro studenty vysokých škol ve věku od 19 do 26 let a je zcela anonymní.

Předem děkuji za Váš čas.

Sekce 1: Demografické údaje

Jakého jste pohlaví?

a) Žena
b) Muž
c) ……

Jaký je Váš věk?

……

Jakou studujete vysokou školu?

……

Sekce 2: Zkušenosti s rizikovou komunikací

Odpovězte na následující otázky zaškrtnutím políčka/více políček v každém řádku, pokud jste se s daným jevem setkali v některém ze zkoumaných období. (Nikdy, ZŠ, SŠ, VŠ)				
	Nikdy	ZŠ	SŠ	VŠ
Setkali jste se s manipulativním chováním skrze internetovou komunikaci? (lákání k zasílání osobních informací/intimních materiálů)				
Setkali jste se s manipulativním chováním skrze internetovou komunikaci, kdy se Vás někdo snažil vylákat na osobní schůzku?				
Obdrželi jste někdy podvodný (phishingový) e-mail nebo zprávu na soc. síti?				

Stali jste se obětí phishingu? (zcizení osobních údajů vlivem podvodných e-mailů/zpráv)				
Byli jste někdy pozváni na osobní schůzku s neznámým člověkem, kterého jste potkali na internetu?				
Setkali jste se s neznámým člověkem, kterého jste poznali na internetu?				
Byli jste ochotni se s takovým člověkem setkat, i když k setkání samotnému nakonec nemuselo dojít?				
Byli jste někdy Vy iniciátorem osobní schůzky s neznámým člověkem z internetu?				
Stali jste se obětí kyberšikany?				
Znáte ve svém okolí někoho, kdo se stal v některém ze zkoumaných období obětí kyberšikany? (stal se jí na ZŠ, SŠ, nebo VŠ?)				
Šikanovali jste Vy někdy někoho v kyberprostředí?				
Setkali jste se s nenávistnými projevy na internetu? (příspěvky na soc. sítích, komentáře pod příspěvky, online diskuze,...)				
Byl někdy nenávistný projev ve veřejném prostoru na internetu namířen proti Vám?				
Projevili jste se někdy nenávistně ve veřejném prostou na internetu?				
Provozovali jste někdy sexting? (zasílání vlastních sexuálně laděných obsahů - fotek, videí, text. zpráv)				
Obdrželi jste bez Vašeho souhlasu intimně laděnou zprávu, video či fotografii?				

Sekce 3: Doplňující otázky

Skrze jakou komunikaci se nejčastěji setkáváte s podvodnými zprávami?

a) E-maily
b) Zprávy na sociálních sítích
c) Chatovací místnosti
d) Nikdy jsem se s ničím takovým nesetkal/a

e) ……..

Pokud víte o někom z Vašeho okolí, kdo se stal obětí kyberšikany, jakého pohlaví byl?

a) Muž
b) Žena
c) Jiné
d) Nikoho takového neznám

Jak často se setkáváte s nenávistnými projevy na internetu?

a) Vůbec
b) Velmi zřídka
c) Několikrát do měsíce
d) Několikrát do týdne
e) Denně

Projevujete se nenávistně ve veřejném prostoru na internetu?

a) Vůbec
b) Velmi zřídka
c) Několikrát do měsíce
d) Několikrát do týdne
e) Denně

Jakým způsobem nejčastěji provozujete sexting?

a) Fotografie
b) Videa
c) Intimně laděné textové zprávy
d) Neprovozuji sexting
e) ……